รายงานฉบับสมบูรณ์

โครงการขอรับการส่งเสริมและสนับสนุนจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ

โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร

Technology Transfer and Human Resource Development of Perfectly Secure Quantum Communications

สุวิทย์ กิระวิทยา และคณะ

ธันวาคม พ.ศ. 2560

กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (สำนักงาน กสทช.)

รายงานฉบับสมบูรณ์

ทุนส่งเสริมและสนับสนุนการวิจัยและพัฒนา
สัญญารับทุนเลขที่ T3-1-0002 / 57

โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร

Technology Transfer and Human Resource Development of Perfectly Secure Quantum Communications

คณะนักวิจัย

1. ผู้ช่วยศาสตราจารย์ ดร. สุวิทย์ กิระวิทยา	นักวิจัยหัวหน้าโครงการ
2. ดร. เกียรติศักดิ์ ศรีพิมานวัฒน์	นักวิจัยร่วม
3. นางสาวจุฑาเพชร เวชรังษี	นักวิจัยร่วม
4. นายปรมินทร์ แสงวงษ์งาม	นักวิจัยร่วม

กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (สำนักงาน กสทช.)

ธันวาคม พ.ศ. 2560

บทสรุปผู้บริหาร

โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร ธันวาคม พ.ศ. 2560

เทคโนโลยีสารสนเทศเชิงควอนตัมคือเทคโนโลยีอุบัติใหม่ที่ประยุกต์ใช้คุณสมบัติเชิงควอนตัมในการจัดการกับข้อมูลข่าวสาร มีการคาดการณ์ว่าเทคโนโลยีนี้จะถูกนำมาใช้ร่วมกับเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบัน ในอีกไม่กี่ปีข้างหน้า โดยเทคโนโลยีนี้แบ่งออกได้เป็น 2 สาขาหลัก คือ การคำนวณเชิงควอนตัม (Quantum Computing) และ การสื่อสารเชิงควอนตัม (Quantum Communication) โดยการสื่อสารเชิงควอนตัมกำลังได้รับความสนใจจากทั่วโลกสำหรับการนำไปใช้ในการเครือข่ายสื่อสารยุคหน้า

การนำเทคโนโลยีเชิงควอนตัมมาใช้ในด้านการสื่อสารโทรคมนาคม มีข้อดีที่เด่นชัดด้านการรักษาความลับในการสื่อสารแบบสูงสุด ซึ่งตัวอย่างที่เด่นชัดในปัจจุบันคือ เทคโนโลยีการเข้าหัสลับเชิงควอนตัมโดยใช้โฟตอนเดี่ยวซึ่งทำให้ข้อมูลที่ส่งมีความปลอดภัยสูง โดยวิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography) เป็นศาสตร์แขนงใหม่ ที่มีการเรียนการสอนในระดับอุดมศึกษาขั้นสูงในหลายประเทศ และกำลังเป็นหัวข้อวิจัยที่ได้รับความสนใจและมีการพัฒนาอย่างรวดเร็ว จากการศึกษาวิจัยตามโครงการนี้ พบว่าศาสตร์ด้านนี้มีการพัฒนาการในด้านเทคนิคต่าง ๆ อย่างรวดเร็ว และได้มีการเริ่มทดสอบการใช้งานของเทคโนโลยีรหัสลับควอนตัมในกิจการโทรคมนาคมของประเทศต่าง ๆ (จีน ญี่ปุ่น ยุโรป และ อเมริกา) แล้ว

โครงการนี้มีวัตถุประสงค์ส่วนหนึ่งเพื่อดำเนินการเพื่อเป็นการติดตามเทคโนโลยีที่ได้รับการพัฒนาการอย่างต่อเนื่อง และ มีแนวโน้มจะถูกนำมาใช้จริงในระบบสื่อสารโทรคมนาคมของโลกผ่านเครือข่ายสื่อสารที่มีอยู่เดิม โดยประเทศไทยมีความจำเป็นอย่างยิ่งยวดในการสร้างกลุ่มบุคลากรให้มีความพร้อมในการรับเทคโนโลยีนี้จากต่างประเทศ รวมถึงการสร้างบุคลากรที่เข้าใจและนำเทคโนโลยีนี้ไปใช้อย่างถูกต้องด้วยการสร้างความเข้าใจสาธารณะในการรองรับเทคโนโลยีการสื่อสารด้วยความปลอดภัยสูงสุดด้วยวิทยาการรหัสลับเชิงควอนตัมอันเป็นเทคโนโลยีพื้นฐานที่มีศักยภาพการสูงในอนาคต โดยการดำเนินการตามโครงการ ได้มีการจัดอบรม สัมมนาในหัวข้อที่ดังกล่าว มีการรวมกลุ่มผู้สนใจในภาคการศึกษาและวิจัย มีการศึกษา แปลและติดตามการพัฒนามาตรฐานรหัสลับควอนตัมของโลก รวมทั้งการจัดทำเอกสารเพื่อสร้างความตระหนักและผลักดันสู่แผนแม่บทที่เกี่ยวข้องของประเทศไทยในอนาคตด้วย ทั้งนี้จะดำเนินการสร้างความร่วมมือและรับการถ่ายทอดเทคโนโลยีจากต่างประเทศ เพื่อการต่อยอดการวิจัยและพัฒนาที่จะสามารถพึ่งพาตนเองกับเทคโนโลยีใหม่นี้ได้ในอนาคตโดยอาศัยความร่วมมือของบุคลากรในระดับปฏิบัติการของสถาบันอื่นๆ ในประเทศด้วย รวมทั้งการจะสร้างผลกระทบให้กว้างขวางขึ้นผ่านทางการบรรยาย ฝึกอบรมและการผลิตสื่อและเอกสารเผยแพร่สาธารณะต่าง ๆ เพื่อการพัฒนาบุคลากรและการเตรียมพร้อมกับเทคโนโลยีอุบัติใหม่ ด้านสารสนเทศเชิงควอนตัมของประเทศไทยสู่ระยะต่อไป

บทคัดย่อ

สุวิทย์ กิระวิทยา

ธันวาคม พ.ศ. 2560

โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร ที่ได้รับการสนับสนุนจากสำนักงาน กสทช. โดยมีวัตถุประสงค์ของการดำเนินโครงการคือ

1. เพื่อสร้างความเข้าใจสาธารณะในการรองรับเทคโนโลยีการสื่อสารด้วยความปลอดภัยสูงสุดด้วยวิทยาการรหัสลับเชิงควอนตัมอันเป็นเทคโนโลยีพื้นฐานที่มีศักยภาพสูงในอนาคต โดยการรวมกลุ่มผู้สนใจทั้งภาคนโยบาย ภาคการศึกษาและวิจัย และผู้ใช้งาน
2. เพื่อศึกษาและติดตามการพัฒนามาตรฐานรหัสลับควอนตัมของโลก รวมทั้งสร้างความตระหนักและผลักดันสู่แผนแม่บทที่เกี่ยวข้องของประเทศไทย
3. เพื่อสร้างความร่วมมือ รับการถ่ายทอดเทคโนโลยีจากต่างประเทศ และต่อยอดการวิจัยและพัฒนาเพื่อพึ่งพาตนเองกับเทคโนโลยีใหม่นี้ได้ในอนาคต
4. เพื่อผลิตสื่อและเอกสารเผยแพร่สาธารณะ เพื่อการฝึกอบรมถ่ายทอดความรู้และการพัฒนาบุคลากร

วิธีการดำเนินโครงการเพื่อให้บรรลุวัตถุประสงค์ของโครงการประกอบด้วยกิจกรรม 3 ด้านคือ

1. การถ่ายทอดเทคโนโลยีจากต่างประเทศ โดยอาศัยความร่วมมือของบุคลากรในระดับปฏิบัติการ โดยประกอบด้วย การบรรยายพิเศษ การร่วมศึกษาและนำเสนอเทคโนโลยีที่เหมาะสมสำหรับประเทศไทย และ การสร้างความร่วมมือทางการวิจัยในระยะยาว

2. การพัฒนาบุคลากร ได้แก่ การจัดทำเอกสารและสื่อออนไลน์เพื่อนำเสนอข้อมูลเชิงเทคนิคระดับพื้นฐานและระดับกลาง การจัดทำการสำรวจสถานะงานวิจัย ทรัพย์สินทางปัญญาของเทคโนโลยีและผลิตภัณฑ์ที่เกี่ยวข้องทั่วโลก (สิทธิบัตร ผลงานตีพิมพ์ ผลิตภัณฑ์ กลุ่มวิจัย อุตสาหกรรม และประเทศที่เกี่ยวข้อง เป็นต้น) และการจัดสัมมนา ฝึกอบรม และ รวมกลุ่มวิจัยเฉพาะทาง

3. การจัดทำสรุปมาตรฐานโลกด้านวิทยาการรหัสลับเชิงควอนตัม โดยประกอบด้วยการแปลและติดตามพัฒนาการของมาตรฐานโลก ที่นำเสนอโดย ETSI (European Telecommunications Standards Institute) การสัมมนารับฟังความคิดเห็นของผู้ที่เกี่ยวข้องกับเทคโนโลยีด้านนี้ (สถานศึกษา – หน่วยงานของรัฐ - ภาคอุตสาหกรรม) และการเผยแพร่และประชาสัมพันธ์การมีและการประยุกต์สำหรับอนาคต

ผลการศึกษาที่แสดงในรายงานนี้ประกอบด้วย รายงานการจัดอบรมและรายงานการเผยแพร่และประชาสัมพันธ์สู่สาธารณะซึ่งแสดงอยู่ในบทที่ 2 รายงานการบรรยายพิเศษโดยผู้เชี่ยวชาญเฉพาะทางและทีมงานในบทที่ 3 รายงานสรุปผลการสัมมนา ฝึกอบรม หรือการประชุมรวมกลุ่มวิจัยเฉพาะทาง และรายงานสรุปผลการสัมมนารับฟังความคิดเห็นของผู้ที่เกี่ยวข้อง (รัฐ อุตสาหกรรม วิชาการ) ในบทที่ 4 นอกจากนี้ ในภาคผนวกได้มีการนำเสนอเอกสาร “เทคโนโลยีสารสนเทศเชิงควอนตัมกับการประยุกต์” ฉบับที่เผยแพร่แล้วในภาคผนวก ก สื่อเผยแพร่ “ควอนตัมกับการสื่อสาร คืออะไร เพื่ออะไร” ในภาคผนวก ข รายงานการสำรวจสถานะทรัพย์สินทางปัญญาของเทคโนโลยีและผลิตภัณฑ์ของทั่วโลกในภาคผนวก ค บทสรุปมาตรฐานรหัสลับควอนตัมโลก พ.ศ. 2557-2558 ในภาคผนวก ง และ รายงานการร่วมศึกษา “อนาคตประเทศไทยกับสารสนเทศเชิงควอนตัม” ในภาคผนวก จ ซึ่งทั้งหมดนี้เป็นเอกสารที่เผยแพร่แล้วตามโครงการนี้

Abstract

Suwit Kiravittaya

December 2017

The project entitled “Technology Transfer and Human Resource Development of Perfectly Secure Quantum Communications” is supported by Office of the National Broadcasting and Telecommunications Commission (NBTC). The objectives of this project are

1. To raise the public awareness of the perfectly secure quantum communication technology, which has a promising potential in the future, by grouping among policy development, education, as well as research sectors.

2. To study and follow the development of quantum cryptography standard in the world. This includes the raising awareness and developing the master plan of Thailand.

3. To establish an international cooperation/technology transfer. Moreover, to further perform research and development by ourselves with this new technology in the future.

4. To produce media and public documents for training, knowledge transfer and human resource development.

In order to achieve the above objectives, three activities are operated within this project:

1. The technology transfer from foreign researchers by using personnel collaborations. It includes organizing special lectures, perform joint study and propose appropriate technology for the long-term research and development in Thailand.

2. Development of human resources, including creating documentation and online media to present technical information on basic and intermediate levels. This includes making a report from the survey research on the intellectual property and technology related products worldwide (patents, publications and related products, industry research groups, etc.) and organizing training seminars and developing specialized research groups.

3. Preparation of a summary of the quantum cryptography standard. This includes the translation and monitoring of the development of global standards proposed by ETSI (European Telecommunications Standards Institute), organizing seminars to hear the opinions of those who involved with this technology (education, state agencies, and the industry) as well as promoting the existence and applications for the future.

Result shown in this report consists of the contents of the seminars (in Chapter 2). In Chapter 3, the summarized reports of the special lectures by experts are presented. Chapter 4 presents a summarized report of the result from the discussion after the seminar and the overall summary of the report from related persons. The appendices show the "Quantum Information Technology and Its Applications" (App. A), Information on "Quantum and Communication: What is it and what is it for?" (App. B), Report on the related intellectual property and product (App. C), the summary of the standard related to quantum security 2014-5015 (App. D) and the report on "the Future of Thailand about the Quantum Information" (App. E). All documents have been publicized according to this project.

สารบาญ

สารบาญ (ต่อ)

สารบาญตาราง

หน้า

สารบาญรูปภาพ

หน้า

สารบาญรูปภาพ (ต่อ)

สารบาญรูปภาพ (ต่อ)

หน้า

สารบาญรูปภาพ (ต่อ)

หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

เทคโนโลยีสารสนเทศเชิงควอนตัม (Quantum Information Technology: Quantum IT) คือ เทคโนโลยีอุบัติใหม่ที่ประยุกต์ใช้คุณสมบัติเชิงควอนตัมในการจัดการกับข้อมูลข่าวสาร มีการคาดการณ์ว่าเทคโนโลยีนี้จะถูกนำมาใช้ร่วมกับเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบัน ในอีกไม่กี่ปีข้างหน้า โดยเทคโนโลยีนี้แบ่งออกได้เป็น 2 สาขาหลัก คือ การคำนวณเชิงควอนตัม (Quantum Computing) และ การสื่อสารเชิงควอนตัม (Quantum Communication) โดยการสื่อสารเชิงควอนตัมกำลังได้รับความสนใจจากทั่วโลกสำหรับการนำไปใช้ในการเครือข่ายสื่อสารยุคหน้า (Next Generation Network: NGN)

การนำเทคโนโลยีเชิงควอนตัมมาใช้ในด้านการสื่อสารโทรคมนาคม มีข้อดีที่เด่นชัดที่สามารถอธิบายด้วยปรากฏการณ์ด้านความเร็วที่สูงขึ้นและการรักษาความลับในการสื่อสารแบบสูงสุด ซึ่งตัวอย่างที่เด่นชัดในปัจจุบันคือ เทคโนโลยีการเข้าหัสลับเชิงควอนตัมซึ่งทำให้ข้อมูลที่ส่งมีความปลอดภัยสูง โดยวิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography) เป็นศาสตร์แขนงใหม่ ที่มีการเรียนการสอนในระดับอุดมศึกษาขั้นสูงในหลายประเทศ และ กำลังเป็นหัวข้อวิจัยที่ได้รับความสนใจและมีการพัฒนาอย่างรวดเร็ว จากการศึกษาวิจัยเชิงนโยบายเรื่อง “ทิศทางการวิจัยและพัฒนาเทคโนโลยีสารสนเทศเชิงควอนตัมของประเทศไทย” ในปีพ.ศ. 2555 โดยสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ที่ศึกษาสถานภาพการวิจัยด้านเทคโนโลยีสารสนเทศเชิงควอนตัมทั้งภายในและต่างประเทศ รวมถึงแนวโน้มภายใต้กรอบระยะเวลา 10 ปี โดยพบว่า ในส่วนของรหัสลับควอนตัมเพื่อกิจการโทรคมนาคมประเทศไทยจะเริ่มมีความต้องการทดสอบระบบวิทยาการรหัสลับเชิงควอนตัมในปี ค. ศ. 2016

เพื่อเป็นการติดตามเทคโนโลยีที่ได้รับการพัฒนาการอย่างต่อเนื่อง และ มีแนวโน้มจะถูกนำมาใช้จริงในระบบสื่อสารโทรคมนาคมของโลกผ่านเครือข่ายสื่อสารที่มีอยู่เดิม ประเทศไทยจึงมีความจำเป็นอย่างยิ่งยวดในการสร้างกลุ่มบุคลากรให้มีความพร้อมในการรับเทคโนโลยีนี้จากต่างประเทศ รวมถึงการสร้างบุคลากรที่เข้าใจและนำเทคโนโลยีนี้ไปใช้อย่างถูกต้องด้วยการสร้างความเข้าใจสาธารณะในการรองรับเทคโนโลยีการสื่อสารด้วยความปลอดภัยสูงสุดด้วยวิทยาการรหัสลับเชิงควอนตัมอันเป็นเทคโนโลยีพื้นฐานที่มีศักยภาพการสูงในอนาคต โดยการรวมกลุ่มผู้สนใจทั้งภาคนโยบาย ภาคการศึกษาและวิจัย และผู้ใช้งานโดยจะศึกษาและติดตามการพัฒนามาตรฐานรหัสลับควอนตัมของโลก รวมทั้งจะสร้างความตระหนักและผลักดันสู่แผนแม่บทที่เกี่ยวข้องของประเทศไทยในอนาคตด้วย ทั้งนี้จะดำเนินการสร้างความร่วมมือและรับการถ่ายทอดเทคโนโลยีจากต่างประเทศ เพื่อการต่อยอดการวิจัยและพัฒนาที่จะสามารถพึ่งพาตนเองกับเทคโนโลยีใหม่นี้ได้ในอนาคต โดยอาศัยความร่วมมือของบุคลากรในระดับปฏิบัติการของสถาบันอื่นๆ ในประเทศด้วย รวมทั้งการจะสร้างผลกระทบให้กว้างขวางขึ้นผ่านทางการบรรยาย ฝึกอบรมและการผลิตสื่อและเอกสารเผยแพร่สาธารณะต่าง ๆ เพื่อการพัฒนาบุคลากรและการเตรียมพร้อมกับเทคโนโลยีอุบัติใหม่ ด้านสารสนเทศเชิงควอนตัมของประเทศไทยสู่ระยะต่อไป

1.2 วัตถุประสงค์ของโครงการ

โครงการนี้สอดคล้องกับหลักการความจำเป็น ตรงตามเป้าหมายของการจัดสรรเงินตามมาตรา ๕๒ ของกอง-ทุนฯ ของ กสทช. คือ

1. เพื่อสร้างความเข้าใจสาธารณะในการรองรับเทคโนโลยีการสื่อสารด้วยความปลอดภัยสูงสุดด้วยวิทยาการรหัสลับเชิงควอนตัมอันเป็นเทคโนโลยีพื้นฐานที่มีศักยภาพสูงในอนาคต โดยการรวมกลุ่มผู้สนใจทั้งภาคนโยบาย ภาคการศึกษาและวิจัย และผู้ใช้งาน
2. เพื่อศึกษาและติดตามการพัฒนามาตรฐานรหัสลับควอนตัมของโลก รวมทั้งสร้างความตระหนักและผลักดันสู่แผนแม่บทที่เกี่ยวข้องของประเทศไทย
3. เพื่อสร้างความร่วมมือ รับการถ่ายทอดเทคโนโลยีจากต่างประเทศ และต่อยอดการวิจัยและพัฒนาเพื่อพึ่งพาตนเองกับเทคโนโลยีใหม่นี้ได้ในอนาคต
4. เพื่อผลิตสื่อและเอกสารเผยแพร่สาธารณะ เพื่อการฝึกอบรมถ่ายทอดความรู้และการพัฒนาบุคลากร

1.3 ขอบเขตของกิจกรรมตามแผนการดำเนินงาน

โครงการนี้มีกิจกรรมสำคัญและจะดำเนิน 3 ด้านหลักๆ ได้แก่

1. การถ่ายทอดเทคโนโลยีจากต่างประเทศ โดยอาศัยความร่วมมือของบุคลากรในระดับปฏิบัติการ โดยมีกิจกรรมย่อย คือ

1.1 การบรรยายพิเศษ จากนักวิจัยทางด้านการสื่อสารเชิงควอนตัม จากกลุ่มวิจัยจากมหาวิทยาลัยต่าง ๆ และ จากกลุ่มความร่วมมืออื่น ๆ

1.2 การร่วมศึกษาและนำเสนอเทคโนโลยีที่เหมาะสมสำหรับประเทศไทย

1.3 การสร้างความร่วมมือทางการวิจัยในระยะยาว

2. การพัฒนาบุคลากร มีกิจกรรมย่อยคือ

2.1 การจัดทำเอกสารและสื่อออนไลน์เพื่อนำเสนอข้อมูลเชิงเทคนิคระดับพื้นฐานและระดับกลาง

2.2 จัดทำการสำรวจสถานะงานวิจัย ทรัพย์สินทางปัญญาของเทคโนโลยีและผลิตภัณฑ์ที่เกี่ยวข้องทั่วโลก (สิทธิบัตร ผลงานตีพิมพ์ ผลิตภัณฑ์ กลุ่มวิจัย อุตสาหกรรม และประเทศที่เกี่ยวข้อง เป็นต้น)

2.3 จัดสัมมนา ฝึกอบรม และ รวมกลุ่มวิจัยเฉพาะทาง

3. การจัดทำสรุปมาตรฐานโลกด้านวิทยาการรหัสลับเชิงควอนตัม โดยมีกิจกรรมย่อย คือ

3.1 การแปลและติดตามพัฒนาการของมาตรฐานโลก ที่นำเสนอโดย ETSI (European Telecommunications Standards Institute)

3.2 การสัมมนารับฟังความคิดเห็นของผู้ที่เกี่ยวข้องกับเทคโนโลยีด้านนี้ (สถานศึกษา – หน่วยงานของรัฐ - ภาคอุตสาหกรรม)

3.3 การเผยแพร่และประชาสัมพันธ์การมีและการประยุกต์สำหรับอนาคต

1.4 แผนการดำเนินงาน

ขั้นตอนการดำเนินงาน แบ่งเป็นกิจกรรมย่อย และ มีแผนการดำเนินงานดังตารางข้างล่างนี้

ตารางที่ 1.1 แผนการดำเนินงาน

กิจกรรม	ระยะเวลา																							
	ไตรมาสที่ 1			ไตรมาสที่ 2			ไตรมาสที่ 3			ไตรมาสที่ 4			ไตรมาสที่ 5			ไตรมาสที่ 6			ไตรมาสที่ 7			ไตรมาสที่ 8		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
ก 1.1 บรรยายพิเศษโดยผู้เชี่ยวชาญ											x	x											x	x
ก 1.2 ร่วมศึกษาและแนะนำเทคโนโลยี	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ก 1.3 สร้างความร่วมมือ	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ก 2.1 จัดทำเอกสาร/สื่อออนไลน์						x	x	x	x								x	x	x	x				
ก 2.2 สำรวจสถานะการวิจัย	x	x	x	x	x	x																		
ก 2.3 จัดสัมมนาอบรม					x	x					x	x					x	x					x	x
ก 3.1 การแปลและติดตามพัฒนาการของมาตรฐานโลก	x	x	x	x	x	x	x	x	x	x	x	x												
ก 3.2 การสัมมนารับฟังความคิดเห็นของผู้ที่เกี่ยวข้อง					x	x					x	x					x	x					x	x
ก 3.3 เผยแพร่ประชาสัมพันธ์การมีและการประยุกต์											x	x											x	x

ก. = กิจกรรม

1.5 ผลที่คาดว่าจะได้รับ

ผลลัพธ์ที่จะได้จากโครงการนี้จะสร้างผลกระทบได้เป็นรูปธรรมที่สามารถชี้วัดได้ดังนี้

1. ภาคประชาชนได้เข้าถึงองค์ความรู้ของเทคโนโลยีอุบัติใหม่นี้ เกิดความเข้าใจและสามารถติดตามความก้าวหน้าได้สะดวก เกิดรวมกลุ่มเพื่อเตรียมการคุ้มครองสิทธิของผู้ใช้งานในอนาคต
2. ภาคการศึกษาและการวิจัยเกิดการรวมกลุ่มเพื่อขับดันกลยุทธ์การพัฒนาด้านอื่นๆได้ต่อไป เช่น วิจัยและพัฒนาที่เหมาะสมกับประเทศไทยและการปรับแนวทางรองรับการพัฒนาบุคลากรและองค์ความรู้ให้เหมาะสม
3. ภาคอุตสาหกรรม หรือผู้จะนำเทคโนโลยีใหม่นี้ไปใช้งานหรือให้บริการ ได้รับการส่งเสริมให้สามารถติดตามเข้าถึงและปรับตัวกับเทคโนโลยีใหม่นี้ได้รวดเร็วขึ้นกับทั้งมาตรฐานและผลิตภัณฑ์ที่เกี่ยวข้องตั้งแต่การเริ่มต้นของเทคโนโลยีขณะนี้
4. ภาครัฐโดยผู้กำหนดนโยบาย แผนแม่บทโทรคมนาคมและความปลอดภัยสารสนเทศ ได้ตระหนักถึงศักยภาพและเตรียมความพร้อมรับกับผลกระทบของเทคโนโลยีอุบัติใหม่ของโลกรหัสลับเชิงควอนตัมนี้
5. กสทช. สามารถนำผลลัพธ์จากโครงการนี้ไปใช้เพื่อกำหนดแนวทางสนับสนุนส่งเสริมทุกภาคส่วน (จากข้อ 1-4) ที่เกี่ยวข้องกับการสื่อสารด้วยเทคโนโลยีใหม่นี้ได้ในอนาคต

บทที่ 2
รายงานการจัดอบรมและการเผยแพร่และประชาสัมพันธ์สู่สาธารณะ

สำหรับในบทนี้ จะเป็นเนื้อหาทางวิชาการที่นำมาจัดอบรม ที่ดำเนินการตามโครงการ และรายงานลักษณะการอบรมและการเผยแพร่และประชาสัมพันธ์สู่สาธารณะ

2.1 เนื้อหาทางวิชาการของเทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

สำหรับหัวข้อนี้จะเป็นการอธิบายหลักการและทฤษฎีที่เกี่ยวข้องกับเทคโนโลยีด้านการสื่อสารปลอดภัยสูง โดยเริ่มต้นจาก ทฤษฎีพื้นฐานของเกี่ยวกับเทคโนโลยีการสื่อสารปลอดภัยสูง ซึ่งแนวการใช้รหัสลับในปัจจุบันนี้แบ่งออกเป็น 2 วิธี คือ การใช้กุญแจลับ และ การใช้กุญแจสาธารณะ แล้วจากนั้นจึงนำเสนอเทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

2.1.1 พื้นฐานการสื่อสารปลอดภัยสูง: วิทยาการรหัสลับ

วิทยการรหัสลับ (Cryptography) เป็นวิทยาการที่สร้างขึ้นเพื่อทำให้การสื่อสารมีความปลอดภัยภายใต้สภาวะที่สมมติว่ามีความพยายามในการคุกคามหรือโจมตีระบบสื่อสาร โดยการพิจารณาระบบการติดต่อสื่อสารในวิทยาการด้านนี้ เราจะสมมติให้มีบุคคลสองฝ่าย คือ ผู้ส่งและผู้รับสาร ให้ชื่อเป็น อลิซ (Alice) และ บ๊อบ (Bob) ตามลำดับ โดยบุคคลทั้งสองจะพยายามติดต่อสื่อสารถึงกันผ่านระบบคอมพิวเตอร์ และ มีบุคคลที่สามที่ให้ชื่อเป็น อีฟ (Eve) เป็นผู้ที่พยายามคุกคามหรือโจมตีระบบการติดต่อสื่อสารนี้ โดยในวิทยาการด้านนี้ เราจะพิจารณาด้านความปลอดภัยของข้อมูลที่ส่งผ่านช่องทางการสื่อสารต่าง ๆ ที่สนใจพิจารณา เช่น ระบบเครือข่ายโทรศัพท์ไร้สาย ระบบเครือข่ายอินเทอร์เน็ตผ่านดาวเทียม หรือ ระบบเครือข่ายอินเทอร์เน็ตผ่านเส้นใยนำแสง (ดูรูปที่ 2.1)

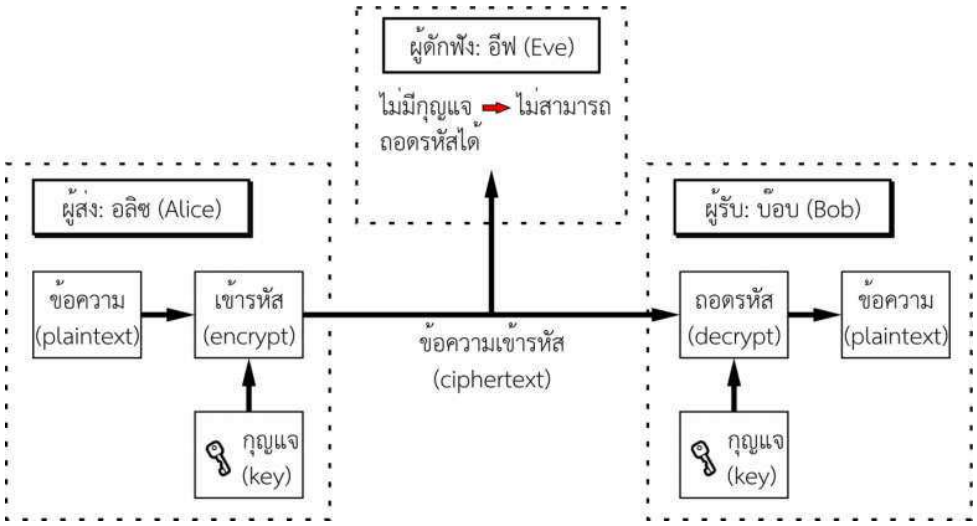
รูปที่ 2.1 แบบจำลองการติดต่อสื่อสารระหว่างอลิซกับบ๊อบโดยมีอีฟเป็นผู้ที่พยายามคุกคามหรือโจมตีระบบ

ในการพิจารณาระบบสื่อสารในวิทยาการรหัสลับนี้ เราจะคิดค้นวิธีการแก้ปัญหาต่าง ๆ ในการสื่อสารเพื่อให้ระบบสื่อสารนี้ปลอดภัย โดยปัจจุบัน วิทยาการด้านนี้ได้รับความสนใจอย่างมาก และมีการประยุกต์ใช้งานจริงทั้งในหน่วยงานด้านความมั่นคงต่าง ๆ ทั่วโลก และ ในเชิงพาณิชย์ โดยรหัสลับที่ใช้ในวิทยาการนี้แบ่งได้เป็นสองประเภทใหญ่ ๆ คือ รหัสลับชนิดกุญแจลับ (Secret Key) และ รหัสลับชนิดกุญแจสาธารณะ (Public Key) ซึ่งวิทยาการที่ใช้รหัสลับทั้งสองชนิดเกิดจากแนวคิดในการสื่อสารที่ต่างกันอย่างมากแต่ก็มีการนำไปใช้งานกันอย่างแพร่หลายในปัจจุบัน โดยวิทยาการแต่ละประเภทมีรายละเอียดดังต่อไปนี้

วิทยาการรหัสลับกุญแจลับ (Secret-Key Cryptography)

วิทยาการรหัสลับชนิดกุญแจลับ (Secret Key Cryptography) มีหลักการการเข้ารหัส/ถอดรหัสแบบสมมาตร โดยมีลักษณะทั่วไปในการสื่อสารดังแสดงในรูปที่ 2.2 โดยในขั้นแรกอลิซจะเป็นผู้ที่ต้องการนำข้อความ ซึ่งอาจเป็นข้อมูลประเภทต่าง ๆ เช่น อีเมล ไฟล์ภาพ ข้อมูลเสียง ส่งไปยังผู้รับคือบ๊อบ โดยก่อนที่อลิซจะส่งข้อความดังกล่าวไปในระบบสื่อสาร อลิซจะทำการเข้ารหัสข้อความโดยใช้กุญแจ ซึ่งเป็นข้อมูลอีกประเภทหนึ่งที่มีการกำหนดไว้ก่อนหน้านี้และมีเพียงอลิซและบ๊อบเท่านั้นที่มีข้อมูลกุญแจนี้ เมื่อเข้ารหัสแล้ว ข้อความที่ต้องการส่งจะกลายเป็นข้อความเข้ารหัส ดังนั้นหากมีการดักฟังข้อความนี้โดยอีฟ แม้อีฟจะสามารถคัดลอกข้อความเข้ารหัสนี้ แต่หากอีฟไม่มีกุญแจที่ใช้ในการถอดรหัส อีฟก็จะไม่สามารถล่วงรู้ข้อความที่ส่งออกจากอลิซไปยังบ๊อบได้ ดังนั้นการสื่อสารลักษณะนี้จะมีความปลอดภัย โดยเนื่องจากการเข้ารหัสลับประเภทนี้ ทั้งผู้ส่งและผู้รับจะต้องมีการแบ่งปันหรือกำหนดกุญแจที่ใช้ในการเข้ารหัสและถอดรหัสก่อน จึงจะสามารถสื่อสารกันได้ เราจึงเรียกวิทยาการรหัสลับประเภทนี้ว่าอีกชื่อหนึ่งว่า วิทยาการรหัสลับแบบสมมาตร (Symmetric Cryptography)

เทคโนโลยีวิทยาการรหัสลับลักษณะนี้ที่มีการใช้งานอยู่ในปัจจุบัน บรรจุอยู่ใน มาตรฐานการเข้ารหัสข้อมูล DES (Data Encryption Standard) และ มาตราฐานการเข้ารหัสขั้นสูง AES (Advanced Encryption Standard) โดยมาตรฐานทั้งสองมีรายละเอียดในการใช้กุญแจในการเข้ารหัสและถอดรหัสที่แตกต่างกัน โดยมีลักษณะทั่วไปคือ หากการเลือกกุญแจที่ดีและมีการกำหนดความซับซ้อนในการเข้ารหัสและถอดรหัสที่มากเพียงพอ การถอดรหัสโดยที่ไม่ทราบข้อมูลกุญแจแต่ใช้การค้นหากุญแจ (brute force) จะทำไม่ได้เนื่องจากจะต้องอาศัยการคำนวณที่ซับซ้อนเป็นระยะเวลานานเกินขีดความสามารถของเครื่องคอมพิวเตอร์ในปัจจุบัน



รูปที่ 2.2 ลักษณะทั่วไปของการใช้วิทยาการรหัสลับชนิดกุญแจลับในการสื่อสารปลอดภัยสูง

อย่างไรก็ตาม ในการใช้วิทยาการรหัสลับชนิดกุญแจลับ มีข้อด้อยคือ จะต้องมีการกำหนดข้อมูลกุญแจและรูปแบบการเข้ารหัส/ถอดรหัสระหว่างอลิซและบ๊อบก่อนที่จะมีการส่งข้อความ ซึ่งการสื่อสารข้อมูลกุญแจลับนี้จะปลอดภัยเมื่อมีการใช้ช่องทางการสื่อสารช่องทางอื่นประกอบ เช่น ผ่านการพบปะกันโดยตรง หรือ ผ่านการสื่อสารด้วยช่องทางอื่น ๆ นอกเหนือจาก การใช้คอมพิวเตอร์ (เช่น การใช้โทรศัพท์ หรือ จดหมาย) เพราะหากผู้ส่งและผู้รับ ยังคงใช้การสื่อสารผ่านคอมพิวเตอร์ ก็ยังคงมีความเป็นไปได้ที่อีฟซึ่งเป็นผู้ดักฟังจะสามารถได้รับข้อมูลกุญแจที่ใช้ในการถอดรหัสได้

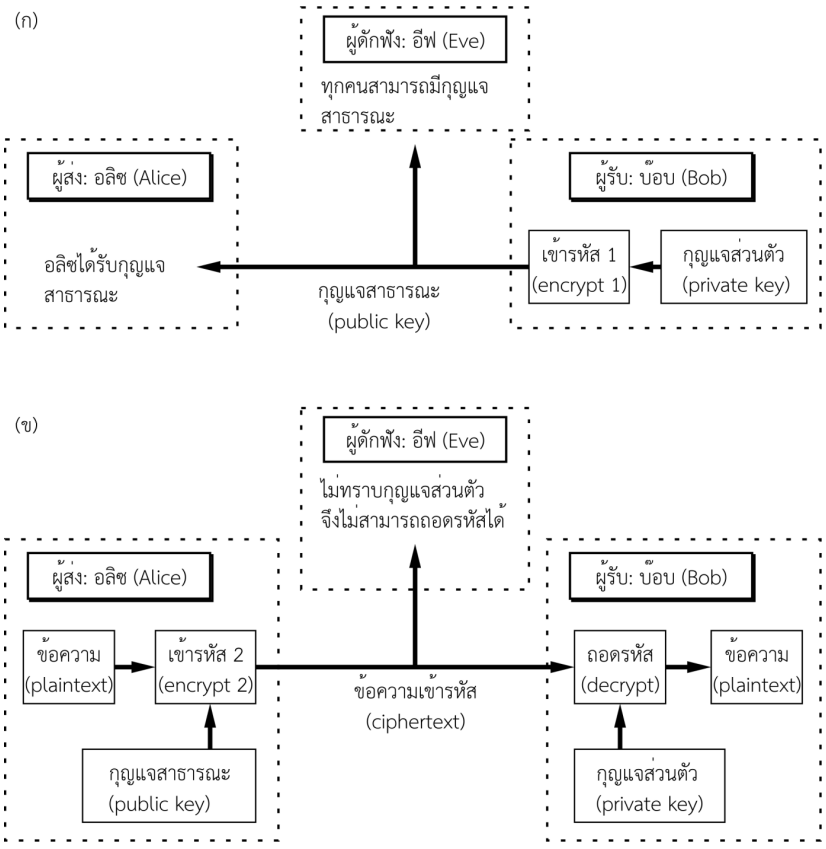
ในการใช้งานในทางปฏิบัติ เราอาจมีผู้ส่งและผู้รับสารหลาย ๆ คน ซึ่งแต่ละคนอาจมีความต้องการในการติดต่อสื่อสารมากน้อยต่างกัน ดังนั้น การแจกจ่ายกุญแจในการใช้วิทยาการรหัสลับชนิดกุญแจลับนี้จะมีความยุ่งยากซับซ้อนมากขึ้นด้วย เพราะจะต้องมีการกำหนดรูปแบบการกำหนดกุญแจขึ้นอีก ซึ่งในกรณีนี้จะทำให้การสื่อสารมีความปลอดภัยต่ำลง

วิทยาการรหัสลับกุญแจสาธารณะ (Public-Key Cryptography)

วิทยาการรหัสลับชนิดกุญแจลับ เป็นวิทยาการที่มีการใช้งานมานานจนกระทั่งในปี ค.ศ. 1976 W. Diffie และ M. Hellman ได้คิดค้นวิทยาการรหัสลับอีกแขนงขึ้นซึ่งมีวิธีการต่างออกไปจากเดิมและเรียกวิทยาการนี้ว่า วิทยาการรหัสลับชนิดกุญแจสาธารณะ (Public-key Cryptography) หรือวิทยาการรหัสลับชนิดกุญแจอสมมาตร (Asymmetric Cryptography) โดยแนวคิดในการสร้างวิทยาการรหัสลับประเภทนี้มาจากการพยายามกำจัดความยุ่งยากในการจัดการกุญแจในวิทยาการรหัสลับชนิดกุญแจลับที่กล่าวไปก่อนหน้านี้ โดยหลักการสำคัญของวิทยาการรหัสลับชนิดกุญแจสาธารณะคือ การกำหนดให้มีกุญแจ 2 ประเภท คือ กุญแจ

ลับหรือกุญแจส่วนตัว (Secret Key or Private Key) ซึ่งผู้รับเท่านั้นที่มีข้อมูลกุญแจนี้ และ กุญแจสาธารณะ (Public Key) ซึ่งเป็นกุญแจที่มีการแจกจ่ายให้ทุกคนที่ต้องการสื่อสารกับผู้รับข้อความ

ในขั้นตอนแรกของการสื่อสารปลอดภัยสูงโดยใช้วิทยาการรหัสลับกุญแจสาธารณะนี้ บ๊อบ (ผู้รับ) จะทำการกำหนดกุญแจลับหรือกุญแจส่วนตัวด้วยตนเองจากนั้นจึงทำการเข้ารหัสกุญแจของตนเองเพื่อสร้างกุญแจสาธารณะ โดยการเข้ารหัสนี้จะกระทำโดยการใช้คุณสมบัติบางประการของฟังก์ชันทางคณิตศาสตร์ที่ทำให้การถอดรหัสนั้นทำได้ยาก ตัวอย่างเช่น การกำหนดกุญแจลับคือเลขจำนวนเฉพาะ และ การเข้ารหัสเป็นการคูณกันของเลขจำนวนเฉพาะ การถอดรหัสก็จะเป็นการหาตัวประกอบของจำนวนเต็ม ซึ่งทำได้ยากหากเลข (กุญแจ) ที่ใช้มีความซับซ้อนมาก เมื่อได้กุญแจสาธารณะแล้ว บ๊อบก็จะทำการส่งให้กับผู้ที่ต้องการติดต่อ โดยกุญแจนี้จะเป็นข้อมูลที่เปิดเผยให้ทุกคนทราบ (ดูรูปที่ 2.3 (ก)) เมื่ออลิซได้รับกุญแจสาธารณะจากบ๊อบแล้ว อลิซก็จะทำการเข้ารหัสข้อความที่ต้องการส่งให้บ๊อบกับกุญแจสาธารณะที่ได้รับจากบ๊อบ ซึ่งเมื่อเข้ารหัสแล้ว แม้อลิซเอง (หรือใครก็ตาม) ก็ไม่สามารถถอดรหัสและอ่านข้อความที่เข้ารหัสนี้ได้ มีเพียงแต่บ๊อบเท่านั้นที่มีกุญแจลับหรือกุญแจส่วนตัวที่ใช้ในการถอดรหัสเพื่ออ่านข้อความที่ส่งมาได้



รูปที่ 2.3 ลักษณะทั่วไปของการใช้วิทยาการรหัสลับชนิดกุญแจสาธารณะในการสื่อสารปลอดภัยสูง (ก) ขั้นการแจกจ่ายกุญแจ และ (ข) ขั้นการสื่อสารข้อความ

จากที่กล่าวมานี้จะเห็นได้ว่า วิทยาการรหัสลับชนิดกุญแจสาธารณะ เป็นวิทยาการที่ลดขั้นตอนการจัดการกับกุญแจลับ ซึ่งเหมาะกับการสื่อสารผ่านระบบเครือข่ายอินเทอร์เน็ตในปัจจุบัน เพราะผู้ส่งและผู้รับไม่จำเป็นต้องทำการตกลงเรื่องกุญแจลับกันล่วงหน้า แต่ใช้การส่งกุญแจสาธารณะแทน โดยทั้งนี้ การคุกคามหรือโจมตีอย่างหนึ่งที่อาจเกิดขึ้นได้คือการที่ผู้ดักฟัง (อีฟ) สร้างกุญแจสาธารณะปลอมมาหลอกให้ผู้ส่ง (อลิซ) ส่งข้อความไป ซึ่งในกรณีนี้ผู้รับตัวจริง (บ๊อบ) จะไม่สามารถอ่านข้อความได้ ดังนั้น วิทยาการรหัสลับชนิดนี้จะต้องใช้ร่วมกับการพิสูจน์ตัวจริงด้วยเทคนิคอื่น ๆ ประกอบ เพื่อให้การสื่อสารมีความปลอดภัยสูง

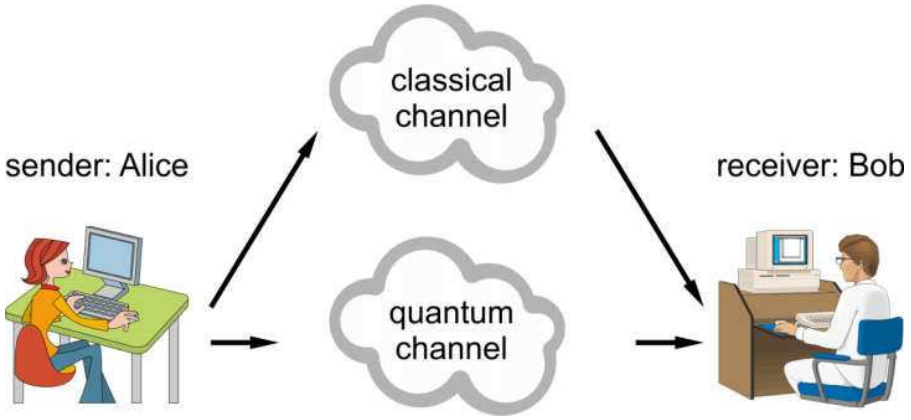
เทคโนโลยีรหัสลับชนิดกุญแจสาธารณะที่มีการใช้งานกันอย่างแพร่หลายในปัจจุบัน คือ ระเบียบวิธี RSA (ตั้งตามชื่อผู้คิดค้น คือ Ronald Rivest, Adi Shamir, และ Len Adleman) ซึ่งระเบียบวิธีนี้อาศัยความซับซ้อนในการคำนวณการแยกตัวประกอบของจำนวนเฉพาะในการสร้างกุญแจสาธารณะ โดยอาศัยความซับซ้อนในการแยกตัวประกอบของตัวเลขทางคณิตศาสตร์ เราสามารถกล่าวได้ว่า ข้อความที่สื่อสารมีความปลอดภัยอยู่ระดับหนึ่ง ทั้งนี้เพราะว่าผู้ดักฟังข้อมูลจะพัฒนาความสามารถสำหรับพยายามถอดรหัสแต่ต้องใช้เวลานานมากด้วยศักยภาพของคอมพิวเตอร์ความเร็วสูงสุดในท้องตลาดปัจจุบันนี้ แต่ถ้าเมื่อใดที่กุญแจรหัสลับซึ่งเป็นส่วนสำคัญในการถอดรหัสถูกโจรกรรมไปได้ด้วยแม้เพียงบางส่วนจะทำให้ความยากในการถอดรหัสลดลงไปได้ ยิ่งทราบกุญแจรหัสลับมากเท่าใดยิ่งถอดรหัสออกได้ง่ายขึ้นทำให้วิทยาการรหัสลับแบบเดิมไม่ถือว่ามีความปลอดภัยสูงสุด เพราะเมื่อศักยภาพของเครื่องคำนวณหรือคอมพิวเตอร์สูงมากขึ้น (รวมทั้งการกำเนิดและใช้งานได้จริงของควอนตัมคอมพิวเตอร์) และมีพัฒนาการรวดเร็วขึ้นจึงต้องมีการพัฒนาของวิทยาการรหัสลับขึ้นมาใหม่ จึงได้เริ่มมีการนำความรู้กลศาสตร์ควอนตัมมาประยุกต์ใช้ในการรับส่งกุญแจรหัสลับ เรียกรหัสลับแบบนี้ว่า “วิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography)” เพื่อให้การรับส่งกุญแจรหัสลับมีความปลอดภัยมากขึ้น

สำหรับรายละเอียดของระเบียบวิธีในการเข้ารหัส-ถอดรหัส ตามวิทยาการรหัสลับที่ใช้ในการสื่อสารปลอดภัยสูงนั้น เป็นวิธีการที่เป็นที่รู้จักกันอย่างแพร่หลาย ผู้ที่สนใจสามารถศึกษาได้จากตำราทั้งภาษาไทยและ ภาษาต่างประเทศ ที่แสดงอยู่ในบรรณานุกรมท้ายหัวข้อนี้

2.1.2 เทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

เทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมในถูกคิดค้นขึ้นในปี ค.ศ. 1984 โดย Charles H. Bennett และ Gilles Brassard [Bennett et al., 1984] โดยปัจจุบัน เราเรียกโปรโตคอลนี้ว่า BB84 การสื่อสารด้วยรหัสลับควอนตัมนี้ใช้คุณสมบัติการแบ่งแยกไม่ได้ของโฟตอน หน่วยของแสงที่แบ่งแยกต่อไปไม่ได้อีกแล้วตามทฤษฎีควอนตัม นั่นคือ หากเราทำการใส่ข้อมูลข่าวสารเข้าไปในโฟตอนเพียงหน่วยเดียว ผู้รับข้อมูลเพียงคนเดียวเท่านั้นที่สามารถรับได้ วิธีการที่คิดค้นขึ้นนี้ใช้คุณสมบัติโพลาไรเซชั่นของโฟตอนในการเก็บสถานะของข้อมูล โดยต่อมาวิธีการนี้ได้ถูกพัฒนาขึ้นให้สามารถใช้งานได้จริงในการสื่อสารทางแสงผ่านเส้นใยนำแสง โดยเปลี่ยนวิธีการเก็บสถานะของข้อมูลจากคุณสมบัติโพลาไรเซชั่นเป็นการมอดูเลตเฟส โดย

เทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมนี้มิได้มีเพียงโปรโตคอลเดียว ในปี ค.ศ. 1991 Artur Ekert [Ekert, 1991] ได้เสนอให้ใช้การพัวพันเชิงควอนตัม (Entanglement) ของโฟตอนในการเข้ารหัสข้อมูล และเรียกว่า โปรโตคอล E91 ซึ่งเทคนิคการใช้การพัวพันเชิงควอนตัมนี้กำลังได้รับความสนใจอย่างมากในหมู่นักวิทยาศาสตร์ เนื่องจากเป็นเทคโนโลยีที่สามารถการประยุกต์ใช้ ได้ทั้งกับการคำนวณเชิงควอนตัม (Quantum Computing) และ การสื่อสารเชิงควอนตัม

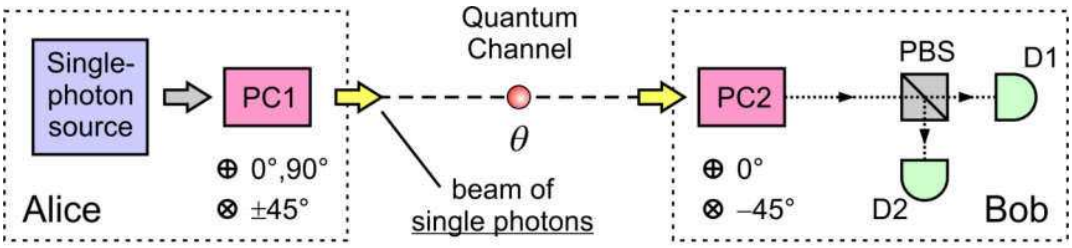


รูปที่ 2.4 ลักษณะทั่วไปของการใช้วิทยาการรหัสลับเชิงควอนตัมในการสื่อสารปลอดภัยสูงสุด

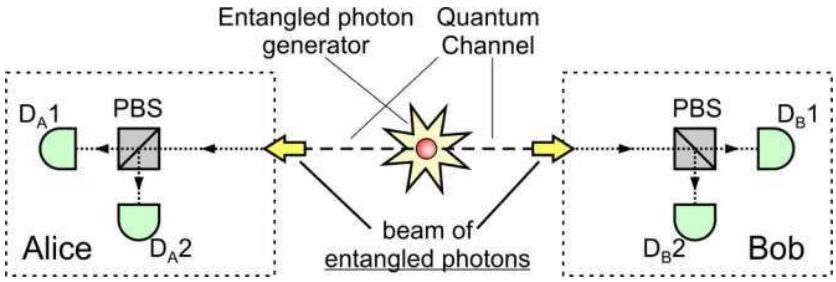
วิทยาการรหัสลับเชิงควอนตัม เป็นระบบของวิทยาการรหัสลับที่ใช้การส่งกุญแจลับผ่านช่องทางการสื่อสารเชิงควอนตัม (Quantum Channel) เช่น เส้นใยนำแสง (Optical Fiber) อากาศ (Free Space) (ดูรูปที่ 2.4) โดยกุญแจรหัสลับจะถูกแทนด้วยสถานะทางควอนตัม เช่น โพลาไรเซชันของโฟตอน หรือมุมเฟสของโฟตอน เป็นต้น และใช้กฎทางควอนตัมฟิสิกส์ช่วยยืนยันความปลอดภัยของระบบ สามารถตรวจพบผู้เข้ามาลักลอบขโมยข้อมูลทางช่องทางการสื่อสารเชิงควอนตัมได้เสมอ การส่งกุญแจรหัสลับหรือการกระจายคีย์ควอนตัม (Quantum Key Distribution) สามารถแบ่งได้เป็นสองรูปแบบคือ

1. รูปแบบการส่งและวัดแบบธรรมดา

การกำหนดสถานะทางควอนตัมแทนบิตข้อมูลแบบดิจิทัล และส่งสถานะระดับควอนตัมจากผู้ส่งไปยังผู้รับโดยยืนยันความปลอดภัยด้วยหลักความไม่แน่นอนของไฮเซนเบิร์ก ซึ่งหากมีการรบกวนจากผู้ลักลอบทางผู้ส่งและผู้รับจะทราบได้จากสถานะที่เกิดการเปลี่ยนแปลง ตัวอย่างการส่งและการวัดสถานะควอนตัมแบบธรรมดา เช่น เกณฑ์วิธี BB84 เกณฑ์วิธี B92 เป็นต้น



รูปที่ 2.5 ตัวอย่างการใช้วิทยาการรหัสลับเชิงควอนตัมในการสื่อสารปลอดภัยสูงสุด โดยเนื่องจากโฟตอนหนึ่งหน่วยไม่สามารถถูกแยกออกได้อีก จึงทำให้ผู้ดักฟังไม่สามารถทำการดักฟังได้โดยที่ผู้ส่ง-ผู้รับไม่ทราบ



รูปที่ 2.6 ตัวอย่างการใช้วิทยาการรหัสลับเชิงควอนตัมในการสื่อสารปลอดภัยสูงสุด โดยใช้คุณสมบัติความพัวพันของอนุภาคควอนตัม ทำให้ผู้รับสามารถรับข้อมูลจากผู้ส่งได้โดยไม่มีการดักฟัง
(หากมีการดักฟัง ข้อมูลที่ส่งจะถูกเปลี่ยนแปลง, โดยในรูปนี้ มีการละเลยส่วนที่ใช้ในการกำหนดข้อมูลด้านผู้ส่ง)

2. รูปแบบการส่งและวัดโดยอาศัยความพัวพัน

วิธีการนี้จะอาศัยคุณสมบัติของความพัวพันทางควอนตัม (Entanglement) โดยทำการกำเนิดคู่อนุภาคที่มีสถานะซึ่งไม่สามารถแยกจากกันได้สองสถานะ จากนั้นทำการส่งอนุภาคที่มีความพัวพันกันไปยังฝั่งผู้ส่งและผู้รับฝั่งละหนึ่งอนุภาค เมื่อทำการวัดสถานะที่ผู้ส่งจะผลต่อสถานะของอนุภาคที่ผู้รับและทำให้ทราบสถานะของอนุภาคที่ผู้รับทันที แต่หากมีการลักลอบดักอนุภาคไปจะเป็นการรบกวนสถานะระบบของอนุภาคที่มีความพัวพันกัน และความพัวพันระหว่างสองอนุภาคดังกล่าวจะถูกทำลายลง ทำให้ทราบได้ว่ามีการลักลอบขโมยอนุภาคเกิดขึ้น (ดูรูปที่ 2.6)

หลักการทำงานของระบบวิทยาการรหัสลับเชิงควอนตัม

การส่งกุญแจรหัสลับโดยระบบวิทยาการรหัสลับเชิงควอนตัม ทำการส่งข้อมูลของกุญแจรหัสลับด้วยการแทนบิตข้อมูลทางดิจิทัลด้วยสถานะเชิงควอนตัมหรือคิวบิต (Quantum Bit หรือ Qubit) โดยบิตข้อมูลเชิง

คลาสสิกเป็นระบบของการใช้สถานะที่แตกต่างกันสองสถานะ กำหนดค่าเป็นบิต “0” และบิต “1” ยกตัวอย่างเช่นสวิตช์เชิงกล ซึ่งเป็นระบบที่สามารถแบ่งได้เป็นสองสถานะอย่างแน่นอน และไม่มีโอกาสที่จะพบสถานะทั้งสองได้พร้อมกัน ส่วนบิตข้อมูลเชิงควอนตัมมีชื่อเรียกว่าคิวบิต เป็นบิตข้อมูลที่แทนด้วยสถานะทางควอนตัมสองสถานะที่แตกต่างกันในระบบสารสนเทศเชิงตวอนตัม เช่น ระบบวิทยาการรหัสลับเชิงควอนตัม

ในระบบวิทยาการรหัสลับเชิงควอนตัมจะใช้กลศาสตร์ควอนตัมเข้ามาแก้ปัญหาเรื่องการเก็บรักษาความลับของกุญแจ ระบบวิทยาการรหัสลับเชิงควอนตัมจะแทนข้อมูลแต่ละบิตด้วยวัตถุในระดับควอนตัมเดี่ยว เช่น โฟตอนเดี่ยว โดยโฟตอนเดี่ยวนี้ไม่สามารถแบ่งหรือทำสำเนาโดยปราศจากการรบกวนสถานะเดิม จากคุณลักษณะดังกล่าวแสดงให้เห็นว่าระบบวิทยาการรหัสลับเชิงควอนตัมไม่ได้ป้องกันการดักจับกุญแจจากผู้อื่น แต่สามารถตรวจสอบว่ากุญแจถูกดักจับไปหรือไม่ จากการตรวจสอบสถานะทางควอนตัมที่เปลี่ยนไป ซึ่งหากกุญแจถูกดักจับผู้ส่งก็สามารถสร้างกุญแจใหม่และส่งไปยังผู้รับได้อีกครั้ง

เกณฑ์วิธีสำหรับระบบวิทยาการรหัสลับ ที่ใช้กันอย่างแพร่หลายในกระบวนการกระจายกุญแจรหัสลับเชิงควอนตัมคือ คือเกณฑ์วิธี BB84 ซึ่งเป็นวิธีการแรกที่ถูกนำเสนอ โดย ชาร์ลส์ เบนเน็ต (Charles H. Bennett) นักวิทยาศาสตร์แห่งศูนย์วิจัยไอบีเอ็ม (IBM research center) ประเทศสหรัฐอเมริกา และ กิลเลส บราสซาร์ด (Gilles Brassard) แห่งมหาวิทยาลัยมอลทรีออล (Montreal University) ประเทศแคนาดา ได้ร่วมกันพัฒนาโพรโตคอลการเข้ารหัสในระบบวิทยาการรหัสลับเชิงควอนตัม สำหรับสร้างและกระจายกุญแจรหัสลับขึ้นเรียกระบบนี้ว่า BB84 และได้สร้างต้นแบบระบบวิทยาการรหัสลับเชิงควอนตัมชุดแรกของโลกสำเร็จในปี ค.ศ. 1989 โดยใช้สมบัติการมีโพลาไรเซชันหรือการจัดเรียงมุมของโฟตอนเดี่ยวในการเข้ารหัสลับ ดังรูปที่ 2.7 ซึ่งต้นแบบดังกล่าวสามารถส่งข้อมูลได้มีระยะทาง 32 เซนติเมตร ด้วยอัตราเร็วในการส่งประมาณ 10 บิตต่อวินาที

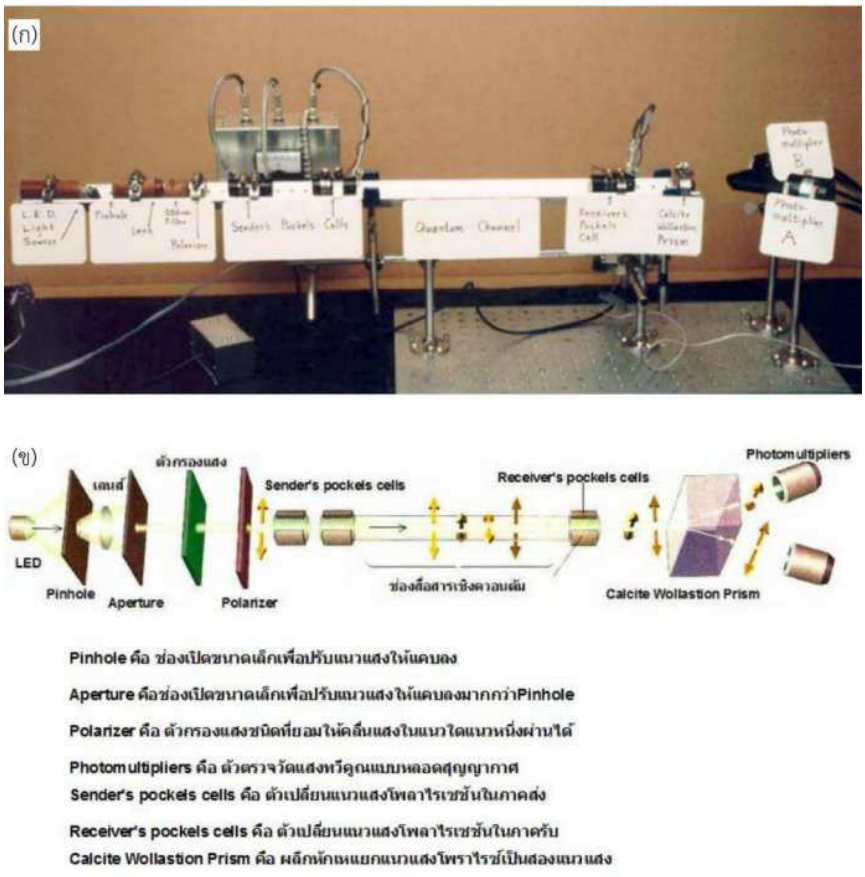
ตัวอย่างหนึ่งของวิทยาการรหัสลับแบบเกณฑ์วิธี BB84 ที่น่าสนใจคือการใช้สมบัติการมีโพลาไรเซชันของโฟตอนเดี่ยว โดยมีหลักความไม่แน่นอนของไฮเซนเบิร์กเป็นแกนหลักในการรักษาความปลอดภัยของระบบวิทยาการรหัสลับเชิง ควอนตัมโดยเกณฑ์วิธี BB84 รูปแบบนี้ ผู้ส่งและผู้รับจะสร้างกุญแจจากสถานะทางควอนตัมที่ใช้คู่ของเวกเตอร์ฐานที่ไม่ตั้งฉากกัน (Nonorthogonal Basis) ขึ้นมาสองชุด ยกตัวอย่างเช่น ในเวกเตอร์ฐานแรกใช้สถานะโพลาไรเซชันของโฟตอนในแนวราบ คือ สถานะ $|\leftrightarrow\rangle$ (Horizontal Polarization) กำหนดเป็น $|H\rangle$ และสถานะโพลาไรเซชันของโฟตอนในแนวตั้ง คือ สถานะ $|\updownarrow\rangle$ (Vertical Polarization) กำหนดเป็น $|V\rangle$ เรียกเวกเตอร์ฐานชุดนี้ว่าเวกเตอร์ฐานเชิงเส้นตรง (Rectilinear Basis) เขียนสัญลักษณ์ว่า $\oplus$ (ดูรูปที่ 2.5) ส่วนเวกเตอร์ฐานที่สองใช้สถานะโพลาไรเซชันของโฟตอนที่มุม 45° คือสถานะ $|\nearrow\rangle$ กำหนดเป็น $|+45^\circ\rangle$ และ สถานะโพลาไรเซชันของโฟตอนที่มุม –45° คือสถานะ $|\searrow\rangle$ กำหนดเป็น $|-45^\circ\rangle$ เรียกเวกเตอร์ฐานชุดนี้ว่าเวกเตอร์ฐานเชิงทแยงมุม (Diagonal Basis) เขียนสัญลักษณ์ว่า $\otimes$ โดยที่ทั้งผู้ส่งและผู้รับจะตกลงเทียบสถานะบิตข้อมูลผ่านทางช่องสื่อสารสาธารณะ โดยในแต่ละเวกเตอร์ฐานเดียวกันจะต้องเป็นบิตข้อมูลต่างกัน เช่น

$$\text{“1”} = |H\rangle \text{ หรือ “1”} = |+45^\circ\rangle$$

$$\text{“0”} = |V\rangle \text{ หรือ “0”} = |-45^{\circ}\rangle$$

หลังจากนี้ผู้ส่งและผู้รับจะติดต่อกันผ่านทางช่องสื่อสารควอนตัมและช่องสื่อสารสาธารณะ โดยผู้ส่งจะสุ่มเวกเตอร์ฐานและบิตข้อมูล โดยเวกเตอร์ฐานและบิตข้อมูลที่สุ่มนี้จะต้องเป็นข้อมูลที่สุ่มอย่างแท้จริง เพื่อยืนยันได้ว่าไม่มีทางที่ผู้ดักจับจะสามารถคาดเดาข้อมูลชุดนี้ได้ จากนั้นผู้ส่งส่งบิตข้อมูลผ่านทางช่องสื่อสารควอนตัม ผู้รับทำการสุ่มเวกเตอร์ฐานในการรับ แล้วผู้รับและผู้ส่งตกลงใช้บิตข้อมูลที่รับได้เฉพาะที่เวกเตอร์ฐานเดียวกัน เรียกว่ากุญแจดิบ (Raw Key)

หลังจากได้กุญแจดิบแล้ว ทั้งผู้ส่งและผู้รับจะต้องตรวจสอบกุญแจที่ได้ด้วยวิธีทางสถิติว่ามีผู้ดักจับหรือไม่ โดยการสุ่มกุญแจดิบขึ้นมาบางส่วนแล้วตรวจสอบว่าตรงกันหรือไม่ ถ้ามีบิตที่ไม่ตรงกันสูงมากแสดงว่าเกิดความผิดพลาดขึ้นระหว่างการส่ง ให้ถือว่ามีผู้ดักจับอยู่ในช่องสื่อสารนั่นเอง วิธีการนี้ทำให้สามารถตรวจสอบการเข้ามาของผู้ดักจับได้เสมอ และถ้าหากพบว่ามีผู้ดักจับจะต้องทิ้งกุญแจดิบนี้ไปแล้วเริ่มส่งกุญแจใหม่ ในกรณีที่กุญแจดิบตรงกันให้ละทิ้งบิตที่ได้เปิดเผยในการตรวจสอบผู้ดักจับนั้นไป บิตที่เหลือจะเป็นกุญแจที่จะนำไปใช้ในการเข้ารหัสด้วยวิธีการที่เหมาะสมต่อไป



รูปที่ 2.7 ต้นแบบระบบวิทยาการรหัสลับเชิงควอนตัมชุดแรกของโลก (ก) ภาพถ่ายระบบจริง และ (ข) ภาพจำลองพร้อมคำอธิบาย [Bennett et al., 1992]

ทฤษฎียืนยันความปลอดภัยของกุญแจ

จากที่กล่าวมาข้างต้นวิทยาการรหัสลับเชิงควอนตัม สามารถยืนยันความปลอดภัยด้วยหลักความไม่แน่นอนของไฮเซนเบิร์ก (Heisenberg Uncertainty Principle) ซึ่งจากหลักความไม่แน่นอนของไฮเซนเบิร์กกล่าวว่า ถ้าวัดโมเมนตัมของอนุภาคในส่วนประกอบตามแนวแกน x โดยมีความไม่แน่นอน Δp_x แล้ว ในขณะเดียวกันเราสามารถวัดตำแหน่งในส่วนประกอบตามแนวแกน x โดยมีความไม่แน่นอนต่ำสุดคือ $\Delta x = \hbar/(2\Delta p_x)$ โดยสรุปแล้ว เป็นไปไม่ได้ที่จะทำการทดลอง เพื่อวัดค่าของตัวแปรสองตัวที่ไม่เป็นอิสระของการวัดระหว่างกันได้อย่างแม่นยำพร้อมกันทั้งสองชุด [Nouredine, 2001] ยกตัวอย่างเช่น คู่ตัวแปรที่ไม่เป็นอิสระของการวัดสองตัวคือตำแหน่งและโมเมนตัม ที่ไม่สามารถหาตำแหน่งและโมเมนตัมของอนุภาคได้อย่างแม่นยำพร้อมกัน จากหลักการนี้สามารถเขียนในรูปทั่วไปได้ว่า ถ้าผู้สังเกต A และ B มีความสัมพันธ์กันแบบไม่เข้าคู่กันของการวัด (Incompatible) เมื่อมีการสังเกตอนุภาคใดๆ ในระบบเชิงควอนตัมด้วยลำดับการสังเกตที่ต่างกัน ทำให้ผลการสังเกตที่ได้มีค่าไม่เหมือนกัน เช่น เหตุการณ์ที่ผู้สังเกต A ทำการสังเกตก่อนผู้สังเกต B จะได้ผลการสังเกตต่างจากเหตุการณ์ที่ผู้สังเกต B เป็นฝ่ายเริ่มสังเกตก่อนแล้วผู้สังเกต A ทำการสังเกตในเวลาถัดมา ปรากฏการณ์ดังกล่าวสามารถอธิบายได้ว่า เมื่อผู้สังเกต A ทำการวัดค่าได้อย่างแม่นยำ ผู้สังเกต B จะไม่สามารถวัดค่าที่ถูกต้องได้หลังจากการสังเกตโดย A [Nouredine, 2001] จากหลักความไม่แน่นอนของไฮเซนเบิร์ก สามารถใช้ในการยืนยันความปลอดภัยของระบบวิทยาการรหัสลับเชิงควอนตัมได้ว่า ถ้ามีผู้ดักจับกุญแจระหว่างที่ผู้ส่งส่งไปยังผู้รับ จะทำให้รูปแบบของกุญแจที่ส่งเปลี่ยนแปลงและสามารถยืนยันได้ว่ามีการดักจับข้อมูลไป เป็นการยืนยันว่าระบบวิทยาการรหัสลับเชิงควอนตัมมีความปลอดภัยมากกว่าระบบวิทยาการรหัสลับอื่นในปัจจุบันที่ไม่สามารถยืนยันและตรวจสอบผู้ดักจับข้อมูลของระบบได้

นอกจากนั้นสำหรับระบบวิทยาการรหัสลับเชิงควอนตัม รูปแบบการสื่อสารจะใช้การแทนบิตของข้อมูลด้วยสถานะเชิงควอนตัมของอนุภาคเดี่ยว ยกตัวอย่างเช่นการแทนด้วยสถานะของโฟตอนเดี่ยว โดยอนุภาคเดี่ยวนี้ไม่สามารถแบ่งหรือทำซ้ำให้เหมือนเดิมทุกประการได้ [Wootters et al., 1982] นั่นคือสามารถยืนยันได้ว่าหากมีการลักลอบดักจับกุญแจรหัสไประหว่างการส่ง ผู้ลักลอบไม่สามารถทำซ้ำกุญแจให้เหมือนเดิมได้อย่างถูกต้องนั่นเอง

วิทยาการรหัสลับเชิงควอนตัมโดยโฟตอนเดี่ยว

วิทยาการรหัสลับเชิงควอนตัมที่อาศัยการส่งข้อมูลด้วยอนุภาคระดับควอนตัม จากผู้ส่งไปยังผู้รับในปัจจุบันมีหลากหลายรูปแบบ [Gisin et al., 2002] วิธีการหนึ่งที่ได้รับความสนใจและเริ่มมีใช้งานจริงในปัจจุบันคือวิทยาการรหัสลับเชิงควอนตัมโดยอาศัยโฟตอนเดี่ยวที่ถูกกำหนดสถานะเชิงควอนตัมแทนบิตข้อมูลจากผู้ส่งแล้วส่งไปยังผู้รับ การจะเข้าใจถึงกระบวนการเชิงลึกเพื่อการทดสอบระบบวิทยาการรหัสลับดังกล่าวจะอาศัยทฤษฎีต่าง ๆ ดังนี้

การอธิบายลักษณะของแสงด้วยกลศาสตร์ควอนตัมนั้น แสงประกอบขึ้นจากอนุภาคจำนวนมากที่ไม่สามารถแบ่งแยกได้ซึ่งเรียกว่าโฟตอน โฟตอนมีมวลนิ่งเป็นศูนย์โดยจะมีพลังงานจากสนามแม่เหล็กไฟฟ้า และเนื่องจากโฟตอนสามารถอธิบายได้ในรูปของคลื่นแม่เหล็กไฟฟ้าจึงมีโมเมนตัมเชิงมุม โฟตอนเคลื่อนที่ด้วยความเร็วคงตัวในสุญญากาศ แต่จะถูกหน่วงให้ช้าลงเมื่อผ่านตัวกลางอื่นๆ นอกจากนี้โฟตอนยังมีคุณสมบัติของคลื่นอยู่ทำให้สามารถแทรกสอดและเลี้ยวเบนได้ [Bachor et al. 2004]

การกำเนิดโฟตอนเดี่ยวสำหรับการประยุกต์ใช้งานต่างๆ นั้น แหล่งกำเนิดโฟตอนเดี่ยวจะต้องมีคุณสมบัติที่สำคัญคือ กำเนิดโฟตอนเพียงโฟตอนเดียวอย่างแท้จริง โดยโฟตอนที่เกิดขึ้นแต่ละโฟตอนมีความยาวคลื่นค่าเดียว แหล่งกำเนิดโฟตอนต้องมีประสิทธิภาพในการกำเนิดโฟตอนสูง และสามารถกำหนดช่วงเวลาในการกำเนิดโฟตอนได้

สำหรับการศึกษาวิจัยในช่วงแรกของการพัฒนาศาสตร์ด้านนี้นั้น ผู้วิจัยจะเน้นการศึกษาวิจัยเกี่ยวกับโฟตอนเดี่ยวดังกล่าวนี้ โดยอาศัยคุณสมบัติของโฟตอนเดี่ยวต่อการส่งสถานะทางควอนตัม วิธีการกำเนิดโฟตอนเดี่ยวที่นิยมใช้ในปัจจุบันคือการใช้สัญญาณพัลส์จากไดโอดชนิดเลเซอร์ความเข้มต่ำแล้วลดทอนความเข้มจนเหลือโฟตอนเดี่ยว ซึ่งความเป็นไปได้ในการเกิดโฟตอนจะเป็นไปตามสถิติของปัวซง (Poisson) เนื่องจากการกำเนิดโฟตอนเดี่ยวโดยอาศัยการลดทอนจำนวนโฟตอน อาจมีอุปสรรคจากบางครั้งที่มีโฟตอนมากกว่าหนึ่งโฟตอนหลุดออกมา รวมทั้งวิธีที่สามารถกำเนิดโฟตอนเดี่ยวคุณภาพที่เรียกว่าปืนยิงโฟตอนที่มีหลักการและกระบวนการต่างกันออกไป เมื่อพิจารณาแหล่งกำเนิดโฟตอนชนิดต่างๆ ที่เหมาะสมสำหรับงานวิจัยขั้นพื้นฐานนั้น จะใช้วิธีการลดความเข้มของแสงจากไดโอดชนิดเลเซอร์จนเหลือโฟตอนเดี่ยว เนื่องจากวิธีนี้มีความสะดวก และมีราคาไม่สูงมาก ทำให้สามารถสร้างชุดต้นแบบต่างๆ ให้มีขนาดเล็กและพร้อมปรับเปลี่ยนเพื่องานการสื่อสารที่คล่องตัวได้

วิธีการกำเนิดโฟตอนเดี่ยวนี้ด้วยวิธีการลดความเข้มจากแสงเลเซอร์จะใช้แสงเลเซอร์ชนิดพัลส์ เริ่มจากการใช้แสงที่เปล่งออกมาจากไดโอดเลเซอร์มาลดทอนความเข้มลง จะได้ความน่าจะเป็นที่จะมีโฟตอนเปล่งออกมาจำนวน n โฟตอน จากจำนวนโฟตอนเฉลี่ย μ โฟตอน ซึ่งเป็นไปตามหลักสถิติของปัวซง ดังนี้

$$P(n,\mu)=\frac{\mu^n}{n!}e^{-\mu} \tag{1}$$

จากสมการนี้มีบางครั้งที่จะเกิดโฟตอนมากกว่าหนึ่งโฟตอน ซึ่งความน่าจะเป็นที่จะเกิดโฟตอนมากกว่าหนึ่งโฟตอนนี้คือ

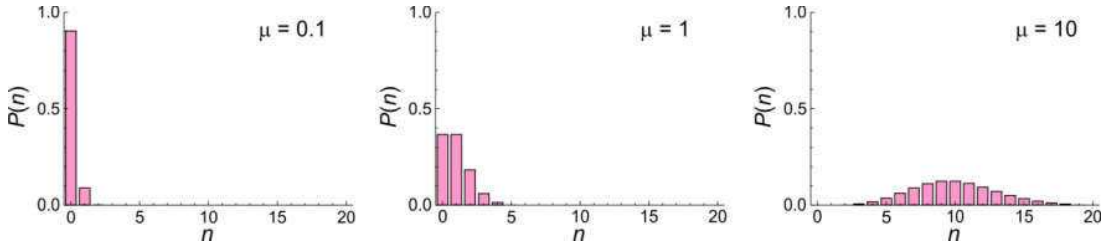
$$\begin{aligned} P(n>1|n>0,\mu) &= \frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)} \\ &= \frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}} \cong \frac{\mu}{2} \end{aligned} \tag{2}$$

วิธีการป้องกันปัญหานี้ทำได้โดยการเลือกใช้โฟตอนที่มีค่าเฉลี่ยต่ำมากๆ เช่นกำหนดให้มีจำนวนโฟตอนเฉลี่ย 0.1 โฟตอน ต่อสัญญาณพัลส์หนึ่งสัญญาณที่ส่งไปขับไดโอดเลเซอร์ (ดูรูปที่ 2.8)

หลังจากมีการส่งโฟตอนแล้ว การตรวจหาโฟตอนเดี่ยวต้องใช้อุปกรณ์ที่มีประสิทธิภาพสูง โดยตัวตรวจหาจะต้องมีคุณสมบัติที่สำคัญคือ มีประสิทธิภาพเชิงควอนตัมสูง มีความสามารถในการวัดโฟตอนเฉพาะช่วงความยาวคลื่นที่เหมาะสม มีอัตราความผิดพลาดในการตรวจหาสัญญาณเนื่องจากคุณสมบัติภายในต่ำ มีความเร็วในการตรวจหาโฟตอนและความเร็วในการคืนสภาพเพื่อตรวจหาโฟตอนในลำดับถัดไปสูง เทคโนโลยีการนับโฟตอนแบ่งเป็นสองรูปแบบคือ ตัวตรวจหาโฟตอนที่สัญญาณออกไม่ขึ้นอยู่กับจำนวนโฟตอน นั่นคือ

สัญญาณออกที่ได้จะมีขนาดเท่าเดิมแม้ว่าจะตรวจหาโฟตอนได้จำนวนกี่โฟตอนก็ตาม และตัวตรวจหาที่ขนาดของสัญญาณออกแปรตามจำนวนโฟตอนนั่นคือ ยิ่งตรวจหาจำนวนโฟตอนได้มากสัญญาณออกที่ได้จะมีขนาดเพิ่มขึ้น ในกรณีตัวตรวจหาโฟตอนสำหรับงานวิจัยนี้จะใช้ตัวตรวจหาที่ขนาดสัญญาณออกไม่ขึ้นกับจำนวนโฟตอน แต่สามารถตรวจสอบว่าโฟตอนที่ได้เป็นโฟตอนเดี่ยวจริงหรือไม่ด้วยวิธีทางสถิติ

จากลักษณะของตัวตรวจหาโฟตอนดังกล่าว ตัวตรวจหาโฟตอนที่มีความเหมาะสมคือ อะวาแลนช์โฟโต้ไดโอด (Avalanche photodiodes, APD) เนื่องจากการใช้งานสะดวก มีประสิทธิภาพเชิงควอนตัมสูงกว่าตัวตรวจหาชนิดอื่น มีขนาดเล็ก และอัตราการตรวจหาสัญญาณผิดพลาดเนื่องจากตัวตรวจหาเองต่ำ



รูปที่ 2.8 การแจกแจงของจำนวนโฟตอนต่อพัลส์แสงที่มีจำนวนโฟตอนเฉลี่ย μ ต่าง ๆ

วิทยาการรหัสลับเชิงควอนตัมโดยใช้คู่โฟตอนพัวพัน

นอกจากระบบวิทยาการรหัสลับเชิงควอนตัมโดยโฟตอนเดี่ยวแล้ว ในปี ค.ศ. 1991 มีการนำเสนอแนวคิดใหม่สำหรับระบบวิทยาการรหัสลับเชิงควอนตัมโดยอาศัยคุณสมบัติความพัวพันของคู่โฟตอน แล้วส่งโฟตอนไปยังผู้ส่งและผู้รับ จากนั้นจึงใช้คุณสมบัติของความพัวพันเชิงควอนตัมในการส่งและยืนยันความปลอดภัยของกุญแจ [Ekert, 1991] ซึ่งระบบการสื่อสารดังกล่าวอาศัยทฤษฎี ดังนี้

ความพัวพัน (Entanglement)

สำหรับระบบที่ประกอบด้วยสถานะเชิงควอนตัมมากกว่าหนึ่งสถานะ เช่น ระบบที่มีสถานะเชิงควอนตัมที่เรียกว่าคิวบิตสองสถานะ ในกรณีที่การอธิบายสถานะทั้งสองคิวบิตนั้นไม่สามารถเขียนแยกออกมาเป็นสถานะที่เป็นอิสระต่อกันได้ ถ้าทำการวัดค่าของคิวบิตแรกจะมีผลกระทบกับค่าของบิตที่สองเกิดขึ้นอย่างทันทีทันใด การที่ไม่สามารถแยกสถานะออกมาเป็นอิสระจากกันได้นั้นเรียกว่าสถานะพัวพัน (Entangled state) การกำหนดคิวบิตนั้นสามารถแสดงได้ในรูปสัญลักษณ์ $|0\rangle$ แทนบิต 0 และ $|1\rangle$ แทนบิต 1 โดยตัวอย่างของความพัวพันที่ชัดเจนคือ การแยกโมเลกุลของอะตอมสองอะตอมที่มีการสปินรวมเป็นศูนย์ โดยแต่ละอะตอมจะมีสปินเป็น 1/2 หลังจากแยกอะตอมและให้แต่ละอะตอมเคลื่อนที่ไปในทิศทางตรงกันข้าม ถ้ากำหนดอะตอมเป็นอะตอมที่ 1 และอะตอมที่ 2 เนื่องจากระบบนี้มีการอนุรักษ์โมเมนตัมเชิงมุม ดังนั้นระบบที่

เกิดขึ้นจะเป็นได้สองรูปแบบคือ อะตอมแรกมีสปินขึ้น อะตอมที่สองมีสปินลง หรือกลับกันคืออะตอมแรกมีสปินลง อะตอมที่สองมีสปินขึ้น โดยแสดงระบบได้ในรูปของฟังก์ชั่นคลื่น ดังนี้

$$\psi_{12} = \frac{1}{\sqrt{2}}\left(\left|\frac{1}{2}\right\rangle_1\left|-\frac{1}{2}\right\rangle_2 - \left|-\frac{1}{2}\right\rangle_1\left|\frac{1}{2}\right\rangle_2\right) \qquad (3)$$

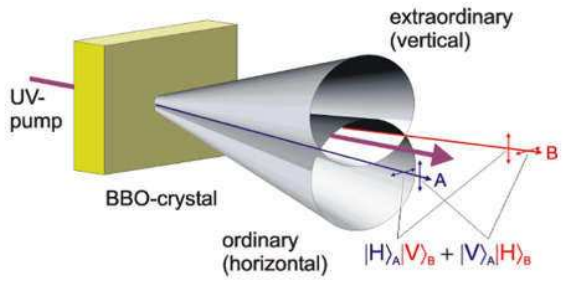
หลังจากการสร้างสถานะพัวพันได้ดังกล่าวแล้ว เมื่อแยกอะตอมทั้งสองอะตอมไปด้านตรงกันข้ามแล้ว การวัดค่าสปินของอะตอมใดๆ จะมีผลทำให้เกิดค่าสปินของอีกอะตอมหนึ่งที่สอดคล้องกับอะตอมแรกในทันที นั่นคือระบบของสองอะตอมนี้ไม่สามารถแยกจากกันได้และถือเป็นระบบเดียวกันแม้อะตอมจะอยู่ห่างกันก็ตาม โดยสถานะของความพัวพันนี้ยังสามารถใช้สำหรับระบบหลาย ๆ สถานะได้ด้วย

ความขัดแย้งของ EPR และทฤษฎีของเบลล์ (The EPR-Paradox and Bell's Theorem)

ในปี พ.ศ. 2478 Einstein, Podolsky และ Rosen ได้นำเสนอแนวคิดที่คาดว่าไม่สมบูรณ์แบบของกลศาสตร์ควอนตัม ซึ่งสามารถกล่าวโดยสรุปได้ว่า ถ้าอนุภาคสองอนุภาคมีอันตรกิริยากันในอดีต คุณสมบัติดังกล่าวนั้นจะไม่มีทางคงอยู่ต่อไปถึงอนาคตหากอนุภาคนั้นแยกจากกัน กล่าวคือการสังเกตสถานะเชิงควอนตัมของอนุภาคใดอนุภาคหนึ่งจะไม่มีผลกระทบกับอนุภาคที่อยู่ห่างออกไป ซึ่งหากการนำเสนอนี้เป็นจริงจะกล่าวได้ว่าทฤษฎีควอนตัมไม่สมบูรณ์ และความพัวพันเชิงควอนตัมจะไม่เกิดขึ้นจริง การถกเถียงปัญหาดังกล่าวมีอย่างยาวนานจนกระทั่งในปี พ.ศ. 2507 John Bell ได้ค้นพบวิธีการทดสอบระบบที่มีความพัวพันเชิงควอนตัม โดยอาศัยสมการทางคณิตศาสตร์ซึ่งเรียกว่าหลักความไม่สมดุลของเบลล์ (Bell's inequality) [Bell, 1964] ซึ่งจากสมการนี้สามารถใช้ได้กับระบบที่มีเพียงสองอนุภาคเท่านั้น โดยถ้าหากอสมการของเบลล์ถูกหักล้างได้ด้วยผลการทดลองใดๆ ก็ตามแสดงว่า กลศาสตร์ควอนตัมเป็นทฤษฎีที่ถูกต้อง ซึ่งในที่สุดก็มีการทดลองที่หักล้างอสมการนี้และยืนยันได้ว่ากลศาสตร์ควอนตัมมีความสมบูรณ์

การกำเนิดโฟตอนที่มีความพัวพันด้วยปรากฏการณ์ Spontaneous Parametric Down Conversion

Spontaneous Parametric Down Conversion (SPDC) คือ กระบวนการการทำลายโฟตอน แล้วให้กำเนิดโฟตอนสองโฟตอนที่มีความถี่ของคลื่นเป็นครึ่งหนึ่งของโฟตอนที่ถูกทำลาย แต่การจะเกิดเหตุการณ์นี้ได้ต้องจัดให้โฟตอนมีอันตรกิริยากับตัวกลางผลึกที่มีคุณสมบัติทัศนศาสตร์ไม่เชิงเส้น เมื่อโฟตอนเดี่ยวผ่านเข้าไปในผลึกมีความเป็นไปได้ที่จะเกิดโฟตอนออกมาสองโฟตอน ซึ่งคู่โฟตอนที่ออกมานั้นจะมีความพัวพัน โดยพลังงานและโมเมนตัมรวมของคู่โฟตอนจะเท่ากับโฟตอนเดี่ยวที่ผ่านเข้าไปในผลึกตามกฎการอนุรักษ์พลังงานและโมเมนตัม



รูปที่ 2.9 ปรากฏการณ์ SPDC ที่ทำให้เกิดการปลดปล่อยโฟตอนสองโคน [Bohm, 2003]

ในการจัดอุปกรณ์ เมื่อให้แสงเคลื่อนที่ผ่านผลึกที่มีคุณสมบัติไม่เชิงเส้นเช่น BBO (Beta-Barium Borate) ในแนวที่เหมาะสมจะทำให้เกิดโฟตอนออกมามีความน่าจะเป็นที่จะพบโฟตอนมีลักษณะเป็นกรวยสองกรวย กรวยหนึ่งเป็นแสงโพลาไรซ์แนวนอน อีกกรวยหนึ่งเป็นแสงโพลาไรซ์แนวตั้ง จุดที่กรวยทั้งสองตัดกันจะเป็นผลรวมของโพลาไรเซชันทั้งสองชนิด ซึ่งเป็นจุดที่เกิดคู่โฟตอนพัวพันซึ่งหากไม่ทำการวัดจะไม่สามารถทราบได้ว่าเป็นแสงโพลาไรซ์แนวตั้ง หรือแนวนอน โดยการจัดอุปกรณ์แสดงดังรูปที่ 2.9 [Bohm, 2003]

ในการจัดอุปกรณ์สำหรับกำเนิดคู่โฟตอนพัวพันโดยการผ่านผลึกที่มีคุณสมบัติเชิงทัศนศาสตร์ไม่เป็นเชิงเส้นจะมีปัญหาเรื่องของการที่โฟตอนที่มีโพลาไรซ์ในแนวนอน และแนวตั้ง เคลื่อนที่มาไม่พร้อมกันเนื่องจากคุณสมบัติของการเคลื่อนที่ผ่านผลึก จึงต้องมีการปรับให้แนวโฟตอนทั้งสองมาพร้อมกันโดยการใช้ผลึกครึ่งคลื่น (Half wave plate) มาหน่วงการเคลื่อนที่ของโฟตอนเพื่อให้เคลื่อนที่มาพร้อมกัน และสามารถนำคู่โฟตอนพัวพันนี้ไปใช้งานอื่นๆ ต่อไป [Bohm, 2003]

2.1.3 เครือข่ายควอนตัมที่ใช้ทดสอบวิทยาการรหัสลับเชิงควอนตัมในปัจจุบัน

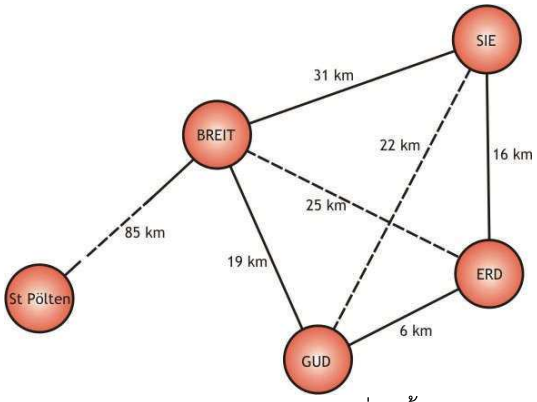
จากการศึกษาถึงความก้าวหน้าและสถานะภาพงานวิจัยของระบบวิทยาการรหัสลับเชิงควอนตัม เพื่อพิจารณาถึงแนวทางของงานวิจัยที่กำลังเป็นที่สนใจจากหน่วยงานต่างๆ ทั่วโลก และนำมาปรับใช้กับการดำเนินโครงการนี้ รวมทั้งเพื่อสร้างความตระหนักต่องานวิจัยที่เกี่ยวข้อง มีข้อสรุปดังนี้

-ทวีปยุโรป

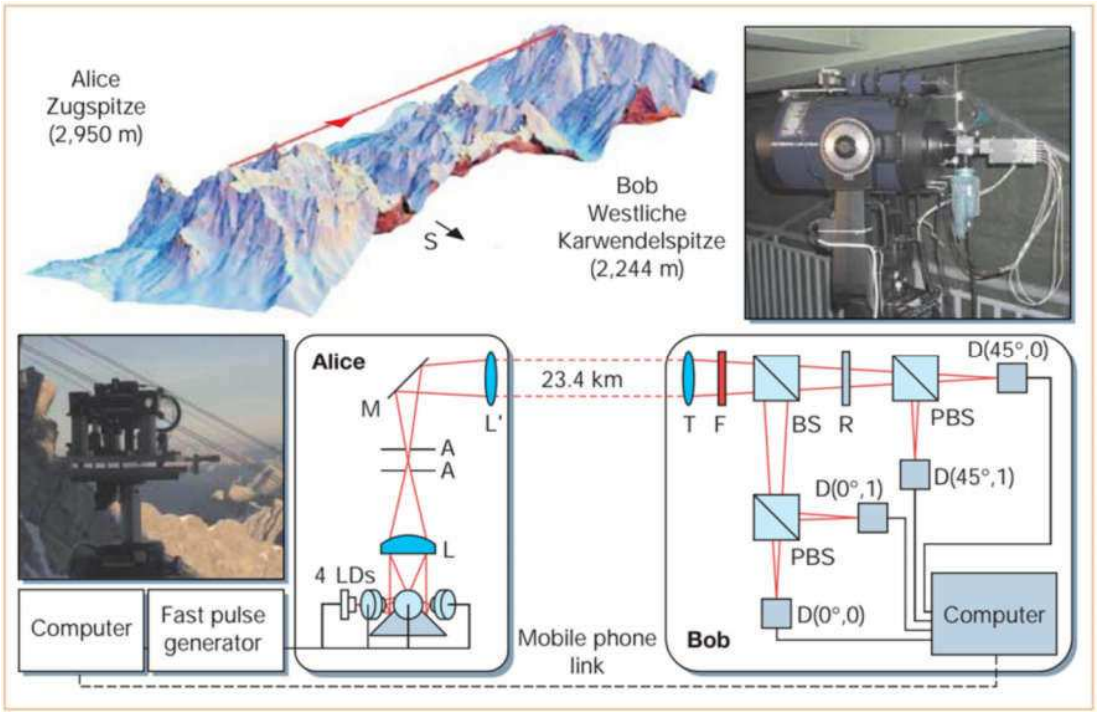
Development of a Global Network for Secure Communication based on Quantum Cryptography (SECOQC) เป็นกลุ่มงานวิจัยของทวีปยุโรป ได้ก่อตั้งกลุ่มวิจัยที่ประกอบด้วยสมาชิก 12 ประเทศด้วยงบประมาณกว่า 11 ล้านยูโร เพื่อแก้ปัญหาเรื่องความปลอดภัยของการส่งข้อมูลข่าวสารด้วยระบบวิทยาการรหัสลับเชิงควอนตัม กลุ่ม SECOQC ได้นำเสนอการสาธิตการทำงานแบบโครงข่ายของระบบ

วิทยาการรหัสลับเชิงควอนตัมแรกที่สมบูรณ์ประกอบด้วย 6 โนด 8 เส้นทาง ในวันที่ 8-10 ตุลาคม พ.ศ. 2551 [Peev et al., 2009]

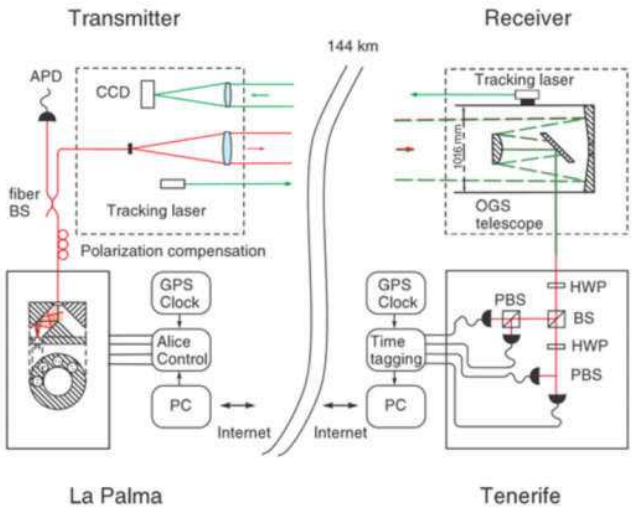
โดยก่อนหน้านั้น กลุ่มวิจัย Max Planck Institute for Quantum Optics จากมหาวิทยาลัย Ludwig Maximilians University of Munich ประเทศเยอรมนี ได้ทดสอบระบบวิทยาการรหัสลับเชิงควอนตัม โดยใช้โพลาไรเซชันของโฟตอนเดี่ยวตามเกณฑ์วิธี BB84 ส่งผ่านอากาศ ระยะทาง 23.4 กิโลเมตร ด้วยอัตราการส่งข้อมูล 1 กิโลบิตต่อวินาที มีความผิดพลาดร้อยละ 5 ในปี พ.ศ. 2545 (ดูรูปที่ 2.11) ถัดมาในปี พ.ศ. 2550 ทางสถาบันได้ร่วมมมือกับนักวิจัยจากหลายสถาบันในสหภาพยุโรป ทำการทดลองระบบวิทยาการรหัสลับเชิงควอนตัม โดยใช้โพลาไรเซชันของโฟตอนเดี่ยว ชนิด BB84 ส่งผ่านอากาศ ระยะทาง 144 กิโลเมตร ด้วยอัตราการส่งข้อมูล 12 บิต ต่อวินาที [Schmitt-Manderbach et al., 2007] (ดูรูปที่ 2.12)



รูปที่ 2.10 ลักษณะเครือข่าย SECOQC ที่ก่อตั้งในปีพ.ศ. 2551



รูปที่ 2.11 ภาพลักษณะการทดลองสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมที่ทดลองในปี พ.ศ. 2545 [Kurtsiefer et al., 2002]

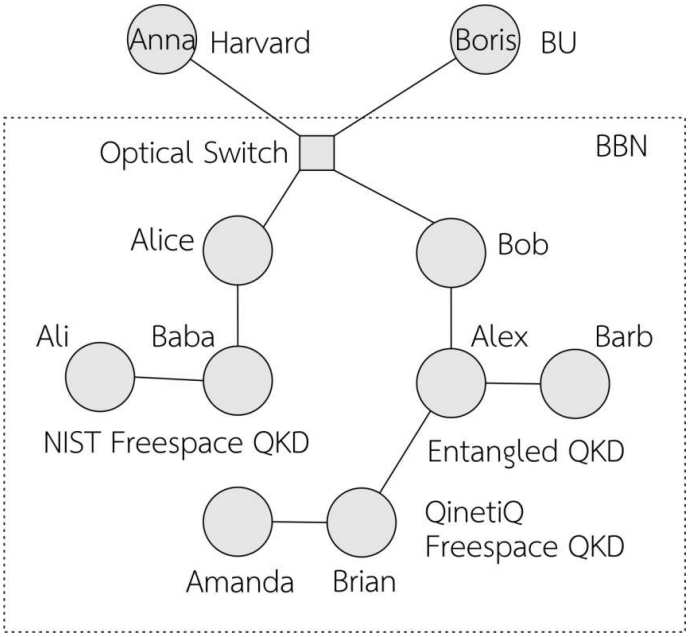


รูปที่ 2.12 ภาพลักษณะการทดลองสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม ที่ทดลองในปี พ.ศ. 2550 [Schmitt-Manderbach et al., 2007]

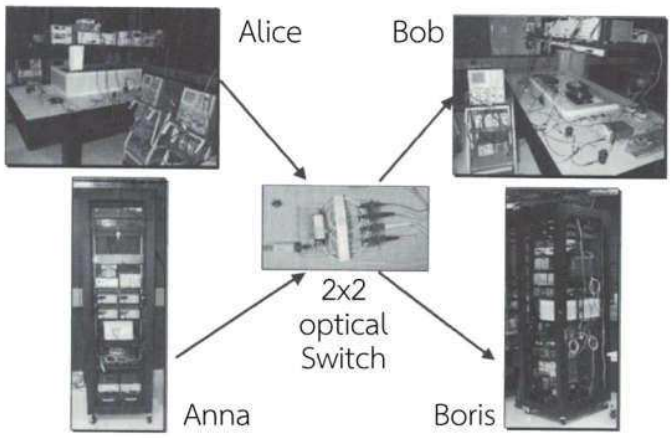
กลุ่มวิจัยจาก University of Vienna ประเทศออสเตรีย ทำการทดสอบระบบวิทยาการรหัสลับเชิงควอนตัมชนิดแหล่งกำเนิดชนิดคู่โฟตอนพัวพัน สำหรับการสื่อสารจริงในการทำธุรกรรมทางการเงิน ด้วยระยะทาง 1.45 กิโลเมตร ผ่านเส้นใยแสง ที่ความยาวคลื่น 810 นาโนเมตร ผลปรากฏว่ามีอัตราการส่งข้อมูล 80 บิตต่อวินาที ในปี พ.ศ. 2547 ต่อมาในปี พ.ศ. 2550 มีความร่วมมือกับนักวิจัยจากหลายสถาบันในสหภาพยุโรป ทดสอบระบบวิทยาการรหัสลับชนิดแหล่งกำเนิดคู่โฟตอนพัวพัน สื่อสารผ่านอากาศด้วยระยะทาง 144 กิโลเมตร ด้วยอัตราการส่งข้อมูล 178 บิตภายในเวลา 75 วินาที [Ursin et al., 2007]

-ทวีปอเมริกา

ประเทศสหรัฐอเมริกา มีการรวมกลุ่มกันสร้างโครงข่ายระบบวิทยาการรหัสลับเชิงควอนตัม โดยหน่วยงาน DARPA ซึ่งเป็นหน่วยงานของกระทรวงกลาโหมประเทศสหรัฐอเมริกา ให้ทุนในการสร้างเครือข่าย กลุ่มความร่วมมือของโครงการนี้ประกอบด้วยหน่วยงานหลัก ๆ คือ BBN Technologies เป็นบริษัทที่วิจัยและพัฒนาเทคโนโลยีชั้นสูงในประเทศสหรัฐอเมริกา สถาบันวิจัย Las Alamos ซึ่งเป็นสถาบันวิจัยแห่งชาติของประเทศสหรัฐอเมริกา National Institute of Standards and Technology (NIST) ของประเทศสหรัฐอเมริกา และ บริษัท QinetiQ จากสหราชอาณาจักร โดยปัจจุบันมีเครือข่ายทั้งหมด 10 จุด และสามารถใช้งานได้อย่างสมบูรณ์ [Elliott et al., 2005] (ดูรูปที่ 2.13) ตัวอย่างภาพถ่ายฮาร์ดแวร์ที่เชื่อมต่อในโครงข่ายนี้แสดงดังรูปที่ 2.14



รูปที่ 2.13 ลักษณะเครือข่าย DARPA [van Meter, 2014]



รูปที่ 2.14 ภาพถ่ายองค์ประกอบส่วนหนึ่งในเครือข่าย DARPA [van Meter, 2014]

-ทวีปเอเชีย

ประเทศญี่ปุ่น กลุ่ม Space Communications ของหน่วยงาน National Institute of Information and Communications Technology (NICT) ประสบความสำเร็จในการวัดคุณสมบัติโพลาไรเซชันของแหล่งกำเนิดเลเซอร์จากดาวเทียมวงโคจรต่ำ (low-earth-orbit: LEO) ผ่านชั้นบรรยากาศมายังพื้นดิน การวัดในครั้งนี้จะทำให้เกิดความก้าวหน้าของการสื่อสารโดยใช้แสงเลเซอร์ผ่านอากาศรวมไปถึงการออกแบบระบบการกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศในอนาคตด้วย [Toyoshima et al., 2009]

ประเทศสิงคโปร์ได้จัดตั้งศูนย์วิจัยเพื่อทำการวิจัยเกี่ยวกับเทคโนโลยีเชิงควอนตัม ณ มหาวิทยาลัยแห่งชาติประเทศสิงคโปร์ (The National University of Singapore) โดยได้รับงบประมาณ 150 ล้านเหรียญดอลลาร์สิงคโปร์ จาก Research Centre of Excellence (RCE) ในปี พ.ศ. 2550 ด้วยการลงทุนเชิญนักวิจัยที่มีชื่อเสียงระดับโลกเข้าร่วมงาน และวางแผนการสร้างเครือข่ายสื่อสารด้วนรหัสลับเชิงควอนตัมแรกบนเกาะสิงคโปร์ในอนาคตอันใกล้

จากการศึกษาข้อมูลงานวิจัยโดยสถาบันวิจัยต่างๆ พบว่าประเทศชั้นนำหลาย ๆ ประเทศของโลกมีหน่วยงานที่ทำงานวิจัยด้านวิทยาการรหัสลับเชิงคอนตัม รวมถึงมีการรวมกลุ่มวิจัยเพื่อพัฒนางานร่วมกัน พร้อมทั้งมีผลงานความก้าวหน้ามากขึ้นโดยลำดับ คณะผู้วิจัยฯ จึงได้พยายามสร้างความร่วมมือมาอย่างต่อเนื่องกับหลายหน่วยงานที่สำคัญข้างต้น เช่น NICT ประเทศญี่ปุ่นและกลุ่มวิจัย University of Vienna ประเทศออสเตรีย รวมถึงการเชิญนักวิจัยหลักระดับโลกเป็นนักวิจัยพี่เลี้ยง (Mentor) ดังรายละเอียดในบทที่ 4 ทั้งนี้เพื่อให้ประเทศไทยมีโอกาสได้ก้าวทันกับเทคโนโลยีนี้ที่ยังอยู่ในช่วงเริ่มต้น และสามารถพัฒนาจุดแข็งของงานนี้ไปสู่ความสำเร็จต่อไปได้

2.1.4 ผลิตภัณฑ์ที่เกี่ยวข้องกับเทคโนโลยี

คณะผู้วิจัยได้ทำการศึกษาและวิเคราะห์ข้อมูลทางธุรกิจ ณ ปัจจุบัน เพื่อศึกษาติดตามผลิตภัณฑ์ต่างๆ ที่มีพื้นฐานและเกี่ยวข้องกับการกำเนิดโฟตอนสำหรับการสื่อสารปลอดภัยที่เป็นที่สนใจโครงการวิจัยนี้ และเพื่อศึกษาทิศทางการประยุกต์รวมทั้งแนวโน้มเชิงพานิชย์ มีบทสรุปโดยสังเขปดังนี้

อุปกรณ์เชิงควอนตัมด้วยชุดโฟตอนเดี่ยว

- บริษัท Id Quantique ประเทศสวิตเซอร์แลนด์

Clavis II (รูปที่ 2.15) เป็นต้นแบบของชุดกระจายกุญแจเชิงควอนตัมเพื่อเป็นเครื่องมือสำหรับงานวิจัย โดยมีคุณสมบัติที่โดดเด่นต่อการสนับสนุนเครือข่ายวิทยาการรหัสลับด้วยอุปกรณ์ WDM สำหรับการแบ่งช่วงความยาวคลื่นเพื่อลดจำนวนสายไฟเบอร์ที่ใช้รับส่งข้อมูล มีระบบชดเชยความเสียหายที่เกิดจากการลดทอนได้แบบอัตโนมัติ แลกเปลี่ยนกุญแจรหัสลับด้วยอัตราเรวเฉลี่ย 1000 บิต/วินาทีที่ระยะทาง 100 กิโลเมตร ด้วยโปรโตคอล BB84 และ โปรโตคอล SARG (อุปกรณ์ชุดนี้มีราคาประมาณ 4,500,000 บาท พ.ศ. 2553)

รูปที่ 2.15 เครื่อง ClavisII [idquantique.net]

รูปที่ 2.16 เครื่อง Cerberis [idquantique.net]

Cerberis (รูปที่ 2.16) เป็นเครื่องสำหรับการเข้ารหัสที่เชื่อมต่อโดยสายแบบจุดต่อจุดที่ใกล้เคียงการรักษาความปลอดภัยของเครือข่าย เป็นการรวมผลิตภัณฑ์ของสองบริษัท คือบริษท Id Quantique ประเทศสวิตเซอร์แลนด์ กับบริษัท Senetas ประเทศออสเตรเลีย ซึ่งเครื่องมือนี้ออกแบบให้สามารถเชื่อมต่อ CypherNet ซึ่งเป็นอุปกรณ์สำหรับการเข้ารหัส จำนวนหลายตัวกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมเพียงเครื่องเดียวได้ เนื่องจากการใช้งานจริงจะส่งกุญแจรหัสลับเฉพาะบางเวลาเท่านั้น เครื่องชุดนี้จึงสามารถประหยัดเครื่องกระจายกุญแจรหัสลับเชิงควอนตัมได้ (อุปกรณ์ชุดนี้มีราคาประมาณ 4,500,000 บาท พ.ศ. 2553)

- บริษัท MagiQ Technologies ประเทศสหรัฐอเมริกา

MAGIQ QPN 7505 Security Gateway (รูปที่ 2.17) เป็นต้นแบบแรกของชุดกระจายกุญแจเชิงควอนตัมที่วางจำหน่ายของบริษัทนี้ สำหรับใช้ในเครือข่ายการสื่อสารแบบจุดต่อจุด โดยมีระยะในการส่งข้อมูลสูงสุด 120 กิโลเมตร ผ่านเส้นใยนำแสง สามารถสร้างกุญแจรหัสลับอย่างต่อเนื่องแบบเวลาจริงที่อัตราเร็ว 25.6 กิโลบิตต่อวินาที (ราคาประมาณ 5,000,000 บาท พ.ศ. 2553) MAGIQ QPN 8505 Security Gateway เป็นเครื่องที่พัฒนามาจากรุ่น 7505 สามารถใช้ในเครือข่ายการสื่อสารแบบจุดต่อจุด มีระยะในการส่งข้อมูลสูงสุด 140 กิโลเมตร ผ่านเส้นใยนำแสง และเพิ่มพอร์ตเชื่อมต่อผ่าน LAN (อุปกรณ์ชุดนี้มีราคาประมาณ 6,000,000 บาท พ.ศ. 2553)

รูปที่ 2.17 เครื่อง MAGIQ QPN 7505 และ QPN 8505 [magiq.net]

- บริษัท Smartquantum ประเทศฝรั่งเศส

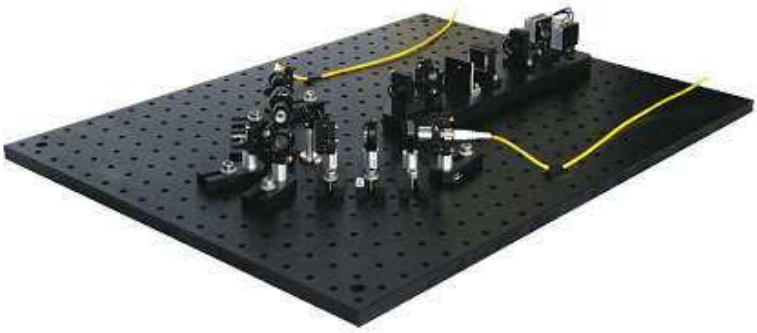
SQBox Defender (ดูรูปที่ 2.18) เป็นเครื่องมือที่ออกแบบให้สามารถใช้งานร่วมกับ QKD module และ Encryption module โดยเครื่องนี้สามารถเข้ารหัสลับได้ด้วยอัตราเร็ว 1 จิกะบิตต่อวินาที โดยใช้อัลกอริธัม AES ด้วยความยาวกุญแจรหัสลับ 192 บิต แลกเปลี่ยนกุญแจรหัสลับได้ระยะทาง 80 กิโลเมตร และระบบการทำงานเป็นแบบ Plug & Play (ราคาประมาณ 2,200,000 บาท พ.ศ.2553) ส่วน SQKey Generator เป็นชุดที่ใช้ในการสร้างกุญแจรหัสลับ โดยใชเทคโนโลยีเส้นใยนำแสง 1 เส้น สามารถส่งแสงได้ 2 ความยาวคลื่น สามารถแลกเปลี่ยนกุญแจรหัสลับได้ระยะทาง 80 กิโลเมตร และระบบการทำงานเป็นแบบ Plug & Play (ราคาประมาณ 2,000,000 บาท พ.ศ. 2553)

รูปที่ 2.18 เครื่อง SQBox Defender และ SQKey Generator [smartquantum.net]

อุปกรณ์เชิงควอนตัมด้วยชุดกำเนิดคู่โฟตอนพัวพัน

- บริษัท qutools ประเทศเยอรมันนี

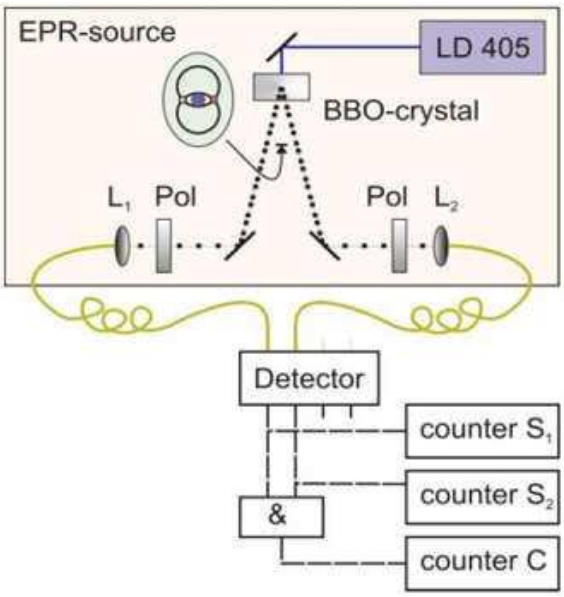
quED Entanglement Demonstrator (ดูรูปที่ 2.19) เป็นชุดกำเนิดคู่โฟตอนพัวพัน ซึ่งหลักการทำงานของ quED คือ การบังคับให้แสงเคลื่อนผ่านผลึก BBO ทำให้เกิดคู่ของแสงที่พัวพันกันโดยใช้แหล่งกำเนิดแสงเลเซอร์ขนาด 15 มิลลิวัตต์ ซึ่งมีผลต่อการเกิดอัตราสัญญาณที่มีความพัวพันกันมากกว่า 1 เมกกะเฮิรต์ และประสิทธิภาพของการเกิดคู่โฟตอนพัวพันมากกว่า 96% (อุปกรณ์ชุดนี้มีราคาประมาณ 900,000 บาท พ.ศ. 2553)



รูปที่ 2.19 เครื่อง quED Entanglement Demonstrator [qued.net]

- สถาบัน AIT (Austrian Institute of Technology) ประเทศออสเตรีย

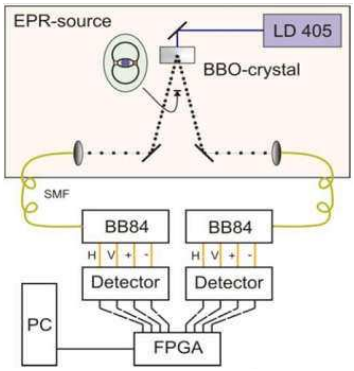
ชุดทดสอบระดับห้องปฏิบัติการ “Exploring entanglement” (ดูรูปที่ 2.20) ระบบนี้ประกอบด้วยแหล่งกำเนิดคู่โฟตอนพัวพัน และอุปกรณ์ที่จำเป็นสำหรับการพิสูจน์กฎความไม่ขึ้นกับตำแหน่ง ซึ่งเป็นจริงสำหรับกรณีของความพัวพัน ซึ่งการปรับโพลาไรเซชันทำได้โดยการหมุนโพลาไรเซอร์ ก่อนที่จะปรับแนวโฟตอนเขาสู่เส้นใยนำแสง หลังจากการตรวจหาโฟตอน ค่าที่นับได้จากเครื่องนับจำนวนโฟตอน (Photon Counter) ของตัวตรวจหาที่ 1 ตัวตรวจหาที่ 2 และตัวตรวจหาสำหรับโฟตอนที่มาพร้อมกัน (Coincidence) จะได้รับผลเนื่องจากความสัมพันธ์ของโพลาไรเซชัน (อุปกรณ์ชุดนี้มีราคาประมาณ 2,000,000 บาท พ.ศ. 2553)



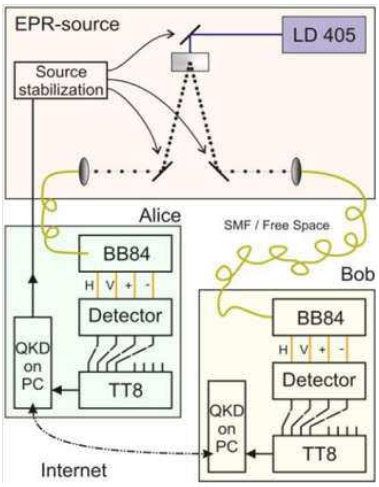
รูปที่ 2.20 การติดตั้ง “Exploring entenglement” [ait.net]

ชุดทดสอบระดับห้องปฏิบัติการ “EPR–photon pair source for QKD” ในระบบ QKD ที่ใช้แหล่งกำเนิดที่มีความพัวพัน เช่นการใช้คู่โฟตอนพัวพัน จะมีผลกระทบเนื่องจากการส่งผ่านเส้นใยนำแสง (เช่น การหมุนของโพลาไรเซชัน) จึงจำเป็นต้องมีการปรับชดเชยเพื่อลดจำนวนเหตุการณ์ที่ไม่ได้คู่โฟตอนตามที่คาดหวัง ความพัวพันของโพลาไรเซชันที่เกิดขึ้นจะถูกวิเคราะห์โดยชุดรับ BB84 ต้องมีการหมุนโพลาไรเซชันเพื่อลดผลกระทบเนื่องจากเส้นใยนำแสง โดยการหมุนโพลาไรเซชันเพื่อให้ตัวตรวจจับวัดได้เหตุการณ์ที่มีความพัวพันกัน ที่ปลายทั้งสองด้านของอุปกรณ์ โดยต้องมีการนับอัตราของโพลาไรเซชันในแนวแกนนอน (Horizontal: H) แนวแกนตั้ง (Vertical: V) แนวทแยงขวา (+45 องศา) และแนวทแยงซ้าย (-45 องศา) ได้เหมือนกับจำนวนที่เกิดขึ้นพร้อมกัน จากนั้นจะทำการปรับแหล่งกำเนิดแสงให้ได้โพลาไรเซชันที่ทำให้เกิด QBER ต่ำสุด (อุปกรณ์ชุดนี้มีราคาประมาณ 3,100,000 บาท พ.ศ. 2553)

ชุด QKD “Entanglement based QKD, secret key for Alice and Bob” (ดูรูปที่ 2.21 และ 2.22) อุปกรณ์ทุกชิ้นที่จำเป็นต่อระบบ QKD ถูกควบคุมด้วยคอมพิวเตอร์ซึ่งทำหน้าที่เป็นทั้ง QKD stack และจุดเก็บข้อมูล จากระบบนี้สามารถที่จะพัฒนาโปรโตคอลใหม่ๆ (เช่น Error Collection Routines) ได้โดยตรงจากการจัดอุปกรณ์ ความแตกต่างของอุปกรณ์ชุดนี้กับรุ่นอื่นๆ คือมีโมดูล Time-tagging เพื่อให้ทั้งระบบมีฐานเวลาเดียวกัน เพื่อให้สามารถยืนยันช่วงเวลาที่โฟตอนมาพร้อมกันได้ (อุปกรณ์ชุดนี้มีราคาประมาณ 5,200,000 บาท พ.ศ. 2553)



รูปที่ 2.21 การติดตั้ง “EPR-photon pair source for QKD” [ait.net]



รูปที่ 2.22 การติดตั้งชุด QKD ด้วยชุดกำเนิดคู่โฟตอนพัวพัน [ait.net]

จากการศึกษาและวิเคราะห์ข้อมูลทางธุรกิจของผลิตภัณฑ์ด้านวิทยาการรหัสลับเชิงควอนตัม พบว่า ปัจจุบันผลิตภัณฑ์ที่มีจำหน่ายในเชิงพาณิชย์ อาศัยวิธีการส่งข้อมูลด้วยสถานะเชิงควอนตัมของโฟตอนเดี่ยว เป็นส่วนใหญ่ แต่การศึกษาวิจัยและพัฒนาความรู้ด้านการสื่อสารเชิงควอนตัมพบว่า การส่งสถานะข้อมูลด้วยคู่โฟตอนพัวพันมีความเหมาะสมต่อการใช้งานในสภาพแวดล้อมจริง และสร้างความปลอดภัยให้กับข้อมูลได้มากกว่าการสื่อสารด้วยโฟตอนเดี่ยว [Jennewein et al., 2000] ทำให้หลายหน่วยงานเริ่มให้ความสนใจและพยายามศึกษาวิจัยและพัฒนาอุปกรณ์ด้านวิทยาการรหัสลับเชิงควอนตัมโดยอาศัยคู่โฟตอนพัวพันให้มีประสิทธิภาพสูงขึ้นเพื่อรองรับการใช้งานในอนาคต และในปัจจุบันยังไม่มีมาตรฐานใดรองรับการทำงานของชุดวิทยาการรหัสลับเชิงควอนตัม เนื่องจากเป็นเทคโนโลยีใหม่ที่เพิ่งเกิดขึ้นแต่เริ่มมีการใช้งานจริงในเชิงพาณิชย์ ทำให้หลายหน่วยงานของโลกที่กำลังศึกษาและพัฒนาเทคโนโลยีดังกล่าวพยายามรวมกลุ่มกัน เพื่อกำหนดมาตรฐานของการสื่อสารเชิงควอนตัมให้เป็นมาตรฐานสากล ภายใต้องค์กรที่ทำหน้าที่กำหนดมาตรฐานอุตสหกรรมทางด้านโทรคมนาคมแห่งสหภาพยุโรป หรือ ETSI (รายละเอียดเกี่ยวกับมาตราฐานที่ประกาศโดย ETSI แสดงดังภาคผนวก) การกำหนดมาตรฐานสำหรับการสื่อสารเชิงควอนตัมขณะนี้ยังอยู่ในช่วงเริ่มต้น คณะผู้วิจัยได้มีการประสานงานและมีความร่วมมือกับหน่วยงานที่เป็นสมาชิกของ ETSI เพื่อติดตามเทคโนโลยีที่มีผลกระทบ รวมถึงการมีส่วนร่วมในการกำหนดมาตรฐานสำหรับวิทยาการรหัสลับเชิงควอนตัมต่อไปด้วย

2.2 ลักษณะการอบรมและการเผยแพร่และประชาสัมพันธ์สู่สาธารณะ

ในการจัดสัมมนา ฝึกอบรม หรือการประชุมรวมกลุ่มวิจัยเฉพาะทางตามโครงการนี้ จะมีหัวข้อหลักที่บรรยายคือ เรื่องพื้นฐานและพัฒนาการเกี่ยวกับ การสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม โดยนอกจากการอบรม สัมมนาโดยมีวิทยากรคือผู้ดำเนินโครงการ (ผศ.ดร.สุวิทย์ กิระวิทยา) ผู้ร่วมโครงการ (ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์) และอาจารย์หรือเจ้าหน้าที่ที่เกี่ยวข้อง ยังมีการบรรยายพิเศษโดยผู้เชี่ยวชาญ และการสัมมนาภายหลังจากการอบรมอีกด้วย รูปที่ 2.23-2.26 แสดงตัวอย่างภาพบรรยากาศที่บันทึกระหว่างและหลังการบรรยาย


รูปที่ 2.23 ภาพบรรยากาศการในระหว่างการจัดอบรมวันที่ 19 กุมภาพันธ์ 2559 ณ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร


รูปที่ 2.24 ภาพบรรยากาศการในระหว่างการจัดอบรมวันที่ 21 มีนาคม 2559 ณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

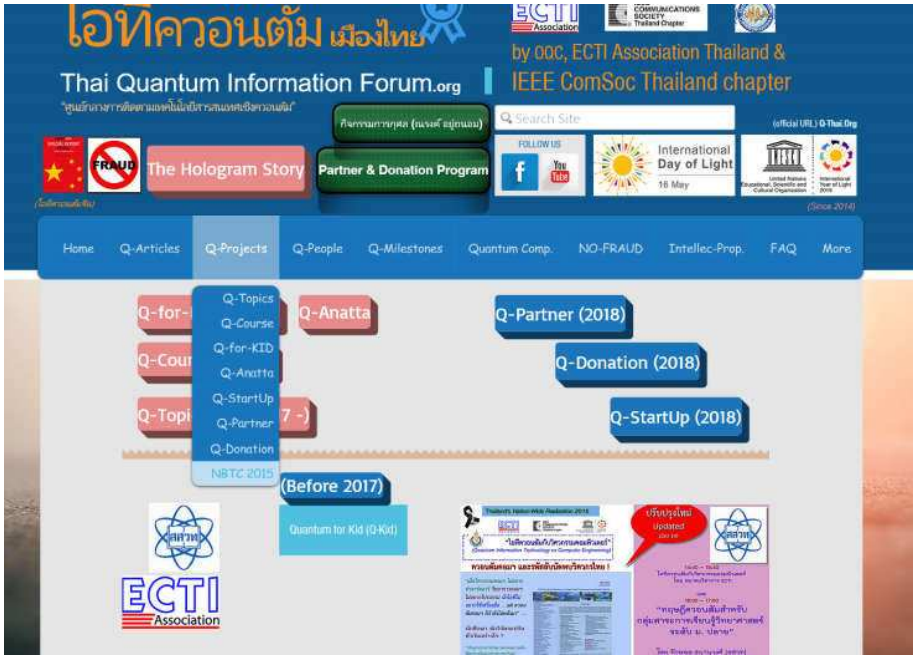

รูปที่ 2.25 ภาพบรรยากาศการในระหว่างการจัดอบรมวันที่ 25 มีนาคม 2559 ณ คณะอุตสาหกรรมสร้างสรรค์ มหาวิทยาลัยกาฬสินธุ์


รูปที่ 2.26 ภาพบรรยากาศการในระหว่างการจัดอบรมวันที่ 1 มิถุนายน 2559 ณ โรงเรียนมัธยมสาธิตมหาวิทยาลัยนเรศวร จังหวัดพิษณุโลก

สำหรับการเผยแพร่และประชาสัมพันธ์สู่สาธารณะเนื้อหาวิทยาการรหัสลับควอนตัมที่จัดทำขึ้นนั้น ทำผ่านอินเทอร์เน็ตเป็นหลัก ซึ่งมี 3 ช่องทางได้แก่

1. http://www.quantum-thai.org/
2. http://www.qinfo.nu.ac.th
3. เฟสบุ๊คกลุ่ม QuantumCryptoThailand

รูปที่ 2.27-29 แสดงตัวอย่างหน้าเวปดังกล่าว โดยรูปที่ 2.27 แสดงตัวอย่างหน้าเวป http://www.quantum-thai.org/ ที่มีเนื้อหาหลักที่นำเสนอในภาคผนวกของรายงานฉบับแสดงอยู่ภายใน



รูปที่ 2.27 http://www.quantum-thai.org/

รูปที่ 2.28 http://www.qinfo.nu.ac.th

รูปที่ 2.29 เฟสบุ๊คกลุ่ม QuantumCryptoThailand

2.3 บรรณานุกรม

[ลัญฉกร วุฒิสิทธิกุลกิจ และคณะ, 2548] ลัญฉกร วุฒิสิทธิกุลกิจ และคณะ, วิทยาการรหัสลับเบื้องต้น, สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, พ.ศ. 2548

[ait.net] [ait.net] http://www.ait.ac.at

[Bachor et al., 2004] H. A. Bachor, T. C. Ralph. A guide to experiments in quantum optics. second, revised and enlarged edition. Wiley-VCH verlag GmbH., Berlin. 2004.

[Bell, 1964] J. S. Bell, On the Einstein Podolsky Rosen paradox. Physics 1, pp 195-200, 1964.

[Bennett et al., 1984] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, Proc. IEEE Int. Conf. Computers, Systems and Signal Processing (Bangalore, India) 175-179, 1984.

[Bennett et al., 1992] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, Experimental Quantum Cryptography, Journal of Cryptology vol.5, no.1, pp. 3-28, 1992.

[Bohm, 2003] H. Bohm, A compact source for polarization entangled photon pairs, Master's thesis, Vienna University of. Technology, 2003.

[Ekert, 1991] A. K. Ekert, Quantum cryptography based on Bell’s theorem, Phys. Rev. Lett. 67, pp 661–663, 1991.

[Gisin et al., 2002] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. 74, 145-192, 2002.

[idquantique.net] http://www.idquantique.com

[Jennewein et al., 2000] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, Quantum Cryptography with Entangled Photons, Phys. Rev. Lett. 84, pp. 4729-4732, 2000.

[Kurtsiefer et al., 2002] C. Kurtsiefer P. Zarda, M. Halder et al., A step towards global key distribution, Nature 419, 450, 2002.

[magiq.net] http://www.magiqtech.com

[Nouredine, 2001] Z. Nouredine, Quantum Mechanics Concept and Applications, John Wiley & Suns, Inc, NewYork. 2001.

[Peev et al., 2009] M. Peev, C. Pacher, R. Alleaume et al., The SECOQC quantum key distribution network in Vienna, New J. Phys. 11, 2009.

[qued.net] http://www.qutools.com

[Schmitt-Manderbach et al., 2007] T. Schmitt-Manderbach, H. Weier, M. Furst et al., Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, Phys. Rev. Lett. 98, 2007.

[smartquantum.net] http://www.smartquantum.com

[Stallings, 2014] W. Stallings, Cryptography and Network Security, 6th Edition, Pearson, 2014

[Toyoshima et al., 2009] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, Y. Koyama, H. Kunimori, Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space, Optics Express, Vol. 17, Issue 25, pp. 22333-22340, 2009.

[Ursin et al., 2007] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach et al., Entanglement-based quantum communication over 144 km, Nature Physics 3, pp. 481 – 486, 2007.

[van Meter, 2014] R. Van Meter, Quantum Networking, ISTE Ltd 2014.

[Wootters et al., 1982] W. K. Wootters, and W. H. Zurek, A single quantum cannot be cloned, Nature (London) 299, 802–803. 1982.

บทที่ 3
รายงานสรุปการบรรยายพิเศษโดยผู้เชี่ยวชาญเฉพาะทางและทีมงาน

ในการจัดอบรมตามโครงการนี้มีการบรรยายพิเศษโดยผู้เชี่ยวชาญทั้งสิ้น 4 ครั้ง จากทั้งนักวิจัยไทยและต่างประเทศ โดยสรุปตามลำดับเหตุการณ์ ดังแสดงในตารางที่ 3.1 เนื้อหาที่นำเสนอในการบรรยายแต่ละครั้ง แสดงรายละเอียดไว้ในบทนี้

ตารางที่ 3.1 สรุปเหตุการณ์การบรรยายพิเศษที่จัดขึ้นในโครงการ

ผู้เชี่ยวชาญ	วันที่ และ สถานที่	หัวข้อที่บรรยาย
ผศ.ดร. วรานนท์ อนุกูล (ม.เชียงใหม่)	2 กันยายน 2558 ม. สุรนารี (นครราชสีมา)	การกักอะตอม: การวิจัยและพัฒนาที่ ม. เชียงใหม่
ศ.ดร. ประภาส จงสถิตย์วัฒนา (จุฬาลงกรณ์มหาวิทยาลัย)	21 มีนาคม 2559 ม. นเรศวร (พิษณุโลก)	การประยุกต์ใช้ควอนตัมอัลกอริทึม
Dr. Yi-Bo Zhao (Anhui Qasky Tech. Inc.)	28 มิถุนายน 2559 ECTI-CON 2016 (เชียงใหม่)	Quantum Cryptography Updating from China
Assoc. Prof. Dr. Wei Chen (University of Science and Technology, China)	28 มิถุนายน 2559 ECTI-CON 2017 (ภูเก็ต)	Applying Quantum Key Distribution Technology in Real-life Networks

3.1 การบรรยายพิเศษโดย ดร. วรานนท์ อนุกูล

การบรรยายพิเศษมีวิทยากรคือ ดร. วรานนท์ อนุกูล หัวหน้าห้องปฏิบัติการทัศนศาสตร์เชิงอะตอมควอนตัม ภาควิชาฟิสิกส์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ บรรยากาศการบรรยายแสดงในรูปที่ 3.1 โดยในการบรรยายนี้เป็นการกล่าวถึงรายละเอียดของระบบเชิงควอนตัมที่มีการศึกษากันในประเทศไทย (ที่ ม. เชียงใหม่) ซึ่งผู้ฟังได้แก่นักวิจัยจากศูนย์ซิงโครตรอนแห่งชาติ คณาจารย์ ม. สุรนารี และนักศึกษาระดับปริญญาตรี-โท-เอก โดยผู้ฟังให้ความสนใจอย่างมากในการอธิบายศาสตร์เชิงลึกด้านควอนตัมให้เข้าใจอย่างถ่องแท้เพื่อให้สามารถนำความรู้เหล่านี้มาประยุกต์ใช้ในด้านต่าง ๆ รวมถึงด้านการสื่อสารเชิงแสงโดยการเข้ารหัสลับควอนตัมด้วย

รูปที่ 3.1 ภาพบรรยากาศในระหว่างการบรรยายพิเศษโดยผู้เชี่ยวชาญ (ดร. วรานนท์ อนุกูล)

สาระสำคัญจากการบรรยายพิเศษโดยผู้เชี่ยวชาญครั้งที่ 1 สามารถสรุปได้ดังนี้ คือ เรา (ประเทศไทย) จำเป็นต้องมีหรือค้นหาเทคนิคใหม่ ๆ ในการสร้างระบบกำเนิดแสงที่มีความพัวพันและนำไปประยุกต์ใช้ในแง่ต่าง ๆ โดย ดร. วรานนท์ ได้นำเสนอการใช้ระบบดักจับอะตอมที่เป็นไอออน (ion trap) ที่กำลังพัฒนาขึ้นในห้องวิจัยทัศนศาสตร์อะตอมควอนตัมคณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ โดยในเบื้องต้นจะมีความพยายามสร้างอินเตอร์เฟียร์โรเมทรีเชิงอะตอม เพื่อก่อให้เกิดการปฏิสัมพันธ์ระหว่างอะตอมและแสง โดยผลการศึกษานี้จะสามารถนำไปประยุกต์ได้ในแง่ต่าง ๆ โดยการสื่อสารด้วยรหัสลับควอนตัมและการคำนวณเชิงควอนตัมก็เป็นแนวทางการประยุกต์แนวทางหนึ่งด้วย นอกจากนี้ยังอาจไปใช้ประโยชน์ในแง่การสำรวจแหล่งน้ำมันและก๊าซธรรมชาติได้อีกด้วย

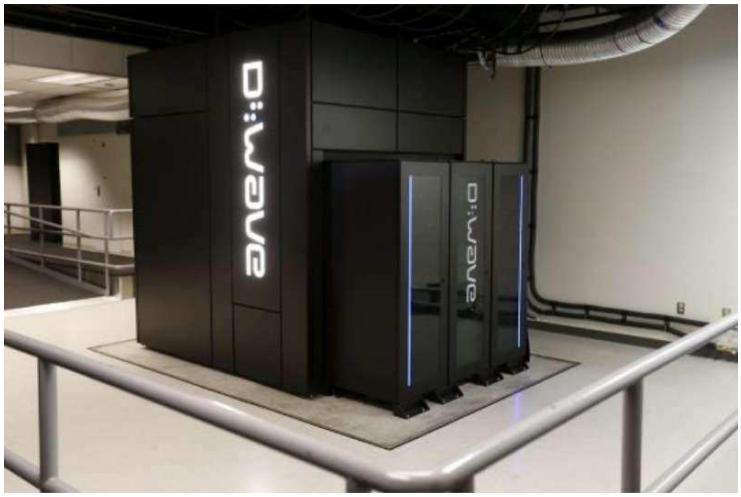
นอกจากอาจารย์วรนนท์ที่เชิญมาบรรยายแล้วยังมี นายจิรวัฒน์ ตั้งปณิธานนท์ นักศึกษาทุน พสวท. ที่กำลังศึกษาในระดับปริญญาเอก ณ Centre for Quantum Technologies, National University of Singapore ประเทศสิงคโปร์ ยังได้นำเสนองานวิจัยที่กำลังดำเนินงานอยู่ นั่นคือ การออกแบบและสร้างควอนตัมคอมพิวเตอร์ที่มีจำนวนคิวบิตมาก ๆ โดยเน้นถึงการนำเสนอปัญหาในการออกแบบ นั่นคือ การเพิ่มขึ้นเป็นทวีคูณของหน่วยความจำของคอมพิวเตอร์ปกติที่จำเป็นต้องใช้ในการออกแบบควอนตัมคอมพิวเตอร์ขนาดใหญ่

3.2 การบรรยายพิเศษโดย ศ.ดร. ประภาส จงสถิตย์วัฒนา

สำหรับในหัวข้อนี้ จะเป็นเนื้อหาเกี่ยวกับการบรรยายพิเศษโดยศาสตราจารย์ ดร.ประภาส จงสถิตย์วัฒนา อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย ที่จัดขึ้นที่ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร ในวันที่ 21 มีนาคม 2559 ในหัวข้อเรื่อง “การประยุกต์ใช้ควอนตัมอัลกอริทึม” ซึ่งเป็นส่วนสำคัญในการทำความเข้าใจการทำงานของระบบที่ใช้ถอดรหัสลับในการสื่อสารที่ใช้อยู่ในปัจจุบัน โดยการบรรยายทำโดยผ่านสื่อสไลด์และสื่อออนไลน์ (youtube)

หลักการทำงานของควอนตัมคอมพิวเตอร์

เริ่มต้นจากการเก็บข้อมูลที่เล็กที่สุดขนาด 1 บิต ซึ่งมีตัวเลขสัญลักษณ์ “0” และ “1” ถ้าเป็นคอมพิวเตอร์จะเก็บเป็นเลข 0 และ 1 แต่ควอนตัมคอมพิวเตอร์นั้นเก็บโอกาสที่จะเกิดเลข 0 และ 1 ทั้งนี้ยังสามารถเก็บข้อมูลที่เป็น 0 และ 1 ได้พร้อมกันด้วย ความพยายามที่จะเก็บตัวเลขแบบนี้ได้ต้องใช้อุปกรณ์ทางฟิสิกส์ที่ซับซ้อนมาก แต่เมื่อ 1 บิต ของควอนตัมมาต่อกันหลายๆ บิต แล้วทำให้การคำนวณเกิดขึ้นได้อย่างรวดเร็วขึ้น เพราะว่า 2 บิต แทนที่จะเป็นไปได้ 4 อย่าง แต่ 2 บิตในควอนตัมคอมพิวเตอร์สามารถคำนวณได้มากกว่านั้น เครื่องคอมพิวเตอร์ในรูปที่ 3.2 คือ เครื่องควอนตัมแอลนิลลิ่ง ซึ่งเป็นเครื่องคอมพิวเตอร์เฉพาะทางผลิตโดยบริษัท D-wave โดยให้ google ร่วมด้วย NASA ได้ใช้เครื่องคอมพิวเตอร์นี้เพื่อทดสอบ เครื่องนี้มีความจำประมาณ 1,000 คิวบิต การทำงานต้องอยู่ในความเย็นจัดใกล้ 0 องศาสัมบูรณ์ แต่ว่าการลดอุณหภูมิภายในเครื่องลงไปได้จนถึงอุณหภูมิดังกล่าวนั้นต้องใช้เวลาเกือบ 1 เดือน



รูปที่ 3.2 เครื่องควอนตัมแอลนิลลิ่ง (ควอนตัมคอมพิวเตอร์) ที่ผลิตโดยบริษัท D-wave

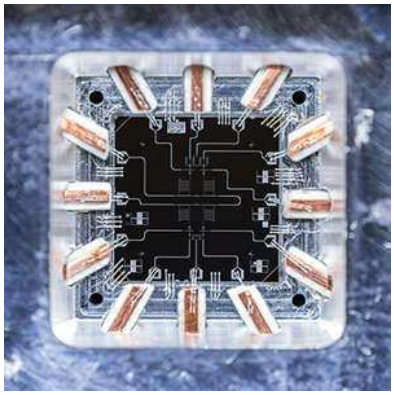
รูปร่างของเซอร์กิตที่ทำงานคำนวณของ quantum ภายในเครื่อง เซอร์กิตนี้ต้องแช่อยู่ในอุณหภูมิเย็นจัด นอกจากนี้ยังมีรูปร่างที่ค่อนข้างใหญ่ไม่เหมือนกับวงจรอิเล็กทรอนิกส์ทั่วๆไป (รูปที่ 3.3)

รูปที่ 3.3 รูปภายในของเครื่องควอนตัมคอมพิวเตอร์

การที่จะทำให้ควอนตัมคอมพิวเตอร์ทำงานได้นั้นต้องเขียนโปรแกรมเหมือนกับคอมพิวเตอร์ในปัจจุบัน นักวิทยาศาสตร์ได้คิดวิธีขึ้นมาหลายวิธีโดยวิธีเหล่านี้เราเรียกว่า อัลกอริทึม (algorithm) สำหรับควอนตัมอัลกอริทึมที่มีชื่อเสียงและทำให้คนทั่วโลกหันมาสนใจเทคโนโลยีควอนตัม คือ อัลกอริทึมการแบ่งแยกเลขจำนวนเต็ม โดยในปี 1994 Peter Shor ซึ่งเป็นนักคณิตศาสตร์ สามารถคิดวิธีคำนวณเพื่อแบ่งแยกเลขจำนวนขนาดใหญ่ แต่ถ้าเป็นวิธีที่ใช้ควอนตัมคอมพิวเตอร์ก็จะสามารถทำงานได้เร็วขึ้นจนนำมาใช้งานจริงได้ถ้ามีเครื่องควอนตัมคอมพิวเตอร์

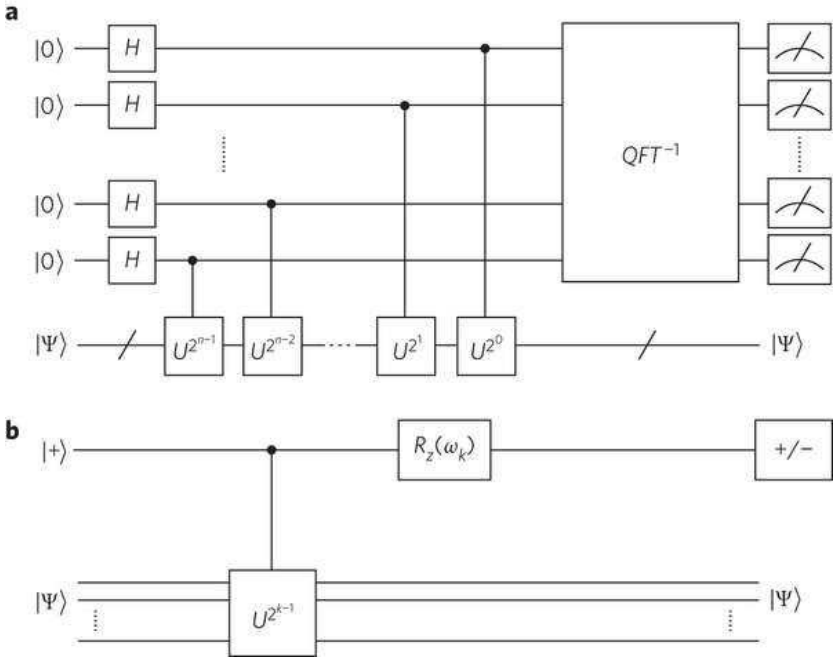
การคำนวณแยกตัวประกอบเฉพาะนั้นมีความสำคัญอย่างไร?

ในการรักษาความลับข้อมูลโดยการเข้ารหัสมีหลักการว่าไม่สามารถคำนวณองค์ประกอบเลขจำนวนเฉพาะขนาดใหญ่ได้ในเวลาอันรวดเร็ว ดังนั้นถ้าอัลกอริทึมของ Shor สามารถทำงานได้เร็วขึ้นก็จะทำให้การรักษาความลับด้วยคอมพิวเตอร์ในปัจจุบันล้มเหลวทั้งหมด อย่างไรก็ตามวิธีของ Shor ก็ยังคงต้องใช้วงจรควอนตัมจำนวนมาก ตัวอย่างเช่น ถ้ามีเลขจำนวน 4,096 บิต ก็ต้องใช้วงจรควอนตัมถึง 4,947,802,324,992 วงจร นอกจากนี้วงจรควอนตัมก็เป็นเรื่องที่นักวิทยาศาสตร์พยายามคิดค้นอยู่ หนึ่งในนั้นคือ วงจรควอนตัมสำหรับ 4 คิวบิตของบริษัท IBM ซึ่งเปิดตัวเมื่อปีที่แล้วแสดงดังรูปที่ 3.4



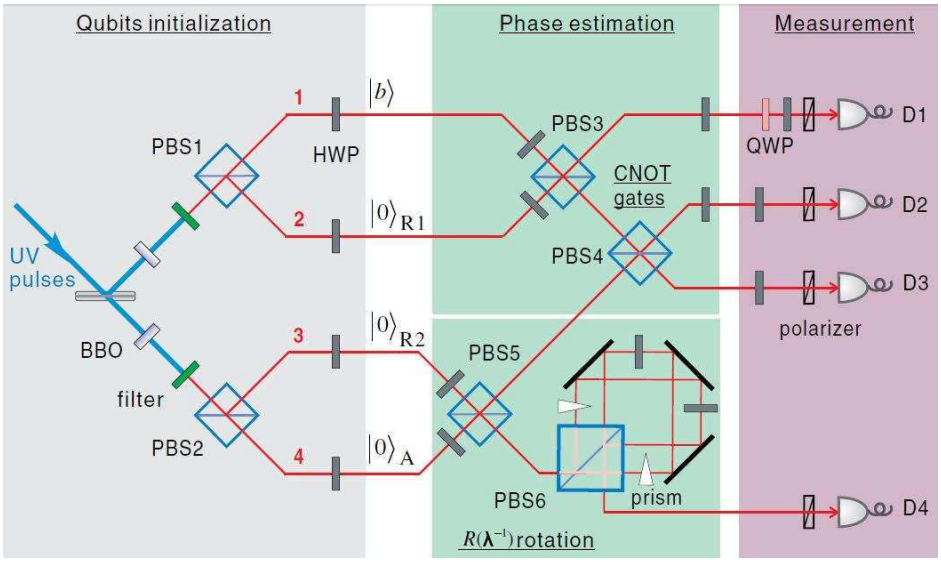
รูปที่ 3.4 วงจรควอนตัมของบริษัท IBM

โปรแกรมของควอนตัมคอมพิวเตอร์รูปสี่เหลี่ยมที่ปรากฏในรูปที่ 3.5 คือ หน่วยคำนวณประกอบด้วยวงจรควอนตัมเล็ก ๆ ภายใน โปรแกรมสำหรับควอนตัมคอมพิวเตอร์นี้คิดไม่เหมือนกับคอมพิวเตอร์ในปัจจุบัน แต่มีลักษณะคล้ายกับระบบแอนาล็อกที่ใช้ในช่วงสงครามโลกครั้งที่ 2 ดังนั้นการมองควอนตัมคอมพิวเตอร์ให้เป็นรูปวงจรคือการต่อวงจรเข้าด้วยกัน ด้านขวามือมีมิเตอร์เพื่อวัดสภาพในวงจร อย่างไรก็ตามถ้าต้องการให้เกิดการคำนวณนั้น คิวบิตในควอนตัมคอมพิวเตอร์ต้องอยู่ในสถานะพัวพัน (entangled state)



รูปที่ 3.5 วงจรควอนตัม

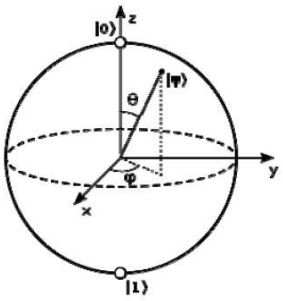
นอกจากเราจะสร้างควอนตัมเกตและต่อวงจรให้เป็นควอนตัมคอมพิวเตอร์ด้วยวงจรไฟฟ้าด้วยสภาพความเย็นจัดแล้ว อีกวิธีหนึ่งคือ การใช้แสง โดยภายในวงจรจะมีกระจกสะท้อนแสง แยกแสง สภาพโพลาไลเซชั่นของแสงเป็นต้น ทางขวามือของรูปที่ 3.6 เป็นการวัดผลที่เกิดขึ้น



รูปที่ 3.6 วงจรควอนตัมที่ใช้แสง

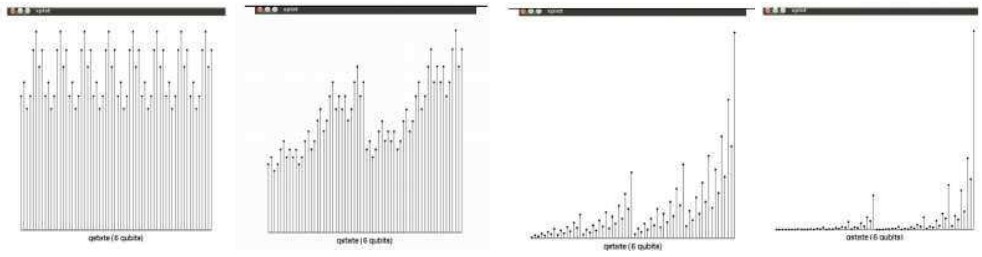
ปัญหา optimization

การศึกษาการทำงานของควอนตัมคอมพิวเตอร์ โดยการยกตัวอย่างปัญหา optimization ซึ่งเป็นงานวิจัยของอาจารย์ประภาสเมื่อปีค.ศ. 2012 การทำ optimization แบบหนึ่งซึ่งมีอยู่ในคอมพิวเตอร์ในปัจจุบันอยู่แล้ว โดยสนใจนำควอนตัมคอมพิวเตอร์มาแก้ปัญหานี้ แล้วลองเปรียบเทียบกัน ปัญหานี้ใช้เวลานานมาก แต่ถ้าใช้ ควอนตัมคอมพิวเตอร์แล้วทำงานได้เร็วขึ้นหรือไม่ โดยการทดลองขยับคำตอบเพื่อให้ได้คำตอบที่ดีที่สุด แต่ในโจทย์นี้มีตัวแปรจำนวนมา เสียเวลามาก และก็ไม่รู้ว่าคำตอบนั้นดีที่สุดหรือไม่ โดยเลือก 1 คิวบิต แทนด้วยรูปทรงกลม โดยค่าจะเป็นจุดๆหนึ่งบนพื้นผิวในวงกลมนี้ โดยขั้วโลกเหนือเป็นเลข 0 และขั้วโลกใต้เป็นเลข 1 ดังนั้นจะมีสองมุมที่กำกับค่าโอกาสการเป็น 0, 1 รูปทรงกลมนี้เรียกว่าแบบจำลองการคำนวณ 1 คิวบิต (รูปที่ 3.7) แต่ถ้าเรามีข้อมูลเป็นตัวเลข 1000 ค่า เราต้องการหาค่าที่มากที่สุด ถ้าเป็นคอมพิวเตอร์ในปัจจุบันต้องใช้เวลานามาก แต่ถ้าเป็นควอนตัมคอมพิวเตอร์ก็จะแสดงตัวเลขที่มีค่ามากที่สุดออกมาอย่างรวดเร็วและมีความรวดเร็วเท่ากันในการค้นหาคำตอบไม่ว่าจะมีจำนวนข้อมูลมาก-น้อย ซึ่งเป็นความแตกต่างอย่างสิ้นเชิงของคอมพิวเตอร์ปกติและ ควอนตัมคอมพิวเตอร์แต่ก็มีข้อเสียคือ อาจจะได้ตัวแปรขาเข้าและขาออกคนละแบบ ซึ่งอาจจะต้องมีการถามหลาย ๆ ครั้งเพื่อให้เกิดคำตอบที่ซ้ำกันและนั้นก็คือคำตอบที่ดีที่สุด



รูปที่ 3.7 แบบจำลองการคำนวณ

คำตอบที่วัดได้จากควอนตัมคอมพิวเตอร์แกน y คือ โอกาสที่คำตอบจะเป็น 0 (บน) หรือ 1 (ล่าง) แกน x คือ qc 6 bits ทั้งหมด 32 สถานะ โดยพบการกระจายคำตอบที่เปลี่ยนแปลงไป จนถึงคำตอบเกือบสุดท้ายทางขวามือสุดซึ่งก็มีโอกาสที่จะเป็นคำตอบที่ดีที่สุด (รูปที่ 3.8) จากผลการวิจัยพบว่าควอนตัมคอมพิวเตอร์สามารถคำนวณงานได้เร็วกว่าคอมพิวเตอร์มากในระดับเอกซ์โพเนลเชียล โดยการทดลองนี้แสดงให้เห็นว่าควอนตัมคอมพิวเตอร์เป็นการทำงานที่เร็วมาก แต่ข้อเสียคือปัจจุบันเรา (ประเทศไทย) ยังไม่มีควอนตัมคอมพิวเตอร์นั่นเอง



รูปที่ 3.8 คำตอบที่วัดได้จากควอนตัมคอมพิวเตอร์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการคำนวณเชิงควอนตัมนี้ ผู้สนใจสามารถศึกษาเพิ่มเติมได้จาก เวปไซท์ของอาจารย์ประภาส คือ http://www.cp.eng.chula.ac.th/~piak/talk/2016/issues-in-quantum-computing.htm

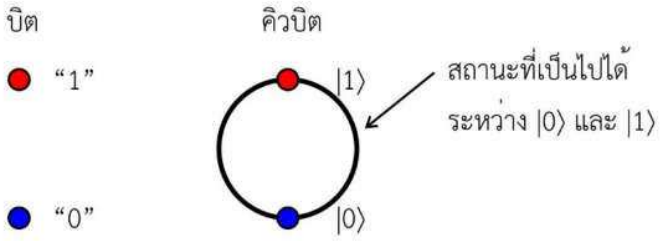
3.3 การบรรยายพิเศษโดย Dr. Yi-Bo Zhao

สำหรับในหัวข้อนี้ จะเป็นเนื้อหาเกี่ยวกับการบรรยายพิเศษโดย Dr. Yi-Bo Zhao ซึ่งเป็นผู้จัดการทั่วไปของบริษัท Anhui Qasky Technology Co. Ltd. (ประเทศจีน) ที่จัดขึ้นที่ โรงแรมดิเอ็มเพรส เชียงใหม่ ในการประชุมวิชาการ ECTI-CON 2016 ในวันที่ 28 มิถุนายน 2559 ในหัวข้อเรื่อง “Quantum Cryptography Updating from China” ซึ่งผู้เชี่ยวชาญท่านนี้เป็นบุคคลสำคัญในการดำเนินโครงการการสร้างเครือข่ายความปลอดภัยสูงด้วยรหัสลับควอนตัมในประเทศจีนทั้งในระบบเครือข่ายเส้นใยนำแสงและระบบสื่อสารผ่านดาวเทียม

หลักการทำงานของการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

เริ่มต้นจากการแนะนำให้รู้จัก สารสนเทศที่ใช้งานอยู่ในปัจจุบัน เทียบกับ สารสนเทศเชิงควอนตัม โดยสารสนเทศที่ใช้อยู่ในปัจจุบันจะมีการเก็บข้อมูลที่มีหน่วยเล็กที่สุดเป็นบิต ซึ่งใช้ตัวเลขสัญลักษณ์ “0” และ “1” แทนข้อมูลที่เก็บ แต่ถ้าหากเป็นสารสนเทศเชิงควอนตัมนั้น เราจะเก็บข้อมูลเป็นคิวบิต (qubit) ซึ่งก็คือโอกาสที่จะเกิด “0” และ “1” (มิใช่ข้อมูลระหว่างเลข 0 และ 1, ดูรูปที่ 3.9) โดยคิวบิตนี้มีคุณสมบัติที่สำคัญ คือ การที่ไม่มีใครสามารถทำซ้ำ (copy) ข้อมูลเชิงควอนตัมในคิวบิตนี้ได้อย่างถูกต้องร้อยเปอร์เซ็นต์ โดยคุณสมบัตินี้เป็นคุณสมบัติของอนุภาคเชิงควอนตัมที่เป็นที่มาของแนวคิดการใช้ปรากฏการณ์ทางควอนตัมในการส่งข้อมูลที่ต้องการความปลอดภัยสูง และแตกต่างจากข้อมูลแบบดั้งเดิมที่ใช้อยู่ในปัจจุบันที่เก็บอยู่ในรูปแบบต่าง ๆ ที่เราสามารถทำการทำซ้ำได้อย่างง่ายดาย

ในการส่งข้อมูลที่กล่าวถึงในการบรรยายนี้ เราจะพิจารณาเฉพาะโฟตอน (แสง) เท่านั้น เนื่องจากมีความเร็วสูงและในปัจจุบันเราก็ใช้แสงในการส่งข้อมูลกันอยู่แล้วเช่นในเครือข่ายเส้นใยนำแสง

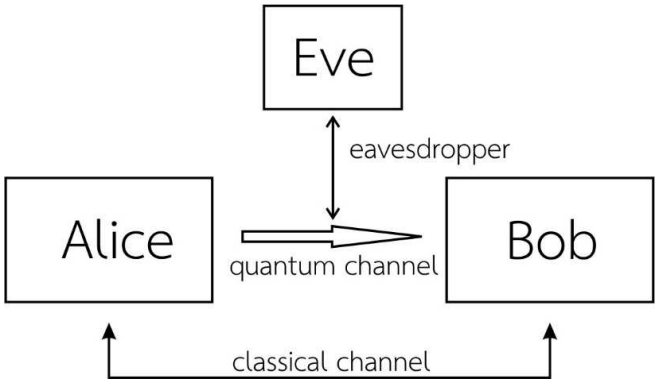


รูปที่ 3.9 บิตและคิวบิต

โปรโตคอลหลักที่ใช้ในการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม คือ โปรโตคอล BB84 ซึ่งมีรายละเอียดที่มากเกินกว่าจะกล่าวถึงได้ทั้งหมดในที่นี้ แต่สามารถกล่าวถึงส่วนสำคัญหลักได้คือ ในระบบสื่อสาร เราจะมีผู้ส่งสาร คือ อลิซ (Alice) ผู้รับสาร คือ บอบ (Bob) และ มีผู้ที่คอยดักฟัง คือ อีฟ (Eve) (ดูรูปที่ 3.10) เมื่ออลิซทำการส่งโฟตอนเดี่ยวออกไป การที่จะตรวจพบโฟตอนนั้น (โดยบอบหรืออีฟ) ก็จะทำให้โฟตอนนั้นถูกดูดกลืนหายไปด้วย ดังนั้นผู้ที่รับโฟตอนจะทำให้โฟตอนหายไปและไม่สามารถทำซ้ำโฟตอนนั้นได้ถูกต้องร้อยเปอร์เซ็นต์ นั่นคือ หากอีฟเป็นผู้รับโฟตอน อีฟก็จะต้องสร้างโฟตอนตัวใหม่ที่อาจจะมีคุณสมบัติต่างอออกไป ออกมาแล้วส่งไปให้บอบ เมื่อบอบกับอลิซตรวจสอบโฟตอนที่ส่งถึงกันผ่านทางช่องทางสื่อสารปกติก็จะสามารถทราบการมีอยู่ของอีฟได้ โดยเราจะทำการนำข้อมูลที่ต้องการส่งไปปรับเปลี่ยนคุณสมบัติของโฟตอนเดี่ยวที่ส่งออกไป

หากมีผู้ดักฟัง (อีฟ) ในระบบสื่อสาร อีฟอาจลักลอบอ่านคุณสมบัติของโฟตอนที่ส่งและได้รับข้อมูลได้ การที่อีฟได้รับข้อมูลที่ส่งในเบื้องต้นนั้น อีฟก็ยังไม่สามารถตีความข้อมูลนั้นออกมาได้ เนื่องจาก ลักษณะของการส่งข้อมูลรหัสลับเชิงควอนตัม เราจะทำการส่งคีย์ดิบ (raw key) ซึ่งเป็นสิ่งที่จะใช้ในการวิเคราะห์ความปลอดภัยของช่องทางสื่อสาร ก่อนที่เราจะนำไปใช้ในการเข้ารหัสต่อไป โดยข้อมูลที่อีฟอ่านได้ในเบื้องต้นนี้จะต้องถูกอ่านอย่างถูกต้องด้วยจึงจะได้ข้อมูลที่ถูกต้อง/เชื่อถือได้ออกมา ซึ่งอีฟจะยังไม่สามารถบอกหรือทราบความถูกต้อง/เชื่อถือได้ของข้อมูลในการดักเก็บข้อมูลในตอนต้นนี้

โดยแนวคิดของการสื่อสารเชิงควอนตัมที่กล่าวถึงนี้ ได้รับการพิสูจน์ในเชิงคณิตศาสตร์แล้วว่า จะทำให้ระบบสื่อสารมีความปลอดภัยสูงสุด



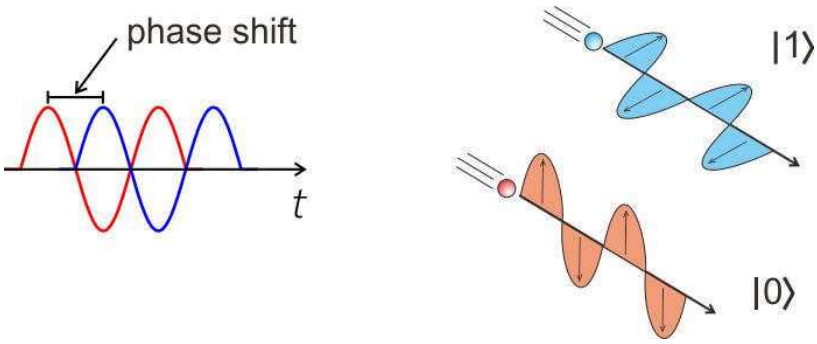
รูปที่ 3.10 รูปแบบการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

ความปลอดภัยของการสื่อสารเชิงควอนตัม

ในการส่งข้อมูลที่มีความสำคัญ ปัจจุบันเราจะทำการเข้ารหัสข้อมูลสำคัญนี้ด้วยคีย์ โดยคีย์ที่ใช้ในปัจจุบันเรียกว่า คีย์สาธารณะ (public key) การถอดรหัสข้อความนี้จะทำได้โดยผู้ที่ทราบคีย์ส่วนตัว (private key) ที่นำมาใช้ในการสร้างคีย์สาธารณะนี้ การทำทำได้โดยการนำคีย์มาผ่านฟังก์ชันทางคณิตศาสตร์ที่ซับซ้อน

ในกระบวนการสื่อสารเชิงควอนตัมให้มีความปลอดภัยสูงสุดนั้น เราจะอาศัยการส่งข้อมูลผ่านควอนตัมแชนแนลก่อน โดยข้อมูลนี้จะเป็นคีย์ของการส่งข้อมูลจริงต่อไป ดังนั้นคีย์ที่ใช้ก็จะปลอดภัยจากการดักฟังอย่างแน่นอน โดยเราเรียกการสื่อสารเชิงควอนตัมนี้ว่า การกระจายคีย์เชิงควอนตัม (quantum key distribution, QKD)

ปัจจุบันเทคนิคของการสื่อสารทางควอนตัมมีการพัฒนาไปในหลากลายทิศทาง เช่นการใช้เทคนิคตัวแปรต่อเนื่อง (continuous variable) สำหรับการสื่อสารด้วยโปรโตคอล BB84 มีการพัฒนาและสร้างระบบจริงโดยการนำข้อมูลไปใส่ในสถานะทางเฟสของโฟตอน และ การนำไปใส่ในสถานะทางโพลาไรซ์ของโฟตอน



รูปที่ 3.11 การเข้ารหัสโดยใช้การเลื่อนเฟส และ การใช้สถานะทางโพลาไรซ์ของโฟตอน

การวัดในระบบทางควอนตัม หากมองเป็นคณิตศาสตร์ ก็คือ การทำการใส่ตัวดำเนินการเข้าไปแล้วทำการอินทริเกรตเพื่อหาความน่าจะเป็นของผลการวัดที่พิจารณา ความปลอดภัยของการสื่อสารสามารถพิสูจน์ได้โดยใช้พื้นฐานของคณิตศาสตร์สำหรับการวัดระบบเชิงควอนตัมนี้

การพิสูจน์ว่าระบบสื่อสารหนึ่ง ๆ นั้นปลอดภัย เราสามารถกล่าวได้อย่างมั่นใจว่า ระบบสื่อสารทางด้านควอนตัมนั้นปลอดภัย แต่เราจะต้องพิจารณาระบบสื่อสารแบบดั้งเดิมด้วย ทั้งนี้เพราะระบบสื่อสารปลอดภัยสูงสุดจะใช้ทั้งระบบสื่อสารเชิงควอนตัมและระบบสื่อสารแบบดั้งเดิม ในการใช้ระบบสื่อสารแบบดั้งเดิม เราจะยังคงต้องมีการระบุตัวตน (authentication) ด้วย เพื่อให้มั่นใจในตัวผู้ส่งสารและผู้รับสาร โดยระบบการสื่อสารทางควอนตัมจะเป็นระบบที่เสริมเข้าไป เพื่อให้คีย์ที่ใช้มีความปลอดภัยสูงสุด โดยการใช้คีย์นี้จะทำตั้งแต่กระบวนการระบุตัวตนก่อนจะทำการสื่อสารจริง

โดยทั่วไป การระบุตัวตน (authentication) ไม่มีทางปลอดภัยร้อยเปอร์เซ็นต์ เนื่องจาก อีฟอาจทำตัวเหมือนบอบได้อย่างที่ไม่สามารถแยกแยะด้วยเครื่องมือใด ๆ ที่มีในระบบสื่อสารได้ ดังนั้นการสื่อสารจะปลอดภัยสูงสุดได้นั้น เราจะต้องมีการปรับปรุงวิธีการระบุตัวตนซึ่งเป็นกระบวนการดั้งเดิมด้วย

การสื่อสารปลอดภัยสูงนี้ อาจไม่จำเป็นสำหรับระดับบุคคลแต่มีความสำคัญมากสำหรับประเทศ เช่น ในอเมริกา หรือ ญี่ปุ่นนั้น มีการพัฒนางานด้านนี้ไปมาก โดยไม่มีการเปิดเผยข้อมูลเชิงลึก ผู้บรรยายเชื่อว่าปัจจุบันการสื่อสารหลาย ๆ ช่องทางในหลายประเทศในโลกนี้ไม่ปลอดภัย (คือถูกดักฟังอยู่) ดังนั้น เมื่อมีการสื่อสารข้อมูลอะไรที่สำคัญ ก็มีความเป็นไปได้ว่า มีผู้อื่นรู้และนำไปใช้ประโยชน์ได้ ตัวอย่างในประวัติศาสตร์เช่น การทำสงครามในอิรัค อเมริกาได้ทำการทำลายระบบเครือข่ายสื่อสารในอิรัค ทำให้ทหารฝ่านอิรัคไม่สามารถต่อสู้ได้อย่างมีประสิทธิภาพส่งผลให้แพ้สงครามในที่สุด

นอกจากนี้ การพัฒนาควอนตัมคอมพิวเตอร์อย่างรวดเร็ว จะบังคับให้เราต้องเปลี่ยนกระบวนการเข้ารหัสที่ใช้ในการสื่อสารในปัจจุบัน เนื่องจากควอนตัมคอมพิวเตอร์นี้สามารถนำมาใช้ถอดรหัสของกระบวนการเข้ารหัสที่ใช้ในการสื่อสารที่เราใช้อยู่ในปัจจุบันได้อย่างมีประสิทธิภาพ เมื่อมองในแง่นี้ เราสามารถกล่าวได้ว่า กระบวนการทางควอนตัมนำมาซึ่งทั้งควอนตัมคอมพิวเตอร์และวิธีการเข้ารหัสเชิงควอนตัม โดยมีการทำนายว่า เราจะต้องเปลี่ยนวิธีการเข้ารหัสให้ปลอดภัยจากการคุกคามของควอนตัมคอมพิวเตอร์ภายในระยะเวลา 10 ปี

ระบบสื่อสารปลอดภัยสูงสุดที่พัฒนาขึ้นในประเทศจีน

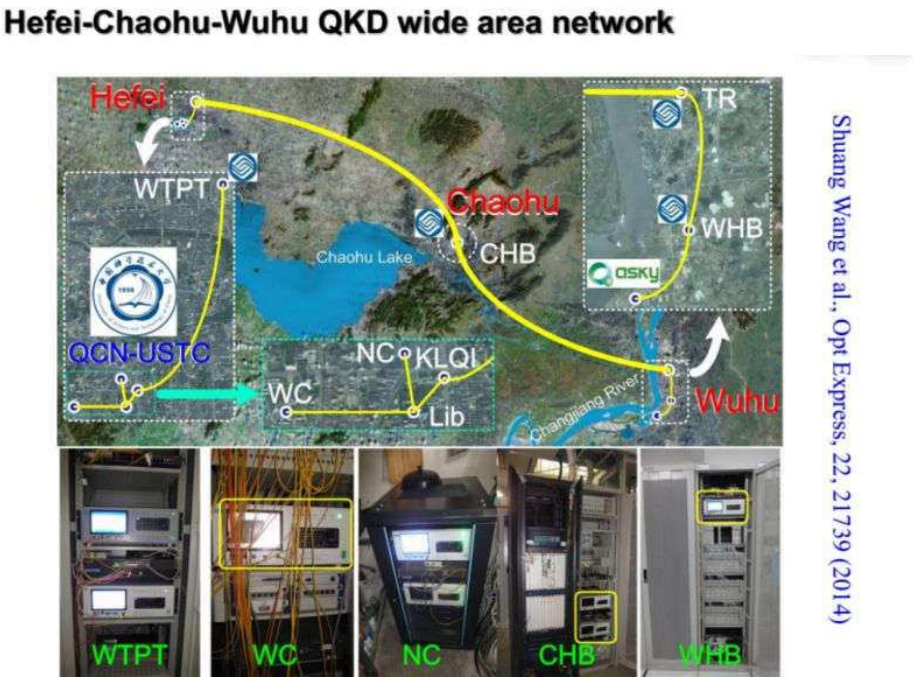
สำหรับการสื่อสารปลอดภัยสูงสุดที่พัฒนาในประเทศจีน คณะวิจัยได้เริ่มต้นในปี ค.ศ. 2001 ซึ่งปัจจุบันได้ล้ำหน้าการพัฒนาในประเทศอื่น ๆ (อเมริกา ญี่ปุ่น ออสเตรีย) ไปแล้ว ปัจจุบันระบบที่ใช้ทดสอบอยู่เป็นรุ่นที่ 3 โดยในระบบรุ่นที่ 1 เป็นระบบที่ยังสร้างอยู่บนโต๊ะออปติคอยู่ เพื่อสาธิตการทำงาน และ มีความพยายามทำเป็นผลิตภัณฑ์ ในรุ่นที่ 2 สำหรับรุ่นที่ 3 นี้ เป็นรุ่นที่พร้อมจำหน่ายและที่จะนำไปใช้จริง

รูปที่ 3.12 ระบบตัวกระจายคีย์เชิงควอนตัมที่จำหน่ายโดย บริษัท Qasky

ในการพัฒนาระบบสื่อสารนี้ เรามีการทดสอบการใช้จริงหลายครั้ง โดยครั้งแรกทำในปีค.ศ. 2004 ระหว่างเมือง Anhui และ ปักกิ่ง โดยได้ทดสอบด้วยเส้นใยนำแสงที่เช่าจากบริษัทสื่อสาร ซึ่งหลังจากนั้น ก็ได้

ทำการสร้างเครือข่ายขึ้นเอง ที่เมืองปักกิ่ง โดยเครือข่ายที่สร้างขึ้นนี้เป็นเครือข่ายที่สองในโลก ที่สร้างเพื่อใช้กับการสื่อสารด้วยรหัสลับควอนตัม โดยในการทดสอบแต่ละครั้ง ก็มีการนำเสนอผลการทดสอบในรูปแบบบทความด้วย

ในปีค.ศ. 2011 ได้มีการพัฒนาระบบสื่อสารเชิงควอนตัมที่ใช้ความถี่สูงระดับประมาณ 1 GHz และส่งข้อมูลในระยะไกล ประมาณ 260 กิโลเมตร ซึ่งการพัฒนาเทคนิคการส่งข้อมูลนี้ (ด้วยตัวตรวจจับแสงแบบตัวนำยิ่งยวด) ทำให้สามารถส่งข้อมูลได้อย่างมาก และทำให้ได้ ความเร็วในการส่งข้อมูล มากกว่า 40 Kpbs โดยการพัฒนานี้ เป็นความร่วมมือระหว่าง รัฐบาลจีนและมหาวิทยาลัย (University of Science and Technology of China) โดยมหาวิทยาลัยได้นำความรู้ด้านเทคโนโลยีต่าง ๆ มาร่วมก่อตั้งเป็นบริษัท Startup ชื่อ Qasky ปัจจุบันบริษัทนี้มีเทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมทั้งชนิดจากจุดหนึ่งไปยังจุดหนึ่งและชนิดเครือข่ายจำหน่าย นอกจากนี้ยังมีการพัฒนาอุปกรณ์สื่อสารอื่น ๆ ด้วย เช่น ควอนตัมเราเตอร์ ตัวตรวจวัดโฟตอนเดี่ยว เป็นต้น โดยปัจจุบันบริษัทมีสิทธิบัตรมากกว่า 40 ฉบับ



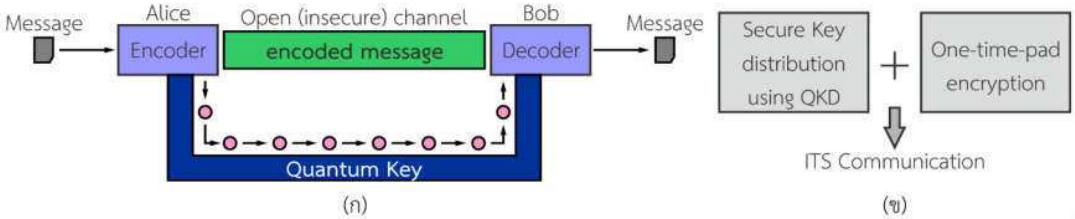
รูปที่ 3.13 ระบบเครือข่ายที่ใช้พัฒนาระบบสื่อสารเชิงควอนตัม

3.4 การบรรยายพิเศษโดย Assoc. Prof. Dr. Wei Chen

สำหรับในบทนี้ จะเป็นเนื้อหาเกี่ยวกับการบรรยายพิเศษโดย Assoc. Prof. Dr. Wei Chen ซึ่งเป็นอาจารย์จาก University of Science and Technology (UTSC) ประเทศจีน โดยการบรรยายนี้จัดขึ้นในการประชุมวิชาการ ECTI-CON 2017 ในวันที่ 28 มิถุนายน 2560 ในหัวข้อเรื่อง “Applying Quantum Key Distribution Technology in Real-life Networks” ซึ่งผู้เชี่ยวชาญท่านนี้เป็นบุคคลสำคัญในการดำเนินโครงการการสร้างเครือข่ายความปลอดภัยสูงด้วยรหัสลับควอนตัมในประเทศจีนทั้งในระบบเครือข่ายเส้นใยนำแสงและระบบสื่อสารผ่านดาวเทียม สำหรับการบรรยายครั้งนี้ ได้มีการบันทึกเสียงและเผยแพร่ผ่านเว็บไซท์ YouTube (https://www.youtube.com/watch?v =04Lv7O_Ogc8)

แนะนำเบื้องต้นเกี่ยวกับการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

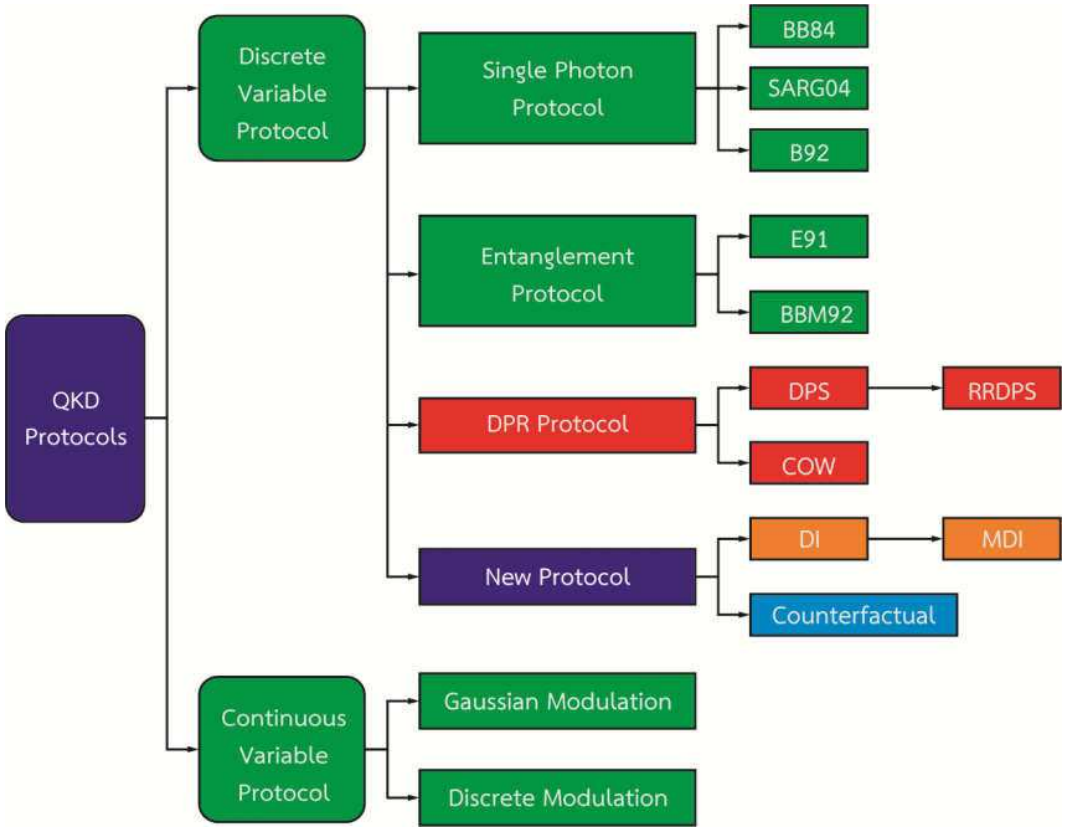
เริ่มต้นจากการแนะนำให้รู้จัก เกี่ยวกับเทคโนโลยีควอนตัม ซึ่งมีหัวข้อที่เป็นที่สนใจมากที่สุดในปัจจุบัน คือ การคำนวณเชิงควอนตัม หรือ ควอนตัมคอมพิวติ้ง (quantum computing) โดยกล่าวถึงว่าการคำนวณนี้สามารถถูกนำมาใช้ในการถอดรหัสข้อมูลที่เข้ารหัสและส่งถึงกันในอินเทอร์เน็ตได้ ซึ่งความสามารถดังกล่าวถือเป็นภัยคุกคามอย่างหนึ่ง ทำให้ผู้ที่ทำงานด้านการสื่อสารข้อมูลจะต้องสนใจเทคโนโลยีที่นำมาแก้ปัญหานี้ หากว่ามีการนำควอนตัมคอมพิวเตอร์มาใช้กันอย่างแพร่หลาย การสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมเป็นวิธีการหนึ่งที่สามารถนำมาใช้แก้ปัญหาข้างต้นได้ โดยระบบเชิงควอนตัมที่กล่าวถึงนี้ เรียกว่า การกระจายกุญแจเชิงควอนตัม (Quantum Key Distribution) โดยการใช้เทคนิคที่ปลอดภัยสูงสุดที่เรียกกว่า one-time-pad ร่วมกับการส่งสถานะทางควอนตัมของโฟตอนในช่องทางสื่อสารที่แยกออกมาต่างหาก การสื่อสารด้วยระบบนี้จะทำให้เราสามารถส่งข้อมูลได้อย่างปลอดภัยสูงสุด แม้ว่าจะมีการใช้งานควอนตัมคอมพิวเตอร์แล้วก็ตาม รูปที่ 3.14(ก) แสดงลักษณะการส่งข้อมูลในระบบการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม โดยกุญแจเชิงควอนตัมจะถูกส่งผ่านควอนตัมแชนแนลด้วยอัตราเร็วค่อนข้างต่ำ และถูกนำไปใช้เข้ารหัสข้อมูลที่ส่ง



รูปที่ 3.14 (ก) ลักษณะทั่วไปของการใช้วิทยาการรหัสลับเชิงควอนตัมในการสื่อสารปลอดภัยสูงสุด และ (ข) แนวคิดของการเข้ารหัสสำหรับการสื่อสารปลอดภัยสูงสุด

ปกติเพื่อให้เกิดการส่งข้อมูลที่ปลอดภัยสูงสุด รูปที่ 3.14(ข) แสดงแนวคิดของการเข้ารหัสสำหรับการสื่อสารปลอดภัยสูงสุด

โปรโตคอลเกี่ยวกับการส่งข้อมูลเชิงควอนตัมในปัจจุบันมีมากมายหลายโปรโตคอล ซึ่งแต่ละโปรโตคอลก็จะมีเทคนิคทางการประมวลสัญญาณต่างกันและแสดงสรุปได้ดังในรูปที่ 3.15 ในปัจจุบันฮาร์ดแวร์และระบบการสื่อสารปลอดภัยสูงสุดด้วยกุญแจเชิงควอนตัมที่ถูกทดสอบกันมากที่สุดจะใช้โปรโตคอล BB84 เป็นหลัก โดยโปรโตคอลนี้จะเป็นชนิดตัวแปรไม่ต่อเนื่อง และ การส่งข้อมูล จะใช้คุณสมบัติโฟตอนเดี่ยว ในการนำเสนอนี้ จึงขอกล่าวถึงโปรโตคอล BB84 นี้เป็นหลักเท่านั้น



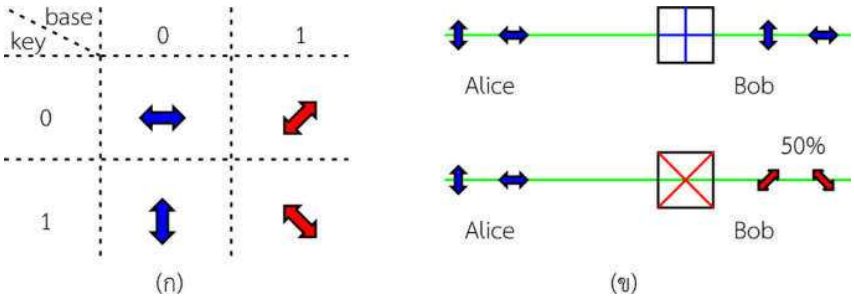
รูปที่ 3.15 ภาพสรุปการแบ่งโปรโตคอลของการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

อุปกรณ์สำหรับการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: จากแนวคิดสู่อุปกรณ์จริง

แนวคิดเบื้องต้นของการใส่ข้อมูลเข้าไปในสถานะทางควอนตัมของแสง คือ การกำหนดสถานะโพลาไรซ์ของแสง โดยกำหนดให้ฐาน (base) ของการมอดูเลตสัญญาณมีสองแบบคือ 0 และ 1 และกำหนดให้กุญแจ (key) ที่จะส่งอยู่ในรูปของรหัสเลขฐาน 2 ซึ่งก็คือ 0 หรือ 1 จะได้ว่า สถานะโพลาไรซ์ที่ส่งออกไป มีได้ 4 ลักษณะ ดังแสดงในรูปที่ 3.16(ก) ซึ่งการกำหนดลักษณะนี้เป็นแนวคิดเบื้องต้นของโปรโตคอล BB84 โดยหลักการแล้ว ผู้ส่ง (คือ Alice) จะกำหนดฐานที่ใช้แบบสุ่มและส่งข้อมูลคีย์ซึ่งได้จากการสุ่มผ่านไปให้ผู้รับ (คือ Bob) โดยมอดูเลตไปกับทิศทางโพลาไรซ์ของโฟตอนเดี่ยว คีย์ที่ส่งให้ขั้นต้นนี้เรียกว่า Raw key และผู้รับก็จะเลือกฐานที่ใช้ในการถอดรหัสข้อมูลคีย์นี้อย่างสุ่มโดยการเลือกแกนของการดีมอดูเลตโพลาไรซ์ของแสง ดังนั้นโอกาสที่ผู้รับจะเลือกฐานเดียวกันกับผู้ส่ง จะมีค่าความน่าจะเป็นเป็น 50% ดังรูปที่ 3.16(ข) จากนั้นจึงมีการสื่อสารระหว่างผู้รับและผู้ส่งผ่านช่องทางปกติ เพื่อกรองคีย์ข้อมูลให้เหลือเพียงข้อมูลที่แน่นอน ที่เรียกว่า Sifted key โดยผู้รับและผู้ส่งจะไม่ส่งตัวคีย์ที่ส่งในควอนตัมแชนแนลให้แก่กัน

หากมีผู้เข้ามาดักจับข้อมูล (คือ Eve) ผู้ดักจับจะต้องสร้างสัญญาณข้อมูลโฟตอนเดี่ยวใหม่ เพื่อมิให้ผู้รับทราบว่ามีการดักจับข้อมูล ซึ่งเมื่อ ผู้สร้างข้อมูลใหม่นี้ไม่ทราบฐานของการมอดูเลต การส่งข้อมูลโดยผู้ดักจับข้อมูลนี้ก็จะสามารถถูกตรวจสอบได้โดยง่าย จากผู้รับและผู้ส่งตัวจริง และ เมื่อระบบทราบว่าไม่ปลอดภัย (เนื่องจากมีผู้ดักจับข้อมูล) ระบบนี้ก็จะหยุดทำงาน เพื่อเป็นการป้องกันรักษาความลับของข้อมูล

แนวคิดการส่งข้อมูลในการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมนี้ นำไปสร้างได้จริง โดยเริ่มจากด้านระบบควอนตัม คือการใช้แหล่งกำเนิดโฟตอนเดี่ยวสร้างโฟตอนและส่งไปยัง อุปกรณ์มอดูเลตทางแสง โดยการส่งข้อมูลด้วยสถานะทางควอนตัมของแสงในโลกปัจจุบัน มี 2 ทาง คือ ทางอากาศ (free space) และทางเส้นใยนำแสง (fiber) และสำหรับการรับข้อมูลโฟตอนเดี่ยวนี้ เราจะต้องมีอุปกรณ์ดีมอดูเลตสัญญาณโฟตอนเดี่ยวและตัวตรวจจับโฟตอนเดี่ยวติดตั้งอยู่ที่ฝั่งผู้รับ และเนื่องจากการข้อมูลที่ส่งในลักษณะโฟตอนเดี่ยวนี้มีความบอบบางมาก ทำให้เราจำเป็นต้องแยกช่องทางการส่งอย่างชัดแจ้ง คือ ระบบการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมนี้ไม่สามารถใช้ทรัพยากรร่วมกับระบบสื่อสารที่มีอยู่เดิมได้

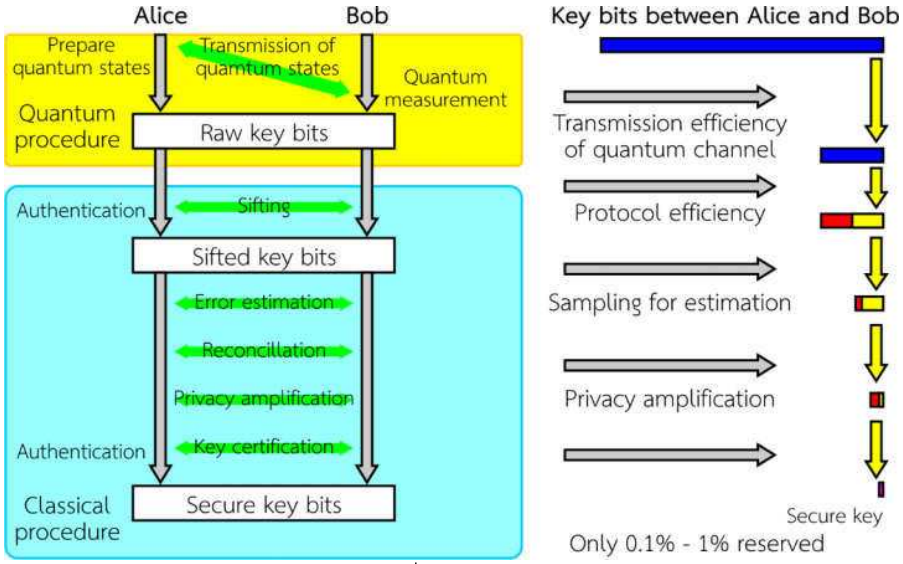


รูปที่ 3.16 (ก) ภาพการกำหนดทิศทางการโพลาไรซ์ของแสงที่ส่งออกไปด้วยชนิดของฐานและกุญแจ และ (ข) ลักษณะการรับและแปลงข้อมูลโดย Bob โดยรูปบน Bob ใช้ฐานที่ถูกต้องและรูปล่าง Bob ใช้ฐานที่ผิด ทำให้ความน่าจะเป็นที่ Bob จะอ่านค่าในแต่ละแบบเป็น 50%

ภาพรวมเกี่ยวกับการส่งข้อมูลจากผู้ส่งถึงผู้รับ แสดงได้ดังรูปที่ 3.17 โดยในการส่งคีย์ในลำดับแรกจะใช้กระบวนการทางควอนตัม และหลังจากนั้นจะเป็นกระบวนการสื่อสารปลอดภัยสูงที่ใช้การส่งข้อมูลผ่านช่องทางปกติ ซึ่งเมื่อได้ Sifted Key แล้ว จะต้องมีการใช้ข้อมูลบางส่วนในการตรวจสอบการมีผู้ดักจับข้อมูล และอีกบางส่วนในการเพิ่มความมั่นใจในการสื่อสารว่าปลอดภัย ซึ่งเป็นกระบวนการแบบดั้งเดิม และสุดท้ายผู้รับและผู้ส่งจะมีคีย์ที่มั่นใจได้ 100% ว่าปราศจากการดักฟัง แล้วจึงนำคีย์เหล่านั้นไปใช้ในการส่งข้อมูลจริงต่อไป ด้วยกระบวนการเข้ารหัสแบบ one-time-pad ซึ่งเป็นกระบวนการที่มีการยืนยันทางคณิตศาสตร์แล้วว่าปลอดภัยอย่างแน่นอน

สำหรับตัวฮาร์ดแวร์ที่ใช้ในการส่งข้อมูลในระบบการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมนั้นจะมี 2 ระบบ แยกกันอย่างชัดเจน คือ การมอดูเลตโพลาไรซ์ของโฟตอนเดี่ยวในการส่งในอากาศ และ การมอดูเลตเฟสของโฟตอนเดี่ยวในการส่งโฟตอนเดี่ยวในเส้นใยนำแสง โดยการใช้ตัวมอดูเลตเฟสทำให้เราสามารถเปลี่ยนสถานะทางเฟสของโฟตอนเดี่ยวในเส้นใยนำแสงได้ในลักษณะเดียวกันกับการใช้โพลาไรซ์เซอร์และตัวแยกลำแสงในกรณีการส่งในอากาศ

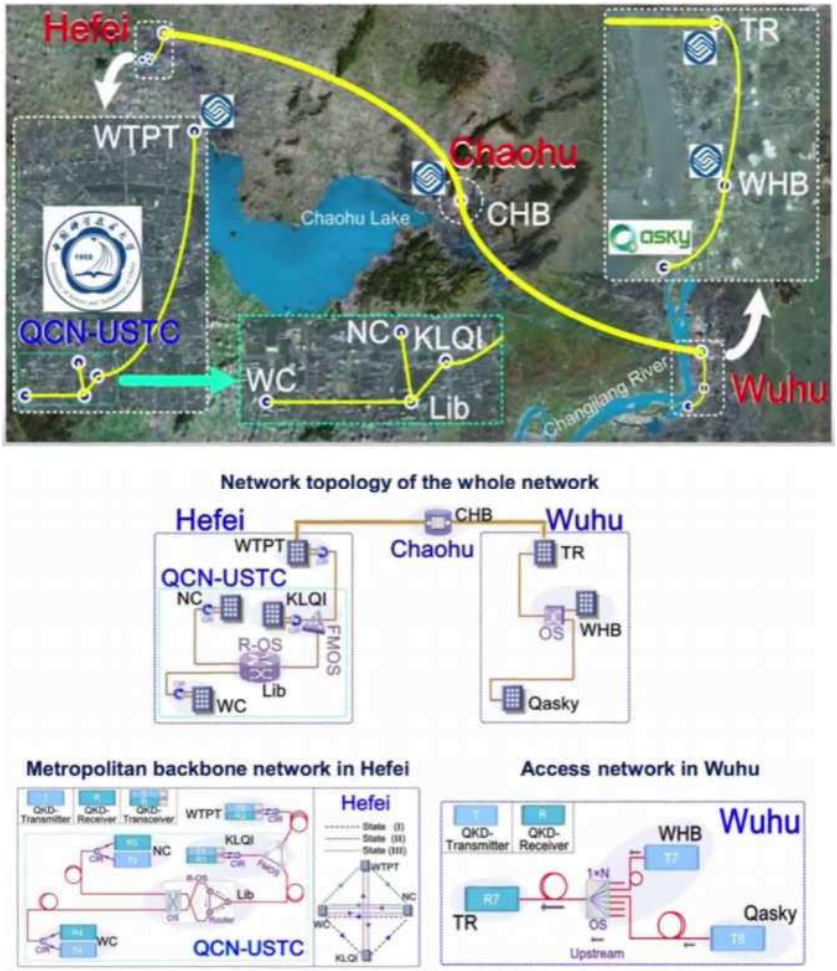
ทั้งตัวรับและตัวส่ง จะมี/สร้างได้ 2 ลักษณะ คือ เป็นแบบที่ออกแบบให้เป็นตัวรับหรือตัวส่งอย่างใดอย่างหนึ่งเท่านั้น และอีกลักษณะคือออกแบบให้เป็นได้ทั้งตัวรับและตัวส่งในตัวเดียวกัน สำหรับความซับซ้อนของการรับส่งข้อมูลถูกแบ่งออกเป็น 3 ระดับ คือ แบบ P2P เป็นแบบที่กำหนดให้มีผู้รับและผู้ส่งได้เพียงคนเดียว แบบ Network คือแบบที่มีการเชื่อมต่อการส่งข้อมูลแบบ P2P หลาย ๆ ลิงค์ทำให้สามารถสื่อสารได้ในวงกว้างขึ้น และ แบบทั่วไป คือการนำเครือข่ายการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมมาใช้ร่วมกันกับเครือข่ายเดิม ทำให้สามารถทำงาน/ใช้งานได้จริงในวงกว้าง



รูปที่ 3.17 ภาพกระบวนการรับส่งข้อมูลในการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม โดยภาพทางขวามือแสดงปริมาณข้อมูลก่อนที่จะได้คีย์ที่มั่นใจว่าปราศจากผู้ดักฟัง (secure key)

เครือข่ายสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การออกแบบและสร้าง

สำหรับการออกแบบเครือข่ายสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม หรือ เครือข่ายควอนตัมนี้ เราจะต้องกำหนดก่อนว่าจะใช้การส่งแบบใด (เลือกโปรโตคอลใด) โดยปัจจุบัน เครือข่ายที่ใช้อุปกรณ์ทางแสงแบบพาสซีฟ เป็นลักษณะเครือข่ายที่ได้รับความสนใจมากที่สุด ซึ่งเครือข่ายนี้จะมีอุปกรณ์คือ ตัวแยกลำแสง สวิตช์ทางแสง และ การมอดูเลตโดยการแบ่งความยาวคลื่น ปัญหาหลักที่จะต้องพิจารณาคือ การสูญเสียโฟตอนในเครือข่าย จะต้องต่ำมาก เนื่องจากเราต้องการส่งแสงความเข้มต่ำมาก ในระดับโฟตอนเดี่ยว ในเครือข่ายนี้ ปัจจุบันเครือข่ายนี้กำลังถูกทดสอบและมีแผนจะขยายออกไปอีก โดยรูปที่ 3.18 แสดงลักษณะการเชื่อมโยงระหว่างเมืองต่าง ๆ ในประเทศจีนด้วยเครือข่ายเส้นใยนำแสง โดยมีโนดทั้งิ้น 12 โนดและระยะทางรวมทั้งสิ้นมากกว่า 220 กิโลเมตร



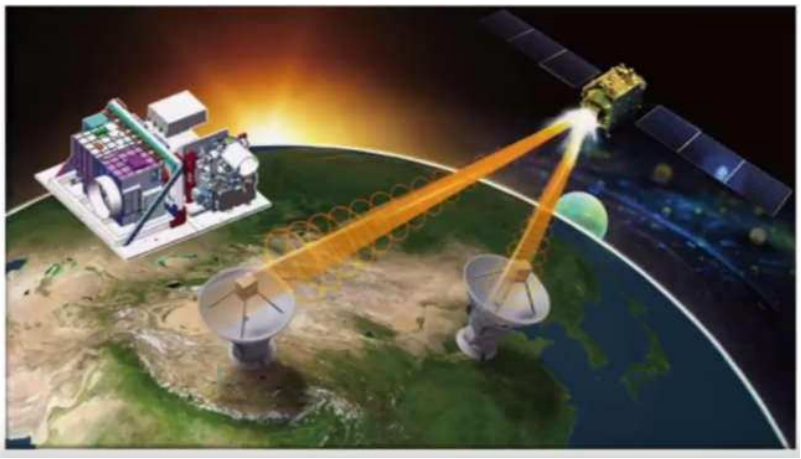
รูปที่ 3.18 ภาพบนแสดงการเชื่อมโยงเครือข่ายควอนตัมด้วยเส้นใยนำแสงระหว่างเมืองในประเทศจีน และภาพล่างแสดงลักษณะโทโพลอยีของเครือข่ายที่มีการทดสอบและใช้งานแล้ว

ความก้าวหน้าเกี่ยวกับการวิจัยด้านสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมที่ USTC

ปัจจุบันการวิจัยด้านเครือข่ายควอนตัมในประเทศจีนมีความรุดหน้าไปมาก ได้มีการลงทุนมากกว่า 0.56 พันล้านหยวน (ประมาณ 2.8 พันล้านบาท) โดยเป็นการลงทุนสร้างเครือข่ายเส้นใยนำแสงใหม่ที่เชื่อมต่อเมืองสำคัญตั้งแต่ปักกิ่งไปจนถึงเซียงไฮ้ โดยมีความยาวทั้งสิ้น 2000 กิโลเมตร และคาดว่าเครือข่ายนี้จะพร้อมใช้งานจริงในเร็ว ๆ นี้ โดยเครือข่ายนี้จะผนวกเข้ากับเครือข่ายเดิม ที่ติดตั้งอยู่ที่เมือง Hefei และวางแผนว่าจะมีผู้ใช้หลัก คือ ธนาคารจีนและสำนักข่าว Xinhua ของจีน รูปที่ 3.19 แสดงแผนที่ส่วนของประเทศจีนที่เกี่ยวข้องกับโครงการดังกล่าว

นอกจากการสื่อสารผ่านเส้นใยนำแสงแล้ว ยังมีโครงการดาวเทียมควอนตัมที่มีหัวหน้าโครงการคือ Prof. Jian-Wei Pan โดยดาวเทียมถูกส่งขึ้นไปเมื่อกลางปีที่แล้ว และมีการทดสอบการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมผ่านการสื่อสารผ่านดาวเทียมทั้งแบบที่ใช้โฟตอนเดี่ยวและแบบที่ใช้ความพัวพันทางควอนตัมอีกด้วย โดยผลงานนี้เป็นที่กล่าวถึงมากทั้งในประเทศและในต่างประเทศ เนื่องจากเป็นการส่งข้อมูลแบบควอนตัมจากจุดไปจุด ที่มีระยะทางมากที่สุด (มากกว่า 1200 กิโลเมตร) รูปที่ 3.20 แสดงภาพที่ใช้ประชาสัมพันธ์เกี่ยวกับการสื่อสารด้วยดาวเทียมควอนตัม

รูปที่ 3.19 แผนที่ส่วนของประเทศจีนที่เกี่ยวข้องกับโครงการเครือข่ายควอนตัม



รูปที่ 3.20 ภาพเกี่ยวกับโครงการเครือข่ายควอนตัมผ่านดาวเทียมของประเทศจีน

การสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมในเชิงพาณิชย์ในประเทศจีน

สำหรับการใช้งานการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมในเชิงพาณิชย์ในประเทศจีน ได้มีการวางแผนไว้แล้ว โดยมีบริษัทที่เกี่ยวข้องหลัก ๆ 2 บริษัท คือ Qasky และ QuantumCTek ซึ่งเป็นบริษัทที่แยกตัวออกมาจากกลุ่มวิจัยในมหาวิทยาลัย UTSC โลโก้ของบริษัทที่เกี่ยวข้องและสนใจเทคโนโลยีนี้แสดงในรูปที่ 3.21

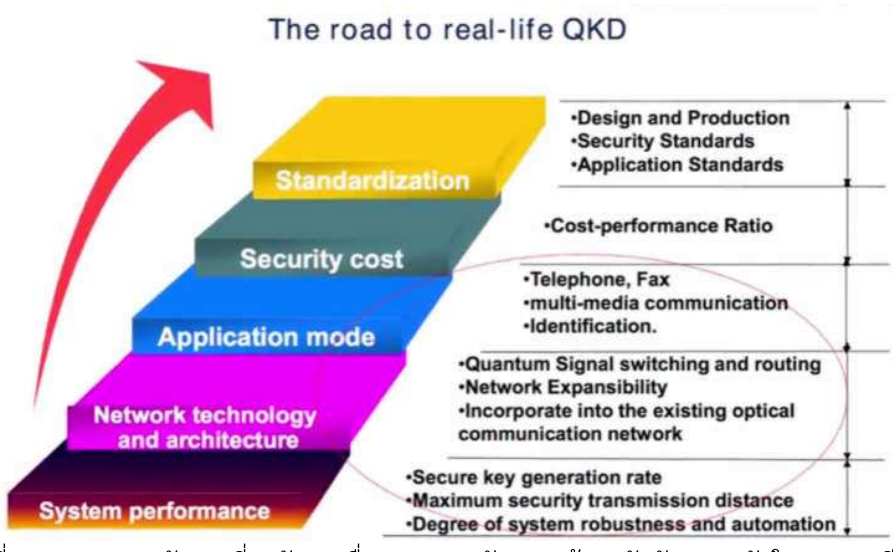
สำหรับการใช้งานในเชิงพาณิชย์นี้ อาจแบ่งได้เป็นสองประเภทใหญ่ ๆ คือ สำหรับ e-government และ สำหรับการบริการทางการเงิน ซึ่งปัจจุบันกำลังมีการก่อนสร้างระบบที่รองรับงานทั้งสองประเภท โดยการเชื่อมต่อเครือข่ายในเมืองต่าง ๆ ดังแสดงตัวอย่างในรูปที่ 3.22

รูปที่ 3.21 ภาพโลโก้บริษัทที่เกี่ยวข้องและสนใจเครือข่ายควอนตัมในประเทศจีน

รูปที่ 3.22 แผนการพัฒนาเครือข่ายควอนตัมในเชิงพาณิชย์ในประเทศจีน

อนาคตของการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม

ในอนาคตอันใกล้ จะมีการพัฒนาระบบการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม ให้เป็นมาตรฐานและผนวกเข้ากับระบบสื่อสารเดิม โดยจะมีการศึกษาในทุกระดับขั้นเพื่อให้นำไปสู่การใช้งานที่แพร่หลายต่อไป รูปที่ 3.23 แสดงลักษณะการพัฒนา จากระดับล่าง คือการศึกษาสมรรถนะของระบบ จนไปสู่เทคโนโลยีเครือข่ายควอนตัมและสถาปัตยกรรมที่เกี่ยวข้อง จากนั้นจึงนำไปใช้ในการสื่อสารพื้นฐาน เช่น การโทรศัพท์ การส่งแฟกซ์ โดยจะพัฒนาให้มีประสิทธิภาพดี มีราคาที่เหมาะสม และนำไปสู่การสร้างมาตรฐานด้านความปลอดภัยใหม่



รูปที่ 3.23 แผนการพัฒนาเกี่ยวกับการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัมในประเทศจีน

บทที่ 4
รายงานสรุปผลการจัดกิจกรรม

4.1 รายงานสรุปผลการสัมมนา ฝึกอบรม หรือการประชุมรวมกลุ่มวิจัยเฉพาะทาง

สรุปภาพรวมเกี่ยวกับกิจกรรมการสัมมนา ฝึกอบรม หรือการประชุมรวมกลุ่มวิจัยเฉพาะทาง ที่ดำเนินการตามโครงการนี้ตามลำดับเหตุการณ์ จะมีทั้งสิ้น 12 ครั้ง ดังแสดงในตารางที่ 4.1 โดยในแต่ละครั้งจะมีกลุ่มผู้สนใจหลักคือ คณาจารย์ นิสิต นักศึกษา จากสถาบันต่าง ๆ โดยมีผู้เข้าฟังหลักคือ นิสิต นักศึกษา ในสถาบันนั้น ๆ และมีจำนวนผู้เข้าร่วมอบรมรวมทั้งสิ้นมากกว่า 400 คน

ตารางที่ 4.1 สรุปเหตุการณ์การสัมมนา ฝึกอบรม หรือการประชุมรวมกลุ่มวิจัยเฉพาะทาง

ครั้งที่	วันที่	สถานที่
1	2 กันยายน 2558	ม. สุรนารี (นครราชสีมา)
2	30 มกราคม 2559	ม. นเรศวร (พิษณุโลก)
3	19 กุมภาพันธ์ 2559	ม. นเรศวร (พิษณุโลก)
4	21 มีนาคม 2559	ม. นเรศวร (พิษณุโลก)
5	25 มีนาคม 2559	ม. กาฬสินธุ์ (กาฬสินธุ์)
6	1 มิถุนายน 2559	โรงเรียนสาธิต ม.นเรศวร (พิษณุโลก)
7	1 สิงหาคม 2559	ม. นเรศวร (พิษณุโลก)
8	18 พฤศจิกายน 2559	จุฬาลงกรณ์มหาวิทยาลัย (กรุงเทพฯ)
9	25 พฤศจิกายน 2559	ม. นเรศวร (พิษณุโลก)
10	6 มกราคม 2560	พสวท. (กรุงเทพฯ)
11	1 พฤษภาคม 2560	ม. ขอนแก่น (ขอนแก่น)
12	13 ธันวาคม 2560	ม. เทคโนโลยีราชมงคล ล้านนา พิษณุโลก

4.2 รายงานสรุปผลการสัมมนารับฟังความคิดเห็นของผู้ที่เกี่ยวข้อง

ในการบรรยายพิเศษโดยผู้เชี่ยวชาญ และ การสัมมนา ฝึกอบรม หรือการประชุมรวมกลุ่มวิจัยเฉพาะทางแต่ละครั้ง ก็มีการสัมมนารับฟังความคิดเห็นของที่ผู้สนใจเข้าร่วมกิจกรรม และนอกจากนี้ ก็มีการทำแบบสอบถาม โดยสำหรับคำถาม-คำตอบทั่วไปที่มีการกล่าวถึงและเกี่ยวข้องกับเทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม สรุปได้ดังนี้

1. ศาสตร์ด้านควอนตัมคืออะไร ?

ควอนตัมปริมาณทางกายภาพที่เล็กที่สุดที่ไม่สามารถแบ่งแยกได้อีก ศาสตร์ด้านควอนตัมกำเนิดจากแนวคิดที่ใช้อธิบายปรากฏการณ์ที่เกิดขึ้นกับ อนุภาคเล็ก ๆ เช่น อิเล็กตรอน อะตอม โมเลกุล โดยแนวคิดนี้ขัดแย้งกับสามัญสำนึกของมนุษย์โดยทั่วไป ทฤษฎีนี้ถูกพัฒนาขึ้นในช่วงปีค.ศ. 1900-1927 และถูกนำมาใช้เป็นพื้นฐานในการสร้างเทคโนโลยีสมัยใหม่ต่อมามากมายทั้งการสื่อสาร การคำนวณ การเทียบ(มาตร)วัดต่าง ๆ จนถึง การส่งถ่าย (teleportation) แห่งโลกอนาคต ฯลฯ

2. ควอนตัมคอมพิวเตอร์ที่มีการจำหน่ายแล้ว ... เป็นภัยต่อรหัสลับไหม ?

จากข้อมูลช่วงต้นปีค.ศ.2015 ที่กูเกิล (Google) ประกาศว่าได้ทดสอบควอนตัมคอมพิวเตอร์สำเร็จแล้ว และพบว่า ควอนตัมคอมพิวเตอร์เร็วกว่าคอมพิวเตอร์ทั่วไป 100 ล้านเท่าในการประมวลผลปัญหาบางอย่าง แต่ก็รายงานว่าคอมพิวเตอร์นี้ยังไม่เป็นภัยต่อความปลอดภัยทางอินเทอร์เน็ต แม้ว่าหน่วยประมวลผล Dwave 2X ที่กูเกิลอ้างนั้นสร้างโดยใช้หลักการคล้ายคลึงกับควอนตัมคอมพิวเตอร์ แต่ยังใช้ได้เฉพาะบางการแก้ปัญหาบางอย่างเท่านั้น โดยการถอดรหัส (การทำลายระบบความปลอดภัย) อินเทอร์เน็ตที่ใช้อยู่ในปัจจุบันมิได้ถูกรวมอยู่ในปัญหาประเภทที่ควอนตัมคอมพิวเตอร์เครื่องนี้สามารถแก้ไขปัญหาได้เร็ว

3. รหัสลับควอนตัมคืออะไร

การสื่อสารปลอดภัยเมื่อเข้ารหัสลับแล้วจะไม่มีใครถอดได้นอกจากผู้ที่ผู้ส่งต้องการส่งข้อความไปหาเท่านั้น โดยกุญแจรหัสลับส่งไปกับการอาศัยคุณสมบัติทางควอนตัมของโฟตอน (photon) หรือหน่วยเล็กสุดของ “แสง” ทั้งนี้จากทฤษฎีควอนตัมที่ว่าไม่มีใครสามารถคัดลอกสถานะทางควอนตัมของโฟตอนได้โดยไม่ไปกระทบหรือเปลี่ยนแปลงสถานะของตัวมัน ดังนั้น หากมีใครมายุ่งจะทำให้ระบบสื่อสารรู้ตัว จึงมั่นใจได้ว่าการสื่อสารด้วยวิทยาการนี้ปลอดภัยสูงสุด

4. รหัสลับทั่วไปที่มีใช้กันอย่างแพร่หลายแล้วทำไมจึงต้องใช้รหัสลับควอนตัม และระบบนี้มีใช้แล้วหรือ ?

เราต้องใช้ระบบสื่อสารด้วยรหัสลับควอนตัมเพราะเป็นระบบที่มีการสร้างกุญแจรหัสลับที่ใช้ครั้งเดียวแล้วทิ้ง (one time pad : OTP) จึงปลอดภัยจากการถูกถอดรหัสด้วยวิธีการต่าง ๆ 100% โดยระบบนี้มีใช้มา

นานเกินสิบปีแล้ว มีบริษัทที่ผลิตออกจำหน่ายทั้งจากทั้งยุโรป สหรัฐฯ จีน เกาหลีใต้ ราคาชุดสื่อสารจุดต่อจุดละเกือบแปดล้านบาท

5. ปัจจุบัน วิทยาการด้านรหัสลับเชิงควอนตัมทั่วโลกเขาทำอะไรกันอยู่ ?

ยุโรปประกาศการปฏิวัติควอนตัมยุคที่สอง โครงการพันล้านยูโรระยะเวลาสิบปี ญี่ปุ่นสร้างเครือข่ายโตเกียวสาธิตและทดสอบตลอดวัน จีนเปิดเครือข่ายปักกิ่ง – เซี่ยงไฮ้ และขึ้นดาวเทียมทดลองแล้ว เกาหลีใต้เปิดโครงการสองปีผลิตขาย สิงคโปร์สามปีลงทุนมากกว่าพันล้านบาทเพื่อสร้างบุคลากร สหรัฐอเมริกานำหน้าจำนวนสิทธิบัตรมากสุดในโลก จีนตามติดแต่มีผลผลิตด้านวิชาการสูงที่สุด ฯลฯ ... โลกได้มีพัฒนาการมากว่าสามทศวรรษ และมีการนำเสนอผลการวิจัยใหม่ ๆ ในวารสารชั้นนำเช่น Nature อย่างต่อเนื่อง

6. มีข่าวออกมาว่า รหัสลับควอนตัมถูกแฮก (hacking) ได้แล้ว แสดงว่าไม่ปลอดภัยจริง ใช่หรือไม่ ?

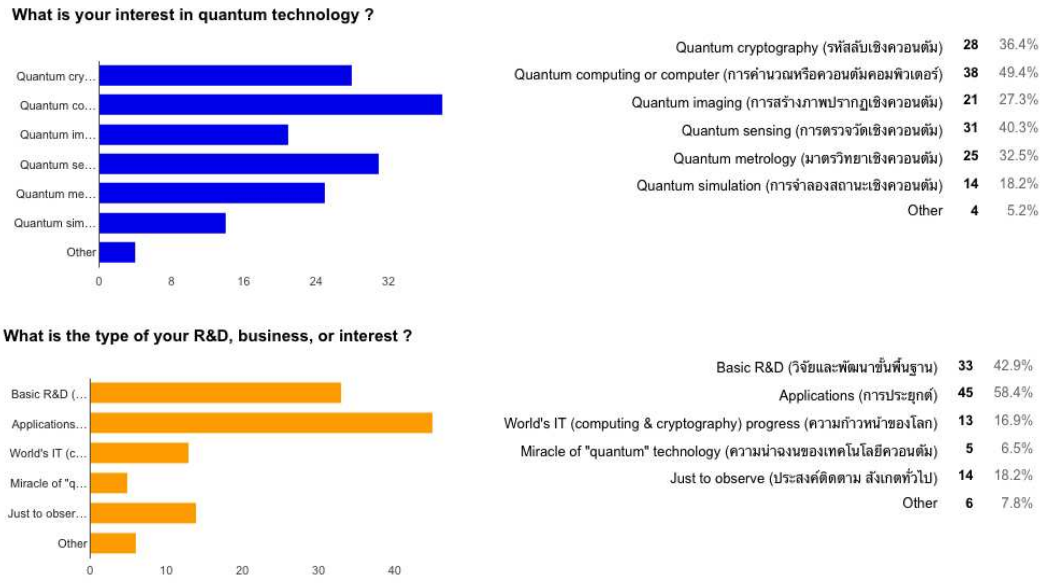
ไม่ใช่ ... เพราะเรื่องข่าวที่ว่าเกิดจากช่องว่างการสื่อสารระหว่างนักฟิสิกส์กับวิศวกรสื่อสารเท่านั้น คำจัดความ quantum hacking คือโฆษณาแฝง เป็นบ่อดักให้หลงสนใจบริษัทขายเครื่องรหัสลับควอนตัม และกรณีนักวิจัยทำงานเด่นด้านตัวรับแสง แต่กลับตั้งชื่องานให้เอียงเข้ามาพ่วงชื่อเสียงของรหัสลับควอนตัมเรื่องการแฮก เป็นทั้งการลองวิชา อุดมคติและความไม่สมบูรณ์ของอุปกรณ์ แต่มาพ่วงใช้ชื่อจากโลกไอทีเดิมจนทำให้สับสน

7. ประเทศไทยควรตั้งเป้าหมายอย่างไรในอนาคต ?

ผู้ทำโครงการเสนอว่า เรา (คนไทย) ควรเป็นผู้ซื้ออย่างฉลาดให้ได้ก่อนเพื่อเป็นบันไดขั้นแรกติดตามความรู้สู่อนาคต และจากนั้นจึงเป็นผู้ศึกษาระบบ ช่วยกันตั้งข้อสังเกต ศึกษาหาคำตอบและแบ่งปันให้ความรู้จริงปรากฏ ของเทียมควรลดจางหายไม่ให้กระทบต่อสังคมฐานความรู้วิทยาศาสตร์ ช่วยกันหาทางป้องกันแม้กระทั่งกับวงการวิชาการ (ควอนตัมของเทียม) ก็ควรช่วยกันเร่งแก้ไข ปรับปรุงตนเอง !

นอกจากการถาม-ตอบด้วยวาจาแล้ว ยังมีการทำแบบสอบถามในเรื่องที่เกี่ยวข้องกับเทคโนโลยีควอนตัม ทั้งในรูปแบบออนไลน์และทำในกระดาษ ผลการตอบแบบสอบถาม (จากผู้ตอบแบบสอบถามจำนวน 77 คน) แสดงได้ดังต่อไปนี้

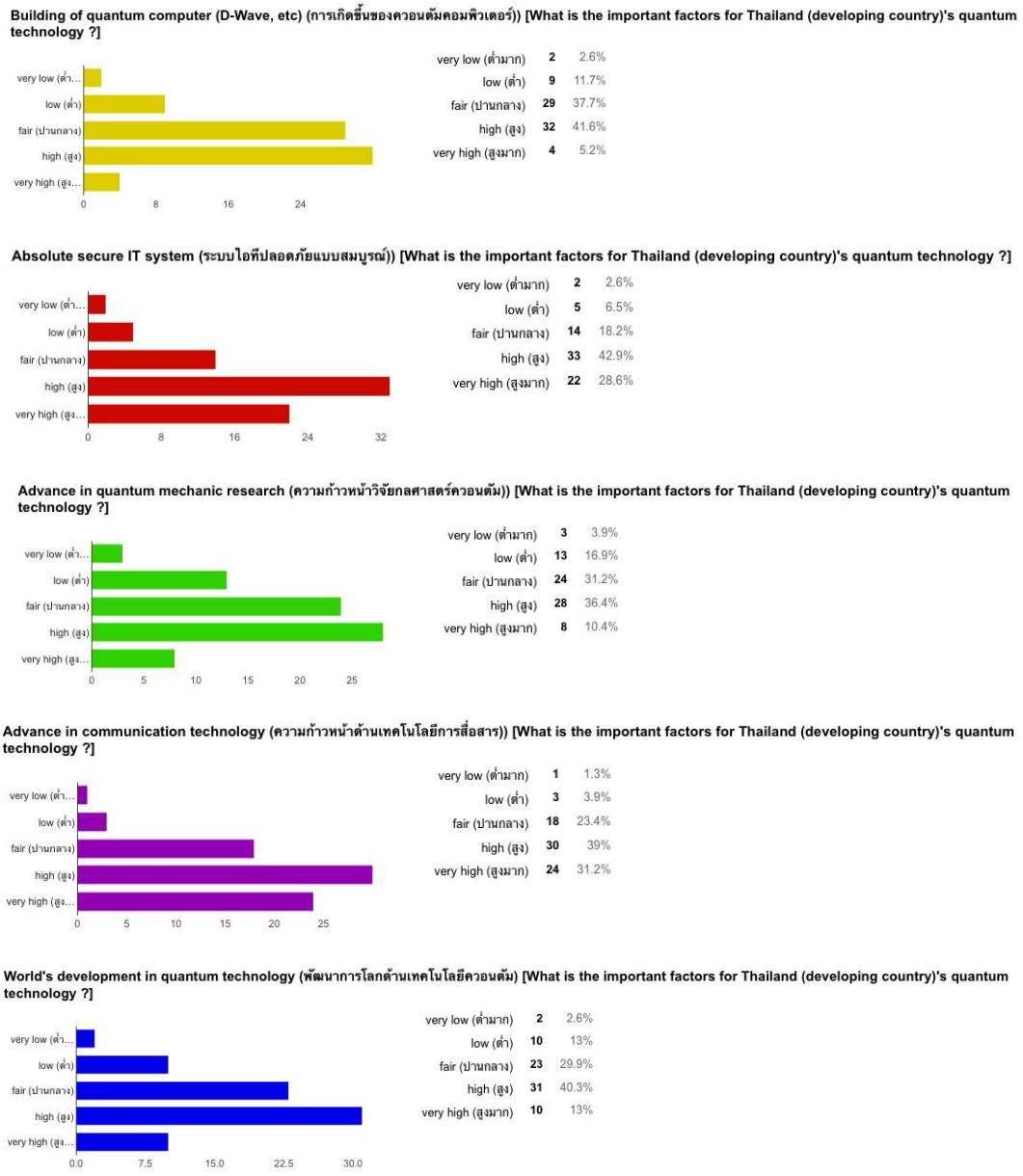
ผลการรับฟังความคิดเห็นจากผู้ที่เกี่ยวข้องที่ประมวลจากแบบสำรวจความคิดเห็นแสดงดังในรูปที่ 4.1 โดยพบว่าเทคโนโลยีเกี่ยวกับการคำนวณหรือควอนตัมคอมพิวเตอร์เป็นเทคโนโลยีเกี่ยวกับควอนตัมที่สนใจมากที่สุดคิดเป็น 49.4% รองลงมาได้แก่ เทคโนโลยีการตรวจวัดเชิงควอนตัมที่เกี่ยวข้องกับเทคโนโลยีควอนตัม คิดเป็น 40.3% และอันดับที่สามคือเทคโนโลยีรหัสลับเชิงควอนตัม คิดเป็น 36.4% และผู้ร่วมตอบแบบสอบถามให้ความสนใจกับการทำวิจัยเชิงประยุกต์ คิดเป็น 58.4% รองลงมาได้แก่ ทำวิจัยและพัฒนาขั้นพื้นฐานคิดเป็น 42.9%



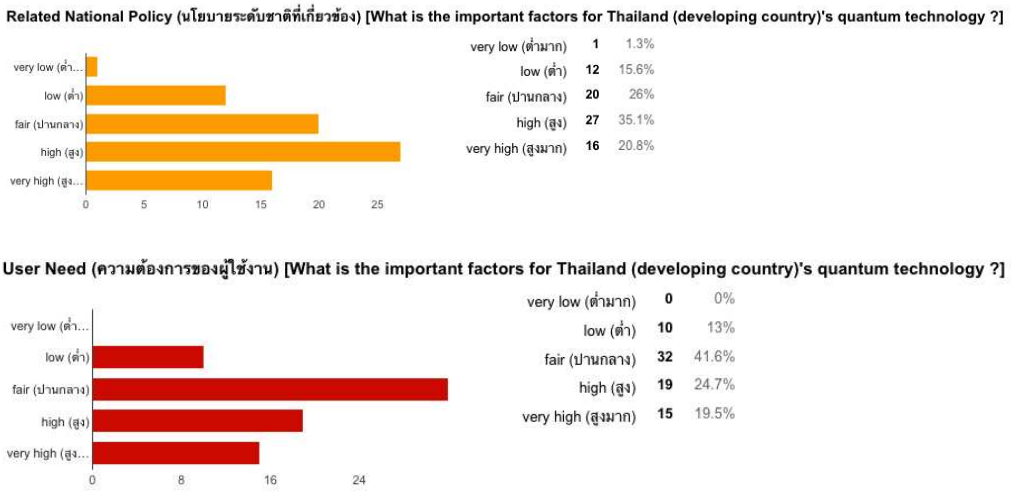
รูปที่ 4.1 ผลการรับฟังความคิดเห็นในส่วนของความสนใจของผู้ตอบแบบสอบถาม

จากผลของแบบสอบถามพบว่า ปัจจัยที่สำคัญสำหรับประเทศไทยในการพัฒนาเทคโนโลยีควอนตัม (รูปที่ 4.2) อันดับแรกคือ การสร้างหรือการมีระบบสารสนเทศที่ปลอดภัยโดยสมบูรณ์มีความสำคัญสูง (42.9%) ถึงสูงที่สุด (28.6%) จากนั้นในอันดับรองลงมาคือ การสร้างควอนตัมคอมพิวเตอร์ ที่ผู้ตอบแบบสอบถามเห็นว่ามีความสำคัญสูง (41.6%) โดยผู้ตอบแบบสอบถามเห็นว่าปัจจัยอื่น ๆ ได้แก่ การทำวิจัยด้านกลศาสตร์ควอนตัม การพัฒนาเทคโนโลยีการสื่อสาร การพัฒนาด้านเทคโนโลยีควอนตัม การมีนโยบายระดับชาติที่เกี่ยวข้อง ล้วนแต่เป็นปัจจัยที่สำคัญสำหรับประเทสไทยในการพัฒนาเทคโนโลยีควอนตัม โดยมีปัจจัยข้อเดียว คือ ความต้องการของผู้ใช้งาน ที่ผู้ตอบแบบสอบถามเห็นว่าเป็นปัจจัยที่มีความสำคัญรองลงมา (ระดับปานกลาง) โดยผลการตอบแบบสอบถามในส่วนนี้แสดงให้เห็นว่า ผู้ที่เกี่ยวข้องและผู้เชี่ยวชาญส่วนใหญ่

เชื่อว่า การสร้างหรือการมีระบบสารสนเทศที่ปลอดภัยโดยสมบูรณ์มีความสำคัญสูงในการพัฒนาเทคโนโลยีควอนตัมของประเทศ โดยในส่วนของผู้ใช้อาจมีความต้องการในการพัฒนาเทคโนโลยีด้านนี้เพียงระดับปานกลาง



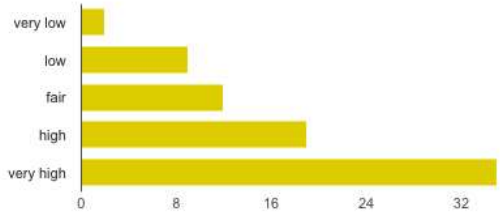
รูปที่ 4.2 ผลการรับฟังความคิดเห็นในส่วนของปัจจัยที่สำคัญ
สำหรับประเทศไทยในการพัฒนาเทคโนโลยีควอนตัม



รูปที่ 4.2 ผลการรับฟังความคิดเห็นในส่วนของปัจจัยที่สำคัญ
สำหรับประเทศไทยในการพัฒนาเทคโนโลยีควอนตัม (ต่อ)

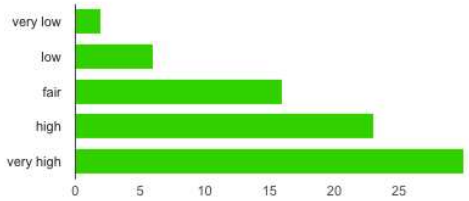
สำหรับความเห็นเกี่ยวกับข้อจำกัดของประเทศไทยในการพัฒนาเทคโนโลยีควอนตัม (รูปที่ 4.3) ผู้ตอบแบบสอบถามส่วนใหญ่เห็นว่าประเทศไทยมีข้อจำกัดหลาย ๆ ด้านโดยด้านหลัก ๆ ได้แก่ การขาดแคลนทรัพยากรบุคคล (สูง 24.7% และสูงมาก 45.5%) การขาดแคลนทุนสนับสนุนงานวิจัย (สูง 29.9% และสูงมาก 39%) การขาดแคลนห้องปฏิบัติการและสนามทดสอบ (สูง 36.4% และสูงมาก 32.5%) การขาดแคลนมาตรฐานที่เกี่ยวข้อง (สูง 44.2% และสูงมาก 14.3%) และการขาดนโยบายประเทศ (สูง 33.8% และสูงมาก 29.9%) โดยมีความรู้พื้นฐานที่จำกัดและการปราศจากผู้ใช้งานของเทคโนโลยีควอนตัมนี้ ผู้ตอบแบบสอบถามส่วนใหญ่เห็นว่าเป็นปัจจัยจำกัดของประเทศไทยในระดับปานกลาง (จำนวน 33.8% ในทั้งสองข้อ) ซึ่งจากผลการวิเคราะห์แบบสอบถามในส่วนนี้แสดงให้เห็นว่า ประเทศไทยควรมีการเสริมสร้าง/พัฒนาทรัพยากรบุคคล ทุนสนับสนุนงานวิจัย ห้องปฏิบัติการและสนามทดสอบ มาตรฐานที่เกี่ยวข้อง และนโยบายประเทศในส่วนที่เกี่ยวข้องกับเทคโนโลยีนี้เพื่อให้เกิดการพัฒนาเทคโนโลยีด้านนี้ในประเทศไทย เพื่อที่จะทำให้เกิดการสร้างนวัตกรรมและประยุกต์ใช้งานจริงในอนาคตต่อไป

Human resource (ทรัพยากรบุคคล) [What is the important restraints for Thailand on quantum technology ?]



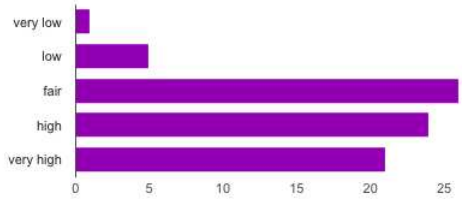
very low	2	2.6%
low	9	11.7%
fair	12	15.6%
high	19	24.7%
very high	35	45.5%

Research funding (ทุนสนับสนุนงานวิจัย) [What is the important restraints for Thailand on quantum technology ?]



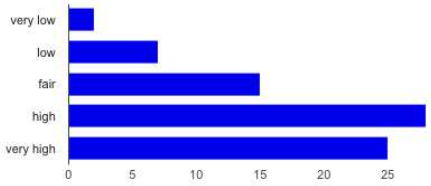
very low	2	2.6%
low	6	7.8%
fair	16	20.8%
high	23	29.9%
very high	30	39%

Limited basic knowledge (ความรู้พื้นฐานที่จำกัด) [What is the important restraints for Thailand on quantum technology ?]



very low	1	1.3%
low	5	6.5%
fair	26	33.8%
high	24	31.2%
very high	21	27.3%

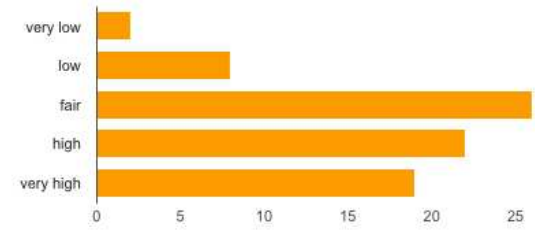
Laboratory and testbed (ห้องปฏิบัติการและสนามทดสอบ)) [What is the important restraints for Thailand on quantum technology ?]



very low	2	2.6%
low	7	9.1%
fair	15	19.5%
high	28	36.4%
very high	25	32.5%

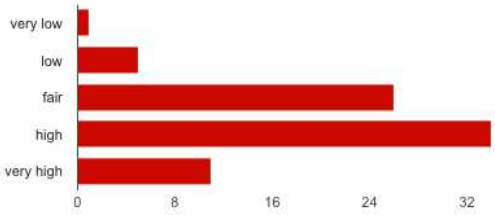
รูปที่ 4.3 ผลการรับฟังความคิดเห็นในส่วนของข้อจำกัดของประเทศไทย
ในการพัฒนาเทคโนโลยีควอนตัม

Lack of user (ปราศจากผู้ใช้งาน) [What is the important restraints for Thailand on quantum technology ?]



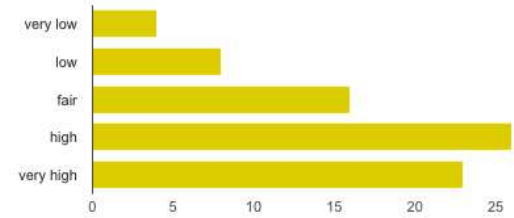
very low	2	2.6%
low	8	10.4%
fair	26	33.8%
high	22	28.6%
very high	19	24.7%

Related standard (มาตรฐานที่เกี่ยวข้อง) [What is the important restraints for Thailand on quantum technology ?]



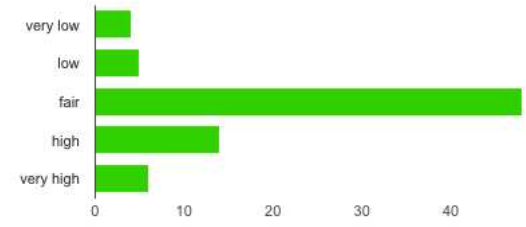
very low	1	1.3%
low	5	6.5%
fair	26	33.8%
high	34	44.2%
very high	11	14.3%

National Policy (นโยบายในประเทศ) [What is the important restraints for Thailand on quantum technology ?]



very low	4	5.2%
low	8	10.4%
fair	16	20.8%
high	26	33.8%
very high	23	29.9%

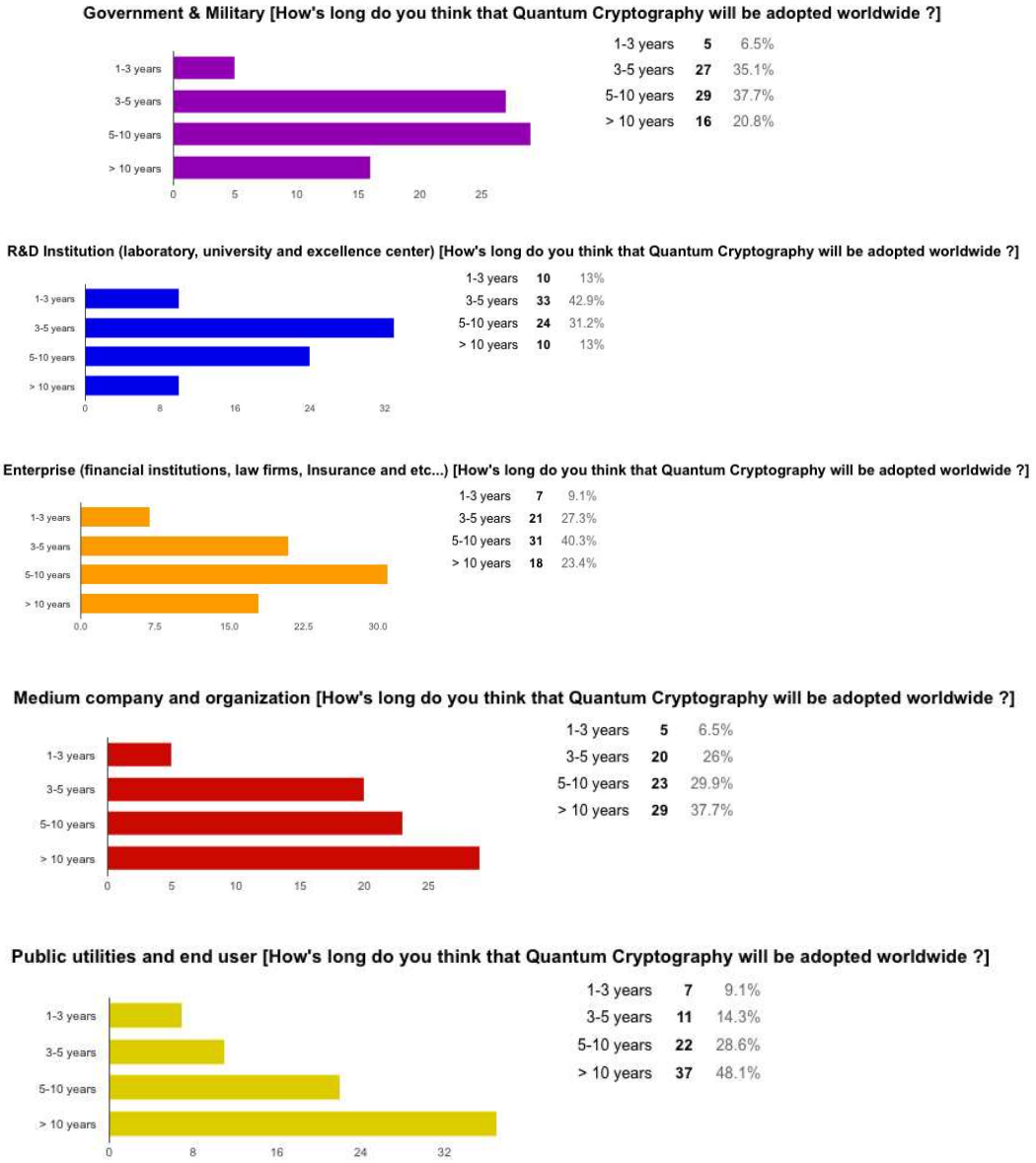
Other restraints (ข้อจำกัดอื่น ๆ) [What is the important restraints for Thailand on quantum technology ?]



very low	4	5.2%
low	5	6.5%
fair	48	62.3%
high	14	18.2%
very high	6	7.8%

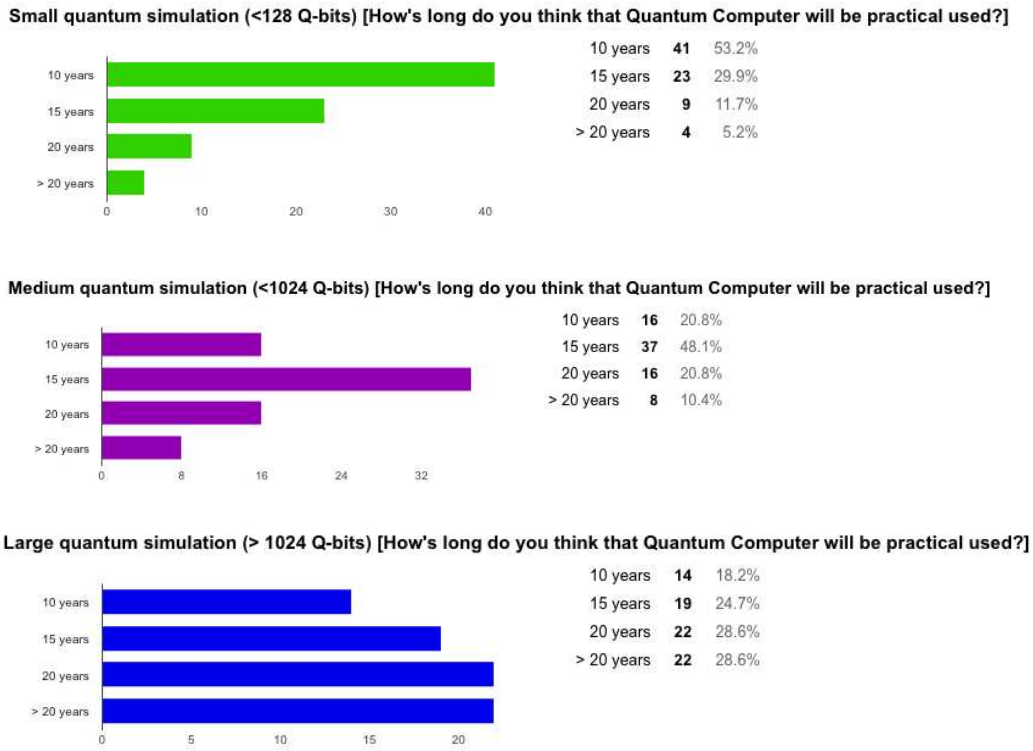
รูปที่ 4.3 ผลการรับฟังความคิดเห็นในส่วนของข้อจำกัดของประเทศไทย
ในการพัฒนาเทคโนโลยีควอนตัม (ต่อ)

ในส่วนความเห็นเกี่ยวกับการประยุกต์ใช้เทคโนโลยีรหัสลับควอนตัมในโลกนั้น (รูปที่ 4.4) เป็นส่วนสำคัญส่วนหนึ่งที่จะกำหนด/บังคับให้ประเทศไทยใช้เทคโนโลยีนี้ โดยผู้ตอบแบบสอบถามส่วนใหญ่เห็นว่า การใช้เทคโนโลยีนี้จะเกิดขึ้นในห้องปฏิบัติการ มหาวิทยาลัย หรือ ศูนย์ความเป็นเลิศต่าง ๆ ก่อน (3-5 ปี, 42.9%) จากนั้นจึงมีการใช้ในหน่วยงานรัฐและทางทหาร (5-10 ปี, 37.7%) และองค์กรขนาดใหญ่ (5-10 ปี, 40.3%) จากนั้นจึงเกิดการใช้งานในองค์กรหรือบริษัทขนาดกลาง (> 10 ปี, 37.7%) และ การใช้งานทั่วไปกับผู้ใช้รายงานย่อย (> 10 ปี, 48.1%)



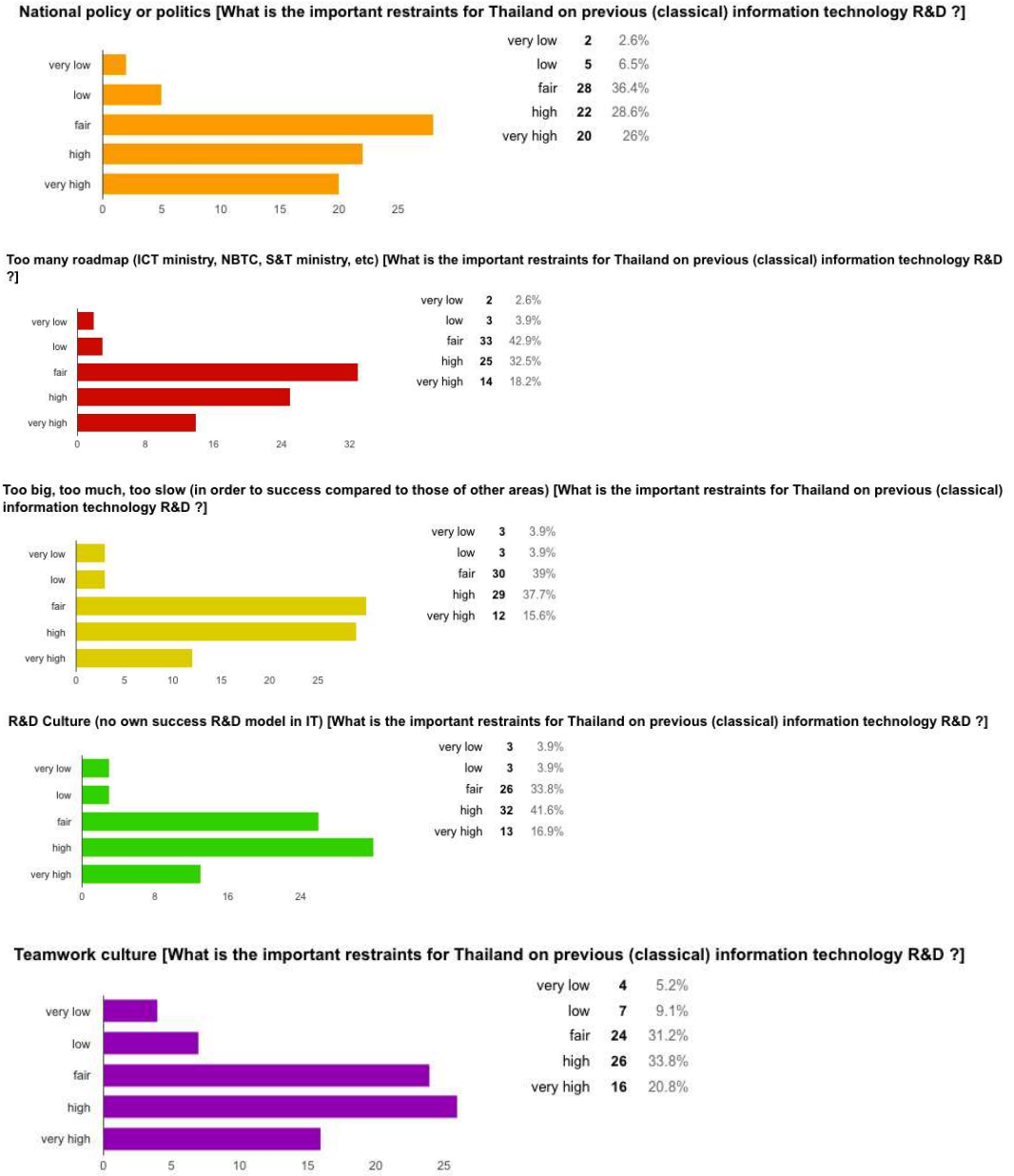
รูปที่ 4.4 ผลการรับฟังความคิดเห็นในส่วนของการประยุกต์ใช้เทคโนโลยีรหัสลับควอนตัม

สำหรับความเห็นเกี่ยวกับการประยุกต์ใช้เทคโนโลยีควอนตัมคอมพิวเตอร์ซึ่งเป็นเทคโนโลยีสำคัญที่ผลักดันให้ต้องมีการใช้เทคโนโลยีรหัสลับควอนตัม (เนื่องจากควอนตัมคอมพิวเตอร์จะสามารถถอดรหัสที่ใช้ในการสื่อสารในปัจจุบันได้อย่างรวดเร็ว/มีประสิทธิภาพ และทำให้การเข้ารหัสที่ใช้ในปัจจุบันไม่ปลอดภัยอีกต่อไป) มีข้อสรุปดังแสดงในรูปที่ 4.5 พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่คิดว่าการจำลอง/คำนวณด้วยควอนตัมคอมพิวเตอร์ขนาดเล็ก (< 128 คิวบิต) นั้นจะทำได้ในช่วงเวลา 10 ปี (53.2%) และการจำลอง/คำนวณด้วยควอนตัมคอมพิวเตอร์ขนาดกลาง (< 1024 คิวบิต) นั้นจะทำได้ในช่วงเวลา 15 ปี (48.1%) โดยสำหรับการจำลองด้วยควอนตัมคอมพิวเตอร์ขนาดใหญ่ (> 1024 คิวบิต) ซึ่งเป็นขนาดที่สามารถใช้ในการถอดรหัสของการเข้ารหัสที่ใช้อยู่ในปัจจุบันได้นั้น อาจต้องใช้เวลามากถึง 20 ปี (28.6%) หรือมากกว่านั้น (28.6%) ในการพัฒนาเพื่อให้สามารถใช้งานได้จริง



รูปที่ 4.5 ผลการรับฟังความคิดเห็นในส่วนของการประยุกต์ใช้เทคโนโลยีควอนตัมคอมพิวเตอร์

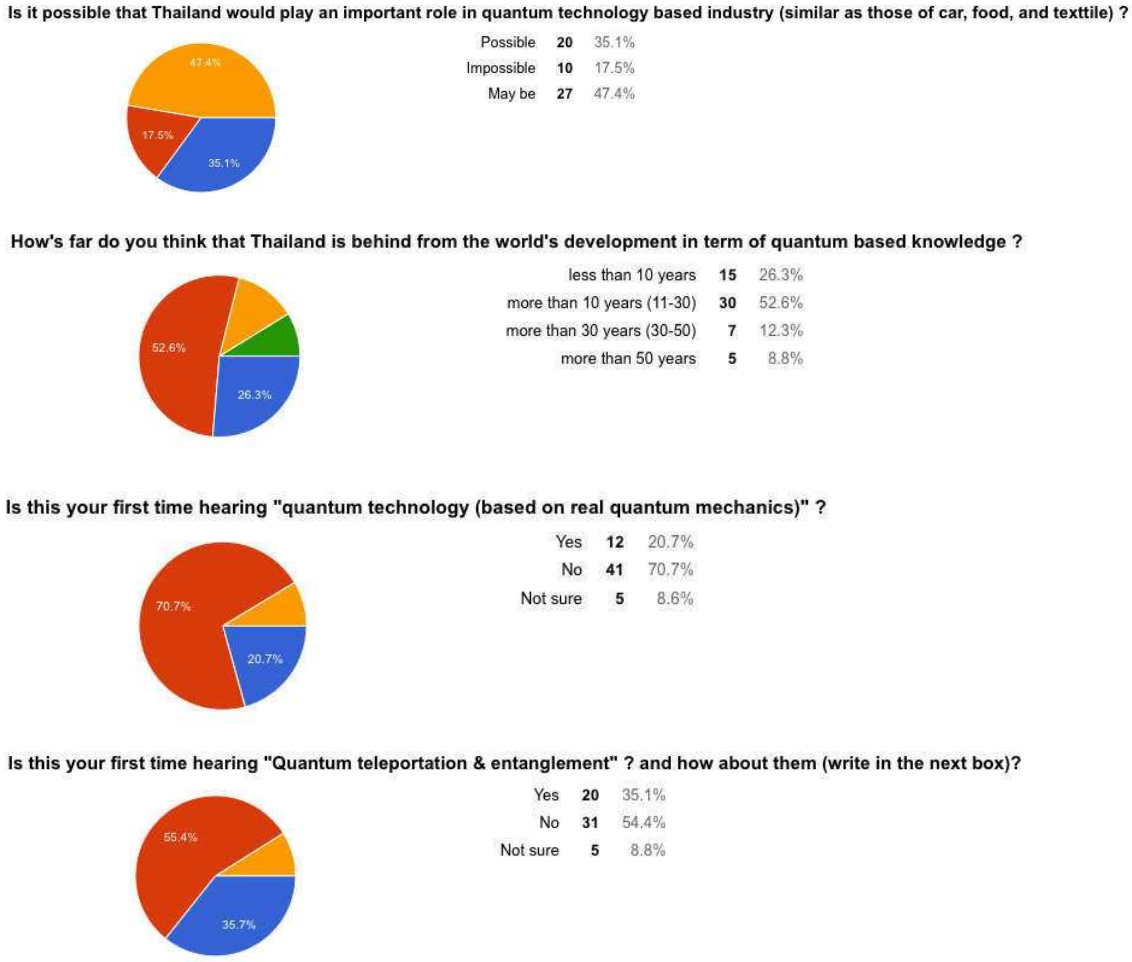
ผลการรับฟังความคิดเห็นในส่วนของข้อจำกัดของประเทศไทยในการพัฒนาเทคโนโลยีด้านสารสนเทศที่มีมาก่อนหน้านี้แสดงผลสรุปดังในรูปที่ 4.6 จากภาพรวมจะเห็นได้ว่า ผู้ตอบแบบสอบถามเห็นว่าปัญหา/ข้อจำกัดหลักของประเทศไทยในการพัฒนาเทคโนโลยีด้านสารสนเทศที่มีมาก่อนหน้านี้ได้แก่ วัฒนธรรมการวิจัยและพัฒนาในประเทศไทย (สูง 41.6% และสูงมาก 16.9%) ที่แสดงให้เห็นว่าเรายังไม่มีรูปแบบการวิจัยและพัฒนาในด้านเทคโนโลยีสารสนเทศที่ประสบความสำเร็จโดยอันดับรองลงมาคือ วัฒนธรรมการทำงานเป็น



รูปที่ 4.6 ผลการรับฟังความคิดเห็นในส่วนของข้อจำกัดของประเทศไทย
ในการพัฒนาเทคโนโลยีด้านสารสนเทศที่มีมาก่อนหน้านี้

ทีม (สูง 33.8% และ สูงมาก 20.8%) ที่มีส่วนทำให้เราวิจัยและพัฒนาเทคโนโลยีด้านสารสนเทศได้อย่างจำกัด โดยปัจจัยอื่น ๆ ที่เกี่ยวข้อง (นโยบาย การวาง roadmap และขนาดขององค์กร) มีผลต่อการพัฒนาด้านสารสนเทศนี้เช่นกัน

สำหรับผลการรับฟังความคิดเห็นในแง่อื่น ๆ (รูปที่ 4.7) สรุปได้คือ ผู้ตอบแบบสอบถามส่วนใหญ่ (47.4%) เห็นว่าประเทศไทยอาจจะเป็นส่วนสำคัญในการพัฒนาอุตสาหกรรมที่ใช้เทคโนโลยีควอนตัมเป็นฐาน โดยคิดว่าประเทศไทยล้าหลังในด้านการพัฒนาองค์ความรู้ด้านควอนตัมอยู่ประมาณ 11-30 ปี (52.6%) โดยผู้ตอบแบบสอบถามส่วนใหญ่เคยได้ยินหรือทราบเกี่ยวกับเทคโนโลยีควอนตัมมาก่อนหน้านี้แล้ว (70.7%) และเคยได้ยินหรือทราบเกี่ยวกับการเทเลพอร์ตเชิงควอนตัมและการพัวพัน (ซึ่งเป็นหัวข้อวิจัยที่มีการนำความรู้ด้านกลศาสตร์ควอนตัมมาอธิบายการทำงาน) มาก่อนหน้านี้แล้ว (54.4%)



รูปที่ 4.7 ผลการรับฟังความคิดเห็นเกี่ยวกับเทคโนโลยีควอนตัมในแง่อื่น ๆ

4.3 สรุป ปัญหาและอุปสรรค

รายงานนี้เป็นรายงานฉบับสมบูรณ์ ที่จัดทำขึ้นภายใน 911 วัน นับถัดจากวันลงนามในสัญญา ตามโครงการ การสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร ที่ได้รับการสนับสนุนในการทำโครงการจาก กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (สำนักงาน กสทช.) เนื้อหาในรายงานประกอบด้วย

บทนำที่แสดงถึงที่มาและความสำคัญที่นำมาสู่การศึกษาวิจัยตามโครงการนี้ รวมถึงวัตถุประสงค์ของโครงการ ขอบเขตของกิจกรรมตามแผนการดำเนินงานโดยรวม แผนการดำเนินงาน และ ผลที่คาดว่าจะได้รับ โดยบทที่ 2 รายงานเนื้อหาทางวิชาการที่เกี่ยวข้องกับเทคโนโลยีการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม ผลการบรรยายพิเศษโดยผู้เชี่ยวชาญได้ถูกนำเสนอในบทที่ 3 จากนั้นในบทที่ 4 เป็นรายงานสรุปกิจกรรมต่าง ๆ ที่ได้ดำเนินการมาตามโครงการนี้

สำหรับเอกสารประกอบการอบรมที่จัดทำขึ้นตามโครงการนี้ ได้แก่ “เทคโนโลยีสารสนเทศเชิงควอนตัมกับการประยุกต์” สื่อเผยแพร่ “ควอนตัมกับการสื่อสาร คืออะไร เพื่ออะไร” รายงานการสำรวจสถานะทรัพย์สินทางปัญญาของเทคโนโลยีและผลิตภัณฑ์ของทั่วโลก บทสรุปมาตรฐานรหัสลับควอนตัมโลก พ.ศ. 2557-2558 และรายงานการร่วมศึกษา “อนาคตประเทศไทยกับสารสนเทศเชิงควอนตัม” ได้แสดงในภาคผนวก ก-จ ตามลำดับ

สำหรับการดำเนินโครงการนี้ที่ผ่านมา มีความก้าวหน้าตามแผนการที่วางไว้เป็นส่วนใหญ่ และมีกิจกรรมที่เกี่ยวข้องที่นอกเหนือจากที่กำหนดในข้อเสนอโครงการ โดยในตอนต้นของการดำเนินงานนี้ผู้ดำเนินโครงการมีแผนที่จะจัดอบรมรวมเป็นคณะใหญ่ คือ มีทั้งการอบรมความรู้พื้นฐาน การอบรมความรู้เฉพาะด้าน (ควอนตัม การเข้ารหัส การคำนวณ) การสัมมนา การบรรยายพิเศษ และการอภิปรายกลุ่ม ในคราวเดียวกัน แต่เนื่องจากเทคโนโลยีด้านควอนตัมเป็นเทคโนโลยีใหม่ที่ผู้ที่สนใจใคร่รู้ จะมีความรู้พื้นฐานในด้านต่าง ๆ ที่แตกต่างกันมากพอสมควร (ฟิสิกส์ วิศวกรรมไฟฟ้า วิศวกรรมคอมพิวเตอร์ และวิทยาการคอมพิวเตอร์ เป็นหลัก) ทำให้การจัดอบรมต้องถูกแบ่งเป็นส่วน ๆ และจัดให้เหมาะสมกับกลุ่มผู้ฟังแต่ละกลุ่ม โดยเชื่อว่าในการดำเนินการต่อ ๆ ไปตามโครงการนี้ เมื่อคณะดำเนินงานมีการเผยแพร่เอกสารต่าง ๆ ได้อย่างกว้างขวางมากยิ่งขึ้น จะทำให้ผู้ที่สนใจศึกษาเทคโนโลยีนี้มีมากขึ้น และมีการนำความรู้ที่ได้รวบรวมในการทำโครงการนี้ไปใช้ต่อไป

ภาคผนวก

ภาคผนวก ก
เอกสาร “เทคโนโลยีสารสนเทศเชิงควอนตัมกับการประยุกต์”

หมายเหตุ ผู้จัดทำได้มีการเปลี่ยนชื่อเอกสารนี้ก่อนการเผยแพร่เพื่อให้เป็นที่น่าสนใจมากขึ้น

กทปส ECTI Association IEEE COMMUNICATIONS SOCIETY Thailand Chapter

ตลอดคริสต์ศตวรรษที่ 20 ที่ผ่านมา ทฤษฎีควอนตัมได้ทำให้
นักวิทยาศาสตร์เข้าใจธรรมชาติของสสารที่อยู่รอบตัวเรา
และในอนาคตความเข้าใจและการประยุกต์ใช้สสาร
รูปแบบใหม่ ๆ ก็จะมีมากขึ้นเป็นทวีคูณ
เมื่อเรามีเครื่องจักรโมเลกุล (molecular machine)
ตัวนำยวดยิ่งอุณหภูมิห้อง (room temperature superconductor)
รถไฟเหาะ (maglev train) เตาปฏิกรณ์นิวเคลียร์ (fusion reactor)
เลเซอร์พลังงานสูง (high powered laser) เครื่องยนต์ที่ขับเคลื่อน
โดยปฏิกิริยาระหว่างสสารกับปฏิสสาร (matter-antimatter engine)
และคอมพิวเตอร์ควอนตัม (quantum computer)

(ศ.ดร.สุรัตน์ ยกล้าน)

Free Distribution

ISBN 978-616-406-831-5

(วิทยาทาน)

Optical & Quantum Communications

มูลค่า ๑๘๐ บาท

United Nations Educational, Scientific and Cultural Organization

International Year of Light 2015

กสทช.

ชุดหนังสือสารสนเทศเชิงควอนตัม ๓/๒

รูป รส กลิ่น เสียง สัมผัส
ไอทีควอนตัม (2)

การประยุกต์ควอนตัม
(๒๕๕๙)

Q-Thai Forum

ทีวีสารคดีชื่อดัง "ดิสคัฟเวอรี่ (Discovery)" เคยจัดสิบอันดับการประยุกต์ใช้งาน**กลศาสตร์ควอนตัม**ในโลกความเป็นจริง *(ที่ไม่ใช่ข้างเคียงเอาชื่อควอนตัมไปใช้แต่กลายเป็นขายของหรือบริการแปลก ๆ จนถึงผสมกันให้เชื่อ เช่น เครื่องรางของขลังยี่ห้อ "ควอนตัม")* ซึ่งต่อมาปรับปรุงเป็นไม่จำกัดจำนวน เพราะมีมากมายในโลกแล้ว "There are plenty of real-world applications for quantum mechanics you may not realized are at the tips of your fingers, ..." เป็นตัวอย่างการเริ่มต้นเรื่องควอนตัมที่ดีเหมือนกันเพื่อสานไปต่ออีกสารพันวันข้างหน้าด้วย

สิบตัวอย่างแรกสุดประโยชน์ที่มากเหลือของ "ควอนตัม" ตัวจริง

แต่...ปัจจุบัน

รูป รส กลิ่น เสียง สัมผัส ไอทีควอนตัม (2)
การประยุกต์ควอนตัม (๒๕๕๙)

(จัดพิมพ์เป็นวิทยาทาน)

โดย: สุวิทย์ กิระวิทยา *(หัวหน้าโครงการ)*
ปรมินทร์ แสงวงษ์งาม จุฑาเพชร เวชรังษี
เกียรติศักดิ์ ศรีพิมานวัฒน์ *(บรรณาธิการ)*

สนับสนุนการจัดทำ: มหาวิทยาลัยนเรศวร/สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE)/สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI)/และกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส-กสทช)

พิมพ์ครั้งที่ 1: มกราคม 2559 *(99 เล่ม)*

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
เกียรติศักดิ์ ศรีพิมานวัฒน์
รูป รส กลิ่น เสียง สัมผัส ไอทีควอนตัม (2) การประยุกต์ควอนตัม (2559).
-- กรุงเทพฯ: จรัลสนิทวงศ์การพิมพ์, 2559
56 หน้า

1. เทคโนโลยีสารสนเทศ. I. ชื่อเรื่อง.

306.4833
ISBN: 978-616-406-831-5

ชุดหนังสือสี่ลำดับขั้นสารสนเทศเชิงควอนตัม: *ขั้นที่ ๓ (อ่านเล่น) เล่มที่ ๒*
ข้อมูลเพิ่มเติม: *www.facebook.com/QuantumCryptoThailand และ Q-Thai.Org*
รูปเล่ม: *ภาพลิขสิทธิ์จาก Shutterstock โดย fastbook.com*
กิจกรรมปีแห่งแสงสากล (IYL2015): *www.light2015.org*

คำนิยม

นับตั้งแต่สมัยกรีกโบราณ ปราชญ์ในสมัยนั้นคิดว่า เอกภพประกอบด้วยธาตุ 4 ชนิดคือ ดิน น้ำ ลม และไฟ แต่นักปรัชญา Democritus กลับเชื่อว่า ธาตุดังกล่าวยังประกอบด้วยชิ้นส่วนเล็กที่เขาเรียกว่า atom

ในความพยายามจะเห็น atom และอธิบายพฤติกรรมของ atom ต้องประสบความล้มเหลว จนกระทั่ง ค.ศ.1925 เมื่อทฤษฎีควอนตัมเริ่มถือกำเนิด และทฤษฎีนี้ได้ปฏิรูปวงการวิทยาศาสตร์ เพราะสามารถอธิบายพฤติกรรมของสสารหลากหลายรูปแบบได้เกือบสมบูรณ์ โดยอาศัยหลักการง่าย ๆ เพียงสองหลักการคือ พลังงานของอนุภาคในอะตอมมีค่าไม่ต่อเนื่อง คือเป็นหน่วย ๆ เรียก quantum และอนุภาคต่าง ๆ ในอะตอมสามารถแสดงสมบัติของคลื่นและอนุภาคได้

ตลอดคริสต์ศตวรรษที่ 20 ที่ผ่านมา ทฤษฎีควอนตัมได้ทำให้นักวิทยาศาสตร์เข้าใจธรรมชาติของสสารที่อยู่รอบตัวเรา และในอนาคตความเข้าใจและการประยุกต์ใช้สสารรูปแบบใหม่ ๆ ก็จะมีมากขึ้นเป็นทวีคูณ เมื่อเรามีเครื่องจักรโมเลกุล (molecular machine) ตัวนำยวดยิ่งอุณหภูมิห้อง (room temperature superconductor) รถไฟเหาะ (maglev train) เตาปฏิกรณ์ฟิวชัน (fusion reactor) เลเซอร์พลังงานสูง (high powered laser) เครื่องยนต์ที่ขับเคลื่อนโดยปฏิกิริยาระหว่างสสารกับปฏิสสาร (matter-antimatter engine) และคอมพิวเตอร์ควอนตัม (quantum computer)

สิ่งต่าง ๆ ที่ยกมาเป็นตัวอย่างนี้ล้วนถือกำเนิดจากการใช้ทฤษฎีควอนตัมที่คนส่วนใหญ่ในประเทศเราอาจไม่รู้

ดังนั้นจึงเป็นเรื่องดีมากที่คุณสุวิทย์ กิระวิทยาและคุณเกียรติศักดิ์ ศรีพิมานวัฒน์ ได้จัดทำหนังสือ "การประยุกต์ควอนตัม" ขึ้นมา เพื่อเผยแพร่ความรู้ในประเด็นนี้ให้สังคมได้รู้และเข้าใจยิ่งขึ้น เพื่อให้ทุกคนได้รับรู้และเตรียมตัวการใช้ชีวิตในโลกเทคโนโลยีอนาคตที่จะเป็นโลกแห่งเทคโนโลยีควอนตัม

ศ.ดร.สุทัศน์ ยกส้าน
ราชบัณฑิต มหาวิทยาลัยศรีนครินทรวิโรฒ
กรุงเทพฯ มกราคม 2559

คำนำ

ไอน์สไตน์ผู้โด่งดังบอกว่า
"ยิ่งทฤษฎีควอนตัมเป็นจริงมากเท่าไร ก็ยิ่งทำให้ดูไร้สาระมากขึ้นเท่านั้น
(The more success the quantum theory has, the sillier it looks)"

ควอนตัมชื่อนี้มักพบเห็นผู้ที่ได้ยินแล้วจะมีสองอาการปกติทั่วไป คือทำนองว่า **หนึ่ง**ไม่รู้เรื่อง และ**สอง**สนใจแต่เรื่องของปลอมที่ทำความเข้าใจได้ง่ายกว่าของแท้ (เช่น เหรียญอาคมของขลังที่ชื่อควอนตัมหรือเรื่องปาฏิหาริย์ต่าง ๆ) จึงเป็นเหตุที่ต้องมาเร่งพยายามทำสื่อทุกวิถีทางเพื่อการสื่อสารวิทยาศาสตร์แขนงแห่งอนาคตนี้ในทางที่ถูกต้องและเข้าใจให้ได้ง่ายขึ้นเพื่อแก้อาการทั้งสองข้างต้น การเล่าแจ้งด้านการนำควอนตัมไปประยุกต์ก็เป็นวิธีที่นิยมใช้เยียวยาอาการดังกล่าวดังเนื้อหาหลักที่อยู่ในหนังสือนี้

เล่มแรกของเรื่องรวมการประยุกต์**ควอนตัม**บรรจุไว้สิบหัวข้อหลักซึ่งอาจจะกลายเป็นเรื่องรองหรือตัวประกอบในอีกไม่กี่ปีหรือเดือนข้างหน้าก็เป็นได้ เพราะการเปลี่ยนแปลงของโลกด้านนี้รวดเร็วมาก จึงอาจมีอีกเป็นร้อยหรือมากกว่ากับการประยุกต์ใช้ควอนตัมที่จะได้ตามมา มาเริ่มต้นด้วยสิบแนวทางนี้กันก่อนแล้วค่อย ๆ เพิ่มมากขึ้นโดยจะเน้นกันเฉพาะกับงานไอทีกันในเล่มต่อไป และแม้สิบงานประยุกต์แรกนี้ประสงค์แด่สังคมได้เข้าใจ**ควอนตัม**แบบที่คิดกันว่าง่ายมากแล้ว แต่ก็ทำใจไว้เช่นกันว่า เสียงบ่นและกรน (เพราะอ่านแล้วหลับ) คงมีตามมาไม่น้อยเป็นปกติ

ดังนั้น จึงควรทวนคาถาในการเข้าถึงสิ่งที่อยู่ในเล่มนี้ด้วยบทที่ 15-18 ของ *"รูป รส กลิ่น เสียง สัมผัส ไอทีควอนตัม (1)"* จากเล่มก่อนหน้าที่ว่าด้วยประสาทสัมผัสทั้งห้าของมนุษย์เข้าไม่ถึงตรง ๆ กับปรากฏการณ์ควอนตัม

หากจะเข้าใจได้ก็ต้องมีหน่วยวัดตรวจจับหรือเซ็นเซอร์ประพฤติเป็นตัวรับรู้หรือประสาทสิ่งที่หก แล้วแปลความหมายมาให้เข้าใจได้แทน ... (งงไหม ?)

รวมทั้งจากสารคดีชุดแรกเรื่องที่ *โจนาธาน อัททีเบอร์รี่ (Jonathan Atteberry)* เผยแพร่สารคดีในดิสคัฟเวอรี่[1] นำเสนอสิบการประยุกต์ที่น่าสื่นเต้นของ**ควอนตัม**ตัวจริง ซึ่งต่อมาได้ปรับเพิ่มเปลี่ยนแปลงไปกับข้อมูลที่มากมายขึ้น *โจนาธาน* ก็ได้เกริ่นนำไว้คล้ายกันกับเรื่องความพยายามสื่อสารให้ผู้อ่านผู้ชมเข้าใจได้ง่าย เช่น

*"เป็นเวลาหลายพันปีที่มนุษย์**ใช้สัญชาตญาณ**ในการอธิบายสิ่งต่าง ๆ ในโลก บางครั้งวิธีนี้ก็ทำให้เกิดความเข้าใจผิดพลาดในตอนแรก เช่น แนวคิดที่ว่าโลกแบน แต่ท้ายที่สุดวิธีที่ว่าก็ยังคงใช้ได้ดี มนุษย์พยายามทำความเข้าใจทุกสิ่งอย่างที่พบเจอ ซึ่งมันก็เป็นไปได้อย่างช้า ๆ แต่มั่นใจด้วยการอธิบายด้วยกฎต่าง ๆ ทางฟิสิกส์ที่ไปอยู่บนพื้นฐานของการใช้**สัญชาตญาณ**" ...*

กลศาสตร์ควอนตัมมีแนวทางคณิตศาสตร์ที่รัดกุม แต่เมื่อไรที่คิดถึงมันโดยพยายามใช้**สัญชาตญาณ**จากประสบการณ์ในชีวิตประจำวัน ก็จะพบว่ามันมีความแปลกประหลาดในหลาย ๆ มุม ความแปลกของกลศาสตร์ควอนตัมนั่นกลับทำให้เกิดการคิดค้นทางเทคโนโลยีที่เปลี่ยนแปลงโลกในช่วงศตวรรษที่ผ่านมา และก็เชื่อกันว่ามันจะยังทำให้เกิดการคิดค้นสิ่งใหม่ ๆ ต่อไปได้[2]

หวังว่าการพยายามสื่อเรื่องนี้ให้ง่ายจะได้เกิดประโยชน์กับสังคมฐานความรู้ไทย และยามใดที่กลายเป็นสินค้าใหม่ ๆ มาขาย ประเทศไทยจะได้เตรียมตัวเป็นผู้ซื้ออย่างฉลาด ไม่ถูกเอารัดเอาเปรียบและรู้เท่าทันของใหม่ได้บ้าง

[1] *http://dsc.discovery.com/tv-shows/curiosity/topics/10-real-world-applications-of-quantum-mechanics.htm*

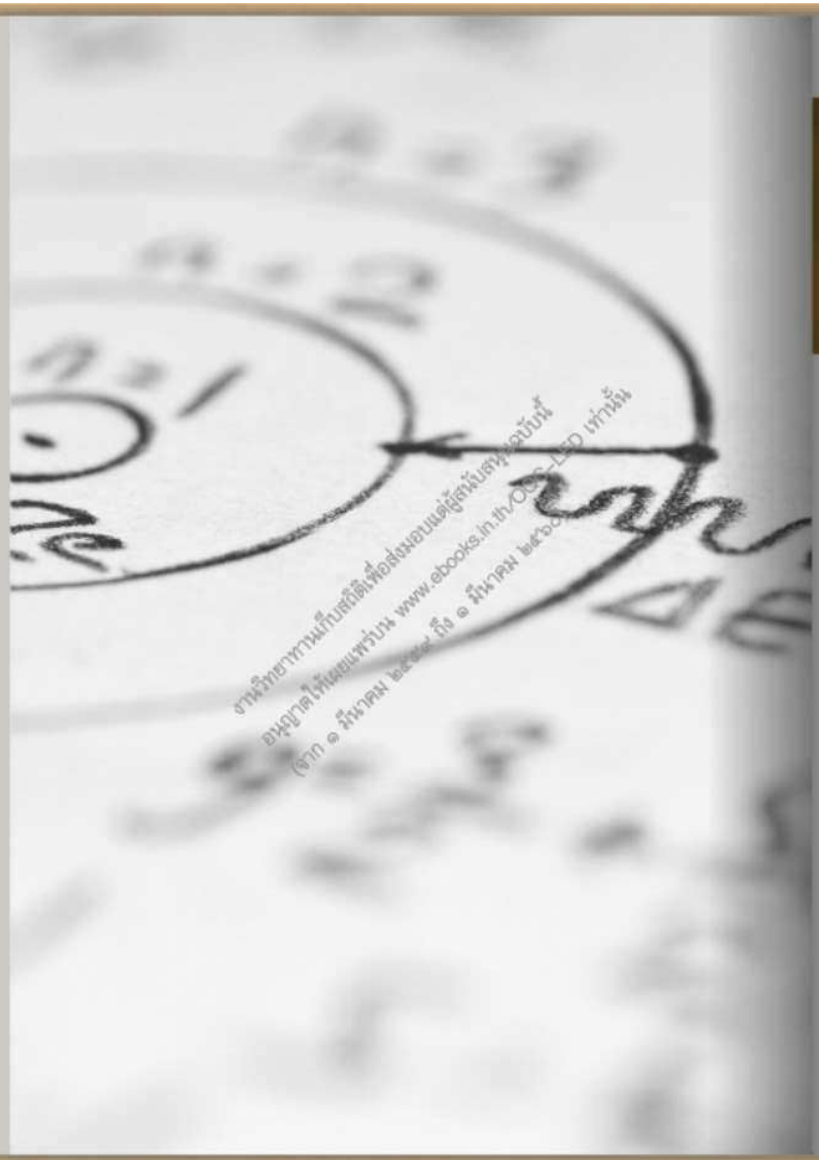
[2] *ควอนตัม (quantum) กำเนิดจากแนวคิดที่สามารถนำมาใช้อธิบายปรากฏการณ์ที่เกิดขึ้นกับอนุภาคเล็กมาก เช่น อิเล็กตรอน อะตอม โมเลกุล ได้อย่างถูกต้อง แต่ก็ขัดแย้งกับสามัญสำนึกของคนทั่วไป ทฤษฎีนี้ถูกพัฒนาในช่วง ค.ศ. 1900 – 1925 และนำมาใช้เป็นพื้นฐานในการสร้างเทคโนโลยีสมัยใหม่ได้*

ขอขอบคุณ กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส-กสทช) สำหรับการสนับสนุนโครงการ *"การสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร"* อันเป็นต้นทางของโอกาสในการทำงานสาธารณะกับหนังสือเล่มนี้ อีกครั้งหนึ่ง

คณะผู้จัดทำ

"แสง-ควอนตัม-สื่อสาร-แอลอีดี"

สารบัญ



เกริ่นกันก่อน

คล้อยหลัง ช่วงหลายปีของทศวรรษ พ.ศ. 2550 มานี้ วิทยาการด้านกลศาสตร์ควอนตัมที่มีอายุเป็นทางการมาใกล้ร้อยปีแล้วนับตั้งแต่ปี ค.ศ. 1925 (พ.ศ. 2468) และได้รับการกล่าวถึงมากขึ้น แม้จะยังดูลึกลับซับซ้อนกับการนำไปใช้งานหรือเพื่อการอธิบายปรากฏการณ์ต่าง ๆ ของหลากหลายวงการ ทั้งอุปกรณ์อิเล็กทรอนิกส์ การคำนวณยุคใหม่ การสื่อสาร กระทั่งความเกี่ยวข้องกับงานด้านชีววิทยาและสิ่งแวดล้อมก็มี หรือว่าควอนตัมได้มาอยู่รอบข้างรอบตัวจริง ๆ นานแล้วเพียงแต่มิได้สังเกต ?

กลศาสตร์ควอนตัมถูกคิดค้นขึ้นโดยมีจุดประสงค์เพื่อใช้อธิบายสิ่งต่าง ๆ ที่มีขนาดเล็กมาก ๆ แต่กำลังมีประโยชน์ที่ไม่เล็กเลย หากส่งผลกระทบกว้างใหญ่ต่อมนุษย์มากและมากขึ้นเรื่อย ... มาเริ่มดูความสำคัญกันไปตามหัวข้อที่วางเรียงอิสระดังต่อไปนี้ ของใหม่อื่น ๆ อีกมากมายจะทยอยตามมาในลำดับชิ้นงานเพื่อสาธารณะเล่มต่อไป

10 ทรานซิสเตอร์ (Transistor)

"ฉันคนชาวนา หน้าตาเซ่อ ฟังทรานซิสเตอร์ ก็พอ ใจ
ไปไหน ก็เอาไปด้วย ขึ้นเขาลงห้วย ก็เอา ไป ..."

เพลงอีสาวทรานซิสเตอร์ของ พุ่มพวง ดวงจันทร์ เป็นจดหมายเหตุได้ดีเกี่ยวกับการเข้ามาของเทคโนโลยีวงจรขยายสัญญาณในเครื่องวิทยุที่ขยับจากการใช้หลอดขยายที่ใหญ่เทอะทะ มาเป็นอุปกรณ์ขนาดจิ๋ว ทำให้เกิดเครื่องรับวิทยุที่เล็กตามไปด้วย จะขึ้นเขาลงห้วยก็สะพายแขวนใช้พลังไฟจากถ่านไฟฉายได้ จึงเป็นเรื่องฮิตของวัยรุ่น (รุ่นพุ่มพวง) ที่จะมีอุปกรณ์รับสัญญาณเสียงวิทยุเอเอ็มตามท้องไร่ท้องนาแล้วจึงเป็นที่มาของเพลงดัง (มาก) เพลงนั้น

แต่นั่นก็ทำให้เห็นได้ว่า สามสิบกว่าปีที่มีมาในประเทศไทยนั้น สิ่งประดิษฐ์นี้ใช้เวลาถึงอีกสี่สิบกว่าปีถึงจะมาสู่สยาม เพราะการคิดค้นทรานซิสเตอร์เริ่มงานมีมาตั้งแต่ พ.ศ. 2482 (ค.ศ. 1939 สำเร็จปี ค.ศ. 1947) หรือตั้งแต่ปีเกิดของนักร้องลูกทุ่งรุ่นย่า ผ่องศรี วรนุช ที่เพลงรุ่นนั้นต้องฟังจากแผ่นเสียงมาก่อนนั่นเลยทีเดียว ต่อมาภายหลังจะฟังเพลงของลูกทุ่งรุ่นหลัง เช่น วิรดา วงศ์เทวัญ ก็ได้เปลี่ยนมาฟังจากไฟล์ในโทรศัพท์เคลื่อนที่หรือจากอินเทอร์เน็ตสด ๆ กันแล้ว เล็กลงเร็วขึ้นสะดวกมากมายกว่า

ย้อนไปในปี พ.ศ. 2488 กองทัพสหรัฐอเมริกาสร้างคอมพิวเตอร์เครื่องแรกของโลกที่ชื่อ "อินิแอค (ENIAC)" จากหลอดสุญญากาศได้สำเร็จ โดยอินิแอคมีขนาดประมาณบ้านหลังเล็ก ๆ ทีเดียว ขณะที่อยู่ระหว่างการสร้าง ห้องปฏิบัติการวิจัยเบลล์ (Bell labs) ได้พัฒนาทรานซิสเตอร์ที่สามารถนำมาแทนที่หลอดสุญญากาศได้เป็นอย่างดี ทรานซิสเตอร์ที่เล็กกว่ามากนั้นทำงานเป็นได้ทั้งตัวขยายและสวิตช์หรือสลับสัญญาณ โดยการขยายและสวิตช์นี้เป็นสิ่งจำเป็นในอุปกรณ์อิเล็กทรอนิกส์ (เช่น ไอซี) ทำให้คอมพิวเตอร์มีพัฒนาการด้านขนาดที่เล็กลงเรื่อย ๆ ซึ่งกลศาสตร์ควอนตัมใช้อธิบายการสร้างการใช้งานของสิ่งที่เล็กลงเหล่านั้น ยิ่งเล็กก็ยิ่งสำคัญและทำให้เกิดการพัฒนาอย่างรวดเร็วจนไอแพดปี 53 (iPad2010) ทำงานเก่งขึ้นจากอินิแอคถึงประมาณ 5.6 พันล้านเปอร์เซ็นต์เข้าไปแล้ว

ทฤษฎี**ควอนตัม**ถูกพัฒนาและนำไปใช้อธิบายปรากฏการณ์การเคลื่อนที่ของอิเล็กตรอนในของแข็งได้ ซึ่งก็สามารถนำมาใช้พัฒนาและทำความเข้าใจการทำงานของทรานซิสเตอร์ได้เช่นกัน

อุปกรณ์ขยายสัญญาณต่าง ๆ

ผู้สร้างทรานซิสเตอร์สามท่านแรก ได้รับรางวัลโนเบลฟิสิกส์ปี ค.ศ. 1956
(ภาพจาก IEEE Global History Network: ieeeghn.org)

จดหมายเหตุ

พ.ศ. 2491 (ค.ศ. 1948) เกิดพัฒนาการสองเรื่องสำคัญที่ควรต้องจารึกไว้ นั่นคือการประดิษฐ์ทรานซิสเตอร์โดย ชอคลีย์ (Shockley) บาร์ดีน (Bardeen) และแบรทเทน (Brattain) ในช่วงต้นปี และการตีพิมพ์บทความของโคลด แชนนอน (Claude Shannon) หัวข้อ "ทฤษฎีคณิตศาสตร์สำหรับการสื่อสาร (Mathematical Theory of Communication)" ในปีเดียวกัน ซึ่งทั้งสี่คนนี้ล้วนแล้วแต่เป็นนักวิจัยจากหน่วยปฏิบัติการเบลล์ (Bell Laboratories) พัฒนาการของทั้งสองเรื่องที่เกิดขึ้นนี้ได้กลายเป็นรากฐานสำคัญสำหรับเทคโนโลยีของช่วงเวลาถัด ๆ มา ช่วยเปิดโลกสู่ยุคดิจิทัลและการสื่อสารข้อมูลอีกด้วย[1, 2]

[1] ประวัติย่อ "การสื่อสารโลก" (A Brief History of Communications) ISBN 978-974-10-4920-2
[2] ท่องไปในพิพิธภัณฑ์ไฟฟ้า ISBN 978-974-88238-7-4

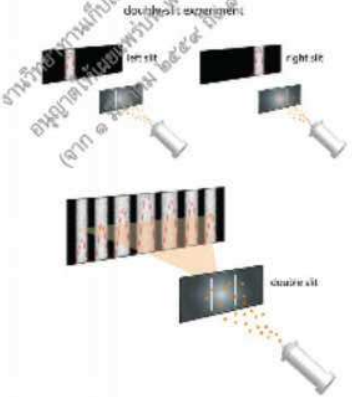
9 ตัวเก็บเกี่ยวพลังงาน (Energy Harvester)

ทุกครั้งที่ขับรถโดยใช้พลังงานจากน้ำมันในการเดินเครื่องยนต์ นอกจากกำลังทางกลที่ได้แล้วยังได้ความร้อนออกมามากอีกด้วย ความร้อนเหล่านี้จะถูกปล่อยให้สูญเสียไปในอากาศ นักวิจัยจำนวนหนึ่งมีแนวคิดที่น่าพลังงานความร้อนนั้นกลับมาใช้ประโยชน์ โดยใช้วัสดุเทอร์โมอิเล็กทริก (Thermoelectric) ที่สามารถเปลี่ยนความร้อนเป็นไฟฟ้าได้ และด้วยกลไกประยุกต์ช่วยเก็บความร้อนของแผงเซลล์สุริยะ (solar cell) ให้เป็นไฟฟ้าและช่วยคลายความร้อนของแผงได้อีก วัสดุนี้มีประสิทธิภาพสูงและมีความหนาเพียงแค่ในระดับหน่วยไมโครเมตร โดยไม่มีส่วนที่ต้องขยับหรือเคลื่อนที่และไม่ทำให้เกิดมลพิษ ก็เป็นอีกหนึ่งเรื่องที่ใช้ควอนตัมอธิบาย ออกแบบ สร้าง แม้ชื่อจะยังไม่มีเข้าไปเกี่ยวข้องตรง ๆ

เป็นที่ทราบกันในหมู่นักวิทยาศาสตร์ว่า ปรากฏการณ์**การแทรกสอดเชิงควอนตัม (quantum interference)** เป็นสิ่งที่เกิดขึ้นในระหว่างการเคลื่อนที่ของอิเล็กตรอน แต่แนวคิดที่จะนำปรากฏการณ์นี้มาใช้ร่วมกับการเหนี่ยวนำให้เกิดกระแสไฟฟ้าจากความร้อนนั้นเพิ่งตามมา ด้วยการพยายามออกแบบให้อุปกรณ์ที่สร้างจากวัสดุเทอร์โมอิเล็กทริกสามารถนำคลื่นความร้อนได้ในทิศทางเดียว ก็จะทำให้เกิดกระแสไฟฟ้าที่เหนี่ยวนำจากความร้อนนี้ไหลไปในทิศทางเดียวด้วย โดยวัสดุที่ได้จะมีประสิทธิภาพสูงและมีความหนาระดับแค่หนึ่งในล้านส่วนของหน่วยเมตร

ควอนตัมกับการปรากฏการณ์การแทรกสอด (quantum interference) คือคุณสมบัติความเป็นคลื่นและอนุภาคระดับควอนตัม (อิเล็กตรอน) โดยตำแหน่งที่มีการแทรกสอดแบบเสริมกันในตัวอุปกรณ์คือตำแหน่งที่มีโอกาสพบอนุภาคนั้นมาก ส่วนตำแหน่งที่มีการแทรกสอดแบบหักล้างโดยสมบูรณ์ก็คือตำแหน่งที่จะไม่มีโอกาสพบนั่นเอง

นักวิจัยมีแผนการใหญ่หลายเรื่องสำหรับวัสดุนี้ เช่น คาดกันไว้ว่าหากใช้วัสดุนี้กับระบบรถยนต์คันหนึ่ง จะสร้างไฟฟ้าได้เท่ากับหลอดไฟ 100 วัตต์ ประมาณ 200 หลอด นอกจากนั้น วัสดุนี้ยังสามารถเสริมการทำงานของเซลล์แสงอาทิตย์ได้อีกด้วย ซึ่งโดยทั่วไปเซลล์แสงอาทิตย์จะสูญเสียพลังงานในรูปของความร้อน การใช้วัสดุเทอร์โมอิเล็กทริกเพื่อแปลงความร้อนเป็นไฟฟ้าจะทำให้ได้พลังงานที่เพิ่มขึ้น เซลล์แสงอาทิตย์ก็จะมีประสิทธิภาพมากยิ่งขึ้นด้วยเพราะจะทำงานด้วยอุณหภูมิที่ต่ำลง

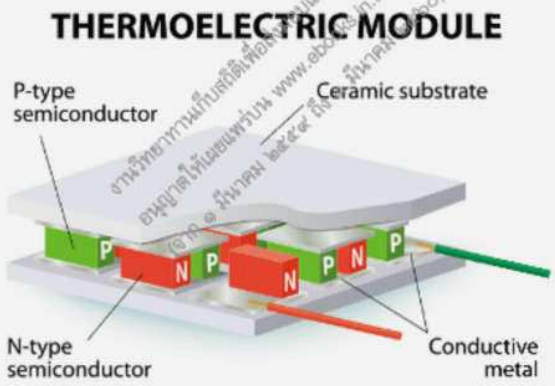


ภาพแสดงพื้นฐานเรื่องการแทรกสอดจากการทดลองสลิทคู่ คล้ายกับที่พบได้ในห้องเรียนสมัยมัธยม

จดหมายเหตุ

พ.ศ. 2344 (ค.ศ. 1801) โทมัส ยัง (Thomas Young) ประดิษฐ์การทดลองพื้นฐานเรื่องช่องคู่ (double-slit experiment) ที่ต่อมานำมาใช้อธิบายปรากฏการณ์อนุภาคและคลื่นรวมมาถึงการแทรกสอดเชิงควอนตัมให้เกิดความเข้าใจได้สะดวก

ปรากฏการณ์การแทรกสอดเชิงควอนตัมนี้ต่อมาพบเห็นได้ในการประยุกต์กับงานด้านอุปกรณ์ตัวนำยวดยิ่ง (superconducting quantum interference device (SQUID)) รวมถึงรหัสลับและการคำนวณเชิงควอนตัมมากมายแล้ว



ภาพแสดงโครงสร้างของวัสดุเทอร์โมอิเล็กทริก

นาฬิกาเที่ยงตรงสูง (Ultraprecise Clocks) 8

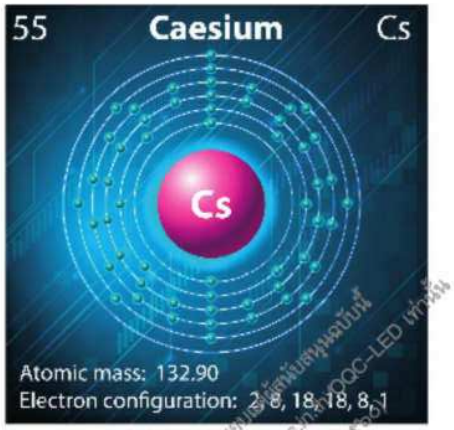
นาฬิกา ไม่ว่าจะแบบเข็ม ตัวเลข จนถึงการย้อนยุค (ไปในอนาคต) กับนาฬิกาฉลาดจากทั้งสองค่าย (iWatch & Android) จะช้าหรือเร็วไปกี่วินาทีคงไม่สำคัญนักกับเรา ๆ ท่าน ๆ แค่ไม่ทำให้ตกรถ ตกเที่ยวบินเป็นพอ ... แต่สำหรับหน่วยงานที่ทำหน้าที่รักษามาตรฐานเวลา เช่น กรมอุทกศาสตร์ 1811 หรือสถาบันมาตรวิทยา จะสำคัญมากเพื่อบริการสำหรับกิจกรรมด้านความมั่นคง ชั่วพริบตา การสื่อสารความเร็วสูงยิ่ง ตลาดหลักทรัพย์กับการซื้อขายและการเงินนาทีท้าย ๆ การขนส่งทางน้ำทางอากาศและพิกัดดาวเทียมและอื่น ๆ อีกมาก แม้การเทียบท่าของยานกับสถานีอวกาศที่ก็พลาดเวลาไม่ได้ เศษเสี้ยววินาทีที่แตกต่างจะมีผลกระทบที่สูงมาก

หลายหน่วยงานที่ให้บริการทั่วโลกได้ใช้นาฬิกาอะตอม (atomic clock) ในการเทียบวัดเวลาให้ถูกต้องอยู่เสมอ ความถูกต้องที่ดีของนาฬิกานี้สร้างจากอะตอมของซีเซียม (Cesium) ซึ่งให้ "ความไม่แน่นอน" ของเวลาเพียง 1 วินาทีในทุก ๆ 20 ล้านปี และความไม่ถูกต้องดังกล่าวเกิดจากสิ่งที่เรียกว่า **"การรบกวนเชิงควอนตัม (quantum noise)"** ... การทำความเข้าใจประยุกต์ใช้กลศาสตร์ควอนตัมจะเป็นส่วนสำคัญที่ทำให้สามารถสร้างนาฬิกาความเที่ยงตรงและผลกระทบสูงนี้ได้ดีด้วย

แม้เหมือนไกลตัวแต่ก็ได้ใช้อยู่ใกล้ ๆ แบบไม่รู้สึกตัว ...
"ควอนตัม" ได้เข้ามาใกล้ในชีวิตประจำวันกันมากขึ้น
กระทั่งเรื่องการสร้างการควบคุมเศษเสี้ยวของเวลาก็เช่นกัน !

เวลาคือมูลค่าทางเศรษฐกิจ เราจึงมีเวลาเป็นเงินเป็นทอง !

เวลาของการกิจในห้วงอวกาศต้องแม่นยำสูงยิ่ง มีผลต่อทั้งพลังงานที่ใช้ การสื่อสารเพื่อการควบคุมระยะไกลมาก ตำแหน่ง หรือความปลอดภัย ฯลฯ



อะตอมของซีเซียม (Cesium หรือ Caesium)

หนึ่งวินาที คือ ค่าช่วงระยะเวลาที่เกิดการแผ่รังสีกลับไปมาระหว่างอะตอมซีเซียม-133 สองอะตอมจำนวน 9,192,631,770 ครั้ง ... (the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the caesium 133 atom ~ *The International System of Units (SI)*)

ควอนตัมกับ "การรบกวน" (quantum noise) เป็นปรากฏการณ์ของระบบที่ถูกรบกวนจากต้นเหตุความเป็นควอนตัมโดยธรรมชาติ เช่น ในสัญญาณไฟฟ้าตัวอย่างขนาดต่ำมากจะเห็นความไม่ต่อเนื่องจากการไหลของอิเล็กตรอน ก่อให้เกิดความไม่สม่ำเสมอของสัญญาณอันยากที่จะคาดเดาได้ ซึ่งก็คือการรบกวนเชิงควอนตัมแบบหนึ่งนั่นเอง

จดหมายเหตุ

พ.ศ. 2403 (ค.ศ. 1860) โรเบิร์ต บันเซ็น (Robert Bunsen) นักเคมีชาวเยอรมัน และ กุสตาฟ เคอร์ชอฟ (Gustav Kirchhoff) นักฟิสิกส์ ค้นพบธาตุซีเซียม (Cesium หรือ Caesium)

พ.ศ. 2464 (ค.ศ. 1921) กองอุทกศาสตร์ได้รับการยกฐานะเป็นกรมอุทกศาสตร์ทหารเรือ (ให้บริการเทียบเวลา โทร.1811)

พ.ศ. 2540 (ค.ศ. 1997) สถาปนาสถาบันมาตรวิทยาแห่งชาติ ตาม พ.ร.บ.พัฒนาระบบมาตรวิทยาแห่งชาติ พ.ศ.2542 (ให้บริการปรับเทียบเวลามาตรฐานประเทศไทยจากนาฬิกาซีเซียมมีความไม่แน่นอนอยู่ที่ 20 นาโนวินาที)

พ.ศ. 2558 (ค.ศ. 2015) ข้อมูลดาวพลูโตจากยาน "ฟ้าขอบใหม่" (New Horizons) ใช้เวลาสี่ชั่วโมงครึ่งจากการเดินทางสามพันล้านกิโลเมตรมายังโลก (สถานีที่สเปน สหรัฐฯ หรือออสเตรเลีย) ต้องใช้ฐานเวลาที่แม่นยำมากเช่นกัน

เครื่องสร้างสัญญาณนาฬิกาแบบอะตอม (atomic clock)

7 รหัสลับเชิงควอนตัม (Quantum Cryptography)

ตั้งแต่โบราณสมัยกรีก ความลับของการศึกสงครามสามารถส่งข้อความผ่านไปโดยการเขียนไว้บนแถบกระดาษหรือผ้าที่พันอยู่รอบแท่งไม้ได้พอดิบพอดี จากนั้นก็แกะมันออกก่อนส่ง ข้อความเหล่านั้นดูเหมือนไม่มีความหมายหากไม่ได้พันกลับเข้าไปในแท่งไม้ขนาดเท่าเดิม จนมาถึงมือผู้รับที่รู้หลักการพันกระดาษหรือผ้านั้นจึงได้ความลับคืนมา หลักการเข้ารหัสแบบนี้ยังใช้ได้ดีแต่เหมาะกับข้อความไม่กี่ตัวอักษรหรือสั้นมาก หากต่อมาข้อความนับเกินหลักล้านอักขระในแต่ละวัน มัวแต่พันกระดาษรอบไม้การศึกคงได้แพ้ราบคาบเป็นแน่ … หว่าศาสตร์การเข้ารหัสบนแท่งไม้นี้ได้มีพัฒนาการเป็นรากฐานรหัสลับของอนาคตตั้งแต่นั้นมา รู้ไว้ใช่ว่า !

จนมาถึงการใช้ความรู้เรื่องกลศาสตร์ควอนตัมในการเข้ารหัสข้อมูลที่เรียกว่า "รหัสลับเชิงควอนตัม" ทำให้มนุษย์ได้วิธีการเข้ารหัสที่สมบูรณ์ (อย่างน้อยก็ในเชิงทฤษฎี) โดยการใช้ควอนตัมจากหน่วยที่เล็กที่สุดของแสงหรือโฟตอนเป็นกุญแจควอนตัมเพื่อการเข้ารหัสยุคเริ่มแรก และจากการทดลองในห้องปฏิบัติการเมื่อปี พ.ศ. 2535 ได้กลายมาเป็นนวัตกรรมไอทียุคใหม่มีขายกันแล้ว โดยที่เจ้าของบริษัท ID Quantique (Gregoiry Ribordy) แจ้งว่าขายดีขึ้นมากหลังจากที่เอ็ดเวิร์ด สโนว์เดน (Edward Snowden) ดีแผ่วิธีการแกะรหัสลับแบบพื้น ๆ ทั่วไปของรัฐบาลอเมริกัน บริษัทนี้ได้โครงการใหม่ ๆ ขยายใหญ่ตามมาอีกมาก ควอนตัมใช้ได้ขายได้รวยได้แล้วหรือนี่

เครื่องกระจายกุญแจรหัสลับเชิงควอนตัม

เจ้าของบริษัท IDQ พื้นฐานนักฟิสิกส์ญี่ปุ่น ตั้งตนเองเป็นวิศวกรต่อจากงานวิทยานิพนธ์ที่สำเร็จปริญญาเอก สร้างตนเองเก็บเกี่ยวผลสัมฤทธิ์ จนเป็นควอนตัมเจ้าเดียวของโลกที่ยังอยู่ยงคงกระพันโดยไม่ได้อาศัยงบวิจัยของรัฐฯ เป็นพลัง ประหยัดสุด ๆ มาเมืองไทยด้วยตั๋วชั้นประหยัดแบบถามมาก่อนด้วยว่าค่าแท็กซี่ไปกลับสนามบิน (550 บาท) แพงไหม 7 แบบนี้จะไม่ให้รวยได้อย่างไรกับการเป็นนักวิศวกรฟิสิกส์ ผู้ขายเครื่องรหัสลับควอนตัมราคาร่วม 5 ล้านบาทต่อเครื่อง

ควอนตัม (quantum) เป็นปริมาณทางกายภาพที่เล็กที่สุดที่ไม่สามารถแบ่งแยกได้อีก สำหรับแสงที่ใช้ในการสื่อสารจะมีหน่วยเป็น โฟตอน (photon) วิทยาการรหัสลับควอนตัมอาศัยคุณสมบัติทางควอนตัมของโฟตอนหน่วยเดียวที่ว่า ไม่มีใครสามารถคัดลอกสถานะทางควอนตัมของโฟตอนเดี่ยวได้โดยไม่เปลี่ยนแปลงสถานะดั้งเดิมของมัน เมื่อนำมาใช้เป็นรหัสจึงทำให้มั่นใจได้ว่าการสื่อสารด้วยวิทยาการนี้ปลอดภัยสูงสุด

ควอนตัมนำมาใช้กับงานไอทีได้โดยอาศัยหลักความไม่แน่นอน (Uncertainty Principle) ของนักวิทยาศาสตร์รางวัลโนเบล *แวร์เนอร์ ไฮเซนแบร์ก (Werner Heisenberg)*

จดหมายเหตุ

พ.ศ. 2527 (ค.ศ. 1984) ชาร์ลส์ เบนเนตต์ (Charles Bennett) และ จิลส์ บราสซาร์ด (Gilles Brassard) เสนอวิธีการกระจายกุญแจรหัสลับด้วยกลศาสตร์ควอนตัม (Quantum Key Distribution) เป็นครั้งแรก

พ.ศ. 2532 (ค.ศ. 1989) ชาร์ลส์ เบนเนตต์ และคณะ แสดงการทดลองการกระจายกุญแจเชิงควอนตัมครั้งแรกระยะเพียง 30 ซม.

พ.ศ. 2547 (ค.ศ. 2004) ก่อตั้งบริษัท ID Quantique (IDQ) ณ ประเทศสวิตเซอร์แลนด์ จำหน่ายเครื่องกระจายกุญแจรหัสลับควอนตัมแรกของโลก

พ.ศ. 2558 (ค.ศ. 2015) กลุ่มความปลอดภัยสื่อสารอิเล็กทรอนิกส์ (CESG) องค์การแห่งชาติเพื่อความมั่นคงข่าวสารของเกาะอังกฤษ เสนอรัฐบาลว่ายังไม่ควรใช้เพราะระดับและผลของเทคโนโลยียังไม่นิ่ง !

ข่าวแปลกในวงการ !

"กลศาสตร์ควอนตัม แฝงตัวอยู่ในแวดวงไอทีและอุตสาหกรรมมานานแล้ว"

รูปแบบการเข้ารหัสนี้ทำให้ไม่มีใครสามารถดักจับข้อมูลได้ แต่ก็มีนักวิจัยพยายามพิสูจน์ว่าการดักจับข้อมูลนั้นทำได้ โดยการหลอกเครื่องอ่านข้อมูลและตั้งชื่อที่สับสนคนไอทีว่า การแฮกควอนตัม (quantum hacking) ซะด้วย !

ท่าว การสนทนาของเซียนไอทีควอนตัมในวงกาแฟกล่าวไว้ว่า

"รหัสลับควอนตัมสมบูรณ์แบบป้องกันวิธีดักข่อยสาย (wire tapping) หรือขโมยระหว่างทาง แต่กิจกรรมแบบที่นักฟิสิกส์กลุ่มที่นอร์เวย์และแคนาดาแจ้งทำนองการไปฝังตัวอยู่ในภาครับแสง (detector) นั้น เขาเรียกว่าปล้น ! ไม่ใช่การขโมยแล้ว แถมปล้นโฟตอนหรือแสงยังไม่ใช่ตัวข้อมูลแล้วก็ไม่ใกล้เคียงกันเลย เข้าใจอะไรเพี้ยนไปตั้งไหญ่แล้ว (ในเมืองไทยก็มีจิ๊กจี้ทำตามอยู่เหมือนกัน)

quantum hacking จึงเป็นสองสิ่งที่คนในวงการให้คำจัดความว่า self-promote อันหมายถึงโฆษณาแฝงเป็นบ่อดักคนหลงเชื่อของบริษัทที่ประสงค์ขายของวิธีแปลก หรืออีกพวกที่ทำงานเด่นดีด้านตัวรับแสงแต่กลับตั้งชื่องานให้เอียงสีข้างเข้ามาพ่วงชื่อเสียงกับรหัสลับควอนตัมซะอย่างนั้นทั้งที่ไม่เกี่ยวกัน

หากปล้นแสงได้ที่บ้านผู้ใช้แบบนั้นจะต่อสายไฟเบอร์ให้ยุ่งยากทำ (...) อะไรก็ขอรหัสผ่านหรือสำเนาข้อมูลไปจากเครื่องผู้ใช้เลยง่ายกว่า แหม ! ป้องกันขโมยดันมาปล้น หากเข้าถึงบ้านได้แล้วก็ยกเครื่องควอนตัมไปเลย หมดเรื่อง !"

6 เครื่องกำเนิดจำนวนสุ่มเชิงควอนตัม (Randomness Generator)

ทำไมนักวิทยาศาสตร์จึงพยายามที่จะหาจำนวนสุ่มด้วยวิธีทางควอนตัม ในเมื่อเขาก็สามารถทำได้โดยเพียงแค่การทอยลูกเต๋า ?

ก็เพราะว่าหากนักวิทยาศาสตร์มีข้อมูลเพียงพอเกี่ยวกับลูกเต๋าที่ทอย ก็จะสามารถจำลองการทอยและทำนายผลลัพธ์ได้อย่างถูกต้อง ไม่ว่าจะเป็นการหมุนวงล้อ โยนเหรียญหรือการสร้างตัวเลขสุ่มด้วยคอมพิวเตอร์ทั่วไปก็เช่นกัน ที่ท้ายสุดผลลัพธ์ของการสุ่มด้วยวิธีพื้น ๆ เหล่านี้สามารถทำนายหรือคาดเดาผลได้ก่อน ... จนได้ เมื่อมีใครรู้ผลล่วงหน้านั้นแล้วประโยชน์ก็ไม่เหลือ !

แต่ในโลกแห่งควอนตัมสิ่งต่าง ๆ ล้วน "คาดเดาล่วงหน้าไม่ได้" การสุ่มที่แท้จริงจะเกิดขึ้นในระดับควอนตัมนี้เท่านั้น นักวิจัยจึงได้ใช้ประโยชน์มาสร้างเป็นลูกเต๋าควอนตัมขึ้น เช่น จากความผันผวนในสุญญากาศหรือสร้างสัญญาณรบกวนเชิงควอนตัม จึงสามารถสร้างจำนวนสุ่มที่แท้จริงนำไปใช้ได้มากมาย ตั้งแต่เพื่อการเข้ารหัสข้อมูลความปลอดภัยสูง การจำลองสภาพอากาศและการทดสอบอย่างหลากหลาย...

คำถาม:

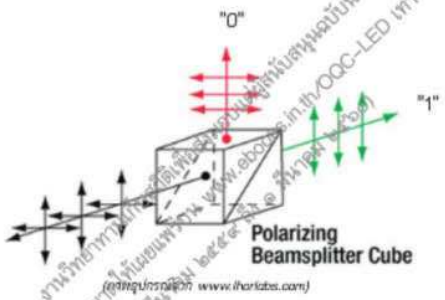
"แล้วการขูดเสา เรียไม้ตะเคียน แกะเลขจากรอยพญานาค ดูต้นไม้ใหญ่ผนังกุสุสานจนเลข (ธนสิบ) ใบลานขึ้นมาเอาไปซื้อหวยก็ถือว่าเป็นเครื่องกำเนิดจำนวนสุ่มแบบธรรมชาติที่ง่ายจริง มีทั่วไปไม่ใช่หรือ ?"

บอกใบ้:

"แล้วแหล่งข้อมูลแบบนั้นไม่เคยให้เลขลำเอียงเลยหรือ ?"

เช่น แปลกไหมที่วิธีไทย ๆ เหล่านั้นไม่มีใครขูดได้เลขไทยฐานสอง (๐ ๑) หรือฝรั่งฐานแปดและฐานสิบหก (0 – F) บ้างเลย หากทำได้จะได้นำเข้าเครื่องคำนวณดิจิทัลได้ทันที อยู่เมืองไทยเล่นออกแต่ฐานสิบแบบฝรั่งนั้นดูช่างลำเอียง เป็นความสามารถส่วนตัวมิใช่ธรรมชาติแท้ แล้วจะเป็นเลขสุ่มจริงได้อย่างไรกัน

ผลึกแยกลำแสง (beam splitter) สะท้อน (50%) : ทะลุผ่าน (50%)



(ดูเพิ่มเติมที่ www.thorlabs.com)

วิธีการสร้างจำนวนสุ่มแท้จากโฟตอนเดี่ยว (single photon) เชิงควอนตัมแบบง่าย ๆ

ลำแสงที่เดินทางผ่านไปยังผลึก (เส้นสีดำ-ซ้าย) โฟตอนหน่วยเดียว (ปริมาณแสงที่จางที่สุดจนเหลือเป็นโฟตอนเดี่ยว) จะเลือกเส้นทางที่มีโอกาสเท่าเทียมกัน 50:50 ว่าจะไปในทาง เส้นสีแดง-บน หรือ สีเขียว-ขวา หากกำหนดให้มีภาครับแสงดิจิทัลอยู่ทั้งด้าน เช่น สีแดงเป็น "0" สีเขียวได้เป็น "1" บิตข้อมูลที่ได้จะมีโอกาสเกิด "0" และ "1" เท่ากัน

ควอนตัม อธิบายการเกิดแนวทางสุ่มอย่างแท้จริง (true randomness) ทฤษฎีนี้อาศัยพื้นฐานเรื่องความน่าจะเป็น โดยอนุภาคในทางควอนตัมนั้นไม่สามารถแยกได้อีก เช่น โฟตอนหนึ่งหน่วย ดังนั้น โฟตอนเดี่ยวจะต้องเลือกเส้นทางในการเคลื่อนที่ผ่านตัวแยกลำแสงออกไปในเส้นทางเดียวเท่านั้น (ไม่สะท้อนก็ทะลุผ่าน)

จดหมายเหตุ

พ.ศ. 2553 - 2557 - ช่วงเวลาที่เคยมีบริการแหล่งกำเนิดจำนวนสุ่มเชิงควอนตัมและการทดสอบจำนวนสุ่มในประเทศ (Web service: Quantum Random Number Generation and Testing Service) *ThaiRAND*

พ.ศ. 2556 (ค.ศ. 2013) - เอ็ดเวิร์ด สโนว์เดน (Edward Snowden) แฉว่ารหัสลับจากวิธีสุ่มเลขแบบ Dual EC DRBG ที่ใช้กันทั่วโลกอินเทอร์เน็ต คือประตูหลังที่หน่วยงานความมั่นคง (NSA) สหรัฐฯ แอบเปิดเข้าไปยุ่งกับข้อมูลของผู้อื่นแม้จะแนะนำรับรองโดยหน่วยงานมาตรฐานระดับโลก (NIST) ของประเทศเดียวกันก็ตาม

สุ่มตัวเลขแบบเต๋า ๆ

เลขการสุ่มที่ดูดีเลย มีสองครั้งที่ซ้ำกันเลยเชียว

การสุ่มดิจิทัลในชีวิตประจำวันใกล้ตัว

เคยทราบไหมว่ามีจำนวนสุ่มวิ่งวนอยู่รอบตัวทั้งในแอปโทรศัพท์เคลื่อนที่ การเปิดปิด ลากเมาส์ เข้าเว็บ การกรอกรหัสผ่าน ใช้งานเวปและกิจกรรมบนคอมพิวเตอร์ มีการสร้างจำนวนสุ่มที่คาดเดาได้ (run dry) .. ปลอดภัยกันไว้ก่อน !

ทฤษฎีกับโลกแห่งความจริง

จำนวนสุ่มเชิงควอนตัมตามทฤษฎีข้างต้นที่ให้ผลเป็นเลิศเหมาะแก่การประยุกต์ใช้ให้รหัสลับมีความปลอดภัยเป็นยอด แต่ก็แค่อุดมคติเพราะไม่มีอะไรที่มนุษย์สร้างจะเป็น "สิ่งสัมบูรณ์" จากหลักการ 50:50 ผลอาจได้ 49.9% กับ 50.1% (หรือ 50.0001 กับ 49.9999) ออกมาแทน เป็นต้น .. ปลอดภัยกันไว้นะ !

แหล่งกำเนิดจำนวนสุ่มควอนตัม(สัมพัทธ์)แบบพร้อมใช้งาน

จำนวนสุ่มดิจิทัลเพื่อสาธารณะ

เคยมีเวปให้บริการจำนวนสุ่มควอนตัมออนไลน์ (web service) เพื่อการทดสอบงานวิจัยทางวิทยาศาสตร์ คณิตศาสตร์ และรหัสลับในเมืองไทย ปกติจะมีผู้ใช้งานเข้าบ้าง แต่กลับมีการจราจรอินเทอร์เน็ตหนาแน่นทุกช่วงเช้าของวันที่ 1 และ 16 ของทุกเดือน .. หวย ?

คำเตือน:

ไม่เคย .. การพนันมิเคยเป็นการสุ่มให้ใครได้รวยจริง แต่ตั้งใจกำหนดกันก่อนแล้วว่าให้ผู้หลงงมงายนั้น ๆ หมดอนาคตหมดตัวแน่ .. ขอบอก

5 เลเซอร์ (Lasers)

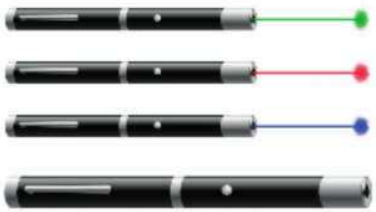
การศึกษาเลเซอร์ในช่วงแรกเริ่มเกิดจากความอยากรู้ด้านวิชาการโดยมิได้คำนึงถึงการนำไปประยุกต์ใช้ แต่ต่อมาแสงเลเซอร์กลับกลายเป็นหัวใจของอุปกรณ์และเครื่องมือไฮทีหลายชนิด ตั้งแต่ของใช้ลิดบ้านกับเครื่องเล่นซีดี เครื่องมือแพทย์ เครื่องมือวัดความเร็วรถของตำรวจทางหลวง การสื่อสารความเร็วสูง ไปจนถึงระบบแจ้งพิกัดเพื่อป้องกันจรวดนำวิถี เป็นต้น

เลเซอร์ทั่วไปทำงานด้วยการกระตุ้นอิเล็กตรอนในวงโคจรของอะตอมให้ไปอยู่ในระดับพลังงานที่สูงขึ้น จากนั้นจึงทำให้มันปลดปล่อยพลังงานในรูปของแสงหนึ่งหน่วยที่เรียกว่าโฟตอนมีทั้งพลังงานและทิศทางเดียวกันทั้งหมด จึงทำให้ได้ลำเลเซอร์ออกมาในที่สุด

กระบวนการทั้งหมดนี้เกิดจากการเข้าใจหลักการของกลศาสตร์ควอนตัมที่เสนอโดยนักฟิสิกส์ทฤษฎีชื่อ แมกซ์ พลังค์ (Max Planck) ได้กล่าวไว้ว่า ระดับพลังงานของอะตอมมีค่าไม่ต่อเนื่องมีลักษณะเป็นกลุ่มก้อนที่เรียกว่า **ควอนต้า (quanta)** โดยแนวคิดนี้ใช้ในการอธิบายการเปล่งแสงที่มีระดับพลังงานเจาะจงในการเกิดเลเซอร์นั่นเอง

ควอนตัมอธิบายการเกิดเลเซอร์ได้จากที่อะตอมและโมเลกุลมีระดับพลังงานของอิเล็กตรอนแบบไม่ต่อเนื่องอันเป็นปรากฏการณ์พื้นฐานของกลศาสตร์ควอนตัม และเมื่อได้รับการกระตุ้นเหมาะสมก็จะปล่อยแสงเลเซอร์ออกมา (อีกแนวทางหนึ่งอันเกิดจากการเปล่งแสงแบบถูกเร้า (stimulated emission) อิเล็กตรอนจะถูกกระตุ้นให้มีระดับพลังงานลดลงทำให้เกิดโฟตอนที่มีคุณสมบัติเป็นแสงเลเซอร์ออกมาได้ด้วยเช่นกัน)

แมกซ์ พลังค์ หนึ่งในผู้ก่อตั้งทฤษฎีควอนตัม



พัฒนาการของเทคโนโลยีสำคัญแขนงที่มีความสำคัญต่อมาในระยะยาวคู่มากับการใช้งานแสงเลเซอร์เพื่อการสื่อสารข้อมูลหรือไอทีนั่นคือ เส้นใยนำแสง (Optical Fiber)[3] ซึ่งเกิดขึ้นประมาณระหว่างกลางถึงปลายทศวรรษที่ ค.ศ. 1960 นักวิจัยที่เกี่ยวข้องได้ทำการพัฒนาเลเซอร์อันมีคุณสมบัติโคฮีเรนท์ (coherent) ปรับลำแสงขนาน (collimated) และสร้างลำแสงเอกรงค์[4] (monochromatic beams) ได้

ย้อนกลับไปในช่วงแรกของเลเซอร์ซึ่งเป็นเพียงเครื่องมือวิจัยที่ใช้อยู่ในห้องปฏิบัติการเท่านั้น แต่วิศวกรสื่อสารได้ตระหนักว่าเลเซอร์นี้มีศักยภาพที่เหมาะสมสำหรับการใช้ส่งข้อมูลปริมาณมหาศาลได้ เนื่องจากแสงเลเซอร์อยู่ในช่วงความถี่แสงที่ครอบคลุมพื้นที่ความถี่ใช้งานที่สูงยิ่ง ซึ่งตามหลักการแล้วจะทำให้มีขนาดของช่วงกว้างความถี่ใช้งานหรือที่เรียกว่าแบนด์วิดท์ และอัตราการส่งข้อมูลที่จะทำได้สูงมหาศาล แต่อย่างไรก็ตาม การนำความสามารถของเลเซอร์มาใช้ประโยชน์ในงานด้านการสื่อสารให้ได้ดีนั้น ต้องการการพัฒนาด้านการลดค่าสูญเสียของกำลังส่ง (low-loss) การพัฒนาเพื่อนำพาสัญญาณแสงไปในตัวกลางที่ใช้ให้ได้ผลดีด้วย

[3] ประวัติย่อ "การสื่อสารโลก" (A Brief History of Communications) ISBN 978-974-10-4920-2

[4] ข้อมูลเชิงเทคนิคเฉพาะของแสงเลเซอร์ที่ทำให้มีคุณลักษณะเหมาะสมกับการนำมาใช้งานด้านการสื่อสาร

จากนั้นต่อมา ถึงปีที่สำคัญ ค.ศ. 1966 ได้เกิดจุดเปลี่ยนอันเป็นปรากฏการณ์จากผลการพัฒนาที่ยิ่งใหญ่ในวงการสื่อสารเชิงแสง ...

ซึ่งได้เกิดขึ้นเมื่อ *ชาร์ล เกา (Charles Kuen Kao)* และ *จี เอ ฮอคแฮม (G. A. Hockham)* คิดค้นและนำเสนอเส้นใยนำแสงที่ทำมาจากแก้วเพื่อการใช้งานเป็นเสมือนช่องทางสำหรับการนำพาสัญญาณแสงไปได้ โดยได้ทำนายแนวโน้มของเทคโนโลยีนี้ด้วยว่าจะสามารถลดค่าการสูญเสียกำลังส่งลงได้ต่ำลงเหลือในอัตราที่ 20 เดซิเบลต่อกิโลเมตร (dB/km) การคาดการณ์ที่ต้องบันทึกไว้นี้เกิดขึ้นในขณะที่กำลังส่งของสัญญาณผ่านเส้นใยนำแสงยังมีการสูญเสียสูงอยู่ในระดับ 1,000

แล้วโลกการสื่อสารจึงเปลี่ยนไปอย่างมหาศาล ...

จดหมายเหตุ:

พ.ศ. 2503 (ค.ศ. 1960) ธีโอดอร์ ไมแมน (Theodore H. Maiman) ประดิษฐ์สิ่งที่ได้การยอมรับว่าเป็นเลเซอร์ชิ้นแรกของโลก

พ.ศ. 2552 (ค.ศ. 2009) ชาร์ล เกา (Charles Kuen Kao) ได้รับรางวัลโนเบลสาขาฟิสิกส์

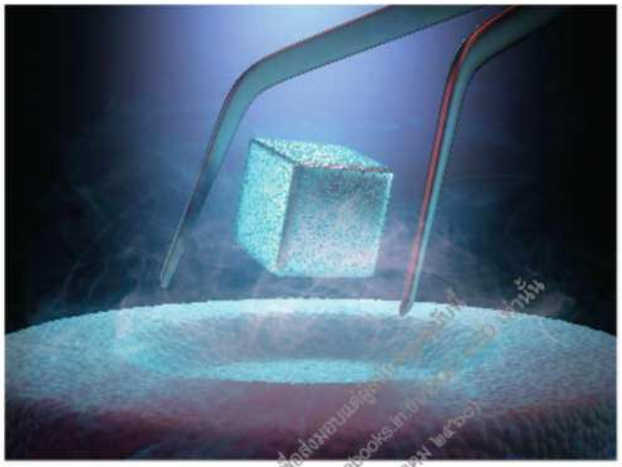
พ.ศ. 2553 (ค.ศ. 2010) ฉลองห้าสิบปีเลเซอร์ (Laser Fest) กับการสดุดีประโยชน์ที่มากมายในครึ่งศตวรรษที่ผ่านมา

4 เทอร์โมมิเตอร์ความเที่ยงตรงสูงมาก (Ultra-precise Thermometers)

เทอร์โมมิเตอร์วัดไข้ในโรงพยาบาล หากนำมาวัดอุณหภูมิเพื่อการทดลองทางวิทยาศาสตร์ที่ต่ำมากในระดับหนึ่งในร้อยองศาสัมบูรณ์ เจ้าแห่งปรอทก็คงไม่ทำงานเป็นแน่แล้ว จึงต้องมีการพัฒนาเทอร์โมมิเตอร์ที่ใช้วัดอุณหภูมิในระดับนั้นให้ได้และด้วยความแม่นยำที่สูงด้วยอีก ... ทำอย่างไร ?

การค้นหาและสร้างเทอร์โมมิเตอร์ความแม่นยำสูงมาก ๆ เพื่อการนั้น นักวิทยาศาสตร์พบว่า ปรากฏการณ์การทันเนลหรือการลอดอุโมงค์แบบควอนตัม (quantum tunneling) ของคลื่นอิเล็กตรอนสามารถทำให้เกิดสัญญาณทางไฟฟ้าที่ขึ้นกับอุณหภูมิ ซึ่งสามารถวัดและนำมาใช้เป็นเทอร์โมมิเตอร์ที่ใช้บอกค่าอุณหภูมิโดยมีระดับความเที่ยงมากได้

คงไม่ผิดที่จะบอกว่าจะไม่เจอควอนตัมเทอร์โมมิเตอร์ในร้านเครื่องมือทั่ว ๆ ไป จึงไกลตัวเรา ๆ ท่าน ๆ มากเชียว เพราะมันเป็นเครื่องมือวัดเฉพาะในห้องปฏิบัติการวิจัยสำหรับนักวิจัยที่ทำกับงานอุณหภูมิต่ำมาก และต่างก็หวังว่าจะได้ปรับปรุงความแม่นยำของเทอร์โมมิเตอร์แบบนี้ที่ใช้งานภายใต้สภาวะหลากหลายเพื่อพัฒนาสิ่งอื่นที่ยิ่งใหญ่ต่อไปได้ด้วยอีก แม้มีผู้ใช้น้อยแต่ผลที่ได้ช่างยิ่งใหญ่นัก



ควอนตัม กับการลอดอุโมงค์แบบควอนตัม (quantum tunneling) คือปรากฏการณ์ที่กระแสอิเล็กตรอนผ่านฉนวนไฟฟ้าหรือน้อยนั้นขึ้นกับอุณหภูมิ (การสั่นของโครงอะตอม) ที่บริเวณรอยต่อ จากความสัมพันธ์นี้ทำให้สามารถสร้างเทอร์โมมิเตอร์ที่มีความละเอียดสูงได้

จดหมายเหตุ

พ.ศ. 2558 (ค.ศ. 2015) นักวิจัยมหาวิทยาลัยนอตติงแฮม (Nottingham) นำเสนอผลงานที่สามารถวัดการเปลี่ยนแปลงอุณหภูมิในระดับที่ขนาดเล็กมาก (microscopic) หรือเข้าถึงไอโอในระดับเซลล์เลยทีเดียว

มาดูอีกสามเรื่องสำคัญต่อจากนี้ของการประยุกต์ใช้งานกลศาสตร์ควอนตัมในโลกความเป็นจริง ที่ดูยิ่งใหญ่มากและขึ้นกับสิ่งที่เล็กมากของศาสตร์แขนงนี้ โดยกำลังขับเคลื่อนจากอุปกรณ์เทียบวัดสู่ไอทีการสื่อสารกับการคำนวณที่รอดอย (มานานแสนนาน) ทั้งสามความยิ่งใหญ่กับการค้นพบของมนุษย์มีดังนี้...

3 ควอนตัมคอมพิวเตอร์ (Quantum Computers)

บทความที่ดีดีพิมพ์ในเดือนเมษายน ปี พ.ศ. 2508 ของกอร์ดอนมัวร์ซึ่งเป็นหนึ่งในผู้ก่อตั้งบริษัทอินเทลได้ทำนายเกี่ยวกับอนาคตของคอมพิวเตอร์ไว้ว่า ความหนาแน่นของทรานซิสเตอร์บนชิปคอมพิวเตอร์จะเพิ่มขึ้นสองเท่าทุก ๆ ช่วงประมาณเกือบสองปี โดยคำทำนายนี้เป็นจริงมายาวนานทว่า หากเมื่อถึงปี พ.ศ. 2563 ขนาดของทรานซิสเตอร์แต่ละตัวจะเล็กลงจนเข้าสู่ย่านที่กฎทางควอนตัมมีผลต่อการทำงานแทน หรือการพัฒนาจะทำให้เล็กลงไปแบบเดิม ๆ ท่วนองความกฎของมัวร์ต่อไปอีกไม่ไหวแล้วนั่นเอง

ขยับจากการต่อสู้กับกฎทางควอนตัมในโครงสร้างทรานซิสเตอร์ กำลังมีการพัฒนาควอนตัมคอมพิวเตอร์ที่ทำงานด้วยกฎทางควอนตัมแทน โดยจะมีข้อได้เปรียบจาก**การประมวลผลแบบขนาน (parallel processing)** ที่สามารถทำงานหลาย ๆ อย่างพร้อมกันแทนที่จะทำตามลำดับเหมือนในคอมพิวเตอร์ทั่วไป ผลที่ได้คือประสิทธิภาพที่สูงมาก (คาดการณ์กันไว้สุดฤทธิ์) แบบที่โลกไม่เคยเห็นมาก่อน

ก่อนที่จะมีควอนตัมคอมพิวเตอร์ให้ใช้งานจริงแบบแพร่หลายได้ นักวิทยาศาสตร์ทั่วโลกยังต้องพยายามแก้ปัญหาที่ท้าทายอยู่อีกหลายประการ แม้บริษัท D-Wave สัญชาติแคนาดาผู้ประกาศตัวว่าสร้างได้และขายให้กูเกิล นาซา และล็อกฮีดมาร์ตินไปแล้ว แต่ก็ถูกแย้งยันหัวชนฝาว่าเป็นควอนตัมแท้หรือเทียมกันแน่ มีข้อมูลมาถกเถียงกันมาก และไม่ได้ข้อยุติแม้ขายราคาสูงมากไปได้ก่อนหน้านั้น (2015)

ควอนตัมคอมพิวเตอร์ D-Wave

ควอนตัมคอมพิวเตอร์ที่สร้างโดยบริษัท D-Wave อาศัยปรากฏการณ์ควอนตัมแอนนีลลิ่ง (quantum annealing) หรือหลักการทำงานเพื่อการไล่หาผลคำตอบที่ดีที่สุด (optimization) สำหรับหน่วยประมวลผลสร้างโดยใช้ตัวนำไฟฟ้ายิ่งยวดจึงต้องทำงานที่อุณหภูมิต่ำมาก (ยังเป็นที่ถกเถียงเชิงวิชาการเรื่องประสิทธิภาพและอื่น ๆ (2015))

จดหมายเหตุ:

พ.ศ. 2520 (ค.ศ. 1977) เกิดการสร้างแบบจำลองและข้อสังเกตเกี่ยวกับลิจิก (Logic) แบบควอนตัม

พ.ศ. 2522 (ค.ศ. 1979) รอล์ฟ ลานเดาเออร์ และ ชาร์ลส์ เบนเนตต์ (Rolf Landauer & Charles Bennett) ศึกษาฟิสิกส์ของวงจรการคำนวณด้านการคำนวณที่ย้อนกลับได้ และพิสูจน์ว่าการลบข้อมูลเป็นกระบวนการย้อนกลับไม่ได้

พ.ศ. 2523 (ค.ศ. 1980) ยูริ แมนิน (Yuri Manin) เสนอการจำลองระบบเชิงควอนตัม (quantum simulation) เป็นภาษารัสเซีย

พ.ศ. 2524 (ค.ศ. 1981) ริชาร์ด ฟายน์แมน (Richard Feynman) เสนออีกการจำลองของระบบเชิงควอนตัมและอธิบายเพิ่มเติม

พ.ศ. 2528 (ค.ศ. 1985) เดวิด ดอยช์ (David Deutsch) เสนอเครื่องกลทูริงเชิงควอนตัม

พ.ศ. 2537 (ค.ศ. 1994) ปีเตอร์ ชอร์ (Peter Shor) ค้นพบกระบวนวิธีเชิงควอนตัมสำหรับการแยกตัวประกอบ

พ.ศ. 2542 (ค.ศ. 1999) ก่อตั้งบริษัท D-Wave ประเทศแคนาดา และประกาศการผลิตเครื่องควอนตัมคอมพิวเตอร์แรกเมื่อ 11 พฤษภาคม 2554

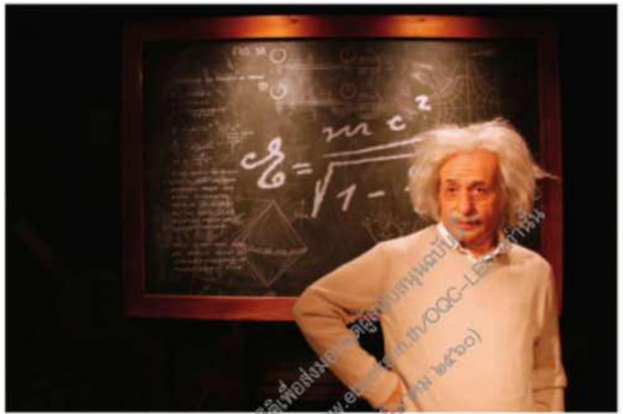
2 การสื่อสารแบบทันทีทันใด (Instantaneous Communication)

อาจคิดกันว่า โทรศัพท์เคลื่อนที่ อีเมล และการส่งข้อความสั้นผ่านแอปใด ๆ เป็นการสื่อสารแบบทันทีทันใด แต่จริง ๆ แล้ว ภาพ เสียง อีเมลและข้อความ ต้องใช้เวลาเล็กน้อยในการเดินทาง ซึ่งก็มิใช่ปัญหาใหญ่นักในการสื่อสารบนโลก หากอนาคตมนุษย์ต้องเดินทางในอวกาศ การสื่อสารด้วยความเร็วแม้ใกล้เคียงแสงก็อาจยังไม่เร็วพอ นักวิทยาศาสตร์คิดกันว่ากลศาสตร์ควอนตัมเป็นกุญแจที่จะใช้สร้างการสื่อสารแบบทันทีทันใดได้โดยไม่ขึ้นกับระยะห่างระหว่างกันในอวกาศ อาจแถมกลับมาใช้บนโลกได้เร็วกว่าอินเทอร์เน็ตความเร็วสูงที่มีอยู่ด้วยซ้ำ

กุญแจสำคัญในการสร้างการสื่อสารแบบทันทีทันใดนี้คือ **การพัวพันแบบควอนตัม (quantum entanglement)** ที่ไอน์สไตน์เรียกว่า "spooky action at a distance" (ถอดความเพื่อการเรียนการสอนคือ "การกระทำที่ระยะไกล" ส่วนแบบทั่วไปคือ "ภววิสัยที่ห่างไกล") นั่นคือ เมื่อสองอนุภาคพัวพันกันการเปลี่ยนแปลงที่เกิดขึ้นกับอนุภาคหนึ่งจะทำให้เกิดการเปลี่ยนแปลงแบบทันทีทันใดกับอีกอนุภาคหนึ่งซึ่งไม่ขึ้นกับระยะห่างระหว่างอนุภาคนั้น ๆ หากแทนการเปลี่ยนแปลงนั้นด้วยข้อมูลก็จะทำให้เกิดการสื่อสารแบบทันทีทันใดได้ ทั้งนี้ มีการทดลองและใช้งานการพัวพันควอนตัมในระยะทางสั้นเกิดขึ้นมากมายแล้วทั่วโลกแล้ว (รวมทั้งในประเทศไทย) ... แต่แบบไกลกันข้ามโลกนั้นคงยังไม่ต้องพูดถึง อีกนาน (ควรนานกว่าฟุตบอลไทยจะได้ไปบอลโลก !)

ควอนตัม อธิบายได้จากการทำงานของการพัวพันแบบควอนตัม (quantum entanglement) อันเป็นปรากฏการณ์ที่อาศัยความเชื่อมโยงกันของอนุภาคควอนตัมที่เกิดขึ้นในขณะสร้าง โดยหากใช้โฟตอน (แสง) สองหน่วยที่พัวพันกัน จะสามารถทราบสถานะของโฟตอนหน่วยใดได้จากการวัดสถานะของโฟตอนอีกหน่วยหนึ่งแทน เพราะสถานะของทั้งสองหน่วยที่พัวพันกันจะเหมือนกัน

ปรากฏการณ์ในธรรมชาติทั้งกรณีคู่แฝดและการเล่นจั๊กจี้ของเด็ก (Freeklabs) ถูกยกมาใช้เปรียบกับปรากฏการณ์ความพัวพันทางควอนตัมที่ยากมาก



จดหมายเหตุ

พ.ศ. 2478 (ค.ศ. 1935) อัลเบิร์ต ไอน์สไตน์ ร่วมกับ บอริส โพโดลสกี และนาธาน โรเซน (Einstein, Podolsky, Rosen) เสนอการทดลองทางความคิดเกี่ยวกับ ความพัวพันเชิงควอนตัมเรียกว่า 'EPR paradox' ซึ่งขัดกับทฤษฎีการมีอยู่จริง ณ ตำแหน่งใด ๆ (local realism) ของกลศาสตร์ยุคเดิม

พ.ศ. 2525 (ค.ศ. 1982) เดนนิส ดีคส์ (Dennis Dieks) พิสูจน์ทฤษฎีการไม่สามารถคัดลอกสถานะควอนตัมได้ (No Cloning Theorem) และพิสูจน์ว่าความพัวพันทางควอนตัมไม่ได้ทำให้เกิดการสื่อสารที่ความเร็วเหนือแสง

พ.ศ. 2534 (ค.ศ. 1991) อาเทอร์ เอ็เคิร์ต (Artur Ekert) เสนอวิธีประยุกต์ใช้ความพัวพันเชิงควอนตัมมาช่วยในการกระจายกุญแจรหัสลับ (Entanglement-based QKD) กับการสื่อสาร

หมายเหตุ: *การสื่อสารด้วยวิธีพัวพันเชิงควอนตัม ฝ่ายส่ง (Alice) มีบิตข้อมูลอะไร ฝ่ายรับ (Bob) ก็จะมีข้อมูลบิตนั้นในทันที*

1 การส่งถ่าย การเทเลพอร์ต (Teleportation)

การนำกลศาสตร์ควอนตัมมาประยุกต์ใช้งานของมนุษย์กับเรื่องที่น่าสนใจสูงคงหนีไม่พ้นสิ่งที่ต้องแปลกใหม่ ไม่คุ้นเคยมาก่อนและแน่นอนว่าเกินขอบเขตที่เทคโนโลยีร่วมสมัยจะมีรองรับได้ทั่วไป ทั้งไม่เคยได้เห็นหรือได้ใช้งานมาก่อน ลำดับแปลกสุด ๆ จากสิบเรื่องที่โยงมาถึง **การส่งถ่าย การเทเลพอร์ต (Teleportation)** หรืออีกนัยกับ "การเคลื่อนย้าย" ที่ไม่วายคิดไปถึงมวลสาร

ประโยชน์จากกลศาสตร์ควอนตัมที่อยากจัดให้ เป็นสิ่งยิ่งใหญ่อันเป็นความหวังของนักวิทยาศาสตร์ (และนักเขียนนิยายวิทยาศาสตร์) รวมทั้งหนังดังสตาร์เทรค (Star Trek) ที่เล่นมุกการส่งถ่ายนี้ แล้วเจ้าสิ่งนี้ส่งไปที่นั่น สิ่งนั้นส่งมาที่นี่ มันคืออะไร ?

ควอนตัมอธิบายการทำงานการส่งถ่าย (teleportation) จากกฎทางควอนตัมฟิสิกส์ที่สามารถทราบสถานะของอนุภาคควอนตัมหนึ่งได้โดยการวัดสถานะของอีกอนุภาคหนึ่งที่พัวพันกันอยู่ ทำให้นักวิทยาศาสตร์ขยายแนวคิดไปสู่การส่งถ่าย ซึ่งการทดลองที่สำเร็จแล้วเป็นการส่งถ่ายข้อมูล

การทดลองส่งถ่ายหรือเทเลพอร์ตอิเล็กตรอนในเพชร
(www.tudelft.nl)

อาจเคยเห็นหรือได้ยินเรื่องราวของการเคลื่อนย้ายมวลสาร "แว็บไปแว็บมา" ก็จากฉากในภาพยนตร์หรือนิยายวิทยาศาสตร์ เกี่ยวกับการส่งถ่ายสิ่งใดจากสถานที่แห่งหนึ่งไปอีกสถานที่ใหม่ หากเป็นภาพยนตร์เรื่องสตาร์เทรคก็จะพอคุ้นเคย แต่ในชีวิตจริงทำได้หรือ ? อย่างนั้นมาเริ่มจากหลักกิโลหรือหลักไมล์ของความก้าวหน้าอันแปลกประหลาดนี้กันที่..

จุดเริ่มต้น

ปี ค.ศ. 1993 (พ.ศ. 2536) ทีมนักวิจัยหกคนของบริษัทไอบีเอ็มได้พิสูจน์ทางทฤษฎีว่า การเทเลพอร์ตวัตถุทั้งชิ้นเป็นเรื่องที่ทำได้ โดยวัตถุเริ่มต้นต้องถูกทำลายในกระบวนการนี้ ทั้งนี้เพราะว่าการคัดลอกคุณสมบัติของวัตถุเริ่มต้นในระดับควอนตัมจะเปลี่ยนคุณสมบัติของมัน โลกจึงรู้กันว่าการเทเลพอร์ตวัตถุนั้นทำได้โดยมิได้ขัดกับหลักการใด ๆ ทางฟิสิกส์ เว้นหลักการ *"ส่งโดยไม่ได้ส่งหรือไม่ต้องมีพาหะหรือยานพาหนะนำส่ง จึงยังเกิดขึ้น"* ส่วนทำได้จริงไหมไปว่ากันต่อ

ปีค.ศ. 1998 (พ.ศ. 2541) นักวิจัยจากสถาบันเทคโนโลยีแคลิฟอร์เนีย (Caltech) ได้ผลทดลองอันสามารถเทเลพอร์ตข้อมูลด้วยแสงโดยใช้การพัวพันแบบควอนตัมบนฐานวางอุปกรณ์แม้มีระยะเพียงเมตรเดียว ความก้าวหน้าของทีมวิจัยนี้เป็นการพัฒนาที่ทำให้ยอมรับกันว่า การเทเลพอร์ตสามารถสร้างให้เกิดขึ้นจริงได้แล้วบนโลก และต่อมาอีกสิบปี ..

ปี ค.ศ. 2008 (พ.ศ. 2551) มหาวิทยาลัยแมริแลนด์ (Maryland) เล่นกับข่าวสารระหว่างอะตอมได้และส่งถ่ายได้ระยะ 1 เมตร เป็นอีกครั้งที่โลกได้รับทราบการเปลี่ยนแปลงความรู้ที่สะสมกันมา ว่าอะไรที่กำลังเกิดขึ้นในอนาคตข้างหน้าจะน่าตื่นเต้นเพียงใด

มีใช่แค่ฟากตะวันตก ความก้าวหน้าในส่วนของกลุ่มงานปรมาจารย์ชาวจีน ณ เหอเฟย เจียน เหวย พั่น (Jian-Wei Pan) ได้นำแสงที่มีความพัวพันมาทำการเทเลพอร์ตในปี **ค.ศ. 2010** (พ.ศ. 2553) ได้ระยะทางถึง 16 กิโลเมตร

สองปีต่อมาเมื่อคู่หูลูกศิษย์กับอาจารย์บันลือโลก (เจียน เหวย พัน กับ อันตัน ไซลิงเงอร์ - Anton Zeilinger) ต่างก็นำเสนอในปีเดียวกัน ระยะ 97 กิโลเมตรด้วยแสงพัวพันผ่านอากาศเกิดที่ประเทศจีน และเทคนิคคล้ายกันแต่ได้ระยะถึง 143 กิโลเมตรก็ตามมาด้วยการข้ามเกาะที่สเปนของกลุ่มเวียนนาใช่แล้ว *"ส่งโดยไม่ต้องส่งอะไรไป"* มันไปได้ไกลจริง ๆ จนมาถึง...

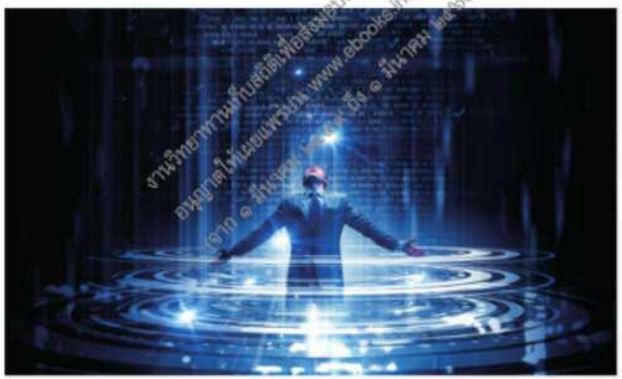
ค.ศ. 2014 กับประเทศทีมอันดับสามฟุตบอลโลกจากมหาวิทยาลัยเทคโนโลยีเดลฟท์ (Delft University of Technology) ที่ทำระยะเพียง 10 ฟุต ระหว่างมุมห้องเป็นการใช้อิเล็กตรอนในเพชร แต่ที่ทำให้ตะลึงกันก็คือความแม่นยำถูกต้องสูงมากอันต่างจากของมหาวิทยาลัยแมรีแลนด์หกปีก่อนหน้าที่ทำสำเร็จได้สักเพียงครั้งก็มาจากความพยายามนับร้อยล้านครั้ง คราวนี้จึงทำได้แบบมั่นอกมั่นใจกันแล้ว

แสงหรือโฟตอนก็ส่งถ่ายได้แล้ว อะตอมก็ใช่ อิเล็กตรอนก็ไป แต่ระดับโมเลกุลความก้าวหน้าของโลกยังไปไม่ถึง เอ่ ! พอมาถึงตรงนี้ก็กำลังคิดจินตนาการไปถึงการส่งถ่ายมวลกันอยู่ใช่ไหม ?

หลายฝ่ายได้ทิ้งท้ายเอาไว้ด้วยว่า "ไม่รู้ว่าผู้คนยุคนี้ (2016) จะอยู่ถึงวันที่ได้เห็นมนุษย์เทเลพอร์ตตัวเองหรือไม่ ?"

ระหว่างการรับรู้เรื่องแปลกเหล่านี้ก็อย่าลืม "กาลามสูตร"
คืออย่าเชื่อง่ายนักหากยังมิได้พิสูจน์ทราบด้วยตนเองกับวิทยาศาสตร์
ที่มีความรู้และข้อมูลมากมายให้ศึกษา

... มาเริ่มกันเลย อีกนับไม่ถ้วนของการประยุกต์ใช้กลศาสตร์ควอนตัม
มีรออยู่ข้างหน้า



แหล่งข้อมูล:

Q-Thai.org และคอลัมน์ไอที OQC/LED เดลินิวส์ออนไลน์
(www.dailynews.co.th/article/OQC_slash_LED)

หน่วยงานในประเทศที่เกี่ยวข้อง (กลศาสตร์ควอนตัมด้านสารสนเทศ):

ดร.วรานนท์ อนุกูล
ห้องปฏิบัติการทัศนศาสตร์เชิงอะตอมควอนตัม
ศูนย์ความเป็นเลิศด้านฟิสิกส์/ ภาควิชาฟิสิกส์และวัสดุศาสตร์
มหาวิทยาลัยเชียงใหม่
Web: qaocmu.org
(เล่นกับอะตอมและแสง)

ดร.สุวิทย์ กิระวิทยา
ห้องปฏิบัติการเทคโนโลยีเชิงแสงขั้นสูง
(Advanced Optical Technology Lab.)
ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์ มหาวิทยาลัยนเรศวร
Web: www.ecpe.nu.ac.th/suwit
(เล่นกับแสงและการสื่อสาร)

กลุ่มสารสนเทศเชิงควอนตัมไทย
สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ
(ECTI) (Thai Quantum Information Forum)
Web: Q-Thai.org
(ช่วยเล่นทุกอย่าง)

ภาคผนวก ข
สื่อเผยแพร่ “ควอนตัมกับการสื่อสาร คืออะไร เพื่ออะไร”

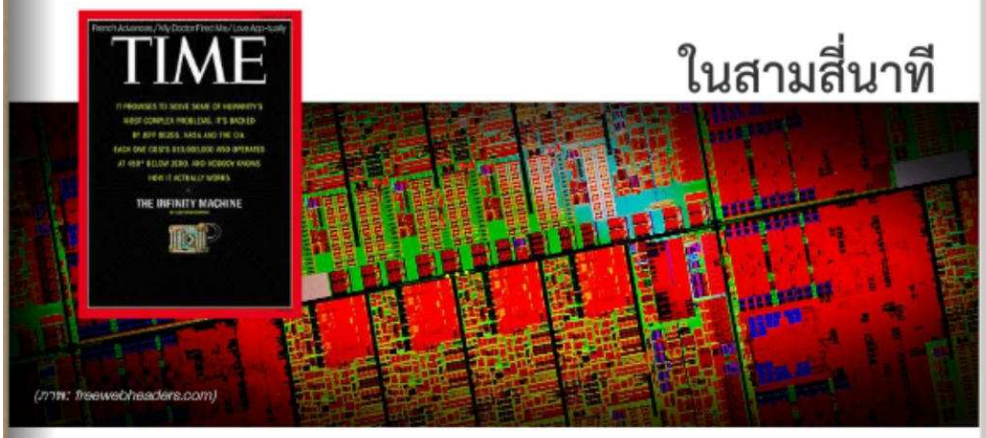
หมายเหตุ ผู้จัดทำได้มีการเปลี่ยนชื่อเอกสารนี้ก่อนการเผยแพร่เพื่อให้เป็นที่น่าสนใจมากขึ้น

ECTI Association

IEEE COMMUNICATIONS SOCIETY Thailand Chapter

10 Q&A : QuantumIT (part I)

ตอบคำถาม "ไอทีควอนตัม" (๑)



ในสามสี่นาที

รหัสลับเชิงควอนตัมคือ ? ประโยชน์?

คอมพิวเตอร์แบบควอนตัมดี ...

หรือหลอก ?

วิชาการเพียงนิดเดียว... เดี๋ยวเข้าใจ

๑. ควอนตัม (quantum) ... สั้น ๆ นะ มันคืออะไร ?

(www.ebooks.in.th/ebook/38617/)

ปริมาณทางกายภาพที่เล็กที่สุดที่ไม่สามารถแบ่งแยกได้อีก ... ควอนตัมกำเนิดจากแนวคิดที่ใช้อธิบายปรากฏการณ์ที่เกิดขึ้นกับอนุภาคเล็ก ๆ เช่น อิเล็กตรอน อะตอม โมเลกุล แต่ขัดแย้งกับสามัญสำนึกของมนุษย์โดยทั่วไป (รับรู้ด้วยประสาทสัมผัสพื้นฐานทั้งห้าโดยตรงไม่ได้) ทฤษฎีนี้ถูกพัฒนาเป็นทางการ ค.ศ. 1925 ถูกนำมาใช้เป็นพื้นฐานในการสร้างเทคโนโลยีสมัยใหม่ต่อมามากมายทั้งการสื่อสาร การคำนวณ การเทียบ(มาตร)วัด จนถึง การส่งถ่าย (teleportation) แห่งโลกอนาคต ฯลฯ

“๑๐ คำถามตอบ - กับควอนตัม - ด้านไอที”

๒. ควอนตัมคอมพิวเตอร์มาแล้ว ... เป็นภัยต่อรหัสลับไหม ?

กูเกิล (Google) ประกาศว่าควอนตัมคอมพิวเตอร์ที่สำเร็จแล้ว เร็วกว่าคอมพิวเตอร์ทั่วไป 100 ล้านเท่า แต่ยังไม่เป็นภัยต่อความปลอดภัยทางอินเทอร์เน็ต แม้ว่าหน่วยประมวลผล Dwave 2X ที่กูเกิลอ้างนั้นสร้างโดยใช้หลักการคล้ายคลึงกับควอนตัมคอมพิวเตอร์ แต่ยังใช้ได้**เฉพาะบางปัญหา**เท่านั้น โชคดีที่โจทย์การทำลายระบบความปลอดภัยอินเทอร์เน็ตที่กังวล ... ยังไม่ได้รวมอยู่ในนั้น

(quantum safe cryptography คือ วิธีที่รหัสในระบบอินเทอร์เน็ตจะใช้สู้กับควอนตัมคอมฯ ในอนาคต มาเตรียมพร้อมกัน)

เร็วกว่าร้อย**ล้าน**เท่า

..กว่าสี่ร้อย**ล้าน**บาท

๓. รหัสลับควอนตัมคืออะไร ?

การสื่อสารปลอดภัยเมื่อเข้ารหัสลับแล้วจะไม่มีใครแกะถอดได้ โดยกุญแจรหัสลับส่งไปกับการอาศัยคุณสมบัติทางควอนตัมของโฟตอน (photon) หรือหน่วยเล็กสุดของ "แสง" ทั้งนี้ *"ไม่มีใครสามารถคัดลอกสถานะทางควอนตัมของโฟตอนได้โดยไม่ไปกระทบหรือเปลี่ยนแปลงสถานะดั้งเดิม"* ดังนั้น หากมีใครมายุ่งจะทำให้ระบบสื่อสารรู้ตัว จึงมั่นใจได้ว่าการสื่อสารด้วยวิทยาการนี้ปลอดภัยสูงสุด แต่ยังเหมาะเพียงกับการสื่อสารเฉพาะจุดต่อจุด (point-to-point)

"ใครขโมยกุญแจก็รู้ เมื่อรู้ก็เลิก ... ปลอดภัย"

(facebook.com/QuantumCryptoThailand)

๔. รหัสลับทั่วไปก็มี แล้วทำไมต้องใช้ควอนตัมล่ะ ... มีขายแล้วหรือ ?

เพราะเป็นระบบที่สร้างกุญแจรหัสลับใช้ครั้งเดียวแล้วทิ้ง (one time pad : OTP) จึงปลอดภัย 100% ... มีใช้มานานเกินสิบปีแล้ว มีขายจากทั้งยุโรป สหรัฐฯ จีน เกาหลีใต้

ราคาชุดสื่อสารจุดต่อจุดละเกือบ**แปดล้าน**บาท

FRAUD – SCANDAL – FAKE !

๕. แล้ว “ครีมหน้าเด้งยี่ห้อควอนตัม กระติกน้ำสะสมพลังงานลึกลับควอนตัม กิจกรรมกายภาพช่วยรักษาผู้ป่วยด้วยเหรียญและเครื่องตรวจร่างกายชื่อควอนตัม”เกี่ยวเรื่องลับ ๆ ที่ว่านั้นไหม ?

... ไม่เกี่ยว !

ไม่ใช่ ไม่เป็นวิทยาศาสตร์

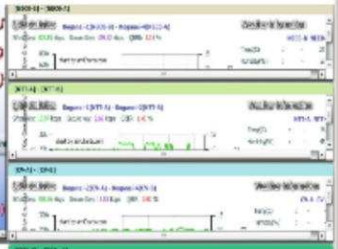
“สารพันเรื่องชวนหัว – ตั้งชื่อสินค้าว่าควอนตัม”

เมื่อใดที่... กลศาสตร์ควอนตัมถูกอ้างอิงหรือใช้เป็นชื่อสินค้า กิจกรรมทางสังคม วัฒนธรรมหรือประเพณีอันมีความสวยงามทางสังคมหรือจิตวิญญาณ กลายเป็นความเชื่อไปแล้วเหมือนทั้ง GT200 บั้งไฟพญานาค ฯลฯ บัดนั้น ก็ต้องกลับมาเริ่มต้นวิ่งไล่แก้ไขความเข้าใจผิดที่ยากมากกว่าการปูพื้นฐานวิทยาศาสตร์ที่ถูกต้อง

ตั้งแต่แรก !

Worldwide Developments

๖. รหัสลับเชิงควอนตัม ทั่วโลกเขาทำอะไรกันอยู่ ?



ยุโรปประกาศการปฏิวัติควอนตัมยุคที่สอง โครงการพันล้านยูโรระยะเวลาสิบปี **ญี่ปุ่น**สร้างเครือข่ายโตเกียวสาธิตและทดสอบตลอดวัน **จีน**เปิดเครือข่ายปักกิ่ง – เซี่ยงไฮ้ และขึ้นดาวเทียมทดลองแล้ว **เกาหลีใต้**เปิดโครงการสองปีผลิตขาย **สิงคโปร์**สามปีลงทุนมากกว่าพันล้านบาทเพื่อสร้างบุคลากร สหรัฐอเมริกานำหน้าจำนวน**สิทธิบัตร**มากสุดในโลก จีนตามติดแต่มีผลผลิตด้าน**วิชาการ**สูงที่สุด ฯลฯ ... โลกได้มีพัฒนาการมากว่าสามทศวรรษ *(แล้ว ประเทศไทยอยู่ระดับไหน ?)*

๗. มีข่าวแปลกเรื่องลึกล้ำ ...

งานวิชาการของนักวิจัย นักวิทยาศาสตร์แนวประหลาดในหลากสาขา ทั้งวงจรไฟฟ้าควอนตัมตามใจนึก (quantum cost) เก็บกุญแจรหัสควอนตัมไว้ใช้คำนวณงานภายหลัง (quantum key) โด่งดังกระทั่งควอนตัมกระโดดขึ้นเครือข่ายโทรศัพท์เคลื่อนที่ (quantum key on mobile) มีจริงหรือ ...วิทย์เทคโนฯเทียมแบบนี้เมืองไทยมีไหม ? ..... **มี !**

จากเหตุพื้นบ้านความสับสนปนวิทยาการแปลกปลอมในอดีตมากสาขา เป็นปัญหาสังคมพื้นเดิมอยู่แล้วทั้ง จีที (GT200) ไฟจุดติดเองได้ในบ้าน ฯลฯ การมาของเทคโนโลยีใหม่ด้านไอทีควอนตัมที่ทรงพลังก็อาจเหนี่ยวนำให้เกิดการหลงทิศผิดทางมากขึ้นได้อีก โดยเฉพาะหากนักวิชาการนำทางสังคมไปในเส้นทางสีเทา ๆ เหล่านั้น เช่น

ก) การทดลองที่ระบุว่าประดิษฐ์สร้างงานควอนตัมแสงความเร็วสูงได้ แต่ปฏิบัติด้วยอุปกรณ์ความเร็วต่ำมาก ไม่ครบองค์ประกอบสร้างได้จริง ทว่า ตีพิมพ์ผลจากจินตนาการ นำเสนอด้วยภาพนิ่ง และไม่มีใครสามารถขอเยี่ยมชมทัศนศึกษาสิ่งประดิษฐ์นั้นได้

ข) งานประยุกต์อุปกรณ์สร้างเครือข่ายสื่อสารปกติ *"มิได้ใช้สถานะทางควอนตัมฟิสิกส์"* ต่างจากเครือข่ายควอนตัมปกติทั่วไป (quantum network) แต่มีข่าวประชาสัมพันธ์ผลงานเต็มพิกัดว่า *"การประยุกต์ใช้รหัสลับที่รับประกันด้วยกฎทางฟิสิกส์ ว่าด้วยทฤษฎีห้ามคัดลอกมาช่วยเพิ่มความปลอดภัยบนระบบ !"*

ค) งานจินตนาปราศจากหลักวิศวกรรมโทรคมนาคมว่าโลกสื่อสารไร้สายอนาคตเป็นดังที่ปรารถนาเอง เช่น ระบบโทรศัพท์เคลื่อนที่มีคุณสมบัติควอนตัมแสงไปสร้างอยู่ได้ทั้งบนตัวระบบและลูกข่าย

... ระบุว่าสาธิตได้ด้วยแล้ว

เรื่องแปลกที่

"เกิดขึ้นจริง"

ในเมืองไทย ..

มาช่วยกัน
แก้ไขโดยด่วน !

๘. รหัสลับควอนตัมถูกแฮก (hacking) ได้แล้ว แสดงว่าไม่ปลอดภัยจริง ?

เปล่า ... เป็นเพียงเรื่องช่องว่างการสื่อสารระหว่างนักฟิสิกส์กับวิศวกรสื่อสารเท่านั้น

คำจัดความ quantum hacking คือโฆษณาแฝง เป็นบ่อดักให้หลงสนใจบริษัทขายเครื่องรหัสลับควอนตัม และกรณี**นักวิจัยทำงานเด่นด้านตัวรับแสง** แต่กลับตั้งชื่องานให้เอียงเข้ามาพ่วงชื่อเสียงของรหัสลับควอนตัมเรื่องการแฮก เป็นทั้งการ**ลองวิชา อุดมคติและความไม่สมบูรณ์ของอุปกรณ์** แต่มาพ่วงใช้ชื่อจากโลกไอทีเติมจนป่วน **ที่สำคัญมีผู้บริหารวิทย์และเทคโนฯไทยหลุดไหลไปกับเพียงหัวข้อข่าวนี้ด้วยแล้วแบบ ...**

... "ไม่ชัด แต่เชื่อ แล้วรีบแชร์" แย่เลย ...

๙. ประเทศไทยทำอะไรมาแล้วบ้างกับรหัสลับเชิงควอนตัม ?

๑ ๒ ๓ ๔ ... มีสี่หัวข้อใหญ่ที่ควรลองศึกษาดูเองดีกว่า ณ facebook.com/QuantumCryptoThailand และ Q-Thai.Org ... ขอเชิญ

๑๐. ประเทศไทยควรตั้งเป้าหมายอย่างไรในอนาคต ?

๑.**"เป็นผู้ซื้ออย่างฉลาด"** ให้ได้ก่อนเพื่อเป็นบันไดขั้นแรกติดตามความรู้สู่อนาคต ... ๒. **"เป็นผู้ฉลาดศึกษา"**ช่วยกันตั้งข้อสังเกต ศึกษาหาคำตอบและแบ่งปันให้ความรู้จริงปรากฏ ของเทียมควรลดจางหายไม่ให้กระทบต่อสังคมฐานความรู้วิทยาศาสตร์ ช่วยกันหาทางป้องกัน แม้กระทั่งกับวงการวิชาการ (ควอนตัมของเทียม) ก็ควรช่วยกันเร่งแก้ไข ปรับปรุงตนเอง !

พบกับ ... ตอบคำถาม"ไอทีควอนตัม" (๒)

เมืองไทยกับบันได สี่ขั้นสู่การเป็นผู้ซื้ออย่างฉลาด

สร้าง **"ภูมิคุ้มกันตนเอง"** ความหวังกับคนรุ่นใหม่ ... นักเรียนไอทีควอนตัมไทย

(**ภาพ:** เครื่อง *Dwave: เปรียบคอมพิวเตอร์ทั่วไปในปัจจุบันเป็นเครื่องคิดเลข (บวก ลบ คูณ หารทีละอย่าง) แต่ควอนตัมคอมพิวเตอร์เสมือนเครื่องคิดเลขที่สามารถบวก ลบ คูณ หาร ได้**ในเวลาเดียวกัน**โดยใช้หน่วยประมวลผลตัวเดียว ... ฤๅ จะเป็น "อภินิหาร" พัฒนาการเทคโนฯ ของมนุษย์บนพื้นฐานกลศาสตร์ควอนตัม !)*

(version 1.0: August 2016 ใช้เพื่อการศึกษาและสื่อสารสาธารณะ)

กลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย (Q-Thai.Org)

Thai Quantum Information Forum (Q-Thai Forum)

โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร
(กทปส – กสทช) *(cut & print : K Satjen)*

ภาคผนวก ค
รายงานการสำรวจสถานะทรัพย์สินทางปัญญาของเทคโนโลยีและผลิตภัณฑ์ของทั่วโลก

ECTI Association

IEEE COMMUNICATIONS SOCIETY Thailand Chapter

ชุดหนังสือสารสนเทศเชิงควอนตัม ๔/๒

ชุดหนังสือสารสนเทศเชิงควอนตัม ๔/๒
ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)
Survey of Intellectual Properties on Quantum Cryptography (2016)

"หนังสือที่กลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทยภายใต้การประสานงานของดร.เกียรติศักดิ์ ได้รวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับผลงานเชิงวิชาการและทรัพย์สินทางปัญญาของวิทยาการด้านรหัสลับเชิงควอนตัมจากฐานข้อมูลที่น่าเชื่อถือของโลก แสดงให้เห็นถึงศักยภาพและความก้าวหน้าของแต่ละประเทศ (รวมทั้งประเทศไทย) ในการวิจัยและพัฒนาเทคโนโลยีเปิดแดนเรื่องนี้

ผมอยากแนะนำให้ผู้บริหารนโยบายวิทยาศาสตร์และเทคโนโลยีของประเทศและนักเรียนพสวท.ได้อ่านหนังสือเล่มนี้ทุกคน"

ศ.(เกียรติคุณ) ดร. กิรณ์ติมน์ วิลัยทอง
ศูนย์ความเป็นเลิศด้านฟิสิกส์

Free Distribution

9 786164 138469
ISBN 978-616-413-846-9

จัดพิมพ์เป็นวิทยาทาน

Optical & Quantum Communications

มูลค่าการจัดพิมพ์ ๑๙๐ บาท

ทรัพย์สินทางปัญญา

INTELLECTUAL PROPERTY

เทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)

Q-Thai Forum

ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)
Survey of Intellectual Properties on Quantum Cryptography (2016)

โดย

กลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย
Thai Quantum Information Forum
(Q-Thai Forum)

สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI)
และ
ชมรมไฟฟ้าสื่อสาร (IEEE Communications Society Thailand chapter)
สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE)

นำเสนอร่วม
โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม:
การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร มหาวิทยาลัยนเรศวร
สนับสนุนโดย กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์
และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส - กสทช)

ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)
Survey of Intellectual Properties on Quantum Cryptography (2016)
(จัดพิมพ์เป็นวิทยาทาน)

ข้อมูลและทีม รังสิมา เพ็ชรเม็ดใหญ่ ปรมินทร์ แสงวงษ์งาม จุฑาเพชร เวชรังษี
จันทิรา ปัญญา จิรวัฒน์ ตั้งปณิธานนท์ สุวิทย์ กิระวิทยา
ที่ปรึกษา สุทัศน์ ยกส้าน Gaby Lenhart
เรียบเรียง เกียรติศักดิ์ ศรีพิมานวัฒน์ *(บรรณาธิการ)*
สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI) และชมรมไฟฟ้าสื่อสาร สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE)
ขอขอบคุณ มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร และกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการ โทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส. - กสทช)
พิมพ์ครั้งที่ 1: กรกฎาคม 2559 *(99 เล่ม)*

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
เกียรติศักดิ์ ศรีพิมานวัฒน์.
ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙).– กรุงเทพฯ: จรัลสนิทวงศ์การพิมพ์, 2559.
81 หน้า.

1. ทรัพย์สินทางปัญญา. I. ชื่อเรื่อง.
346.048
ISBN 978-616-413-846-9

ข้อมูลเพิ่มเติม: *www.facebook.com/QuantumCryptoThailand และ Q-Thai.Org*
ข้อมูลร่วมและจัดพิมพ์พร้อมกับ : *"เทคโนโลยีการส่องสว่างข้อมูลกับทรัพย์สินทางปัญญา (พ.ศ.๒๕๕๙)" (ISBN 978-616-413-843-8)*
โครงการร่วมกิจกรรมปีแห่งแสงสากล (IYL2015) : *www.light2015.org*

คำนิยม

ผมรู้จัก ดร. เกียรติศักดิ์ มานานนับสิบปี ได้พบกันครั้งแรก ๆ ในช่วงปี พ.ศ. ๒๕๒๘ – ๒๕๓๑ ที่มหาวิทยาลัยเชียงใหม่ และหลังจากนั้นก็ทราบว่า ดร.เกียรติศักดิ์ได้เข้าทำงานที่ศูนย์วิจัยแห่งชาติทางด้านที่เกี่ยวข้องกับโทรคมนาคม การทำงานคนละสายงานทำให้แทบไม่ได้พบปะกันเลย เราทั้งสองคนไม่เคยคิดมาก่อนว่า เทคโนโลยีอุบัติใหม่เชิงควอนตัมจะทำให้ได้มีโอกาสมาพบกันในแวดวงวิชาการที่ท้าทายอีกครั้งหนึ่ง

อาจกล่าวได้ว่า การปฏิวัติควอนตัมยุคแรกได้เริ่มขึ้นหลังสงครามโลกครั้งที่สอง เมื่อกลศาสตร์ควอนตัมเป็นพื้นฐานของเทคโนโลยีที่นักฟิสิกส์และวิศวกรใช้ในการพัฒนาทรานซิสเตอร์และเลเซอร์ ขณะนี้การปฏิวัติควอนตัมยุคที่สองได้มาถึงแล้ว และกลศาสตร์ควอนตัมก็ยังมีบทบาทสำคัญในการศึกษาวิจัยทางสารสนเทศเชิงควอนตัม ซึ่งมีเทคโนโลยีการคำนวณและวิทยาการรหัสลับเชิงควอนตัมเป็นสองเทคโนโลยีหลัก

ดร. เกียรติศักดิ์ เป็นนักวิชาการรุ่นแรก ๆ ที่ได้ตระหนักถึงความสำคัญของเทคโนโลยีฐานควอนตัมที่มีต่อวงการสารสนเทศ และได้บุกเบิกการศึกษาวิจัยเทคโนโลยีอุบัติใหม่นี้ รวมทั้งได้สนับสนุนการจัดตั้งห้องปฏิบัติการวิจัยตามมหาวิทยาลัยในเครือข่ายเพื่อสร้างพื้นฐานและบรรยากาศทางวิชาการของประเทศ จึงเป็นที่มาของกลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย

ดร. เกียรติศักดิ์ และกลุ่มฯ ได้เล่าเรื่องราวด้านวิทยาการใหม่เชิงควอนตัมในรูปของเอกสารรวมเล่มมาแล้วสี่ชิ้น ชิ้นที่สี่เป็นเรื่องเกี่ยวกับการพัฒนาวิทยาการด้านรหัสลับเชิงควอนตัม ซึ่งได้พิมพ์ขึ้นเมื่อปี พ.ศ. ๒๕๕๗ ทำให้เราได้ทราบถึงวิวัฒนาการของวิทยาการด้านนี้จากอดีตถึงปัจจุบัน

หนังสือทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม เป็นหนังสือที่กลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทยภายใต้การประสานงานของ ดร. เกียรติศักดิ์ ได้รวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับผลงานเชิงวิชาการ และทรัพย์สินทางปัญญาของวิทยาการด้านรหัสลับเชิงควอนตัม จากฐานข้อมูลที่มีความน่าเชื่อถือของโลก แสดงให้เห็นถึงศักยภาพและความก้าวหน้าของแต่ละประเทศ (รวมทั้งประเทศไทย) ในการวิจัยและพัฒนาเทคโนโลยีเปิดแดนเรื่องนี้

ผมอยากแนะนำให้ผู้บริหารนโยบายวิทยาศาสตร์และเทคโนโลยีของประเทศและนักเรียน พสวท. ได้อ่านหนังสือเล่มนี้ทุกคน

ศ.(เกียรติคุณ) ดร. ถิรพัฒน์ วิลัยทอง
ศูนย์ความเป็นเลิศด้านฟิสิกส์

คำนำ

และข้อบ่งใช้ (disclaimer)

"ไอทีควอนตัม" คำนี้ใช้เป็นทางการครั้งแรกกับการนำเสนองานความรู้ทั่วไปเรื่อง "รูป รส กลิ่น เสียง สัมผัส" ไอทีควอนตัม (1) (พ.ศ.2557) โดยมีการคำนวณและวิทยาการรหัสลับเชิงควอนตัมเป็นสองเทคโนโลยีการประยุกต์หลัก ระยะเวลาต่อเนื่องมาปรากฏข่าวความก้าวหน้ามากขึ้นทั่วโลก ทั้งด้านควอนตัมคอมพิวเตอร์รุ่นใหม่ของบริษัท D-Wave หรือการที่ไอบีเอ็ม (IBM) ได้เปิดระบบ 5 คิวบิตให้ทดสอบผ่านคลาวด์ ส่วนงานด้านรหัสลับควอนตัมนั้น บริษัทกูเกิล เริ่มงานทดสอบกับระบบปฏิบัติการโครม (Chrome - quantum safe cryptography) เพื่อป้องกันการสื่อสารปัจจุบันต่อการแกะรหัสของควอนตัมคอมพิวเตอร์ในอนาคตและข่าวบริษัท iDQuantique ออกสินค้ารุ่นใหม่ความเร็วการเข้ารหัสลับสูงขึ้น เป็นต้น รวมทั้งหลายประเทศในยุโรปเปิดตัวงานวิจัยและพัฒนาด้านไอทีควอนตัมเป็นวาระแห่งชาติด้วย ทั้งหมดนี้ บ่งบอกการเปลี่ยนผ่านเทคโนโลยีครั้งใหญ่ของโลก หรือที่บุคลากรในยุโรปเรียกกันว่า**"การปฏิวัติควอนตัมยุคที่สอง"** (second quantum revolution) อันได้มาถึงแล้ว

ขณะที่ประเทศไทย ยังคงห่างไกลมากขึ้นจากวิทยาการสาขาใหม่ไอทีควอนตัมทั้งสองด้านหลักนั้น แม้ในอดีตได้เคยมีการเริ่มโครงการด้านรหัสลับเชิงควอนตัมมาระยะหนึ่ง แต่ก็ต้องย้อนกลับสู่จุดเริ่มต้นใหม่ ที่ยังต้องขวนขวายหาวิถีทางอื่นที่ยั่งยืนต่อ ๆ ไป

โดยระหว่างทางการพัฒนา แนวทางศักยภาพหนึ่งที่อาจทำให้พบโอกาสช่องทางใหม่ขึ้นได้ นั่นคือ การพิจารณาเน้นหนักกับทรัพย์สินทางปัญญาของเทคโนโลยีอุบัติใหม่ที่เพิ่งได้รับความสนใจในโลกและยังมีการยื่นขอรับสิทธิบัตรคุ้มครองการประดิษฐ์คิดค้นที่ยังไม่สูงมากนัก การเร่งสืบค้นแสวงหาผ่านช่องทางสิทธิบัตรนั้น อาจได้พบโอกาสให้เกิดการสอดแทรกขึ้นในเวทีใหม่นี้ได้บ้างและทันต่อวัฏจักรอายุของเทคโนโลยี ทั้งน้ำหนักด้านการศึกษาวิจัยและพัฒนาอุตสาหกรรมการผลิตหรือบริการ เป็นต้น อีกทั้งโอกาสด้านการศึกษาภาคสังคมที่ควรได้มีภูมิคุ้มกันจากการเป็นประเทศผู้บริโภคเทคโนโลยีโดยสมบูรณ์ ที่อาจได้มีการหลงคล้อยตามประเทศที่พัฒนาแล้วในมุมการโฆษณาชวนเชื่อที่มิควร การร่วมกันสกัดและเผยแพร่ข้อมูลที่เหมาะสมและเพียงพอร่วมจากแหล่งนี้ อาจนำไปสู่การถอดรหัสวิทยาการใหม่ให้เกิดประโยชน์กับสังคมได้บ้างต่อไป

ข้อมูลร่วมสมัยที่ได้สำรวจและประเมินจากรายงานนี้ จะได้ผลักดันต่อยอดสู่ข้อเสนอโครงการด้านที่เกี่ยวข้องของประเทศไทยและแผนแม่บทอื่น ๆ ต่อไปด้วย ทั้งนี้ขอขอบคุณ งานบริการความรู้และห้องสมุด ฝ่ายบริการความรู้ทางวิทยาศาสตร์และเทคโนโลยี (STKS)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) สำหรับข้อมูลสิทธิบัตรที่ใช้งานร่วมกันกับคอลัมน์ข่าวสารหนังสือพิมพ์รายสัปดาห์[1] รวมถึงส่วนข้อมูลวิเคราะห์ที่ใช้งานในโครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: *การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร* (Technology Transfer and Human Resource Development of Perfectly Secure Quantum Communications) ร่วมอยู่กับโครงการของกลุ่มแอลอีดีประยุกต์ LED-SmartCoN.Org ด้วย

ขอขอบคุณ ผู้อำนวยการ ศูนย์ความเป็นเลิศด้านฟิสิกส์ (ThEP Center) และสถาบันวิจัยดาราศาสตร์แห่งชาติ (NARIT) รวมทั้ง กรรมการอำนวยการ สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย และสมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ ที่ได้ให้ข้อเสนอแนะแนวทางความร่วมมือสำหรับอนาคตต่อการเริ่มต้นวิทยาการรหัสลับเชิงควอนตัมในประเทศไทยได้ใหม่อย่างจริงจังและทันต่อเป้าหมายของ"การเป็นผู้ซื้ออย่างฉลาด" ซึ่งจะได้ร่วมกันผลักดัน ขอขอบคุณ มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนาและมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ที่สนับสนุนสนามการระดมสมองในงานประชุมวิชาการ (ECTI-CON & CARD 2016) รวมถึงกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส. - กสทช)

อนึ่ง หนังสือเชิงรายงาน (white paper) นี้จัดทำคู่ขนานสู่การสนับสนุนข้อมูลต่อโครงการลำดับถัดไป คือ *"ศูนย์ทดสอบฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed) : 2016"* เพื่อเร่งกระตุ้นสร้างความตระหนักของภาคสาธารณะและอุตสาหกรรมไอทีในประเทศไทยร่วมกับผลผลิตอื่น ๆ ที่ได้ระดมสรรพกำลังจัดทำมาก่อนหน้าแล้วทั้ง *"พัฒนาการสารสนเทศเชิงควอนตัม" (พ.ศ. ๒๕๕๕) และ"สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗)"* โดยหวังเป็นอย่างยิ่งว่า อุตสาหกรรมและภาคนโยบายไอทีไทยจะสามารถปรับตัวได้ทันเวลา ลดการสูญเสียทุกมิติจากเช่นที่ผ่านมาลงได้บ้างแม้ประเทศไทยจะเป็นผู้ซื้อเทคโนโลยีโดยสมบูรณ์

Thai Quantum Information (Q-Thai) Forum

1 *www.dailynews.co.th/article/OQC_slash_LED* **หรือ** *LED-SmartCoN.Org เมนู LED-Column*

บทสรุปพิเศษ

(Executive Summary)

การพัฒนางานด้านวิทยาการใหม่เชิงควอนตัมสี่ชิ้นก่อนหน้า เริ่มจากทั้งวิชาการพื้นฐาน[2] ความรู้ทั่วไปและการประยุกต์[3] รวมถึงการนำเสนอบทสรุปประสบการณ์พัฒนาการในประเทศไทยด้านนี้สำหรับผู้กำกับดูแลนโยบายด้วยงานชิ้นที่สี่ "สารสนเทศเชิงควอนตัมประเทศไทย: *พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ. ๒๕๕๗)*"[4] แล้วจึงได้ขยายผลมาสู่ชิ้นงานชิ้นที่ห้า อันเป็นงานในระดับข้อมูลเชิงนโยบายนี้และเป็นการต่อยอดเชิงลึกด้วยการสำรวจผลงานวิชาการ และทรัพย์สินทางปัญญาจากทั่วโลกด้านรหัสลับเชิงควอนตัม เพื่อสร้างฐานข้อมูลสนับสนุนการตัดสินใจสู่การนำเสนอโครงการอนาคต *"ศูนย์ทดสอบฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม"* ต่อไป

ที่ผ่านมาได้มีการรวมตัวของกลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย (Thai Quantum Information Forum) เพื่อทั้งติดตามความก้าวหน้าของเทคโนโลยีสารสนเทศเชิงควอนตัมโลก เพื่อการวางแผนที่นำทางและแนวทางและการพยากรณ์อนาคตรองรับ เร่งสร้างโครงสร้างพื้นฐาน พัฒนาบุคลากร สนับสนุนหลักสูตรการเรียนการสอนและงานวิจัยในประเทศจนถึงเพื่อการรวมกลุ่มและยกระดับการเรียนรู้สารสนเทศเชิงควอนตัมในสู่การวิจัยและพัฒนาและใช้งานที่เหมาะสม โดยต่อไปยังการส่งเสริมสนับสนุนการสื่อสารวิทยาศาสตร์ พัฒนาคุณภาพการศึกษายกระดับองค์ความรู้และถ่ายทอดองค์ความรู้สู่สังคม และเตรียมความพร้อมและทัศนคติที่ถูกต้องเหมาะสม สำหรับเทคโนโลยีที่จะอุบัติใหม่ในอนาคตของกลศาสตร์ควอนตัมเชิงสาธารณะ รวมทั้ง เพื่อบูรณาการเสริมสร้างความเข้มแข็งและปรับใช้กับวิทยาการสาขาอื่น ๆ หรือด้านที่เกี่ยวข้องและเพื่อสร้างความร่วมมือระหว่างหน่วยงานในประเทศ ทั้งภาคการศึกษา นโยบายและอุตสาหกรรมที่เกี่ยวข้องเตรียมพร้อมรับการถ่ายทอดเทคโนโลยีอุบัติใหม่ในอนาคตแล้วนั้น หวัง วัตถุประสงค์ดังกล่าวยังคงมีพัฒนาการไม่ถึงระดับนัยที่สำคัญใด ๆ อันจะส่งผลต่อการเปลี่ยนแปลงสถานะภาพได้

ดังนั้น จึงยังคงต้องเร่งพัฒนาแนวปฏิบัติทุกวิถีทางต่อไป ในการนี้ การสร้างความตระหนักถึงคุณค่าของทรัพย์สินทางปัญญา คือ กลยุทธ์หนึ่งที่ได้รับการนำเสนอในช่วงที่ผ่านมา

2 *พัฒนาการสารสนเทศเชิงควอนตัม www.ebooks.in.th/ebook/7748/*

3 *www.ebooks.in.th/ebook/30570/ และ www.ebooks.in.th/ebook/38617/*

4 *สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗)*
ISBN: 978-616-374-830-0 http://www.ebooks.in.th/ebook/30625/

ทั้งนี้ สืบเนื่องจากการประเมินอันดับขีดความสามารถในการแข่งขัน (The Global Competitiveness Report 2014 – 2015) ของประเทศต่าง ๆ เพื่อเป็นข้อมูลบ่งชี้สถานภาพจากหลายหัวข้อพบว่า ประเทศไทยถูกจัด**ระดับความสามารถการแข่งขันอยู่ที่ 31 ด้านการศึกษาระดับอุดมศึกษาอยู่ที่อันดับ 59 ความพร้อมทางด้านเทคโนโลยีอยู่ในอันดับที่ 65 และการสร้างนวัตกรรมอยู่ในลำดับที่ 67 จาก 144 ประเทศทั่วโลก** ส่วนองค์การทรัพย์สินทางปัญญาโลก (WIPO) จัดทำ**ดัชนีชี้วัดนวัตกรรมของโลกปี พ.ศ. 2558 ประเทศไทยอยู่ในอันดับที่ 55 จาก 141 เขตเศรษฐกิจทั่วโลก** (ลดลงจากอันดับที่ 48 ของปี ค.ศ.2014 หรือ พ.ศ. 2557) ประเทศไทยอยู่ในกลุ่มประเทศที่มีรายได้ปานกลาง (Upper-Middle Income Economy) และอยู่ในลำดับที่ 4 จากทั้งหมด 8 ประเทศที่พิจารณาของกลุ่มอาเซียนรองลงมาจากประเทศสิงคโปร์ มาเลเซีย และแม้แต่เวียดนาม

รวมทั้งด้านดัชนีความคุ้มครองด้านการเป็นเจ้าของสินทรัพย์ของภาคเอกชนประจำปี ค.ศ.2015 ของ 129 ประเทศทั่วโลก ประเทศไทยได้รับ 4.9 คะแนน ลดลงจาก ปี ค.ศ. 2014 ลงมา 0.4 คะแนน โดยมีหลายด้านที่พิจารณาซึ่งใน**เรื่องเสถียรภาพทางการเมืองและทรัพย์สินทางปัญญามีคะแนนที่ต่ำมาก** โดยประเทศในกลุ่มอาเซียนที่ได้คะแนนมากที่สุดคือสิงคโปร์ (8.1) อันดับสองมาเลเซีย (6.6) และฟิลิปปินส์ (5.1) ส่วนประเทศไทยมีคะแนนเท่ากับประเทศอินโดนีเซียอยู่ในลำดับสี่ร่วม

โดยจากข้อมูลข้างต้นที่มีความสัมพันธ์กันบ่งชี้ได้ถึงความล้าหลังของประเทศ และเมื่อพิจารณาถึงสาขาเฉพาะทางด้านสารสนเทศเชิงควอนตัมกับทรัพย์สินทางปัญญาแล้ว เป็นที่แน่นอนว่าประเทศไทยยังคงไกลห่างมากจากต้นกำเนิดและไม่มีแนวโน้มการพึ่งพาตนเองได้ในอนาคตอันใกล้ จึงควรมาร่วมด้วยช่วยกันของทุกภาคส่วนเพื่อทั้งการสร้างความรู้ความเข้าใจสู่สังคมและการพัฒนาการศึกษาวิจัยและพัฒนาที่ยังห่างไกลจุดมวลวิกฤติในทุก ๆ ด้าน ให้ได้มีการพัฒนาดีกว่าเดิมก้าวหน้ามากขึ้นจากสถานะเดิมนั้น

และอีกมุมหนึ่งของพัฒนา เมื่อได้พิจารณาเน้นหนักลงลึกกับทรัพย์สินทางปัญญาโดยเฉพาะกับเทคโนโลยีอุบัติใหม่ที่เพิ่งได้รับความสนใจในโลกเช่นรหัสลับเชิงควอนตัมนี้ โดยยังมีการยื่นขอรับการคุ้มครองการประดิษฐ์คิดค้นที่ไม่สูงมากนัก อาจได้พบกับมุมมองที่สามารถเร่งสร้างโอกาสให้เกิดการสอดแทรกขึ้นในเวทีของสาขาใหม่เหล่านั้นทันเวลาได้บ้างด้วย อันเป็นการแสวงหาโอกาสของประเทศที่มีช่องทางอยู่น้อยได้ หรืออย่างน้อยที่สุดก็เพื่อการติดตามการลดช่องว่างที่กำลังห่างขึ้นอย่างยิ่งจากประเทศพัฒนาแล้วอื่น ๆ เกิดประโยชน์ขั้นต่ำในการเลือกซื้อจัดหาหรือใช้งานได้อย่างคุ้มค่าให้มากที่สุดหรือแม้จะเป็นเพียงการสร้างภูมิคุ้มกันทางภูมิปัญญาให้สามารถพึ่งตนเองได้หากเกิดข้อพิพาทการจัดซื้อจัดหาหรือใช้งานเทคโนโลยีแขนงใหม่เหล่านั้นในอนาคต

เริ่มต้นที่การสำรวจด้านวิชาการอันเป็นพื้นฐานการศึกษาแนวทางของทรัพย์สินทางปัญญา พบความก้าวหน้าของวงการวิทยาการรหัสลับเชิงควอนตัมโลกปรากฏแนวโน้มจำนวนเพิ่มมากขึ้นทุกปีและมาจากฝั่งตะวันออกสูงขึ้นทั้งจากประเทศจีน ญี่ปุ่นและสิงคโปร์ แต่ยังอยู่ในขั้นพัฒนาการพื้นฐานเนื่องจากตาบเกี่ยวกับด้าน**สาขาวิชาฟิสิกส์สูงถึง 70%** โดย**การประยุกต์กับสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมศาสตร์พัฒนาตาบเกี่ยวใน 25% และ 23% โดยลำดับ** ประเทศจีนเป็นผู้มีความก้าวหน้าของวงการวิชาการสูงที่สุดจากผลรวมของกลุ่มจากมหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศจีน (USTC)

เมื่อนำมาสู่ภาพรวมและสถิติกลุ่มเอกสารสิทธิบัตร โดยรายงานนี้ได้ทำการพิจารณารวบรวมจากฐานรวมมากกว่า 22 ล้านชุดด้วยการใช้เครื่องมือสำรวจของ Thomson Innovation ผลสรุปภาพรวมสิทธิบัตร พบว่า แม้ศาสตร์นี้กำเนิดมาตั้งแต่ปี ค.ศ.1984 แต่ยังปรากฏทรัพย์สินทางปัญญาไม่มากนักจนกระทั่งมาถึงช่วงสหัสวรรษใหม่ จากฐานข้อมูลถึงเดือนเมษายน ปี ค.ศ. 2016 พบสิทธิบัตรจำนวน **827** เรื่อง (280 DWPI กลุ่ม Families) ซึ่งบ่งชี้ความสัมพันธ์ที่สำคัญหลายหัวข้อ ประเทศที่มีการยื่นขอจดสิทธิบัตรและได้รับการคุ้มครองมากที่สุดได้แก่ สหรัฐอเมริกา โดยมีแนวโน้มสิทธิบัตรทั่วโลกเพิ่มสูงขึ้น บริษัทผู้ขอและได้รับความคุ้มครองสิทธิบัตรได้แก่ Magiq Technologies ของสหรัฐฯ เช่นกัน ขณะที่ประเทศจีนมีการเติบโตสูงจนเป็นที่น่าจับตายิ่ง

ส่วนด้านผลิตภัณฑ์กับสินค้าอุปกรณ์กระจายกุญแจรหัสลับเชิงควอนตัม (quantum key distributor) ที่ได้เริ่มมีจำหน่ายตั้งแต่ ปี พ.ศ.2546 มาแล้วนั้น บริษัท id Quantique ของประเทศสวิสเซอร์แลนด์ ยังคงเป็นบริษัทต้นแบบผลิตสินค้าด้านรหัสลับเชิงควอนตัมแถวหน้าของโลก มีสิทธิบัตรคุ้มครองครบวงจรของระบบหลัก แต่ก็ได้มีแนวโน้มว่าบริษัทจากประเทศจีนและเกาหลีใต้จะกลายมาเป็นคู่แข่งในอนาคต

สำหรับในกลุ่มประเทศอาเซียน หน่วยงานการวิจัยและพัฒนาจากประเทศสิงคโปร์และมาเลเซียซึ่งเคยเป็นสมาชิกของสถาบันมาตรฐานโทรคมนาคมแห่งยุโรป (ETSI) มีส่วนร่วมกับการสร้างทรัพย์สินทางปัญญาของวงการนี้ในระดับหนึ่ง อีกทั้งมีผลงานด้านวิชาการปรากฏจำนวนมากที่สุดในเขตเศรษฐกิจอาเซียนตามลำดับลักษณะเช่นเดียวที่ปรากฏกับวงการอื่น ๆ

ส่วนประเทศไทยยังไม่ปรากฏข้อมูลที่มีนัยสำคัญด้านสิทธิบัตรแต่อย่างใด หากด้านวิชาการกลับปรากฏมีจำนวนผลงานในระดับที่ไล่หลังประเทศมาเลเซียและสิงคโปร์ ซึ่งแม้ยังห่างพอสมควรแต่ก็เป็นที่น่าสนใจถึงที่มา ซึ่งเมื่อได้ศึกษาเชิงลึกในระดับตัวผลงานย่อยเหล่านั้นแล้วกอปรข้อมูลสาธารณะด้านโครงการวิจัยและพัฒนา สภาพความพร้อม บุคลากร ประวัติและผลงานต่าง ๆ ในประเทศด้วยแล้ว ปรากฏเป็นที่น่ากังวลเรื่องการพัฒนาในทิศทางด้านลบ

สำหรับแนวทางเทคนิค“รหัสลับเชิงควอนตัม”ของทรัพย์สินทางปัญญาที่พบส่วนใหญ่เป็นการนำเสนอรูปแบบการประยุกต์เข้ากับระบบสื่อสารโทรคมนาคมปกติ ส่วนพัฒนาการด้านเทคนิคพบด้านการพัฒนาการอุปกรณ์ประกอบ และการกำเนิดจำนวนสุ่มต้นทางของการสร้างรหัสลับ สำหรับการสร้างสถานะเชิงควอนตัมนั้นพบเทคนิคผสมทั้งเฟส โพราไรซ์ และเทคนิคอื่น (continuous variable) ส่วนเทคนิคความพัวพัน (entanglement) นั้นพบน้อยมาก ซึ่งสัมพันธ์กับข่าวความก้าวหน้าทั่วโลกที่ไม่มีสินค้าจากพื้นหลักการหลังนี้ออกมาแต่อย่างใด เนื่องจากให้ค่าการกำเนิดความพัวพันที่นำมาสร้างเป็นรหัสลับควอนตัมได้ในระดับต่ำความเร็วไม่เพียงพอต่อการใช้งานกับเครือข่ายสื่อสารทั่วไปได้ แม้เป็นแนวทางที่มีศักยภาพเชิงหลักการและได้รับการนำเสนอเพื่อกำเนิดสถานะความพัวพันผ่านดาวเทียมในหลายประเทศแล้ว หากการพัฒนาสร้างจริงทั่วโลกยังคงต้องใช้เวลาสั่งสมความรู้และประสบการณ์อีกมาก

ทั้งนี้ รายงาน “ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙) Survey of Intellectual Properties on Quantum Cryptography (2016)” ที่ดีพิมพ์เผยแพร่นี้ ได้นำเสนอตัวอย่างในรายละเอียดกับการศึกษา“7 สิทธิบัตรตัวอย่างเด่น” ด้วย เพื่อให้เป็นแนวทางตัวอย่างการกระตุ้นสังคมวงกว้าง ให้มีส่วนร่วมศึกษาสิทธิบัตรอีกจำนวนมากและกำลังเติบโตเพิ่มมากขึ้นตลอด โดยในระยะยาวสมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI) และชมรมไฟฟ้าสื่อสาร สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE) จะได้ร่วมกันเป็นเจ้าภาพแกนหลักเพื่อให้โครงการนี้พัฒนาตนเองจากความร่วมมือกันโดยเป็นสาธารณะเกิดเป็นโครงการย่อย **“สังคมสิทธิบัตร – รหัสลับเชิงควอนตัม”** บนสังคมออนไลน์ ให้เติบโตได้ตามการพัฒนาของวงการและการยื่นขอคุ้มครองสิทธิบัตรใหม่ ๆ ที่จะได้ปรากฏมากขึ้นต่อเนื่องได้ตลอดไป และผลพลอยได้จากการศึกษารายงานนี้ อาจได้ผลเพิ่มเติมในมุมที่มิได้มีการนำเสนอสาธารณะทั่วไป เช่น กลยุทธ์การยื่นจดสิทธิบัตรคุ้มครองที่แยบยล เป็นต้น

โดยสรุปสำหรับประเทศไทย *นอกจากด้านทรัพย์สินทางปัญญาแล้ว ไม่ว่าจะเป็นผลงานวิชาการ การศึกษาการเรียนการสอน งานวิจัยและพัฒนา ณ พ.ศ.2559 นั้น พบว่ายังไม่มีนัยสำคัญใดทุกส่วนงาน* และจากประสบการณ์ด้านงานวิจัยและพัฒนาระบบโทรคมนาคมของประเทศที่ต้องอาศัยแนวทางเฉพาะ (7 OSI layers) และประสบความล้มเหลวจำนวนมากแล้วจากความคาดหวังของสังคมที่แตกต่างในอดีต รายงานนี้จึงเป็นการเตรียมการอีกมุมมองที่นักวิจัย นักศึกษา ผู้กำกับนโยบายในประเทศและที่เกี่ยวข้อง ควรได้ตระหนักนำไปประกอบการคาดการณ์สู่การวางแผนการรองรับให้ดียิ่งขึ้นกว่าอดีตต่อไป แม้จะเป็นเพียงเพื่อการจัดซื้อจัดหาเทคโนโลยีเพื่อการประยุกต์ใช้งานเพียงอย่างเดียวในอนาคตก็ตาม อันสอดคล้องกับสถานะภาพที่เป็นอยู่ของอุตสาหกรรมไอทีหรือสื่อสารโทรคมนาคมไทย

สำหรับแนวทางของข้อเสนอที่อาจเป็นไปได้จากการเลือกสรร ณ พ.ศ.2559 จากเดิมที่ปรากฏว่าในประเทศมีความพร้อมเพียงส่วนน้อยกับระดับงานด้าน transportation layer 4 (ของ 7 OSI layers) เมื่อเทียบเคียงทั้งด้านวิชาการและโอกาสสร้างทรัพย์สินทางปัญญาที่น้อยมากของประเทศ และยังไม่มีแนวโน้มการสร้างผลงานที่ผลกระทบสูงได้ ดังนั้น จึงอาจเป็นการเหมาะสมที่จะเลือกลงทุนทรัพยากรต่าง ๆ กับจุดแข็งเดิมนั้นเพื่อความต่อเนื่อง ก่อนขยายสู่ระดับอื่นรอบข้างที่ยังคงขาดแคลนโดยสมบูรณ์ อีกทั้ง ระดับงานของ OSI layer 4 เป็นส่วนงานด้านวิศวกรรมศาสตร์เน้นหนักกับการสื่อสารและคอมพิวเตอร์ ซึ่งมีอัตราส่วนของทั้งนักศึกษา นักวิชาการ นักวิจัยในประเทศจำนวนสูงมากกว่าสาขาฟิสิกส์ *(ที่เหมาะสมกับงานระดับล่าง (physical layer) และมีบุคลากรน้อยมากยังไม่มีแนวโน้มของการเริ่มต้นได้)* จึงอาจเป็นแนวทางความหวังในการสร้างงานวิจัยสู่การสร้างทรัพย์สินทางปัญญาได้เองบ้างต่อไป

รายงานฉบับนี้ จัดทำคู่ขนานและเป็นส่วนหนึ่งของการสนับสนุน “ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed): 2016” ซึ่งสะสมต่อยอดมาจากงานก่อนหน้าอื่น ๆ ของกลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย และจะได้ร่วมกันผลักดันต่อไปกระทั่งปัจจัยสำคัญของการพัฒนาทั้งสี่จากแผนกลยุทธ์ คือ **ยุทธศาสตร์การระดมทุน การพัฒนาบุคลากร วิทยาการร่วมเรียนรู้โลก และนโยบายการเป็นผู้ซื้ออย่างฉลาด** มีความพร้อมและดำเนินการไปสู่เป้าหมายต่อไป

.....

สารบัญ

เกริ่นนำพื้นฐานทรัพย์สินทางปัญญา 1

สิทธิบัตร (Patent) หมายถึง หนังสือสำคัญที่รัฐออกให้เพื่อคุ้มครองการประดิษฐ์ (Invention) หรือการออกแบบผลิตภัณฑ์ (Product Design) ที่มีลักษณะตามที่กฎหมายกำหนด เป็นสิทธิพิเศษที่ให้ผู้ประดิษฐ์คิดค้นหรือผู้ออกแบบผลิตภัณฑ์ มีสิทธิที่จะผลิตสินค้า จำหน่ายสินค้าแต่เพียงผู้เดียว ในช่วงระยะเวลาหนึ่ง ...
(อ้างอิง: กรมทรัพย์สินทางปัญญา)

a government authority or license conferring a right or title for a set period, especially the sole right to exclude others from making, using, or selling an invention
(Oxford Dictionaries)

[5]เมื่อกล่าวถึงเรื่องทรัพย์สินกับการคุ้มครองสิทธิในทรัพย์ประเภทต่าง ๆ นั้น ความคุ้นเคยโดยพื้นฐานของสังคมที่ปรากฏอยู่กับข่าวทั่วไปมักจะเกี่ยวข้องกับเรื่อง "ลิขสิทธิ์" เนื่องจากเป็นสิ่งใกล้ตัวและเข้าใจได้ง่ายกว่า เช่น ลิขสิทธิ์เพลงหรือภาพยนตร์ เป็นต้น หากแต่ทรัพย์สินทางปัญญามีการแบ่งประเภท[6]มากกว่านั้น คือ ทั้งกับเรื่อง การประดิษฐ์ การออกแบบผลิตภัณฑ์ สิทธิบัตร/ อนุสิทธิบัตร แบบผังภูมิของวงจรรวม เครื่องหมายการค้า ชื่อทางการค้า สิ่งบ่งชี้ทางภูมิศาสตร์ คุ้มครองพันธุ์พืช ภูมิปัญญาท้องถิ่น โดยมีรายละเอียดแยกย่อยลงไปอีกพอสมควร และโดยทั่วไปเมื่อกล่าวถึงสิ่งเหล่านี้จะเกี่ยวข้องกับหน่วยงานในประเทศที่มีหน้าที่ดูแลโดยตรงคือ "กรมทรัพย์สินทางปัญญา"

ด้วยภารกิจของหน่วยงานนี้อันทำหน้าที่ส่งเสริมให้เกิดการตระหนัก *"เพื่อคุ้มครองปกป้องสิทธิในทรัพย์สินทางปัญญาทั้งในประเทศและต่างประเทศ ส่งเสริมความรู้ การสร้างสรรค์ และการใช้ประโยชน์ทรัพย์สินทางปัญญาในเชิงพาณิชย์ เพื่อให้คนไทยมีความรู้ มีการสร้างสรรค์ และใช้ประโยชน์ทรัพย์สินทางปัญญาในเชิงพาณิชย์เพิ่มขึ้นรวมทั้งเพื่อสร้างจิตสำนึกให้ตระหนักถึงความสำคัญ ประโยชน์ และเคารพสิทธิในทรัพย์สินทางปัญญาและเพื่อ*

5 *ข้อมูลส่วนเกริ่นนำนี้ ใช้และนำเสนอร่วมกับกับรายงานชิ้นอื่น ๆ ของสมาคมวิชาการ ECTI (LED-SmartCoN.Org)*
6 *www.kmutt.ac.th/rjopc/ipcat.htm*

สร้างเครือข่ายด้านทรัพย์สินทางปัญญาในทุกระดับ[7]" ความรู้ด้านทรัพย์สินทางปัญญาจึงได้รับการเผยแพร่และมีการศึกษากันมากขึ้น ทั้งระดับนโยบาย การศึกษาวิจัยและพัฒนา และกับทั้งภาคธุรกิจแวดวงต่าง ๆ ถึงกระนั้น สถานะภาพทรัพย์สินทางปัญญาในประเทศยังอยู่ในระดับพื้นฐาน มีความก้าวหน้าที่แสดงได้ด้วยสถิติและดัชนีชี้ผลต่าง ๆ จากทั่วโลกและโดยจากข้อมูลของประเทศไทยเองปรากฏในระดับที่ต่ำมาก รวมถึงข้อมูลที่สัมพันธ์ด้านที่เกี่ยวข้องอื่น ๆ ด้วย เช่น

จากการประชุมกลุ่มเศรษฐกิจโลก (World Economic Forum: WEF) ได้เผยแพร่รายงานการจัดอันดับชีดความสามารถในการแข่งขันของ ประเทศต่างๆ ใน 144 ประเทศทั่วโลก (The Global Competitiveness Report 2014 - 2015)[8] พบว่า ภาพรวมเศรษฐกิจของประเทศไทยถูกจัด อยู่ในกลุ่ม Efficiency-Driven Economies โดยระดับความสามารถในการแข่งขันโดยรวมอยู่ในอันดับที่ 31 ด้านการศึกษาในระดับอุดมศึกษาอยู่ที่อันดับ 59 **ด้านความพร้อมทางด้านเทคโนโลยีอยู่ในอันดับที่ 65 และการสร้างนวัตกรรมอยู่ในลำดับที่ 67**

องค์การทรัพย์สินทางปัญญาโลก (WIPO) จัดทำดัชนีชี้วัดนวัตกรรมของโลกปี พ.ศ. 2558[9] ในแนวคิด "ประสิทธิผลของนโยบายนวัตกรรมเพื่อการพัฒนา (Effective of Innovation Policies for Development)[10]" ประเทศไทยถูกจัดอยู่ในอันดับที่ 55 จาก 141 เขตเศรษฐกิจทั่วโลก (ลดลงจากอันดับที่ 48 ของปี ค.ศ.2014 หรือ พ.ศ.2557) รายงานดัชนีชี้วัดนวัตกรรมนี้ วิเคราะห์ปัจจัยต่าง ๆ ที่ส่งเสริมต่อการพัฒนางานนวัตกรรมเพื่อการใช้ประโยชน์เชิงเศรษฐกิจ โดยประเทศที่อยู่ใน 5 อันดับแรก ได้แก่ ประเทศที่มีรายได้สูงทั้งสวิตเซอร์แลนด์ สหราชอาณาจักร สวีเดน เนเธอร์แลนด์ และสหรัฐอเมริกา สำหรับ**ประเทศไทยอยู่ในกลุ่มประเทศที่มีรายได้ปานกลาง (Upper-Middle Income Economy) และอยู่ในลำดับที่ 4 จากทั้งหมด 8 ประเทศที่พิจารณาของกลุ่มอาเซียน**รองลงมาจากประเทศสิงคโปร์ มาเลเซีย และแม้แต่เวียดนาม

ด้านดัชนีความคุ้มครองด้านการเป็นเจ้าของสินทรัพย์ของภาคเอกชน กลุ่มความร่วมมือ PRA (Property Rights Alliance) ได้จัดทำดัชนีเรื่องสิทธิการเป็นเจ้าของสินทรัพย์หรือ "International Property Rights Index (IPRI)[11]" ประจำปี ค.ศ.2015 ของ 129 ประเทศทั่วโลก โดย**ดัชนี IPRI ของประเทศไทยอยู่ที่ 4.9 คะแนน ลดลงจากปีค.ศ. 2014 ลงมา 0.4 คะแนน** โดยมีหลายด้านที่พิจารณาซึ่งในเรื่อง**เสถียรภาพทางการเมือง และทรัพย์สินทางปัญญามีคะแนนที่ต่ำมาก โดยประเทศในกลุ่มอาเซียนที่ได้คะแนน IPRI มากที่สุดคือ สิงคโปร์ (8.1) อันดับสองมาเลเซีย (6.6) และฟิลิปปินส์ (5.1) ส่วนประเทศไทยมีคะแนนเท่ากับประเทศอินโดนีเซียอยู่ในลำดับสี่ร่วม (4.9)**

ในขณะที่ดัชนีเหล่านี้ สามารถบ่งชี้ในระดับมหภาคหรือภาพรวมจากจัดอันดับของหน่วยงานในต่างประเทศ ข่าวทั่วไปในประเทศหลายกรณียังคงวนเวียนอยู่กับการละเมิด คดีความหรือการฟ้องร้องอยู่ทั่วไป อีกทั้งด้านความรู้ความเข้าใจพื้นฐานที่ยังคงเป็นอุปสรรคมากเช่นกัน เช่นบทวิจารณ์ *"ปัญหาทรัพย์สินทางปัญญาที่สำคัญของประเทศไทยเกิดจากการไม่เข้าใจในเรื่องทรัพย์สินทางปัญญาอย่างถูกต้องทั้งในระดับ ประชาชนทั่วไป ไปจนถึงระดับปัญญาชนศึกษา ตลอดจนนักวิชาการทั่วไป ตัวอย่างที่พบมากได้แก่ การไม่เข้าใจในความแตกต่างระหว่างทรัพย์สินทางปัญญาประเภทสิทธิบัตร กับทรัพย์สินทางปัญญาประเภทลิขสิทธิ์ มีการใช้สับสนระหว่างคำว่าสิทธิบัตรกับคำว่าลิขสิทธิ์ค่อนข้างมาก หลายครั้งที่สื่อมวลชนนำเสนอผลงานสิ่งประดิษฐ์ทางวิทยุโทรทัศน์และรายงานว่า สิ่งประดิษฐ์นั้นได้ยื่นขอรับลิขสิทธิ์แล้ว ทั้ง ๆ ที่สิ่งประดิษฐ์ที่ผลิตภัณฑ์ใหม่ หรือกรรมวิธีการผลิตใหม่ หรือการใช้งานใหม่ที่ไม่เคยมีปรากฏ หรือมีการใช้งานที่ใดมาก่อน และไม่เคยเปิดเผยสาระสำคัญของการประดิษฐ์มาก่อน ต้องยื่นขอรับการคุ้มครองตามพระราชบัญญัติสิทธิบัตร พ.ศ. 2522 ขณะที่ลิขสิทธิ์ซึ่งเป็นผลงานทางวรรณกรรม ได้แก่ งานศิลปะ หนังสือ เพลง สื่อบันทึกภาพ สื่อบันทึกเสียง ซอฟแวร์คอมพิวเตอร์ เจ้าของผลงานจะได้รับสิทธิคุ้มครองนานาชาติทันที ตามอนุสัญญากรุงเบิร์น"*[12] ซึ่งทั้งหมดนี้คือภาพสะท้อนมุมทั่วไป ที่สามารถพิจารณาสถานะภาพตนเองได้เป็นอย่างดี

โดยสรุป เมื่อพิจารณาถึงดัชนีที่ใช้วัดผลการพัฒนาประเทศ ทรัพย์สินทางปัญญาคือหนึ่งในหัวข้อสำคัญนั้น โดยจากข้อมูลการพิจารณาข้างต้นที่บ่งชี้ความล้าหลังของประเทศ[13] จึงควรมาร่วมด้วยช่วยกันของทุกภาคส่วนเพื่อทั้งการสร้างความรู้ความเข้าใจสู่สังคมและการพัฒนาการศึกษาวิจัยและพัฒนาที่ยังห่างไกลจุดมวลวิกฤติในทุก ๆ ด้าน ให้ได้มีการพัฒนาดีกว่าเดิมและก้าวหน้ามากขึ้นด้วยจากสถานะเดิมนั้น

7 *กรมทรัพย์สินทางปัญญา www.ipthailand.go.th/index.php?option=com_content&view=article&id=27&Itemid=307*

8 *www.weforum.org/reports/global-competitiveness-report-2014-2015/*

9 *www.wipo.int/wipo_magazine/en/2015/05/article_0002.html*

10 *www.wipo.int/edocs/pubdocs/en/wipo_gii_2015.pdf*

11 *internationalpropertyrightsindex.org/country?c=THAILAND*

12 *www.trf.or.th/index.php?option=com_content&view=article&id=895:2012-01-27-06-18-37&catid=34:research-digest&Itemid=145*

13 *สำหรับประเทศไทยนั้น จากสถิติจากกรมทรัพย์สินทางปัญญาทั้งการยื่นของจดคุ้มครองและสิทธิบัตรที่ได้รับการประกาศคุ้มครองล่าสุดที่สำรวจของปีพ.ศ. 2557 มีจำนวนคำขอรับสิทธิบัตรทั้งหมด (Patent Application) และสิทธิบัตรจดทะเบียนทั้งหมด (Granted Patent) 12,007 และ 3,763 ตามลำดับ (ต้องภาคผนวก)*

และเมื่อพิจารณาถึงความสัมพันธ์ของทรัพย์สินทางปัญญากับสาขาเฉพาะทางด้านสารสนเทศเชิงควอนตัมที่วิทยาการด้านนี้นั้นประเทศไทยมีพัฒนาการที่ไกลห่างมากจากต้นกำเนิด[14]และไม่มีแนวโน้มการพึ่งพาตนเองได้ในอนาคตอันใกล้ ทรัพย์สินทางปัญญาเป็นอีกดัชนีหนึ่งที่ได้มาตอกย้ำความล้าหลังของวิทยาการโลกอนาคตดังกล่าวนี้อีกทางหนึ่ง

ซึ่งที่ผ่านมา ได้เกิดมีการรวมตัวเป็นกลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย (Thai Quantum Information Forum) ขึ้นมาเพื่อทั้งติดตามความก้าวหน้าเทคโนโลยีสารสนเทศเชิงควอนตัมโลก เพื่อการวางแผนที่นำทางและแนวทางและการพยากรณ์อนาคตรองรับสำหรับประเทศไทย เร่งสร้างโครงสร้างพื้นฐาน พัฒนาบุคลากร สนับสนุนหลักสูตรการเรียนการสอนและงานวิจัยในประเทศ จนถึงเพื่อการรวมกลุ่มและยกระดับการเรียนรู้สารสนเทศเชิงควอนตัมในสู่การวิจัยและพัฒนาและใช้งานสารสนเทศเชิงควอนตัมที่เหมาะสม เพื่อส่งเสริมสนับสนุนการสื่อสารวิทยาศาสตร์ พัฒนาคุณภาพการศึกษายกระดับองค์ความรู้และถ่ายทอดองค์ความรู้สู่สังคม และเตรียมความพร้อมและทัศนคติที่ถูกต้องเหมาะสมสำหรับเทคโนโลยีที่จะอุบัติใหม่ในอนาคตของกลศาสตร์ควอนตัมเชิงสาธารณะ รวมทั้ง เพื่อบูรณาการเสริมสร้างความเข้มแข็งและปรับใช้กับวิทยาการสาขาอื่น ๆ หรือด้านที่เกี่ยวข้อง เช่น มาตรวิทยา (quantum metrology) เป็นต้น และเพื่อสร้างความร่วมมือระหว่างหน่วยงานต่าง ๆ ในประเทศ ทั้งภาคการศึกษา นโยบายและอุตสาหกรรมที่เกี่ยวข้องเตรียมพร้อมรับการถ่ายทอดเทคโนโลยีอุบัติใหม่เพื่อสามารถต่อยอดองค์ความรู้สู่งานวิจัยในอนาคต หว่า ยังคงมีพัฒนาการที่ไม่มีนัยสำคัญใด ๆ ที่จะส่งผลต่อการเปลี่ยนแปลงสถานะภาพได้ จึงยังคงต้องพัฒนาแนวปฏิบัติทุกวิถีทางต่อไป ซึ่งการให้เกิดความตระหนักถึงคุณค่าของทรัพย์สินทางปัญญาคือหนึ่งในกลยุทธวิถีการพัฒนาที่เลือกนำมาเสนอในรายงานฉบับนี้

ทั้งนี้ หากได้พิจารณาเน้นหนักลงลึกกับทรัพย์สินทางปัญญาโดยเฉพาะกับเทคโนโลยีอุบัติใหม่ที่เพิ่งได้รับความสนใจในโลกและยังมีการยื่นขอรับการคุ้มครองการประดิษฐ์คิดค้นที่ยังไม่สูงมากนักสาขารหัสลับเชิงควอนตัมนี้ อาจได้พบกับมุมมองที่สามารถสร้างโอกาสให้เกิดการสอดแทรกขึ้นในเวทีของสาขาใหม่เหล่านั้นทันเวลาได้บ้าง อันเป็นการสร้างโอกาสของประเทศที่ยังมีช่องทางน้อยได้ หรือน้อยที่สุดเพื่อการติดตาม ลดช่องว่างที่กำลังห่างมากขึ้นอย่างยิ่งของประเทศอื่น ๆ ที่พัฒนาล้ำหน้าไปมากมายกว่าแล้ว อันจะยังประโยชน์ในการเลือกซื้อจัดหาหรือใช้งานได้อย่างคุ้มค่ามากที่สุดในอนาคต หรือเป็นการสร้างภูมิคุ้มกันทางภูมิปัญญาให้สามารถพึ่งพาตนเองได้มากที่สุดหากเกิดข้อพิพาทในการจัดซื้อจัดหาหรือใช้งานในอนาคต

ทั้งนี้ เนื่องจากความใหม่ของตัววิทยาการด้าน “รหัสลับเชิงควอนตัม” นี้ จึงทำให้ประเภทของทรัพย์สินทางปัญญายังคงปรากฏครอบคลุมอยู่กับเฉพาะประเภท “สิทธิบัตร” ซึ่งมีความสำคัญเพียงแหล่งเดียวที่สามารถนำมาใช้พิจารณาเป็นดัชนีหลักในการวัดผลการพัฒนา แต่ก็สามารถใช้บ่งชี้แนวโน้มอนาคตพัฒนาการของเทคโนโลยี “รหัสลับเชิงควอนตัม” ได้เป็นอย่างดี

รายงาน “ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙) (Survey of Intellectual Properties on Quantum Cryptography (2016)” นี้ จึงเป็นอีกมุมมองที่นักวิจัย นักศึกษา และผู้กำกับดูแลนโยบายวิทยาศาสตร์และเทคโนโลยี รวมถึงภาคอุตสาหกรรมสารสนเทศการสื่อสารและการคำนวณในประเทศและอื่น ๆ ที่เกี่ยวข้อง ควรได้ตระหนักนำไปประกอบการคาดการณ์สู่การวางแผนการรองรับให้ดียิ่งขึ้นต่อไปได้ แม้จะเป็นเพียงเพื่อการจัดซื้อจัดหาเทคโนโลยีเพื่อการประยุกต์ใช้งานเพียงอย่างเดียวตามลักษณะและสถานะภาพการแข่งขันที่เป็นอยู่ของประเทศไทยก็ตาม

14 *ศ.ล.ร.สุทัศน์ ยกส้าน ราชบัณฑิต กล่าวว่า “เขาเหล่านั้นสร้างประเทศมาก่อนหน้าเราด้วยวิทยาศาสตร์มานานแล้ว ประเทศไทยเพิ่งเข้ามาสู่ยุควิทยาศาสตร์ประมาณไม่ถึง 30 – 50 ปีมานี้ ... อาจารย์สิปปนนท์ เกตุทัต* สมัยเรียนจบกลับมาควอนตัมยังไม่ได้สอนในเมืองไทยเลย เราตามหลังเขามากควอนตัมเกิดเมื่อปีค.ศ.1925 อาจารย์สิปปนนท์กลับมาปีค.ศ. 1975 ห้าสิบปีผ่านไปแล้วควอนตัมก็ยังไม่ยังเมืองไทย” (* ศาสตราจารย์กิตติคุณ ดร. สิปปนนท์ เกตุทัต อดีตบ้านเรือนทุน (ครุรสภา) ด้านฟิสิกส์และอดีตรัฐมนตรีว่าการกระทรวงศึกษาธิการและอุตสาหกรรม”)

ข้อมูลงานวิจัยและพัฒนา 2

การศึกษาผลงานวิชาการของ "รหัสลับเชิงควอนตัม" นั้น จะเป็นสิ่งที่ทำให้ทราบความก้าวหน้าพื้นฐานที่เป็นแนวทางการนำไปสู่การคิดค้น จนต่อโยงถึงการประดิษฐ์และการคุ้มครองสิทธิการค้นค้นนั้นด้วยการยื่นขอจดสิทธิบัตรต่อไป และสามารถคาดการณ์ถึงทิศทางของเทคโนโลยีในอนาคตที่เกิดจากต้นกำเนิดวิชาการเหล่านั้นได้ ผลงานวิชาการที่อ้างอิงถึงได้นี้หมายถึงการนำเสนอตีพิมพ์งานวิชาการที่ผ่านการพิจารณาของผู้ทรงคุณวุฒิ (peer review) ในลำดับหนึ่งแล้วด้วย สามารถอ้างอิง (citation) เพื่อพัฒนางานวิชาการที่เกี่ยวข้องอื่น ๆ ต่อไปได้ด้วยเช่นกัน

ทั้งนี้ การสืบค้นผลงานวิชาการดังกล่าว มีสามแหล่งข้อมูลหลักที่มักจะใช้งานเพื่อภารกิจดังกล่าวรวมถึงการสืบค้นสำหรับงานนี้ด้วย แหล่งข้อมูลแรกเกี่ยวข้องกับวงการวิศวกรรมไฟฟ้าและสาขาใกล้เคียงโดยเฉพาะคือ ฐานข้อมูลของสมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ หรือไอทริเปิลอี (IEEE) และต่อมาคือการสืบค้นจากฐานข้อมูลของ Scopus ที่กว้างขวางกว่าครอบคลุมหลายสาขานอกเหนือจากด้านวิศวกรรมไฟฟ้าโดยมีฐานข้อมูลของสาขาและหน่วยงานอื่น ๆ อีกมากที่อาจพบว่าเกี่ยวข้องได้ และสุดท้ายฐานข้อมูลที่เกี่ยวข้องกับวารสารและหนังสือที่อาจมีขอบเขตจำกัดแคบกว่าสองแหล่งแรก แต่ก็เป็นแหล่งข้อมูลเก่าแก่ที่อาจได้พบข้อมูลมุมมองที่แตกต่างแนวอื่นได้คือ ScienceDirect ซึ่งได้นำมาใช้งานและได้ผลดังต่อไปนี้

ก) IEEE Xplore ® Digital Library[15]

สิ่งพิมพ์เผยแพร่และผู้แต่งประพันธ์ของไอทริเปิลอี ได้รับการยอมรับว่าเป็นผู้นำทั้งทางด้านทฤษฎีและด้านปฏิบัติในสาขาเทคโนโลยีที่สำคัญ บทความและมาตรฐานต่าง ๆ ได้ถูกนำมาอ้างอิงมากที่สุดในสิทธิบัตรของประเทศสหรัฐอเมริกา และประเทศในแถบยุโรป[16] นอกจากนี้ วารสารของไอทริเปิลอีก็ยังคงถูกจัดอยู่ในอันดับต้น ๆ ของแต่ละชมรมเทคนิคหรือสาขาวิชา และมีแนวโน้มที่ดีขึ้นทุกปี โดยที่จำนวนงานในระบบฐานข้อมูลของไอทริเปิลอีแบบออนไลน์ หรือ IEEE Xplore ® Digital Library มีสื่อมากกว่า 3.9 ล้านชิ้นแล้ว

---

15 *ieeexplore.ieee.org*

16 *(บทที่ 11) พัฒนาการการประชุมวิชาการวิศวกรรมไฟฟ้าประเทศไทย – ศาสตร์และศิลป์การสร้างสังคมและทรัพยากรมนุษย์ www.ebooks.in.th/ebook/18559/*

ในแต่ละปีไอทริเปิลอีจะจัดงานประชุมวิชาการและงานที่เกี่ยวข้อง (conference & event) จำนวนมากกว่าพันครั้งในทุกสาขาวิชาที่มีสิ่งพิมพ์เผยแพร่ โดยมีจุดมุ่งหมายเพื่อเผยแพร่ผลงานทางวิชาการ แลกเปลี่ยนความรู้และการเจรจาธุรกิจ เป็นต้น ซึ่งสถานที่จัดงานประชุมจะกระจายอยู่ทั่วโลก อันเป็นต้นทางของฐานข้อมูลเพื่อการสืบค้นจำนวนมากดังกล่าว โดยการสืบค้น "รหัสลับเชิงควอนตัม" จากฐานข้อมูลแหล่งนี้มีรายละเอียดและผลดังต่อไปนี้

คำค้น : *Quantum Cryptography*
(สัมพันธ์กับ quantum key distribution & *QKD มีข้อมูลที่ซ้ำซ้อนกันและปรากฏน้อยกว่า)*
ระยะเวลาการค้น : ค.ศ.1981 ถึง เดือนเมษายน ค.ศ. 2016
ขนาดฐานข้อมูลรวม *(29 เมษายน พ.ศ. 2559)* **:** *3,929,418* ชุด

.....

ผลการสืบค้น : ปรากฏ **1,829** ชุดข้อมูล[17]
(Conf. 1,482, *Journal & Mag 339, Book 5, Article 2, และ Course 1)*
เจ้าของผลงานวิชาการสูงสุด 5 อันดับแรก (First five authors list):
1) P.D. Townsend (19)
2) A. J. Shields (19)
3) R. J. Hughes (16)
4) C. G. Peterson (15)
5) J.E. Nordholt (15)
หน่วยงานผลงานวิชาการสูงสุด 5 อันดับแรก (First five affiliations list Affiliation):
1) Los alamos Nat. Lab, USA (7)
2) Telcordia Technol., USA (7)
3) U of Oklahoma, USA (6)
4) Nat. Taiwan U, Taiwan (5)
5) BT Lab, UK (5)
ผลงานจากประเทศไทย: รวมจำนวน 10 บทความประชุมวิชาการ (conf.)

หมายเหตุ: *งานวิจัยด้าน "รหัสลับเชิงควอนตัม" มีพื้นฐานอยู่ในสาขาฟิสิกส์ จึงปรากฏในฐานข้อมูลเทคโนโลยีของ IEEE นี้น้อยมาก*

17 *หมายเหตุคำย่อ: Conf. บทความการประชุมฯ, Journal & Mag วารสารปิยสาร, Article สิ่งพิมพ์, Book หนังสือ และ Course เอกสารการอบรม*

ข) Scopus[18]

นอกเหนือจากของ IEEE ที่เป็นฐานข้อมูลที่เกี่ยวข้องโดยตรงเกี่ยวข้องกับวิศวกรรมไฟฟ้าสื่อสารแล้วนั้น Scopus ฐานข้อมูลที่รวมทั้งด้านวิทยาศาสตร์ เทคโนโลยี การแพทย์ รัฐศาสตร์ ศิลปะ และมนุษยศาสตร์ จากบทความที่ผ่านการพิจารณากลั่นกรอง (peer-reviewed) ของการประชุมวิชาการ หนังสือ และวารสาร ที่มีมากกว่า 22,000 หัวข้อ จากมากกว่า 5,000 สำนักพิมพ์ ฐานข้อมูลวิชาการนี้คืออีกชุดหนึ่งหนึ่งของวงการวิจัยและพัฒนาทั่วโลก แนวทางและผลการสืบค้นจากฐานข้อมูลนี้มีดังนี้

คำค้น : *Quantum Cryptography (สัมพันธ์กับ quantum key distribution & QKD กรองที่ไม่เกี่ยวข้องแล้วด้านสาขาอื่น เช่น สาขาเคมี วัสดุศาสตร์ เป็นต้น)*

หมวด : Article, Title, Abstract, Keywords *(เฉพาะภาษาอังกฤษ)*
ระยะเวลาการค้น : เริ่มมีในระบบฐานข้อมูลปี ค.ศ. 1983 – ค.ศ. 2016
ขนาดฐานข้อมูลรวม *(29 เมษายน พ.ศ. 2559)* **:** มากกว่า 60 ล้านชุด[19]

.....

ผลการสืบค้น : ปรากฏ **17,782** ชุดข้อมูล

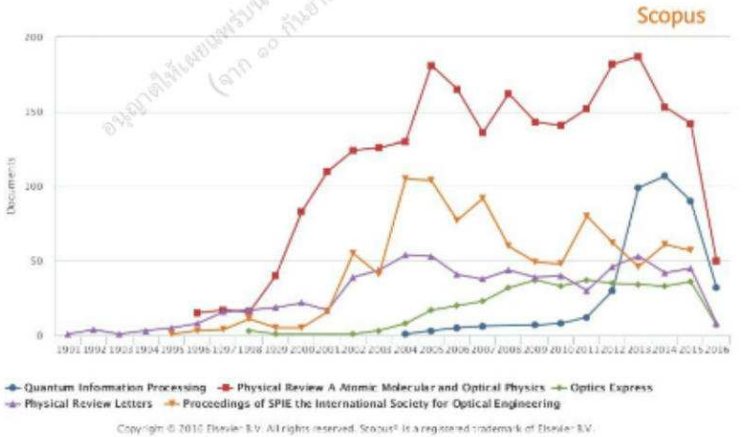
สรุปผล มีสถิติที่ต่างกันมากกับจากที่สืบค้นก่อนหน้าโดย IEEE Xplore ® Digital Library จากฐานข้อมูลของด้านวิศวกรรมศาสตร์นั้น (รหัสลับเชิงควอนตัมยังคงเป็นวิทยาศาสตร์ขั้นพื้นฐานโดยส่วนใหญ่ โดยภาพที่ 1) หลังการกำเนิดวิทยาการรหัสลับเชิงควอนตัมจากการตีพิมพ์ผลงานของ ชาร์ลส์ เบนเนตต์ (Charles Bennett) จากบริษัทไอบีเอ็ม และจิลส์ บราสซาร์ด (Gilles Brassard) จากมหาวิทยาลัยมอลทรีออล ประเทศแคนาดาในปีค.ศ.1984 แล้ว ผลงานที่เกี่ยวข้องจึงได้เริ่มปรากฏสูงขึ้นมาโดยตลอดและมีแนวโน้มสูงมากขึ้น (กรณีท้ายกราฟแสดงผลที่ต่ำลงกว่าปีก่อนหน้านั้นสำรวจถึงเดือนเมษายน ค.ศ. 2016 ซึ่งเมื่อครบทั้งปีแล้วควรได้ผลสูงกว่าเป็นที่แน่นอน) ภาพที่ 2) แหล่งข้อมูลที่ได้รับการตีพิมพ์สูงสุดปรากฏอยู่กับ "Physical review a atomic molecular and optical physics" โดยมี "Quantum Information Processing" เพิ่มสูงขึ้นอยู่ลำดับที่สองในช่วงสามปีก่อนหน้า ส่วนแหล่งอื่น ๆ ด้านแสงหรือทัศนศาสตร์และด้านแขนงวิชาที่เกี่ยวข้องกับฟิสิกส์เชิงควอนตัมจะลดหลั่นลงไป

18 *www.scopus.com*
19 *www.elsevier.com/solutions/scopus/content*

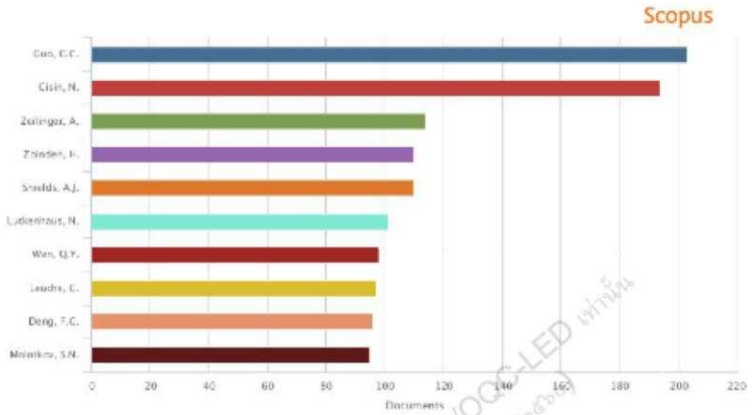
กราฟแสดงผลการสืบค้น *"Quantum Cryptography"*

1) (Year) จำนวนผลงานวิชาการในแต่ละปีที่เริ่มจากค.ศ.1983 ถึง เมษายน ค.ศ.2016

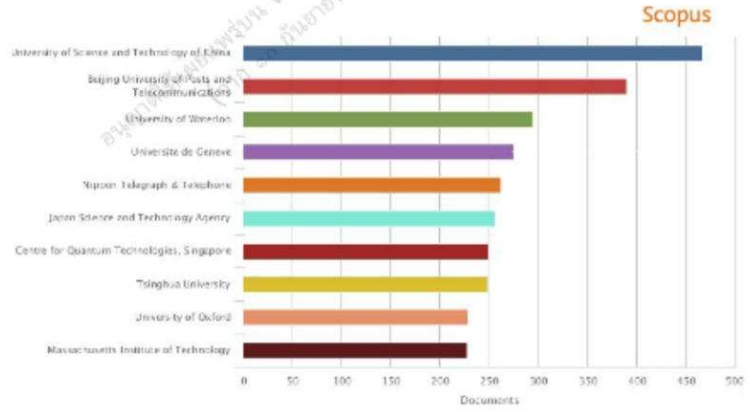
2) (Sources) แหล่งที่มาของข้อมูลวิชาการหรือชื่อวารสารสูงสุดห้าลำดับแรก



3) (Author) สถิติผู้ที่มีจำนวนผลงานวิชาการสูงสุดสิบลำดับแรก



4) (Affiliation) สถิติหน่วยงานที่มีจำนวนผลงานวิชาการสูงสุดสิบลำดับแรก



ข้อสังเกตจากภาพที่ 3) 4) และ 5) คือแหล่งกำเนิดผลงานด้านวิทยาการรหัสลับเชิงควอนตัม โลกเป็นที่ชัดเจนว่าการวิจัยและพัฒนาวิทยาการรหัสลับเชิงควอนตัม ปรากฏชัดเจนอยู่ภายใต้การทำงานของมหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยี (University of Science and Technology of China: USTC) เมืองเหอเฟย (Hefei) มณฑลอันฮุย (Anhui) ซึ่งจัดได้ว่าเป็นเมืองหลวงของวิทยาการรหัสลับเชิงควอนตัมของประเทศจีน[20] เนื่องจากมีทีมงานของนักวิจัยสองกลุ่มหลักของประเทศจีนที่มีชื่อเสียงในระดับโลกนำโดย ศาสตราจารย์ เจิ้งฟู่ หาน (Zheng-Fu Han) และศาสตราจารย์ เจียน เหวย พาน (Jian Wei Pan) โดยมีศาสตราจารย์ เกา (Guo G.C.) เป็นที่ปรึกษาผู้ก่อตั้งยุคบุคเบิกของมหาวิทยาลัยปรากฏเป็นผู้มีผลงานวิจัยมากที่สุดกว่าสองร้อยชิ้นงาน โดยที่บุคคลสำคัญของโลกด้านนี้ปรากฏผลงานตามหลังมาโดยลำดับทั้ง ศาสตราจารย์นิโคลัส จีซิน (Nicholas Gisin) จากมหาวิทยาลัยเจนิวา ประเทศสวิสเซอร์แลนด์ และอันตัน ไซลิงเงอร์ (Anton Zeilinger) จากมหาวิทยาลัยเวียนนา ประเทศออสเตรีย เป็นต้น ซึ่งสังเกตได้ว่าศาสตราจารย์ เกา จากประเทศจีนนั้นคืออดีตผู้บริหารเป็นที่นับถือในวงการภายในของประเทศจีนเป็นอย่างมากด้านการจัดหางบประมาณวิจัย และการประสานความร่วมมือกับภาครัฐ แต่มิได้เป็นผู้ปรากฏตัวในแวดวงวิชาการของโลกด้วยตนเองแต่อย่างใด

หมายเหตุ: *ซึ่งทั้งสองกลุ่มวิจัยของ USTC นี้ ได้นำเสนอผลงานการทดสอบระบบวิทยาการรหัสลับเชิงควอนตัมหลายโครงการใหญ่ จนได้รับการบันทึกไว้เป็นความก้าวหน้าสำคัญไปทั่วโลก อาทิ กลุ่มวิจัยของศาสตราจารย์เจิ้งฟู่ หาน ได้ทดสอบระบบเครือข่ายสำหรับหน่วยงานของรัฐบาลเพื่อใช้งานสำหรับการเข้ารหัสภาพ วีดีโอ เสียงและเอกสารต่าง ๆ ผ่านเส้นใยนำแสงทั้งหมดสี่โครงข่ายหลักในเขตตัวเมืองอู่หู มณฑลอันฮุย[21] ส่วนกลุ่มของศาสตราจารย์เจียน เหวย พาน ที่มีความร่วมมือใกล้ชิดกับกลุ่มเวียนนา (ประเทศออสเตรีย) มีผลงานเทคนิคความพัวพัน (entanglement) และการส่งถ่ายเชิงควอนตัม (teleport)[22] และกำลังเริ่มต้นโครงการการส่งกุญแจรหัสลับผ่านดาวเทียม[23] โดยที่กลุ่มของศาตราจารย์เจิ้งฟู่ หาน มีความร่วมมือและผลงานร่วมช่วงเริ่มต้นกับกลุ่มวิจัยในประเทศไทย ที่ยังคงต้องเร่งประสานขอรับการถ่ายทอดเทคโนโลยีมากขึ้นต่อไป*

---

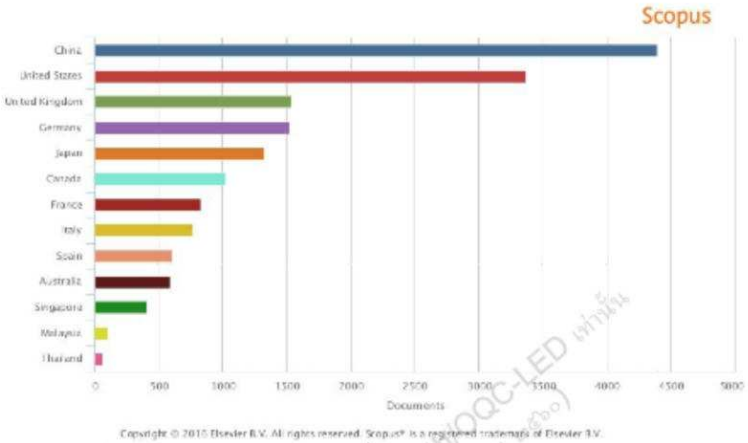
20 *สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗) ISBN: 978-616-374-830-0 หน้า 39 และจากการเยี่ยมชมงานเมื่อปี พ.ศ.2556*

21 *F. Xu, et al., "Field experiment on a robust hierarchical metropolitan quantum cryptography network," Chinese Science Bulletin, vol. 54, no. 17, pp. 2991 – 2997, September 2009. http://arxiv.org/abs/0906.3576*

22 *arxiv.org/abs/1205.2024v1*

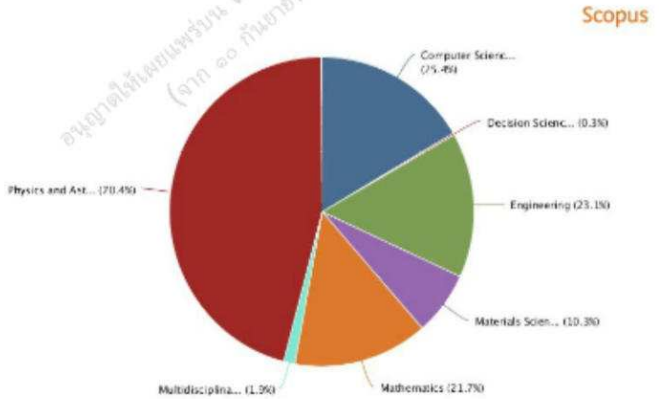
23 *www.nature.com/news/data-teleportation-the-quantum-space-race-1.11958 : http://quantum.ustc.edu.cn/*

5) (Country/ Territory) สถิติประเทศที่มีจำนวนผลงานสูงสุดสิบลำดับแรก และอาเซียน



(ประเทศไทยพบมี 65 ชุดข้อมูลอยู่อันดับที่ 39 น้อยกว่าสิงคโปร์ (409 ชุด อันดับ 15) และมาเลเซีย (105 ชุด อันดับ 32))

6) (Subject) สาขาวิชาที่เกี่ยวข้อง (แสดงอัตราส่วนสาขาซ้อนทับกัน)



ข้อสังเกตเพิ่มเติม สำหรับประเทศจีนมิได้มีเพียงมหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยี (USTC) เท่านั้นที่ขะมักเขม้นกับวิทยาการด้านสารสนเทศเชิงควอนตัมนี้ ยังมีแหล่งใหญ่อื่นอีกมากทั้ง มหาวิทยาลัยไปรษณีย์และโทรคมนาคมแห่งกรุงปักกิ่ง (Beijing university of posts and telecommunications) และมหาวิทยาลัยชิงหัว (Tsinghua University) และอื่น ๆ จึงทำให้ ณ พ.ศ.2559 ประเทศจีนได้ก้าวมามีบทบาทอยู่แถวหน้าของวงการวิจัยและพัฒนา และเมื่อประกอบกับข้อมูลด้านต้นแบบผลิตภัณฑ์ การสาธิตโครงการขนาดใหญ่ต่อสาธารณะและการจัดประชุมวิชาการที่เกี่ยวข้องอีกมากด้วยแล้ว เป็นการยืนยันสถานะผู้นำด้านวิชาการของประเทศจีนกับวิทยาการรหัสลับเชิงควอนตัมได้ชัดเจนที่สุด

และอีกหนึ่งข้อสังเกตของการพัฒนาโครงสร้างพื้นฐานตามแนวทางการการนำ**นโยบาย**และ**งบประมาณ** สองปัจจัยหลักที่เข้มแข็งมากของประเทศสิงคโปร์ก็ได้ปรากฏผลการเหนี่ยวนำเอา**บุคลากร**จากต่างชาติมาปักหลัก ณ เกาะสิงคโปร์เป็นจำนวนมากพร้อมกับผลงานวิจัยจากศูนย์วิจัยเทคโนโลยีควอนตัม (Centre for Quantum Technologies) ที่บ่งบอกถึงการสร้าง**วิทยาการ**ภายในประเทศเองได้สูงขึ้นอย่างมากและสำเร็จได้ในเวลาที่รวดเร็ว

ซึ่งทั้งสองรูปแบบของสองประเทศตัวอย่างนี้ ได้นำเสนอเป็นแนวทางกรณีศึกษาไว้ก่อนและได้ปรากฏผลชัดเจนขึ้นมากแล้วเช่นกัน[24] อันเป็นแนวทางที่ประเทศไทยควรได้เร่งศึกษาและแสวงหาความร่วมมือต่อไปด้วย[25]

สำหรับประเทศในเขตเศรษฐกิจอาเซียนประเทศไทยพบมี 65 ชุดข้อมูลอยู่อันดับที่ 39 น้อยกว่าสิงคโปร์ (จำนวน 409 ชุด อันดับ 15) และมาเลเซีย (จำนวน 105 ชุด อันดับ 32)) แต่ในจำนวนที่ปรากฏมีอยู่ที่น้อยมากเหล่านั้น ก็ยังได้พบปรากฏการณ์เช่นเดียวกับประเทศกำลังพัฒนาอื่น ๆ จำนวนมากที่มีผลงานวิชาการแปลกปลอมที่อาศัยศักยภาพของคำว่า “กลศาสตร์ควอนตัม” ไปอ้างอิง[26] ซึ่งทั่วโลกก็ได้มีการรายงานการตรวจสอบทั้งการเลือกเสนอข้อมูลเพียงบางส่วน (falsification) และการสร้างผลวิจัยเทียมหรือปลอม (fabrication) มากขึ้น ดังนั้น ในขณะที่ประเทศไทยมีสถานะของดัชนีการแข่งขันที่ต่ำมากอยู่นี้ อาจมิเพียงแค่ต้องเร่งปรับปรุงเพื่อให้มีจำนวนเพิ่มขึ้นเท่านั้น แต่อาจต้องกลับมาแก้ไขปัญหาผลงานวิชาการแปลกปลอมเหล่านั้นเป็นวาระที่สำคัญไม่ยิ่งหย่อนกว่ากัน

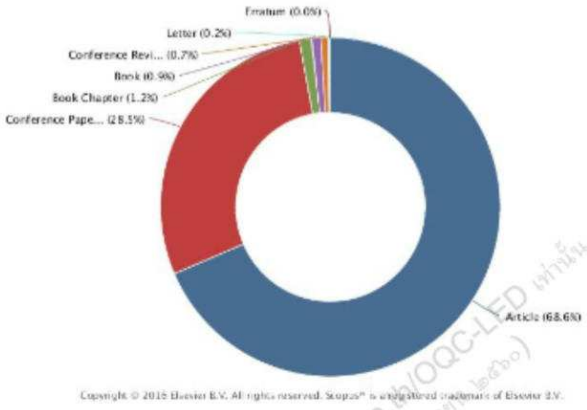
24 *สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗) ISBN: 978-616-374-830-0 หน้า 42*

25 *White paper 2016: ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed 2016) Q-Thai.Org*

26 *โอกีควอนตัมไทยประดิษฐ์ (4) : รู้ไหม ? (www.dailynews.co.th/article/385660) โอกีควอนตัมถูกแฮก (3) : Quantum Hacking ? (www.dailynews.co.th/article/384306) เงิน - โอกีควอนตัมจำแลง (2) : หลงวิชาการ (www.dailynews.co.th/article/382721) ควอนตัมหลอกลวง (1) : "หลง รู้ พลาด ติดบ่วง ขอพ่วงหน่อย" (www.dailynews.co.th/article/381252)* **หรือบันทึกสำรอง ณ Q-Thai.Org**

7) (Document Type) สถิติประเภทของผลงานวิชาการ

Scopus



ความก้าวหน้าของวงการวิทยาการรหัสลับเชิงควอนตัมของโลก ได้ปรากฏอยู่กับทั่วทุกภูมิภาค แม้แหล่งกำเนิดจะเริ่มต้นขึ้นที่ประเทศแถบตะวันตกที่สั่งสมความรู้ด้านสาขากลศาสตร์ควอนตัมมาเป็นเวลานานร่วมศตวรรษแล้วนั้น หากแนวโน้มเริ่มมาปรากฏความก้าวหน้ามากขึ้นในโลกฝั่งตะวันออกทั้งจากประเทศจีน ญี่ปุ่นและสิงคโปร์ รวมทั้งความก้าวหน้าที่น่าทึ่งในช่วงเวลาที่สั้นมากของประเทศเกาหลีใต้[27] แม้จะยังไม่ปรากฏผลงานด้านวิชาการเทียบเท่าสามประเทศเอเชียดังกล่าวแต่ได้ปรากฏต้นแบบเพื่อการจำหน่ายแล้ว

สำหรับข้อมูลผลงานวิจัยเหล่านี้ดังภาพที่ 6) และ 7) อยู่ในหมวดหมู่ที่ประเมินได้ว่ายังอยู่ในขั้นพื้นฐาน และเกี่ยวโยงกับด้านสาขาวิชาฟิสิกส์ถึง 70% โดยการประยุกต์กับสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมศาสตร์คาบเกี่ยวที่ 25% และ 23% โดยลำดับ

จากผลการสำรวจจากฐานข้อมูล Scopus ปรากฏผลโดยรวมคือ วิทยาการด้านนี้กำลังสร้างฐานที่แข็งแกร่งขึ้นทุกปีโดยลำดับ โดยมีประเทศในแถบเอเชียนำโดยประเทศจีนเป็นผู้มีความก้าวหน้าของวงการวิชาการสูงที่สุด

27 *www.dailynews.co.th/article/353827 และ www.dailynews.co.th/article/355248 และ Q-Thai.org*

ค) ScienceDirect[28]

ฐานข้อมูลนี้ บรรจุวาสารทางด้านวิทยาศาสตร์พื้นฐานและสุขภาพ เป็นอีกแหล่งที่สำคัญที่มีขนาดไม่ใหญ่มากเท่า Scopus จึงอาจปรากฏเป็นเพียงส่วนเสริมได้ขึ้นอีกเล็กน้อยจากฐานข้อมูลแหล่งนี้

คำค้น : *Quantum Cryptography*
(สัมพันธ์กับ quantum key distribution & QKD แต่พบน้อยมากไม่มีนัยสำคัญ)
ระยะเวลาการค้น : ค.ศ.1997 จนถึงปี ค.ศ. 2016
ขนาดฐานข้อมูลรวม *(29 เมษายน พ.ศ. 2559)* **:** มากกว่า 14 ล้านชุดข้อมูล จากฐานวารสารมากกว่า 3,800 หัวเรื่อง และหนังสือมากกว่า 35,000 เล่ม

.....

ผลการสืบค้น : ปรากฏ **2,059** ชุดข้อมูล โดยเป็นข้อมูลจากวารสาร (Journal) (1,842) หนังสือ (Book) (326) งานอ้างอิงอื่น ๆ (Reference work) (21)

ปี	จำนวน	หมายเหตุ
2016	67	*(ถึงเดือนเมษายน)*
2015	128	
2014	142	
2013	120	
2012	110	
2011	**152**	
2010	129	
.....		
1997	23	

อนึ่ง ปรากฏมีข้อมูลผลงานจากประเทศไทย 36 ชุดงาน โดยเป็นวารสาร (Journal) 33 และหนังสือ (Book) 3 งานอ้างอิงอื่น ๆ (Reference work) จำนวน 1 ชุด

28 *www.elsevier.com/solutions/sciencedirect*

สรุป ข้อมูลงานวิจัยและพัฒนาจากทั้งสามแหล่งของการสำรวจ คือ ก) IEEE Xplore ข) Scorpus ค) Science Direct โดยปรากฏข้อมูลใน IEEE Xplore ® Digital Library เพียง **1,829** ชุดข้อมูล ซึ่งแหล่งข้อมูลนี้เป็นผลงานส่วนใหญ่จากบุคลกรและหน่วยงานด้านวิศวกรรมการสร้างผลิตหรือประยุกต์ ส่วนฐานของ Scopus ปรากฏมี **17,782** ชุดข้อมูล มีนัยสำคัญกว้างขวางกว่ามาก โดยเป็นผลงานส่วนใหญ่ของบุคลกรและหน่วยงานด้านวิชาการหรือมหาวิทยาลัย และสุดท้ายข้อมูลจากฐาน ScienceDirect แหล่งนี้มีนัยสำคัญน้อยเชิงจำนวน **2,059** และไม่ปรากฏนัยสำคัญที่จะสกัดผลเพื่อนำเสนอได้ชัดเจนนัก

โดยผลการสำรวจข้อมูลด้านงานวิจัยและพัฒนาเหล่านี้ สะท้อนสถานะเชิงวิชาการอันเป็นที่สาขา "รหัสลับเชิงควอนตัม" ยังคงอยู่ในระดับพื้นฐาน สอดคล้องกับสำรวจด้านพัฒนาการก่อนหน้า[29] โดยชัดเจนว่าประเทศประเทศจีนเป็นผู้มีความก้าวหน้าสูงที่สุดของวงการวิชาการด้านนี้

29 *สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๙) ISBN: 978-616-374-830-0*

ตัวอย่างการวิเคราะห์สิทธิบัตร 3

[30]จากข้อมูลของ องค์การทรัพย์สินทางปัญญาโลก (World Intellectual Property Organization: WIPO) ที่มีสำนักงานใหญ่อยู่ ณ กรุงเจนิวา ประเทศสวิสเซอร์แลนด์ ระบุว่า ในปีพ.ศ.2558 สถานะภาพทรัพย์สินทางปัญญาโดยรวมของโลกนั้น ประเทศสหรัฐอเมริกายังคงเป็นผู้นำกับจำนวนการคำขอจดสิทธิบัตรซึ่งสูงสุดอย่างต่อเนื่องมาเป็นเวลาเกือบสี่ทศวรรษแล้ว ตามมาด้วยประเทศญี่ปุ่นและจีน[31] ทั้งนี้ การยื่นขอมีอัตราการเติบโต 1.7% จากของปีก่อนหน้า สำหรับตัวเลขของปี พ.ศ. 2558 นั้น มีการยื่นขอของหน่วยงานจากประเทศสหรัฐฯ สูงถึง 57,385 สิทธิบัตร โดยลดลง 6.7% จากปีก่อนหน้า ส่วนประเทศญี่ปุ่นไล่หลังมาที่จำนวน 44,235 และประเทศจีนอยู่ที่ 29,846 สิทธิบัตร

เมื่อพิจารณาในรายละเอียดระดับประเทศพบว่า จีนนั้นมีอัตราการเติบโตสูงมากและสูงที่สุด ตามมาด้วยอัตราของประเทศเกาหลีใต้ อิสราเอล สวิสเซอร์แลนด์ ญี่ปุ่นและเนเธอร์แลนด์ ซึ่งสังเกตได้ว่าเป็นแนวโน้มที่การเติบโตมาจากฟากเอเชียมากขึ้น และเมื่อสังเกตลึกลงไปก็พบว่าบริษัทด้านกิจการโทรคมนาคมของประเทศจีน นั่นคือ บริษัทหัวเหว่ย (Huawei) เป็นผู้นำมาได้สองปีแล้วสำหรับอัตราการเติบโตระดับรายย่อยสูงสุด ซึ่งก็ได้นำหน้าบริษัทดังด้านโทรคมนาคมอื่น ๆ ทั้งของสหรัฐฯ คือ ควอลคอม (Qualcomm) และบริษัทของประเทศจีนเองอีกรายหนึ่ง นั่นคือ แซททีอี (ZTE)

ทั้งนี้ หากศึกษาข้อมูลย้อนหลังไปช่วงวิกฤติเศรษฐกิจโลกตั้งแต่ก่อน ปี พ.ศ.2553 มานั้น ประเทศจีนได้เริ่มมีการเติบโตของสิทธิบัตรสวนกระแสมาก่อนแล้ว โดยผู้อำนวยการ WIPO (Francis Gurry) เคยได้กล่าวถึงความน่าทึ่งในการเติบโตด้านทรัพย์สินทางปัญญาของประเทศในแถบเอเชียตะวันออกอันหมายถึง จีน เกาหลีใต้และญี่ปุ่นด้วยเช่นกัน ซึ่งช่วงเวลา

30 *ข้อมูลส่วนเกริ่นนำและคำจำกัดความด้านสิทธิบัตรรวมถึงระบบฐานข้อมูล Thomson Innovation (DWPI) ของรายงานนี้ ใช้ฉันละนำเสนอร่วมกับกับรายงานชิ้นอื่น ๆ ของสมาคมวิชาการ ECTI (LED-SmartCoN.Org)*

31 *องค์การทรัพย์สินทางปัญญาโลก (WIPO) (www.wipo.int/portal/en/) คือหน่วยงานความร่วมมือระดับโลกด้านทรัพย์สินทางปัญญาสำหรับนโยบาย บริการ ข่าวสารและความร่วมมือ โดยเป็นหน่วยพิเศษขององค์การสหประชาชาติ (United Nations) ได้ความช่วยเหลือ 188 ประเทศสมาชิกทั่วโลก*

นั้นประเทศจีนก็ได้นำหน้าทั้งประเทศอังกฤษและฝรั่งเศสที่เคยอยู่ในลำดับต้นของโลกมาก่อน บริษัทพานาโซนิกของญี่ปุ่นและ ZTE ของจีนก็เคยอยู่ในลำดับต้น ก่อนที่บริษัทหัวเหว่ยจะได้กลายมาเป็นหน่วยงานรายย่อยที่มีอัตราการเติบโตที่สูงและขึ้นนำในเวลาต่อมา

ดังนั้น จึงเป็นที่ทราบกันชัดเจนแล้วว่า **ประเทศจีน**กับแนวทาง**อุตสาหกรรมโทรคมนาคม**ของปี พ.ศ.2559 คือจุดสนใจหรือสองคำสำคัญ (key words) หลัก เมื่อได้ศึกษาถึงหัวข้อทรัพย์สินทางปัญญาภาพรวมขนาดใหญ่ระดับโลกเหล่านี้ และการสืบค้นสำหรับภารกิจการวิเคราะห์สิทธิบัตรของสาขา"รหัสลับเชิงควอนตัม"เป็นการเฉพาะต่อไปนี้ ก็ปรากฏผลข้อมูลความเชื่อมโยงกับทั้งสองคำสำคัญดังกล่าว อันเป็นทั้งแขนงหนึ่งของวิศวกรรมโทรคมนาคมที่มีจำนวนสิทธิบัตรของโลกกำลังเติบโตสูงที่สุด และมีอัตราการเติบโตสูงสุดที่ยืนตุ้มครองมาจากประเทศจีนนั่นเอง

ทั้งนี้ แนวทางที่ใช้ในการศึกษามีเครื่องมือสืบค้นข้อมูลอยู่มาก ทั้งจากหน่วยงานนานาชาติของ WIPO ซึ่งเป็นข้อมูลรวมของทั้งประเทศสมาชิกทั้งหมด จนถึงฐานข้อมูลแนวกว้างที่เปิดบริการเป็นสาธารณะของกูเกิล (Google patent)[32] ส่วนรายงานฉบับนี้เลือกใช้ของ Thomson Innovation อันมี DWPI หรือ Derwent World Patents Index[33] ที่มีความน่าเชื่อถือสูง การสำรวจสืบค้นเรื่อง quantum cryptography จึงได้ทำการจากเอกสารสิทธิบัตรของ Thomson Innovation[34] นี้ โดยจะทราบถึงความก้าวหน้าของการวิจัยและอื่น ๆ ในเรื่องนี้ของประเทศต่าง ๆ ทั่วโลก ที่มีการยื่นขอความคุ้มครองผลงานการประดิษฐ์คิดค้นเหล่านั้น และโดยเฉพาะระบบที่ใช้งานนี้มีเครื่องมือช่วยในการวิเคราะห์ (analysis tools) มากพอสมควรที่จะได้ทำให้หัวข้อของการวิเคราะห์มีความหลากหลาย น่าสนใจ และเกิดประโยชน์รอบด้าน

อนึ่ง ความรู้พื้นฐานด้านสิทธิบัตรทั่วไป สามารถศึกษาได้จากข้อมูลของกรมทรัพย์สินทางปัญญา (https://www.ipthailand.go.th/)

3.1 วิธีการสืบค้น

การสืบค้นเอกสารสิทธิบัตร"รหัสลับเชิงควอนตัม"ดังกล่าวมีรายละเอียดขั้นตอน จากระบบฐานข้อมูลสิทธิบัตร Thomson Innovation คือ

32 *google.com/patents*

33 *ip.thomsonreuters.com/training/derwent-world-patents-index*

34 *Thomson Innovation ฐานข้อมูล สิทธิบัตรของ Derwent มากกว่า 22 ล้านการคิดค้นหากนับตั้งแต่ปี ค.ศ. 1963 สามารถสืบค้นสิทธิบัตรจากภาษาท้องถิ่นที่มิใช่ภาษาอังกฤษด้วยโดยแปลผลร่วมอยู่ในฐานข้อมูลเดียวกันนี้ เช่น ภาษาจีน ภาษาญี่ปุ่น หรือภาษาเกาหลี เป็นต้น (www.thomsonreuters.com/innovation)*

คำค้น:

ใช้คำค้นที่เป็นเอกลักษณ์ : ***Quantum Cryptography***

การจำกัดผลลัพธ์ด้วย : *หัวข้อ บทคัดย่อ และข้อถือสิทธิ* - ***Title/Abstract/Claims***

เสนอผลลัพธ์ในรูปแบบ:

Text Clustering อันมีความหมายคือ กลุ่มคำที่เกิดจากเทคนิค Text Mining algorithm แสดงผลกลุ่ม/ชุดคำที่สำคัญที่พบจำนวนมาก (word occuring) ที่ปรากฏในเอกสารสิทธิบัตร จัดเรียงลำดับตาม Main Clustering และ Sub Clustering

ThemeScape ซึ่งหมายถึง เครื่องมือหรือแนวทางในการสังเกตการณ์ (visualization tool) ที่สามารถใช้วิเคราะห์เอกสารสิทธิบัตรออกมาเป็นรูปแผนที่หรือภูมิประเทศ เพื่อการนำเสนอ หัวข้อ/ ประเด็นหลัก (Theme) และแสดงถึงความสัมพันธ์ในระหว่างชุดเอกสารที่สำรวจ โดยการใช้ประโยชน์จะสามารถนำมาช่วยหาความสัมพันธ์อื่น ๆ ได้ด้วย คือ Technology Segmentation / Portfolio overview / Interactive "Bird's eye view" Map เป็นต้น

สถิติต่าง ๆ เช่น อันดับจำนวนแยกตามประเทศ ผู้ประดิษฐ์ หน่วยงาน และหมวดหมู่สาขาวิชาของสิทธิบัตร ตามระบบ IPC (International Patent Classification[35]) เป็นหลัก

3.2 ผลลัพธ์และการวิเคราะห์

จากการสำรวจปี พ.ศ. 2559 พบสิทธิบัตรที่เกี่ยวข้องผ่านการกลั่นกรองการซ้ำซ้อนแล้วที่ **827** เรื่อง (280 DWPI Families) ชุด จากทั่วโลกทุกภาษาที่ระบบรองรับ

ทั้งนี้ ผลลัพธ์ได้จัดเรียงการนำเสนอดังนี้คือ *เจ็ดสิทธิบัตรตัวอย่างเด่น การวิเคราะห์สิทธิบัตรเบื้องต้นกับตัวอย่างพิเศษ การวิเคราะห์กลุ่มคำในเอกสารสิทธิบัตร แผนที่สิทธิบัตร (ThemeScape) และบทสรุป* ดังรายละเอียดต่อไปนี้

35 *International Patent Classification: แต่มีสิทธิบัตรหลายชั้นที่มีความใหม่มาก เริ่มมีการอ้างถึง COOPERATIVE PATENT CLASSIFICATION หรือ CPC ระบบการจำแนกสิทธิบัตรของกลุ่มสหภาพยุโรปและสหรัฐอเมริกาบ้างแล้ว*

3.1.1 เจ็ดสิทธิบัตรตัวอย่างเด่น

สิทธิบัตรที่เกี่ยวข้องกับคำค้น **Quantum Cryptography** จำนวนตัวอย่าง 7 เรื่อง อันมีแนวทางการนำเสนอข้อมูลเชิงเทคนิคพื้นฐานสำคัญ ได้กลั่นกรองมาเพื่อเป็นตัวอย่างของรายงานการวิเคราะห์ และเป็นแนวทางรูปแบบเปิดสาธารณะเพื่อการร่วมกันสืบค้น สกัดความรู้สู่การพัฒนาขยายผลต่อให้เกิดประโยชน์ในประเทศต่อไปในวงกว้าง (เสนอตั้งหัวข้อ **"สังคมสิทธิบัตร – รหัสลับเชิงควอนตัม"** ด้านท้ายหัวข้อนี้) โดยมีตัวอย่างดังนี้

ตัวอย่าง 1) US2014/0119537A1*

LEGRE MATTHIEU**

2014-01-14

H04L 9/08

Title: APPARATUS AND METHOD FOR THE DETECTION OF ATTACKS TAKING CONTROL OF THE SINGLE PHOTON DETECTORS OF A QUANTUM CRYPTOGRAPHY APPARATUS BY RANDOMLY CHANGING THEIR EFFICIENCY

DWPI Title: Quantum cryptography apparatus has subsystem which processes the inputs of random changes in at least one setting parameter of single photon detector, and compares measured detection probability values so as to detect active attacks.

Abstract: An apparatus and method for revealing both attack attempts performed on the single-photon detector(s) of a quantum cryptography system and Trojan horse attack attempts performed on quantum cryptography apparatus containing at least one single photon detector. The attacks detection relies on both the random modification of the setting parameters of the said single-photon detector(s) and the comparison of the measured detection probability values for each setting parameter with the expected detection probability values. The modified parameter of the single-photon detector can be its efficiency or its timing of activation for example.

** สิทธิบัตรล่าสุดของบริษัท ID Quantique นี้ เกี่ยวข้องกับ quantum hacking (บทที่ 5)*

*** ดร.แมทธิว จบการศึกษาและเชี่ยวชาญด้านด้านรหัสลับควอนตัมโดยตรง เป็นบุคลากรรุ่นที่สองของหน่วยงาน เคยมาประจำที่เมืองไทยสองรอบในการถ่ายทอดความรู้*

ตัวอย่างแนวทางการศึกษาสิทธิบัตร 1)

US2014/0119537A1 ..... *(หมายเลขสิทธิบัตร ณ สหรัฐอเมริกา)*

LEGRE MATTHIEU ..... *(นอกจากผู้ประดิษฐ์ชื่อแรกแล้วยังมี Grégoire Ribordy เจ้าของบริษัท iDQuantique เป็นผู้ร่วมยื่นจด)*

2014-01-14 ..... *(วันที่ได้รับการประกาศ หรือ Publication date)*

H04L9/08 [36] ..... *(หมายเลขการจัดจำแนกสิทธิบัตรระหว่างประเทศ COOPERATIVE PATENT CLASSIFICATION (CPC) ซึ่งสิทธิบัตรนี้อยู่ในกลุ่ม **Key Management หรือการบริหารจัดการกุญแจรหัสลับ**)*

Title: ..... *(ชื่อสิทธิบัตร **อุปกรณ์และวิธีการสำหรับควบคุมตรวจจับการบุกรุกหน่วยรับแสงโฟตอนเดี่ยว ของรหัสลับเชิงควอนตัมโดยการปรับเปลี่ยนค่าประสิทธิภาพแบบสุ่ม**)*

DWPI Title: ..... *(ชื่อที่ได้รับการจัดแปลงเชิงขยายให้เข้ากับฐานข้อมูลระบบของ Thomson Innovation (DWPI) จากการวิเคราะห์ของระบบเพื่อการสืบค้นจากเทคนิคการซ่อนประเด็นหรืออื่น ๆ ของผู้ประดิษฐ์ โดยตั้งขึ้นใหม่แนวทางการอธิบายโดยสังเขปคือ **"อุปกรณ์ของระบบรหัสลับเชิงควอนตัมอันมีระบบย่อยที่ทำการปรับค่าแบบสุ่มอย่างน้อยหนึ่งค่า เพื่อใช้ตั้งค่าของหน่วยตรวจจับโฟตอนเดี่ยวแล้วเทียบเคียงกับค่าโอกาสการตรวจจับที่ทำการวัดได้ เพื่อภารกิจค้นหาการบุกรุกเชิงรุก"**)*

Abstract: ..... บทคัดย่อ: อุปกรณ์และวิธีหนึ่งของระบบรหัสลับเชิงควอนตัมเพื่อการค้นหาทั้งความพยายามในการโจมตีระบบยังหน่วยตรวจจับสัญญาณแสงโฟตอนเดี่ยว และม้าโทรจัน (ซึ่งวิธีการซ่อนตัวในระบบ) ในเครื่องมือของระบบที่มีหน่วยตรวจจับอย่างน้อยหนึ่งชุด การค้นหาการบุกรุกนั้นกระทำทั้งการปรับแปลงค่าตัวแปรที่เกี่ยวข้องแบบสุ่มเพื่อใช้ตั้งค่าของหน่วยตรวจจับโฟตอนเดี่ยว แล้วเทียบเคียงกับค่าโอกาสการตรวจจับที่ทำการวัดได้ สำหรับการปรับตั้งค่าให้เหมาะกับค่าโอกาสที่คาดว่าจะพบการบุกรุกใด ๆ ค่าที่ปรับนั้นมีดังเช่น ค่าประสิทธิภาพของระบบ ช่วงเวลาการกระตุ้นหรือทำงาน เป็นต้น

36 *COOPERATIVE PATENT CLASSIFICATION หรือ CPC คือ ระบบการจำแนกสิทธิบัตรของกลุ่มสหภาพยุโรป และสหรัฐอเมริกา (European Patent Office (EPO) and the United States Patent and Trademark Office (USPTO)) มีความละเอียดมากขึ้นกว่าของ WIPO (IPC) โดยที่ H04L9/08 คือ กลุ่มใหญ่เสื่อรองรับงานด้านรหัสลับโดยเฉพาะ (or management, e.g. generation, sharing or updating, of cryptographic keys or passwords)*

ตัวอย่าง 2) WO2014058150A1
SK TELECOM CO LTD
2013-08-21
G06F 7/58

Title: RANDOM NUMBER GENERATING METHOD AND APPARATUS USING LIGHT SOURCE AND SINGLE PHOTON DETECTOR.

DWPI Title: Random-number generation apparatus e.g. true random number generator for use in quantum cryptography field, has light source symmetrically emitting luminous flux in central axis, and single photon detectors located in light source.

Abstract: The present invention relates to a random number generating method and apparatus using a light source and a single photon detector. According to an aspect of this embodiment, there is provided the random number generating apparatus that generates a random number and includes: a light source that emits luminous flux, the light intensity distribution of which is symmetrical with respect to a central axis; and a plurality of single photon detectors that are positioned radially apart from each other from an extending line of the central axis of the light source to generate a bit value of either 0 or 1 depending on whether a photon is detected or not.

หมายเหตุ
สิทธิบัตรของ SK TELECOM CO LTD สังเกตได้ว่ามีอีกจำนวนมากในช่วงเวลาไล่เลี่ยกัน เช่น WO2014069773A1 2013-08-21 H04L 9/12 Title: METHOD AND APPARATUS FOR GENERATING AND PROCESSING QUANTUM SIGNAL IN REGULAR FRAME UNIT FOR QUANTUM ENCRYPTION KEY DISTRIBUTION เป็นต้น สอดคล้องกับการนำเสนอต้นแบบสู่สาธารณะในช่วงปีเดียวกัน

ตัวอย่างแนวทางการศึกษาสิทธิบัตร 2)
(สิทธิบัตรต้นฉบับภาษาเกาหลี และยื่นจดร่วม ณ ประเทศจีนและสหรัฐอเมริกา)

WO2014058150A1 .... *(หมายเลขสิทธิบัตรขององค์การทรัพย์สินทางปัญญาโลก (WIPO))*
SK TELECOM CO LTD ..... *(โดย บริษัท เอสเค เทเลคอม ผู้ให้บริการระบบสื่อสารรายใหญ่ของประเทศเกาหลีใต้)*
2014-08-17 ..... *(วันที่ได้รับการประกาศ หรือ Publication date (ยื่น 2013-08-21)*
G06F 7/58 [37] ..... *(หมายเลขการจัดจำแนกสิทธิบัตร กลุ่มการสุ่มหรือการสุ่มหมายเลขแบบเทียม (**Random or pseudo-random number generators**))*

Title: ..... *(ชื่อสิทธิบัตรแปล: **วิธีการและอุปกรณ์สร้างจำนวนสุ่มโดยใช้แหล่งกำเนิดแสงและหน่วยตรวจจับโฟตอนเดี่ยว**)*
DWPI Title: ..... *(ชื่อที่ได้รับการจัดแปลงเชิงขยายให้เข้ากับฐานข้อมูลระบบของ Thomson Innovation (DWPI)**อุปกรณ์สร้างจำนวนสุ่ม เช่น จำนวนสุ่มแท้ เพื่อการใช้งานในงานรหัสลับเชิงควอนตัม โดยมีแหล่งกำเนิดแสงที่ให้ความเข้มสว่างที่สมมาตรกับแกนกลาง แล้วมีหน่วยตรวจจับแสงโฟตอนเดี่ยวติดตั้งในแหล่งกำเนิดแสงนั้น**)*

Abstract : ..... บทคัดย่อ: สิ่งประดิษฐ์นี้เกี่ยวข้องกับวิธีและอุปกรณ์การสร้างจำนวนสุ่มโดยใช้แหล่งกำเนิดแสงและหน่วยตรวจจับโฟตอนเดี่ยว โดยภาพรวมของสิทธิบัตรนี้มีอุปกรณ์สร้างจำนวนสุ่มที่ให้กำเนิดจำนวนสุ่มประกอบด้วย แหล่งกำเนิดแสงที่ให้ความเข้มสว่างที่สมมาตรกับแกนกลาง แล้วมีหน่วยตรวจจับแสงโฟตอนเดี่ยวติดตั้งในแหล่งกำเนิดแสงนั้นจำนวนหนึ่ง ติดตั้งในช่วงระยะห่างจากกันบนแกนกลางร่วมที่แหล่งกำเนิดแสงนั้นติดตั้งอยู่และให้ค่าจำนวนใด ๆ คือ "ศูนย์" หรือ "หนึ่ง" ออกมา ทั้งนี้ขึ้นอยู่กับว่าหน่วยตรวจจับโฟตอนเดี่ยวตรวจรับว่ามีโฟตอนหรือไม่ตามลำดับ

หมายเหตุ: *จำนวนสุ่มใช้เพื่อการเป็นชุดจำนวนเริ่มต้น (seed) เพื่อการใช้สร้างเป็นชุดรหัสลับ หากจำนวนสุ่มมีความเข้มแข็งต่อการคาดเดาหรือคำนวณหาได้ยาก รหัสลับนั้นจะมีความปลอดภัยสูง*

37 worldwide.espacenet.com/classification?locale=de_EP#!/CPC=G06F7/58

ตัวอย่าง 3) US8693685B2

TAPSTER PAUL RICHARD*
2007-08-04
H04K 1/00

Title: Quantum cryptography apparatus.

DWPI Title: Quantum cryptographic receiver has gating unit with electronic clock for generating timing signal and gating signal derived from timing signal.

Abstract: A timing and synchronization apparatus and method for a quantum cryptography system is disclosed. A gating pulse is generated by a clock and synchronized to the receipt of transmitted photons at the detector. The apparatus is arranged to only accept photon detection events occurring during the gating period.

** หน่วยงานที่ยื่นจด คือ บริษัท Qinetiq โดยบริษัทนี้ยังมีสิทธิบัตรที่เกี่ยวข้องอีกมากสำหรับการปกป้องเครือข่ายสื่อสาร เช่น Network having quantum key distribution (US 20100299526 A1) Method of performing authentication between network nodes (US 20110231665 A1) เป็นต้น*

ตัวอย่างแนวทางการศึกษาสิทธิบัตร 3)

US8693685B2 ..... *(หมายเลขสิทธิบัตร ณ สหรัฐอเมริกา)*
TAPSTER PAUL RICHARD ..... *(ผู้ประดิษฐ์ บริษัท Qinetiq Limited**)*
2014-04-08 ..... *(วันที่ได้รับการประกาศ หรือ Publication date (ยื่น 2007-08-04))*
H04K 1/00 [38] ..... *(หมายเลขการจัดจำแนกสิทธิบัตรระหว่างประเทศ COOPERATIVE PATENT CLASSIFICATION (CPC) ซึ่งสิทธิบัตรนี้อยู่ในกลุ่ม **Secret communication หรือการสื่อสารเพื่อการรักษาความลับ**)*

Title: ..... *(ชื่อสิทธิบัตร: **อุปกรณ์รหัสลับควอนตัม**)*
DWPI Title: ..... *(ชื่อที่ได้รับการจัดแปลงเชิงขยายให้เข้ากับฐานข้อมูลระบบของ Thomson Innovation (DWPI) **ภาครับระบบรหัสลับเชิงควอนตัมที่มีหน่วยจัดการเปิดปิด พร้อมด้วยสัญญาณนาฬิกาอิเล็กทรอนิกส์เพื่อให้สัญญาณเวลาอันนำไปสร้างสัญญาณเปิดปิดนั้น**)*

Abstract : ..... บทคัดย่อ: อุปกรณ์และวิธีการด้านการจัดการเวลารวมทั้งการเข้าจังหวะสำหรับระบบรหัสลับเชิงควอนตัม โดยที่สัญญาณพัลซ์เปิดปิดที่สร้างจากสัญญาณนาฬิกาแล้วเข้าจังหวะกันกับการรับโฟตอนที่ถูกส่งออกมายังหน่วยรับสัญญาณ ซึ่งอุปกรณ์นี้จะจัดการเพื่อการตรวจรับโฟตอนกับช่วงเวลาที่หน่วยเปิดปิดนั้นให้สัญญาณเท่านั้น

*** www.qinetiq.com บริษัทจดทะเบียนที่ประเทศอังกฤษและเวลส์ มีกิจการด้านความปลอดภัยทั้งด้านพลเรือนและทหาร เป็นที่สังเกตได้ว่า "ความปลอดภัย" ในโลกอนาคตมีเรื่องการสื่อสารปลอดภัยเข้าไปเกี่ยวข้องและสำคัญยิ่งร่วมอยู่กับงานด้านทหาร โครงสร้างพื้นฐาน (ไฟฟ้าหรือระบบสาธารณูปโภค) และอื่น ๆ อีกหลายสาขา ซึ่งรหัสลับเชิงควอนตัมคือระบบที่จะให้ความปลอดภัยสูงสุดนั้นได้ จึงปรากฏมีงานวิจัยและพัฒนากับกลุ่มงานด้านความมั่นคง (defense) มากขึ้นโดยลำดับ โดยเฉพาะกับประเทศที่เป็นผู้นำด้านการทหาร เช่น ทั้งสหรัฐอเมริกาหรืออังกฤษ เป็นต้น*

38 *www.uspto.gov/web/patents/classification/cpc/html/cpc-H04K.html*

ตัวอย่าง 4) CN103278996A

USTC UNIV SCIENCE TECH CN

2013-05-17

G02F 1/35

Title: Sandwich type high light quantum entanglement photon source

DWPI Title: Sandwich-type high-brightness quantum entangled photon source, has sheet-shaped half wave plate arranged with chip, where inclined angle between half wave plate and nonlinear crystal plane is in specific value

Abstract: The invention discloses a sandwich type high light quantum entanglement photon source which comprises a pump laser light source and a crystal mechanism. The crystal mechanism is used for receiving pump laser light emitted by the pump laser light source and producing two down-conversion beams provided with entanglement photon pairs. The crystal mechanism comprises two non-linear crystals and a semi-wave plate arranged between the two non-linear crystals. The two non-linear crystals meet II type phase matching. Working wavelength of the semi-wave plate is identical with wavelength of the quantum entanglement photon source. The direction of an optical axis of the semi-wave plate forms an angle of 45 degrees with a plane. The plane is determined by the direction of optical axes of the two non-linear crystals and the direction of the pumping laser light. The sandwich type high light quantum entanglement photon source is convenient to adjust, high in integration degree, beneficial to expansion and capable of being applied to application fields of quantum communication, quantum cryptography and the like.

ตัวอย่างแนวทางการศึกษาสิทธิบัตร 4)

(สิทธิบัตรต้นฉบับภาษาจีน แปลความหมายเป็นภาษาอังกฤษ)

CN103278996A ..... *(หมายเลขสิทธิบัตร ณ ประเทศจีน)*

USTC UNIV SCIENCE TECH CN ..... *(โดย มหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศจีน)*

2013-09-04 ..... *(วันที่ได้รับการประกาศ หรือ Publication date (ยื่น 2013-05-17)*

G02F 1/35[39] ..... *(หมายเลขการจัดจำแนกสิทธิบัตร PATENT CLASSIFICATION ซึ่งสิทธิบัตรนี้อยู่ในกลุ่มทัศนศาสตร์ที่ไม่เป็นเชิงเส้น **Non-linear optics**)*

Title: ..... *(ชื่อสิทธิบัตรแปล: **แหล่งกำเนิดโฟตอนพัวพันเชิงควอนตัมความสว่างสูงแบบแซนด์วิช***

DWPI Title: ..... *(ชื่อที่ได้รับการจัดแปลงเชิงขยายให้เข้ากับฐานข้อมูลระบบของ Thomson Innovation (DWPI) **แหล่งกำเนิดโฟตอนพัวพันเชิงควอนตัมความสว่างสูงแบบแซนด์วิชโดยมีแนวแผ่นครึ่งคลื่นจัดวางเรียงบนอุปกรณ์ชิป และโดยการที่มุมเอียงตกกระทบของแผ่นครึ่งคลื่นกับพื้นผลึกแบบที่ไม่เป็นเชิงเส้นนั้นจะมีค่าเฉพาะใด ๆ***

Abstract : ..... บทคัดย่อแปล: การประดิษฐ์นี้เป็นแหล่งกำเนิดโฟตอนพัวพันเชิงควอนตัมความสว่างสูงแบบแซนด์วิช โดยมีระบบกลไกของผลึกที่รับแสงเลเซอร์ที่ปรับปั๊มให้กำเนิดสองแนวลำของคู่โฟตอนพัวพันจากการแปลงผันลง (ความถี่ลดครึ่ง) แนวแผ่นครึ่งคลื่นจัดวางเรียงบนอุปกรณ์ชิป ตอบสนองความยาวคลื่นกับแหล่งกำเนิดโฟตอนพัวพันเชิงควอนตัม และโดยการที่มุมตกกระทบของแผ่นครึ่งคลื่นกับพื้นผลึกแบบที่ไม่เป็นเชิงเส้นนั้นจะมีค่าเฉพาะ คือ 45 องศา แหล่งกำเนิดโฟตอนพัวพันเชิงควอนตัมความสว่างสูงแบบแซนด์วิชนี้สะดวกต่อการปรับค่า มีระดับ (ค่าเฉพาะ) ของการร่วมประกอบเข้ากับงานอื่นได้ดี ขยายต่อได้เหมาะกับการประยุกต์กับการสื่อสารเชิงควอนตัม

หมายเหตุ: *มหาวิทยาลัย USTC ตั้งอยู่ ณ เมืองเหอเฟย (Hefei) มณฑลอันฮุย (Anhui) ซึ่งจัดได้ว่าเป็นเมืองหลวงของวิทยาการรหัสลับเชิงควอนตัมของประเทศจีน เนื่องจากมีที่มงานของนักวิจัยสองกลุ่มหลักของประเทศจีนที่มีชื่อเสียงในระดับโลกนำโดย ศาสตราจารย์ เจิ้งฟู่ หาน (Zheng-Fu Han) และศาสตราจารย์ เจียน เหวย พาน (Jian Wei Pan)*

39 *worldwide.espacenet.com/classification?locale=de_EP#!/CPC=G02F1/35*

ตัวอย่าง 5) US20130334434A1

PRINCETON LIGHTWAVE INC
2013-05-10
H01L 31/107

Title: Dual-SPAD-Based Single-Photon Receiver

DWPI Title: Receiver, has output terminal which is operated for providing third output signal that is based on first output signal and second output signal.

Abstract: A single-photon receiver is presented. The receiver comprises two SPADs that are monolithically integrated on the same semiconductor chip. Each SPAD is biased with a substantially identical gating signal. The output signals of the SPADs are combined such that capacitive transients present on each output signal cancel to substantially remove them from the output signal from the receiver.

ตัวอย่างแนวทางการศึกษาสิทธิบัตร 5)

US20130334434A1 ..... *(หมายเลขสิทธิบัตร ณ สหรัฐอเมริกา)*
PRINCETON LIGHTWAVE INC ..... (โดยบริษัท Princeton Lightwave)
2013-12-19 ..... *(วันที่ได้รับการประกาศ หรือ Publication date (ยื่น 2013-05-10)*
H01L 31/107 [40] *(หมายเลขการจัดจำแนกสิทธิบัตรอยู่ในกลุ่มอุปกรณ์สารกึ่งตัวนำที่ไวต่อความยาวคลื่นแสงย่านอินฟราเรด)*

Title: ..... *(ชื่อสิทธิบัตรแปล:* ***ภาครับโฟตอนเดี่ยวแบบคู่ SPAD****)*
DWPI Title: ..... *(ชื่อที่ได้รับการจัดแปลงเชิงขยายให้เข้ากับฐานข้อมูลระบบของ Thomson Innovation (DWPI)* ***ภาครับสัญญาณที่มีส่วนเชื่อมต่อปลายทางทำงานโดยให้สัญญาณขาออกลำดับที่สาม โดยอยู่บนพื้นฐานจากสัญญาณลำดับต้นและลำดับที่สอง)***

Abstract : ..... บทคัดย่อ: ภาครับสัญญาณโฟตอนเดี่ยวนำเสนอในการประดิษฐ์นี้ โดยประกอบด้วย SPAD สองส่วนที่เชื่อมโยงเป็นส่วนเดียวกันบนชิปอุปกรณ์สารกึ่งตัวนำ โดยแต่ละ SPAD ได้รับการจ่ายไฟเลี้ยงด้วยระดับสัญญาณที่เหมือนกัน สัญญาณขาออกจากทั้งสอง SPAD จะรวมกัน ซึ่งจะทำให้สัญญาณรบกวนเชิงค่าประจุที่เกิดขึ้นตามโอกาสและอยู่ในสัญญาณขาออกใด จะหักล้างกันและหายไปได้หมดจากสัญญาณขาออกที่ต้องการของภาครับได้

** single - photon avalanche diode อุปกรณ์ไดโอดรับแสงสำหรับงานโฟตอนเดี่ยวหรือแสงหน่วยเดียว อุปกรณ์จำพวกนี้มีความสำคัญต่อการตรวจจับสถานะเชิงควอนตัมของแสงที่ต้องอาศัยการทำงานที่ความไวสูงมาก และมีราคาสูงมากเช่นกัน*

40 *worldwide.espacenet.com/classification?locale=de_EP#!/CPC=H01L%2031/107 (ชื่อหมวดสิทธิบัตรภาคขยาย Semiconductor devices sensitive to infra-red radiation, light, electromagnetic radiation of shorter wavelength or corpuscular radiation and adapted either for the conversion of the energy of such radiation into electrical energy or for the control of electrical energy by such radiation; Processes or apparatus peculiar to the manufacture or treatment thereof or of parts thereof; Details thereof)*

ตัวอย่าง 6) JP2013205711A
OKI ELECTRIC IND CO LTD
2012-03-29
G02F 1/39

Title: QUANTUM ENTANGLED PHOTON PAIR GENERATION DEVICE

DWPI Title: Quantum entangled photon pair generator used for quantum information e.g. quantum cryptography, has photon pair extractor that extracts wavelength components to signal and idler photons to output extracted wavelength components .

Abstract: PROBLEM TO BE SOLVED: To provide a quantum entangled photon pair generation device which is capable of easily properly selecting and generating a polarization quantum entangled photon pair as well as a time position quantum entangled photon pair. **SOLUTION:** The quantum entangled photon pair generation device includes an excitation light pulse shaping unit 10-1, an optical interferometer unit 20-1, and a quantum entangled photon pair extraction unit 30-1. The excitation light pulse shaping unit receives a linearly polarized light pulse to select and output one of a polarized excitation light pulse pair being a seed light pulse of a polarization quantum entangled photon pair and a double excitation light pulse pair being a seed light pulse of a time position quantum entangled photon pair. The optical interferometer unit receives the polarized excitation light pulse pair or the double excitation light pulse pair to output a correlation photon pair comprising a signal photon and an idler photon on the basis of a parametric fluorescence process. The quantum entangled photon pair extraction unit selects wavelength components corresponding to respective photons of the quantum entangled photon pair and spatially separates them to output the result as a polarization quantum entangled photon pair or a time position quantum entangled photon pair.

ตัวอย่างแนวทางการศึกษาสิทธิบัตร 6)

(สิทธิบัตรต้นฉบับภาษาญี่ปุ่น แปลความหมายเป็นภาษาอังกฤษ)

JP2013205711A .... *(หมายเลขสิทธิบัตร ณ ประเทศญี่ปุ่น)*
OKI ELECTRIC IND CO LTD .... *(โดย บริษัท โอกิ ผู้ผลิตเครื่องใช้ไฟฟ้ารายใหญ่ของประเทศ)*
2013-10-07 .... *(วันที่ได้รับการประกาศ หรือ Publication date (ยื่น 2012-03-29)*
G02F1/39[41] .... *(หมายเลขการจัดจำแนกสิทธิบัตรระหว่างประเทศ (IPC) กลุ่มการสร้างหรือขยายสัญญาณแสง อินฟราเรด หรือ อุลตราไวโอเลต (parametric generation or amplification of light, infra-red or ultra-violet waves))*

Title: .... *(ชื่อสิทธิบัตรแปล: **อุปกรณ์สร้างคู่โฟตอนพัวพันเชิงควอนตัม**)*
DWPI Title: .... *(ชื่อที่ได้รับการจัดแปลงเชิงขยายให้เข้ากับฐานข้อมูลระบบของ Thomson Innovation (DWPI) **อุปกรณ์กำเนิดคู่โฟตอนพัวพันเชิงควอนตัมเพื่อใช้ในงานด้านสารสนเทศเชิงควอนตัม เช่น รหัสลับเชิงควอนตัม โดยมีการแยกคู่โฟตอนที่องค์ประกอบความยาวคลื่นไปเป็นโฟตอนสัญญาณและอีกโฟตอนที่ว่างไม่ได้ใช้**)*

Abstract : .... บทคัดย่อแปล: **เพื่อการแก้ปัญหา**การเตรียมอุปกรณ์ที่สามารถคัดสรรได้สะดวกและเหมาะสมต่อการให้กำเนิดคู่โฟตอนพัวพันเชิงควอนตัม และสร้างคู่โฟตอนพัวพันที่มีมุมโพลาไรซ์ รวมทั้งคู่โฟตอนพัวพันแบบตำแหน่งที่ระบุเวลาได้ **แนวทางคือ** หน่วยปรับแต่งรูปสัญญาณแสงที่ได้รับการกระตุ้นเมื่อรับสัญญาณแสงโพลาไรซ์เชิงเส้นมาจะเลือกและส่งออกหนึ่งในคู่นั้น เพื่อใช้เป็นต้นกำเนิดของสัญญาณพัลซ์แสงของคู่โฟตอนโพลาไรซ์พัวพันเชิงควอนตัม และควบการเป็นต้นกำเนิดคู่โฟตอนพัวพันที่กำหนดตำแหน่งเวลา ส่วนหน่วยอินเทอร์เฟียโรเมื่อรับคู่สัญญาณพัลซ์แสงที่ได้รับการกระตุ้นหรือคู่สัญญาณพัลซ์ควบ จะไปออกเป็นคู่โฟตอนที่มีความสัมพันธ์กัน ประกอบด้วยโฟตอนที่เป็นตัวสัญญาณกับอีกโฟตอนที่มีสถานะว่าง สำหรับส่วนการแยกคู่โฟตอนพัวพันจะทำหน้าที่เลือกจากองค์ประกอบความยาวคลื่นตอบสนองกับคู่โฟตอนพัวพัน แล้วแยกออกไปเป็นคู่ที่มีมุมโพลาไรซ์ หรือคู่โฟตอนพัวพันแบบตำแหน่งระบุเวลาต่อไป

41 *worldwide.espacenet.com/classification?locale=en_EP#!/CPC=G02F1/39*

ตัวอย่าง 7) CN103051444A

ANHUI ASKY QUANTUM TECHNOLOGY CO LTD

2012-12-31

H04L 9/08

Title: Quantum security digital terminal applied to PSTN (Public Switched Telephone Network)

DWPI Title: Quantum security digital terminal for public switched telephone network (PSTN), has encoding module that converts compressed digital voice signal, and main controller which encrypts digital signal into analogue signal by demodulator

Abstract: The invention discloses a quantum security digital terminal applied to a PSTN (Public Switched Telephone Network). A method for using the quantum security digital terminal comprises the steps that: when a call is received, a modulation and demodulation module converts an analog speech signal into a digital speech signal; a main controller decrypts the digital speech signal by using a quantum secret key, and converts the analog speech signal into the digital speech signal when the call is sent out, a speech compression coding module compresses the digital speech signal to from a compressed digital signal; the main controller encrypts the compressed digital signal by using the quantum secret key to form an encrypted digital signal; and the main controller converts the encrypted digital signal into an analog signal by a modulator-demodulator, and the analog signal is output through a second phone wire interface. The quantum security digital terminal applied to the PSTN is capable of using a quantum encryption technology on the PSTN, and realizes the unconditional security digital communication.

ตัวอย่างแนวทางการศึกษาสิทธิบัตร 7)

(สิทธิบัตรต้นฉบับภาษาจีน แปลความหมายเป็นภาษาอังกฤษ)

CN103051444A ..... *(หมายเลขสิทธิบัตร ณ ประเทศจีน)*

ANHUI ASKY QUANTUM TECHNOLOGY CO LTD ..... *(โดย บริษัทที่ปั่นเพาะออกมาจากงานวิจัยของมหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศจีน USTC)*

2013-04-13 ..... *(วันที่ได้รับการประกาศ หรือ Publication date (ยื่น 2012-12-31)*

H04L9/08[42] ..... *(หมายเลขการจัดจำแนกสิทธิบัตรซึ่งสิทธิบัตรนี้อยู่ในกลุ่ม **Key Distribution** หรือ **การกระจายกุญแจรหัสลับ**)*

Title: ..... *(ชื่อสิทธิบัตรแปล: **อุปกรณ์ปลายทางดิจิทัลเพื่องานรักษาความลับเชิงควอนตัมสำหรับโครงข่ายสายสื่อสารสาธารณะ**)*

DWPI Title: ..... *(ชื่อที่ได้รับการจัดแปลงเชิงขยายให้เข้ากับฐานข้อมูลระบบของ Thomson Innovation (DWPI) คือ **อุปกรณ์ปลายทางดิจิทัลเพื่องานรักษาความลับเชิงควอนตัม สำหรับโครงข่ายสื่อสารสาธารณะที่มีส่วนการเข้ารหัสอันแปลงสัญญาณเสียงเชิงดิจิทัลที่ปิบอัดแล้ว และอีกส่วนหลักของการเข้ารหัสความลับสัญญาณนั้นไปเป็นสัญญาณแอนะล็อก**)*

Abstract : ..... บทคัดย่อแปล: การประดิษฐ์นี้เปิดเผยเรื่องอุปกรณ์ปลายทางดิจิทัลเพื่องานรักษาความลับเชิงควอนตัมสำหรับโครงข่ายสื่อสารสาธารณะ (โทรศัพท์) โดยวิธีการประยุกต์หกขั้นตอนคือ เมื่อมีการรับสายเรียกเข้า ส่วนโมดูลการกลั้วและการถอดการกลั้วสัญญาณจะแปลงสัญญาณเสียงเป็นรูปแบบดิจิทัล ส่วนควบคุมหลักทำหน้าที่ถอดรหัสสัญญาณดิจิทัลด้วยกุญแจรหัสเชิงควอนตัม รวมทั้งหน้าที่การแปลงสัญญาณแอนะล็อกเป็นดิจิทัล ส่วนปิบอัดสัญญาณเสียงทำหน้าที่ปิบอัดสัญญาณดิจิทัล ส่วนควบคุมหลักเข้ารหัสสัญญาณดิจิทัลที่ถูกปิบอัดด้วยการใช้กุญแจควอนตัม เพื่อเป็นสัญญาณเข้ารหัสดิจิทัล ส่วนควบคุมหลักแปลงสัญญาณเข้ารหัสดิจิทัลไปเป็นแอนะล็อก ด้วยหน่วยการกลั้วและคลายและส่วนของการเชื่อมต่อสัญญาณกับระบบโทรศัพท์จะได้สัญญาณแอนะล็อกนั้นออกไป

หมายเหตุ: *การแปลจากต้นฉบับภาษาจีนเป็นอุปสรรคสำคัญแต่กระนั้นสามารถทำให้ทราบภาพรวมการประยุกต์กับเครือข่ายการสื่อสารปกติใกล้ตัวได้มากขึ้น เช่น ระบบโทรศัพท์*

42 *www.uspto.gov/web/patents/classification/cpc/html/cpc-H04L.html*
(or management, e.g. generation, sharing or updating, of cryptographic keys or passwords)

- **สรุปผลภาพรวมสิทธิบัตร (เมษายน พ.ศ.2559)**

สำหรับแนวทาง"รหัสลับเชิงควอนตัม"ที่พบส่วนใหญ่ เป็นการนำเสนอรูปแบบการประยุกต์เข้ากับระบบสื่อสารโทรคมนาคมปกติ ส่วนพัฒนาการด้านเทคนิคพบด้านการพัฒนาการอุปกรณ์ประกอบ และการกำเนิดจำนวนสุ่มต้นทางของการสร้างรหัสลับ ด้านการสร้างสถานะเชิงควอนตัมนั้นจะพบด้านเทคนิคผสมทั้งเฟส โพราไรซ์ และอื่น ๆ (continuous variable) ส่วนเทคนิคความพัวพัน (entanglement) นั้นพบน้อยมากซึ่งสัมพันธ์กับข่าวความก้าวหน้าทั่วโลกที่ไม่มีสินค้าจากพื้นหลักการหลังนี้ออกมาแต่อย่างใด เนื่องจากให้ค่าการกำเนิดความพัวพันที่นำมาสร้างเป็นรหัสลับควอนตัมได้นั้นยังคงน้อยมาก ไม่เพียงพอต่อความเร็วในการใช้งานกับเครือข่ายการสื่อสารทั่วไปได้ แม้เป็นแนวทางที่ไม่มีข้อจำกัดทางหลักการและได้รับการนำเสนอเพื่อกำเนิดสถานะความพัวพันผ่านดาวเทียมในหลายแห่งแล้ว แต่การพัฒนาสร้างจริงทั่วโลกยังคงต้องใช้เวลาสั่งสมความรู้และประสบการณ์อีกมาก

- **สังคมสิทธิบัตร – รหัสลับเชิงควอนตัม**

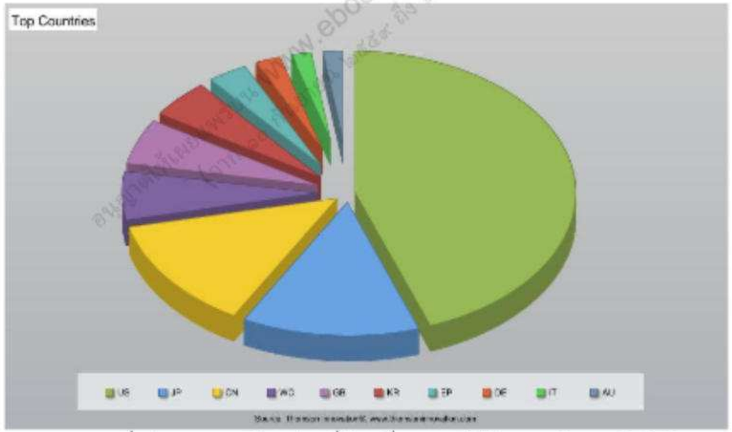
อนึ่ง การสำรวจนี้ทำการรวบรวมรายชื่อและพิจารณาสิทธิบัตรรวมทั้งหมด 827 ตัวอย่าง (จากฐานข้อมูลรวมมากว่า 22 ล้านชุดของ Thomson Innovation) ได้นำเสนอตัวอย่างในรายละเอียดดัง "7 สิทธิบัตรตัวอย่าง" ที่กล่าวมาแล้ว ส่วนตัวอย่างอีกจำนวนมากสามารถศึกษา ร่วมสร้างผลการพิจารณา ร่วมการขัดเกลาผลร่วมความเห็น และร่วมกันใช้งานได้ที่ www.Q-Thai.Org และ www.facebook.com/QuantumCryptoThailand

ขยายความหมายถึง ผู้ใช้งานสามารถร่วมขัดเกลาตัวอย่างที่ได้รับการถอดความบางส่วนแล้ว รวมทั้งสามารถร่วมกันสกัดข้อมูลของสิทธิบัตรที่น่าสนใจอื่น ๆ ร่วมกันเพิ่มเติมได้ อีกทั้ง ร่วมให้ความเห็นต่อแนวทางการพัฒนาความรู้จากสิทธิบัตรกับโครงการเริ่มต้นนี้ได้ต่อไปด้วย โดยในระยะยาว สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI) และชมรมไฟฟ้าสื่อสาร สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE) จะได้ร่วมกันเป็นเจ้าภาพแกนหลักเพื่อให้โครงการนี้พัฒนาตนเองต่อได้จากความร่วมมือกันโดยเป็นสาธารณะ ซึ่งจะได้เกิดเป็นโครงการย่อย " **สังคมสิทธิบัตร – รหัสลับเชิงควอนตัม**" บนสังคมออนไลน์ เติบโตได้ตามการพัฒนาของวงการและการยื่นขอคุ้มครองสิทธิบัตรใหม่ ๆ ที่จะได้ปรากฏมากขึ้นต่อเนื่องไป

3.2.2 การวิเคราะห์สิทธิบัตรเบื้องต้น

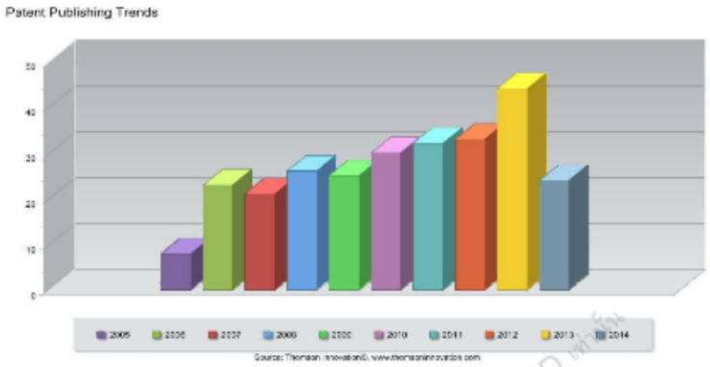
จากการสรุปข้อมูลจากฐานของ Thomson Innovation เดือนเมษายนปี พ.ศ. 2559 ได้แบ่งตามลักษณะออกเป็นสองช่วง[43] คือช่วงข้อมูลทั่วไปที่พบมากและคงที่แล้วของช่วงปีพ.ศ.2549 (ค.ศ.2006) จนถึงเดือนพ.ศ.2557 (ค.ศ.2014) และช่วงที่สองอันเป็นฐานข้อมูลการสำรวจเฉพาะทางที่ตามติดความก้าวหน้าประกอบกับทั้งจากฐานข้อมูลข้างเคียงอื่น ๆ เช่น WIPO และของกูเกิล (Google patent) จนถึงช่วงเวลาของการวิเคราะห์ข้อมูลในรายงานนี้ (เดือนเมษายนปี พ.ศ. 2559) ซึ่งจะนำเสนอในบทที่ 4 (*การสำรวจสิทธิบัตรสามคำสำคัญ*) และบทที่ 5 (*สิทธิบัตรของบริษัท IDQuantique*) โดยที่ข้อมูลส่วนแรกของบทนี้ พบข้อมูลที่มีการยื่นขอจดสิทธิบัตรและได้รับการคุ้มครองชุดสำคัญที่กลั่นกรองทั่วไปแล้วจำนวน **827** เรื่อง สามารถแจกแจงวิเคราะห์ผลการสืบค้นทั่วไปได้ดังต่อไปนี้

ก) ประเทศที่มีการยื่นขอจดสิทธิบัตรและได้รับการคุ้มครองมากที่สุด
อันดับที่ 1 ได้แก่ประเทศสหรัฐอเมริกาตามด้วยประเทศญี่ปุ่นและจีนตามลำดับที่เด่นชัด
ข) แนวโน้มจำนวนสิทธิบัตรที่ตีพิมพ์ทั่วโลก (Patent Publishing Trends)
ข้อมูลตั้งแต่ปีค.ศ.2005 (พ.ศ.2548) พบว่ามีแนวโน้มที่เพิ่มสูงขึ้นเล็กน้อย

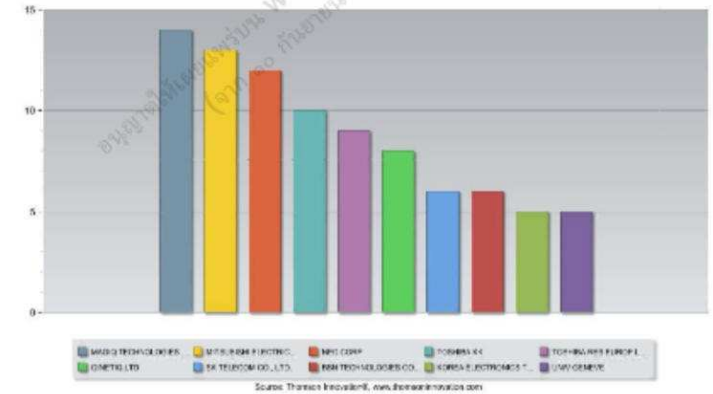


3 ก) รายชื่อประเทศและอัตราส่วนที่มีการยื่นขอและได้รับความคุ้มครองสิทธิบัตร

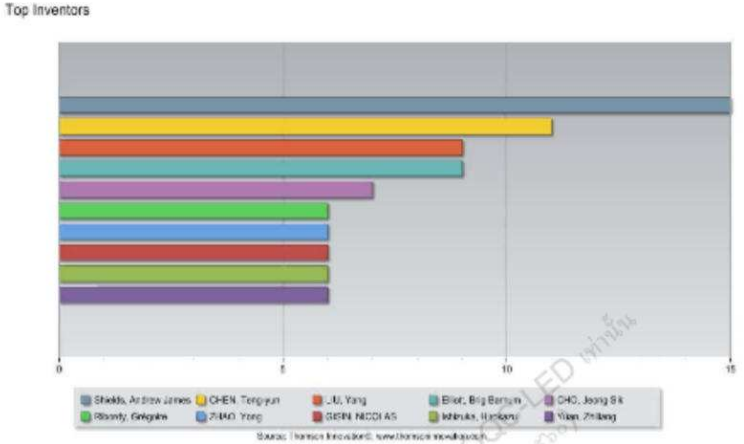
43 *ฐานข้อมูลช่วงแรก พ.ศ.2549 (ค.ศ.2006) จนถึงเดือนพ.ศ.2557 (ค.ศ.2014) และช่วงที่สองจนถึง เม.ย. 2559*



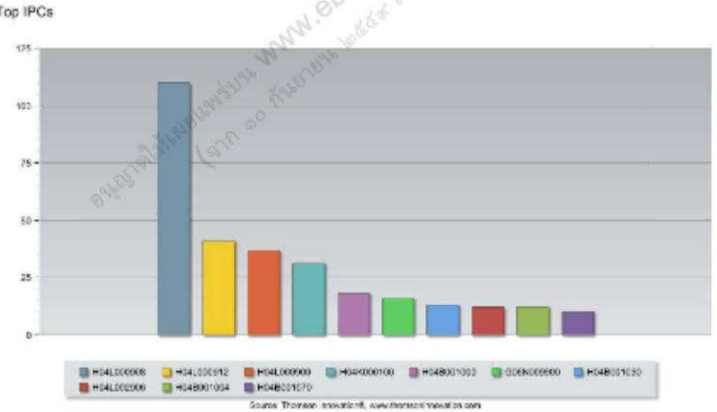
3 ช) แนวโน้มจำนวนสิทธิบัตร"Quantum Cryptography"ทั่วโลก ของช่วงปีพ.ศ.2549 (ค.ศ.2006) จนถึงเดือนพ.ศ.2557 (ค.ศ.2014)



3 ค) รายชื่อบริษัทผู้ยื่นขอและได้รับความคุ้มครอง



3 ง) อันดับรายชื่อนักประดิษฐ์หรือผู้จดสิทธิบัตร



3 จ) หมวดหมู่สาขาวิชาสิทธิบัตรตามระบบ IPC: International Patent Code

ค) รายชื่อบริษัทผู้ขอและได้รับความคุ้มครองสิทธิบัตร (Assignees)
อันดับที่ 1 ได้แก่บริษัท MagiQ Technologies (สหรัฐฯ) ตามด้วยบริษัทของประเทศญี่ปุ่น เช่น Mitsubishi Electronic, NEC Corp และอื่น ๆ โดยยังมีจำนวนไม่ต่างกันมากนัก

ง) นักประดิษฐ์ (Inventors)
อันดับที่ 1 ได้แก่ Shields Andrew James (จาก Toshiba UK) ที่เด่นชัด นอกนั้นกระจายอยู่กับหลากกลายผู้ประดิษฐ์ที่ยังไม่เด่นชัดนัก

จ) หมวดหมู่สาขาวิชาของสิทธิบัตรตามระบบ IPC (International Patent Classification)
อันดับที่ 1 ได้แก่ IPC- หมวด H04L000908 (key distribution) หรือการกระจายกุญแจรหัสลับ

3.2.3 การวิเคราะห์กลุ่มคำในเอกสารสิทธิบัตร (Text Clustering)

จากการสืบค้นคำ "Quantum Cryptography" ฐานข้อมูล Thomson Innovation ได้ผลการวิเคราะห์กลุ่มคำที่เกี่ยวข้องกับเรื่องนี้ออกเป็น 13 กลุ่มคำ สามารถแยกแยะสังเกตแนวโน้มจากจำนวนเรื่องที่ปรากฏอยู่ในแต่ละหมวดและคำสำคัญได้ดังนี้

กลุ่มที่	กลุ่มคำ	รวม[44] (เรื่อง)
1	**dot,photon source,region**	44
2	**signal,phase,polarization**	36
3	node,network,key	34
4	state,quantum state,entity	27
5	qkd,station,key	22
6	polarized-wave,particle,receive device	20
7	quantum cryptography apparatus,laser,quantum cryptography	20
8	signal,avalanche,output signal	16
9	core,component,optical component	15
10	matrix,random,number	14
11	pulse,reference,quantum cryptography communication apparatus	13
12	*anspruch,kennzeichnen,verfahren*	*7*
13	uncategorized (ไม่สามารถจัดหมวดได้)	12

(คำอธิบาย *การกระจายของคำสำคัญใกล้เคียงกันมีมากด้านอุปกรณ์และเทคนิคการสร้างสถานะควอนตัมแสง แสดงถึงการเป็นวิทยาการที่ความสำคัญยังกระจายตัว มีโอกาสกว้างในสาขาย่อยตามกลุ่มคำเหล่านั้น)*

44 *"สิทธิบัตรหนึ่งอาจปรากฏอยู่ในหลายกลุ่มคำได้และอาจมีเลขอ้างเฉพาะบางส่วนที่สำคัญเท่านั้น เนื่องจากรูปแบบวิเคราะห์ (feature) ที่ใช้งานเป็นแบบทดลองจึงมิได้นำเสนอครบทั้งหมด เป็นไปตามคุณลักษณะ (option) ที่ลูกค้าจะเลือกซื้อจากระบบฐานข้อมูลขนาดใหญ่ หากต้องการผลวิเคราะห์อย่างละเอียดต้องมี Data Analyzer ที่เป็น text mining ของบริษัท Thomson Reuters" จำนวนเรื่องรวมจึงแสดงผลเฉพาะที่ระบบใช้งานได้*

3.2.4 การอ้างอิง (Citation)

ฐานข้อมูล Thomson Innovation สามารถแสดงข้อมูลแผนที่การอ้างอิง (Citation Map) ซึ่งเป็นภาพความเชื่อมโยงของการอ้างอิงและการถูกอ้างอิงไปใช้ได้ แต่เนื่องจากสาขานี้ยังมีความใหม่มากจึงมีการอ้างอิงถึงทั้งสองแนวทางน้อยมาก ในบางกรณีมีการอ้างอิงถึงสิทธิบัตรอื่นที่จดคุ้มครองก่อนหน้าซึ่งอาจเป็นสาขาหรือเทคนิคอื่น พบที่เรียกว่าการอ้างอิงแบบย้อนหลัง (Backward) นี้ได้บ้าง แต่การถูกอ้างอิงหรือแบบข้างหน้า (Forward) มักไม่ปรากฏข้อมูล อันหมายถึงสิทธิบัตรด้านรหัสลับเชิงควอนตัมยังคงใหม่มาก และมีความเชื่อมโยงที่สิทธิบัตรอื่นจะอ้างถึงนั้นน้อย โดยการพรรณาข้างต้นนี้สอดคล้องกับการกระจายตัวของกลุ่มคำก่อนหน้า

3.2.5 แผนที่ ThemeScape

ต่อเนื่องมายังความสามารถในการวิเคราะห์ภาพรวมของกลุ่มเอกสารสิทธิบัตร โดยแสดงในรูปแผนที่ ThemeScape อันเป็นแผนที่แบบภูมิทัศน์ (Landscape) โดยจากการสืบค้นภาพที่ได้แสดงกลุ่มคำที่เป็นเทคโนโลยีรอง (Sub technology) ชัดเจนกับเทคโนโลยีด้านที่เกี่ยวข้องหลักคือ

- Band laser application
- Emission photon source
- Filter placed error
- Output bias increasing
- Carrier quantum bit classic เป็นต้น

รวมถึงแสดงความสัมพันธ์ของกลุ่มเอกสารเทคโนโลยีเหล่านั้นที่แสดงผลออกมา สามารถศึกษาได้จากการกระจายตัวของเอกสารสิทธิบัตร (แต่ละจุดในแผนที่หมายถึงเอกสาร 1 ฉบับ) หากเทคโนโลยีมีความสัมพันธ์กันหรือเรื่องที่คล้ายคลึงกัน จุดแสดงจะอยู่ในตำแหน่งที่ใกล้กัน (ดังรูป ฉ)) หากมีจำนวนมากจะเกิดการก่อตัวสูงขึ้นเสมือนเป็นเนินเขาตามจำนวน ส่วนคำที่มีจำนวนน้อยจะมีภูมิทัศน์ที่จางหรือมีพิกัดที่ต่ำลดหลั่นลงไป เหมือนเป็นภาพถ่ายทางอากาศลึกลงยังหุบเขา โดยแนวภาพของแต่ละเนินแสดงความสัมพันธ์ด้วยหากอยู่ใกล้กัน ดังนั้น หากต้องการสร้างงานวิจัยหรือสิ่งประดิษฐ์ที่มีความใหม่ และไม่ซ้ำซ้อนกับงานก่อนหน้าที่มีการยื่นขอรับความคุ้มครองไว้แล้ว จะสามารถพิจารณาจากช่องว่างของภาพภูมิทัศน์นี้ร่วมกับปัจจัยความสัมพันธ์อื่นที่เกี่ยวข้อง ซึ่งจะเป็นวิธีลดทรัพยากรด้านเวลาและเพิ่มคุณค่าให้กับงานวิจัยและพัฒนาได้อย่างมีประสิทธิภาพแนวทางหนึ่ง รวมถึงด้าน "รหัสลับเชิงควอนตัม" จากภาพนี้

3 ฉ) รูปแสดงแผนที่ ThemeScape[45]

โดยภาพรวมของ การวิเคราะห์กลุ่มคำ การอ้างอิง และแผนที่ ThemeScape ให้ผลที่สอดคล้องกันนั่นคือ รหัสลับเชิงควอนตัม จัดได้ว่ายังเป็นสาขาใหม่ที่มีสิทธิบัตรจำนวนไม่สูงนัก การกระจายตัวของทั้งกลุ่มคำ การอ้างอิง และตัวเทคโนโลยีที่เกี่ยวข้อง จึงยังคงกระจายตัว ไม่เด่นชัดที่เรื่องใด

คำอธิบายเบื้องต้น:

การใช้งานฐานข้อมูลออนไลน์ Thomson Innovation สามารถตรวจสอบรายละเอียดของแต่ละจุดบนภาพได้ เป็นภาพแผนที่ที่มีปฏิสัมพันธ์กับผู้ใช้งานเพื่อการแสวงหาช่องโอกาสที่มีอยู่จากมุมมองยุทธศาสตร์ ท่ามกลางความสูงต่ำหรือความหนาแน่นของเทคนิคที่ได้รับการจดสิทธิบัตรคุ้มครองก่อนหน้าไปแล้ว

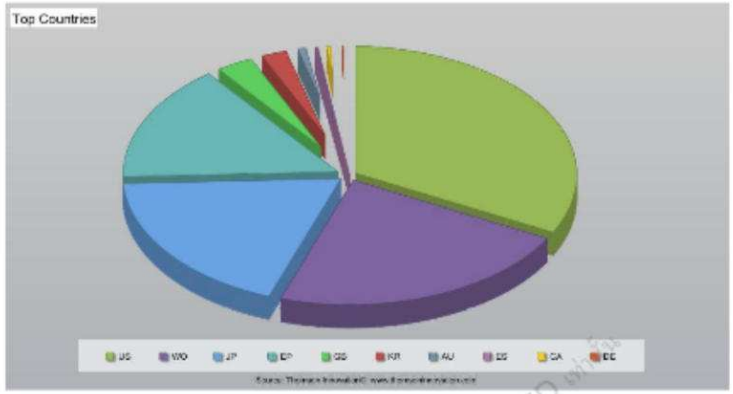
45 *การทดสอบใช้ภาพแผนที่จะแสดงปฏิสัมพันธ์ได้เฉพาะการใช้งานที่มีสิทธิบน ip.thomsonreuters.com/training/derwent-world-patents-index เท่านั้น ซึ่งอาจได้มีการปรับปรุงแสดงเป็นภาพนิ่งที่พัฒนาไปตามเวลา ณ www.Q-Thai.Org เป็นอีกทางเลือกหนึ่งต่อไป*

สำรวจข้อมูลสิทธิบัตรสามคำสำคัญ 4

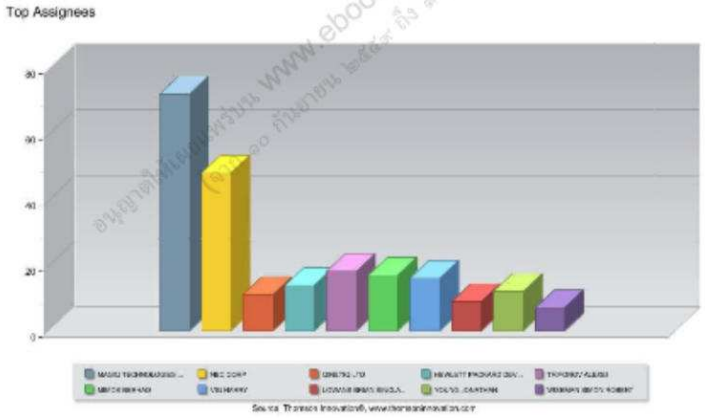
เนื่องจากสาขาวิทยาการรหัสลับเชิงควอนตัมที่เป็นสาขาใหม่ มีสิทธิบัตรจดคุ้มครองที่ปรากฏน้อยกว่าหนึ่งพันเรื่องจากความสามารถสืบค้นของระบบที่เลือกใช้ จากเทคนิคเชิงปฏิบัติการที่การจดสิทธิบัตรโดยทั่วไปจะต่างจากการเผยแพร่ผลงานวิชาการ นั่นคือ การพยายามซ่อนประเด็นสำคัญเชิงคำพูดเพื่อให้คู่แข่งขันทางธุรกิจสืบค้นไม่พบแต่ยังคงข้อถือสิทธิสำคัญ จึงอาจมีประเด็นที่หลุดหลงสืบค้นไปได้มากเช่นกัน ทั้งนี้ ในการสำรวจรายละเอียดปลีกย่อยอาจได้พบทั้งการเลี่ยงการตั้งชื่อเรื่องให้สัมพันธ์กับคำสำคัญ หรือส่วนเนื้อหามีเทคนิคการใช้คำสำคัญอื่น ๆ ฯลฯ ระบบสืบค้นต่าง ๆ อาจสามารถประมวลผลและจัดหมวดหมู่ใหม่โดยสกัดข้อมูลออกมาได้ ส่วนจะมากหรือน้อยนั้นขึ้นอยู่กับเทคนิคและประสบการณ์ในการสืบค้นด้วย รวมทั้งเงื่อนไขการสืบค้นในแต่ละช่วงเวลาอาจมีการเปลี่ยนแปลงจากตัวระบบด้วยเช่นกัน

อีกมุมมองหนึ่งของการสืบค้นวิทยาการรหัสลับเชิงควอนตัม หากได้พิจารณาจากคำสำคัญสามคำที่มีการใช้เรียกชื่อสาขาไอทีอนาคตนี้ในแนวทางที่ต่างกัน อาจได้พบความสัมพันธ์แนวทางอื่นได้ด้วย นั่นคือ 1) quantum cryptography อันหมายถึงตัวระบบครอบคลุมทุกส่วนทั้งหมด 2) quantum key distribution อันหมายถึง ส่วนการกระจายกุญแจรหัสลับเชิงควอนตัมเป็นหลักมิได้รวมถึงระบบสื่อสารทั้งหมดหรือ 3) QKD อันเป็นชื่อย่อเฉพาะของข้อ 2) ซึ่งทั้งสามคำนี้หากได้ทำการสืบค้นร่วมโดยใช้ตัวแปรคัดกรองแบบต่าง ๆ อาจได้ผลที่แตกต่างเช่นกันด้วย ทั้งนี้ ในวงการใหม่นี้ขณะที่ยังไม่มีมาตรฐานอุตสาหกรรมภาคบังคับมากำกับ และความพร้อม (maturity) ของวิทยาการยังไม่ถึงขีดสุด จึงยังคงปรากฏมีการบัญญัติคำใหม่ที่เป็นภาคขยายหรือเสริมคำอื่นที่มีความสำคัญมากขึ้นด้วยเช่น “quantum safe cryptography” [46] [47]อันหมายถึงการปรับแต่งระบบหลายส่วนให้เข้ากับการทำงานของระบบสื่อสารทั่วไป เพื่อความปลอดภัยที่มีอยู่ในยุคสมัยได้หรือคำว่า position-based quantum cryptography device-independent quantum cryptography และ post-quantum cryptography[48] เป็นต้น ดังนั้น การสืบค้นโดยสมบูรณ์จึงยังคงต้องใช้งานระบบที่มีร่วมกับการสืบค้นโดยบุคคล (manual) ที่ควรให้ผลละเอียดได้มากขึ้นนอกเหนือจากเพียงการใช้คำสำคัญหลักใด ๆ

46 *www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography*
47 *en.wikipedia.org/wiki/Quantum_cryptography*
48 *Post-quantum cryptography. Springer, Berlin, 2009. ISBN 978-3-540-88701-0*



4 ก) รายชื่อประเทศและอัตราส่วนที่มีการยื่นขอและได้รับความคุ้มครองสิทธิบัตร



4 ข) รายชื่อบริษัทผู้ยื่นขอและได้รับความคุ้มครอง

ซึ่งผลที่ได้รับจากการพิจารณาผลแยกส่วนด้วยสามคำสำคัญของวงการ พบสิทธิบัตรที่มีความสัมพันธ์ในอีกรูปแบบย่อยหนึ่งจำนวน **342** ชุด (2015-06-24) โดยมีผลสรุปประกอบภาพดังนี้ คือ

แนวโน้มข้อมูลจากรูปที่ 4 ก) สถิติของประเทศที่จดสิทธิบัตรคุ้มครองอาจสังเกตได้ว่าแตกต่างจากบทที่ 3 ที่จำนวนของประเทศสหรัฐอเมริกา ญี่ปุ่นและจีน อยู่ในอันดับสูงสุดตามลำดับ เมื่อพิจารณาในรายละเอียดย่อยแล้วพบว่ายังคงคล้ายคลึงกัน แต่ทำให้ทราบรายละเอียดเพิ่มเติมว่า สิทธิบัตรระบบข้อตกลงสนธิสัญญาสิทธิบัตร PCT (Patent Co-operation Treaty) หรือ WO ที่มีสิทธิบัตรจากประเทศจีนจำนวนมากจดในภาษาต้นฉบับแรก (CN) และขอรับการคุ้มครองในประเทศเป้าหมายอื่น ๆ ต่อตามขั้นตอนของระบบ PCT ที่องค์การทรัพย์สินทางปัญญาโลก (WIPO) จึงปรากฏมีข้อมูลเด่นชัดที่ WO แทนในลำดับที่สองซึ่งรวมสิทธิบัตรจำนวนมากของประเทศจีนและอื่น ๆ ที่มิได้ใช้ภาษาอังกฤษเป็นหลัก

ข้อมูลจากรูปที่ 4 ข) ด้านหน่วยงานผู้ยื่นขอ ยังคงเป็นบริษัท MagiQ Technologies จากประเทศสหรัฐอเมริกาที่มีจำนวนสูงสุด แต่ได้ปรากฏข้อมูล ที่น่า สนใจของ MIMOS BERHAD หน่วยงานการวิจัยและพัฒนาด้านเทคโนโลยีสารสนเทศ จากประเทศมาเลเซีย[49] (MY) ปรากฏเด่นชัดขึ้นมา และเมื่อสืบค้นในรายละเอียดจึงทำให้ทราบถึงกิจกรรมวิจัยที่ได้ผลลัพธ์จำนวนมากจากการพัฒนาต่อยอดเทคโนโลยีของหน่วยงานแห่งนี้ จากการจัดซื้อจัดหามาจากต่างประเทศและเป็นสิทธิบัตรที่จดภายในประเทศก่อนทั้งหมด

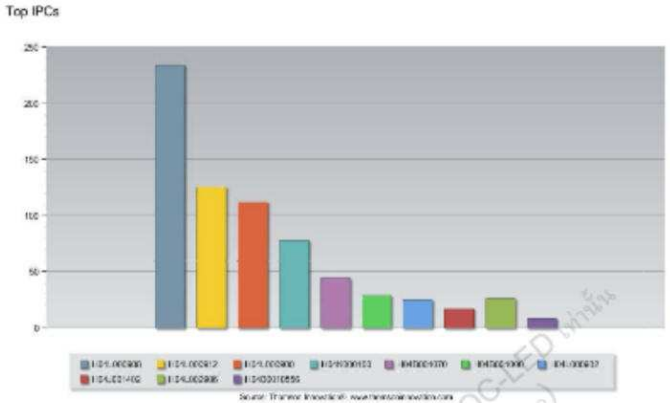
อนึ่ง ประเทศสิงคโปร์และมาเลเซีย เคยเป็นเพียงสองประเทศในเขตเศรษฐกิจอาเซียนที่เป็นสมาชิกของสถาบันมาตรฐานโทรคมนาคมแห่งยุโรป (ETSI)[50] ที่ออกมาตรฐานแนะนำของวิทยาการรหัสลับเชิงควอนตัมโดยเข้าไปมีส่วนร่วมและรับทราบความก้าวหน้าวงใน

ส่วนสถิติอื่น ๆ ยังคงคล้ายคลึงกับบทที่ 3 ที่ยังไม่เด่นชัดอันเนื่องจากเป็นสาขาใหม่ มีจำนวนรวมของสิทธิบัตรน้อย และในส่วนของเทคโนโลยีย่อยพบหมวดสาขาสำคัญ คือ *การสร้างจำนวนสุ่ม การบริหารจัดการกุญแจรหัสลับ ช่องสัญญาณและการสร้างอุปกรณ์ที่ให้ขนาดกระทัดรัดหรือเล็กลง* เช่น

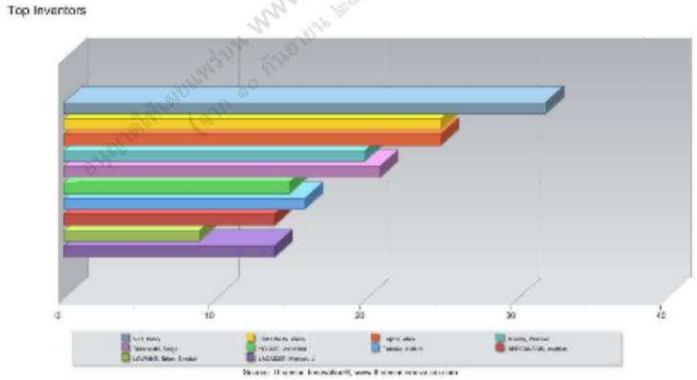
- stabilizer, calibration, Temp compensation, random gen
- higher Key rate, key management, synchronization
- daytime-free space, multi-channel, multi-agent, network, applications
- Integrated Photonics chip, Compact source/ devices

49 *www.mimos.my*

50 *www.etsi.org/technologies-clusters/technologies/quantum-key-distribution*

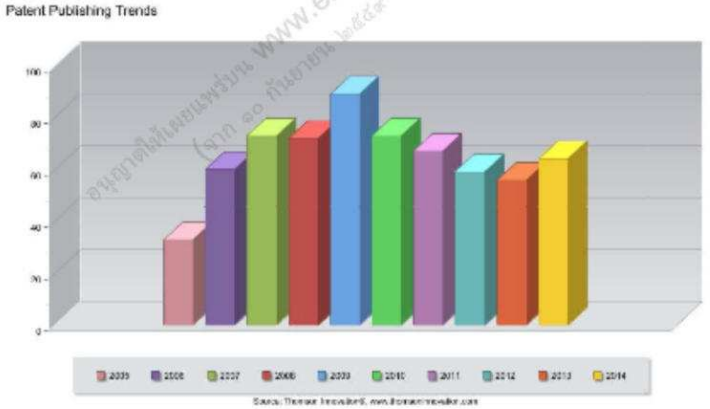


4 ค) หมวดหมู่สาขาวิชาสิทธิบัตรตามระบบ IPC: International Patent Code PC- หมวด H04L000908 (key distribution) หรือ "การกระจายกุญแจรหัสลับ" สูงที่สุด



4 ง) อันดับรายชื่อนักประดิษฐ์หรือผู้จดสิทธิบัตรที่มีได้เด่นชัดกับผู้ใด

4 จ) รูปแสดงแผนที่ ThemeScape



4 ฉ) แนวโน้มจำนวนสิทธิบัตร"ทั่วโลกของ
ช่วงปีพ.ศ.2549 (ค.ศ.2006) จนถึงพ.ศ.2558 (ค.ศ.2015)

ข้อมูลสิทธิบัตรของบริษัท ID Quantique 5

จากต้นกำเนิดการป้องกันคัดลอกธนบัตรด้วยการใช้ "กลศาสตร์ควอนตัม" ของ "สตีเฟน วีสเนอร์" (Stephen Wiesner) ช่วงปี พ.ศ.2513 ได้ถูกนำมาต่อยอดในปี พ.ศ. 2527 หลังจากที่ ชาร์ลส์ เบนเนตต์ (Charles Bennett) จากไอบีเอ็ม และ จิลส์ บราสซาร์ด (Gilles Brassard) แห่งมหาวิทยาลัยมอนทรีออล ได้ร่วมกันวิจัยการใช้สถานะควอนตัมมาแทนข้อมูลที่ทำให้ได้มาซึ่งกุญแจรหัสลับร่วมกันระหว่างคู่ของผู้ที่สื่อสารกันอยู่ จนได้มีการทดลองในห้องปฏิบัติการเพื่อพิสูจน์หลักการเป็นครั้งแรกเมื่อปี พ.ศ.2535 พบว่าสามารถสร้างใช้งานได้จริง

หลังจากนั้น อุปกรณ์กระจายกุญแจรหัสลับเชิงควอนตัม (quantum key distributor) จึงเริ่มมีผลิตจำหน่ายได้ในทศวรรษต่อมาตั้งแต่ ปี พ.ศ.2546 โดยบริษัท iD Quantique ประเทศสวิสเซอร์แลนด์ อันมีต้นกำเนิดมาจากวิทยานิพนธ์ปริญญาเอกของนักศึกษาสัญชาติฝรั่งเศส (Gregoiry Ribordy) กับทีมงานของมหาวิทยาลัยเจนิวา บริษัทนี้ได้รับรางวัลทั้งนวัตกรรมดีเด่นและบริษัทตั้งใหม่ต้นแบบ (startup label[51]) นำสินค้าต้นแบบไปสาธิตกับการรักษาความปลอดภัยข้อมูลการเลือกตั้งมาด้วยแล้ว และยังคงเป็นบริษัทที่เปิดทำการต่อเนื่องแม้เกิดบริษัทคู่แข่งผลิตสินค้าทำนองเดียวกันออกมาหลายแห่ง (BBN MajiQ Toshiba SmartQuantum หรือ SeQureNet ฯ) แต่ได้มีปิดตัวลงหรือเงียบหายไปเช่นกัน กระนั้น บริษัท iDQuantiue ก็ยังคงมีธุรกิจและกิจกรรมที่เด่นชัดมาโดยตลอดกว่าทศวรรษแล้ว จึงนับว่าเป็นบริษัทที่เป็นต้นแบบผลิตสินค้าด้านรหัสลับเชิงควอนตัมที่น่าศึกษายิ่ง

ดังนั้น การศึกษาแนวทางเชิงลึกของเทคโนโลยีจากบริษัทแห่งนี้ผ่านสิทธิบัตรชิ้นสำคัญจึงอาจทำให้พบทั้งประวัติการพัฒนาในอดีตและแนวโน้มในอนาคตได้ด้วย รวมทั้งช่องทางโอกาสอื่น ๆ ด้วยเช่นกัน

นอกจากการสำรวจนอกจากสิทธิบัตรล่าสุดอันเป็นผลมากจากข่าว "การแฮกควอนตัม (quantum hacking)[52]" (*บทที่ 3 ตัวอย่างที่ 1*) แล้ว ได้พบสิทธิบัตรสามชุดสำคัญโดยสัมพันธ์กับสินค้า อันเป็นพัฒนาการของบริษัทเกิดใหม่ (start up) ที่ชัดเจนดังต่อไปนี้

---

51 *www.ctistartup.ch/en/startups/overview-startups/476-id-quantique/*

52 ***US2014/0119537A1** 2014-01-14 (APPARATUS AND METHOD FOR THE DETECTION OF ATTACKS TAKING CONTROL OF THE SINGLE PHOTON DETECTORS OF A QUANTUM CRYPTOGRAPHY APPARATUS BY RANDOMLY CHANGING THEIR EFFICIENCY)*

สิทธิบัตรหมายเลขจดทะเบียน ณ สหรัฐอเมริกา : US7519641B2
(หมายเลขตีพิมพ์อื่น US7447721B2 และ US20070127718A1)

ผู้ยื่น: Ribordy, Gregoire | Guinnard, Olivier
Title: Method and apparatus for generating true random numbers by way of a quantum optics process
ชื่อเรื่อง: วิธีและอุปกรณ์สำหรับการสร้างจำนวนสุ่มแท้โดยวิธีการทางทัศนศาสตร์

หมายเลขถือสิทธิอ้างอิงแรก (Priority number) : US2003497907P
วันที่ถือสิทธิอ้างอิงแรก (Priority date) : 2003-08-27
วันยื่นขอจด (Application date) : 2004-08-17
วันที่ได้รับการประกาศ (Publication date) : 2009-04-14
หมายเลขการจัดจำแนกสิทธิบัตร : G06F000102[53] (Digital function generators) และ G06F000758[54] (Random or pseudo-random number generators)

Abstract: A method and apparatus for generating true random numbers by way of a quantum optics process uses a light source to produce a beam which illuminates a detector array. The detectors of the array are associated with random numbers values. Detection of a photon by one of the detectors yields a number whose value is equal to that associated with the detector. This procedure is repeated to produce sequences of true random numbers. The randomness of the numbers stems from the transverse spatial distribution of the detection probability of the photons in the beam. If the array is made up of two detectors, the true random numbers produced are binary numbers. The process can be sped up using an array having pairs of two detectors. Using an array having more than two detectors also allows generating true random numbers of dimension higher than two. The primary object of the invention is to allow generating true random numbers by way of a quantum optics process.

53 *worldwide.espacenet.com/classification#!/CPC=G06F1/00*
54 *worldwide.espacenet.com/classification#!/CPC=G06F7/58*

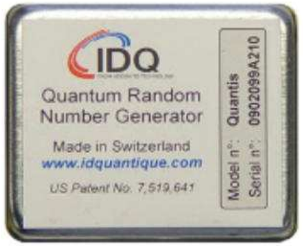
บทคัดย่อ: วิธีการและเครื่องมือสำหรับการสร้างจำนวนสุ่มแท้ด้วยวิธีกระบวนการทางแสงเชิงควอนตัมใช้แหล่งกำเนิดแสงในการผลิตลำแสงเพื่อส่งไปยังชุดของหน่วยตรวจจับสัญญาณ ซึ่งหน่วยตรวจจับเหล่านี้จะสัมพันธ์กับค่าจำนวนสุ่มที่จะได้ นั่นคือ การตรวจจับโฟตอนใดของหน่วยตรวจจับหนึ่งเมื่อตรวจวัดได้จะให้เป็นค่าจำนวนสุ่มหนึ่งที่สัมพันธ์กันด้วยโอกาสที่เท่าเทียมกันกับหน่วยอื่น ๆ ขั้นตอนการตรวจจับและให้จำนวนสุ่มนี้จะทำซ้ำเพื่อการผลิตชุดของจำนวนตัวเลขสุ่มแท้ออกมาในที่สุด โดยรูปแบบของการเป็นจำนวนสุ่มจะเกิดจากการโอกาสกระจายตัวของโฟตอนตามแนวต่าง ๆ ในลำแสง หากชุดตรวจรับจับสุญญาณได้จากหน่วยตรวจจับสองชุด จำนวนสุ่มแท้ที่ได้จะเป็นเลขฐานสองคือ ศูนย์หรือหนึ่ง จากหน่วยใดหน่วยหนึ่ง โดยกระบวนการสร้างชุดจำนวนสุ่มนี้สามารถทำได้เร็วขึ้นด้วยการใช้หน่วยตรวจจับมากกว่าสองช่วยให้การสร้างตัวเลขสุ่มที่แท้จริงของมิติที่สูงขึ้นกว่าจำนวนตัวอย่างแค่สองข้างต้นได้

หมายเหตุ: ผลงานจากสิทธิบัตรนี้ บริษัท ID Quantique ได้นำไปผลิตเป็นสินค้าจำหน่าย โดยมีพัฒนาการการประยุกต์ นอกจากเป็นแหล่งกำเนิดจำนวนสุ่มใช้เพื่อเป็นชุดจำนวนเริ่มต้น (seed) เพื่อการสร้างชุดรหัสลับ (ที่ต้องการจำนวนสุ่มที่มีความเข้มแข็ง ยากต่อการคาดเดาหรือคำนวณหาค่า รหัสลับนั้นจึงจะมีความปลอดภัยสูง) ยังมีการประยุกต์แนวอื่นได้อีกมากและหลากหลาย สินค้านี้ได้รับมาตรฐาน (certified) และมีรูปแบบที่มีคุณลักษณะเฉพาะตัว (specification)[55] ที่เด่นชัด โดยพัฒนาความเร็วของจำนวนสุ่มที่ได้ตั้งแต่เดิมจาก 4 ล้านบิตต่อวินาที (M bps) มาสู่ 16 M bps แล้ว เช่นรูปแบบ

- USB device – random stream ที่อัตรา 4 Mbits/sec
- PCI Express (PCIe) board – random stream อัตรา 4 Mbits/sec และ 16Mbits/sec
- PCI board – random stream 4 Mbits/sec และ 16 Mbits/sec

จึงนับได้ว่าเป็นผลงานวิจัยที่มีความสมบูรณ์ตั้งแต่การเป็นงานวิจัยเพื่อการศึกษา การผันงานวิจัยสู่การเป็นธุรกิจ (spin-off) จนกลายเป็นสินค้าเทคโนโลยีของบริษัทก่อตั้งใหม่ (startup) ที่ประสบผลสำเร็จและพัฒนาตนเองมาอย่างต่อเนื่อง

55 *www.idquantique.com/random-number-generation/quantis-random-number-generator/*



5 ก) ตัวถังขนาดเล็กบรรจุอุปกรณ์ทัศนศาสตร์และอิเล็กทรอนิกส์ เพื่อการกำเนิดจำนวนสุ่มเชิงควอนตัมแสง (หมายเลขสิทธิบัตรบนตัวถัง)

5 ข) การประยุกต์อุปกรณ์กับแผ่นเชื่อมต่อสัญญาณ (PCI board) และแบบ USB เพื่อเพิ่มมูลค่าและแนวทางการสร้างจำนวนสุ่มเชิงควอนตัมแสง

สิทธิบัตรหมายเลขจดทะเบียนโลก : WO2006024939B1

(หมายเลขตีพิมพ์อื่น คือ AT426282T, CN101040483A, CN101040483B, DE602005013393D1, EP1784944A2, EP1784944B1, US7929690, US8995650, US20080292099, US20100239250, WO2006024939A2, และ WO2006024939A3)

ผู้ยื่น: GISIN NICOLAS | RIBORDY GREGOIRE | ZBINDEN HUGO

Title: TWO NON-ORTHOGONAL STATES QUANTUM CRYPTOGRAPHY METHOD AND APPARATUS WITH INTRA-AND INTER-QUBIT INTERFERENCE FOR EAVESDROPPER DETECTION

ชื่อเรื่อง: อุปกรณ์และวิธีการรหัสลับเชิงควอนตัมแบบสองสถานะที่ไม่ตั้งฉากรวมการแทรกสอดทั้งภายในและนอกเพื่อการตรวจจับการดักฟังข้อมูล

หมายเลขถือสิทธิอ้างอิงแรก (Priority number) : US2004606793P

วันที่ถือสิทธิอ้างอิงแรก (Priority date) : 2004-09-02

วันยื่นขอจด (Application date) : 2005-09-01

วันที่ได้รับการประกาศ (Publication date) : 2006-08-17

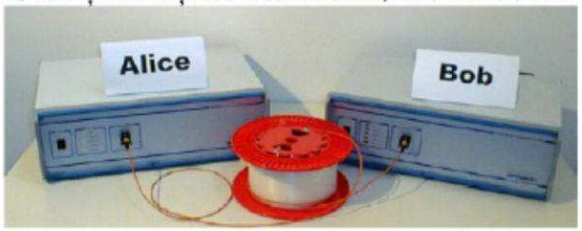
หมายเลขการจัดจำแนกสิทธิบัตร : IPC H04L000908[56] (Key Distribution หรือ การกระจายกุญแจรหัสลับ)

Abstract: An apparatus and method for implementing a secure quantum cryptography system using two non-orthogonal states. For each qubit, the to emitter station prepares a quantum system in one of two non-orthogonal quantum states in the time-basis to code bit values. Intra-and inter-qubit interference is then used to reveal eavesdropping attempts. Witness states are used to help reveal attacks performed across the quantum system separation.

บทคัดย่อ: อุปกรณ์และวิธีการรหัสลับเชิงควอนตัมแบบสองสถานะที่ไม่ตั้งฉาก โดยสำหรับคิวบิตหรือสถานะทางควอนตัมใด ๆ ที่สร้างขึ้นจากการที่ภาคส่งจะเตรียมระบบควอนตัมหนึ่งมาจากสองสถานะทางควอนตัมที่ไม่ตั้งฉากกันบนพื้นฐานของเวลาที่กำหนดเพื่อเข้ารหัสเป็นค่าบิต ซึ่งการแทรกสอดทั้งภายในและนอกต่อระบบจะใช้เพื่อการตรวจจับความพยายามในการดักฟังข้อมูลโดยสถานะเทียบเคียงจะถูกนำมาใช้เพื่อการสำรวจหาการบุกรุกระหว่างตัวระบบ

56 www.uspto.gov/web/patents/classification/cpc/html/cpc-H04L.html
(or management, e.g. generation, sharing or updating, of cryptographic keys or passwords)

5 ค) เครื่องรุ่น Clavis รุ่นแรก ราคาประมาณ 88,000 $ เมื่อปีค.ศ. 2002



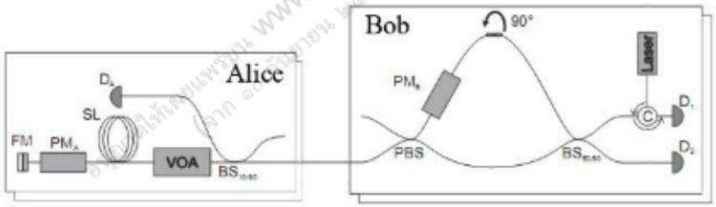
5 ง) เครื่องรุ่น Clavis II ราคาประมาณ 5 ล้านบาท (143,900 CHF) เมื่อ ปีค.ศ. 2009

5 จ) เครื่องรุ่น Cerberis ราคาประมาณ 5 ล้านบาท เมื่อปี ค.ศ. 2008 - 2010

หมายเหตุเทคนิค: *การเข้ารหัสด้วยเฟส (Phase-encoding)*[57]

เครื่องกระจายกุญแจรหัสลับควอนตัมของบริษัท ID Quantique ได้นำหลักการที่จดสิทธิบัตรคุ้มครองมาจัดสร้างเป็นเครื่อง“Plug & Play Autocompensating QKD” จำหน่ายไปทั่วโลก ยังคงเป็นบริษัทเดียวที่สามารถพัฒนาเครื่องต้นแบบและมีโครงการสร้างเครือข่ายสื่อสารปลอดภัยขนาดใหญ่อย่างต่อเนื่องในหลายประเทศลูกค้า ซึ่งระบบบนพื้นฐานสิทธิบัตรดังกล่าวอธิบายการทำงานภายในเพิ่มเติม ดังนี้

สถานะทางควอนตัมจะแทนข้อมูลด้วยมุมเฟสโดยมีอุปกรณ์หลัก คือ กระจกฟาราเดย์ (Faraday Mirror) ซึ่งทำหน้าที่สะท้อนแสงกลับพร้อมทั้งหมุนโพลาไรเซชันไป 90 องศา ทำให้โฟตอนที่เคลื่อนที่จากฝั่ง *Bob* (ภาครับ) ผ่านเส้นทางสั้น หากสมมติว่ามีโพลาไรซ์แนวนอน แต่ในขากลับโพลาไรซ์จะถูกเปลี่ยนเป็นแนวตั้งและถูกสะท้อนที่กระจกแยกลำแสงโพลาไรซ์ (Polarizing beamsplitter: PBS) เข้าสู่เส้นทางยาว ส่วนโฟตอนที่ขาไปผ่านเส้นทางยาว ขาย้อนกลับจะผ่านเส้นทางสั้นด้วยหลักการเดียวกัน ทำให้ระยะทางที่โฟตอนสองสถานะวิ่งผ่านมีระยะเท่ากันทุกประการ และจากการเพิ่มการเลื่อนเฟส (Phase modulation) จะทำให้วิธีดังกล่าวทำเสมือนมาตรแทรกสอดแบบแมส- แชนเดอร์ (Mach-Zehnder interferometer) ที่สมบูรณ์ได้ นอกจากนี้ผลการเปลี่ยนแปลงทิศโพลาไรซ์เนื่องจากสายไฟเบอร์ยังถูกชดเชยอัตโนมัติเมื่อแสงเคลื่อนที่ย้อนกลับดังรูป



5 ฉ) รูปการทำงานของระบบ “Plug & Play Autocompensating QKD” ซึ่งแทนข้อมูลด้วยมุมเฟส เมื่อ FM คือกระจกฟาราเดย์ PM คืออุปกรณ์มอดูเลตทางเฟส SL คือ ขดเส้นใยแสงระยะสั้น D คือตัวตรวจหา VOA คืออุปกรณ์ปรับความเข้มแสง BS คืออุปกรณ์แยกแสง C คืออุปกรณ์เปลี่ยนแนวแสงไปยังเส้นทางทวนเข็มนาฬิกา (idquantique.com)

57 หน้า 2-19: พัฒนาการสารสนเทศเชิงควอนตัม ISBN: 978-616-12-0212-5 (www.ebooks.in.th/ebook/7748/)

สิทธิบัตรหมายเลขจดทะเบียนสหรัฐอเมริกา: US8320774B2
(หมายเลขดีฟิมพ์อื่น US20090010435 A1)

ผู้ยื่น: Zbinden, Hugo
Title: Apparatus and method for adjustment of interference contrast in an interferometric quantum cryptography apparatus by tuning emitter wavelength
ชื่อเรื่อง: อุปกรณ์และวิธีการปรับแต่งการแทรกสอดในอุปกรณ์อิเทอร์เฟียโร ของรหัสลับเชิงควอนตัมโดยการปรับจูนค่าความยาวคลื่นของตัวส่ง

หมายเลขถือสิทธิอ้างอิงแรก (Priority number) : US2007774582A
วันที่ถือสิทธิอ้างอิงแรก (Priority date) : 2007-07-07
วันยื่นขอจด (Application date) : 2007-07-07
วันที่ได้รับการประกาศ (Publication date) : 2012-11-27
หมายเลขการจัดจำแนกสิทธิบัตร : IPC H04B10/00[58] หมวดระบบการสื่อสัญญาณ (transmission systems employing electromagnetic waves other than radio-waves, e.g. infrared, visible or ultraviolet light, or employing corpuscular radiation, e.g. quantum communication)

Abstract: An apparatus and method are disclosed for maximizing interference contrast in an interferometric quantum cryptography system to detect eavesdropping by utilizing a tunable emitter station in communications with a receiver station via a quantum communications channel and a public communications channel. The tunable emitter station tracks and compensates for interferometer drifts by adjusting the interference contrast of the QC system to minimize or eliminate inherent perturbations induced into key bit transmissions. Tuning of the photo emitter's output wavelength is accomplishable using temperature and/or drive current adjustment of the emitter's tunable optical subsystem.

58 *worldwide.espacenet.com/classification#!/CPC=H04B10/00*
(or management, e.g. generation, sharing or updating, of cryptographic keys or passwords)

บทคัดย่อ: อุปกรณ์และวิธีที่เปิดเผยนี้เพื่อการแทรกสอดในอุปกรณ์อินเทอร์เฟียโรของระบบรหัสลับเชิงควอนตัมให้ได้ค่าสูงที่สุด เพื่อการตรวจจับการลักลอบต่อท่อพ่วงสาย ทั้งนี้ ด้วยการใช้ตัวส่งที่ปรับจูนค่าความยาวคลื่นได้เพื่อการสื่อสารกับภาครับ ทั้งในช่องสัญญาณกุญแจรหัสหรือช่องสัญญาณควอนตัมและช่องสัญญาณสาธารณะ โดยสถานีตัวส่งปรับแต่งจากการติดตามและชดเชยค่าที่เกิดการเคลื่อนไปในอุปกรณ์อินเทอร์เฟียโร และด้วยการปรับค่าความชัดเจนของการแทรกสอดในตัวระบบรหัสลับควอนตัม เพื่อที่จะลดการรบกวนที่จะมีผลกับตัวกุญแจรหัสให้มีค่าต่ำที่สุด การปรับค่าที่ความยาวคลื่นนั้นจะกระทำโดยปรับที่ค่าอุณหภูมิและ/หรือ ค่ากระแสที่ใช้ขับระบบย่อยของการส่ง

สรุป ภาพรวมสามสิทธิบัตรหลักของบริษัทผู้ผลิตเครื่องกระจายกุญแจรหัสลับเชิงควอนตัม (quantum key distribution) นี้ ประกอบไปด้วยเทคโนโลยีพื้นฐาน คือ

- วิธีและอุปกรณ์สำหรับการสร้างจำนวนสุ่มแท้โดยวิธีการทางทัศนศาสตร์
  (อุปกรณ์ต้นกำเนิดการสร้างรหัสลับคุณภาพ)
- อุปกรณ์และวิธีการรหัสลับเชิงควอนตัมแบบสองสถานะที่ไม่ตั้งฉากรวมการแทรกสอดทั้งภายในและนอกเพื่อการตรวจจับการดักฟังข้อมูล
  (อุปกรณ์สร้างและกระจายกุญแจรหัสลับเชิงควอนตัม)
- อุปกรณ์และวิธีการปรับแต่งการแทรกสอดในอุปกรณ์อิเทอร์เฟียโรของตัวระบบรหัสลับเชิงควอนตัมโดยการปรับจูนค่าความยาวคลื่นของตัวส่ง
  (อุปกรณ์ปรับแต่งค่าเพื่อเพิ่มประสิทธิภาพของระบบ ฯ)

ซึ่งแนวทางนี้ เป็นเทคโนโลยีหลักของบริษัท ฯ ที่จำหน่ายเครื่องมือเพื่อการรักษาความลับจากการทำการพ่วงหรือต่อท่อโดยบุคคลที่สาม (eavesdropper) กระนั้นอุปกรณ์นี้ก็พบว่ายังมีข้อด้อยเรื่องอัตราการผลิตกุญแจรหัสลับที่ไม่สูงมาก และลดลงตามระยะทางของการสื่อสารผ่านเส้นใยนำแสงสำหรับการเป็นช่องสัญญาณควอนตัมเพื่อการส่งกุญแจรหัส

ต่อมาปี พ.ศ. 2559 บริษัทนี้ได้ออกผลิตภัณฑ์รุ่นใหม่ Clavis III [59]โดยเปลี่ยนพื้นฐานเทคโนโลยีจากการใช้เฟส (Phase-encoding) ข้างต้น มาเป็น Coherent One-Way (COW) Protocol ที่ให้ความเร็วในการสร้างกุญแจรหัสลับได้สูงและมากกว่ารุ่นเดิม

59 *www.idquantique.com/photon-counting/clavis3-qkd-platform/*

อนึ่ง สำหรับสิทธิบัตร **ตัวอย่าง 1) US2014/0119537A1** ของบทที่ 3 นั้น พบว่า มีความสัมพันธ์กับข่าวเรื่องการเจาะระบบควอนตัม (quantum hacking) อันเป็นสิทธิบัตรที่มีคุณค่าทั้งเชิงการพัฒนาระบบ รวมไปถึงการตอบสนองต่อข่าวเทคโนโลยีที่คลาดเคลื่อนได้เป็นอย่างดี (บทความก่อนหน้า[60]) เนื่องจากกิจการด้านความมั่นคงปลอดภัยจะขึ้นอยู่กับความมั่นใจของผู้ใช้งานเป็นหลักด้วยเช่นกัน แม้ข่าวด้านลบที่มิได้เป็นจริงแต่อาจส่งผลเชิงจิตวิทยาและกระทบต่อความเชื่อมั่นได้ โดยมีรายละเอียดดังนี้

รหัสลับเชิงควอนตัมกำเนิดมาเพื่อป้องกันการพ่วง (หรือ tap) ระหว่างการสื่อสารข้อมูลและระหว่างทางของผู้ส่งและผู้รับที่ติดต่อกันอยู่ มีความสมบูรณ์แบบรับประกันด้วยกฎพื้นฐานทางฟิสิกส์ (uncertainty principle) แต่กลับมีข่าวว่าระบบนี้โดนแฮกหรือเจาะระบบได้โดยนักวิจัยจากประเทศนอร์เวย์และแคนาดา[61] (รวมทั้งมีงานวิจัยอ้างถึงนี้จากประเทศไทยอีกด้วย) ปรากฏเป็นข่าวในหลายแห่ง (เช่น บีบีซี BBC)[62] แม้มีข้อสรุปว่ามิได้เกี่ยวข้อง "โดยตรง" เป็นความสับสนการตั้งชื่อและการพยายามอาศัยช่องว่างของความใหม่ในเทคโนโลยีชนิดนี้ แต่กลับเป็นข่าวเทคโนโลยีที่ได้รับความนิยม ซึ่งแน่นอนว่าส่งผลต่อความมั่นใจต่อ "รหัสลับควอนตัมปลอดภัย 100%" และอธิบายได้โดยลำดับพื้นฐานต่อไปนี้

เรื่องการแฮก (hacking) ทั่วไปที่คุ้นเคยนั้น หากมีการแฮกระบบจะหมายถึงการแอบเข้าไปขโมยและทำสิ่งผิดปกติ เช่น เปลี่ยนข้อมูลหรือทิ้งปัญหาทั้งที่จงใจให้ทราบหรือไม่ก็ตาม อาทิ การแฮกที่มหาวิทยาลัยแคลิฟอร์เนีย (Berkeley)[63] ออกข่าวเมื่อ 26 กุมภาพันธ์ ปี พ.ศ. 2559 ว่าได้สำรวจระบบคอมพิวเตอร์จากการถูกโจมตี (cyberattack) บนข้อมูลการเงินของทั้งนักศึกษา ศิษย์เก่า ฯลฯ กว่า 80,000 รายชื่ออันมีช่องโหว่ (data breach) อาจได้รับผลกระทบ ซึ่งก็คือการแอบเข้าระบบ เป็นต้น

เมื่อกลับมาพิจารณาเรื่องระบบรหัสลับเชิงควอนตัมถูกแฮก หมายถึงกรณีที่ฟิสิกส์ทำการ "แฮกแสง (โฟตอน)" ด้วยเทคนิคการไปแอบฝังตัวอยู่ในภาครับแสง (detector) โดยเปิดเครื่องต่ออุปกรณ์ ณ สถานที่ติดตั้งระบบ ซึ่งแม้จะตั้งชื่อเป็นการแฮกเชิงควอนตัมแต่แท้จริงเป็นศึกษาคุณภาพเชิงลึกของอุปกรณ์รับแสง (quantum efficiency) เพื่อจัดการโฟตอนของนักฟิสิกส์ (loopholes in quantum) กับความไม่เป็นอุดมคติหรือสมบูรณ์ของอุปกรณ์ ซึ่งผลก็ได้รับการตีพิมพ์ในวารสารดังระดับโลกจำนวนมาก[64]

60 *ไอที่ควอนตัมถูกแฮก (3) : Quantum Hacking ? เคลียร์ชัวร์ออนไลน์ หรือ https://goo.gl/eS3xRF*

61 *www.vad1.com/lab/*

62 *www.bbc.com/news/technology-14505750*

63 *goo.gl/eg49yF*

64 *www.vad1.com/lab/publications.html*

ข้อสังเกต:

ก) รหัสลับควอนตัมสมบูรณ์แบบป้องการต่อท่อร้อยสาย (eavesdropping/ wire tapping) หรือการขโมยระหว่างทาง แต่กิจกรรมแบบที่นักฟิสิกส์ตั้งชื่อการการแฮกเชิงควอนตัมนั้นเสมือนเป็นการปล้น (มิใช่การขโมย) และเป็นการปล้นระดับโฟตอนหรือแสง (physical layer) มิใช่ตัวข้อมูลที่อยู่ในระดับการสื่อสารมาตรฐานระดับสูง (higher layers – OSI 7 layers) ไม่มีมุมด้านมาตรฐานวิศวกรรมการสื่อสารที่ปฏิบัติได้ครบในระบบไอทีปกติทั่วไป จึงมีคำจัดความว่าอาจคือโฆษณาแฝง (self-promote) คล้ายเรื่องไวรัสคอมพิวเตอร์ที่หลายพันธุ์ถูกปล่อยออกมาจากบริษัทขายซอฟท์แวร์กำจัดไวรัส (anti-virus) นั้นเสียเอง

*ข) สิทธิบัตร **ตัวอย่าง 1)** US2014/0119537A1 (**อุปกรณ์และวิธีการสำหรับควบคุมตรวจจับการบุกรุกหน่วยรับแสงโฟตอนเดี่ยว ของรหัสลับเชิงควอนตัมโดยการปรับเปลี่ยนประสิทธิภาพแบบสุ่ม**) ของบริษัท ID Quantique ได้พัฒนาเพื่อปิดช่องว่างของการ "ขโมย" โฟตอนนั้น แม้ไม่พบว่าการแฮกเชิงควอนตัมจะมีผลใด ๆ ต่อการ "ป้องการต่อท่อร้อยสาย (eavesdropping/ wire tapping) หรือการขโมยระหว่างทาง" ซึ่งสังเกตได้ว่า แม้หลักการของสิทธิบัตรดังกล่าวจะได้นำไปประกอบสร้างใช้งานหรือไม่ก็ตาม แต่สิทธิบัตรนี้อาจมีผลทางจิตวิทยาที่ใช้สร้างความเชื่อมั่นต่อสินค้าของบริษัทเป็นอย่างดีว่า บริษัทที่ได้รับผลกระทบนี้ได้ปรับปรุงดำเนินการป้องกันแล้ว*

อนึ่ง สำหรับผลิตภัณฑ์ต้นแบบหรือการประยุกต์ใช้งานจริงนอกจากของบริษัท ID Quantique นี้แล้ว ยังมีคู่แข่งจากทั้งบริษัท QAsky บริษัทบ่มเพาะ (spin-off) ของมหาวิทยาลัยที่มีผลงานวิชาการสูงสุดในโลกด้านนี้จากประเทศจีน (USTC) และล่าสุดประเทศเกาหลีใต้ได้เริ่มประกาศจำหน่ายแล้วจากบริษัทเอกชนด้านโทรคมนาคมเดิมคือ SK Telecom โดยปรากฏสิทธิบัตรคุ้มครองจำนวนหนึ่งกระจายอยู่ในงานเทคนิคส่วนย่อยต่าง ๆ ในรายการสำรวจนี้ด้วย ส่วนบริษัทที่ก่อตั้งก่อนหน้าทั้ง Toshiba UK มีต้นแบบหลายรุ่นแต่ไม่พบข่าวการจำหน่าย โดยที่บริษัท SmartQuantum MagiQ และ SeQureNet ที่เคยมีชื่อเสียง ได้ทยอยปิดตัวหรือลดส่วนงานที่เกี่ยวข้องกับรหัสลับควอนตัมออกไปแล้ว (*อ้างอิง ข้อมูลสำรวจคู่ขนานใน White paper 2016: ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed 2016), Q-Thai.Org*)

พิจารณ์และข้อเสนอ 6

หลังการกำเนิดวิทยาการรหัสลับเชิงควอนตัมจากการตีพิมพ์ผลงานของ ชาร์ลส์ เบนเนตต์ (Charles Bennett) จาก บริษัทไอบีเอ็ม และจิลส์ บราสซาร์ด (Gilles Brassard) จาก มหาวิทยาลัยมอลทรีออล ประเทศแคนาดาในปี ค.ศ. 1984 แล้ว ผลงานการคิดค้นที่เกี่ยวข้องจึงได้เริ่มปรากฏเพิ่มขึ้นมาโดยตลอดและมีแนวโน้มสูงขึ้นต่อไป นอกจากการศึกษาผลงานวิชาการของ “รหัสลับเชิงควอนตัม” ที่ทำให้ทราบถึงความก้าวหน้าพื้นฐานแล้ว ทรัพย์สินทางปัญญาคืออีกหนึ่งหัวข้อสำคัญอันเป็นดัชนีที่สามารถใช้วัดผลการพัฒนาประเทศได้ด้วย ทั้งนี้ เมื่อได้พิจารณาเน้นหนักลงลึกกับทรัพย์สินทางปัญญาโดยเฉพาะกับ เทคโนโลยีอุบัติใหม่ที่เพิ่งได้รับความสนใจในโลกและยังมีการยื่นขอรับการคุ้มครองการประดิษฐ์คิดค้นที่ยังไม่สูงมาก นักของสาขารหัสลับเชิงควอนตัมนี้ ทำให้ได้พบกับมุมมองที่สามารถสร้างโอกาส รวมทั้งลดช่องว่าง อันจะยังประโยชน์ในการเลือกซื้อจัดหาหรือใช้งานได้อย่างคุ้มในอนาคต รวมทั้งเป็นการสร้างภูมิคุ้มกันทางภูมิปัญญาให้สามารถพึ่งพาตนเองได้มากที่สุดหากเกิดข้อพิพาทจากการลงทุนในอนาคตต่อความซับซ้อนของวิทยาการสาขานี้ได้ เพื่อมิให้เสียโอกาสเช่นในอดีตทั้งกรณีนำเข้าระบบวิทยาการขนาดใหญ่ต่าง ๆ หรือเรื่องหลอกลวง (fraud) ที่อิงเทคโนโลยีเช่น กรณีของ GT200 ที่เกิดความเสียหายสูงมาก เป็นต้น

ความก้าวหน้าวิชาการของวงการวิทยาการรหัสลับเชิงควอนตัมทั่วโลก แนวโน้มมีปรากฏสูงมากขึ้นจากประเทศโลกฝั่งตะวันออกทั้งประเทศจีน ญี่ปุ่นและสิงคโปร์ ข้อมูลผลงานวิจัยเหล่านี้อยู่ในหมวดหมู่ที่ประเมินได้ว่ายังเป็นการพัฒนาขั้นพื้นฐาน เนื่องจากเกี่ยวโยงกับด้านสาขาวิชาฟิสิกส์สูงถึง 70% ขณะที่การประยุกต์กับสาขาวิทยาการคอมพิวเตอร์ และสาขาวิศวกรรมศาสตร์คาบเกี่ยวที่ 25% และ 23% โดยลำดับ สรุปโดยรวมสำหรับวิทยาการรหัสลับเชิงควอนตัม วงการวิชาการกำลังสร้างฐานตนเองที่แข็งแกร่งมากขึ้นทุกปีโดยและประเทศจีนคงความเป็นผู้มีผลงานก้าวหน้าสูงที่สุดอย่างต่อเนื่อง

สำหรับด้านทรัพย์สินทางปัญญา จากสถิติมีแนวโน้มทยอยสูงขึ้นทุกปีเช่นกัน แต่ยังไม่เด่นชัดนักเนื่องจากเป็นสาขาใหม่มีจำนวนรวมของสิทธิบัตรทั่วโลกในระดับน้อย โดยที่ประเทศสหรัฐอเมริกามีจำนวนรวมสูงสุดตามด้วยนัยสำคัญการเติบโตที่สูงมากของประเทศจีน สำหรับในส่วนของหมวดสาขาเทคโนโลยีย่อยพบว่ามีพัฒนาการที่สำคัญกับด้าน การสร้างจำนวนสุ่ม การบริหารจัดการกุญแจรหัสลับ ช่องสัญญาณและการสร้างอุปกรณ์ที่ให้ขนาดกระทัดรัดหรือ

เล็กลง รูปแบบการประยุกต์เข้ากับระบบสื่อสารโทรคมนาคมปกติ เทคนิคการพัฒนาอุปกรณ์ประกอบย่อยอื่น ๆ ส่วนด้านการสร้างสถานะเชิงควอนตัมอันเป็นหัวใจของวิทยาการนี้นั้นพบด้าน เทคนิคผสมทั้งเฟส โพราไรซ์และเทคนิคตัวแปรต่อเนื่อง (continuous variable) ส่วนเทคนิคความพัวพัน (entanglement) นั้นพบน้อยมาก ขณะที่หมวดหมู่ของสิทธิบัตร (IPC) ได้ปรากฏมีหมวดเฉพาะการบริหารการกระจายกุญแจรหัสลับแล้ว คือ H04L000908

ส่วนด้านสินค้าอุปกรณ์กระจายกุญแจรหัสลับเชิงควอนตัม (quantum key distributor) ที่ได้เริ่มมีจำหน่ายมาตั้งแต่ ปี พ.ศ. 2546 มาแล้วนั้น บริษัท iD Quantique ประเทศสวิสเซอร์แลนด์ ยังคงเป็นบริษัทต้นแบบผลิตสินค้าด้านรหัสลับเชิงควอนตัมแถวหน้าของโลก มีสิทธิบัตรคุ้มครองครบวงจรของระบบหลัก แต่กระนั้น ได้มีแนวโน้มว่าบริษัทจากประเทศจีนและเกาหลีใต้จะกลายมาเป็นคู่แข่งในอนาคต

สำหรับในกลุ่มประเทศอาเซียน หน่วยงานการวิจัยและพัฒนาจากประเทศสิงคโปร์และมาเลเซียซึ่งเคยเป็นสมาชิกของสถาบันมาตรฐานโทรคมนาคมแห่งยุโรป (ETSI) มีส่วนร่วมกับการสร้างทรัพย์สินทางปัญญาของวงการนี้ในระดับหนึ่ง ทั้งมีผลงานด้านวิชาการปรากฏจำนวนมากที่สุดในเขตเศรษฐกิจอาเซียนตามลำดับลักษณะเช่นเดียวที่ปรากฏกับวงการอื่น ๆ

ส่วนประเทศไทย ยังไม่ปรากฏข้อมูลที่มีนัยสำคัญด้านสิทธิบัตรแต่อย่างใด หากด้านองค์ความรู้เชิงวิชาการ กลับปรากฏมีจำนวนผลงานในระดับที่ไล่หลังประเทศมาเลเซียและสิงคโปร์ซึ่งแม้ยังห่างพอสมควรแต่เป็นที่น่าสนใจถึงที่มา ซึ่งเมื่อได้ศึกษาเชิงลึกในระดับตัวผลงานย่อยเหล่านั้นแล้วกอปรข้อมูลสาธารณะด้านโครงการวิจัยและพัฒนาในประเทศ สภาพความพร้อม บุคลากร ประวัติและผลงาน ฯ ปรากฏเป็นที่น่ากังวลเนื่องจากพบตัวอย่างเช่น

ก) ผลงานตีพิมพ์นำเสนอการทดลองที่ระบุว่าประดิษฐ์สร้างงานควอนตัมแสงความเร็วสูงได้ แต่การสำรวจวิธีปฏิบัติ พบเพียงอุปกรณ์ความเร็วต่ำมากไม่ครบองค์ประกอบที่สร้างขึ้นได้จริง กลับมีผลจากการจินตนาการ *(เช่น การให้โฟตอนเดี่ยวหรือคู่พัวพันสามารถหยุดและประพฤติตัวตามที่จะสมมติกำหนด)*

ข) มีงานการประยุกต์อุปกรณ์เพื่อการสร้างเครือข่ายสื่อสารปกติ "มิได้ใช้สถานะทางควอนตัมฟิสิกส์" ต่างจากที่มีในเครือข่ายควอนตัมปกติอื่น ๆ ทั่วไป (quantum network) แต่ปรากฏข่าวประชาสัมพันธ์ผลงานสู่สาธารณะกับการตีพิมพ์ผลงานปรากฏว่าเป็น *"การประยุกต์ใช้รหัสลับที่รับประกันด้วยกฎทางฟิสิกส์ ว่าด้วยทฤษฎีห้ามคัดลอกมาช่วยเพิ่มความปลอดภัยบนระบบ"*

ค) งานวิชาการเชิงจินตนาการปราศจากหลักวิศวกรรมไฟฟ้าสื่อสาร โดยสมมติขึ้นเองให้การสื่อสารไร้สายเป็นดังที่นำเสนอ เช่น ระบบโทรศัพท์เคลื่อนที่มีคุณสมบัติเชิงควอนตัมแสงไปสร้างอยู่ได้ทั้งบนตัวระบบและลูกข่าย (handset) พร้อมระบุอีกว่าทดสอบสาธิตได้ด้วยแล้ว

ซึ่งสามารถสรุปได้ว่า[65] ประเทศไทยยังไม่ประสบผลในการสร้างผลงานที่มีผลกระทบจริง แต่กลับได้สร้างดัชนีการแข่งขันเทียมขึ้นจากผลงานวิชาการอันอาจเกิดจากความผิดพลาดทั้งตั้งใจหรือไม่ก็ตามมากกว่าแล้ว จึงควรได้รับการปรับปรุงโดยเร่งด่วนและอย่างยั่งยืน

- **ข้อเสนอแนวทางหัวข้อวิจัยและการสร้างทรัพย์สินทางปัญญา**

จากเป้าหมายขั้นแรกก่อนหน้าของ "การเป็นผู้บริโภคเทคโนโลยีอย่างฉลาด" และ "แนวทางงานวิจัยและพัฒนาในประเทศ" จาก "สารสนเทศเชิงควอนตัมประเทศไทย : พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗) ISBN 9786163748300"[66] โดยที่ปรากฏว่าในประเทศมีความพร้อมเพียงส่วนน้อยกับระดับงานด้าน transportation layer 4 ของ 7 OSI layers เมื่อเทียบเคียงทั้งด้านวิชาการและโอกาสสร้างทรัพย์สินทางปัญญาที่น้อยมากของประเทศ และยังไม่มีแนวโน้มการสร้างผลงานที่ผลกระทบสูงได้

ดังนั้น จึงอาจเป็นการเหมาะสมที่เลือกสรรค์ลงทุนทรัพยากรต่าง ๆ กับจุดแข็งเดิมนั้นก่อน เพื่อความต่อเนื่องก่อนขยายสู่ระดับอื่นรอบข้างที่ยังคงขาดแคลนโดยสมบูรณ์ อีกทั้งระดับงานของ layer 4 เป็นส่วนงานด้านวิศวกรรมศาสตร์เน้นหนักกับการสื่อสารและคอมพิวเตอร์ ซึ่งมีอัตราส่วนของทั้งนักศึกษา นักวิชาการ นักวิจัยในประเทศจำนวนสูงมากกว่าสาขาฟิสิกส์ *(ที่เหมาะสมกับงานระดับล่าง (physical layer) และมีบุคลากรน้อยมากไม่มีนัยสำคัญของการเริ่มต้นได้ (พ.ศ. 2559))* จึงอาจได้เป็นแนวทางในการสร้างงานวิจัยสู่การสร้างทรัพย์สินทางปัญญาได้บ้างต่อไป

---

65 ***ข้อสังเกต:***
1) แม้งานลักษณะนี้ได้รับการตีพิมพ์แล้วในวารสารที่มีผลกระทบ (impact factor) แต่มักปรากฏอยู่นอกกลุ่ม แหล่งข้อมูลวิชาการหรือชื่อวารสารสูงสุดห้าลำดับแรก หรือกลุ่มหลักอื่น ๆ ของวงการ (บทที่ 2 – ข้อมูลงานวิจัยและพัฒนา) โดยปรากฏตีพิมพ์อยู่ในวารสารเฉพาะกิจระดับภูมิภาคหรือวารสารออนไลน์กลุ่มใหม่ ๆ ที่มิได้เกี่ยวข้องโดยตรงกับสาขา
2) ข้อสังเกตเพิ่มเติม มีนักวิชาการที่เล่นกับโอกาสควอนตัมในประเทศน้อยมาก (ลงทะเบียนหรือมีโครงการวิชาการ วิจัยและพัฒนาปรากฏสาธารณะทั่วไป) และยังมีความพร้อมน้อยกับงานด้านการทดลองหรือสร้างต้นแบบที่ต้องลงทุนอีกสูงยิ่ง โดยทุกโครงงานมีอุปสรรคสู่การผลิตผลคล้ายคลึงกัน แต่ดีไม่ดีผลงานด้านการทดลอง (experiment) ไอที่หวือหวารหัสลับควอนตัมหลายแหล่งจากเมืองไทยปรากฏในวารสารและฐานข้อมูลวิชาการโลก

66 *www.ebooks.in.th/ebook/30625/*

และจากการพัฒนางานก่อนหน้าของกลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย ที่สัมพันธ์กับปัจจัยสำคัญของการพัฒนาทั้งสี่นั้น อันได้นำเริ่มมาสร้างเป็นแผนกลยุทธ์แล้ว โดยแยกเป็น**ยุทธศาสตร์การระดมทุน การพัฒนาบุคลากร วิทยาการร่วมเรียนรู้โลก และนโยบายการเป็นผู้ซื้ออย่างฉลาด** ซึ่งจะได้ผลักดันนำสู่การปฏิบัติให้ถึงจุดมวลวิกฤติต่อไปโดยรายงานเปิดกว้าง (white paper) ฉบับนี้ จัดทำคู่ขนานเป็นส่วนหนึ่งของการสนับสนุนต่อยอดสู่ "ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม" ที่จะได้ร่วมกันผลักดันสร้างสนามระดับประเทศเพื่อการเตรียมพร้อมสู่อนาคตร่วมกันต่อไป

.....

ภาคผนวก

ภาพรวมสถิติการยื่นจดสิทธิบัตรในประเทศไทย 5 ปีหลังสุด

(พ.ศ. 2553 -2557)[67]

ปี / Year	คำขอรับสิทธิบัตรทั้งหมด (Patent Application)	การออกแบบผลิตภัณฑ์ (Design)	การประดิษฐ์ (Invention)	คำขอรับสิทธิบัตรทั้งหมด (Granted Patent)	การออกแบบผลิตภัณฑ์ (Design)	การประดิษฐ์ (Invention)
2557 (2014)	**12,007**	**4,077**	**7,930**	3,763	2,477	**1,286**
2556 (2013)	11,209	3,802	7,407	**4,007**	**2,858**	1,149
2555 (2012)	10,227	3,481	6,746	3,115	2,107	1,008
2554 (2011)	7,695	3,789	3,906	2,153	1,253	900
2553 (2010)	5,602	3,614	1,988	2,104	1,332	772

OQC.LED.TTKM
(แสง-ควอนตัม-สื่อสาร-แอลอีดี)

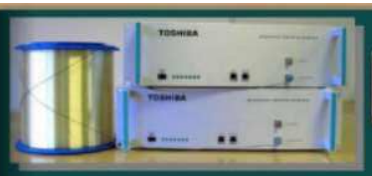
67 *ipthailand.go.th/ สำรวจ ณ เมษายน พ.ศ. 2559*

ภาคผนวก ง
บทสรุปมาตรฐานรหัสลับควอนตัมโลก พ.ศ. 2557 – 2558

เอกสารประกอบการเรียนรู้ ฝึกอบรม
วิทยาการรหัสลับเชิงควอนตัม

"ใช้เพื่อการศึกษาเท่านั้น"

ESTI GS QKD 002 v1.1.1 (2010-06)
Quantum Key Distribution; Use Cases



บทสรุป

มาตรฐานรหัสลับควอนตัมโลก

ESTI GS QKD 002 v1.1.1 (2010-06)

Quantum Key Distribution; Use Cases

บทสรุปมาตรฐานรหัสลับควอนตัมโลก
(Concept of ETSI - QKD Standard)

ปรับปรุงครั้งที่ ๓: สิงหาคม พ.ศ. 2559
(เอกสารแบบเปิดนี้อาจมีการปรับปรุงได้โดยตลอด โดยมิได้แจ้งให้ทราบล่วงหน้า)

โดย

กลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย
Thai Quantum Information Forum
(Q-Thai Forum)

สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI)
และ
ชมรมไฟฟ้าสื่อสาร (IEEE Communications Society - Thailand chapter)
สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE)

โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม:
การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร มหาวิทยาลัยนเรศวร

สนับสนุนโดย
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์
และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส – กสทช)

บทสรุปมาตรฐานรหัสลับควอนตัมโลก
(Concept of ETSI - QKD Standard)

ทีม สุวิทย์ กิระวิทยา ปรมินทร์ แสงวงษ์งาม จุฑาเพชร เวชรังษี เกียรติศักดิ์ ศรีพิมานวัฒน์

ที่ปรึกษา สุทัศน์ ยกส้าน และ Gaby Lenhart *(ETSI)*

ขอขอบคุณ สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI) และชมรมไฟฟ้าสื่อสาร สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE) กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส. - กสทช) และมหาวิทยาลัยนเรศวร

ปรับปรุงครั้งที่ ๑: สิงหาคม พ.ศ. 2559
เชิญชวนร่วมติดตามการปรับปรุง เพื่อพัฒนาเอกสารบทสรุปนี้ต่อเนื่องไป
(เอกสารแบบดิจิตอลนี้อาจมีการปรับปรุงได้โดยตลอด โดยมิได้แจ้งให้ทราบล่วงหน้า)

ข้อมูลเพิ่มเติม: *www.facebook.com/QuantumCryptoThailand และ Q-Thai.Org*

ข้อมูลประกอบ: *"พัฒนาการสารสนเทศเชิงควอนตัม" (พ.ศ.๒๕๕๕) (ISBN 978-616-12-0212-5) "สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗)" (ISBN 978-616-37-4830-0) "ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)" (ISBN 978-616-413-846-9) และ "ศูนย์ทดสอบฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม" (พ.ศ.๒๕๕๙)*

โครงการร่วมกิจกรรมปีแห่งแสงสากล (IYL2015) : *www.light2015.org*

ปกหน้า: *ผลิตภัณฑ์ด้านวิทยาการรหัสลับเชิงควอนตัม*
(บนซ้าย) – Toshiba UK (บนกลางและขวา) - IDQuontique
(กลางและขวาล่าง) – Qasky (ล่างซ้าย) - SeQureNet

คำนำ

"วิทยาการรหัสลับเชิงควอนตัม (quantum cryptography)" สาขาแขนงหนึ่งของสารสนเทศหรือไอทีควอนตัม อันมีพัฒนาการต้นแบบห้องปฏิบัติการชุดแรกตั้งแต่ปี ค.ศ. 1984 มาแล้วนั้น เวลายี่สิบห้าปีต่อมาโลกถึงได้มีมาตรฐานเชิงแนะนำโดย สถาบันมาตรฐานโทรคมนาคมแห่งยุโรป (European Telecommunications Standards Institute (ETSI)) ในปี ค.ศ. 2009 อันเป็นมาตรฐานรหัสลับเชิงควอนตัมลำดับแรกและแห่งเดียวของโลก

มาตรฐานนี้เป็นแนวทางการร่วมงานกันของทั้งภาควิชาการกับภาคอุตสาหกรรม ที่แม้ยังอยู่ในช่วงเวลาอันจัดได้ว่าเป็นระยะเริ่มหรือต้นน้ำ และยังไม่สุกงอม (mature) ทางเทคโนโลยีที่จะนำสู่การผลิตต่อไปยังระดับการบริการหรือปลายน้ำได้ แต่ได้ทำให้โลกสารสนเทศเดิมตระหนักมากขึ้นแล้วต่อการมาถึงของสาขาที่มีผลกระทบสูงนี้ และโดยเฉพาะเมื่อควอนตัมคอมพิวเตอร์ได้รับการประกาศความก้าวหน้าจากยักษ์ใหญ่ในวงการไอทีเดิมทั้ง กูเกิล (Google) และไอบีเอ็ม (IBM) เมื่อช่วงปี ค.ศ.2015-2016 ซึ่งเกรงกันว่าเครื่องคำนวณที่มีศักยภาพความเร็วสูงยิ่งนี้ จะทำให้รหัสลับที่ใช้งานอยู่ทั่วไปในโลกอินเทอร์เน็ตตกอยู่ในความเสี่ยงต่อการถูกถอดรหัสคณิตศาสตร์ได้ด้วยเวลาที่สั้นลงอย่างมาก จึงส่งผลให้วงการวิทยาการรหัสลับเชิงควอนตัมได้รับความสนใจมากขึ้น

สำหรับประเทศไทย หน่วยงานที่ควรได้เกี่ยวข้องโดยตรงและตระหนักต่อมาตรฐานด้านความปลอดภัยข้อมูลแนวนี้อาจได้แก่ กสทช. สพธอ. สรอ. กระทรวงอุตสาหกรรมและไอซีที เป็นต้น ซึ่งควรได้เร่งติดตามและพัฒนาแนวทางนโยบายรองรับให้ได้ทัน เนื่องจากเมื่อใดมาตรฐานเหล่านั้นกลายเป็นการกำหนดใช้งานภาคบังคับ เป็นข้อตกลงเพื่อการร่วมภารกิจระหว่างประเทศ หรือเป็นยุทธศาสตร์การกีดกันทางการค้าอนาคต ก็อาจทำให้เกิดข้อเสียเปรียบหากประเทศไทยยังคงขาดแคลนบุคลากรและนโยบายที่จะสามารถตอบรับต่อข้อกำหนดเหล่านั้นได้ทันเวลา โดยที่วิทยาการแห่งอนาคตนี้พึงต้องการการเตรียมพร้อมล่วงหน้าที่นานและใช้ทรัพยากรสูงมาก และถึงแม้บรรยากาศของระบบเครือข่ายการสื่อสารของประเทศจะยังอยู่ในสภาวะการตรวจสอบที่เข้มข้นจากภาครัฐ (พ.ศ.2559) อันอาจเป็นอุปสรรคต่อการพัฒนานโยบายรองรับเทคโนโลยีความปลอดภัยข้อมูลดังกล่าวนี้แบบเปิดกว้าง หากเมื่อสภาพการต่าง ๆ ของประเทศได้กลับเข้าสู่สภาวะปกติแล้วถึงจะมีการเริ่มพิจารณาโดยมิได้มีการตระเตรียมไว้พร้อมก่อน จักคาดการณ์ได้ว่าจะพึ่งพาตนเองได้น้อยในอนาคตและอาจทำให้ความปลอดภัยของระบบสื่อสารยุคใหม่กว่าตกอยู่ในความเสี่ยงสูง เกิดการเสียรู้เชิงเทคโนโลยีเช่นสาขาอื่น ๆ ก่อนหน้า และมีการใช้งบประมาณที่สูงมากเกินควรตามมาเช่นเดิมได้

กอปรประเด็นเชิงเปรียบเทียบอีกกรณีหนึ่งด้านพัฒนาการในกลุ่มเศรษฐกิจอาเซียน มีเพียงประเทศสิงคโปร์และมาเลเซียเท่านั้น ที่ได้เคยมีส่วนร่วมร่างมาตรฐานนี้แบบวงใน (Group Specification: GS) ส่งผลให้มีความก้าวหน้าทั้งวิชาการและทรัพย์สินทางปัญญาออกมามากกว่าประเทศไทยนานแล้ว จึงเป็นอีกข้อสังเกตให้กับภาคอุตสาหกรรมและนโยบายของประเทศไทย ควรได้เร่งปรับตัวลดระยะห่างของพัฒนาการทุกด้านมุมต่อวิทยาการสาขาใหม่นี้

ในอดีต สมาคมวิชาการสองแห่ง (ECTI & IEEE) จึงได้ร่วมกันจัดกิจกรรมส่งเสริมความรู้ความเข้าใจ ทั้งด้านมาตรฐานโทรคมนาคมและวิทยาการรหัสลับเชิงควอนตัมโดยตรง โดยได้เชิญผู้จัดการอาวุโสส่วนงานมาตรฐานของ ETSI (Ms.Gaby Lenhart, Senior Research Officer at the Strategy & New Initiatives department) ร่วมสัมนาเชิงปฏิบัติการ (*Telecommunications Standards: a Lesson Learn from Europe to Thailand และ Global ICT Standardization)* มาตั้งแต่ปี พ.ศ.2556 และก่อนหน้านั้นเป็นเวลาหลายปีต่อเนื่องได้ร่วมหารือแนวทางที่ประเทศไทยจะมีส่วนร่วมติดตามมาตรฐานดังกล่าว จนถึงการเชื้อเชิญเพื่อเป็นที่ปรึกษาให้กับโครงการวิจัยและพัฒนา ด้านรหัสลับเชิงควอนตัมในประเทศไทยหลายโครงการ รวมถึงการจัดทำบทสรุปมาตรฐานฉบับย่อความนี้ด้วย ทว่า โดยรวมสถานภาพการแข่งขันของประเทศด้านใหม่นี้ก็ยังคงไม่ต่างจากทศวรรษก่อนมากนัก

ทั้งนี้ บทสรุปนี้ จึงควรได้ใช้เพื่อเร่งกระตุ้นสร้างความตระหนักของภาคสาธารณะและอุตสาหกรรมไอทีในประเทศไทยร่วมกับผลผลิตอื่น ๆ ที่ได้ระดมสรรพกำลังจัดทำมาก่อนหน้าแล้วทั้ง *"พัฒนาการสารสนเทศเชิงควอนตัม" (พ.ศ.๒๕๕๕) "สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗)" "ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)"* และ *"ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม" (พ.ศ.๒๕๕๙)* ตลอดจนเพื่อการส่งต่อหน่วยงานที่เกี่ยวข้องอื่น ๆ ในการรับช่วงงานวิชาการเพื่อนำไปต่อยอดสู่การพัฒนานโยบายรองรับให้ได้ โดยหวังเป็นอย่างยิ่งว่าอุตสาหกรรมและภาคนโยบายไอทีไทย จะสามารถปรับตัวได้ทันเวลา ลดการสูญเสียทุกมิติจากเช่นที่ผ่านมาลงได้บ้างแม้ประเทศไทยจะเป็นผู้ซื้อเทคโนโลยีโดยสมบูรณ์

อนึ่ง เอกสารเชิงสาธยายมาตรฐาน ETSI แบบเปิด เพื่อประกอบการฝึกอบรมและเรียนรู้นี้ "มิใช่การแปล" หากเป็นเสมือนเอกสารผู้ตรวจสอบระบบและใช้เพื่อเริ่มการประสานงานเชิงเทคนิคกับระบบไอทีเดิมทั่วไปได้ด้วย จึงขอเชิญชวนร่วมกันติดตามการปรับปรุงต้นฉบับ (ของ ETSI) เพื่อการพัฒนาเอกสารความรู้นี้ให้ทันสมัยขึ้นตามไปด้วยโดยลำดับ

Thai Quantum Information (Q-Thai) Forum

บทสรุปมาตรฐานรหัสลับควอนตัมโลก

จาก

ESTI GS QKD 002 v1.1.1 (2010-06)

Quantum Key Distribution; Use Cases (32 หน้า)

ต้นฉบับเผยแพร่โดย

The European Telecommunications Standards Institute (ETSI)

(www.etsi.org)

ข้อบ่งใช้ (Disclaimer):

ข้อมูลและภาพต้นฉบับเป็นลิขสิทธิ์ของ ETSI โดยบทสรุปมาตรฐานแบบเปิดกว้างที่ร่วมกันพัฒนาต่อเนื่องได้นี้ จัดทำเพื่อช่วยอธิบายข้อมูลและภาพเหล่านั้น ประสงค์จะได้ช่วยวางแนวทางให้ผู้ศึกษาที่อาจมีพื้นฐานแตกต่างกันมาก สามารถทำความเข้าใจพัฒนาการของตัวมาตรฐานผสานกับความรู้พื้นฐานเทคนิคงานชิ้นอื่น ๆ ก่อนหน้า ควบคู่ไปกับการศึกษาจากฉบับจริงในภาษาอังกฤษได้สะดวก จากเดิมที่อยู่ในแนวเทคนิคเฉพาะทางและมีลักษณะภาษาเชิงข้อกำหนด เอกสารนี้ ***มิใช่การแปลและไม่สามารถนำไปใช้งานทดแทนต้นฉบับมาตรฐาน ESTI GS QKD 002 v1.1.1 (2010-06) ได้แต่อย่างใด***

การกระจายกุญแจรหัสลับเชิงควอนตัม : กรณีการนำไปใช้งาน

(Quantum Key Distribution; Use Cases)

(ETSI GS QKD 002 v1.1.1 (2010-06)

เนื้อหา **หน้า**

1. ขอบเขต

เอกสารนี้นำเสนอภาพรวมที่ครอบคลุมสภาพการณ์ต่าง ๆ ที่จะสามารถนำระบบการกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution หรือคำย่อ QKD) [i.1] ไปใช้เป็นส่วนหนึ่งของระบบการสื่อสารข้อมูลที่มีความปลอดภัยสูง ซึ่งเป็นแขนงของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology, ICT)

ระบบ QKD สามารถจัดซื้อเพื่อใช้งานได้โดยมีหลายบริษัทขนาดเล็กที่ทำการผลิตและจำหน่าย นอกจากนี้ระบบ QKD กำลังถูกพัฒนาขึ้นในห้องปฏิบัติการต่าง ๆ ของบริษัทขนาดใหญ่ สถาบันวิจัย และมหาวิทยาลัยอื่นอีกมาก โดยทั่วไป ระบบนี้จะประกอบด้วยสองหน่วยหลัก ซึ่งเชื่อมต่อกันด้วยช่องทางสื่อสารเชิงควอนตัมที่มีระยะทางสูงสุดในระดับ 100 กิโลเมตร โดยการเชื่อมต่อนั้นอาจทำโดยการใช้เส้นใยนำแสงหรือการส่งผ่านอากาศด้วยกล้องโทรทรรศน์ การส่งข้อมูลส่วนนี้จะใช้คุณสมบัติทางกายภาพเชิงควอนตัมของแสง

ผลลัพธ์ที่ได้จากระบบ QKD คือ การส่งข้อมูลลับในระบบเครือข่ายคอมพิวเตอร์ที่จะมีความปลอดภัยสูง โดยกฎทางควอนตัมฟิสิกส์ทำให้ผู้ใช้งานมั่นใจได้ว่า ผู้ดักจับข้อมูลจะไม่สามารถได้ข้อมูลกุญแจที่ส่งในระบบ QKD นี้ โดยทั้งผู้รับและผู้ส่งจะทราบการมีอยู่ของผู้ดักจับข้อมูลในระบบได้อีกด้วย ([i.3] และ [i.4]) ดังนั้น จึงกล่าวได้ว่า ระบบ QKD จะไม่ส่งข้อมูลที่ไม่ปลอดภัย เนื่องจากผลของการมีผู้ดักจับข้อมูลจะทำให้เกิดการลดลงของอัตราการส่งกุญแจ จนอาจทำให้ถึงกับหยุดการส่งเพื่อรักษาสถานะความปลอดภัยนั่นเอง โดยระดับความปลอดภัยของข้อมูลนี้เป็นความปลอดภัยเชิงทฤษฎีข่าวสาร หากกุญแจที่ใช้เป็นแบบสุ่มที่เกือบสมบูรณ์แล้ว ผู้ที่มาดักจับข้อมูลจะมีข้อมูลเกี่ยวกับกุญแจนั้นได้เกือบจะเป็นศูนย์หรือไม่มีเลย ซึ่งระบบ QKD จะสามารถวัดค่าลักษณะภายในที่ต่างออกไปอันเกิดจากการดักจับนั้นได้นั่นเอง

การสร้างอุปกรณ์สำหรับระบบ QKD ทำได้หลายวิธีแบ่งตามการใช้เทคโนโลยีที่ที่นำสร้าง โดยสังเขปคือ การสร้างโดยใช้ตัวแปรไม่ต่อเนื่อง การสร้างโดยใช้ตัวแปรต่อเนื่อง และการสร้างโดยการอ้างอิงเฟสแบบกระจาย ([i.2], [i.12] และเอกสารอ้างอิงด้านใน) อย่างไรก็ดี ระบบ QKD เหล่านี้จะมีลักษณะเหมือนกัน คือ มีระบบย่อยทางแสงที่นำมาใช้เตรียมสถานะของโฟตอนนำมาใช้ต่อเพื่อการส่งข้อมูลกุญแจรหัส ในลักษณะเดียวกันกับระบบคอมพิวเตอร์ที่มีการเตรียมรับข้อมูลเพื่อเริ่มทำงาน ซึ่งระบบนี้จึงเหมือนระบบความปลอดภัยอื่น ๆ ที่อาจมีการหลุดรอดของข้อมูลออกจากขอบเขตที่ปลอดภัยได้ โดยในเอกสารมาตรฐานต้นฉบับนั้น ได้แสดงถึงข้อมูลจำเพาะ และวิธีการที่จะพัฒนาเพื่อให้ระบบ QKD นี้ให้ผ่านการยอมรับด้านความปลอดภัยร่วมกันได้

2. เอกสารอ้างอิง

รายการเอกสารอ้างอิงเหล่านี้ แม้ไม่จำเป็นเพื่อการประยุกต์ใช้งานแต่จะช่วยผู้ใช้ได้ทราบในเรื่องเฉพาะเจาะจงต่าง ๆ เพื่อประกอบการศึกษามาตรฐานต้นฉบับได้สะดวก และเป็นเอกสารเฉพาะส่วนที่สำคัญเพื่อการทำความเข้าใจวิทยาการรหัสลับเชิงควอนตัมแขนงนี้ได้

[i.1] "Quantum Cryptography: Public Key Distribution and Coin Tossing, Proceedings of IEEE International Conference on Computers Systems and Signal Processing", Bangalore India, C.H. Bennett and G. Brassard, December 1984, pp 175-179. NOTE: Online at www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf. (**หมายเหตุ :** *เอกสารนี้เป็นงานตีพิมพ์ชิ้นเป็นต้นกำเนิดการสร้างต้นแบบแรกของโลก*)

[i.2] "Quantum cryptography, Reviews of Modern Physics", Nicolas Gisin, Grègoire Ribordy, Wolfgang Tittel and Hugo Zbinden, Vol. 74, 145-195 (2002). NOTE: Online at http://www.gap-optique.unige.ch/Publications/PDF/QC.pdf.

[i.3] "The security of practical quantum key distribution", Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, Vol. 81, 1301-1351 (2009). NOTE: Online at http://arxiv.org/abs/0802.4155.

[i.4] "Security of quantum key distribution with imperfect devices", D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill,Vol. 5, 325-360) (2004). NOTE: Available at http://arxiv.org/abs/quant-ph/0212066.

[i.5] "White Paper on Quantum Key Distribution and Cryptography", Preprint arXiv:quant-ph/0701168, Alléaume R, Bouda J, Branciard C, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier Ph, Länger T, Leverrier A, Lütkenhaus N, Painchault P, Peev M, Poppe A, Pomin Th, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H, Zeilinger A, 2006 SECOQC. (**หมายเหตุ :** *เอกสารนี้เป็นงานตีพิมพ์อันเนื่องจากการโครงข่ายวิทยาการรหัสลับของกลุ่มวิจัยในสหภาพยุโรป ซึ่งต่อมาสำเร็จผลสาธิตโครงข่าย ณ กรุงเวียนนา ประเทศออสเตรีย เมื่อปี ค.ศ. 2008*)

[i.6] UQC Report: "Updating Quantum Cryptography", Quantum Physics (quant-ph); Cyptography and Security. Donna Dodson, Mikio Fujiwara, Philippe Grangier, Masahito Hayashi, Kentaro Imafuku, Ken-ichi Kitayama, Prem Kumar, Christian Kurtsiefer, Gaby Lenhart, Norbert Luetkenhaus, Tsutomu Matsumoto, William J. Munro, Tsuyoshi Nishioka,

Momtchil Peev, Masahide Sasaki, Yutaka Sata, Atsushi Takada, Masahiro Takeoka, Kiyoshi Tamaki, Hidema Tanaka, Yasuhiro Tokura, Akihisa Tomita, Morio Toyoshima, Rodney van Meter, Atsuhiro Yamagishi, Yoshihisa Yamamoto, and Akihiro Yamamura, 2009. NOTE: Available at http://arxiv.org/abs/0905.4325. (**หมายเหตุ :** *งานตีพิมพ์อันเนื่องมาจากการสาธิตโครงข่ายรหัสลับควอนตัม ณ กรุงโตเกียวประเทศญี่ปุ่น ซึ่งต่อมาเปิดเป็นโครงข่ายให้สังเกตการทำงานได้ตลอดเวลาแบบออนไลน์ ณ tokyoqkd.jp*)

[i.7] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[i.8] IETF RFC 1968: "The PPP Encryption Control Protocol (ECP)".

[i.9] IEEE 802.3u.

[i.10] "Handbook of Applied Cryptography", (Boca Raton: CRC Press) Menezes A J, van Oorschot P C and Vanstone S A 1997.

[i.11] "Applied Cryptography", Schneier B 1996, (New York: John Wiley).

[i.12] "Quantum Cryptography Progress in Optics 49", Dusek, M, Lütkenhaus N and Hendrych M 2006, Edt. E. Wolf , Elsevier 381-454.

[i.13] "Principled Assuredly Trustworthy Composable Architectures Computer Science Laboratory", Neumann P G 2003, SRI International, Menlo Park.

[i.14] "The Case for Quantum Key Distribution Preprint arXiv:0902.2839v1 [quant-ph]", Stebila D, Mosca M and Lütkenhaus N 2009.

[i.15] "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications of the ACM 21,2 120-6", Rivest R L, Shamir A and Adleman L M 1978.

[i.16] "Communication theory of secrecy systems Bell Systems technical Journal", 28 656-715 Shannon C E 1949.

[i.17] "New directions in cryptography IEEE Transactions on Information Theory", 22 644-54, Diffie W and Hellman M E, 1976.

[i.18] "How to Break MD5 and Other Hash Functions Proc. EUROCRYPT 2005, Lecture Notes in Computer Science" 3494 19-35, Wang X, Yu H, 2005.

[i.19] "Finding Collisions in the Full SHA-1 Lecture Notes in Computer Sciences", 3621 17-36, Wang X, Yin Y L and Yu H, 2005.

[i.20] "New Hash Functions and Their Use in Authentication and Set Equality Journal of Computer and System Sciences", 22 265-79, Wegman M N and Carter J L, 1981.

[i.21] "Why Quantum Cryptography?", Preprint arXiv:quant-ph/0406147, Paterson K G, Piper F, Schack R, 2005.

[i.22] "On fast and provably secure message authentication based on universal hashing Proc. Crypto '96, Lecture Notes in Computer Science", 1109 313-28, Shoup V, 1996.

[i.23] ETSI GS QKD 001: "Quantum Key Distribution (QKD); Development and Production of QKD systems; Security Assurance Requirements".".
NOTE: This reference is cited as WI 1 in the present document.

[i.24] ETSI GS QKD 003: "Quantum Key Distribution (QKD); Requirements for QKD systems; Components and Interfaces Requirements".".
NOTE: This reference is cited as WI 3 in the present document.

[i.25] ETSI GS QKD 004: "Quantum Key Distribution (QKD); Requirements for QKD systems; Application Interfaces Requirements Study".".
NOTE: This reference is cited as WI 4 in the present document.

[i.26] ETSI GS QKD 005: "Quantum Key Distribution (QKD); Security evaluation of QKD Systems; Generic Framework for Security Proofs".".
NOTE: This reference is cited as WI 5 in the present document.

[i.27] ETSI GS QKD 007.
NOTE: This reference is cited as WI 7 in the present document.

[i.28] ETSI GS QKD 008.
NOTE: This reference is cited as WI 8 in the present document.

[i.29] ETSI GS QKD 009. NOTE: This reference is cited as WI 9 in the present document.

3. คำจำกัดความและคำย่อ

(หัวข้อนี้ยกเลิกแล้วจากต้นฉบับมาตรฐาน *(เพิ่มเติม) แนวโน้มเกิดคำจำกัดความใหม่มากขึ้นและการนำไปใช้ยังคงมีความแตกต่าง เนื่องจากยังเป็นสาขาขั้นพื้นฐาน)*

4. QKD : นวัตกรรมทางเทคโนโลยีด้านความปลอดภัย

4.1 การจำแนก QKD โดยใช้หลักเกณฑ์ของวิทยาการรหัสลับ

จากการพิจารณาระบบ QKD เป็นหน่วยหนึ่งในระบบการส่งข้อมูลด้วยวิทยาการรหัสลับ ([i.10 และ i.11]) ซึ่งโดยแท้จริงแล้ว *คำว่า "วิทยาการรหัสลับควอนตัม (Quantum Cryptography)" พิจารณาสำหรับระบบการกระจายกุญแจรหัสลับนี้อาจทำให้เข้าใจผิดได้ เนื่องจาก QKD ไม่สามารถแทนที่วิทยาการรหัสลับแบบดั้งเดิม เพียงแต่เสริมให้วิทยาการนี้นั้นมีประสิทธิภาพมากยิ่งขึ้น*

โดยหัวข้อย่อยต่อไปนี้ คือสิ่งที่ต้องพิจารณาในการประเมินระดับความปลอดภัยของระบบ เพื่อที่จะทำให้เกิดการบูรณภาพ (ไม่ถูกเปลี่ยนแปลงในระหว่างที่ส่ง) และการรักษาความลับของข้อมูลโดยยังคงมีการพิสูจน์ตัวตนหรือพิสูจน์ทราบว่า คือต้นฉบับจริงของข้อมูลอยู่ ([i.5], [i.13] และ [i.14])

4.1.1 หลักเกณฑ์การเข้ารหัส

การเข้ารหัสเป็นการทำให้ข้อมูลถูกปิดบัง โดยการเข้ารหัสนี้มีหลายวิธีซึ่งแบ่งเป็นแบบกุญแจสมมาตรและแบบกุญแจอสมมาตร ตัวอย่างการเข้ารหัสแบบกุญแจสมมาตรได้แก่อัลกอ

ริธึม DES (Data Encryption Standard) และอัลกอริธึมอื่น ๆ ที่พัฒนาต่อมาบนพื้นฐานของอัลกอริธึมนี้ คือ Triple DES และ AES และตัวอย่างของการเข้ารหัสแบบกุญแจอสมมาตร คือ อัลกอริธึม RSA [i.15] และอัลกอริธึมจำพวกเส้นโค้งวงรีหรืออิลิปติก[1]

การเข้ารหัสทั้งแบบกุญแจสมมาตรและกุญแจอสมมาตร ที่มีใช้กันอยู่ทั่วไปในการรักษาความลับของข้อมูลนั้นอาศัยความยากหรือซับซ้อน และใช้เวลานานในการถอดรหัสหากผู้ที่ต้องการถอดรหัสไม่ทราบกุญแจต้นทาง ซึ่งวิทยาการกุญแจลับอสมมาตรจะใช้สมมติฐานที่ว่าไม่มีกระบวนการเชิงคณิตศาสตร์ใดสามารถหาอินเวอร์สหรือฟังก์ชันย้อนกลับ ที่จะนำมาใช้ในการเข้ารหัสอย่างรวดเร็วได้

อย่างไรก็ดี ยังมีอัลกอริธึมหนึ่งที่แตกต่างนั่นคือ รหัสผ่านใช้ครั้งเดียว (one time pad)[2] ซึ่งหากใช้อย่างถูกต้องแล้ว วิธีการเข้ารหัสนี้จะปลอดภัยอย่างแน่นอน โดยวิธีการนี้คิดค้นโดย กิลเบิร์ต เวอร์นัม และ โจเซฟ มัลบอร์น (Gilbert Vernam และ Joseph O. Mauborgne) และถูกพิสูจน์ว่าปลอดภัยสูงสุดโดย โคลด แชนนอน (Claude Shanon) ในปี ค.ศ. 1949 [i.16] โดยต่อมา ยังคงมีการใช้วิธีการเข้ารหัสชนิดนี้ในการส่งข้อมูลอันต้องการความปลอดภัยสื่อสารในระดับสูงสุด แม้ว่าวิธีนี้ จะมีรายละเอียดที่ทำให้การเข้ารหัสนำมาใช้งานได้ยากหรือไม่สะดวก (กุญแจรหัสลับที่ใช้จะต้องมีความยาวเท่ากันกับข้อความที่ต้องการเข้ารหัส)[3]

1 **หมายเหตุ :** *วิธีการนี้ภายหลังถูกเปิดเผยโดย เอ็ดเวิร์ด สโนว์เดน (Edward Snowden) ว่าเป็นช่องทางการแอบลอดผ่านเข้าล้วงความลับของหน่วยงานด้านความมั่นคงของสหรัฐอเมริกา ไม่ปลอดภัยอย่างแท้จริง*

2 *รหัสผ่านใช้ครั้งเดียวในโลกสื่อสารที่อาจคุ้นเคย เช่น รหัสผ่านที่ได้รับมาทางข้อความสั้น (SMS) เพื่อใช้เข้าระบบสื่อสารบนิโล ๆ โดยไม่ใช้ซ้ำ จะเปลี่ยนค่าทุกครั้งเมื่อมีการเริ่มระบบใหม่ และแต่ละครั้ง รหัสจะมีอายุสิ้นอายุ 30 วินาที เป็นต้น*

3 *วิธีการนี้จึงไม่เหมาะสมกับการสื่อสารข้อมูลที่มีปริมาณเพิ่มมากขึ้นมาโดยลำดับ เนื่องจากขนาดข้อมูลจะใหญ่ขึ้นเป็นสองเท่า ประสิทธิภาพการสื่อสาร (efficiency) จึงลดลงเหลือเพียงครึ่ง*

4.1.2 หลักเกณฑ์การกระจายกุญแจรหัสลับ

"การส่งข้อมูลบิตแบบสุ่มสองชุดที่เหมือนกันทุกประการไปที่สองแห่งที่เชื่อมต่อกันด้วยช่องทางการสื่อสารแบบควอนตัม"

โดยระบบ QKD ที่จัดเตรียมตามหลักเกณฑ์พื้นฐานนี้ จึงจะกลายเป็นระบบที่มีการรับประกันความปลอดภัยได้สูงสุด

ทั้งนี้ แม้การส่งกุญแจรหัสลับด้วยหลักการอื่น (ที่มิใช่ช่องสัญญาณควอนตัมตามหลักข้างต้น) เช่น การส่งโดยตรงแบบพบเจอกัน หรือโดยใช้วิทยาการรหัสลับกุญแจสาธารณะอื่นนั้นก็สามารถทำได้ แต่ระดับความปลอดภัยของการส่งกุญแจรูปแบบหลังดังกล่าวจะลดลงตามลักษณะการกระจายหรือส่งกุญแจที่ใช้ด้วย ตัวอย่างการส่งกุญแจทั่วไปที่มิต้องมีช่องสัญญาณพิเศษ คือ การใช้ข้อตกลง Diffie-Hellmann ([i.17]) โดยใช้โพรโทคอล Secure Sockets Layer (SSL/https) หรือ การใช้โพรโทคอล Internet Key Exchange (IKE) สำหรับการกำหนดความปลอดภัยในโพรโทคอล IPSec (*ของระบบอินเทอร์เน็ตปกติ*) ส่วนการกระจายกุญแจในระบบ QKD นั้นจะแตกต่าง โดยต้องอาศัยข้อตกลงเพื่อหลีกเลี่ยงการโจมตีแบบ man-in-the-middle ด้วย (ป้องกันจากการมีผู้รับความลับช่วงกลาง ระหว่างการส่งรับปกติ) ซึ่งจะต้องอาศัยการพิสูจน์ตัวตนที่แท้จริงโดยอาจทำผ่านระบบที่น่าเชื่อถือเพิ่มมาอีกระบบหนึ่ง

4.1.3 หลักเกณฑ์การพิสูจน์ตัวตนจริงของข้อความ

สำหรับการส่งข้อมูลลับ การพิสูจน์ตัวตนจริงของข้อความ เป็นการยืนยันว่าข้อความนั้นมีบูรณภาพ (ไม่ถูกเปลี่ยนแปลงในระหว่างที่ส่ง) และมีการยืนยันตัวตนได้ว่า ผู้ส่งคือใคร หลักเกณฑ์การพิสูจน์ตัวตนจริงของข้อความของระบบ Q K D นั้นก็จะมีกระบวนการนี้ร่วมอยู่ด้วยในโพรโทคอลที่ใช้กลั่นกุญแจ (key distillation protocol)

ในระบบ QKD สามารถที่จะใช้กุญแจชุดแรก ๆ ที่สร้างขึ้นในการพิสูจน์ตัวตนจริงของข้อความ โดยไม่จำเป็นต้องอาศัยวิธีการอื่น ๆ (เช่น ทั้งลายเซ็นดิจิทัล หรืออัลกอริธึม MAC [i.21])

4.1.4 สรุปสาระสำคัญ

ตารางที่ 1 แสดงหลักเกณฑ์ของวิธีการเข้ารหัส การกระจายกุญแจ และการพิสูจน์ตัวตนที่แท้จริงที่ได้กล่าวมา โดยแสดงหลักการด้านความปลอดภัยที่ใช้ในวิธีดังกล่าวไว้ด้วย

การเข้ารหัส	**หลักการด้านความปลอดภัยที่ใช้**
การเข้ารหัสแบบสมมาตร *(กุญแจสั้นกว่าข้อความที่ส่ง)*	สมมติฐาน
วิทยารหัสลับกุญแจสาธารณะ	สมมติฐาน
รหัสใช้ครั้งเดียว	ทฤษฎีข่าวสาร
การกระจาย	**หลักการด้านความปลอดภัยที่ใช้**
การใช้ช่องทางการสื่อสารปลอดภัย	สมมติฐาน
วิทยารหัสลับกุญแจสาธารณะ	สมมติฐาน
การกระจายกุญแจเชิงควอนตัม	ทฤษฎีข่าวสาร *(เชิงควอนตัม)*
การพิสูจน์ตัวจริงของข้อความ	**หลักการด้านความปลอดภัยที่ใช้**
วิทยารหัสลับกุญแจสาธารณะ	สมมติฐาน
MAC	สมมติฐาน
ฟังก์ชันแฮช	ทฤษฎีข่าวสาร

5. แผนงานของ ISG-QKD

เอกสารนี้เป็นส่วนหนึ่งของคณะทำงานร่างมาตรฐาน (Group Specification: GS) ซึ่งก่อตั้งเพื่อดำเนินการตามแผนการทำงานของ ETSI ISG-QKD

5.1 การออกใบรับรองด้านความปลอดภัยของระบบ QKD

เพื่อเป็นการทำให้ระบบ QKD มีคุณภาพ น่าเชื่อถือ จึงจำเป็นต้องมีการตรวจสอบคุณภาพในหลายขั้นตอน รวมถึงการกำหนดข้อกำหนดด้านความปลอดภัย การประเมิน และการให้ใบรับรองตามระเบียบวิธีการการทำให้เป็นมาตรฐาน

การให้ใบรับรองด้านความปลอดภัยของระบบ QKD จำเป็นต้องมีเงื่อนไขทั้งในส่วนของฮาร์ดแวร์และซอฟต์แวร์ เช่นเดียวกันกับโมดูลด้านวิทยาการรหัสลับต่าง ๆ นอกจากนี้ระบบยังมีระบบย่อยทางแสงที่อาจถูกโจมตีได้ รูปที่ 1 แสดงรูปแบบการประเมินระบบ QKD

5.1.1 QKD; **คำศัพท์ที่เกี่ยวข้อง** ([i.27])

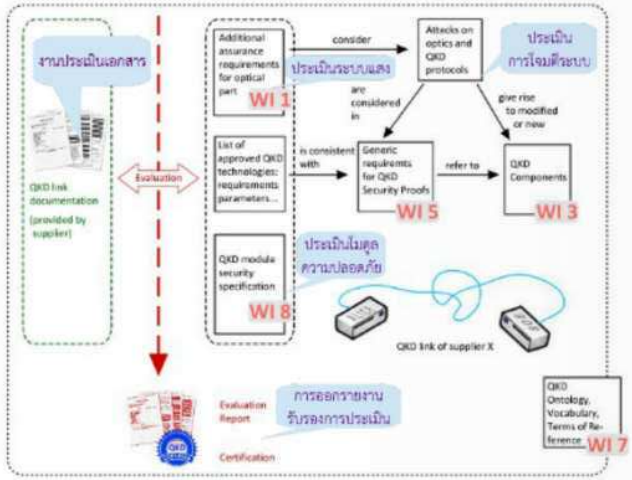
เอกสารเกี่ยวกับคำศัพท์ที่เกี่ยวข้อง จะบรรยายแนวคิด การวัด และ สิ่งต่าง ๆ ที่นักวิทยาศาสตร์ ผู้ผลิต และผู้ใช้ ในระบบ QKD กล่าวถึง โดยจะบรรยาย/อธิบาย นิยามหรือแนวคิดบางอย่างที่ใช้งานด้วย

5.1.2 QKD; **ความต้องการการรับประกัน** ([i.23])

เอกสารเกี่ยวกับความต้องการการรับประกันในด้านต่าง ๆ สำหรับระบบย่อยทางแสงที่ใช้ โดยควรแบ่งเป็นหมวดหมู่พิจารณาตามวิธีการของผู้พัฒนาระบบ QKD วิธีการประเมินด้านความปลอดภัย และการบริการหรือแก้ไขปัญหาในกระบวนการในการนำไปใช้งานจริง

5.1.3 QKD; **ข้อมูลจำเพาะด้านความปลอดภัยของโมดูล** ([i.28])

เอกสารที่แสดงข้อกำหนดด้านข้อมูลจำเพาะด้านความปลอดภัยของระบบ QKD ที่ใช้เพื่อใช้ในการปกป้องข้อมูลที่สื่อสารกัน โดยวิธีการที่ใช้จะเหมือนกันกับโมดูลวิทยาการรหัสลับแบบดั้งเดิม โดยความปลอดภัยใน 11 ด้านจะต้องถูกกำหนด ซึ่งเอกสารนี้จะต้องกำหนดความต้องการต่ำที่สุดของระบบ QKD ที่ต้องมีเพื่อให้ทำงานได้ โดยจะต้องไม่กล่าวถึงความต้องการเกี่ยวกับระบบย่อยทางแสง



รูปที่ 1 รูปแบบในการประเมินระบบ QKD

5.1.4 รายการแสดงเทคโนโลยี QKD ที่ผ่านการตรวจสอบแล้ว

รายการแสดงเทคโนโลยี QKD ที่ผ่านการตรวจสอบแล้ว ควรแสดงอยู่ที่ท้ายเอกสาร "QKD; ข้อมูลจำเพาะด้านความปลอดภัยของโมดูล" [i.28] โดยจะต้องมีการแสดงข้อมูลจำเพาะเกี่ยวกับความต้องการด้านความปลอดภัยที่ใช้ในการสร้างระบบย่อยทางแสง และโพรโทคอลที่ใช้ในการกลั่นกุญแจ QKD รวมถึงตัวแปรพารามิเตอร์ต่าง ๆ ขององค์ประกอบภายใน

5.1.5 QKD; การคุกคามและการโจมตี

เอกสารนี้ควรรวบรวมการโจมตีระบบ QKD ที่มีการศึกษาจากการวิจัยจำนวนมาก โดยควรมีการกล่าวถึงการวัดและแนวทางการแก้ไขปัญหา เพื่อใช้เป็นหลักประกันความสามารถในการทำงานของระบบ QKD โดยเอกสารนี้ควรมีการปรับปรุงและตีพิมพ์ใหม่อยู่อย่างสม่ำเสมอ

5.1.6 QKD; การพิสูจน์ด้านความปลอดภัย [i.26]

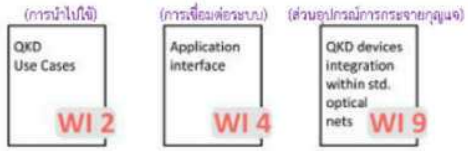
เอกสารนี้ควรแสดงข้อมูลเกี่ยวกับการพิสูจน์ด้านความปลอดภัย โดยใช้ทฤษฎีสารสนเทศเชิงควอนตัมสำหรับระบบย่อยทางแสงที่ใช้เทคโนโลยี QKD แบบต่าง ๆ

5.1.7 QKD; องค์ประกอบและการเชื่อมต่อภายใน [i.24]

เอกสารนี้จะกล่าวถึงระบบภายใน QKD ที่ประกอบด้วยองค์ประกอบทางแสงที่ใช้ทั้งอุปกรณ์แบบดั้งเดิมและอุปกรณ์เชิงควอนตัม โดยการเชื่อมต่อแบบลูกผสมไฮบริดจ์จะต้องถูกรวบเข้ากันและคุณสมบัติที่สำคัญต่าง ๆ ต้องถูกกำหนดเพื่อที่จะทำให้สามารถพิสูจน์ด้านความปลอดภัยได้

5.2 การรวบ QKD เข้าในระบบพื้นฐานที่มีอยู่เดิม

เอกสารเหล่านี้ (รูปที่ 2) ควรรวบรวมข้อมูลจำเพาะสำหรับการเชื่อมต่อ QKD เข้ากับการใช้งานในระบบพื้นฐานด้านการสื่อสารด้วยเส้นใยนำแสง โดยเอกสารนี้ ได้แก่



รูปที่ 2 เอกสารที่เกี่ยวข้องกับการรวบ QKD เข้าในระบบพื้นฐานที่มีอยู่เดิม

5.2.1 QKD; กรณีการนำไปใช้

คือเอกสารมาตรฐาน (Quantum Key Distribution; Use Cases) ฉบับนี้

5.2.2 QKD; การเชื่อมต่อ [i.25]

เอกสารที่แสดงถึงการเชื่อมต่อระบบ QKD เข้ากับระบบสารสนเทศ (ICT) โดยมีการกำหนดวิธีการ การส่งและการจัดการกุญแจรหัส รวมถึงการจัดการระบบ QKD บนระบบ ICT

5.2.3 การรวมอุปกรณ์ QKD เข้าสู่เครือข่ายทางแสงมาตรฐาน [i.29]

เอกสารนี้ควรกำหนดข้อกำหนดเบื้องต้นและความต้องการ สำหรับการรวมเอาอุปกรณ์ QKD เข้าไปในระบบพื้นฐานทางแสงที่มีการใช้ร่วมกัน โดยต้องมีการกำหนดหน้าที่การทำงานและข้อจำกัดของจำนวนฮาร์ดแวร์/ซอฟต์แวร์ที่ใช้ โดยเฉพาะด้านการจัดการระบบและขีดจำกัดด้านกำลังทางแสง

5.3 การวิจัยเสริม

เป็นเอกสารที่ให้ข้อมูลเสริมเกี่ยวกับข้อมูลจำเพาะที่กล่าวถึงก่อนหน้านี้ (รูปที่ 3)

รูปที่ 3 เอกสารเกี่ยวกับการวิจัยเสริม

5.3.1 ผู้สนับสนุนและผู้ขัดขวาง (กีดกัน) การใช้ QKD

เอกสารนี้จะให้ภาพรวมเกี่ยวกับผู้ที่สนับสนุนและผู้ที่ขัดขวางการใช้ระบบ QKD ซึ่งเป็นข้อมูลที่ได้จากการศึกษาและผู้เชี่ยวชาญในเรื่องนี้ โดยเอกสารนี้จะต้องถูกนำเสนอแก่ ISG-QKD สำหรับการอภิปราย โดยจะถูกใช้เป็นข้อมูลให้แก่ผู้เข้าร่วมการประชุมเชิงปฏิบัติการ QKD

5.3.2 ความมุ่งหวังเกี่ยวกับ QKD ในยุโรป

เอกสารนี้ควรประเมินเกี่ยวกับการประยุกต์ใช้ ความต้องการของผู้ใช้ และความคาดหวัง รวมถึงความเสี่ยงที่มีต่อระบบ QKD เมื่อถูกนำไปใช้งานจริงแล้ว โดยจะรวมถึงการเจาะจงผู้สนับสนุนและผู้ขัดขวางการใช้ QKD ในปัจจุบันและอนาคตไว้ด้วย

6. รูปแบบการใช้งาน QKD

การกระจายกุญแจแบบควอนตัม (Quantum Key Distribution) เป็นความมุ่งหวังทางด้านความปลอดภัยอันเป็นที่ต้องการ เพื่อนำไปใช้ในการสร้างระบบการส่งข้อมูลที่มีความปลอดภัยสูง โดยฟังก์ชันการทำงานของวิทยาการรหัสลับอื่น ๆ อาจอาศัยกุญแจรหัสลับควอนตัมนี้ด้วย

ในระบบ ICT ทั่วไปนั้น ยังไม่มีการกำหนดจุดที่ต้องการให้ระบบ QKD เข้าไปเชื่อมต่ออย่างชัดเจน ดังนั้น ในแง่มุมนี้ QKD ก็จะยังไม่มีความแตกต่างไปจากระบบกระจายกุญแจแบบอื่น ๆ ที่มีการติดตั้งและใช้งานกันในระดับชั้นต่าง ๆ โดยในที่นี้ จะนำเสนอความเป็นไปได้แบบต่าง ๆ ของการรวมเอา QKD เข้ากับระบบ ICT เดิม ซึ่งจะกล่าวถึงโดยอ้างอิงถึงรูปแบบโมเดลการเชื่อมต่อ OSI 7 ระดับชั้น [i.6]

6.1 ชั้นการเชื่อมโยงข้อมูล (Data Link Layer)

QKD สามารถถูกนำไปใช้ในโพรโทคอลแบบจุดต่อจุด (Point to Point Protocol (PPP)) โดย PPP (RFC 1661 [i.7]) เป็นโพรโทคอลหนึ่งที่มีใช้ในการเชื่อมต่อ 2 โหนดในเครือข่ายเข้าด้วยกัน กระบวนการเข้ารหัสใน PPP คือ โพรโทคอลการควบคุมการเข้ารหัส (Encryption Control Protocol ECP – RFC [i.8]) ที่จะทำให้มีการเข้ารหัสในเฟรม PPP โดย QKD สามารถนำเข้าไปใช้ในส่วนการแลกเปลี่ยนกุญแจนั้น

QKD สามารถนำมาใช้ในการจัดหากุญแจสำหรับ IEEE 802.1 MACsec โดย MACsec จะเป็นการให้บริการแบบไม่มีการเชื่อมต่อในการบูรณภาพของข้อมูล และการพิสูจน์ตัวจริงสำหรับระบบที่มีการพิสูจน์ตัวตนในเครือข่ายการสื่อสารแบบท้องถิ่นหรือ LAN

QKD ที่มีการสร้างขึ้นและใช้งานมากในลักษณะการเชื่อมต่อจุดต่อจุดผ่านช่องทางสื่อสารแบบควอนตัม ดังนั้น จึงได้มีการรวมโยงเอา QKD กับตัวเข้ารหัสโยง และเรียกว่า ตัวเข้ารหัสโยง QKD (QKD Link Encryptor) ซึ่งอุปกรณ์นี้จะทำให้การเชื่อมต่อนี้ใช้งานได้ง่าย โดยระบบนี้อาจเรียกว่า VPN tunnel โดยที่ตัวเข้ารหัสนี้จะทำให้การส่งกุญแจทำได้ง่ายทั้งสำหรับกระบวนการเข้ารหัสแบบบล็อกและการใช้รหัสแบบใช้ครั้งเดียวทิ้ง อุปกรณ์นี้อาจใช้ในการเชื่อมต่อระหว่างโหนดสองโหนดที่อยู่ติดกันในเครือข่าย ([i.9])

6.2 ชั้นเครือข่าย (Network Layer)

ความปลอดภัยของโพรโทคอลอินเทอร์เน็ต (Internet Protocol Security (IPsec)) เป็นโพรโทคอลในชั้นที่ 3 สำหรับการสื่อสารผ่านระบบที่ต้องการความปลอดภัยในการส่งข้อมูล

การแลกเปลี่ยนกุญแจอินเทอร์เน็ต (Internet Key Exchange (IKE หรือ IKE v2)) เป็นโพรโทคอลที่ใช้ในการติดตั้งระบบความปลอดภัยในโพรโทคอล IPsec โดย IKE ใช้การแลกเปลี่ยนกุญแจแบบ Diffie-Hellman ซึ่งจะมีการกำหนดความลับของส่วนหรือเซชชั่นที่แบ่งปันกัน

QKD สามารถถูกนำไปใช้ปรับเปลี่ยนโพรโทคอล IKE โดยจะใช้สร้างความลับที่แบ่งปันกันนั้น เพื่อใช้ในการเข้ารหัสข้อมูลที่ต้องการความปลอดภัยสูงในการส่ง

6.3 ชั้นขนส่ง (Transport Layer)

ความปลอดภัยในชั้นขนส่ง (Transport Layer Security, TLS) และ ชั้นซอกเกตที่ปลอดภัย (Secure Sockets Layer, SSL) เป็นโพรโทคอลในชั้นที่ 4 ที่กำหนดความปลอดภัยของการบริการการสื่อสารผ่านระบบเครือข่ายจากต้นทางถึงปลายทาง โดยกุญแจของส่วนเซชชั่นที่สร้างนี้ จะสร้างจากการเปลี่ยนกุญแจสาธารณะซึ่งหากใช้ระบบ QKD ก็จะสามารถเปลี่ยนระบบกุญแจเป็นรหัสใช้ครั้งเดียวได้ทันที โดยกุญแจของ QKD อาจใช้ในการพิสูจน์ตัวตนที่แท้จริงแทนที่รหัสหรือโค้ดที่ใช้ในการพิสูจน์ตัวตนจริงแบบเดิม (Hash-based Message Authentication Codes (HMACs)) ที่ใช้อยู่ใน TLS หรือฟังก์ชันสุ่มแบบเทียมใน SSL แบบมาตรฐานได้

6.4 ชั้นแอพพลิเคชัน (Application Layer)

ชั้นที่ 7 นี้เป็นชั้นที่อยู่เหนือชั้นระดับการขนส่ง โดยระบบ QKD อาจนำไปรวมในชั้นนี้ได้ ในการสร้างแอพพลิเคชันที่ต้องการการส่งกุญแจเพื่อให้ผู้ใช้ได้ยืนยันตัวตนจริงและ/หรือการเข้ารหัสข้อมูลที่ต้องการส่งในแอพพลิเคชัน

7. กรณีการนำไปใช้

7.1 การสำรองข้อมูล / การดำเนินการทางธุรกิจแบบต่อเนื่อง

7.1.1 เป้าหมาย

เพื่อใช้ในการป้องกัน การสำรองข้อมูล และกระบวนการทำธุรกรรมทางธุรกิจแบบต่อเนื่อง

7.1.2 ลักษณะเชิงบรรยาย

องค์กรหนึ่งมีระบบเครือข่ายซึ่งมีการถ่ายโอนข้อมูลระหว่างหน่วยงานหลัก (Primary Site) และศูนย์สำรองข้อมูล (Backup Site) โดยการส่งข้อมูลนี้ต้องการให้มีการรักษาความลับด้วย ดังนั้นระบบเข้ารหัสจึงเป็นสิ่งจำเป็น ในกรณีนี้ QKD จะสามารถนำมาใช้สร้างตัวเข้ารหัสและลิงค์ความเชื่อมโยงได้ในตัวเดียว โดยมีรูปแบบดังรูปที่ 4

รูปที่ 4 ตัวเข้ารหัส QKD ลิงค์

7.1.3 แนวคิดในการทำงาน

ในการส่งข้อมูลนั้นสามารถทำได้หลายแนวทางได้แก่

การสำรองข้อมูลประจำวัน เป็นรูปแบบการส่งแบบอซิงโครนัส

การเก็บข้อมูล ณ ขณะหนึ่ง เป็นการรักษาข้อมูลหลักไว้ในศูนย์สำรองข้อมูล โดยการทำซ้ำข้อมูลจากหน่วยงานหลักในศูนย์สำรองข้อมูลนั้น

การสำรองข้อมูลในเครือข่ายสำรองข้อมูล ในกรณีที่การสำรองข้อมูลประจำวันไม่เพียงพอแก่ความต้องการ ซึ่งการสำรองประเภทนี้อาจลดระดับความปลอดภัยในการเก็บรักษาข้อมูล

การทำซ้ำฐานข้อมูล เป็นทางเลือกหนึ่งในการเก็บรักษาฐานข้อมูล เพื่อสำรองไว้ในกรณีที่เกิดความเสียหายขึ้นในหน่วยงานหลัก โดยการทำซ้ำนี้อาจทำในลักษณะอซิงโครนัสหรือซิงโครนัสก็ได้

7.1.4 ผู้ดำเนินการ

ในกรณีนี้คือ เช่น บริษัท ซึ่งเป็นผู้ดูแลหน่วยงานหลักและศูนย์สำรองข้อมูล โดยบริษัทจะต้องเป็นเจ้าของหรือเช่าระบบพื้นฐานในการส่งข้อมูลผ่านเส้นใยนำแสง

7.1.5 ข้อมูลจำเพาะเกี่ยวกับผู้ดำเนินการ

บริษัทจะต้องเป็นเจ้าของ ตัวเข้ารหัส QKD ลิงค์ โดยอุปกรณ์ผู้ส่ง (อลิซ) และผู้รับ (บ็อบ) จะต้องถูกควบคุมได้และต้องอยู่ในอาณาบริเวณที่ปลอดภัยในบริษัทนั้น

บริษัทจะต้องเป็นผู้สร้าง แบ่งปัน และ จัดการ กุญแจต่าง ๆ ด้วยตนเอง

บริษัทจะต้องคำนึงถึงระดับความปลอดภัยโดยรวมของตัวเข้ารหัส QKD ลิงค์

7.1.6 ประโยชน์ที่ผู้ดำเนินการจะได้รับ

บริษัทจะมีระบบการส่งข้อมูลที่ปลอดภัย

บริษัทจะมีการเข้ารหัสที่ใช้งานได้ง่ายและไม่ต้องการการจัดการกุญแจใด ๆ ในระดับแอพพลิเคชัน

7.1.7 การพิจารณาด้านการทำงานและคุณภาพของการบริการ

อัตราการส่งกุญแจที่สูงเพียงพอให้ใช้งานได้ จะขึ้นกับระบบการสร้างกุญแจและคุณสมบัติของช่องทางการสื่อสารเชิงควอนตัม

หากแอพพลิเคชันที่ใช้ ต้องการการทำงานอย่างต่อเนื่อง ตัวเข้ารหัส QKD ลิงค์จะต้องมีระบบที่ใช้การเทียบวัด

กุญแจสำหรับตัวเข้ารหัสลิงค์นี้ควรถูกเปลี่ยนอยู่เสมอ ขึ้นอยู่กับแบนวิดธ์ที่มีและนโยบายด้านความปลอดภัยของผู้ใช้

เส้นใยนำแสงที่ใช้เป็นช่องทางสื่อสารเชิงควอนตัมอาจถูกป้องกันทางกายภาพด้วยการฝังดินหรือมีการป้องกันอีกชั้นหนึ่ง

7.1.8 ลักษณะสมบัติการทำงาน

QKD ลิงค์ที่ใช้อาจมีความบอบบางมาก หรือ อาจเป็นลิงค์ที่แบ่งปันกันในระบบ

ตัวเข้ารหัส QKD ลิงค์จะทำงานอย่างอิสระ ไม่ขึ้นกับอุปกรณ์แม่ข่าย

การลิงค์จะต้องถูกเริ่มต้นอย่างเหมาะสมเพื่อให้เกิดการส่งข้อมูลที่ปลอดภัย

เมื่อการส่งข้อมูลเสร็จสิ้นแล้ว การเชื่อมโยง (ลิงค์) ระหว่างหน่วยนั้นจะต้องถูกตัดการเชื่อมโยง

7.2 เครือข่ายในองค์กร

7.2.1 เป้าหมาย

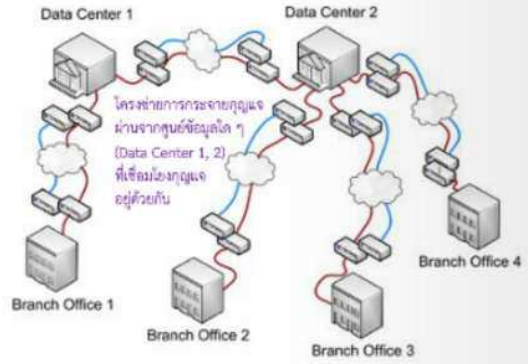
เพื่อใช้ในการป้องกันระบบพื้นฐานและการบริการในเครือข่ายในองค์กร

7.1.2 ลักษณะเชิงบรรยาย

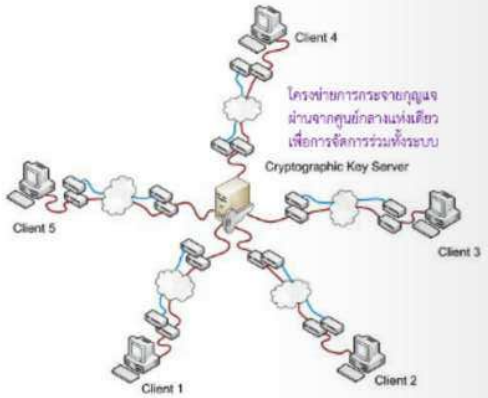
องค์กรหนึ่งหรือหน่วยงานของรัฐที่มีระบบเครือข่าย และมีความต้องการในการส่งข้อมูลระหว่างกัน ซึ่งในหน่วยงานอาจมีศูนย์ข้อมูล (Data Center) และสำนักงานสาขา (Branch Office) ต่าง ๆ โดยข้อมูลที่ส่งนี้อาจเป็น อีเมล สัญญาณเสียง วีดีโอ หรือ ฐานข้อมูล โดยผู้ส่งและผู้รับที่อยู่ในสำนักงานสาขาอาจไม่มีการเชื่อมต่อกันโดยตรง ทำให้ต้องส่งข้อมูลผ่านศูนย์ข้อมูลต่าง ๆ ในระบบเครือข่าย

องค์กรหรือหน่วยงานของรัฐนี้มีความต้องการในการรักษาความปลอดภัยของข้อมูลในขั้นสูงดังนั้นจึงต้องมีการใช้ตัวเข้ารหัส QKD ลิงค์

วิธีการที่ใช้ในปัจจุบันคือ การใช้ Virtual Private Network บน IPsec (ในชั้นเครือข่าย) หรือ TLS (ในชั้นขนส่ง) เพื่อใช้ในการยืนยันตัวตนจริงและการเข้ารหัสของข้อมูลที่ส่งในระหว่างศูนย์ข้อมูลและสำนักงานสาขา



รูปที่ 5 การใช้งานตัวเข้ารหัส QKD ลิงค์ผ่านเครือข่ายสาธารณะขององค์กร



รูปที่ 6 แม่ข่ายกุญแจศูนย์กลางที่ใช้ช่องทางการการจายกุญแจ QKD

7.2.3 แนวคิดในการทำงาน

ในการส่งข้อมูลข้อมูลทั้งหมดจะถูกเข้ารหัสในชั้นเชื่อมโยงข้อมูล ซึ่งจะทำให้มีความปลอดภัยในโพรโทคอลในชั้นสูงขึ้นไปทุกชั้น โดยชั้นแอพพลิเคชันจะใช้การเชื่อมโยงนี้อย่างง่ายเสมือนไม่มีระบบการเข้ารหัสใด ๆ

7.2.4 ผู้ดำเนินการ

ในกรณีนี้ คือ บริษัทหรือหน่วยงานของรัฐ ซึ่งเป็นผู้ดูแลศูนย์ข้อมูลและสำนักงานสาขา โดยบริษัทอาจเป็นเจ้าของหรือเช่าระบบพื้นฐานในการส่งข้อมูลผ่านเส้นใยนำแสง

7.2.5 ข้อมูลจำเพาะเกี่ยวกับผู้ดำเนินการ

เหมือนหัวข้อ 7.1.5

7.2.6 ประโยชน์ที่ผู้ดำเนินการจะได้รับ

ไม่มีความจำเป็นต้องเปลี่ยนแอพพลิเคชันใด ๆ เมื่อมีการเปลี่ยนมาใช้ระบบเครือข่ายที่ใช้ QKD

บริษัทจะมีการเครือข่ายที่เหมาะสำหรับการพัฒนาแอพพลิเคชัน อันต้องการความปลอดภัยของข้อมูลสูง

7.2.7 การพิจารณาด้านการทำงานและคุณภาพของการบริการ

เหมือนหัวข้อ 7.1.7

อัตราการส่งกุญแจที่สูงเพียงพอให้ใช้งานได้นั้นอาจแตกต่างกันในกรณีการส่งจากศูนย์ข้อมูลไปยังศูนย์ข้อมูล และการส่งระหว่างศูนย์ข้อมูลกับสำนักงานสาขา

การส่งข้อมูลอาจเกิดขึ้นแบบอัตโนมัติหรือแบบที่ต้องใช้เจ้าหน้าที่ควบคุม

การส่งข้อมูลระหว่างศูนย์ข้อมูลสองศูนย์อาจกระทำโดยการใช้งานลักษณะเดียวกันกับกรณี 7.1

7.2.8 กรณีการใช้งานที่แตกต่างออกไป: แม่ข่าย QKD

บริษัทหรือหน่วยงานของรัฐอาจใช้แม่ข่ายในการจัดการกุญแจเพื่อที่จะสร้างระบบการเข้ารหัสในส่วนต่าง ๆ ของเครือข่าย โดยเมื่อมีการเรียกร้องการให้บริการโดยผู้ใช้แล้ว แม่ข่ายก็จะดำเนินการผ่านตัวเข้ารหัส QKD ลิงค์ โดยอาจใช้รหัสแบบใช้ครั้งเดียวและการยืนยันตัวจริงของ Wegman-Carter เพื่อให้มีระดับความปลอดภัยสูงสุด

7.2.9 ลักษณะสมบัติการทำงาน

เหมือนหัวข้อ 7.1.8

7.3 การควบคุมโครงสร้างพื้นฐานและการเก็บข้อมูล

7.3.1 เป้าหมาย

เพื่อป้องกันการสื่อสารในการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐาน รวมไปถึงระบบเก็บข้อมูลที่สำคัญมาก (Supervisory Control and Data Acquisition, SCADA)

7.3.2 ลักษณะเชิงบรรยาย

ในประเทศอุตสาหกรรม เศรษฐกิจและสังคมจะดำเนินไปได้โดยอาศัยการทำงานอย่างต่อเนื่องของโครงสร้างพื้นฐานที่เรียกว่า โครงสร้างพื้นฐานวิกฤต (critical infrastructure) ตัวอย่างหนึ่งของโครงสร้างนี้คือระบบการให้บริการด้านการสื่อสาร โดยอินเทอร์เน็ตก็เป็นโครงสร้างพื้นฐานนี้ด้วย เพราะโครงสร้างพื้นฐานวิกฤตหลายประเภทได้อาศัยเครือข่ายอินเทอร์เน็ตในการส่งข้อมูล (ในการควบคุม)

ระบบ SCADA ใช้แนวทางการสื่อสารจำนวนมากในการทำงาน โดยระบบสื่อสารเหล่านั้นจะต้องมีความปลอดภัยสูงด้วย ตัวอย่างเช่น ระบบการควบคุมราง หรือระบบการจ่ายน้ำ ซึ่งจะต้องมีการควบคุมสวิตช์ต่างจำนวนมาก ดังนั้น คำสั่งควบคุมต่าง ๆ ต้องถูกส่งต่ออย่างถูกต้องและปลอดภัย (เป็นความลับ)

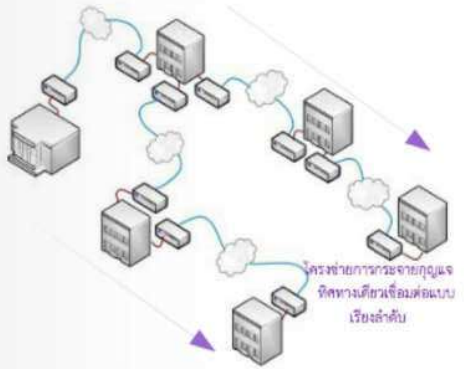
7.3.3 แนวคิดในการทำงาน

โครงสร้างของเครือข่ายโดยรวมคือระบบเครือข่ายระดับกว้างมากหรือ WAN (wide area network) การกระจายกุญแจควรกระทำในชั้นเชื่อมโยงดังแสดงในรูปที่ 4 หรือ ใช้ตัวทวนสัญญาณที่เชื่อถือได้ดังแสดงในรูปที่ 5 โดยเนื่องจากข้อจำกัดของการเชื่อมโยงแบบควอนตัมทำให้การเชื่อมโยงใน WAN จะต้องไม่มีระยะทางเกินขีดจำกัดของ QKD ลิงค์

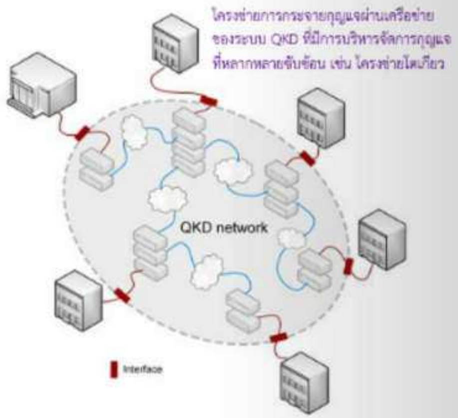
รูปที่ 7 และ 8 แสดงการเชื่อมต่อสองแบบที่มีการจัดการกุญแจที่แตกต่างกัน โดยใน WAN ที่ใช้ QKD ลิงค์แบบเดี่ยว การจัดการกุญแจจะกระทำอย่างชัดเจนที่โหนด ในขณะที่การใช้เครือข่าย QKD จะต้องมีการจัดการกุญแจแบบรวมและต้องมีการเชื่อมต่อที่เหมาะสม

7.3.4 ผู้ดำเนินการ

ในกรณีนี้ ผู้ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานวิกฤต จะเป็นผู้ที่รับผิดชอบให้โครงสร้างทำงานได้อย่างต่อเนื่อง โดยผู้ดำเนินการนี้จะต้องเป็นเจ้าของโหนดเครือข่ายและลิงค์ QKD หรือ เครือข่าย QKD โดยผู้ดำเนินการนี้จะต้องเป็นเจ้าของหรือเช่าเส้นใยนำแสงที่เชื่อมต่อกันด้วย



รูปที่ 7 เครือข่ายสื่อสารแบบ WAN ที่ใช้ลิงค์ QKD แบบเดี่ยว



รูปที่ 8 เครือข่ายสื่อสารแบบ WAN ที่ใช้ระบบ QKD

7.3.5 ข้อมูลจำเพาะเกี่ยวกับผู้ดำเนินการ

ผู้ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานวิกฤตจะต้องเป็นเจ้าของ ตัวเข้ารหัส QKD ลิงค์

อุปกรณ์อลิซและบ็อบ จะต้องถูกควบคุมได้และต้องอยู่ในภายใต้การควบคุมของผู้ดำเนินการนี้

เส้นใยนำแสงระหว่างอลิซและบ็อบ จะอยู่ภายนอกเขตปลอดภัยของผู้ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานและจะไม่ถูกควบคุมโดยผู้ดำเนินการเกี่ยวกับโครงสร้างพื้นฐาน

ผู้ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานวิกฤตจะต้องเป็นผู้สร้าง แบ่งปัน และ จัดการกุญแจต่าง ๆ ด้วยตนเอง

ผู้ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานวิกฤตจะต้อง ต้องการความปลอดภัยระดับสูงสุดสำหรับการการจายกุญแจ การเข้ารหัส และ การยืนยันตัวตนจริง

ผู้ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานวิกฤตจะต้อง ต้องการใช้งานได้ของระบบโครงสร้างพื้นฐาน

7.3.6 ประโยชน์ที่ผู้ดำเนินการจะได้รับ

ผู้ดำเนินการเกี่ยวกับโครงสร้างนี้จะมีระบบการส่งข้อมูลที่ปลอดภัย

ผู้ดำเนินการเกี่ยวกับโครงสร้างนี้จะมีระบบความปลอดภัยในระยะยาว และอาจไม่จำเป็นต้องพบกับความยุ่งยากในการปรับปรุงกระบวนการ

7.3.7 การพิจารณาด้านการทำงานและคุณภาพของการบริการ

ความต้องการการใช้งานได้ตลอดเวลาของโครงสร้างพื้นฐาน ทำให้จำเป็นต้องระมัดระวังอย่างพิเศษในการเทียบวัดและจัดหาเพื่อใช้งานลิงค์ QKD ต่าง ๆ

ความต้องการการใช้งานได้ตลอดเวลาของโครงสร้างพื้นฐาน ทำให้จำเป็นต้องคำนึงถึงกรณีที่ QKD ลิงค์หนึ่งใช้งานไม่ได้เนื่องจากการคุกคามหรือจากปัญหาอื่น ๆ

7.3.8 ลักษณะสมบัติการทำงาน

QKD ลิงค์ที่ใช้อาจมีความบอบบางมาก หรือ อาจเป็นลิงค์ที่แบ่งปันกันในระบบ

การลิงค์จะต้องถูกเริ่มต้นอย่างเหมาะสมเพื่อให้เกิดการส่งข้อมูลที่ปลอดภัย

7.4 การป้องกันแกนหลัก

7.4.1 เป้าหมาย

เพื่อใช้ QKD ในการให้บริการระหว่างโหนดของเครือข่ายแกนหลัก

7.4.2 ลักษณะเชิงบรรยาย

แนวคิดเบื้องหลังกรณีนี้คือการใช้การเชื่อมต่อที่เข้ากันได้กับระบบ QKD ในการเชื่อมต่อโครงสร้างพื้นฐานเพื่อให้สามารถแลกเปลี่ยนข้อมูลกันได้ผ่านช่องทางสื่อสารเชิงควอนตัมซึ่งอาจไม่มีการใช้งานจริง

7.4.3 แนวคิดในการทำงาน

ในกรณีนี้ ต้องการการเชื่อมต่อทางแสงระหว่างแกนหลัก โดยระยะทางในการส่งข้อมูลจะต้องไม่เกินขีดจำกัดของ QKD ที่ใช้ โดยจำเป็นต้องมีระบบการรวมหรือมัลติเพลกซ์โดยการแบ่งความยาวคลื่น (Wavelength Division Multiplexing, WDM) ที่สามารถมัลติเพลกซ์และแยกหรือดีมัลติเพลกซ์สัญญาณเชิงควอนตัมได้

ยิ่งไปกว่านั้น ระบบจะต้องเข้ากันได้กับอุปกรณ์ทางแสงอื่น ๆ เช่น ตัวมัลติเพลกซ์ทางแสงเพิ่ม-ลดแบบปรับแต่งได้ (reconfigurable optical add-drop multiplexers, ROADMs) สวิตช์แสง (optical switch) ตัวขยายแสง (optical amplifiers) หรือ วงจรรวมทางแสง (integrated optical circuit, IOCs) อื่น ๆ

7.4.4 ผู้ดำเนินการ

ผู้ดูแลระบบโครงสร้างพื้นฐาน จะเป็นผู้ดำเนินการในการเชื่อมต่อเครือข่ายแกนหลักโดยการเชื่อมโยงที่ใช้เทคโนโลยี WDM จะทำให้สามารถส่งสัญญาณดิจิทัลได้หลาย ๆ ช่องทางพร้อมกัน รวมถึงช่องทางสื่อสารเชิงควอนตัมด้วย กุญแจที่ QKD สร้างจะถูกใช้โดยผู้ดูแลระบบในการตรวจสอบความลับและยืนยันตัวจริงในการสื่อสารหนึ่ง และผู้ให้บริการที่ใช้งานโครงสร้างพื้นฐานนี้จะเป็นผู้กำหนดบริการทางการค้าแก่ลูกค้า

7.4.5 ข้อมูลจำเพาะเกี่ยวกับผู้ดำเนินการ

ผู้ดูแลระบบโครงสร้างพื้นฐานเป็นผู้ดูแลเครือข่ายแกนหลัก

ผู้ดูแลระบบต้องการจะควบคุมกระบวนการด้านความปลอดภัยและจัดการระบบย่อย

ผู้ดูแลระบบต้องการจัดหาโครงสร้างพื้นฐานแก่ผู้ให้บริการ และผู้ให้บริการก็จะต้องการระบบโครงสร้างพื้นฐานที่เชื่อถือได้และปลอดภัย

7.4.6 ประโยชน์ที่ผู้ดำเนินการจะได้รับ

ผู้ดูแลระบบโครงสร้างพื้นฐาน สามารถปกป้องการควบคุมเครือข่ายและการจัดการแกนหลักของเครือข่ายได้

ผู้ดูแลระบบสามารถจัดหาบริการเสริมแก่ผู้ให้บริการได้

ผู้ให้บริการสามารถให้บริการเสริมแก่ลูกค้าได้

7.4.7 การพิจารณาด้านการทำงานและคุณภาพของการบริการ

ผู้ดูแลและจัดการระบบจะต้องรวมระบบจัดการ WDM ลงไปด้วย

ระบบ QKD จะต้องเข้ากันได้กับโครงสร้างพื้นฐานที่ใช้เส้นใยนำแสง

ระบบ QKD จะต้องไม่ทำให้ระบบ WDM ที่ใช้อยู่เดิมมีประสิทธิภาพลดลงเกิน 10%

ระบบ QKD จะต้องถูกติดตั้งและดูแลร่วมกันโดยผู้ดำเนินการระบบ WDM โดยที่ไม่ต้องการความรู้ทางด้านฟิสิกส์เชิงควอนตัมในการดำเนินการ

7.4.8 ลักษณะสมบัติการทำงาน

-

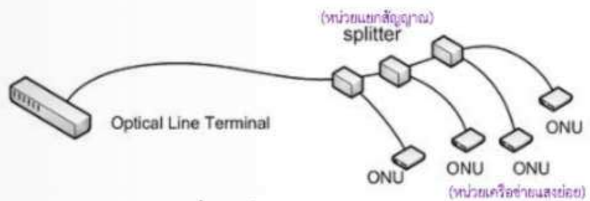
7.5 เครือข่ายที่ต้องการความปลอดภัยสูง

7.5.1 เป้าหมาย

เพื่อให้เกิดการสื่อสารที่ปลอดภัยในเครือข่ายทางแสงแบบพาสซิฟ

7.5.2 ลักษณะเชิงบรรยาย

ระบบ QKD จะถูกใช้ในการกระจายกุญแจให้กับผู้ใช้ปลายทางที่เชื่อมต่อผ่านเครือข่ายทางแสงแบบพาสซิฟ (Passive Optical Network, PON) อย่างที่ใช้ในสถาปัตยกรรมแบบนำเส้นใยนำแสงสู่ที่พักอาศัย (Fiber-to-Home)



รูปที่ 9 เครือข่ายทางแสงแบบพาสซิฟ

PON จะเชื่อมโยงผ่านขั้วปลายทางเชิงแสง (Optical Line Terminal, OLT) ด้วยหน่วยเครือข่ายเชิงแสง (Optical Network Unit, ONU) หลาย ๆ ตัว โดย OLT นี้จะติดตั้งอยู่ที่ผู้ให้บริการในขณะที่ ONU จะติดตั้งอยู่ใกล้กับผู้ใช้ปลายทาง ปัจจุบัน OLT จะให้บริการ 32-128 ONU โดยข้อมูลจะถูกกระจายจาก OLT ไปยังทุก ๆ ONU ในขณะที่การส่งข้อมูลกลับคืนไปจะทำผ่านการมัลติเพลกซ์โดยการแบ่งความถี่

PON จะใช้เฉพาะอุปกรณ์แบบพาสซิฟเท่านั้น โดยแต่ละ ONU จะเห็นสิ่งที่เชื่อมต่อลงมาทั้งหมดจาก OLT ดังนั้นการเข้ารหัสเป็นสิ่งจำเป็นที่จะใช้ป้องกันการดักจับข้อมูล ปัจจุบันใช้การแบ่งปันกุญแจแบบสมมาตรสำหรับการเข้า/ถอดรหัส โดยอาจทำการผ่านระบบสมาร์ทการ์ดหรือใช้วิธีการอสมมาตรอื่นรวมกับกระบวนการยืนยันตัวตนที่แท้จริง

7.5.3 แนวคิดในการทำงาน

ในการส่งข้อมูลระหว่าง OLT และ ONU สามารถใช้การส่งข้อมูลเชิงควอนตัมที่อยู่ในโฟตอนเดี่ยวหรือพัลส์ของแสงแบบอ่านได้ โดยหากส่งข้อมูลเป็นโฟตอนเดี่ยวแล้วตัวรับที่เหมาะสมก็จะได้รับข้อมูลโฟตอนเดี่ยวนั้น ซึ่งหากมีกระบวนการซิงโครนัสสัญญาณแล้วก็จะสามารถส่งกุญแจลับไปได้

7.5.4 ผู้ดำเนินการ

ผู้ให้บริการจะทำการดำเนินการที่ OLT ซึ่งปกติผู้ให้บริการนี้จะเป็นเจ้าของระบบโครงสร้างเส้นใยนำแสงพื้นฐานนี้ ผู้ให้บริการด้านเนื้อหาจะเป็นผู้จัดส่งเนื้อหาไปยังผู้ใช้ปลายทาง โดยในบางกรณีผู้ใช้ปลายทางอาจเป็นผู้จัดส่งเนื้อหานั้นเอง

7.5.5 ข้อมูลจำเพาะเกี่ยวกับผู้ดำเนินการ

ผู้ให้บริการต้องการการเชื่อมต่อที่ใช้ในการสื่อสารที่มีความปลอดภัยและพร้อมใช้งาน

ผู้ให้บริการด้านเนื้อหาจะเชื่อมั่นผู้ให้บริการและส่งข้อมูลออกไป ตัวอย่างเช่น การส่งข้อมูลลับให้กับผู้บริโภคข่าวสาร

ในกรณีที่ผู้ใช้ปลายทางเป็นผู้ให้บริการด้านเนื้อหา ที่จะมีเหตุผลให้เชื่อมั่นด้านความปลอดภัยที่จัดเตรียมโดยผู้ให้บริการสำหรับการส่ง/รับข้อมูล

7.5.6 ประโยชน์ที่ผู้ดำเนินการจะได้รับ

ผู้ให้บริการออกให้บริการที่มีความปลอดภัยในระยะยาว

ผู้ให้บริการด้านเนื้อหาอาจจะสร้างบริการที่ต้องใช้ความปลอดภัยในระยะยาว

การสร้างข้อมูลความลับแบบต่อเนื่อง ในระบบการสร้างกุญแจที่ใช้ QKD เพื่อลดปัญหาการเพิกถอนกุญแจ

7.5.7 การพิจารณาด้านการทำงานและคุณภาพของการบริการ

ในโครงสร้างของ PON ซึ่งมีระยะทางค่อนข้างสั้นทำให้ QKD สามารถสร้างกุญแจได้ด้วยอัตราค่อนข้างสูง ซึ่งสำคัญมากในการกำหนดการใช้งาน โดยการใช้กุญแจลับนี้อาจทำในระบบการเข้ารหัสแบบบล็อกหรือการใช้รหัสแบบใช้ครั้งเดียว

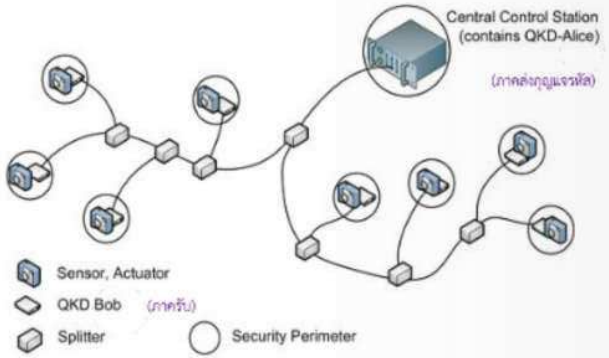
เครือข่ายที่มีความปลอดภัยสูงจะเป็นแอพพลิเคชันสำหรับ QKD ที่ไม่จำเป็นต้องคำนึงถึงระยะทางในการเชื่อมต่อ QKD นั้น จะทำให้ได้อัตราการสร้างกุญแจที่สูง

7.5.8 กรณีการใช้งานที่แตกต่างออกไป: เครือข่ายเซนเซอร์ที่มีการยืนยันตัวตนที่แท้จริงด้วย QKD

ระบบเครือข่ายเซนเซอร์ ประกอบด้วยสถานีควบคุมที่เป็นศูนย์กลางและมีการลิงค์แบบ QKD ในขณะที่โหนดต่าง ๆ จะอยู่ที่อีกด้านหนึ่งของลิงค์นี้ โดยตัวควบคุมศูนย์กลางนี้จะสร้าง QKD กุญแจแล้วแบ่งปันให้กับอุปกรณ์อื่น ๆ

7.5.9 ลักษณะสมบัติการทำงาน

-



รูปที่ 10 เครือข่ายเซนเซอร์ที่มีการยืนยันตัวตนที่แท้จริงด้วย QKD

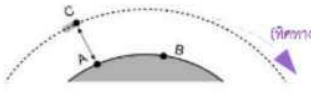


Figure 11: C and A exchange a secret *a*

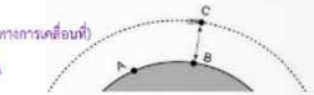


Figure 12: C and B exchange a secret *b*

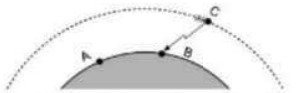


Figure 13: C sends encrypted secret (*a* xor *b*) to B using a classical channel

Figure 14: A and B share a common secret *a*

รูปที่ 11-14 แสดงกระบวนการในการแบ่งบันข้อมูลลับระหว่าง A และ B

(อธิบายการทำงานด้วยหัวข้อ 7.6.3)

7.6 การบริการระยะไกล

7.6.1 เป้าหมาย

เพื่อให้เกิดการกระจายกุญแจที่มีความปลอดภัยสูง ระหว่างตำแหน่งที่อยู่ห่างไกลกันอย่างมากโดยไม่มีการสมมติเกี่ยวกับความไว้วางใจได้ของโหนดระหว่างกลาง

7.6.2 ลักษณะเชิงบรรยาย

สถานีภาคพื้นดิน A และ B เป็นโหนดในระบบเครือข่ายที่ห่างไกลกันอย่างมาก เช่น ระบบสื่อสารผ่านทะเลลึกด้วยสายเคเบิล โดยทุกวันจะมีดาวเทียมผ่าน A และผ่านไปยัง B ดังนั้นสถานีทั้งสองนี้จึงสามารถแบ่งบันกุญแจได้ โดยกุญแจนี้จะใช้ในการเข้ารหัสลับแบบสมมาตรเพื่อที่ใช้ในการสื่อสารระยะไกล

ระบบนี้แตกต่างจากกรณีอื่น ๆ ที่มีการเชื่อมต่อโดยตรงผ่าน QKD ลิงค์ หรือผ่านเครือข่ายที่มีระบบ QKD อยู่ โดยในกรณีนี้ระยะทางที่พิจารณาอาจมีระยะไกลมาก เช่นการส่งผ่านดาวเทียมวงโคจรต่ำ (ระดับความสูง 300-800 กิโลเมตร)

การใช้งานในกรณีที่ต่างออกไปอาจเกี่ยวกับการมีดาวเทียมหลาย ๆ ดวงที่เชื่อมต่อกันผ่านลิงค์ในอวกาศ ซึ่งทำให้สามารถส่งกุญแจได้ด้วยอัตราที่สูงเนื่องจากแทบไม่มีการลดทอนของสัญญาณในอวกาศเมื่อเทียบกับการส่งผ่านอากาศในชั้นบรรยากาศ

7.6.3 แนวคิดในการทำงาน

สถานี A และ B มีระบบ QKD ที่ส่งข้อมูลผ่านอากาศได้ด้วยกล้องโทรทัศน์ทางไกลที่หมุนไปได้เพื่อหาเป้าหมาย C บนท้องฟ้า

เริ่มจากเมื่อ C ผ่าน A แล้วก็จะมีการสร้างข้อมูลลับ a และแบ่งปันกันระหว่าง A และ C โดยจะพิจารณาให้ C นี้เชื่อถือได้และปลอดภัยเนื่องจากสถานีลอยอยู่ห่างไกลกันมาก

จากนั้น C จะผ่าน B แล้วจะทำการสร้างข้อมูลลับ b และแบ่งปันกัน โดยเข้ารหัสข้อมูลนี้ด้วยการใช้รหัสแบบใช้ครั้งเดียว ซึ่งเมื่อ B ได้รหัสนี้แล้วจะสามารถถอดรหัสข้อมูลลับที่ A ส่งมาได้

7.6.4 ผู้ดำเนินการ

ผู้ดำเนินการในกรณีนี้ คือ สถานีภาคพื้นดิน A และ B และเป้าหมายเคลื่อนที่ C ที่ผ่านทั้ง A และ B โดย C นี้จะต้องเป็นของผู้ให้บริการหรือเจ้าของสถานีภาคพื้นดิน

7.6.5 ข้อมูลจำเพาะเกี่ยวกับผู้ดำเนินการ

สถานีภาคพื้นดินอาจอยู่จุดใดก็ได้บนพื้นโลกตราบเท่าที่เป้าหมายเคลื่อนที่ C เข้าถึง (ผ่าน) ได้

เจ้าของสถานีภาคพื้นดินต้องการความปลอดภัยสูงมาก เช่น หน่วยงานของรัฐ ผู้ให้บริการโครงสร้างพื้นฐานวิกฤต หรือกองทัพ

สถานีภาคพื้นดินอาจเป็นของบุคลเดียวหรือหลายบุคลก็ได้

7.6.6 ประโยชน์ที่ผู้ดำเนินการจะได้รับ

การกระจายกุญแจที่มีความปลอดภัยสูงจะทำได้ในระยะทางไกลมาก ๆ ระหว่างสถานีภาคพื้นดินได้

ผู้ให้บริการสามารถให้บริการที่แตกต่างและโดดเด่นได้

สถานีภาคพื้นดินสามารถเคลื่อนที่ได้บนพื้นดินหรือนิ่งอยู่กับที่ก็ได้

7.6.7 การพิจารณาด้านการทำงานและคุณภาพของการบริการ

ใน QKD ที่ส่งผ่านอากาศ การลดทอนอย่างมากด้วยบรรยากาศทำให้การส่งข้อมูลเป็นไปไม่ได้ในบางสภาวะการณ์

การให้บริการ QKD ในระยะทางไกลนี้จะใช้งานได้เมื่อมีช่องทางการกระจายกุญแจเสริมในกรณีที่ระบบหลักใช้งานไม่ได้

ช่วงโอกาสที่สามารถใช้ QKD ได้อาจจะสั้นมากเนื่องจากเป้าหมายมีการเคลื่อนที่

เป้าหมายเคลื่อนที่นี้อาจจะเข้าถึงได้ไม่ง่ายนักเนื่องจากอยู่ในอากาศ ซึ่งสิ่งนี้

อาจพิจารณาเป็นข้อดีในการรักษาความลับหรืออาจเป็นข้อเสียในกรณีที่ระบบใช้งานไม่ได้และต้องการการซ่อมแซม

7.6.8 กรณีการใช้งานที่แตกต่างออกไป: โหนด QKD ที่อยู่ในอากาศ

ในการใช้งานระบบเชื่อมต่อที่เคลื่อนที่ไปอาจทำได้โดยการใช้โหนด QKD ที่ลอยอยู่ในอากาศ

ดังที่แสดงในรูปที่ 5-8 หากแพลตฟอร์ม C ทำให้เกิดการเชื่อมโยงทางกายภาพและเกิดการสื่อสารระหว่างโหนด A และ B ในกรณีนี้ โหนด QKD ที่ลอยไปจะทำงานเหมือนรีเลย์หรือหน่วยผ่านสัญญาณที่เชื่อถือได้ โดยที่มีระยะเวลาประวิงระหว่างการเชื่อมโยงผ่านเครือข่ายที่กำหนด ด้วยเวลาที่เคลื่อนที่จาก A ไปยัง B

ภาคผนวก จ
รายงานการร่วมศึกษา
“อนาคตประเทศไทยกับสารสนเทศเชิงควอนตัม”

หมายเหตุ ผู้จัดทำได้เปลี่ยนชื่อเอกสารนี้ก่อนเผยแพร่เพื่อความเหมาะสมกับเนื้อหาที่สรุปได้จากโครงการ

ศูนย์ทดสอบฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการ รหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)

(Thai Quantum Cryptography Testbed)

Q-Thai Forum ECTI Association IEEE COMMUNICATIONS SOCIETY Thailand Chapter

(สมุดปกขาว)

ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยี ระบบวิทยาการรหัสลับเชิงควอนตัม

โครงการ

“ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยี ระบบวิทยาการรหัสลับเชิงควอนตัม (พ.ศ. ๒๕๕๙) (Thai Quantum Cryptography Testbed)”

พัฒนาจากอดีตข้อเสนอโครงการเดิม
“ศูนย์กลางการทดสอบการใช้งาน การวิจัยและการพัฒนาด้านวิทยาการรหัสลับเชิงควอนตัมของประเทศ”
(Thai Quantum Cryptography Testbed)
(นำเสนอครั้งแรก ปีพ.ศ.2551 ต่อคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.))

โดย

กลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย (Q-Thai.Org Forum)

สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI)
และ
ชมรมไฟฟ้าสื่อสาร (IEEE Communications Society -Thailand chapter)
สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE Thailand Section)

(เอกสารประกอบหลัก)

“พัฒนาการสารสนเทศเชิงควอนตัม” (พ.ศ.๒๕๕๕) (ISBN 978-616-12-0212-5)
“สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗)” (ISBN 978-616-37-4830-0)
“ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๘)” (ISBN 978-616-413-846-9)

ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)
(Thai Quantum Cryptography Testbed)
(จัดพิมพ์เป็นวิทยาทาน)

จัดทำโดย : เกียรติศักดิ์ ศรีพิมานวัฒน์

สนับสนุนเทคนิค : ปรมินทร์ แสงวงษ์งาม และ จุฑาเพชร เวชรังษี (OQC)
ศูนย์ความเป็นเลิศด้านฟิสิกส์ (Thailand Excellence Center in Physics)

นำเสนอร่วม : สุวิทย์ กิระวิทยา (*โครงการการสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม: การถ่ายทอดเทคโนโลยีและพัฒนา บุคลากร กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการ โทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส. - กสทช)*)

สนับสนุนโดย : สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ (ECTI)
ชมรมไฟฟ้าสื่อสาร สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทย (IEEE)

พิมพ์ครั้งที่ 1 (1.0) : *ตุลาคม 2559 (50 เล่ม)*

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
เกียรติศักดิ์ ศรีพิมานวัฒน์.
ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)
(Thai Quantum Cryptography Testbed).– กรุงเทพฯ : จรัลสนิทวงศ์การพิมพ์, 2559.
75 หน้า.

1. วิศวกรรมการสื่อสาร. 2. ระบบสื่อสารข้อมูล. I. ชื่อเรื่อง.
621.38
ISBN 978-616-423-438-3

ข้อมูลเพิ่มเติม : *www.facebook.com/QuantumCryptoThailand และ Q-Thai.Org*
แหล่งข้อมูลร่วม : *"พัฒนาการสารสนเทศเชิงควอนตัม" (พ.ศ.๒๕๕๕) (ISBN 978-616-12-0212-5)*
"สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๙)" (ISBN 978-616-37-4830-0) "ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)" (ISBN 978-616-413-846-9)
และบทสรุปมาตรฐานรหัสลับควอนตัมโลก)
โครงการร่วมกิจกรรมปีแห่งแสงสากล (IYL2015) : *www.light2015.org*
ภาพปกหน้า: *Fraud & โอทีควอนตัมไทยประดิษฐ์*
ภาพปกหลัง: *LEGO-QKD Network Strategy*

คำนำ

วิทยาการรหัสลับเชิงควอนตัม (quantum cryptography) ที่มีพัฒนาคู่ขนานมากับการคำนวณเชิงควอนตัม (quantum computing) ทั่วโลกนั้น ได้เริ่มต้นสร้างองค์ความรู้ในประเทศไทยมาร่วมทศวรรษแล้วนับถึงปี พ.ศ. 2559 โดยบันทึกสมุดปกขาวที่เผยแพร่สาธารณะฉบับนี้ คือข้อมูลส่วนหลักเพื่อการสร้างสนามเรียนรู้ที่เปิดกว้างเชื้อเชิญทุกภาคส่วนมาร่วมกันแต่งแต้มเติมสีสันบนพื้นความรู้ที่สะสมมาเหล่านั้น ให้เกิดเป็นโครงการจากความร่วมมือระดับชาติได้จริงต่อไป ส่วนหนึ่งของสมุดบันทึกนี้ (อดีต) เคยเป็นข้อเสนอโครงการ *"ศูนย์กลางการทดสอบการใช้งาน การวิจัยและการพัฒนาด้านวิทยาการรหัสลับเชิงควอนตัมของประเทศ" (Thai Quantum Cryptography Testbed)* โดยเสนอครั้งแรกเมื่อ ปี พ.ศ.2551 ต่อคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.) *(หลังเหตุการณ์ 19 กันยายน พ.ศ. 2549)* และต่อมามีการนำเสนออีกครั้งโดยลุล่วงแล้ว ผ่านความเห็นชอบจากคณะกรรมการบริหาร กทช.ในขณะนั้นแล้ว แต่ในปี พ.ศ.2553 มีการเปลี่ยนโครงสร้างจาก กทช. เป็น กสทช. รวมกับการเปลี่ยนแปลงภาคการเมืองและนโยบายก่อนหน้าและต่อ ๆ มาตลอดระยะเวลากว่า 8 ปี จึงทำให้โครงการเดิมนั้นต้องหยุดชะงักลง อันเป็นการเสียโอกาสของประเทศรวมถึงทรัพยากรที่ได้ลงทุนก่อนหน้านั้นแล้วทั้งครุภัณฑ์ บุคลากร เวลา รวมทั้งการติดตามความก้าวหน้าเทคโนโลยีของโลกที่ช้าลงด้วย กระนั้น ทีมงานนักวิจัยและบุคลากรที่เกี่ยวข้องได้พยายามรักษาสถานะภาพ องค์ความรู้และความพร้อมด้านต่าง ๆ เพื่อให้มีโอกาสฟื้นกลับมาเริ่มต้นใหม่ได้โดยยังคงต้องได้รับการผลักดันอย่างต่อเนื่องและการสนับสนุนจากทุกฝ่ายที่เกี่ยวข้องเพื่อไปสู่การสร้างเป็น *"ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม"* ดังวัตถุประสงค์ตั้งเดิมนั้นได้จริงต่อไป

องค์ความรู้ที่หยอยสร้างฐานมาตั้งแต่เริ่มการรวมกลุ่ม Q-Thai.Org เมื่อ พ.ศ. 2547 รวมถึงประสบการณ์การสร้างโครงสร้างพื้นฐานขนาดกลาง (*ภาคผนวก ค*) ได้นำมาบูรณาการร่วมกับ *"สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๙)"* และความก้าวหน้าช่วงปีอัตมา โดยได้สรุปรวมเป็นข้อเสนอในร่างใหม่ หากได้พิจารณาร่วมกับข้อมูลจาก *"ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม และบทสรุปมาตรฐานรหัสลับควอนตัมโลก"* อีกสองแหล่งข้อมูลสำคัญที่พัฒนาไว้ล่าสุด (พ.ศ. 2559) ด้วยนั้น ก็จะได้เป็นภาพอนาคตที่ชัดเจนมากขึ้น และเมื่อจตุปัจจัยหลักทั้งสี่คือ **งบประมาณ บุคลากร วิทยาการและนโยบาย** สามารถบังเกิดได้ในเวลาใกล้เคียงกัน ข้อเสนอโครงการเปิดกว้างสาธารณะนี้จึงอาจมีศักยภาพที่จะดำเนินการต่อได้ แต่หากโอกาสการจาตุรงค์ของปัจจัยสี่เหล่านั้นน้อยมากก็มิควรดำเนินการซ้ำแนวทางเดิมอีก อันจะเป็นการสูญเปล่าละลายโอกาสที่มีน้อยในแม่น้ำสายความคาดหวังขนาดใหญ่ซ้ำเติมเช่นอดีต หากอนาคตวิทยาการรหัสลับเชิงควอนตัมในประเทศไทยจำเป็นต้องวนเวียนอยู่แต่กรณีหลัง สมุดปกขาวฉบับนี้อย่างน้อยยังคงได้เป็นบันทึกความรู้ระหว่างทางของการศึกษาวิจัยและพัฒนา เพื่อให้คนรุ่นหลังได้ใช้ประโยชน์จากประสบการณ์ก่อนหน้าได้ และคงมีประโยชน์อื่นอยู่บ้างด้วย เช่น ช่วยป้องกันหรือร่วมสร้างภูมิคุ้มกันให้กับสังคมความรู้วิทยาศาสตร์ไทยต่อเรื่องหลอกลวง (fraud) ต่าง ๆ จากการนำ "ควอนตัม" ไปใช้ผิดทาง รวมทั้งส่งเสริมให้นักวิชาการสาขาที่เกี่ยวข้องในประเทศได้รับการตรวจสอบจากสังคมและกระตุ้นให้อยู่ในแนวทางเชิงสร้างสรรค์ ห่างไกลจากวิทยาศาสตร์เทียม (pseudo science) ต่อไปได้ด้วย

แม้อาจไปไม่ถึงเป้าหมายการสร้างศูนย์ฯ สมุดนี้คือองค์ความรู้สีขาวของรอบทศวรรษที่ผ่านมา ... มิเสียเปล่า

เกียรติศักดิ์ ศรีพิมานวัฒน์

บทสรุปพิเศษ

คำสำคัญ: *ศูนย์ทดสอบ ศูนย์ฝึกอบรมและถ่ายทอดเทคโนโลยี ระบบวิทยาการรหัสลับเชิงควอนตัม การสื่อสารปลอดภัย โครงข่ายสื่อสารทางแสง*

วิทยาการรหัสลับเชิงควอนตัมปรากฏพัฒนาการขัดเจนในหลายประเทศนับจากปี ค.ศ.1984 เป็นต้นมา ได้รับการผลักดันเป็นโครงการระดับชาติทั้งภาคพื้นดินจนขึ้นสู่ดาวเทียม มีสินค้ามากแบบออกจำหน่าย การใช้งานและการสาธิตเกิดขึ้นกับหลายเครือข่ายระดับใหญ่ จึงเป็นที่ประจักษ์ถึงบทบาทอย่างมีนัยสำคัญในอนาคตด้านความปลอดภัยสารสนเทศไปทั่วโลกแล้ว สำหรับประเทศไทยยังคงตามหลังความก้าวหน้าของโลกนั้นห่างไกลมาก มีพัฒนาการที่ยังไปไม่ถึงจุดมวลวิกฤตในทุกด้าน จากการประมวลข้อมูลและประสบการณ์ที่ผ่านมาประเทศไทยควรได้เร่งมุ่งเป้ากับกิจกรรมเพื่อการพัฒนาสร้างบุคลากร และการสร้างสนามเพื่อได้ใช้ทดสอบทดลอง ศึกษาดูงาน รวมทั้งเพื่อการเตรียมพร้อมด้านจริยธรรมและสังคมวิทยาและอื่น ๆ ต่อวิทยาการแขนงใหม่นี้ หรือแม้กับการเตรียมตัวเป็นผู้บริโภคเทคโนโลยีอย่างฉลาด ด้วยการเร่งพัฒนาบุคลากรและสร้างสนามทดสอบ (testbed) ซึ่งเป็นข้อเสนอสำคัญที่อยู่ในโครงการสาธารณะแบบเปิดนี้

กลศาสตร์ควอนตัมเมื่อประยุกต์กับเทคโนโลยีสารสนเทศ จะได้มาซึ่งระบบใหม่ที่มีขนาดเล็กลง เร็วขึ้น ตอบสนองความต้องการได้มากขึ้น เกี่ยวโยงกับอุปกรณ์ การสื่อสารข้อมูลและการประมวลผลข้อมูล เกิดเป็นวิทยาการใหม่ "สารสนเทศเชิงควอนตัม" ที่มีประสิทธิภาพสูงขึ้นมากด้วย จากกฎของ"กอร์ดอน มัวร์ (Gordon Moore)" ที่ทำนายว่าทุกหนึ่งปีครึ่งปริมาณหน่วยความจำและจำนวนเกตลอจิกในชิปหนึ่งตัวจะเพิ่มขึ้นเป็นเท่าตัว และเป็นจริงมาตลอด 30 ปี จนเล็กลงจนเข้าสู่ยุคระดับโมเลกุล อะตอม ไฟตอนหรืออิเล็กตรอน จึงเป็นอีกสาเหตุหนึ่งที่อุปกรณ์การคำนวณจนถึงการสื่อสารในยุคต่อไปจำต้องอธิบายด้วยกลศาสตร์ควอนตัม ที่จะมาเปลี่ยนแปลงความก้าวหน้าของโลกสารสนเทศอย่างมีนัยสำคัญ และหลังจากที่ปีเตอร์ ชอร์ (Peter Shor) ค้นพบวิธีคำนวณเชิงควอนตัมแยกตัวประกอบได้ในเวลาสดลงอย่างมากและหากทำได้ในระบบขนาดใหญ่ได้ หรือที่กล่าวถึงกันกับสิ่งที่เรียกว่าควอนตัมคอมพิวเตอร์ (quantum computer) จะส่งผลให้ความปลอดภัยของข้อมูลที่ใช้การเข้ารหัสแบบกุญแจสาธารณะสูญเสียความมั่นคงหรือปลอดภัยน้อยลงทันที จึงได้เกิดมีงานวิจัยและทดลองการใช้สถานะควอนตัมเพื่อสร้างกุญแจรหัสลับ (Quantum Key Distribution หรือ QKD) ในเวลาต่อมา อันเป็นต้นทางการกำเนิด "วิทยาการรหัสลับเชิงควอนตัม"เพื่อความมั่นคงทางสารสนเทศอนาคตได้ในที่สุด

จากการเปิดตัวควอนตัมคอมพิวเตอร์ของบริษัท D-Wave Systems (ราคาหน่วยละ 15 ล้านเหรียญ) ด้วยเงินทุนวิจัยระดับ 65 ล้านเหรียญโดยร่วมกับองค์กรระดับโลก เช่น กูเกิล (Google) (ที่ได้แถลงผลความก้าวหน้านับย้ำถึงศักยภาพการคำนวณแนวใหม่นี้เมื่อ 8 ธันวาคม พ.ศ.2558 รวมทั้ง การปรับทดสอบระบบปฏิบัติการโครม (Chrome 2016) ให้รองรับการป้องกันการถอดรหัสด้วยควอนตัมคอมพิวเตอร์ในอนาคต ด้วยเทคนิค quantum safe cryptography – 7 กรกฎาคม พ.ศ. 2559) หรือการใช้งานของบริษัทล็อกฮีดมาร์ติน (Lockheed Martin) และนาซา (NASA) ต่อมาบริษัท D-Wave สามารถระดมทุนจากหน่วยงานใหม่รวมถึง 160 ล้านเหรียญ รวมไปถึงการกิจลับของรัฐบาลสหรัฐอเมริกาที่เปิดเผยโดย เอ็ดเวิร์ด สโนว์เดน (Edward Snowden) อดีตพนักงานของสภาความมั่นคงแห่งชาติ (NSA) รายงานว่า มีโครงการลับมูลค่าสูงประมาณ 8 ล้านดอลล่าร์กับงาน "ควอนตัมคอมพิวเตอร์" เพื่อใช้ถอดรหัสภารกิจที่ขับข้อนกันแล้ว ในขณะที่บริษัทไอบีเอ็ม ได้เปิดให้ทดสอบระบบคำนวณควอนตัม 5 คิวบิต ผ่านเครือข่ายสื่อสารคลาวน์ (4 พฤษภาคม 2559) และยุโรปประกาศแผนลับปีมูลค่า 1 พันล้านยูโร กับการผลักดันเทคโนโลยีด้านควอนตัม (quantum manifesto: 17-18 พฤษภาคม 2559) ทั้งหมดนี้ ก็ยิ่งได้ทำให้เกิดการตระหนักที่จะต้องมีระบบรหัสลับเชิงควอนตัมเพื่อป้องกันไว้ล่วงหน้ากันแล้ว ทั้งนี้ โลกได้เข้าสู่สังคมดิจิทัลจึงมีความต้องการการรักษาความปลอดภัยสูงสุด (unconditioned security) มากขึ้นและสำคัญอย่างยิ่ง โดยเฉพาะสำหรับภาคการเงินการธนาคารและความมั่นคงของชาติ มีความจำเป็นที่ต้องเร่งรัดพัฒนาเทคโนโลยีที่สามารถรับมือกับภัยคุกคามเหล่านั้นให้ได้ นั่นก็คือการมีส่วนร่วมของ "รหัสลับเชิงควอนตัม" ในระบบสังคมเศรษฐกิจดิจิทัลด้วยนั่นเอง

รหัสลับบนพื้นฐานเชิงกลศาสตร์ควอนตัมนี้ได้รับการคาดการณ์ไว้ทั่วโลกมาหลายทศวรรษแล้วในอดีต เช่น ปี พ.ศ. 2549 RAND Corporation ระบุวิฏจักรเทคโนโลยีของโลกสำหรับค.ศ.2020 ว่า จะเป็น 1 ใน 16 เทคโนโลยีที่จะมีการใช้ในเชิงธุรกิจทั่วไปอย่างแพร่หลาย ปีพ.ศ.2551 Global Industry Analysis คาดการณ์ว่ามูลค่าการตลาดจะสูงถึง 842 ล้านเหรียญดอลล่าร์สหรัฐฯ และพ.ศ.2554 Technology Review โดยสถาบันเอ็มไอที (MIT) ให้เป็นหนึ่งในสิบเทคโนโลยีที่จะเปลี่ยนแปลงโลก เป็นต้น ต่อเนื่องมา จากการคาดการณ์นำมาสู่การเป็นแผนที่นำทางเทคโนโลยี (roadmap) ในที่สุด ซึ่งชุดแรกของโลกได้มีการจัดทำขึ้นนานแล้วโดยหน่วยงานด้านกลาโหมประเทศสหรัฐอเมริกาเป็นเจ้าภาพกับการคาดการณ์ระยะสิบปีเมื่อปี พ.ศ.2547 ครอบคลุมทุกมุมเทคโนโลยี ตามมาด้วยแผนที่นำทางระดับประเทศขึ้นนำอีกจำนวนมากทั้งจีน ญี่ปุ่น สิงคโปร์ และสหภาพยุโรป

สำหรับด้านมาตรฐานอุตสาหกรรมและความร่วมมือ สถาบันมาตรฐานอุตสาหกรรมโทรคมนาคมแห่งสหภาพยุโรป (ETSI) กำหนดมาตรฐานอุตสาหกรรมโดยมีกลุ่มทำงาน ISG-QKD เริ่มต้นขึ้นเมื่อปี พ.ศ.2552 และมีมากกว่า 20 ประเทศทั่วโลกเข้าร่วมกลุ่มแล้ว รวมถึงกลุ่มอาเซียนซึ่งเคยมีประเทศสิงคโปร์และมาเลเซียเท่านั้นที่เข้าร่วม ส่วนทรัพย์สินทางปัญญาและแนวโน้มอนาคตพบว่า ข้อมูลสิทธิบัตรโดยผลสรุปของช่วงปี ค.ศ.2001 ถึง ปี ค.ศ.2014 ประเทศสหรัฐอเมริกายื่นขอจดสิทธิบัตรและได้รับการคุ้มครองมากที่สุด ส่วนประเทศญี่ปุ่นและจีนติดตามมาอย่างใกล้ชิดและแนวโน้มทั่วโลกมีจำนวนสูงขึ้น[1] จนมาถึงปี พ.ศ.2556 รัฐบาลสหราชอาณาจักรตั้งงบถึงประมาณมากกว่าหนึ่งหมื่นสี่พันล้านบาท (270 ล้านปอนด์) ในการสนับสนุนการวิจัยด้านเทคโนโลยีเกี่ยวโยงกับกลศาสตร์ควอนตัมรวมห้าปีนั้น ได้สร้างแรงขับดันและการตื่นตัวไปในวงกว้างอีกกรณีหนึ่ง

มีข้อมูลอื่น ๆ ที่เกี่ยวข้องที่สามารถสะท้อนแนวโน้มความน่าจะเป็นสำหรับอนาคตของวิทยาการนี้ได้ด้วย เช่น รายงานทัศนคติสาธารณะเทคโนโลยีควอนตัมโดย "Sciencewise" ระบุว่าอนาคตอันใกล้มีโอกาสสูงมากที่เทคโนโลยีนี้จะส่งผลกระทบอย่างมีนัยสำคัญทั้งสุขภาพ การป้องกันความเป็นส่วนตัวในโลกออนไลน์และผลกระทบกับสิ่งแวดล้อมจึงมีความจำเป็นเร่งด่วนที่จะต้องปรับปรุงความเข้าใจสาธารณะ และจากการคาดการณ์นวัตกรรมโลกอนาคตของ Thomson Reuter ด้วยข้อมูลจากบทความวิจัยและสิทธิบัตร สรุปแนวโน้มที่จะมีการค้นพบยิ่งใหญ่ในทศวรรษหน้าพบว่า งานสารสนเทศเชิงควอนตัมเป็นหนึ่งในสิบหัวข้อสำคัญดังกล่าว เป็นต้น

กระทั่งปี พ.ศ.2558 ความก้าวหน้าล่าสุดของโลกพบว่าหลายประเทศกำลังพยายามผลักดันให้เป็นเทคโนโลยีในระดับชาติทั้งสหรัฐอเมริกา สหภาพยุโรป ญี่ปุ่น จีน สิงคโปร์ เกาหลีใต้และรัสเซีย โดยมีตัวอย่างที่โดดเด่นของประเทศเกาหลีใต้ที่ถูกโจมตีระบบสื่อสารดลอดช่วงเวลา จึงได้พัฒนาขีดความสามารถการรักษาความลับและความมั่นคงของตนเอง ส่วนหนึ่งมาจากระบบวิทยาการรหัสลับเชิงควอนตัมที่ทำสำเร็จในระยะเวลาเพียงสามปีกับงบลงทุนนับพันล้านบาท และกำลังพัฒนาบุคลากรระดับถึง 3,000 คนภายใน ปี ค.ศ.2020 อีกด้วย ตลอดจนการรวมกลุ่มของสหภาพยุโรป ได้ประกาศการปฏิวัติควอนตัมยุคที่สอง (second quantum revolution) ด้วยการร่วมประกาศ "quantum manifesto 2016" ที่จะลงงบประมาณหนึ่งพันล้านยูโรระยะเวลาสิบปีเพื่อการนั้น (ก่อนหน้าการลงประชามติแยกตัวของสหราชอาณาจักรหรือ Brexit) โดยโลกมีความก้าวหน้ามาโดยลำดับทั้งปรากฏสินค้าด้านรหัสลับเชิงควอนตัมและการสร้างโครงข่ายเพื่อการทดสอง การใช้งานจริง สู่การเชื่อมโยงที่กำลังกว้างขวางขึ้น ทั้งภาคพื้นดินจนสู่การทดสอบเชื่อมโยงผ่านดาวเทียม (ประเทศจีน) ด้วยแล้ว ซึ่งเป็นความก้าวหน้าที่ชัดเจนต่อมาถึงช่วง พ.ศ.2559

จากการคาดการณ์ของหลายสำนักและความก้าวหน้าต่าง ๆ บ่งชี้ได้ชัดเจนว่า วิทยาการรหัสลับเชิงควอนตัมกำลังจะมีบทบาทสูงมากในอนาคต หลายประเทศกำลังพยายามผลักดันโครงการของตนเองเนื่องจากเล็งเห็นถึงผลกระ

1 *ศึกษาพัฒนาการ "ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๔)" (ISBN 978-616-413-846-9)*

ทบและประจักษ์แล้วว่าวิทยาการนี้จะมีบทบาทอย่างมีนัยสำคัญ แม้ความรู้ความเข้าใจภาคสาธารณะจะยังคงเป็นเรื่องที่แปลกใหม่และมีอุปสรรคมาโดยตลอดกับวิทยาการแขนงนี้ ส่วนของประเทศไทยนั้นยังคงอยู่ในระยะเริ่มต้นพัฒนาการที่ผ่านมาจึงยังไม่ถึงจุดมวลวิกฤติ ทั้งด้านการพัฒนาบุคลากรใหม่ที่ต้องมีสาขาเชี่ยวชาญต่างกันถึงอย่างน้อยเจ็ดส่วนงาน (แต่ขาดแคลนทั้งหมด) ผลงานวิจัยและพัฒนาการศึกษาและการสื่อสารภาคสังคมยังคงมีช่องว่างต่างจากความคาดหวังที่กว้างมากเช่นเดียวกันกับเทคโนโลยีอุบัติใหม่อื่น ๆ ก่อนหน้า อันเป็นอุปสรรคที่หน้าหน่วงเช่นเดิม

และจากการรวบรวมสถานะภาพที่เกี่ยวข้องในประเทศไทยของโครงการที่เกี่ยวข้องในอดีตเพื่อเทียบเคียงและแสวงหาความเชื่อมโยง พบว่านอกจากสี่ปัจจัยพัฒนาสำคัญทั้ง **"นโยบาย งบประมาณ บุคลากร และเทคโนโลยี"** ประเทศไทยยังคงขาดแคลนมาก และกอปรสภาพเชิงสังคมไทยที่คำว่า "ควอนตัม" อาจนำพาความเข้าใจสาธารณะไปสู่แนวทางด้านลบหรือเรื่องหลอกลวง (fraud) ได้มากกับสินค้า บริการ และเรื่องวิทยาศาสตร์เทียม (pseudo science) ซึ่งต้องหาแนวทางป้องกันโดยล่วงหน้า ทั้งหมดนี้จึงได้นำมาสู่แนวทางอนาคตที่เหมาะสมกับสภาพสำหรับการพัฒนาด้วยข้อเสนอโครงการนี้ที่ **"ประเทศไทยควรมุ่งเป้าดังกล่าวกับกิจกรรมเพื่อการพัฒนาสร้างบุคลากรและการสร้างสนามเพื่อได้ใช้ทดสอบ ทดลอง ศึกษา ดูงาน รวมทั้งเพื่อการเตรียมพร้อมด้านจริยธรรมและสังคมวิทยาและอื่น ๆ"**หรือ การเป็นผู้บริโภคเทคโนโลยีอย่างฉลาดด้วยการการพัฒนาบุคลากรและสร้างสนามทดสอบ (testbed)

ดังนั้น กลุ่มวิจัยและพัฒนาเทคโนโลยีสารสนเทศเชิงควอนตัมไทย ร่วมกับหน่วยงานและเครือข่ายพันธมิตรจึงนำเสนอโครงการแบบเปิดกว้างนี้ เพื่อร่วมกันพัฒนาโอกาสสู่การเป็นโครงสร้างพื้นฐาน ศูนย์กลางการทดสอบ การใช้งาน การวิจัยและพัฒนาด้านการสื่อสารปลอดภัย การสื่อสารเชิงแสงและวิทยาการรหัสลับเชิงควอนตัมของประเทศโดยสามารถพึ่งพาตนเองได้ในระยะยาว เพื่อการรักษาความปลอดภัยของข้อมูลที่เหมาะสมสำหรับประเทศไทย รวมทั้งเพื่อสร้างและสะสมองค์ความรู้ด้านเทคโนโลยีสารสนเทศเชิงควอนตัมที่เกี่ยวข้อง และเร่งพัฒนาศักยภาพต่อยอดจากโครงสร้างพื้นฐานไปสู่นวัตกรรมใหม่และผลลัพธ์ที่เหมาะสม โดยควรได้ส่งเสริมการวิจัยและพัฒนาอุตสาหกรรมการสื่อสารโทรคมนาคมกับเทคโนโลยีสารสนเทศเชิงควอนตัมในประเทศที่เกี่ยวข้องไปพร้อมด้วย ทั้งสร้างความร่วมมือการถ่ายทอดเทคโนโลยี การเข้าร่วมวิจัยและมาตรฐานกับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศเพื่อติดตามเทคโนโลยีใหม่ที่มีผลกระทบ รวมถึงส่งเสริมและพัฒนาการเรียนการสอน การฝึกอบรมวิทยาการที่เกี่ยวข้องให้ก้าวทันในระดับภูมิภาคและการสื่อสารวิทยาศาสตร์แขนงใหม่นี้ที่ถูกต้องต่อสังคมเชิงสร้างสรรค์ต่อสังคม โดยมีบุคลากรที่มีความสามารถและองค์ความรู้เป็นผลผลิตหลัก

ทั้งนี้ โครงการนี้ได้พยายามพัฒนาข้อเสนอให้สอดรับกับแผนแม่บทเศรษฐกิจดิจิทัลสำหรับประเทศไทย โดยมีแนวทางเดียวกันกับโครงการ Smart Thailand ที่ครอบคลุมอยู่ใน 5 กลุ่มของ 10 กลุ่มอุตสาหกรรมเป้าหมายของประเทศ แนวทางการพัฒนาสารสนเทศเชิงควอนตัมอาจสามารถจัดให้อยู่ในกลุ่ม "อุตสาหกรรมอิเล็กทรอนิกส์อัจฉริยะ (Smart Electronics)" ที่จะได้สอดรับไปกับการรักษาความปลอดภัยในสังคมเศรษฐกิจดิจิทัลนั้นอย่างมีเป้าหมายด้วย โดยในส่วนยุทธศาสตร์หลักแรกของข้อเสนอโครงการแบบเปิดนี้ เน้นหนักที่การระดมทุนในการจัดสร้างศูนย์ ฯ อันมีสามกลยุทธ์สำคัญเพื่อการสร้าง ก) โครงสร้างพื้นฐาน ข) จัดหาอุปกรณ์เสริม และ ค) ดำเนินกิจกรรมวิจัยวิชาการและการศึกษา ดังนั้น ข้อเสนอโครงการระดมทุนการสร้าง "ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม" ระยะที่หนึ่ง กรอบเวลาสามปีนี้ จึงมีเป้าขั้นต้น เพื่อจัดหางบประมาณ (เฉพาะโครงสร้างพื้นฐาน) มากกว่า 23 ล้านบาท กับผลลัพธ์โครงข่ายวิทยาการรหัสลับเชิงควอนตัมอย่างน้อย 3 โหนดในสามปีแรกที่สามารถขยายเพิ่มโครงข่ายได้สะดวก เป็นศูนย์การผลิตบุคลากรวิจัยบัณฑิตศึกษามากกว่า 2 คน การฝึกอบรมประชุมวิชาการและสื่อสารสาธารณะรวมมากกว่า 10 กิจกรรม ผู้ผ่านการฝึกอบรมอย่างน้อย 200 คนรวมทั้งเกิดโครงการวิจัยต่อเนื่อง 3 โครงการกับ 3 หน่วยงานที่เข้าร่วมงานและได้รับประโยชน์จากศูนย์กลางฯ แห่งนี้ โดยสามารถขยายพร้อมรับไปกับการเปลี่ยนแปลงในอนาคตและอื่น ๆ เพื่อบรรลุดังวัตถุประสงค์ได้ต่อไป

"จึงนำเสนอเพื่อเป็นข้อเสนอสาธารณะผ่านสมุดปกขาวนี้เพื่อการมีส่วนร่วมกันของทุกภาคส่วน"

Executive Summary

Key Words : *quantum cryptography, optical communication network, testbed, education & training center*

Understanding quantum information technology (QIT), is that the two sides of the same coin. This kind of technology has been applying with quite a high potential. However, that quantum based technology is appeared to the public not only in positive side of its benefit, but also misled to negative attitude showing serious dramatic fraud. First side of that coin can be shown by worldwide quotes on applications in computing and communication areas such as: *"once quantum computer becomes powerful enough, our present and future secret information might be disclosed"*. That means secure communication is then on high risk. *"Though vast quantities of today data are being intercepted even if no capability to decrypt them yet, but they could be stored for future decryption too"*. In parallel, quantum cryptography, is that the absolute secure technique in order to prevent from that threatening. Since the history of quantum mechanics started formally in 1925, its applications have been widely adopted into various industries, and shown big impact on "Quantum IT" recently. A number of technology forecasting with many national roadmaps have been announced. Obviously, they have emphasized that future quantum based IT is indispensable. Major IT industrial players are involving in quantum computer, such as IBM, Google, Microsoft, NASA, and etc. Meanwhile, products on quantum cryptography or QKD have been released from new comers i.e. IDQuantique, SK telecom, MagiQ, Toshiba, and etc. Moreover, an industrial (ETSI) standard on QKD, academical progresses, and establishment of quantum based center worldwide, are also announced and highlighted. It leads to higher number of filled patent each year. China is ranked the highest in terms of academical results while USA is at the top on patent filling. Finally, more marketable applications in use today as a part of IT security.

Meanwhile those impressive scientific development have been showing but they are still in just a small group of people mostly in academia. However, another side of the same coin, there are a number of frauds by entitling "quantum" in many kind of products (nothing related to quantum mechanics) such as quantum pedant, bracelet, thermos bottle, cosmetics, health checker, or accessories, with miracle promoted specifications and results. In addition, a higher number of scandals from misconducted researches have been found in academic society. These negative impacts cover wider group of people and easier to be accessed. This dark side of the coin leads to high lost and destroyed many parts of science community. Those similar cases are presently so serious in the Thailand as well.

In conclusion, quantum technology is acknowledged to be an extremely difficult topic to understand and explain, public attitude is still in doubt with this new technology around the globe. But there is also evidence of conditional acceptance of the emerging technologies and in use today. We then have to aware both sides of this coin.

Situation in Thailand, it is still at the beginning. Developments over the past ten years has not yet reached any critical point lacking of four main key factors of success. Those are "budget, policy, personnel, and technology". Meanwhile, in the present social conditions the word 'quantum' may unbalance the public to the negative side or fraud (pseudo science) at higher weight. All of these statement of problems should lead to the national mission as **'Thailand should target such activities to develop human resources and a QKD testbed for education & training as well as to prepare the related ethics and sociology, and many others'**.

Understanding of both impact and fraud of Quantum Information Technology through realization on QKD testbed, is the project goal. It' s vision is in order to raise awareness the potential of quantum IT to the social, and to also prevent them from related fraud as "forewarned is forearmed" by having a QKD testbed. Since there have been many previous cases of scandal in Thailand including quantum titled product or pseudoscience, it is then necessary to solve the past properly and to prepare a sustainable future solution as well.

Therefore, Thai Quantum Information Forum (Q-Thai.Org) is proposing hereby a white paper of open-project proposal for the "Thai Quantum Cryptography Testbed". It is an opportunity to jointly develop the first national QKD infrastructure, as well as to create and to accumulate knowledge and technology-oriented quantum involved. Its benefit are to be a test & training center, research and development of secure communications, human resource development, science communications, and also for IT industrial linkage. Moreover, this paper has been developed in line with the master plan of Thailand's digital economy. The project is attempted to align with the "Smart Thailand" concept covering five of those 10 industrial groups.

Finally, the possible first phase of Thai Quantum Cryptography Testbed is proposed here in three-year time frame. Estimated budget on only the main infrastructure, is over 23 million baht for minimum three QKD nodes. Outcomes are such as more than 10 technical activities with at least 200 people trained including R&D projects, a number of graduate students involved, and many others. Further phase of activities and expansion could be constructed on this infrastructure well. This white paper welcomes all parties to jointly build up **"the first national quantum IT playground"**.

สารบัญโครงการ

(white paper)

Thai Quantum Cryptography Testbed

1. ชื่อโครงการ (ไทย) **ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม**
(อังกฤษ) **Thai Quantum Cryptography Testbed**

2. ระยะเวลาของโครงการ 3 ปี (ระยะที่ 1)

3. สถานที่ปฏิบัติงาน หน่วยงานการศึกษา มหาวิทยาลัย สถาบันวิจัยหรือพื้นที่ความร่วมมือที่เหมาะสม

4. ที่ปรึกษาโครงการ *(เรียงตามอักษรภาษาอังกฤษ)*

รศ.ดร.อธิคม อุกษ์บุตร	รองอธิการบดี มหาวิทยาลัยเทคโนโลยีมหานคร
รศ.บุญรักษา สุนทรธรรม	ผู้อำนวยการ สถาบันวิจัยดาราศาสตร์แห่งชาติ
รศ.ดร.เอกชัย ลีลารัศมี	คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Gaby Lenhart	European Telecommunications Standards Inst.
John DuBoise	ประเทศออสเตรเลีย
ศ.ดร.โกสินทร์ จำนงไทย	คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
รศ.ดร.โกศล เพียรสุวรรณ์	อดีตอธิการบดี สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร ลาดกระบัง
คุณขวัญชัย หล้าอุบล	ที่ปรึกษา สสวท. สวทน.
ศ.ดร.ไมไนย ไกรฤกษ์	อดีตรักษาการอธิการบดี สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร ลาดกระบัง
รศ.ดร.ณรงค์ อยู่ถนอม	รองอธิการบดี มหาวิทยาลัยศรีปทุม
ดร.พันธ์ศักดิ์ ศิริรัชตพงษ์	ที่ปรึกษาสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติและผช.รัฐมนตรีกระทรวงเทคโนโลยีสารสนเทศ ฯ
ศ.ดร.ประยุทธ อัครเอกฆาลิน	คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
คุณรังสรรค์ จันทร์นฤกุล	รองกรรมการผู้จัดการใหญ่ บริษัท ทีโอที จำกัด (มหาชน)
ศ.ดร.สวัสดิ์ ตันตระรัตน์	ภาคีสมาชิก ราชบัณฑิต
ศ.เศรษฐพร คูศรีพิพัทษ์	อดีตคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.)
ศ.ดร.สุทัศน์ ยกส้าน	ราชบัณฑิต
ดร.ทวีศักดิ์ กอซนันตกูล	ผู้อำนวยการ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
ศ.เกียรติคุณ ดร.ถิรพัฒน์ วิสัยทอง	ผู้อำนวยการ ศูนย์ความเป็นเลิศด้านฟิสิกส์ *(ประธาน)*
รศ.ดร.ทิพรัตน์ วงษ์เจริญ	รองอธิการบดี มหาวิทยาลัยกรุงเทพฯ
ศ.นพ.วิจารณ์ พานิช	นายกสภามหาวิทยาลัยมหิดล

5. ผู้อำนวยการโครงการ นายก สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ
ประธาน IEEE ComSoc Thailand *(เสนอรายชื่อ)*

6. คณะกรรมการเทคนิค ตัวแทนภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์
มหาวิทยาลัยที่เข้าร่วมโครงการ

ตัวแทนภาควิชาวิทยาการคอมพิวเตอร์และไอที
มหาวิทยาลัยที่เข้าร่วมโครงการ

ตัวแทนภาควิชาฟิสิกส์
มหาวิทยาลัยที่เข้าร่วมโครงการ

ตัวแทนสำนักบริการไอที คอมพิวเตอร์
มหาวิทยาลัยหรือหน่วยงานที่เข้าร่วมโครงการ

ตัวแทนศูนย์ความเป็นเลิศด้านฟิสิกส์

ตัวแทนคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์
และกิจการโทรคมนาคมแห่งชาติ (กสทช.)

ตัวแทนชมรมไฟฟ้าสื่อสาร
สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์

ตัวแทนสาขาโทรคมนาคม
สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและสารสนเทศ

ตัวแทนหน่วยงานผู้สนับสนุน

และ ตัวแทนหน่วยงานที่เกี่ยวข้องอื่น ๆ

7. หลักการและเหตุผล

การสื่อสารระหว่างผู้ส่งและผู้รับที่มีต้องการให้ผู้อื่นเข้าใจถึงข้อมูลที่ทำการส่งและรับนั้นต้องอาศัยการสื่อสารที่เรียกว่า วิทยาการรหัสลับ (cryptography) เพื่อป้องกันผู้อื่นล่วงรู้ถึงข้อมูลที่ทำการส่งและรับ ซึ่งกระบวนการสำคัญของวิทยาการรหัสลับนี้คือการเก็บรักษา**กุญแจลับที่**ใช้เข้ารหัสข้อมูลไม่ให้ผู้อื่นทราบ การเข้ารหัสตั้งแต่อดีตกาลเชิงบุคคลจนถึงปัจจุบันผ่านระบบอินเทอร์เน็ตนั้นจะใช้เทคนิควิธีทางคณิตศาสตร์ ซึ่งสามารถยืนยันความปลอดภัยของข้อมูลด้วยความยากในการแก้สมการทางคณิตศาสตร์ที่นำมาใช้เหล่านั้น แต่ด้วยความก้าวหน้าของวิทยาการด้านการคำนวณที่รวดเร็วขึ้นจากคอมพิวเตอร์ยุคต่อ ๆ มา ได้กลายเป็นปัจจัยสำคัญที่ทำให้คณิตศาสตร์ของรหัสลับแบบดั้งเดิมนั้นอยู่ในความเสี่ยงต่อการถูกแกะรหัสได้ในเวลาที่รวดเร็วขึ้น กระทั่ง ได้มีการนำเอากฎทางฟิสิกส์มาใช้รับประกันความปลอดภัยของข้อมูลข่าวสาร ซึ่งจะมีความปลอดภัยมากกว่าระบบวิทยาการรหัสลับรุ่นก่อนหน้า โดยการนำความสัมพันธ์เชิงควอนตัม (หลักความไม่แน่นอนของไฮเซนเบิร์ก (Heisenberg Uncertainty Principle)) มาประยุกต์ใช้กับระบบการสื่อสาร**กุญแจลับ**ผ่านช่องสัญญาณพิเศษที่เรียกว่าช่องสื่อสารเชิงควอนตัม (quantum channel) ร่วมกับการสื่อสารที่มีอยู่ปกติ เกิดเป็นวิทยาการรหัสลับเชิงควอนตัม (quantum cryptography) จึงทำให้ให้ผู้ส่งและผู้รับข้อมูลสามารถติดต่อสื่อสารที่เป็นความลับบนช่องสื่อสารทั่วไปได้โดยสมบูรณ์ ไม่มีผู้สามารถขโมยความลับด้วยการรับประกันจากหลักการทางฟิสิกส์

หลักการพื้นฐานโดยสังเขป คือ ข้อความ (plaintext) ที่ผู้ส่งต้องการส่งไปให้ผู้รับ จะถูกแปลงเพื่อให้เป็นข้อความที่ไม่สามารถเข้าใจได้ (ciphertext) โดยกระบวนการเข้ารหัส (encryption) ซึ่งผู้ส่งจะใช้กุญแจในการเข้ารหัส โดยที่ผู้รับซึ่งทราบ**กุญแจลับ**ที่ใช้ในการเข้ารหัสจะสามารถถอดรหัส (decryption) เพื่อแปลงกลับเป็นข้อความเดิมที่สามารถเข้าใจได้ ส่วนผู้ดักจับ (eavesdropper) จะไม่สามารถเข้าใจข้อความนั้นหากไม่ทราบ **กุญแจลับ** กระนั้นหากการขโมยข้อมูลความลับนั้น ก็สามารถอาจจะถูกแกะรหัส**กุญแจลับ**ได้ในอนาคตหลังจากการขโมยไป ไม่ว่าจากการแกะของเครื่องคำนวณทั่วไปหรือควอนตัมคอมพิวเตอร์ที่ได้กลายเป็นปัจจัยเสี่ยงสูงสุดเนื่องจากมีความเร็วในการทำงานที่สูงยิ่งยวด ซึ่งทั้งหมดนี้คือวิทยาการรหัสลับแบบดั้งเดิม

ส่วนความปลอดภัยของกุญแจรหัสลับหากได้ปรับมาใช้ร่วมกับหลักการทางฟิสิกส์เชิงควอนตัมแล้วนั้น จะรับประกันความปลอดภัยได้โดยสมบูรณ์จากการถูกขโมย โดยหลักการ "การใช้ครั้งเดียวทิ้ง (one time pad)" และการตรวจจับการเปลี่ยนแปลงของสถานะเชิงควอนตัมที่นำมาใช้แทนค่า**กุญแจลับ**หากมีผู้บุกรุกได้ด้วย วิทยาการรหัสลับเชิงควอนตัมจึงกลายเป็นเทคโนโลยีเสริมที่สามารถนำมาประยุกต์ใช้ป้องกันปัญหาอาชญากรรมการลักลอบขโมยข้อมูลและลดการสูญเสียทางเศรษฐกิจได้อย่างมีศักยภาพ เช่น การใช้กับระบบการเงิน การทหารและความมั่นคง เป็นต้น

ทั้งนี้ จากการคาดการณ์ถึงพัฒนาการของการสร้างคอมพิวเตอร์เชิงควอนตัม ที่กำลังมีความก้าวหน้ามากขึ้นเรื่อย ๆ นั้น เป็นอีกหนึ่งแรงขับดันให้วิทยาการรหัสลับเชิงควอนตัมเติบโตและต้องพัฒนาเร่งด่วนมากขึ้น เนื่องจากควอนตัมคอมพิวเตอร์จะกลายเป็นปัจจัยคุกคามต่อความปลอดภัยของข้อมูลในโลกไอทีปัจจุบัน อันหมายถึง รหัสลับต่าง ๆ จะสามารถถูก (ขโมย) ถอดรหัส**กุญแจลับ**ได้ในเวลาที่รวดเร็วขึ้นกว่าเดิมมาก หลายประเทศจึงได้เล็งเห็นความสำคัญ ได้คาดการณ์และวางแผนที่นำทางเทคโนโลยีวิทยาการรหัสลับเชิงควอนตัมมาตั้งแต่อดีตกันแล้ว โดยได้มีพัฒนาการความก้าวล้ำนวิชาการ ทรัพย์สินทางปัญญาหรือสิทธิบัตร สินค้า บริการเกิดขึ้นทั่วโลกตามมาอย่างมากมายเช่นกัน โดยโครงการ ฯ นี้ ได้นำเสนอข้อมูลเหล่านั้นโดยละเอียดสู่สาธารณะก่อนหน้าโดยลำดับแล้ว ทั้ง

- *"พัฒนาการสารสนเทศเชิงควอนตัม" (พ.ศ.๒๕๕๕) (ISBN 978-616-12-0212-5)*
- *"สารสนเทศเชิงควอนตัมประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ อดีตสู่อนาคต (พ.ศ.๒๕๕๗)" (ISBN 978-616-37-4830-0)*
- *"ทรัพย์สินทางปัญญาเทคโนโลยีรหัสลับเชิงควอนตัม (พ.ศ.๒๕๕๙)" (ISBN 978-616-413-846-9) และ*
- *บทสรุปมาตรฐานรหัสลับควอนตัมโลก" (พ.ศ.๒๕๕๙)*

ซึ่งกลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย ได้ติดตามและกลั่นกรองมาจากองค์ความรู้ ประสบการณ์กับหลายโครงงานก่อนหน้ามาจนถึงตลอดช่วงปี พ.ศ. 2559 และจะคงดำเนินการต่อเนื่องไป ณ Q-Thai.Org

ต่อเนื่องมาสู่กรอบแนวคิดของข้อเสนอโครงการการสร้าง **"ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed)"** นี้ ซึ่งได้ยกร่างขึ้นจากการร่วมสำรวจและวิเคราะห์ศึกษาอีกหลายส่วนเพิ่มเติมจากแหล่งข้อมูลที่จัดทำข้างต้นแล้วนั้น เช่น จากผลการคาดการณ์โลกอนาคตล่าสุดของสำนักต่าง ๆ แนวทางของเทคโนโลยีที่จะมีผลต่อการเปลี่ยนโลกอนาคต การศึกษาการสร้างสนามทดสอบไอที่ควอนตัมจากทั่วโลก โดยแยกย่อยไปที่กลุ่มสหภาพยุโรปอันมีตัวอย่างการลงทุนอนาคตของสหราชอาณาจักรในระดับหมื่นล้านบาท รวมทั้งแนวทางของประเทศจีนที่กำลังก้าวไปเป็นผู้นำโลกในหลากหลายด้าน จนถึงใกล้บ้านกับอนาคตของการพัฒนาสารสนเทศเชิงควอนตัมที่เป็นเอกลักษณ์แบบประเทศสิงคโปร์ และจากปัจจัยเสี่ยงการคุกคามด้านความมั่นคงทำให้ประเทศเกาหลีใต้และรัสเซียได้มีพัฒนาการแบบก้าวกระโดด สู่การพัฒนาสร้างรายได้ได้แล้ว เป็นอีกตัวอย่างที่ได้รับการสำรวจมาเพิ่มเติม เป็นต้น โดยทั้งหมดมาจากทั้งการสืบค้น การเยี่ยมชมดูงาน การร่วมหารือแนวทางและนโยบายของประเทศต่าง ๆ ที่เกี่ยวข้องกับบุคลากรจากหลายสถาบัน และอื่น ๆ

ขณะที่คู่ขนานไปกับการรวบรวมประสบการณ์และถอดบทเรียนที่เกี่ยวข้องในประเทศไทยในอดีต ซึ่งโครงการฯ นี้ พยายามแสวงหาความเชื่อมโยงข้อมูลเหล่านั้นเพื่อนำมาปรับใช้ โดยได้พบว่าสี่ปัจจัยพัฒนาสำคัญทั้ง "นโยบาย งบประมาณ บุคลากร และเทคโนโลยี" ยังคงขาดแคลนยิ่งและไม่มีแนวโน้มจะปรากฏขึ้นได้ในเวลาอันใกล้ กอปรสภาพเชิงสังคมไทยที่มีการนำคำว่า "ควอนตัม" มาใช้งานนอกวัตถุประสงค์ด้านวิทยาศาสตร์และเทคโนโลยี อันอาจได้นำพาความเข้าใจสาธารณะไปสู่แนวทางด้านลบหรือเรื่องหลอกลวง (fraud) ได้มากกับสินค้า บริการ และเรื่องวิทยาศาสตร์เทียม (pseudo science) ซึ่งต้องหาแนวทางป้องกันล่วงหน้านั้น

เมื่อประมวลผลจากข้อมูลทั้งหมดดังกล่าวข้างต้นแล้ว จึงนำมาสู่หลักการและเหตุผลที่ว่า **"ประเทศไทยควรมุ่งเป้าดังกล่าวกับกิจกรรมเพื่อการพัฒนาสร้างบุคลากรและการสร้างสนามเพื่อได้ใช้ทดสอบ ทดลอง ศึกษา ดูงาน รวมทั้งเพื่อการเตรียมพร้อมด้านจริยธรรมและสังคมวิทยาและอื่น ๆ"** นั่นคือ การเน้นหนักกับภารกิจ

"การพัฒนาบุคลากรและสร้างสนามทดสอบ (testbed)"

8.วัตถุประสงค์และขอบเขตของโครงการ

การดำเนินโครงการมีแนวทางแบ่งออกเป็นกรอบระยะ เพื่อพัฒนาในแต่ละช่วงให้เหมาะสมกับความพร้อมที่มีอยู่ โดยได้วางกรอบสองระยะแรกและเน้นหนักในข้อเสนอโครงการนี้ที่ระยะที่ 1 ดังรายละเอียด

- ระยะแรก (ปีที่ 1-ปีที่ 3) จะดำเนินการจัดสร้างเป็นศูนย์กลางการทดสอบ ฝึกอบรม วิจัย ถ่ายทอดความรู้และจัดตั้งโครงข่ายระบบวิทยาการรหัสลับเชิงควอนตัมด้านโครงสร้างพื้นฐาน (testbed)
- โดยระยะต่อไป (ระยะสอง ปีที่ 4-ปีที่ 5) เป็นการประเมินผลกระทบและต่อยอดโครงการให้มีความแข็งแรงและเป็นที่รู้จักทั้งในประเทศและในเวทีนานาชาติมากขึ้น
- และโครงการอนาคตลำดับต่อไป ๆ จากนั้นจะเป็นการต่อยอดโครงการที่อยู่บนพื้นฐานของศูนย์ฯ (testbed) นี้ได้โดยสะดวก (ดังวิธีดำเนินการและผลลัพธ์ หัวข้อที่ 9 และ 10)

สำหรับข้อเสนอโครงการแบบเปิดที่จะดำเนินงานระยะสำคัญลำดับแรกนี้ เพื่อสร้างรากฐานหรือสนามของระบบวิทยาการรหัสลับเชิงควอนตัมในประเทศไทยอย่างมีประสิทธิภาพขึ้นมาก่อน เพื่อใช้ทั้งการส่งเสริมความรู้ การพัฒนาบุคลากร และการสร้างเครือข่ายความร่วมมือวิจัย โดยโครงการมีพันธกิจ วิสัยทัศน์ และวัตถุประสงค์ ดังนี้

พันธกิจ (Mission)

สังคมมีความรู้ความเข้าใจ ตระหนักต่อเทคโนโลยี
วิทยาการสารสนเทศเชิงควอนตัมและที่เกี่ยวข้องพร้อมรับกับการเปลี่ยนแปลง

วิสัยทัศน์ (Vision)

การเป็นศูนย์กลางการทดสอบ การใช้งาน การวิจัยและพัฒนาด้านการสื่อสารปลอดภัย
การสื่อสารเชิงแสงและวิทยาการรหัสลับเชิงควอนตัมของประเทศไทย

วัตถุประสงค์ (Objectives)

1) เพื่อ**พัฒนาโครงสร้างพื้นฐาน**สู่การเป็นศูนย์กลางการทดสอบ การใช้งาน การวิจัยและพัฒนาด้านการสื่อสารปลอดภัย การสื่อสารเชิงแสงและวิทยาการรหัสลับเชิงควอนตัมแห่งแรกของประเทศโดยพึ่งพาตนเองได้ในระยะยาว

2) เพื่อ**ศึกษา วิจัยและพัฒนา** พร้อม**ฝึกอบรม**วิทยาการรหัสลับเชิงควอนตัม เพื่อการรักษาความปลอดภัยของข้อมูลที่เหมาะสมสำหรับประเทศไทย

3) เพื่อ**สร้างและสะสมองค์ความรู้**ด้านเทคโนโลยีสารสนเทศเชิงควอนตัมที่เกี่ยวข้องและเร่งพัฒนาศักยภาพต่อยอดจากโครงสร้างพื้นฐานไปสู่นวัตกรรมใหม่ที่เหมาะสม ทั้งการจดสิทธิบัตรที่มีศักยภาพ องค์ความรู้ใหม่ และต้นแบบซึ่งมีผลกระทบทางด้านความมั่นคงในอนาคต

4) เพื่อ**ส่งเสริมการวิจัยและพัฒนาอุตสาหกรรม**การสื่อสารโทรคมนาคม กับเทคโนโลยีสารสนเทศเชิงควอนตัมในประเทศที่เกี่ยวข้องให้ทัดเทียมกับนานาประเทศ โดยสร้างความร่วมมือการ**ถ่ายทอดเทคโนโลยี** การเข้าร่วมวิจัยและมาตรฐานกับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ

5) เพื่อ**ติดตามเทคโนโลยีใหม่**ที่มีผลกระทบทางด้านสารสนเทศเชิงควอนตัม รวมถึงส่งเสริมและพัฒนาการเรียนการสอน การฝึกอบรมด้านวิทยาการและเทคโนโลยีรหัสลับ การสื่อสารเชิงแสง ควอนตัมฟิสิกส์และวิทยาการที่เกี่ยวข้องอื่น ๆ ให้ก้าวทันในระดับภูมิภาค รวมทั้งการสื่อสารวิทยาศาสตร์แขนงใหม่นี้ที่ถูกต้องต่อสังคมเชิงสร้างสรรค์

6) เพื่อ**สร้างบุคลากร**ที่มีความสามารถ และเร่งยกระดับศักยภาพของบุคลากร ของกลุ่มวิจัยเทคโนโลยีสารสนเทศควอนตัมไทย ให้มีทั้งปริมาณและคุณภาพเพื่อรองรับอนาคตในระยะยาว

ขอบเขตเป้าหมายโครงการ (Goals)

โครงสร้างพื้นฐานเครือข่ายวิทยาการรหัสลับเชิงควอนตัมอย่างน้อย 3 โหนดในสามปีแรก ที่สามารถขยายเพิ่มโครงข่ายได้สะดวก พร้อมเป็นศูนย์การผลิตบุคลากรวิจัยระดับบัณฑิตศึกษา 2 คน การฝึกอบรม ประชุมวิชาการและสื่อสารสาธารณะรวมมากกว่า 10 กิจกรรม มีผู้ผ่านการฝึกอบรมอย่างน้อย 200 คน รวมทั้งเกิดโครงการวิจัยต่อเนื่องบนศูนย์กลางแห่งนี้ 3 โครงการกับ 3 หน่วยงานที่เข้าร่วมงานและได้รับประโยชน์

ยุทธศาสตร์ (Strategic)

โครงการการสร้าง "ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed)" นี้ มีที่มาและแนวคิดต่อยอดจากโครงการเดิมคือ *"การสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม:การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร)"* จากการสนับสนุนโดยกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส.) - กสทช. (คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช) พ.ศ.2558 - 2559)[2] เพื่อพัฒนาบุคลากรผ่านการฝึกอบรม และส่งเสริมสนับสนุนการสื่อสารวิทยาศาสตร์ด้านสารสนเทศเชิงควอนตัม ผ่านทางหน่วยงานสถาบันการศึกษาและอื่น ๆ ในช่วงก่อนหน้า รวมทั้ง จะเป็นการสืบงานด้านการสร้างโครงสร้างพื้นฐานที่ได้พัฒนาไว้ส่วนหนึ่งแล้วจาก (อดีต) ข้อเสนอโครงการ *"ศูนย์กลางการทดสอบการใช้งาน การวิจัยและการพัฒนาด้านวิทยาการรหัสลับเชิงควอนตัมของประเทศ"* (Thai Quantum Cryptography Testbed) เสนอครั้งแรกเมื่อปีพ.ศ.2551 ต่อคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.)[3] (หลังเหตุการณ์ 19 กันยายน พ.ศ.2549) และแม้ต่อมามีการนำเสนออีกสองครั้งโดยลุล่วงแล้วผ่านความเห็นชอบจากคณะกรรมการบริหารกทช.ในขณะนั้นแล้วก็ตาม แต่ในปี พ.ศ.2553 มีการเปลี่ยนโครงสร้างจาก กทช. เป็น กสทช. รวมกับการเปลี่ยนแปลงภาคการเมืองและนโยบายก่อนหน้าและต่อ ๆ มาตลอดระยะเวลากว่า 8 ปี จึงทำให้โครงการเดินมั่นต้องหยุดชะงักลง อันเป็นการเสียโอกาสของประเทศไปรวมถึงทรัพยากรที่ใส่ลงทุนก่อนหน้านั้นแล้วทั้งครุภัณฑ์ บุคลากร เวลา รวมทั้งโอกาสติดตามเทคโนโลยีความก้าวหน้าของโลกที่ช้าลง โดยทีมงานนักวิจัยและบุคลากรที่เกี่ยวข้องได้พยายามรักษาสถานะภาพองค์ความรู้และความพร้อมทุกด้านเพื่อให้มีโอกาสฟื้นกลับมาเริ่มต้นใหม่อีกครั้ง และเป็นโอกาสอันดีที่ปัจจุบัน (พ.ศ.2559) โครงการได้เริ่มกลับมาขับเคลื่อนงานส่วนย่อยด้านการพัฒนาบุคลากรแล้ว ซึ่งยังคงต้องได้รับการผลักดันอย่างต่อเนื่องและการสนับสนุนจากทุกฝ่ายที่เกี่ยวข้องเพื่อให้กลับเข้าสู่การสร้างเป็น "ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม" ดังวัตถุประสงค์ข้างต้นได้ต่อไป

โดยการจัดตั้งศูนย์ฯนี้ จะได้นำประสบการณ์ในอดีตมาปรับใช้เพื่อทั้งเร่งสร้างแนวทางการพัฒนาสำหรับอนาคตพร้อมลดความเสี่ยงจากปัจจัยสำคัญต่าง ๆ ทั้งสี่คือ **1. งบประมาณ 2. บุคลากร 3. การถ่ายทอดเทคโนโลยี** และ **4 . นโยบายที่เกี่ยวข้อง**[4] ที่ได้ประเมินความไม่สมบูรณ์ของโครงการในอดีตมาด้วยแล้ว และนำมาสู่การวางยุทธศาสตร์ที่มีทั้งความรู้ใหม่และประสบการณ์เดิมสู่การสร้างแผนกลยุทธ์ได้ รวมทั้งโครงการฯ ได้ศึกษาแนวทางของประเทศต่าง ๆ ที่กำลังดำเนินการงานด้านที่เกี่ยวข้อง (ดังภาคผนวก ข) เพื่อใช้เป็นทั้งแบบอย่างแนวทางและเพื่อสร้างความเชื่อมโยงเป็นพันธมิตรทางวิชาการ ดังรายละเอียดของยุทธศาสตร์ต่อไปนี้

2 *https://bitly.nbtc.go.th/annoucement/detail/959*

3 *โครงการความร่วมมือเดิม (MOU) ระหว่าง กทช. และศูนย์เทคโนโลยีไบโอเทคของอินเตอร์แห่งชาติ (ประเทศ) สวทช.*

4 *ปัจจัยสี่ของสิ่งหลัก (ภาคผนวก ข.4)*

ยุทธศาสตร์ที่ 1. ระดมทุน *(สร้างสนามเทคโนโลยีควอนตัม)*

ในการจัดสร้างศูนย์ ฯ ดังวัตถุประสงค์ดังที่แจ้งแล้วนั้น งบประมาณเพื่อการจัดซื้อจัดหาเครื่องมือหลักจะเป็นส่วนสำคัญที่สุดเสมือนโครงสร้างหลักของอาคารหรืออารามที่ต้องเริ่มต้นขึ้นก่อน จากนั้นจึงเป็นการจัดวางทั้งอุปกรณ์ ส่วนประกอบตัวงานหรือกิจกรรมและกำลังคนบนฐานรากดังกล่าว งบประมาณส่วนนี้มีขนาดและความสำคัญตามลำดับดังรายละเอียดของกลยุทธ์ ก) โครงสร้างพื้นฐาน ข) อุปกรณ์เสริม ค) กิจกรรมวิจัยวิชาการและการศึกษา ที่ได้ออกแบบพร้อมแล้วเพื่อการปฏิบัติได้ต่อเนื่องดังต่อไปนี้

กลยุทธ์ ก) โครงสร้างพื้นฐาน *(สร้างองค์ประธาน)*

อ้างอิงจากโครงสร้างระเบียบวิธีของการพัฒนาในหัวข้อที่ 9 รูปแบบการจัดหาเทคโนโลยีก้าวหน้าด้านวิทยาการรหัสลับเชิงควอนตัม จะเริ่มต้นด้วยเครื่องมือพื้นฐานที่มาประกอบกันเป็นโหนดของการสื่อสารเชิงควอนตัมด้วยยุทธศาสตร์การขยายแบบ LEGO-QKD network strategy ส่วนงานนี้จึงมีความสำคัญที่สุดอันเป็นหน้าที่หลักของภาครัฐในการสนับสนุนโครงสร้างพื้นฐานนี้ เฉกเช่นเดียวกับแนวทางอื่น ๆ ของต่างประเทศ (ภาคผนวก ข.1) ที่หากปราศจากการเริ่มต้นในส่วนนี้แล้ว จะไม่เกิดประโยชน์อันใดในการติดตามความก้าวหน้าวิทยาการสารสนเทศเชิงควอนตัม จะคงเหลือเพียงความรู้ส่วนบุคคลเท่านั้นดัง (ภาคผนวก ข.7) ที่ได้สรุปผลของโครงการในอดีตก่อนหน้า การจัดหาอุปกรณ์ดังกล่าวนี้ ก็เพื่อนำมาประกอบเป็นโครงสร้างของเครือข่ายวิทยาการรหัสลับเชิงควอนตัมให้ถึงจุดมวลวิกฤติพื้นฐานเป็นโครงข่ายได้ อันจะประกอบด้วยโหนดเชิงควอนตัม (Quantum Key Distribution node : QKD Node) จำนวนสามโหนดขั้นต่ำ (*เครือข่ายรหัสลับเชิงควอนตัมที่มีลักษณะของการรวมแล้นทางการเชื่อมต่อแบบจุดต่อจุดเข้าด้วยกัน (Point-to-Point)*) ซึ่งมีมูลค่าโดยรวม**มากกว่ายี่สิบสามล้านบาท** โดยประมาณ **(โหนดละขั้นต่ำเจ็ดล้านบาท)** และต้องใช้เวลาติดต่อประสานงานในการจัดหาอุปกรณ์วิจัยอีกประมาณ 1 ปี จึงหากลงทุนต่ำกว่านี้อาจได้เพียงการสื่อสารจุดต่อจุดมิใช่เครือข่ายสารสนเทศแต่อย่างใด[5] และอาจกลายเป็นการ "ตำน้ำพริกละลายแม่น้ำ" ดังเช่นประสบการณ์ในอดีตซ้ำเติมอีกได้ ดังนั้น สามโหนดพื้นฐานนี้จึงเปรียบเสมือนพระประธานในอารามที่จำเป็นยิ่งก่อนการเริ่มกิจกรรมอื่นหรือการจัดหาส่วนเพิ่มใด ๆ ในศูนย์ฯ โครงสร้างพื้นฐานส่วนหลักนี้จัดเป็นระดับงานชั้นที่สอง (layer 2) ของรูปที่ 10.1 ว่าด้วยโครงข่ายแบบขยายได้ในอนาคตใน**ยุทธศาสตร์ที่ 2 (สร้างบุคลากร)** ดังจะนำเสนอในหัวข้อต่อไป

ในช่วงที่สภาพเศรษฐกิจของประเทศไม่เอื้ออำนวย และหน่วยงานของรัฐทั้งภาคการศึกษาและวิทยาศาสตร์และเทคโนโลยีไม่สามารถขยายกิจกรรมวิจัยกับโครงสร้างพื้นฐานขนาดใหญ่ได้ (โดยโครงการนี้ต้องการครุภัณฑ์และเครื่องมือราคาสูงจำนวนมาก) จึงอาจมีแนวทางเลือกหลักคือ **การสนับสนุนโครงสร้างพื้นฐานปีโดยตรงจาก กสทช. ซึ่งมีภารกิจสอดคล้องและมีศักยภาพมากที่สุดที่จะสามารถเริ่มต้นได้ครบในระดับมวลวิกฤติพื้นฐาน (สามโหนด)**

โครงสร้างพื้นฐานหลักส่วนนี้ มีความเป็นไปได้แม้จะน้อยมากจากการบริจาครายใหญ่จากภาคส่วนต่าง ๆ แต่หากไม่ถึงจุดมวลวิกฤตหรือได้รับมาพร้อมเพรียงกันก็จะไม่มีคุณค่าดังวัตถุประสงค์ แต่หากมีโอกาสได้รับพร้อมทั้งสองส่วนทั้งจากกสทช.และภาคส่วนอื่น ๆ (มากกว่าสามโหนด) ก็จะกลายเป็นการขยายโครงข่ายให้มีศักยภาพสูงขึ้นได้ รวมทั้งใช้งานสำรองหรือทดแทนได้ด้วยเช่นกันตามแนวทาง LEGO-QKD network strategy **อนึ่ง** *แต่ละโหนดมีอายุการใช้งาน 3-5 ปีตามปกติของเทคโนโลยีที่เกี่ยวข้องทั่วไป*

5 *โหนดเครือข่ายเชิงควอนตัม (quantum node network) หมายถึงมีจำนวนโหนดการสื่อสารตั้งแต่สามโหนดขึ้นไปที่จะสามารถทำให้ทุกโหนดสื่อสารถึงกันได้*

กลยุทธ์ ข) จัดหาอุปกรณ์เสริม *(ปลูกป่าในอาราม)*

ในการประกอบเป็นศูนย์ฯ เพื่อกิจกรรมดังวัตถุประสงค์ข้างต้น เมื่อได้จัดวางโหนดหลักของการปฏิบัติงานได้แล้วนั้นในขั้นต่ำหรือถึงจุดมวลวิกฤติ กิจกรรมที่คู่ขนานคืออุปกรณ์เสริมหรืออุปกรณ์เฉพาะทาง อาทิ หน่วยวัดแสงความไวสูงมาก (เช่น controllable single photon detector) และอุปกรณ์ทัศนศาสตร์เชิงควอนตัมอื่น ๆ ที่ต้องจัดหาพิเศษเนื่องจากมีผู้ผลิตน้อยราย และเทคโนโลยีอีกหลายส่วนยังไม่เป็นที่เปิดเผยทั่วไปในสาขาสารสนเทศเชิงควอนตัมนี้

การออกแบบกลยุทธ์ส่วนนี้ (ดังรูปที่ 10.1) ได้ประมาณจุดมวลวิกฤติไว้ที่ 1 0 ส่วนงานพื้นฐานของการเป็นศูนย์ฯ อันจะมีความพร้อมในการซ่อม สร้าง และเตรียมการพัฒนาขั้นต้น ซึ่งมีมูลค่าโดยรวมคือหนึ่งล้านบาท (ส่วนละหนึ่งแสนบาท) โดยประมาณ ทั้งนี้ต้องการได้รับการสนับสนุนพร้อมร่วมกับโครงสร้างพื้นฐานของ**กลยุทธ์ ก)** จึงจะสามารถจัดสร้างส่วนประกอบให้แต่ละโหนดงานทำงานได้

ทั้งนี้ ในอนาคตระยะต่อไปของโครงการ ส่วนของอุปกรณ์เสริมต่าง ๆ เหล่านี้จะสามารถร่วมจัดหาจากหน่วยงานอื่นร่วมเพิ่มเติมได้ เนื่องจากระดับราคาอยู่ในวิสัยที่องค์กรระดับประเทศทั้งของรัฐและเอกชนรายใหญ่จำนวนหนึ่งสามารถสนับสนุนโดยมีกิจกรรมรองรับกับศูนย์ฯ ที่จะได้**ประโยชน์ร่วมกันในลักษณะโครงการร่วม (joint project) เช่น การฝึกอบรมพนักงาน การทดสอบเชิงเทคนิคที่เกี่ยวข้อง การสนับสนุนเชิงสื่อสารองค์กร (CSR) ที่เกี่ยวข้อง และเพื่อการซ่อมบำรุงโหนดสื่อสารเชิงควอนตัมในระยะยาวด้วย** เป็นต้น

ทั้งหมดนี้ เมื่อนำมาประกอบกันจึงเสมือนกลยุทธ์การทยอยปลูกโครงสร้างส่วนประกอบเสริมในระดับรองลงมาเพื่อสนับสนุนโครงสร้างพื้นฐาน**กลยุทธ์ ก)** อันเป็นองค์ประกอบที่จำเป็นสำหรับการเริ่มต้นเช่นกัน ดังนั้นแล้วศูนย์กลางฯจึงจะสามารถที่พึ่งพาตนเองในระยะต่อ ๆ ไปได้ ด้วยกิจกรรมที่สำคัญและสัมพันธ์กับโครงสร้างพื้นฐาน (testbed) นี้

อ นี่ ง สำหรับครุภัณฑ์วิทยาศาสตร์ ไฟฟ้าอิเล็กทรอนิกส์ เครื่องมือช่างและอุปกรณ์พื้นฐานทั่วไปนั้น ควรสนับสนุนโดยหน่วยงานที่เข้าร่วมเอง (เช่น มิเตอร์ ออสซิลโลสโคป (oscilloscope) หน่วยวิเคราะห์สัญญาณ (analyzer) ในระดับพื้นฐานที่มีใช้อยู่เพื่อการศึกษาในห้องปฏิบัติการ หรืองานการเรียนการสอนเดิมอยู่แล้ว เป็นต้น)

กลยุทธ์ ค) กิจกรรมวิจัยวิชาการและการศึกษา *(ชวนทำวิทยาทาน)*

จากการจัดกิจกรรมวิจัยวิชาการและอื่น ๆ ขั้นต่ำทั้ง 10 ครั้งในสามปี (ดังหัวข้อที่ 12) อันเป็นการสัมนา ฝึกอบรม เยี่ยมชมดูงาน การประชุมวิชาการ ฯ โดยประมาณการกิจกรรมขั้นต่ำกิจกรรมละ 50,000 บ า ท (รวม 750,000 บาท) ซึ่งงบประมาณระดับกิจกรรมนี้สามารถจัดหาเพิ่มเติมมาประกอบจากหน่วยงานต่าง ๆ ซึ่งอยู่ในวิสัยที่ไม่สูงเกินไป สามารถขยายผลการจัดกิจกรรมให้มากและหลากหลายขึ้นได้อีกในอนาคต

และเมื่อโครงสร้างพื้นฐานของ **ก)** และ**ข)** มีความพร้อมของอุปกรณ์เครื่องมือของศูนย์เพียงพอในระดับหนึ่งแล้ว ก็จะสามารถเชิญชวนผู้สนใจทั้งภาครัฐและเอกชนเข้าร่วมรับการฝึกอบรมและร่วมสนับสนุนการพัฒนาในระดับกิจกรรม **ค)** นี้ต่อได้มากขึ้นโดยลำดับ อันจะเป็นการขยายผลให้ได้ใช้ประโยชน์ศูนย์กลางฯให้กว้างขวางขึ้น ซึ่งแนวกลยุทธ์นี้เปรียบได้กับการร่วมสร้างวิทยาทานของผู้มีศักยภาพทั่วไปจำนวนมาก ในลักษณะการ**ระดมทุน (crowd funding) หรือการส่งเสริมภาพลักษณ์องค์กร (CSR)** เป็นต้น

ยุทธศาสตร์ที่ 2. สร้างบุคลากร *“ประตูสู่ควอนตัมโลก”*

การพัฒนาโครงการใด ๆ บุคลากรคือปัจจัยพื้นฐานที่สำคัญสุด หากแต่ในสาขาใหม่ด้านนี้ในประเทศไทยอาจกล่าวได้ว่ายังห่างไกลยิ่งจากจุดมวลวิกฤติ หรือไม่สามารถเพียงจะเริ่มปฏิบัติงานได้ครบระบบมาก่อน เช่น แม้เพียงเฉพาะการนำเทคโนโลยีรหัสลับเชิงควอนตัมที่มีอยู่แล้วไปประยุกต์ใช้งานกับระบบงานสารสนเทศที่มีอยู่ ก็ยังคงไม่สามารถรวมบุคลากร ผู้รู้หรือรวมส่วนงานได้ครบทุกระดับสำคัญ (7 OSI layers ภาคผนวก ข.5) จึงมีความสำคัญสูงยิ่งที่ต้องเร่งพัฒนาร่วมไปกับการสร้างสนามให้นักศึกษานักวิจัยหรือผู้ปฏิบัติงานได้เริ่มต้นของ**ยุทธศาสตร์ที่ 1**.

สำหรับประวัติการพัฒนาบุคลากรด้านที่เกี่ยวข้องนั้น ตั้งแต่เริ่มการรวมกลุ่มผู้สนใจในประเทศเมื่อปีพ.ศ.2547 พบว่ามิได้ขาดแคลนผู้สนใจ แต่หากไม่มีผู้ประสงค์จะปฏิบัติงานระยะยาวหรือตั้งใจจะยึดงานสาขาสารสนเทศเชิงควอนตัมเป็นอาชีพ (ข้อมูลน้อยมากและไม่มีนัยสำคัญด้านจำนวนหรือสถิติ) สำหรับแวดวงการศึกษามีนักศึกษาเข้าร่วมทำโครงงานหรือศึกษาสาขานี้น้อยและผิวเผิน รวมทั้ง บุคลากรวิจัยเต็มเวลามีอัตราการเปลี่ยนงาน (turn over) สูงมากเช่นกัน[6] ในอดีต**ด้านการจัดสรรทุนการศึกษาทั้งในและต่างประเทศ ได้มีการนำเสนอแผนการพัฒนาบุคลากรจนได้รับการสนับสนุนจำนวนหนึ่ง มีผู้รับทุนของกระทรวงวิทยาศาสตร์และเทคโนโลยีศึกษาต่อด้าน*วิทยาการรหัสลับเชิงควอนตัม*ในต่างประเทศ 3 คนจากจำนวน 4 ทุน (สละสิทธิ์ 1) โดยจบการศึกษาแล้ว 2 คนและเปลี่ยนสาขาการปฏิบัติงานแล้วทั้งหมด (พ.ศ.2558) และยังไม่ปรากฏว่ามีหน่วยงานใดมีแผนการสร้างบุคลากรสาขานี้เพิ่มเติมเป็นทางการอีก**

ทั้งหมดนี้ จึงเป็นตัวอย่างของประสบการณ์ที่จำเป็นต้องแสวงหาแนวทางใหม่ที่สามารถนำมาปรับใช้เป็นกลยุทธ์สู่อนาคต โดยในเบื้องต้นโครงการฯ ได้ศึกษารูปแบบกว้างของการพัฒนาบุคลากรของประเทศต่าง ๆ พบว่าแม้แนวทางของประเทศสิงค์โปร์มีความเป็นไปได้ดีที่สุด แต่การเชิญชวนผู้เชี่ยวชาญต่างชาติมาทำงานประจำในสถาบันต่าง ๆ ของประเทศที่สร้างขึ้นรองรับโดยเฉพาะ ซึ่งต้องใช้งบประมาณสูงมาในคราวเดียว (ภาคผนวก ข.3.4) อาจไม่สามารถนำมาใช้กับโครงการในประเทศไทยนี้โดยตรงได้ จึงต้องปรับแปลงและได้เกิดเป็นสองแนวทางย่อยโดยทั้งจะเชื่อมโยงกับยุทธศาสตร์ที่ 3 ด้านวิทยาการและการถ่ายทอดเทคโนโลยีร่วมกับกลุ่มอาเซียนและประเทศผู้ผลิตและการเร่งพัฒนาบุคลกรระดับพื้นฐานเชิงวิจัย (มิใช่นักประยุกต์ระยะสั้นเช่นในอดีต) เพื่อพึ่งพาตนเองให้ได้มากที่สุดด้วย โดยมีแผนกลยุทธ์คือ

กลยุทธ์ ก) สร้างสำนักวิชา

หน่วยงานด้านการศึกษาและสร้างบุคลากรที่เข้าร่วมโครงการ ควร**จัดสรรงบประมาณด้านทุนการศึกษา (matching fund) ตามอัตราส่วนระยะเวลาอย่างน้อยปีละสองทุน** อันเป็นการสร้างฐานชั้นล่างและชั้นที่หนึ่ง (layer 1) ดัง รูปที่ 10.1 ขอบเขตโครงการด้วยโครงข่ายแบบขยายได้ในอนาคต (LEGO-QKD network strategy) โดยมีหัวหน้าและผู้จัดการตามโครงสร้างภายในเป็นผู้รับผิดชอบ

กลยุทธ์ ข) ปลูกบัณฑิต

ต่อยอดจากการฝึกอบรมของโครงการฯ สำหรับบุคคลทั่วไป การเร่งสร้างหลักสูตรรองรับวิทยาการสาขาใหม่นี้เพื่อสร้างบัณฑิตในระดับต่าง ๆ ก็มีความจำเป็นยิ่ง โดยโครงการฯจะเริ่มจากการสร้างรายวิชา การฝึกกับสนาม (testbed) ที่มีอยู่ให้เป็นส่วนหนึ่งของหลักสูตรเดิม และพัฒนาหลักสูตรเฉพาะทางตามขั้นตอนปกติของมหาวิทยาลัยที่เข้าร่วมโครงการต่อไป รวมทั้งสร้างความร่วมมือเพื่อเชื่อมโยงข้ามหน่วยงานกับสถาบันการศึกษาและวิจัยที่เกี่ยวข้องอื่น ๆ เพื่อร่วมแบ่งปันทรัพยากร กำลังคน ฯ โดยหากโครงการได้เริ่มต้นขึ้น ควรผลิตนักศึกษาระดับบัณฑิตศึกษาที่มีความสามารถด้านวิทยาการรหัสลับเชิงควอนตัมได้ตั้งแต่ปีที่สองของโครงการเป็นต้นไป

6 “[illegible]” 2014 ISBN 9786163748300 หน้า 63)

ยุทธศาสตร์ที่ 3. วิทยาการ *"ร่วมเรียนรู้โลก"*

"เขาเหล่านั้นสร้างประเทศมาก่อนหน้าเราด้วยวิทยาศาสตร์มานานแล้ว
ประเทศไทยเพิ่งเข้ามาสู่ยุควิทยาศาสตร์ประมาณไม่ถึง 30 – 50 ปีมานี้ ...
อาจารย์สิปนนท์ เกตุทัต สมัยเรียนจบกลับมาควอนตัมยังไม่ได้สอนในเมืองไทยเลย เราตามหลังเขามาก*
ควอนตัมเกิดเมื่อปีค.ศ.1925 อาจารย์สิปนนท์กลับมาปีค.ศ. 1975 ห้าสิบปีผ่านไปแล้วควอนตัมก็ยังไม่ยังเมืองไทย"
(ศ.ดร.สุทัศน์ ยกส้าน)

** ศาสตราจารย์กิตติคุณ ดร. สิปนนท์ เกตุทัต อดีตนักเรียนทุน (คุรุสภา) ด้านฟิสิกส์และอดีตรัฐมนตรีว่าการกระทรวงศึกษาธิการและอุตสาหกรรม*

เนื่องจากประเทศไทยเป็นผู้ติดตามความก้าวหน้าทางด้านวิทยาศาสตร์และเทคโนโลยีทุกแขนง และมีระยะที่ห่างมาก และจากแนวทางและประวัติการสร้างวิทยาการของประเทศต่าง ๆ โดยเฉพาะกับด้านสาขาวิทยาการรหัสลับเชิงควอนตัมที่ได้ประเมินแนวทางไว้ (ดังภาคผนวก ข. 7) *ที่มากกว่าสามสิบปีเมื่อครั้งเริ่มต้นโครงการแรกในประเทศ* และได้ทิ้งระยะที่อาจไกลมากขึ้นจนประเมินถึงได้ยากแล้ว ซึ่งบทสรุปจากผลประเมินก่อนหน้านั้นทำให้ต้อง **เร่งศึกษาและรับการถ่ายทอดเทคโนโลยีทั้งมากและเร่งด่วนสองทิศทางคือ เพื่อทั้งลดระยะห่างหรือความล้าหลังและเพื่อเร่งติดตามความก้าวหน้าของโลกในอนาคต** ซึ่งข้อมูลทั้งหมดมาจากการที่โครงการนี้ได้ทำการสำรวจและติดต่อประสานหน่วยงานต่าง ๆ ตลอดระยะเวลากว่า 8 ปี[7] โดยมีกิจกรรมร่วมทั้งงานวิชาการ มาตรฐาน งานวิจัย การจัดสร้างอุปกรณ์ การจัดซื้อเครื่องมือ ฯ ดังบันทึกจดหมายเหตุ (milestones) ดังกล่าว และเมื่อนำมาศึกษาประมวลแล้ว จึงได้แนวทางที่โครงการจัดสร้างศูนย์กลางฯนี้พบว่าเหมาะสมกับสภาพปัจจุบันมากที่สุดที่จะได้นำมาปฏิบัติงานการถ่ายทอดวิทยาการจากต่างประเทศ

โดยปกติการถ่ายทอดเทคโนโลยีไม่มีรูปแบบวิธีการที่แน่นอน ขอบเขตของการถ่ายทอดเทคโนโลยีแต่ละโครงการอาจแตกต่างกันไป ขึ้นกับความรู้ความเข้าใจในเทคโนโลยี พื้นฐานอุตสาหกรรม และงบประมาณเงินทุนของผู้รับการถ่ายทอด ทั่วไปวิธีการถ่ายทอดเทคโนโลยี มี 3 วิธี[8] คือ

แนวทางที่ 1 *ถ่ายทอดอย่างเดียวโดยสมบูรณ์ ไม่มีการวิจัยและพัฒนา*
แนวทางที่ 2 *ถ่ายทอดเทคโนโลยี มีการวิจัยและพัฒนาภายหลังจากการได้รับการถ่ายทอดเทคโนโลยีแล้ว และได้รับสิทธิ์สามารถทำการผลิตและส่งออกหรือถ่ายทอดเทคโนโลยีต่อได้*
แนวทางที่ 3 *ถ่ายทอดโดยควบคู่ไปพร้อมกับการทำงานวิจัยและพัฒนา*

โดยวิทยาการที่เกี่ยวข้องด้านใหม่นี้ยังไม่มีผู้ผลิตรายใดมีความพร้อมโดยสมบูรณ์ ยังคงกำลังวิจัยและพัฒนาแนวทางแห่งอนาคตที่ต้องปรับปรุงในทุก ๆ ด้านอยู่เช่นกัน ดังนั้น แนวทางที่ประมวลไว้ ณ พ.ศ.2559 จึงควรเป็นดังนี้

กลยุทธ์ ก) สิงคโปร์-ไทย *(น้ำพึ่งเรือ-เสือพึ่งป่า)*

การพัฒนางานด้านนี้ของประเทศสิงคโปร์ (ภาคผนวก ข.3.4) ประสบผลสำเร็จอย่างต่อเนื่องมาโดยตลอดแม้จะขาดแคลนบุคลากรและวิทยาการสองปัจจัยหลัก หากแต่การมีนโยบายที่เข้มแข็งและกำลังงบประมาณที่เพียงพอสองปัจจัยหลัง จึงทำให้เกิดการเหนี่ยวนำผู้เชี่ยวชาญจากยุโรปมาประจำเต็มเวลา เกิดการชดเชยสองปัจจัยแรกที่ขาดนั้นได้เป็นอย่างดี

7 หนังสือ *"สารสนเทศเชิงควอนตัมประเทศไทย ๆ" 2014 ISBN 9786163748300*
8 http://www.matichon.co.th/news/28146

สำหรับสถานะภาพปัจจุบันจากการขยายงานและกิจกรรมกับการมีห้องปฏิบัติการขั้นสูงจำนวนมาก แต่ยังต้องการบุคลากรระดับนักศึกษาและผู้ร่วมงานอีกมากนั้น ประเทศไทยโดยศูนย์ความเป็นเลิศทางฟิสิกส์และภาควิชาฟิสิกส์ (มช.) จึงได้เริ่มความร่วมมือการแบ่งปันทรัพยากรงานกันแล้วโดยด้านสิงคโปร์เชิญชวนให้นักศึกษานักวิจัยไทยไปร่วมใช้งานห้องปฏิบัติการแทนการสร้างขึ้นเองใหม่ทั้งหมดซึ่งมีมูลค่าสูงมาก โดยจะได้พัฒนาสู่ความร่วมมือที่ก้าวหน้าขึ้นต่อ ๆ ไปด้วย ทั้งนี้ เป็นกิจกรรมสารสนเทศเชิงควอนตัมที่เน้นหนักด้านอุปกรณ์และการคำนวณ ส่วนด้านการสื่อสารหรือรหัสลับเชิงควอนตัมนั้นยังมิได้เริ่มต้น จึงเป็นโอกาสดีที่จะได้ปฏิบัติรูปแบบเดียวกันในลำดับต่อไป

ดังนั้น การสนับสนุนให้โครงการนี้มีโอกาสได้สร้างความร่วมมือกับเพื่อนบ้านอาเซียนที่มีความพร้อมเทียบเท่าหลายกลุ่มงานของประเทศในแถบหวีปยุโรปนั้น จะเป็นโอกาสที่ดีสอดรับกับการเปิดเขตเศรษฐกิจอาเซียนเมื่อปลายปีพ.ศ. 2558 ที่ผ่านมา โครงการนี้จึงได้วางแนวกลยุทธ์ "สิงคโปร์-ไทย" เพื่อพึ่งพาอาศัยกันในภูมิภาคโดยสัมพันธ์กับ**ยุทธศาสตร์ที่ 2** เรื่องการสร้างบุคลากร ซึ่งก็จะสามารถพัฒนาให้เป็นความร่วมมือจากระดับมหาวิทยาลัยสู่องค์กรที่เกี่ยวข้อง อาทิ กสทช. และกิจกรรมระหว่างประเทศต่อไปได้ในลักษณะเช่นเดียวกับเครือข่ายความร่วมมือเขตเศรษฐกิจยุโรปกับโครงข่ายรหัสลับควอนตัม SECOQC 2008 ที่เคยเป็นกิจกรรมที่ใหญ่ที่สุดของโลกมาก่อน ดังนั้น การแบ่งปันและร่วมถ่ายทอดเทคโนโลยีจากประเทศสิงคโปร์จึงเป็นแนวทางสำคัญประการหนึ่งทั้งยังเป็นประตูเปิดสู่โลกวิทยาการด้านนี้เชื่อมต่อกับประเทศในภูมิภาคอื่น ๆ ต่อไปที่หน่วยงานเหล่านั้นได้เริ่มต้นและสำเร็จผลร่วมกันมานานแล้วกับหน่วยงานของเกาะแห่งนี้

กลยุทธ์ ข) จีน-ไทย *(ที่น้องกัน)*

ความสัมพันธ์ไทยจีนมีมาช้านานในทุกด้านโดยเฉพาะในช่วงหลายปีที่ผ่านมา ทั้งด้านเศรษฐกิจ ภาษา หรือวิทยาศาสตร์และเทคโนโลยี รูปแบบความร่วมมือในลักษณะ**การขอรับความช่วยเหลือ (donation) ถ่ายทอดเทคโนโลยีและผู้เชี่ยวชาญร่วมกิจกรรม (technologies & experts transfer)** เกิดขึ้นกับหลากหลายโครงการและประสบความสำเร็จเป็นจำนวนมากในอดีต สำหรับด้านวิทยาการรหัสลับเชิงควอนตัมนั้น โครงการได้ประสานความร่วมมือมาแล้วตั้งแต่ปีพ.ศ.2556[9] ผ่านความร่วมมือระหว่างกระทรวงการต่างประเทศของไทยกับกระทรวงวิทยาศาสตร์ของประเทศจีน (SINO-Thai cooperation) กับหน่วยวิจัยขนาดใหญ่ที่สุดของประเทศจีนที่มหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยี (USTC) ซึ่งได้รับการตอบรับเป็นอย่างดีต่อแนวทางดังกล่าว

แต่ความร่วมมือต่าง ๆ ได้สะดุดลงจากทั้งเหตุการณ์อุทกภัยใหญ่ในประเทศปี พ.ศ.2554 และเหตุการณ์ทางการเมืองในกรุงเทพมหานคร ทำให้ระดับความร่วมมือลดลงไปอย่างมาก จึงควรได้รับการสนับสนุนให้เกิดการรื้อฟื้นความร่วมมือที่มีศักยภาพสูงเพื่อการถ่ายทอดวิทยาการสู่ระดับมวลวิกฤติได้เร็วแนวทางนี้กลับมาใหม่ ด้วยการสนับสนุนจาก กสทช. และที่เกี่ยวข้อง ทั้งด้านการเยี่ยมชม ดูงาน สัมนา การประชุมและถ่ายทอดในทุกระดับ รวมทั้งการแลกเปลี่ยนนักศึกษาและนักวิจัยเยี่ยมเยือนในรูปแบบโครงการระยะสั้นและต่อเนื่อง

ทั้งนี้ โครงการจะได้แสวงหากลไกอื่นจากแนวทางที่ได้พบเห็นความสำเร็จของกิจกรรมทางสังคมอื่นระหว่างสองประเทศมาประกอบด้วย เช่น ความร่วมมือหอการค้าและองค์กรการกุศลต่าง ๆ ฯลฯ เพื่อเชื่อมโยง**การขอรับความช่วยเหลือการถ่ายทอดเทคโนโลยีและผู้เชี่ยวชาญร่วมกิจกรรม** ให้ประสบผลอีกโครงการหนึ่งกับด้านวิทยาการรหัสลับเชิงควอนตัมต่อไปด้วย

9 หนังสือ *"สารสนเทศเชิงควอนตัมประเทศไทย ๆ" 2014 ISBN 9786163748300* **หน้า 39**

กลยุทธ์ ค) จัดซื้อ ถ่ายทอด ร่วมวิจัย

จาก**ยุทธศาสตร์ที่ 1.** เพื่อการจัดซื้อระบบเครื่องมือเพื่อการสร้างโหนดการสื่อสารเชิงควอนตัมดังที่กล่าวมาแล้ว โครงการฯ จะได้คัดสรรเทคโนโลยีที่เหมาะสมและเข้าร่วมกันเป็นสนามที่มีความหลากหลายได้ เช่น หนึ่งในผู้ผลิตหน้าใหม่ของโลก SK telecom หรือ สินค้าที่ได้รับการยอมรับทั่วโลกของบริษัท idQuantique และจากบริษัท QAsky ที่ต่อยอดงานวิจัยออกมาจากมหาวิทยาลัย USTC ที่ได้เริ่มมีความร่วมมือแล้ว เพื่อการร่วมโครงการ **"จัดซื้อ ถ่ายทอด ร่วมวิจัย"** อันจะเป็นอีกแนวทางหนึ่งที่ชัดเจนในลักษณะการจัดซื้อจัดหาระบบพื้นฐาน การถ่ายทอดเทคโนโลยีล่าสุดและการร่วมงานต่อยอดอย่างเป็นระบบ

ทั้งนี้ กลยุทธ์ที่คล้ายคลึงกันนี้จะสามารถปรับใช้กับผู้ผลิตรายอื่น ๆ ที่มีเทคโนโลยีแตกต่างกัน (ดังหัวข้อ **9.1** ตามลักษณะเฉพาะของแต่ละความต้องการ ไม่จำกัดเพียงประเทศสำคัญที่ได้นำเสนอนี้แต่อย่างใด

อนึ่ง เทคโนโลยีจากประเทศญี่ปุ่นที่ได้เข้าสู่ระยะการเตรียมการผลิตของภาคอุตสาหกรรมแล้วนั้น (semi-classified) โครงการ ฯ เคยได้มีความร่วมมือมาเป็นระยะเวลานานแล้วเช่นกัน แต่ยังขาดกลไกที่จะเชื่อมโยงนำมาสู่ระยะแรกของโครงการจัดสร้างศูนย์ฯ แห่งนี้ได้ โดยโครงการฯ จะพยายามมากขึ้นในลำดับต่อ ๆ ไป เช่นเดียวกันเทคโนโลยีจากประเทศรัสเซีย และอื่น ๆ อีกหลายแห่งมีศักยภาพและความก้าวหน้าสูงเช่นกัน ทั้งนี้ กลยุทธ์ ค) นี้ จะเริ่มต้นขึ้นได้ก็ด้วยการที่ยุทธศาสตร์ที่ 1 หรือการลงทุนสร้างโครงสร้างพื้นฐานที่มีมูลค่าสูงนั้นได้เริ่มไปพร้อมกันด้วยเท่านั้น

โดยสรุป ทั้งสามกลยุทธ์หลัก ก - ค) ข้างต้น จะทำให้เกิดการถ่ายทอดเทคโนโลยีที่สอดคล้อง เมื่อได้พิจารณาร่วมกับความพร้อมของประเทศทั้งด้านการลงทุนโครงสร้างพื้นฐานและการพัฒนาบุคลากรโดยสมบูรณ์ก่อน

ยุทธศาสตร์ 4. นโยบาย *"เป็นผู้ซื้ออย่างฉลาด"*

จากบทสรุปของ *"สารสนเทศเชิงควอนตัมประเทศไทย ๆ (2014)"* และภาคผนวก ข.6 โดยเฉพาะกิจกรรมวิจัยและพัฒนาด้านเทคโนโลยีโทรคมนาคมและสารสนเทศที่ต้องอาศัยสี่ปัจจัยหลัก (งบประมาณ บุคลากร วิทยาการ และนโยบายที่สอดคล้อง) เพื่อดำเนินการได้ครบทั้งเจ็ดส่วนสำคัญ (7 OSI layers) อีกจะทำให้ไปถึงเป้าหมายได้ แต่ในอดีต กิจกรรมต่าง ๆ ที่เกี่ยวข้องกับสาขาดังกล่าวนี้ กล่าวได้ว่าไม่ประสบความสำเร็จและเกิดความคาดหวังของเป้าหมายที่ต่างกันอย่างชัดเจน เช่น โครงการวิจัยระบบโทรคมนาคมสำหรับโทรศัพท์เคลื่อนที่ยุคที่ 3 และ UAV- ยานบินไร้คนบังคับ มีความคาดหวังในการไปถึงอุตสาหกรรมลดการนำเข้าหรือทดแทนได้ในระดับปลายน้ำ หว่าสามปัจจัยหลักนั้นล้าหลังมากแม้มีการอ้างอิงว่าได้รับงบประมาณสูงมาก (มากกว่า 20 และ 100 ล้านบาทตามลำดับ) แต่ทั้งหมดเป็นเพียงจุดเริ่มต้นที่ห่างไกลจุดมวลวิกฤติมาก เมื่อเทียบกับการนำงบประมาณส่วนที่เท่ากันไปลงทุนกับงานอื่นที่มีระดับเทคโนโลยี (OSI layer) น้อยและไม่ต่างกันนักและให้ผลเฉพาะทางได้ จึงกลายเป็นช่องว่างของผู้ปฏิบัติกับนโยบายที่อาจกล่าวได้ว่าเป็นปรากฏการณ์ "OSI effect" เพื่อใช้อธิบายความคาดหวังที่ต่างกันมากนั้น

ทั้งนี้ เมื่อกลับมาพิจารณาถึงโครงการศูนย์ฯ นี้แล้ว ปรากฏการณ์ "OSI effect" ดังกล่าวจะยิ่งชัดเจนมากกว่า เนื่องจากงานด้านวิศวกรรมโทรคมนาคมทั้งสองข้างต้นทั้งสังคมและนักวิชาการ หรือนักวิจัย มีความคุ้นเคยมากกว่าและมีประชากรที่ศึกษารวมทั้งทำงานอยู่ใกล้เคียงในสาขาเหล่านี้มากกว่า และใช้เวลาสั้นกว่ามาก เมื่อเทียบกับสารสนเทศเชิงควอนตัม ดังนั้น แนวทางที่เหมาะสมเมื่อพิจารณาร่วมกับปัจจัยสำคัญทั้งสี่แล้ว โครงการฯ จึงนำเสนอหนึ่งในสี่ทางเลือกทั่วไป *(ก) การเป็นผู้บริโภคเทคโนโลยีอย่างฉลาด ข) การเป็นผู้มีส่วนร่วมในการสร้างเทคโนโลยี ค) การพึ่งพาตนเองได้ ง) การเป็นเจ้าของวิทยาการเทคโนโลยีหรือทรัพย์สินทางปัญญา*) ที่ชัดเจนตั้งแต่ต้นสำหรับผู้สนับสนุน ผู้ใช้งาน (นักศึกษา นักวิจัย ภาคอุตสาหกรรม) และผู้กำกับนโยบายว่า ประเทศไทยกับเทคโนโลยีสารสนเทศเชิงควอนตัมด้านวิทยาการรหัสลับ ควรเลือกเส้นทางสำหรับเทคโนโลยีอนาคตด้านวิทยาการรหัสลับเชิงควอนตัมคือ **"การเป็นผู้บริโภคเทคโนโลยีอย่างฉลาด"** อย่างชัดเจน เพื่อมิให้เป็นการสูญเสียและผิดความคาดหวังเช่นโครงการต่าง ๆ ในอดีตเป็นเบื้องต้นก่อน

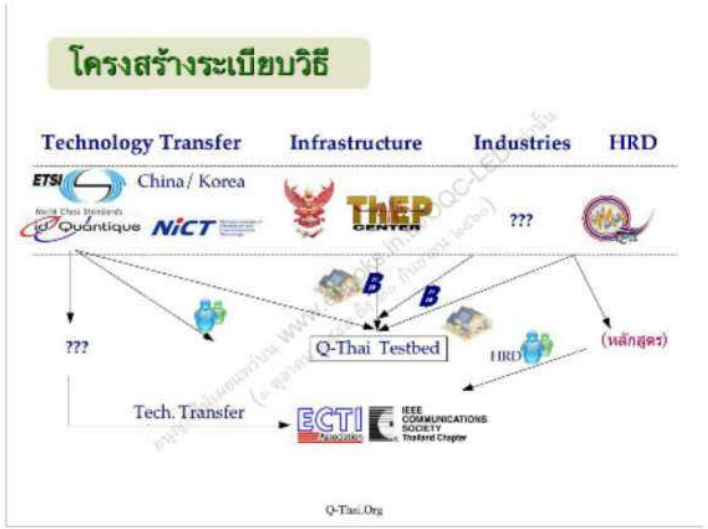
ดังนั้น ผลลัพธ์ระยะยาวในอนาคต ประเทศไทยควรจะไม่ตกอยู่ในสภาวะการซื้อวิทยาการใหม่หรือแปลกปลอมที่มีหลายมากอีก เช่น การจัดซื้อ GT200 บอลลูนตรวจการ เวชภัณฑ์ราคาแพงเกินจริงหรือแม้แต่ระบบโทรคมนาคมที่ไม่สามารถลดหรือทดแทนได้อย่างมีนัยสำคัญ และเกิดการสูญเสียสูงมากมาแล้วในอดีต เป็นต้น

อนึ่ง ยังมีประเด็นสำคัญอีกกรณีหนึ่งที่โครงการนี้อาจได้ช่วยลดปัญหาความเข้าใจคลาดเคลื่อนของสังคมต่อคำว่า "ควอนตัม" ในลักษณะเรื่องหลอกลวง (fraud) กับทั้งสินค้าและบริการที่นำชื่อควอนตัมไปใช้งาน แต่มิได้เกี่ยวข้องกับวิทยาการสมัยใหม่ของโครงการนี้แต่อย่างใด และที่สำคัญ ประเด็นของความคลาดเคลื่อนทางวิชาการในประเทศก็ปรากฏขึ้นมาด้วยแล้ว มีทั้งที่รู้เท่าไม่ถึงการและเข้าข่ายละเมิดจริยธรรมการศึกษา วิจัยและพัฒนา[10] และแม้วิทยาการด้านนี้จะมีลำดับความสำคัญ (priority) ต่อประเทศกำลังพัฒนาไม่สูงมากนัก และผลลัพธ์ของศูนย์ฯยังคงมีไม่มากพอที่จะได้สื่อสารออกสู่สังคมเทียมเท่าสาขาสำคัญอื่น ๆ แต่การเร่งพัฒนาเพื่อนอกจากวัตถุประสงค์ที่ได้แจ้งแล้วที่สังคมจะได้เตรียมพร้อมรับการเปลี่ยนแปลงในอนาคต ทั้งยังมีประโยชน์อื่นที่โครงการนี้จะได้การป้องกันหรือสร้างภูมิคุ้มกันให้กับสังคมฐานความรู้วิทยาศาสตร์ และส่งเสริมให้นักวิชาการที่ผิดแนวทางได้รับการตรวจสอบจากสังคม กระตุ้นให้กลับคืนสู่แนวทางเชิงสร้างสรรค์ต่อไปได้ด้วย

10 *www.dailynews.co.th/article/OQC_slash_LED "ควอนตัมไทยประดิษฐ์" หรือ Q-Thai.Oq สลิปน์ Q-Column*

9. วิธีดำเนินการพัฒนา

ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม มีพื้นฐานที่จะเกี่ยวโยงความร่วมมือระหว่างหน่วยงานวิจัยต่าง ๆ ทั้งภาครัฐและเอกชน ตลอดจนสถาบันการศึกษาภายในและต่างประเทศ เพื่อร่วมวิจัยและพัฒนาการสื่อสารโทรคมนาคมและเทคโนโลยีสารสนเทศ และควรได้ต่อยอดการพัฒนาไปสู่ภาคอุตสาหกรรมเมื่อมีโอกาสเป็นไปได้ โครงการฯจึงได้มีการจัดโครงสร้างระเบียบวิธีโดยเน้นหนักการจัดการในสามกลุ่มที่เกี่ยวข้องกัน ทั้งด้าน**การบริหารการถ่ายทอดเทคโนโลยี**จากต่างประเทศ **การบริหารโครงสร้างพื้นฐาน**ร่วมกับผู้สนับสนุนและหน่วยงานที่มีประสบการณ์ตรงเกี่ยวข้องกับวิทยาการพื้นฐาน รวมทั้ง**อุตสาหกรรมและการพัฒนาบุคลากร** ดังภาพรวมรูปที่ 9.1 โดยมีรายละเอียดภาคขยายดังต่อไปนี้



รูปที่ 1 โครงสร้างระเบียบวิธีการดำเนินงาน

9.1 เทคโนโลยี (Technology)

สืบเนื่องจากการวาง**ยุทธศาสตร์ที่ 3.** ด้านวิทยาการ เป็นที่ทราบแล้วว่าประเทศไทยมีระยะห่างการพัฒนาในสาขาพื้นฐานด้านที่เกี่ยวข้องมากกว่าสามสิบปี การพัฒนาโครงการนี้จึงต้องได้รับการถ่ายทอดเทคโนโลยีจากต่างประเทโดยเร่งด่วน ซึ่งในช่วงทศวรรษที่ผ่านมา กลุ่มความร่วมมือสารสนเทศเชิงควอนตัมไทย (Q-Thai.Org) (ภาคผนวก ค.) ได้พยายามสร้างแนวทางเพื่อก่อให้เกิดการถ่ายทอดเทคโนโลยีแลกเปลี่ยนความรู้ ประสบการณ์ บุคลากรจากเครือข่ายทั้งภายในและจากต่างประเทศนอกเหนือจากความพยายามสร้างบุคลากรจัดส่งนักเรียนทุนไปศึกษาในต่างประเทศ (**ยุทธศาสตร์ที่ 2.** สร้างบุคลากร) สำหรับหน่วยงานในต่างประเทศ โดยภาพรวมมีสถาบันที่สามารถสร้างความร่วมมือไว้แล้วและที่ยังคงประสานต่อเนื่องมาสู่โครงการนี้ได้ โดยมีโอกาสและศักยภาพแสดงดังตารางที่ 9.1

ตารางที่ 9.1 ความร่วมมือเพื่อการถ่ายทอดเทคโนโลยีจากต่างประเทศ

สถาบัน	ประเทศ	ความร่วมมือ	กิจกรรม/ผลงานที่ผ่านมา
European Telecommunications Standards Institute (ETSI)	กลุ่มสหภาพยุโรป	มาตรฐานระบบวิทยาการรหัสลับเชิงควอนตัม ข้อมูลความก้าวหน้าของโลก และ ETSI-QKD workshop	1. การร่วมบรรยายพิเศษ[11] 2. ที่ปรึกษาโครงการทุน กทปส. (กสทช.) 2558-2559 [12] 3. การแปลมาตรฐาน ETSI-QKD
ID Quantique (www.idquantique.com)	สวิตเซอร์แลนด์	การพัฒนาซอฟต์แวร์การกระจายกุญแจรหัสลับเชิงควอนตัม (QKD)	1. การสร้างต้นแบบโปรแกรมการกระจายกุญแจรหัสลับเชิงควอนตัม 2. จัดซื้อครุภัณฑ์เครื่องกำเนิดรหัสลับเชิงควอนตัมสองชุด[13]
Senetas Corporation Ltd (www.senetas.com)	ออสเตรเลีย	การพัฒนาอุปกรณ์เข้ารหัสลับ	1. ความร่วมมือด้านวิทยาการรหัสลับแบบเดิม (Classical) โครงการข้อมูลการแพทย์ 2. จัดซื้ออุปกรณ์
USTC: University of Science and Technology of China, Hefei	จีน	1. SINO-Thai cooperation 2. การเตรียมการถ่ายทอดเทคโนโลยี	1. เยี่ยมชม ดูงาน[14] 2. ผลงานวิจัยร่วม[15]
National Institute of Information and Communications Technology	ญี่ปุ่น	การเตรียมการถ่ายทอดเทคโนโลยีสารสนเทศเชิงควอนตัม	1. เยี่ยมชม ดูงาน[16] 2. ความร่วมมือเดิม (MOU) ระหว่าง NICT กับหน่วยงานของกระทรวงวิทยาศาสตร์และเทคโนโลยี
SK telecom	เกาหลีใต้	เตรียมการจัดซื้อ ถ่ายทอดเทคโนโลยี และร่วมวิจัย	เยี่ยมชม ดูงาน[17]

11 https://goo.gl/1XKd8s
12 http://bbp.nbtc.go.th/announcement/detail/959
13 https://goo.gl/25bi8
14 http://www.dailynews.co.th/article/292043 และ https://goo.gl/QRlW6
15 http://cpb.iphy.ac.cn/EN/Y2014/V23/I8/090310
16 http://www.dailynews.co.th/article/288626
17 http://www.dailynews.co.th/article/353827 และ http://www.dailynews.co.th/article/355248

9.2 โครงสร้างพื้นฐาน (Infrastructure)

พื้นฐานชั้นต่ำสุดของโครงสร้างเครือข่ายวิทยาการรหัสลับเชิงควอนตัมประกอบด้วยโหนดเชิงควอนตัม (Quantum Key Distribution Node : QKD Node) จำนวนสามโหนด (*หากต่ำกว่าสามจะไม่จัดเป็นเครือข่ายสื่อสารหากจะเป็นเพียงการสื่อสารเฉพาะกิจจุดต่อจุด point-to-point*) โดยมีเส้นทางการเชื่อมต่อเชิงควอนตัม (Quantum Key Distribution Link: QKD Link) จำนวนสามเส้นทาง โดยเครือข่ายเป็นลักษณะของการรวมเส้นทางการเชื่อมต่อแบบจุดต่อจุดนั้นเข้าด้วยกัน (ring network) เพื่อกระจายกุญแจรหัสลับเชิงควอนตัมระหว่างโหนด ซึ่งทั้งสามโหนดนี้สามารถขยายต่อในอนาคตได้โดยอิตหยุ่นเพื่อเพิ่มเติมเป็นโครงข่ายใกล้เคียงสภาพจริงได้ (mesh network)

และจาก**ยุทธศาสตร์ที่ 3** ด้านวิทยาการ ที่จะสามารถนำมาจัดสร้างเป็นเครือข่ายของศูนย์ฯได้ดัง**รูปที่** 10.1 แบบขยายสะดวกในอนาคต (LEGO-QKD network strategy) นั้น มีต้นแบบและแหล่งเทคโนโลยีรวมถึงข้อจำกัดที่ได้สำรวจไว้จากประเทศผู้นำด้านรหัสลับควอนตัมของโลกปัจจุบัน คือ

ก) **SECOQC** เทคโนโลยียุโรปรวมจากหลายประเทศแต่สลายตัวไปแล้ว เป็นแนวทาง testbed แรกของโลก
ข) ประเทศญี่ปุ่น กับโอกาสความร่วมมือกับบริษัท **NICT** เจ้าภาพหลักและเครือข่ายวิจัยที่เกี่ยวข้อง
ค) เกาหลีใต้ มีโอกาสความร่วมมือกับบริษัทเกิดใหม่ **SK telecom** ที่ต้องการขยายฐานลูกค้า
ง) สวิตเซอร์แลนด์ สินค้าโดยบริษัท **IDQuantique** เป็นเทคโนโลยีปิด ถ่ายทอดเทคโนโลยีเพียงบางส่วน
จ) **USTC** ประเทศจีน มีเทคโนโลยีหลากหลายแต่มีเงื่อนไขด้านความมั่นคงกำกับ ไม่สามารถเผยแพร่ได้มาก

การพัฒนาสามโหนดพื้นฐานด้วยการจัดหาเทคโนโลยี จึงได้ออกแบบการรองรับเทคโนโลยีที่เหมาะสมกับโครงการนี้ (ณ พ.ศ.2559) ไว้ดังนี้

โหนด 1. ระบบของบริษัทชั้นนำ (SK telecom และ IDQuantique)

แนวทางสมบูรณ์แบบของการเป็นศูนย์กลาง (Testbed) ที่จะจัดหา ถ่ายทอดเทคโนโลยี และร่วมวิจัย เกิดการเรียนรู้ได้มาก แต่อิงเป็นเทคโนโลยีที่ใหม่มากและอาจต้องพึ่งพาแนวทางนี้ต่อเนื่องระยะยาวในการขยายผลสู่ระยะในอนาคต

โหนด 2. ระบบ CV-QKD จากประเทศญี่ปุ่นหรือยุโรป

แนวทางเทคโนโลยีการเข้าและถอดรหัสที่มีความเสถียรและความเร็วสูงที่สุด เหมาะสมกับการประยุกต์ในโครงข่ายสำหรับใช้งานจริงมากที่สุด แต่การถ่ายทอดเทคโนโลยีจะมีข้อจำกัดเพราะเป็นเทคโนโลยีปิดมากับสินค้าของบริษัทผู้ผลิต หากจะได้รับประโยชน์มากขึ้นจะต้องทำวิศวกรรมย้อนกลับ (reverse engineering) กับเครื่องมือเหล่านั้นเอง เพื่อสามารถที่จะเรียนรู้เทคโนโลยีภายในและทำตามแบบอย่างได้ แต่พึงมีความเสี่ยงจากมูลค่าที่สูงและอาจต้องเสียสภาพของเครื่องมือนั้นไป (**หมายเหตุ**: *SK telecom เคยใช้วิธีการนี้จนประสบผลสำเร็จสร้างตันแบบของตนเองได้*)

โหนด 3. ระบบ Entanglement จากยุโรปหรือประเทศจีน

แนวทางหลักนี้เพื่อพึ่งพาตนเองได้มากในอนาคตและเพื่อสามารถใช้เป็นชุดศึกษาและการสื่อสารวิทยาศาสตร์สู่สังคมที่สั่นเกตผลเรื่อง **"ควอนตัมคืออะไร ?"** ได้ชัดเจนที่สุด จะทำให้เกิดการพัฒนาต่อยอดได้สะดวกที่สุดอีกทั้งเป็นเทคโนโลยีเปิดยังไม่มีมาตรฐานกำกับจึงมีโอกาสพัฒนาต่อได้หลากหลาย แม้การประยุกต์ใช้งานในโครงข่ายจะมีศักยภาพต่ำกว่าแนวทางของสองโหนดก่อนหน้า แต่เป็นแนวทางเลือก (trade off) เพื่อการสร้างพื้นฐานความรู้สู่สังคมได้ดี รวมทั้งเป็นส่วนสร้างความพร้อมของผู้ปฏิบัติสู่ความร่วมมือเชิงเทคนิคกับต่างประเทศได้ เช่น สิงคโปร์ ฯ

ทั้งนี้ ในอนาคตคุณลักษณะเฉพาะของทุกโหนดสามารถขยาย ปรับเปลี่ยนหรือขยายแนวทางของโหนดได้เพื่อให้เหมาะสมกับปัจจัยเกี่ยวข้องอื่น ๆ ทั้งเทคโนโลยีที่เปลี่ยนไป ราคาต้นทุน การเกิดแนวทางเลือกใหม่อื่น ๆ เช่น ตัวอย่างโหนดที่ 1 อาจปรับใช้กับทั้งสามโหนดเพื่อที่จะเป็นการจัดหาและส่งมอบแบบสมบูรณ์ (turn key) ด้วยเทคโนโลยีของ SK telecom หรือ IDQuantique เพียงแบบเดียวได้เพื่อความสะดวก หรืออาจจะปรับทั้งหมดเป็นโหนดใช้งานดูแลความปลอดภัยเครือข่ายโดยสมบูรณ์ด้วยรูปแบบโหนดที่ 2 เพียงอย่างเดียว แต่เพื่อการศึกษาวิจัยอาจไม่เหมาะหรือสะดวก เป็นต้น (**หมายเหตุ** : *อุปกรณ์โหนดดังกล่าวทั้งหมดยังมิใช่อุปกรณ์สำเร็จรูป plug & play ดังเช่นเครื่องใช้ไฟฟ้าทั่วไป ต้องใช้ความรู้ ทักษะเฉพาะทางในการประกอบระบบ ใช้งาน รักษาและซ่อมบำรุง ยังคงเป็นอุปกรณ์ต้นแบบกึ่งวิจัย*)

นอกจากนั้น ยังมีส่วนเสริมสู่การเป็นโครงสร้างพื้นฐานประกอบโหนดเหล่านี้อีกคือ ช่ายสายของเส้นใยนำแสง (optical fiber) อุปกรณ์ระบบเครือข่ายสื่อสารและคอมพิวเตอร์ (router, switching, etc) และอุปกรณ์อิเล็กทรอนิกส์อันเป็นเทคโนโลยีทั่วไป สามารถจัดหาและทดแทนได้จากภายในประเทศ ไม่ซับซ้อนเทียบเท่ากับกรณีของอุปกรณ์เชิงควอนตัม (QKD-Node)

9.3 บุคลากรและอุตสาหกรรม (HRD / Industry)

การบริหารเครือข่ายบุคลากรทั้งในและต่างประเทศ รวมทั้งกับภาคอุตสาหกรรมนั้น ข้อเสนอโครงการนี้มีความเชื่อมโยงกับสิ่งที่ได้ปฏิบัติมาแล้วระยะหนึ่งในอดีตก่อนหน้า จนถึงปัจจุบันและมีแนวทางต่อไปในอนาคตดังนี้

9.3 ก) ความเชื่อมโยงของกลุ่มวิจัยด้านเทคโนโลยีสารสนเทศควอนตัมไทย

กลุ่มวิจัยเทคโนโลยีสารสนเทศควอนตัมไทย *(ภาคผนวก ค.)* (Thai Quantum Information Forum : Q-Thai Forum)		
ลำดับ	**มหาวิทยาลัย ที่ทำการวิจัย**	**โครงการ**
1	มหาวิทยาลัย นเรศวร (วิศวฯ)	การสื่อสารปลอดภัยสูงสุดด้วยรหัสลับควอนตัม:การถ่ายทอดเทคโนโลยีและพัฒนาบุคลากร
2	มหาวิทยาลัย เชียงใหม่ (ฟิสิกส์)	(ร่าง) การพัฒนาชุดทดลองสำหรับวิจัยและฝึกอบรมเทคโนโลยีด้านการสื่อสารเชิงแสงและควอนตัม

ด้วยข้อมูลจากหัวข้อ **ยุทธศาสตร์ที่ 2** เรื่องการสร้างบุคลากร จำนวนผู้เกี่ยวข้องในประเทศมีน้อยมากในสาขาสารสนเทศเชิงควอนตัมที่มีสาขาและงานแขนงย่อยออกไปตามความถนัด (เช่น แสง อะตอม โมเลกุล ฯ) จึงได้มีความพยายามรวมกลุ่มเพื่อสร้างเสริมความเข้มแข็ง แบ่งปันข้อมูลและทรัพยากร และจะพยายามขยายทั้งเพิ่มจำนวนและปรับจูนแนวทางร่วมกันต่อ ๆ ไป ทั้งนี้ จะพยายามต่อความเชื่อมโยงบุคลากรที่มีอยู่ไปยังต่างประเทศด้วย เช่น สิงคโปร์ ดังยุทธศาสตร์การพัฒนาบุคลการและการถ่ายทอดเทคโนโลยีดังที่ได้กล่าวมาก่อนหน้าแล้ว รวมถึง***กลุ่มนักเรียนนักศึกษาไอทีควอนตัมไทยในต่างประเทศ*** ทั้งที่ได้รับการสนับสนุนทุนการศึกษาจากหน่วยงานภาครัฐ เช่น โครงการ พสวท. ทุนกระทรวงวิทยาศาสตร์และเทคโนโลยี หรือทุนส่วนตัว เป็นต้น ซึ่งได้มีกิจกรรมร่วมกันก่อนหน้ามาพอสมควรแล้วรวมไปถึง **สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.)** ด้วยเช่นกัน[18]

18 *www.facebook.com/QuantumCryptoThailand/notes และ https://goo.gl/3nYxCF*

9.3 ข) ความเชื่อมโยงกลุ่มวิชาชีพที่เกี่ยวข้อง

การสนับสนุนให้คำปรึกษาเชิงเทคนิค (technical support) ของหน่วยงานที่เกี่ยวข้องแนวทางใกล้เคียงกันจะเสมือนการมีพี่เลี้ยง (mentor) ที่ไม่มีส่วนได้ส่วนเสียโดยตรง (stakeholder) ให้คำแนะนำ และจากมุมมองของกลุ่มคนหลากหลายรุ่นที่จะมีโอกาสได้รับทราบรายละเอียดของโครงการสู่การมีส่วนร่วมกิจกรรมเชิงสาธารณะ ไม่แสวงกำไรและมิใช่ธุรกิจ อาจได้มาซึ่งข้อแนะนำการปรับปรุงหรือขัดเกลาข้อเสนอ การดำเนินงาน การประเมินความเสี่ยง ฯ ให้ดีขึ้นได้อีก โครงการการจัดสร้างศูนย์กลางฯ นี้ เปิดกว้างสาธารณะให้ทุกภาคส่วนได้รับประโยชน์ อันสอดคล้องกับบทบาทของกลุ่มวิชาชีพที่ได้เกิดการรวมตัวกันมาก่อนหน้านานแล้ว ดังนั้น จึงจะได้เริ่มต้นโครงการฯ ให้สอดคล้องสนองแนวทางการพัฒนาวิชาชีพเหล่านั้นไปพร้อมกันด้วยเช่นกัน โดยกลุ่มวิชาชีพและองค์กรที่เกี่ยวข้องดังกล่าวในประเทศที่จะมีความเชื่อมโยงด้วย คือ

- **IEEE Comsoc Thailand กับความเชื่อมโยงในระดับสากล**

ชมรมไฟฟ้าสื่อสาร เป็นกลุ่มสาขาวิชาชีพหนึ่งของสมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ หรือที่คุ้นเคยกับคำเรียกทั่วไปคือ *ไอทริปเปิลอีคอมซอก* (IEEE Communication Society) โดยเป็นเครือข่ายความร่วมมือของบุคลากรวิชาชีพ วิศวกร นักวิจัยและนักศึกษาสาขาการสื่อสารโทรคมนาคมหรือที่เกี่ยวข้องจากทั่วโลก มีสมาชิกชมรมไฟฟ้าสื่อสารทั่วทุกภูมิภาคของโลกรวมมากกว่า 45,000 คน จากสมาชิกทั้งหมดของสมาคมไอทริปเปิลอีทุกชมรมรวมกันกว่า 350,000 คนทั่วโลก อันเป็นสมาคมวิชาชีพด้านเทคนิคที่ใหญ่ที่สุดของโลกด้วย สำหรับสาขาประเทศไทย (Thailand section) นั้น *คอมซอก* (Thailand chapter) มีสมาชิกซึ่งประกอบด้วยคนไทยเป็นส่วนใหญ่ร่วมกับชาวต่างชาติที่ประกอบวิชาชีพด้านนี้ในระดับสองร้อยคน จากจำนวนสมาชิกสมาคมทุกสาขากว่าสี่ร้อยคนที่ลงทะเบียนมีถิ่นพำนักอยู่ในประเทศไทย

บทบาทที่ชมรมไฟฟ้าสื่อสารและสมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์แห่งประเทศไทยได้ดำเนินการคือ ให้การสนับสนุนทางด้านวิชาชีพ ร่วมกับภาคการศึกษาและการวิจัยจัดการสัมมนาและการประชุมวิชาการขึ้นอย่างต่อเนื่อง นอกเหนือจากนี้ยังได้มีการจัดกิจกรรมต่าง ๆ ที่ช่วยส่งเสริมความรู้ด้านทางวิศวกรรมไฟฟ้าสื่อสารด้วย โดยกิจกรรมสำคัญมีทั้ง การจัดทำสื่อหรือหนังสือและการเชื่อมโยงผู้เชี่ยวชาญด้านวิศวกรรมสื่อสารสาขาต่าง ๆ ทั่วโลกด้วย ซึ่งสาขาใหม่ด้านการสื่อสารเชิงควอนตัมก็สามารถได้รับประโยชน์จากกลไกที่มีอยู่แล้วของสมาคมนั้นได้ เป็นช่องทางหนึ่งในการเชื่อมโยงโครงการนี้สู่ทั้งบุคลากร วิทยาการ มาตรฐานและโอกาสต่าง ๆ ในระดับสากลได้ด้วย

- **ECTI Association เครือข่ายความร่วมมือภายในประเทศ** (www.ecti.or.th)

สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์โทรคมนาคม และเทคโนโลยีสารสนเทศ (Electrical Engineering/Electronics,Computer, Telecommunications and Information Technology Association:ECTI) เกิดขึ้นจากการรวมตัวเพื่อจัดกิจกรรมวิชาการของคณาจารย์ นักวิชาการ นักวิจัยในสาขาไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและเทคโนโลยีสารสนเทศ อันเนื่องมาจากพบว่าประเทศไทยควรมีสมาคมวิชาการด้าน วิศวกรรมไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและเทคโนโลยีสารสนเทศ ที่จะร่วมเป็นแกนนำสำคัญในการพัฒนาวิชาการในสาขาดังกล่าวของประเทศให้แข็งแกร่งและมีศักยภาพในระดับสากล ในลักษณะคล้ายกับบทบาทหน้าที่ของสถาบันไอทริเปิลอี (The Institute of Electrical and Electronics Engineers:IEEE) ก่อตั้งขึ้น ณ ประเทศสหรัฐอเมริกา สถาบันไออีไอซีอี (The Institute of Electronics, Infomation and Communication Engineers: IEICE) ก่อตั้งขึ้นโดยประเทศญี่ปุ่น และสถาบันไออีอีเค (The Institute of Electronics Engineers of Korea: IEEK) ของประเทศเกาหลีใต้ รวมไปถึงสถาบันไอดับเบิลอี (Institute of Electrical Engineers: IEE) ก่อตั้งขึ้นที่ประเทศสหราชอาณาจักร ซึ่งต่อมาเปลี่ยนชื่อเป็นสถาบันไออีที (The

Institution of Engineering and Technology:IET) ดังนั้น คณาอาจารย์ นักวิชาการ นักวิจัยในสาขาดังกล่าว จึงรวมตัวกันก่อตั้งและจดทะเบียนขึ้นเป็นสมาคมในปีพ.ศ.2545 มีวัตถุประสงค์คือ เพื่อส่งเสริม สนับสนุน ให้คำปรึกษา เผยแพร่ความรู้ พัฒนามาตรฐานด้านวิชาการในสาขาวิศวกรรมไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคมและเทคโนโลยีสารสนเทศ ของประเทศไทย จัดประชุมวิชาการระดับประเทศ และระดับนานาชาติจัดอบรมวิชาการบรรยายต่าง ๆ โดย ผู้เชี่ยวชาญ เผยแพร่นิตยสาร วารสารวิชาการและแลกเปลี่ยนประสบการณ์ และความรู้ด้านเทคนิคในสาขาวิชาของสมาคม รวมถึงการประสานงานกับสมาคมและสถาบันต่าง ๆ ทั้งในประเทศและต่างประเทศเพื่อขยายพันธมิตรสร้างความร่วมมือทางวิชาการ จึงเป็นอีกหนึ่งช่องทางหนึ่งที่โครงการนี้จะได้แสวงหาความเชื่อมโยงเพื่อตอบวัตถุประสงค์ดังยุทธศาสตร์ที่เกี่ยวข้องที่แจ้งแล้วเช่นกัน

- **Thailand Excellence Center in Physics (TheP) ศูนย์ความเป็นเลิศด้านฟิสิกส์**

จากแนวทางของศูนย์ ThEP (thep-center.org) ศูนย์การวิจัย และศึกษาด้านฟิสิกส์ในระดับสูง (advanced study) เพื่อสร้างผลงานที่มีประสิทธิภาพและมาตรฐานในระดับสากล อันจะเป็นอีกปัจจัยหนึ่งที่ช่วยส่งเสริมให้วงการวิชาการไทยมีส่วนร่วม อย่างมีศักดิ์ศรีในเวทีโลก และสะท้อนกลับเป็นการพัฒนาการศึกษาวิทยาศาสตร์และการพัฒนาเทคโนโลยีของชาติ แบบพึ่งพาตนเองได้ซึ่งเป็นการเติบโตที่ยั่งยืน อีกทั้งมีวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่โครงการนี้สามารถร่วมตอบสนองได้โดยตรง และที่ผ่านมาโครงการได้เข้าร่วมกิจกรรมและเตรียมความพร้อมกับ**โครงการจัดตั้งห้องปฏิบัติการวิจัย**ตามแนวทางของศูนย์ TheP แล้ว ซึ่งจะได้พัฒนาความร่วมมือให้ก้าวหน้ายิ่งขึ้นต่อไป

ดังนั้น การบริหารโครงสร้างพื้นฐานนี้โดยเชื่อมโยงกับหน่วยงานที่มีประสบการณ์ตรงเกี่ยวข้องกับวิทยาการพื้นฐานสาขาด้านฟิสิกส์นั้น จะทำให้สามารถเพิ่มความเข้มแข็งและลดความเสี่ยงลงได้เพื่อเกิดประโยชน์สูงสุดต่อสังคม

9.3 ค) ความเชื่อมโยงอุตสาหกรรม

จาก**ยุทธศาสตร์ที่ 3** ด้านวิทยาการที่ประเมินให้ทราบได้ว่าประเทศไทยล้าหลังกว่าวิทยาการของโลกด้านรหัสลับเชิงควอนตัมนี้มาก พื้นฐานไม่เพียงพอต่อการเป็นผู้ผลิตได้ในเวลาที่ยากต่อการคาดการ ดังนั้น แนวทางของ**ยุทธศาสตร์ 4** ด้านนโยบายที่ตั้งไว้เพื่อให้เกิดการพัฒนาสู่ขั้นแรกในการเป็น "เป็นผู้ซื้ออย่างฉลาด" ได้นั้น จึงเป็นกรอบการปฏิบัติที่จะได้ลดช่องว่างของผู้ปฏิบัติกับความคาดหวัง (ปรากฏการณ์ "OSI effect") ของผู้ให้การสนับสนุนหรือจากฟากนโยบายหรือผู้บริหารแนวทางวิทยาศาสตร์และเทคโนโลยีของประเทศและเมื่อพิจารณาโดยเฉพาะกับความเชื่อมโยงสู่ภาคอุตสาหกรรมไทยแล้วนั้น จึงมีระยะห่างจากวิทยาการสาขาใหม่อย่างที่ประเมินมิได้

ถึงกระนั้น โครงการนี้จะพยายามเชิญชวนภาคเอกชนและอุตสาหกรรมที่เกี่ยวข้องเพื่อเข้าร่วมกับโครงการในมิติอื่น ๆ โดยในอดีตเคยได้เริ่มความร่วมมือไม่เป็นทางการด้วยการบรรยาย เชิญเยี่ยมชมจากหลายหน่วยงานด้านความมั่นคงและผู้ให้บริการระบบสื่อสารโทรคมนาคม (service provider) ซึ่งทุกหน่วยงานทั้งหมดเหล่านั้นมีความต้องการเพียงความช่วยเหลือด้วยระบบที่พร้อมทุกส่วนเพื่อภารกิจหลักของหน่วยงานเท่านั้น ส่วนวิทยาการรหัสลับเชิงควอนตัมที่ยังคงอยู่ในช่วงเริ่ม (technology trigger) ยังคงต้องใช้ความรู้และทักษะเฉพาะทางในการทำงานดังรายละเอียดของหัวข้อโครงสร้างพื้นฐานดังที่แจ้ง จึงอาจยังไม่เหมาะกับช่วงเวลานี้ที่อุตสาหกรรมที่เกี่ยวข้องจะเข้าร่วมในลักษณะ**ผู้ใช้งาน** และถึงแม้ช่วงเวลาดำเนินการของโครงการนี้จะยังไม่สามารถทำให้เกิดความเชื่อมโยงเชิงวิจัยและพัฒนากับภาคอุตสาหกรรมได้ แต่การเข้าร่วมเชิง**การสร้างบุคลากรรองรับอนาคต การร่วมติดตามเทคโนโลยีและคาดการณ์ รวมทั้งการสร้างภาพลักษณ์องค์กร (CSR)** ด้วย จะยังคงมีความสำคัญยิ่งและมีโอกาสสูงกว่า

ทั้งนี้ โครงการฯ จะอาศัยช่องทางที่เหมาะสมเพื่อพยายามเชื่อมโยงกับอุตสาหกรรมโทรคมนาคมในประเทศจากเครือข่ายที่มีอยู่ และจากข้อแนะนำจากที่ปรึกษาและฝ่ายต่าง ๆ ที่จะตามมาเพิ่มในอนาคตอีกด้วยทางหนึ่ง

10. ผลลัพธ์ระยะที่ 1

โดยโครงการศูนย์กลางฯจะแบ่งออกเป็น 2 ระยะ คือ ระยะแรก (ปีที่ 1-ปีที่ 3) และระยะที่สอง (ปีที่ 4 - ปีที่ 5) ซึ่งภายใต้โครงการระยะแรกจะมีการสร้างศูนย์กลางฝึกอบรมและถ่ายทอดความรู้และจัดตั้งโครงข่ายระบบวิทยาการรหัสลับเชิงควอนตัม สำหรับระยะที่สองจะเป็นการประเมินผลและต่อยอดโครงการให้มีความแข็งแรงและเป็นที่รู้จักระดับชาติและในเวทีโลกมากขึ้นรวมทั้งการขยายโครงข่ายต่อเนื่อง ดังนั้น ระยะที่ 1 จะมีผลลัพธ์ดังนี้

ปีที่ 1 พัฒนาสร้างศูนย์ทดสอบ วิจัยพัฒนา ฝึกอบรมและถ่ายทอดเทคโนโลยีวิทยาการรหัสลับเชิงควอนตัม
ปีที่ 2 การสร้างโครงข่ายทดสอบระบบวิทยาการรหัสลับเชิงควอนตัม
ปีที่ 3 การจัดทำโครงข่ายระบบวิทยาการรหัสลับเชิงควอนตัมระหว่างหน่วยงาน

11. ประโยชน์ที่คาดว่าจะได้รับ

11.1 มีศูนย์กลางเผยแพร่ความรู้ทั้งหลักการและการปฏิบัติครบวงจรด้านการสื่อสารเชิงแสงและวิทยาการรหัสลับเชิงควอนตัมแห่งแรกของประเทศไทย ที่พัฒนาเป็นเครือข่ายความรู้เฉพาะด้านในระยะยาวได้รวมทั้งสามารถดึงดูดนักศึกษาที่สนใจในระดับปริญญาโทและปริญญาเอกเข้ามาร่วมทีมวิจัย เพื่อให้เกิดการพัฒนาบุคลากรที่มีคุณภาพสูงขึ้น

11.2 เกิดความตระหนักของสังคมต่อวิทยาการแขนงใหม่และกระตุ้นให้เกิดการเตรียมพร้อมในทุกด้านกับทั้งนักศึกษา นักวิจัยจากสถาบันการศึกษา หน่วยงานทั้งภาครัฐและเอกชน

11.3 ความสามารถบุคลากรของกลุ่มวิจัยเทคโนโลยีสารสนเทศควอนตัมไทยจากสถาบันต่าง ๆ ได้รับการพัฒนาต่อเนื่อง

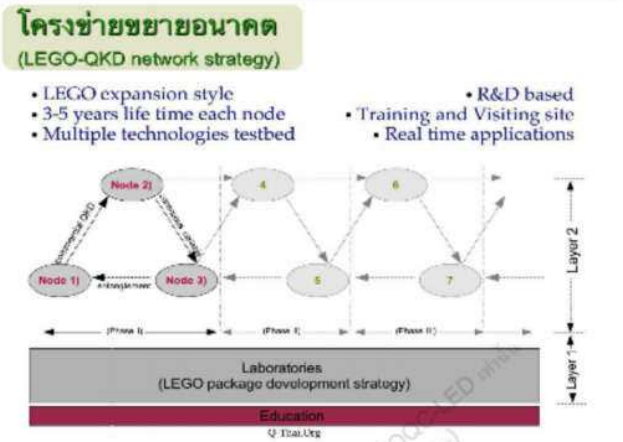
11.4 มีความพร้อมเพื่อพัฒนาให้เกิดเป็นหลักสูตรการเรียนการสอน การฝึกอบรมวิทยาการและเทคโนโลยีรหัสลับ การสื่อสารเชิงแสง ควอนตัมฟิสิกส์ และอื่น ๆ อันเป็นรากฐานสำคัญที่ยั่งหาตนเองได้ในอนาคต

11.5 ได้แนวทางการศึกษา วิจัย และพัฒนาเทคโนโลยีวิทยาการรหัสลับเชิงควอนตัมสำหรับการรักษาความปลอดภัยของข้อมูลที่เหมาะสมสำหรับประเทศไทยในลำดับต่อ ๆ ไป

11.6 เกิดแนวทางการส่งเสริมและสนับสนุนการวิจัยและพัฒนาอุตสาหกรรมการสื่อสารโทรคมนาคมและเทคโนโลยีสารสนเทศที่เกี่ยวข้องได้ชัดเจนขึ้น รวมทั้งแนวทางการติดตามและถ่ายทอดความก้าวหน้าจากต่างประเทศได้

11.7 สังคมได้รับความรู้ความเข้าใจและเกิดทัศนคติที่ดีต่อเทคโนโลยีเชิงควอนตัมที่จะเข้ามาเปลี่ยนแปลงโลกในอนาคตและสามารถร่วมกระจายผลถ่ายทอดความรู้ในวงกว้างต่อได้

11.8 เกิดความร่วมมือของสถาบันวิจัย อุตสาหกรรมโทรคมนาคม และผู้ใช้งานในอนาคต ที่ยั่งหาตนเองในประเทศได้มากขึ้น



รูปที่ 2 ขอบเขตโครงการด้วยโครงข่ายแบบขยายได้ในอนาคต
(LEGO-QKD network strategy) ตามกำลัง ทรัพยากรและประสบการณ์

รูปที่ 3 การดำเนินงานโครงการสามปี ระยะที่ 1

12. แผนการดำเนินโครงการและแนวทางผลงาน

รวมสรุปผลงานในโครงการระยะแรกดังตารางนี้คือ

ผลงานที่ได้รับ (รวม)	ปีที่1	ปีที่2	ปีที่3
โครงสร้างพื้นฐาน (4)	1 หน่วย (Lab)	1 โหนด (QKD node)	2 โหนด (QKD node)
โครงการวิจัย (2)		1 โครงการใหม่	1 โครงการใหม่
บุคลากร ปริญญาโท (จบการศึกษา 3) ปริญญาเอก (ศึกษา 2)	-	ปริญญาโท 1 คน	ปริญญาโท 2 คน ปริญญาเอก 2 คน
ต้นแบบ	-	-	ต้นแบบโครงข่าย ทดสอบใช้งาน
ร่วมจัดการประชุมวิชาการระดับประเทศ (1)	-	1 ครั้ง	-
ร่วมจัดการประชุมวิชาการระดับนานาชาติ (1)	-		1 ครั้ง
สัมมนาฝึกอบรมย่อย (7)/ ฝึกอบรมใหญ่ (3)	2/ 1 ครั้ง	2/ 1 ครั้ง	3/ 1 ครั้ง
หน่วยงานที่เข้าร่วมโครงการ (3)		1 หน่วยงาน	2 หน่วยงาน

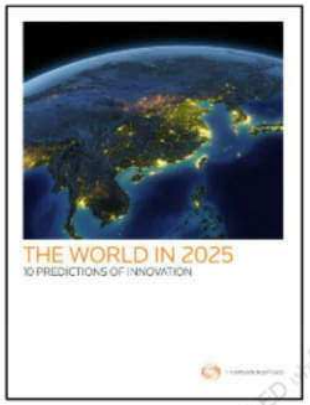
ภาคผนวก

ภาคผนวก ก)

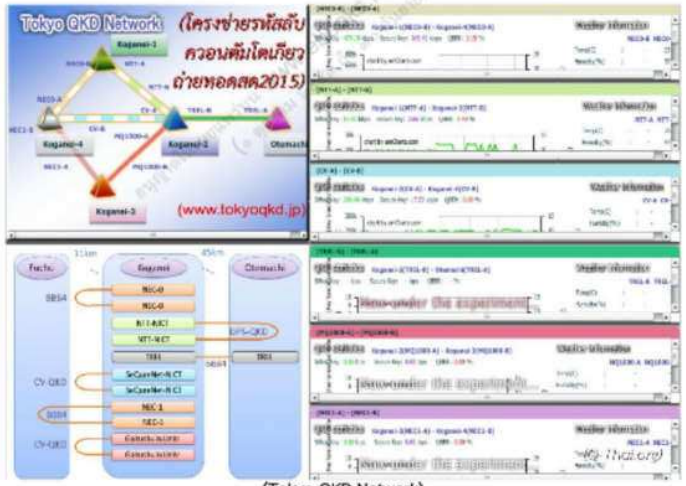
การวิเคราะห์สถานภาพปัจจุบัน จุดแข็ง จุดอ่อน อุปสรรค และโอกาส (SWOT)

องค์ประกอบหลัก/ตัวแปร	จุดแข็ง	จุดอ่อน
ปัจจัยด้านโครงสร้างพื้นฐาน	1. ประสบการณ์ในอดีตนำมาสู่แนวทางใหม่ (LEGO-QKD model) ที่มีโอกาสความสำเร็จที่สูงขึ้น	1. วิทยาการพื้นฐานสาขาใหม่ที่ต้องอาศัยทรัพยากรสูงมากขึ้นวิกฤต 2. ยังขาดโครงสร้างหลักที่ใช้ในการงานวิจัยและพัฒนาอีกมาก ราคาแพงและเปลี่ยนแปลงไว
ปัจจัยด้านบุคลากร	1. บุคลากรที่มีอยู่มีความพร้อมด้านทัศนศาสตร์เชิงควอนตัม โทรคมนาคม และด้านการประมวลผลสัญญาณที่เกี่ยวข้อง 2. บุคลากรมีความมุ่งมั่นต่อความสำคัญในการวิจัยและพัฒนาด้านวิทยาการรหัสลับเชิงควอนตัม 3. บุคลากรมีประสบการณ์ด้านใกล้เคียง (quantum dot, cryptography, optical communication) > 5-10 ปี	1. รวมบุคลากรหลักมีจำนวนน้อยมาก 2. ขาดแคลนบุคลากรสนับสนุน (นักศึกษา นักวิจัย และอื่น ๆ) 3. งานด้านไอทีที่ต้องการความร่วมมือของบุคลากรที่มีความถนัดหลากหลายระดับ (OSI 7 layers)
ปัจจัยด้านเครือข่ายวิจัย	1. เครือข่ายความร่วมมือด้านสารสนเทศเชิงควอนตัม มีประสบการณ์การรวมกลุ่มก่อนหน้ามาระยะหนึ่งแล้ว ทั้งภายในประเทศ (กลุ่มวิจัยเทคโนโลยีสารสนเทศควอนตัมไทย (Quantum Information Forum: Q-Thai forum)) และกับต่างประเทศ มีความพร้อมพอสมควร	1. ความร่วมมือกับต่างประเทศเพื่อถ่ายทอดเทคโนโลยีและแลกเปลี่ยนความรู้และบุคลากร ยังต้องการกลไกสนับสนุนอื่น ๆ อีกมาก

องค์ประกอบหลัก/ตัวแปร	โอกาส	อุปสรรค
ปัจจัยด้านนโยบายและการพัฒนาวิทยาการรหัสลับเชิงควอนตัม	1. ความก้าวหน้าของโลกยังอยู่ในช่วงเริ่มต้น ส่งผลให้เทคโนโลยียังพัฒนาไม่ถึงจุดอิ่มตัว ดังนั้นจึงเป็นโอกาสที่จะพัฒนาศักยภาพเทคโนโลยีรหัสลับเชิงควอนตัมในประเทศให้สูงขึ้นเพื่อลดการพึ่งพาเทคโนโลยีจากต่างประเทศได้ 2. เทคโนโลยีรหัสลับเชิงควอนตัมได้รับการคาดการณ์ (forecast) ด้านศักยภาพในอนาคตจากองค์กรสำคัญระดับนานาชาติ จึงเป็นที่สนใจของระดับนโยบายของหลายประเทศที่จะส่งผลถึงประเทศไทย	1.การลงทุนพัฒนาเทคโนโลยีสารสนเทศเชิงควอนตัมใช้งบประมาณสูงและเห็นผลลัพธ์ในอนาคตที่ใช้เวลานานและมีความเสี่ยงสูงกว่ามากด้วยเมื่อเทียบกับภารกิจด้านอื่น เช่น การแพทย์ การเกษตร ฯ จึงยังไม่มีนโยบายที่เกี่ยวข้องใด ๆ ในประเทศไทย (พ.ศ.2558) ให้การสนับสนุน 2. ภาคนโยบายสารสนเทศหรือไอทีในประเทศยังมิได้เริ่มต้นเป็นทางการกับวิทยาการใหม่นี้ จึงขาดกลไกรองรับในทุกระดับงานจากภาครัฐ
ปัจจัยด้านงบประมาณ	1. เทคโนโลยีรหัสลับเชิงควอนตัมสามารถนำมาประยุกต์ใช้ในการการสื่อสารปลอดภัยในอนาคตได้ มีโอกาสสร้างรายได้สูงมากรวมทั้งลดการสูญเสีย เพิ่มความมั่นคงด้านการสื่อสารข้อมูลโดยมิสามารถประเมินค่าได้	1.การเปลี่ยนแปลงเทคโนโลยีอย่างรวดเร็ว การลงทุนสูงจึงมีความเสี่ยง 2. การพัฒนายังอยู่ในระดับต้นน้ำต้องการความต่อเนื่องระยะยาวที่ต้องมีการลงทุนด้านบุคลากรและโครงสร้างพื้นฐานด้วยงบประมาณสูงต่อเนื่องและใช้เวลานาน



(The World In 2025: 10 Predictions of Innovation)



(Tokyo QKD Network)

ภาคผนวก ข)

หลักการและเหตุผลของศูนย์ฯ (ภาคขยาย)

จากกรอบแนวคิดพื้นฐาน (หลักการและเหตุผล) ที่เน้นหนักการสร้างศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed) ของช่วงระยะเวลาของโครงการ 3 ปี (ระยะที่ 1) โครงการ ฯ ได้ร่างขึ้นจากการสำรวจและวิเคราะห์ละเอียดโดยศึกษานำมาจากหลายส่วน ทั้งด้านการคาดการณ์โลกอนาคต การศึกษาสนามทดสอบไอทีควอนตัมจากทั่วโลกรวมถึงการเยี่ยมชมดูงาน พร้อมการเทียบเคียงกับเทคโนโลยีแขนงอื่น ๆ ที่ได้รับการคาดหมายว่าจะมีผลกระทบต่อโลกขององค์กรสำคัญต่าง ๆ กระทั่ง ได้หยิบยกแนวทางและนโยบายที่เกี่ยวข้องกับวิทยาการรหัสลับเชิงควอนตัมจากทั่วโลก ทั้งพัฒนาการที่เกี่ยวข้องของทวีปยุโรปมีการลงทุนมูลค่าที่สูงมาก การเร่งพัฒนาและประสบผลตามแนวทางของประเทศจีน มาจนถึงประเทศใกล้เคียงในแถบอาเซียนของสิงคโปร์มาพิจารณา จากการสำรวจล่าสุดพบว่าประเทศที่อาศัยปัจจัยเสี่ยงหรือคุกคามที่ได้นำมาสร้างเป็นแรงผลักดันสู่การพัฒนาสร้างขึ้นได้ในเวลาที่รวดเร็ว ก็เป็นอีกแนวทางหนึ่งที่เกิดขึ้นกับประเทศเกาหลีใต้และรัสเซีย ซึ่งทั้งหมดได้นำมาประมวลเข้าด้วยกันแล้ว

โดยที่ขนานไปกับการสำรวจดังกล่าว การรวบรวมสถานะภาพที่เกี่ยวข้องในประเทศกับงานด้านสารสนเทศหรือไอทีเดิมนั้นมีปัจจัยพัฒนาที่สำคัญโดยบ้างที่พึงได้รับการนำเสนอ และประสบการณ์จากแนวทางเดิมที่ได้พัฒนามาสู่การเป็นศูนย์ทดสอบฝึกอบรมและถ่ายทอดฯ ของประเทศของข้อเสนอนี้ควรนำมาปฏิบัติต่อเช่นใดต่อไป แนวทางอนาคตที่เหมาะสมสำหรับการพัฒนาบุคลากรและการสร้างสนามทดสอบหรือ testbed ที่กล่าวถึงมาแล้วนั้น นำเสนอดังข้อมูลภาคขยายของหลักการและเหตุผลต่อไปนี้

ข.1 โลกอนาคตค.ศ. 2025: สนามทดสอบไอทีควอนตัมทั่วโลก

ข้อมูลด้านที่เกี่ยวข้องกับสนามทดสอบหรือ Testbed ของโลกเริ่มด้วยข้อมูลการพยากรณ์ระดับโลก โดยที่เมื่อ *"วันที่ 30 มิถุนายน ปีค.ศ.2014 บริษัท Thomson Reuters โดยแผนก IP & Science Business ได้เปิดเผยรายงานการสำรวจทศวรรษอนาคตเรื่อง "สิบอันดับการคาดการณ์นวัตกรรม" (The World In 2025: 10 Predictions of Innovation)*[19] *ด้วยการวิเคราะห์ข้อมูลจากบทความวิจัยวิชาการและเอกสารสิทธิบัตร เพื่อสรุปแนวโน้มที่จะมีการค้นพบที่ยิ่งใหญ่ที่สุดในทศวรรษหน้า โดยใช้หลักการวิเคราะห์ citation ranking/ most cited papers ของบทความตีพิมพ์งานวิจัยด้านวิทยาศาสตร์จากฐานข้อมูล Web of Science/ Thomson Innovation/ Thomson Reuters Incites และวิเคราะห์ด้วยเอกสารสิทธิบัตรจากฐานข้อมูลสิทธิบัตร Derwent World Potent Index ที่มีการยื่นขอจดจากปีค.ศ.2012 เป็นต้นมาพบว่า งานที่เกี่ยวข้องกับสารสนเทศเชิงควอนตัมจะเป็นหนึ่งในสิบหัวข้อดังกล่าวในอีก 10 ปีข้างหน้าโดยให้รายละเอียด คือ "Teleportation Is tested" หรือการมีสนามทดสอบการส่งถ่ายเชิงควอนตัม"*[20] ซึ่งเป็นแนวทางที่กระตุ้นให้เห็นแนวโน้มของโลกเทคโนโลยีที่ไม่สามารถปฏิเสธได้ และในระยะเวลาอีกไม่นาน (พ.ศ.2568)

สำหรับพัฒนาการที่**เด่นชัดที่สุด**ด้านการสร้างสนามจริงมีใช้งานในโลก เป็นการดำเนินงาน โดยสำนักงานเทคโนโลยีสารสนเทศและการสื่อสารแห่งประเทศญี่ปุ่น (NICT) ตั้งแต่ตัวอย่างแรกที่ร่วมกับบริษัทเอกชนและหน่วยงานที่เกี่ยวข้องจัดตั้งโครงการวิจัยระบบวิทยาการรหัสลับเชิงควอนตัมระยะยี่สิบปี (พ.ศ.2544 - 2563) เพื่อพัฒนาและสร้างระบบเครือข่ายความปลอดภัยระดับสูงด้วยเทคโนโลยีควอนตัมทั้งแบบไฟดอนเดี่ยว เชิงหัวพัน รวมทั้งการ กระจายรหัสลับผ่านดาวเทียม โดยตั้งแต่ปี พ.ศ.2548 มาแล้วนั้น NICT ได้ร่วมกับบริษัท เอ็นอีซี (NEC) ทดสอบ และสาธิต

19 *sciencewatch.com/tags/2025*

20 *การส่งถ่ายเชิงควอนตัม (quantum teleport) คือวิธีการหนึ่งที่สามารถประยุกต์ใช้กับวิทยาการรหัสลับเชิงควอนตัมได้*

เครือข่ายระบบที่ทำระยะทางได้ 16 กิโลเมตรผ่านเส้นใยนำแสงมีระยะยาวนานที่สุด 2 สัปดาห์ (ก่อนหน้าที่ฟากยุโรปจะทำข้ามปี (โดยบริษัท IDQ) และในปีพ.ศ.2549 ได้ทดสอบการรับ – ส่งแสงจากดาวเทียมวงโคจรต่ำ (Low Earth Orbit : LEO) มายังภาคพื้นดินเพื่อเตรียมการสำหรับการกระจายกุญแจรหัสลับผ่านฟ้าในอนาคต ซึ่งเป็นความก้าวหน้ามากที่สุดโดยรวมของช่วงเวลานั้น ขณะที่ทั้งสหรัฐอเมริกาและสหภาพยุโรปมีแผนการก่อนหน้าแต่กลับยังไม่มีผลเช่นของประเทศญี่ปุ่น

ต่อมา NICT พร้อมสำนักงานส่งเสริมเทคโนโลยีสารสนเทศ (IPA) และสถาบันพัฒนาวิทยาศาสตร์และเทคโนโลยีอุตสาหกรรม (AIST) ร่วมกับบริษัทเอกชน สาธิตระบบวิทยาการรหัสลับเชิงควอนตัมที่ประกอบด้วย 6 โหนด 6 เส้นทาง ในวันที่ 18 - 20 ตุลาคม พ.ศ. 2553 ณ กรุงโตเกียว (งาน UQCC 2010) ซึ่งเป็นการสาธิตสดครั้งที่สองของโลก (ต่อจากงาน SECOQC 2008 แบบเป็นทีมของสหภาพยุโรป) โดยในงาน UQCC 2010 นั้น ได้มีการนำเสนอข้อมูลเน้นย้ำที่ประเทศญี่ปุ่นให้ความสำคัญกับเทคโนโลยีสารสนเทศเป็นอย่างมาก เนื่องจากภาคส่วนนี้มีขนาดโตเป็น 10% ของ GDP (ผลิตภัณฑ์มวลรวม) ของประเทศเทียบเท่าอุตสาหกรรมยานยนต์ที่ยิ่งใหญ่ ส่วนการจ้างงานในอุตสาหกรรมไอซีที (ICT) มีถึง 1.78 ล้านตำแหน่ง มากกว่ายานยนต์ซึ่งมีอยู่ที่ 1.71 ล้านตำแหน่งในปีพ.ศ.2553 (ค.ศ.2010) และสารสนเทศเชิงควอนตัมก็คือส่วนหนึ่งของอนาคตอุตสาหกรรมไอซีทีที่ว่านั้น โดยพื้นฐานแล้วประเทศญี่ปุ่นจัดได้ว่ามีความก้าวหน้าทางเทคโนโลยีสูงในทุกด้าน รวมถึงมีความพร้อมและความเข้มแข็งของหน่วยงานวิจัยภาคธุรกิจและบุคลากรจำนวนมากในประเทศเอง จึงมีพัฒนาการคล้ายกับกลุ่มจานของสหภาพยุโรปที่ร่วมกันทำกิจกรรมด้านนี้จากหลากหลายประเทศ แต่ที่ประเทศญี่ปุ่นสามารถจัดทำเองได้ทั้งหมด **มีบุคลากรและวิทยาการพร้อม**นานมาแล้ว

NICT เป็นหน่วยงานหลักของประเทศได้จัดทำแผนที่นำทางเทคโนโลยีสารสนเทศเชิงควอนตัมขึ้นด้วย ภายใต้กรอบระยะยาวซึ่งนานมากถึง **40 ปี (ปีค.ศ.2000-2040)** และได้จัดตั้งห้องปฏิบัติการเพื่อวิจัยเทคโนโลยีสารสนเทศเชิงควอนตัมขึ้น โดยภาพรวมของแผนที่นำทาง การประยุกต์และการขับดันกิจกรรมที่ NICT นำเสนอนั้น มีความท้าทายสูงมากจากการลงทุนทั้งงบประมาณและบุคลากรที่มากเช่นกัน จึงเป็นที่จับตามองของทั่วโลก

อนึ่ง NICT เคยมีข้อตกลงความร่วมมือกับหน่วยงานในประเทศไทยมาเป็นระยะเวลานานมากเริ่มตั้งแต่งานร่วมด้านการแปลภาษาในยุคเริ่มแรกของอินเทอร์เน็ต ส่วนงานด้านวิทยาการรหัสลับเชิงควอนตัมนั้นมีการหารือความร่วมมือกันหลายครั้งจนกระทั่ง NICT เข้าสู่ระยะที่สอง "semi-classified" แล้ว โดยจะเหลือเฉพาะกลุ่มงานภายในของประเทศญี่ปุ่นกันเองเท่านั้น จึงเป็นการยุติความร่วมมือกันไปโดยปริยาย (เตรียมสู่การทำจำหน่ายสร้างรายได้)

ในช่วงทศวรรษแรกของแผนที่นำทางนั้น NICT ให้ความสำคัญกับการพัฒนาการกระจายกุญแจรหัสลับ (QKD) และเทคโนโลยีพื้นฐานที่เกี่ยวข้อง โดยได้สนับสนุนการวิจัยและพัฒนาต่อภาคเอกชนและองค์กรสาธารณะ เช่น บริษัทมิตซูบิชิและเอ็นอีซี (NEC) มหาวิทยาลัยโตเกียว สถาบันวัสดุศาสตร์แห่งชาติ สถาบันสารสนเทศแห่งชาติ มหาวิทยาลัยนิปปอนและอีกหลายหน่วยงานและมีผลงานมากขึ้นอย่างต่อเนื่องเป็นรูปแบบเฉพาะ โดยจ่ายทรัพยากรจากส่วนกลางสู่หน่วยย่อย ๆ เพื่อร่วมงานกันแล้วนำกลับมารวมเป็นผลภาพใหญ่

หากพิจารณาด้วยสี่ปัจจัยประเมินแนวทางอนาคตคือ **1. วิทยาการ 2. คน 3. ทรัพยากรหรืองบประมาณ 4. นโยบาย** แล้วประเทศญี่ปุ่นมีครบทั้ง **"นโยบายนำกับแผนถึงสี่สิบปี งบประมาณพร้อม บุคลากรและวิทยาการมีสั่งสมและสร้างเองได้หมดแล้ว"** กระทั่งมีข่าวใหญ่ที่สนามทดสอบรหัสลับเชิงควอนตัมโตเกียว (Tokyo Testbed)[21] ซึ่งผ่านการพัฒนาต่อมาอีกห้าปี ก้าวหน้าจนเปิดเครือข่ายรหัสลับควอนตัมแบบเวลาจริง (real time) ได้แล้ว โดยเฝ้าสังเกตข้อมูลและพัฒนาการผ่านเวปเพียงหน้าเดียวได้ตลอดเวลา

21 www.toshiyoga.jp

อีกหนึ่งตัวอย่างที่ได้รับการกล่าวถึงมากช่วงเวลาปีพ.ศ.2558 เป็นต้นมา นั่นคือสนามทดสอบใหม่ล่าสุดของประเทศเกาหลีใต้ ที่เกิดจากแรงผลักดันของการต่อสู้กับการรุกรานทางเครือข่ายออนไลน์ของประเทศเพื่อนบ้าน โดยกลุ่มเอกชนรายใหญ่ด้านสื่อสารโทรคมนาคม SK telecom[22] ได้ติดตั้งระบบกระจายกุญแจรหัสลับควอนตัม (QKD) ในสามสนามหลักคือ

1. National test bed (live network): ณ เมืองแดจอง (Daejeon) ระยะทาง 11 กิโลเมตร
2. National test bed : ระหว่างเมือง Bundang กับ Yongin (ระยะทางรวม 50 กิโลเมตร: 25 กม. loop back)
3. SKT commercial network : เพื่อการทดสอบร่วมระบบไวไฟ (WiFi backbone network) ระหว่างเมือง Bundang กับ Sungsu (SKT Switching Center) ระยะทาง 34 กิโลเมตร

โดยล่าสุด (มีนาคม พ.ศ. 2559) ทำระยะทางรวมไปแล้วถึง 256 กิโลเมตร และเกิดรูปแบบการทำงานประสานกับหน่วยงานอื่น ๆ ทั้งธนาคารและฝ่ายความมั่นคง ทั้งนี้ที่สำคัญ กระทรวงวิทยาศาสตร์รวมทั้งกระทรวงไอซีที ให้การสนับสนุนต่อโครงการสร้างและใช้สนาม (testbed) เหล่านี้ จึงเป็นตัวอย่างที่สำคัญที่เป็นการรวมกลุ่ม (consortium) ของทุกภาคส่วนที่ควรได้รับการติดตามเป็นอย่างยิ่งเนื่องจากใช้เวลาเพียง**สองปี**เท่านั้นกับความก้าวหน้านี้

อนึ่ง สำหรับสนามทดสอบแห่งอื่น ๆ ของโลกก่อนหน้านี้ทั้งที่สหรัฐฯ หรือยุโรป (SECOQC 2008) ซึ่งได้เคยได้เริ่มต้นขึ้น แต่ได้แปลงรูปไปในแนวทางอื่น ๆ แล้ว ไม่เด่นชัดเท่าของฟากเอเชียตะวันออก (ญี่ปุ่น จีนและเกาหลีใต้)

ข.2 เทคโนโลยีเปลี่ยนโลกค.ศ. 2022 (IEEE Computer Society)

เนื่องจากการทำนายอนาคตจะช่วยให้นักวิจัยได้สำรวจทราบว่าเทคโนโลยีกำลังจะย้ายผลกระทบไปในทิศทางใด สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) โดยชมรมคอมพิวเตอร์ (computer society) ส่วนกลางที่สหรัฐอเมริกา จึงได้เป็นเจ้าภาพร่วมกับบุคลากรจากทั้งเฟสบุ๊ก กูเกิล ห้องปฏิบัติการซิวเลตต์-แพคการ์ด และไมโครซอฟท์ รวมกับนักวิชาการของมหาวิทยาลัยเทคโนจอร์เจียและเพนน์เสตต ค้นคว้าสู่การทำนายเทคโนโลยีพื้นหรือฐานรากวิทยาการคอมพิวเตอร์และอุตสาหกรรมที่เกี่ยวข้องที่หากมีการขยับพัฒนาไปแล้ว จะเกิดผลเปลี่ยนแปลงวงการใหญ่ได้

โดยระบุเทคโนโลยีที่ขับดันโลกไปต่อในอีกไม่กี่ปีหรือค.ศ. 2022 (พ.ศ. 2565) ซึ่งสำรวจมาจากวิธีวิจัยครอบคลุมความเห็นจากสมาชิกหลายพันคน เปิดรับคำวิจารณ์กลับไปใช้ มีกรรมการบอร์ดใหญ่พิจารณาซึ่งอ้างอิงได้ได้ผลระบุออกมากับ 23 ตัวตั้ง[23] มีผลสำรวจกลับมาด้วยที่ก็คล้ายกันโดย *ความยั่งยืนของพลังงาน ความพร้อมของระบบสื่อสารไร้สายและบรอดแบนด์ รวมไปถึงกระบวนการทางการแพทย์* สูงเป็นสามอันดับแรกของปัจจัยขับ (drivers) ขณะที่ตัวเปลี่ยนโลกเทคโนโลยี (disruptors) สามเรื่องแรกได้แก่ *การพิมพ์สามมิติ แรงงานหุ่นยนต์และไอที การคำนวณแบบคลาวด์ (cloud)* ที่ผลบ่งมาว่าแรงที่สุด

22 http://goo.gl/q7JoTr

23 รายงานฉบับเต็ม (IEEE CS 2022 Report) www.computer.org/cms/Computer.org/ComputingNow/2022Report.pdf

โดยมีหัวข้อเกี่ยวข้องอยู่สามเรื่องที่สัมพันธ์กับโครงการนี้ โดยสองเรื่องแรกเกี่ยวข้องกับ *การคำนวณเชิงควอนตัม (quantum computing) และการเรียนรู้ของเครื่องและระบบชาญฉลาด (Machine Learning and Intelligent Systems)* ทั้งนี้ ในปีพ.ศ. 2558 โลกได้เรียนรู้แล้วว่าระบบดังกล่าวพัฒนาไปมาก กูเกิล ไมโครซอฟท์ ไอบีเอ็ม ฯ มีข่าวการสร้างระบบนี้ที่อาศัยการคำนวณความเร็วสูงและรองรับข้อมูลปริมาณมหาศาลสู่การเป็นสมองเทียมที่คิด คาดการณ์ ตัดสินใจได้เร็วขึ้นเรื่อย ๆ ซึ่งจะทำให้เกิดการคุกคามต่อความปลอดภัยของการสื่อสารข้อมูลหรือรหัสลับต่าง ๆ ด้วย โดยเฉพาะหาก "ควอนตัมคอมพิวเตอร์" มีความพร้อมสำหรับใช้งานแล้วเมื่อใดรหัสลับที่ใช้งานทั่วไปอาจตกอยู่ภาวะเสี่ยงสูง จึงเป็นแรงขับที่ทำให้วิทยาการรหัสลับเชิงควอนตัมที่สมบูรณ์แบบดังกล่าวนั้นได้รับการเร่งพัฒนาอยู่ทั่วโลกในขณะนี้

สำหรับเรื่องที่สาม *เทคโนโลยีเกี่ยวกับแสง (Photonics)* อันเนื่องมาจากยุคของการใช้แสงเพื่อกิจกรรมไอทีใกล้เข้ามามาก ทั้งนี้ด้วยศักยภาพที่ทั้งเร็ว แรง ช่องสัญญาณกว้างขวาง เริ่มตั้งแต่ชิปอุปกรณ์แสงที่มาร่วมงานกับอิเล็กทรอนิกส์ การเชื่อมต่อสัญญาณทางแสง เครือข่ายโทรคมฯแสง ชุมสายเชิงแสง (switching) ฯ เป็นต้น การที่เรื่องเทคโนโลยีของแสงมีความสำคัญสูงขึ้น เนื่องจากกิจกรรมที่ใช้อิเล็กตรอนหรืออุปกรณ์อิเล็กทรอนิกส์ที่มีใช้งานอยู่ทั่วไปนั้นมีโอกาสการพัฒนาไปถึงขอบเขตสิ้นสุดในอนาคตอันใกล้ทางตามกฎของมัวร์ (Moore's law[24]) ซึ่งก็จะทำให้โลกก้าวเข้าสู่ยุคของ "ไอทีควอนตัม" หรือควอนตัมแสง (quantum optics) ด้วยต่อไปนั่นเอง

(การพัฒนาต้องอาศัยคำพยากรณ์เพื่อลดความเสี่ยงและวางแผนการลงทุน)

24 *กฎของมัวร์ (Gordon E. Moore) ผู้ร่วมก่อตั้งบริษัทอินเทล ระบุเมื่อ ค.ศ. 1965 ว่าเทคโนโลยีไมโครอิเล็กทรอนิกส์จะสามารถบรรจุส่วนประกอบเล็ก ๆ ได้เป็นสองเท่าขณะที่ใช้พื้นที่เท่าเดิมและราคาจะลดเหลือครึ่งของมูลค่าเดิมในทุกช่วงเวลา 18 เดือน อุปกรณ์เครื่องใช้จะเล็กและถูกลงตามไปด้วย ... จาก "ไมโคร" หนึ่งในล้านส่วนไปสู่หนึ่งในพันล้านส่วนของระดับ "นาโน" จึงกำลังเข้าสู่ย่านวิทยาการควอนตัมต่อไป*

ข.3 แนวทางและนโยบายทั่วโลก 2015

หากอนาคตของการพัฒนาไอทีควอนตัมสามารถบ่งชี้ด้วยสี่ปัจจัยหลักจาก **1) วิทยาการพื้นฐาน 2) บุคลากร 3) งบประมาณ และ 4) นโยบายการสนับสนุนที่สอดคล้อง** ซึ่งอาจทำให้คาดการณ์ได้ว่าประเทศไทยควรจะเลือกเดินทางไปต่อแบบไหนได้ชัดเจนขึ้น ดังนั้น เมื่อพิจารณาด้วยปัจจัยทั้งสี่นี้แล้วนำไปศึกษากรณีตัวอย่างของต่างประเทศที่ประสบผลสำเร็จ จะทำให้ทราบถึงแนวทางที่ประเทศไทยจะได้นำมาปรับใช้ต่อไปได้ *(ทั้งนี้แนวทางของประเทศสหรัฐอเมริกามีความพร้อมโดยสมบูรณ์ทุกปัจจัยแตกต่างจากแหล่งอื่น ๆ เป็นปกติดังได้เสนอไว้โดยละเอียดแล้ว)*[25]

ข.3.1) พัฒนาการของยุโรป

จากการสำรวจเดิมของสหภาพยุโรปอันเป็นภาคพื้นต้นกำเนิดวิทยาการของโลกแขนงต่าง ๆ มากมาย ซึ่งได้ให้ความสำคัญกับงานวิจัยสารสนเทศและการสื่อสารเชิงควอนตัม (QIPC) เป็นอย่างสูงโดยอยู่ภายใต้ขอบเขตแกนหลักชื่อ"เทคโนโลยีสารสนเทศและการสื่อสาร (ICT)" มายาวนาน ซึ่ง QIPC เป็นสาขาวิจัยที่รวมทั้งการคำนวณและรหัสลับเชิงควอนตัม และเป็นเทคโนโลยีแห่งอนาคต โดยจัดเป็นโครงการริเริ่มภายใต้เทคโนโลยีอุบัติใหม่แห่งอนาคต (Future Emerging Technology: FET) โดยคณะกรรมาธิการยุโรป (EC) ให้การยอมรับศักยภาพและสนับสนุนการวิจัยและกิจกรรมต่าง ๆ ตั้งแต่เริ่มต้นการวิจัยพื้นฐานไปจนกระทั่งการวิจัยประยุกต์ หรือครบเครื่องเรื่อง**"นโยบายไอซีที"**

และกิจกรรมที่ยุโรปมีพัฒนาการมาอย่างยาวนานทยอยมีผลมาหลายทศวรรษแล้ว นับตั้งแต่ช่วงปลายทศวรรษที่ค.ศ. 1 9 8 0 มาจนถึงทศวรรษที่ค.ศ. 1 9 9 0 สหภาพยุโรปได้จัดสรรทุนสำหรับงานวิจัยเชิงควอนตัมโดยมีจุดมุ่งหมายเพื่อให้เกิดเครื่องมือหรืออุปกรณ์ใหม่ ๆ โดยในช่วงกรอบโครงการที่ 4 (Framework Program หรือ FP4: ค.ศ.1995-1998) ได้วางรากฐานสำหรับขอบเขตการวิจัยวิทยาศาสตร์และเทคโนโลยีของ QIPC ดังกล่าว จึงได้กลายเป็นกรอบเทคโนโลยีสารสนเทศเชิงควอนตัมที่ชัดเจนของยุโรปเองได้ในที่สุดจากกว่าสามทศวรรษนานมาแล้ว

ต่อมาถึงช่วงที่ 5 หรือ FP5 (ค.ศ.1999-2002) มีการสนับสนุนงานด้านเทคโนโลยีสารสนเทศเชิงควอนตัมจำนวน 25 โครงการ ไต่เพดานรวมไปถึง 41 ล้านยูโร ตามด้วยการสนับสนุนช่วงที่ 6 หรือ FP6 (2003-2006) มีสามโครงการบูรณาการที่ประสบความสำเร็จและได้รับทุนจากสหภาพยุโรปรวมไม่น้อยกว่า 25 ล้านยูโร และกำเนิดศูนย์ประสานงานด้านเทคโนโลยีควอนตัมขึ้นด้วยคือ"QUROPE" ซึ่งมีสมาชิกร่วมกันจาก 35 สถาบัน เกิดบริษัทใหม่ (spinoff) และธุรกิจซื้อขายรวมบริการด้วยเทคโนโลยีนี้ตามมาอีกด้วย เช่นที่ประเทศฝรั่งเศสและสวิสเซอร์แลนด์

ตัวอย่างโครงการที่ประสบความสำเร็จคือ โครงการ SCALA (9.4 ล้านยูโร) เพื่อขีดความสามารถของควอนตัมคอมพิวเตอร์ โครงการประยุกต์ QAP (9.9 ล้านยูโร) โครงการ EuroSQIP (6 ล้านยูโร) เพื่อพัฒนาระบบประมวลผลเชิงควอนตัม 3-5 คิวบิตและ SECOQC อันเป็นโครงการความร่วมมือด้านวิทยาการรหัสลับเชิงควอนตัมที่ใหญ่ที่สุดดำเนินการในช่วงเวลาเมษายน พ.ศ.2547 ถึง ตุลาคม พ.ศ.2551 โดยได้รับการสนับสนุนงบเฉพาะจากอียูเองมากกว่า 11 ล้านยูโร (รวมกับแหล่งอื่นอีกมาก) เป็นต้น

ในช่วงการสนับสนุนล่าสุดของ FP7 (ค.ศ.2007-2013) มีกลุ่มวิจัยจากประเทศภายนอกยุโรปเข้าร่วมงานวิจัยเทคโนโลยีสารสนเทศเชิงควอนตัมด้วยแล้วทั้งจาก สหรัฐอเมริกา ออสเตรเลียและสิงคโปร์ โดย FP7 นี้สนับสนุนโครงการด้าน QIPC ใหม่ ๆ ภายใต้งบประมาณที่สูงมหาศาลครอบคลุมทั้งสองสาขาหลักของสารสนเทศเชิงควอนตัมคือ การคำนวณ (computing) และการสื่อสาร (communications)

25 หนังสือ *"สารสนเทศเชิงควอนตัมประเทศไทย ฯ" 2014 ISBN 9786163748300 (http://www.ebooks.in.th/ebook/30625/)*

Picture from

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography

Future and Emerging Technologies European Commission

by Ales Fiala

5-7 OCTOBER 2015

Korea

(การพัฒนากำลังคนของกลุ่มสหภาพยุโรป)

Picture from

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography

Future and Emerging Technologies European Commission

by Ales Fiala

5-7 OCTOBER 2015

Korea

(การลงทุนของกลุ่มสหภาพยุโรป)

หมื่นล้านเพื่องานควอนตัม

(การลงทุนของสหราชอาณาจักร)

นำมาสู่การวิเคราะห์ต่อมาได้ว่าการสนับสนุน**งบประมาณ**ที่ผ่านมาของสหภาพยุโรปที่ให้ทุนวิจัยและพัฒนาไอทีควอนตัมไปนั้น จากข้อมูลในแผนที่จำลองจะเห็นการกระจายงบกับการสร้างความพร้อมกำลังคนใน**ยี่สิบปี**จากต้นสหวรรษใหม่เป็นต้นมา สองปัจจัยหลักนี้มีตัวเลขรวม 2,500 คนของการระดมพลและงบก้อนใหญ่มากสูงถึง 550 ล้านยูโร ซึ่งแม้ตัวเลขจะสูงแต่ก็กระจายเหลือเป็นก้อนเล็กลงไปในหลายแห่งและใช้เวลานานมากหลายปี

ส่วนด้าน**บุคลากร**เมื่อพิจารณาแยกย่อยดูในแต่ประเทศ เช่น ออสเตรีย สวีเดน นอร์เวย์หรือสวิสเซอร์แลนด์ แต่ละชาติมีประชากรทั้งประเทศน้อยกว่าพลเมืองแค่ของกทม. *(แต่กำลังซื้อประชาชาติต่อคนหรือผลิตภัณฑ์มวลรวมในประเทศสูงตั้งแต่กว่าสามหมื่นถึงห้าหมื่นเหรียญสหรัฐฯ มากกว่าสามจนถึงกว่าห้าเท่าขึ้นไป)* แต่เมื่อมารวมบุคลากรร่วมกันจึงทำให้เกิดการรวมกลุ่มได้เพียงพอด้านบุคลากร และจากการที่**วิทยาการ**มีสะสมและพัฒนามานาน ร่วมกับ**นโยบาย**ที่กำลังกลับมาเข้มข้นขึ้นทั้งหมดทำให้สี่ปัจจัยหลักมีมิติที่น่าจะสำเร็จยิ่งใหญ่ได้ต่อไป

โดยสรุป สหภาพยุโรปมี **"นโยบายนำ รวมงบประมาณ คนแต่ละประเทศมีน้อยรวมทีมข้ามประเทศจนมีความพร้อม วิทยาการได้สั่งสมเข้มแข็งมานับศตวรรษแล้ว"** เมื่อครบร่วมกันทั้งสี่ปัจจัยภารกิจงานชิ้นใหญ่จึงเกิดขึ้นได้

(ความร่วมมือของเนเธอร์แลนด์และเดนมาร์ก)

ข.3.2) การลงทุนอนาคตของสหราชอาณาจักรระดับหมื่นล้าน

ปลายปีค.ศ.2013 เป็นต้นมาและต่อไปอีกถึงห้าปีที่รัฐบาลสหราชอาณาจักรจะได้ใช้จ่ายถึง £ 270 ล้านปอนด์ หรือประมาณมากกว่า**"หนึ่งหมื่นสี่พันล้านบาท"**ในการสนับสนุนงานวิจัย "เทคโนโลยีควอนตัม" ซึ่งแม้จะมีเป้างบประมาณสูงแต่ผ่านการพิจารณาจากรัฐสภามาได้ด้วยความรวดเร็ว ซึ่งโครงการนี้รัฐบาลประสงค์จะใช้เพื่อหลักสถานะของประเทศที่เคยเป็นผู้นำด้านวิทยาการมานับศตวรรษให้กลับมา จึงเลือกโจทย์ใหญ่ของอนาคตเรื่องนี้เป็นที่ตั้ง

ทั้งนี้ โดยมี 132 บริษัท 12 มหาวิทยาลัยเข้าร่วมโครงการ ตามเป้าหมายจะพัฒนาไปให้ถึงการสร้างสินค้า (product) ด้วย ซึ่งนับว่าเป็นโครงการจัดสรรงบที่สร้างความตื่นตะลึงไปทั่วโลกเกี่ยวข้องกับเรื่องอนาคตแม้ปัจจุบันยังคงมีความเข้าใจที่สับสนอยู่ทั่วทุกวงการกับคำว่า "ควอนตัม"

และยังมีอีกกรณีเด่นด้านการสนับสนุนของรัฐบาลต่องานด้านเทคโนโลยีควอนตัมนี้ โดยปรากฏขึ้นที่ประเทศเดนมาร์กกับเนเธอร์แลนด์ ซึ่งได้รวมตัวกันเพื่อจะสร้างควอนตัมคอมพิวเตอร์ โดยการลงนามความร่วมมือเมื่อต้นปีพ.ศ.2558 ที่มีสักขีพยานคือ นายกรัฐมนตรีหญิงเดนมาร์กกับสมเด็จพระราชาธิบดีและสมเด็จพระราชินีของเนเธอร์แลนด์เสมือนเป็นการแจ้งสู่สาธารณะว่าเป็นโครงการระดับชาติจริงจัง โดยสถาบันนีลส์บอร์ (Danish Niels Bohr Institute) ของเดนมาร์กซื่อเดียวกับผู้ก่อตั้งและนักวิทย์ในเบลโครงสร้างอะตอม สถานที่ ๆ บ่มเพาะความรู้มานานเกือบศตวรรษเทียบใกล้อายุแชมงวิชากลศาสตร์ควอนตัมของโลกด้วย และเป็นที่รวมตัวของนักวิทยาศาสตร์ระดับโลกก่อนสงครามโลกครั้งที่สอง ได้มาร่วมงานกับมหาวิทยาลัยเทคโนโลยีเดลฟท์ (TU Delft) ของเนเธอร์แลนด์ เพื่อการพลิกสถานะการเป็นแถวหน้าของโลกด้านฟิสิกส์พื้นฐานอีกเช่นกัน

ข.3.3) แนวทางของประเทศจีน

ประเทศจีนมีการจัดทำแผนที่นำทางด้านเทคโนโลยีสารสนเทศเชิงควอนตัมด้วยระยะเวลานานถึง**สี่สิบห้าปี** อยู่ในแผน 3 ช่วงระยะ คือ ระยะสั้น (ปีค.ศ.2005-2020) ระยะกลาง (ปีค.ศ.2020-2035) และระยะยาว (ปีค.ศ.2035-2050) ที่ครอบคลุมสาขากว้างมากของวิทยาศาสตร์และเทคโนโลยี และเป็นความภาคภูมิใจโดยนำเสนอการคาดการณ์ที่เกี่ยวข้องว่า ในปีค.ศ.2050 (Roadmap 2050) ประเทศจีนอาจเป็นประเทศที่ร่ำรวยที่สุดในโลก (ในเชิงค่าการเติบโตทางเศรษฐกิจ - GDP) จึงควรร่วมเป็นประเทศผู้สร้างอารยะธรรมด้านวิทยาศาสตร์และเทคโนโลยีไว้ให้กับสังคมโลกด้วยความรับผิดชอบ แผนการฉบับนี้สร้างโดยสถาบันวิทยาศาสตร์จีน CAS (The Chinese Academy of Science) ก่อมาตั้งแต่เมื่อปี ค.ศ.1949 โดยในรายละเอียดที่เกี่ยวข้องแบ่งกลุ่มเป้าหมายเป็นเทคโนโลยีอินเทอร์เน็ตเครือข่าย เซ็นเซอร์ และเชิงบริการต่าง ๆ 5 สาขาหลัก (Internet System and Technology, Sensor Network and the Internet of Things, Network Service, Human-Machine Interaction และ Network Science) ซึ่งไอทีควอนตัมอยู่ภายใต้สาขาท้ายสุด

ทว่า สิ้นปีพ.ศ.2557 กองทุนการเงินระหว่างประเทศ (หรือ IMF) แจงแล้วว่า จีนได้เติบโตเป็นประเทศเศรษฐกิจใหญ่ที่สุดอันดับหนึ่งของโลกแซงหน้าสหรัฐฯ แล้ว มีจีดีพีคิดเป็นมูลค่าราว 17.6 ล้านล้านดอลล่าร์ ขณะที่สหรัฐฯ อยู่ในระดับ 17.4 ล้านล้านดอลล่าร์ ซึ่งต่างกันเพียงเล็กน้อย และอนาคตข้างหน้าก็สามารถคาดการณ์ได้แล้วว่าประเทศจีนจะก้าวสู่ตำแหน่งลำดับต้นของโลกเป็นที่แน่นอน

สำหรับการวิจัยและพัฒนาด้านวิทยาการรหัสลับเชิงควอนตัมมีงานวิจัยและพัฒนาวิทยาการรหัสลับเชิงควอนตัมมีอยู่หลายแห่งในประเทศ มาปรากฏชัดอยู่ในมหาวิทยาลัยอยู่ที่เมืองเหอเฟย มณฑลอันฮุย ซึ่งจัดได้ว่าเป็นเมืองหลวงของวิทยาการแขนงนี้ โดยมีถึงสองห้องปฏิบัติการวิจัยหลักของประเทศที่มีชื่อเสียงระดับโลกอยู่ร่วมภายในมหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยี (USTC) เดียวกันคือ กลุ่มของศาสตราจารย์ เจิ้งฟู่ หาน (Zheng-Fu Han) และศาสตราจารย์ เจี่ยน เหวย พาน (Jian Wei Pan)

ทั้งสองกลุ่มงานนี้ ได้นำเสนอผลงานการทดสอบระบบวิทยาการรหัสลับเชิงควอนตัมในหลายโครงการใหญ่จนเป็นบันทึกความก้าวหน้าสำคัญของโลก เช่น กลุ่มวิจัยของศาตราจารย์เจิ้งฟู่ หาน (Zheng-Fu Han) สร้างระบบเครือข่ายสำหรับหน่วยงานของรัฐฯ เข้ารหัสภาพ วีดีโอ เสียงและเอกสารต่าง ๆ ผ่านเส้นใยนำแสงในสี่โครงข่ายหลักเขตตัวเมืองอู่หู มณฑลอันฮุย และตั้งบริษัท Q-Asky ส่วนกลุ่มของศาสตราจารย์เจี่ยน เหวย พาน (Jian Wei Pan) ร่วมมือใกล้ชิดกับกลุ่มเวียนนา (ประเทศออสเตรีย) มีผลงานเทคนิคด้านความพัวพัน (Entanglement) และการส่งถ่ายเชิงควอนตัม (Teleport) ที่เด่นชัดกำลังเริ่มโครงการกระจายกุญแจรหัสลับผ่านดาวเทียม[26] (พ.ศ.2559) รวมทั้งเส้นทางกว่าพันกิโลเมตรภาคพื้นดินจากปักกิ่งกับเซี่ยงไฮ้ ก็เป็นโครงการแสดงศักยภาพที่โลกได้จับตามองทั้งด้านเทคโนโลยีและความพร้อมด้านงบประมาณรวมถึงกำลังคน

เมื่อพิจารณา ณ มหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยี (USTC) กับตัวอย่างหนึ่งเดียวของห้องปฏิบัติการด้านสารสนเทศเชิงควอนตัมกลุ่มวิจัยของศาตราจารย์เจิ้งฟู่ หาน ที่ทำกิจกรรมด้านนี้มานานพร้อมด้วยงบประมาณที่ใช้จ่ายไปแล้วถึงระดับพันล้านหยวน โดยมีนักศึกษาปริญญาเอกกว่ายี่สิบคนในช่วงเวลาใด ๆ ผลงานวารสารวิชาการรวมกว่า 400 และมากกว่า 20 ชิ้นจำนวนนั้นสิพิมพ์ในวารสารอันดับหนึ่ง "Nature" ผลงานมีพร้อมด้วยต้นแบบและได้รับการจัดตั้งเป็นบริษัทจากผลงานวิจัย (spin-off) โดยสังเกตได้ว่าที่กล่าวถึงอยู่นี้เป็นผลจากกลุ่มเดียวแค่จากมหาวิทยาลัยแห่งเดียว หากรวมผลทั้งประเทศจีนที่มีหลายหน่วยงานกำลังขะมักเขม้นสร้างสรรค์งานด้านนี้อยู่นั้นจะทำให้จีนกลายเป็นประเทศผู้นำด้านวิทยาการใหม่เรื่องนี้ไปโดยปริยาย

ในขณะที่ภาพรวมของประเทศจีน CAS (Chinese Academy of Science) หน่วยงานหลักที่สนับสนุนภายในประเทศและกิจกรรมวิจัยของ USTC นั้น ก็ยังได้ตั้งเป้าหมายพัฒนา**ควอนตัมคอมพิวเตอร์**ที่ยิ่งใหญ่ภายในปีค.ศ.2050 (พ.ศ.2593) อีกด้วย ซึ่งคอมพิวเตอร์แห่งอนาคตนี้จะเกิดผลกระทบส่งผลให้รหัสลับเชิงควอนตัมมีความสำคัญสูงขึ้นเป็นอย่างมาก

โดยโครงการฯ เคยมีโอกาสเดินทางไปเยี่ยมกลุ่มของศาตราจารย์เจิ้งฟู่ หาน เจ้าของผลงานมหาศาลที่เกริ่นข้างต้นเมื่อกลางปี 2013 ที่เมืองอันฮุย มณฑลเหอเฝย โดยกระทรวงการต่างประเทศของไทยกับกระทรวงวิทยาศาสตร์ของจีนให้การสนับสนุน และได้ร่วมงานต่อเนื่องกับกลุ่มวิจัยนี้โดยเริ่มต้นมีการออกผลบ้างแล้ว[27] แต่ด้วยตั้งแต่เหตุการณ์ความไม่สงบในประเทศปลายปีพ.ศ.2556 เป็นต้นมา ทำให้ความร่วมมือหยุดชะงักลง ซึ่งต้องการการเริ่มต้นฟื้นฟูใหม่อีกระยะหนึ่งต่อไป

จากประวัติฯที่ยี่สิบปีก่อนหน้า ประเทศจีนเริ่มมีการทำชุดโครงงานเพื่อให้นักศึกษาได้เรียนรู้ทดลองด้านรหัสลับเชิงควอนตัมด้วยงบประมาณต่ำกว่าห้าร้อยบาท มาบัดนี้ ประเทศจีนกำลังสร้างโครงข่ายการสื่อสารรหัสลับเชิงควอนตัมที่ใหญ่และไกลสุดในโลก และใช้งบโอฬีควอนตัมรวมเข้าสู่หลักหมื่นล้านบาทแล้วด้วย โดยสรุป ***"การมีนโยบายนำ งบประมาณพร้อม บุคลากรที่ขยับจำนวนมาก วิทยาการก็ได้เรียนรู้ซึมซับมา[28] จากต่างประเทศจนสามารถสร้างเองได้"*** จึงรวมครบทั้งสี่ปัจจัยหลักและมีแนวโน้มจะนำหน้าทุกกลุ่มของโลกไปใกล้ในอนาคต

26 http://www.bbc.com/news/world-asia-china-37091833

27 http://cpb.iphy.ac.cn/EN/V2014/V23/I9/090310

28 http://www.wsj.com/articles/chinas-latest-leap-forward-isnt-just-greatits-quantum-1471269555

โครงข่ายรหัสลับควอนตัมใหญ่สุด 2015

Hefei-Chaohu-Wuhu QKD wide area network

Shuang Wang et al., Opt Express, 22, 21739 (2014)

ประเทศจีนทำรหัสลับควอนตัมขายแล้ว

Anhui Quantum Ctek Co. Ltd.

(3rd ETSI/IQC Workshop on Quantum-Safe Cryptography)
The Chinese QKD Networks, by Hong Xiang, 5-7 OCTOBER 2015, Korea)

ข.3.4) อนาคตแบบสิงคโปร์

องค์การพัฒนาสารสนเทศสิงคโปร์ (IDA) ได้จัดทำรายงานการคาดการณ์ชื่อ "Infocomm Foresights" เป็นแผนที่นำทางเทคโนโลยีสารสนเทศฉบับที่ 5 หรือแผนกลยุทธ์ระยะยาว 1 0 ปี (จนถึงปีพ.ศ.2558) โดยมีเทคโนโลยีสำคัญ 3 ด้าน คือ 1) Computing Wave 2) Communications Wave และ 3) Sentient Wave ซึ่งในส่วนของ Computing และ Sentient Wave มีเทคโนโลยีสารสนเทศเชิงควอนตัมร่วมอยู่ด้วย

งานวิจัยและพัฒนาด้านไอทีควอนตัมของประเทศเล็กแต่ร่ำรวยแห่งนี้จึงเริ่มต้นโดยการจัดตั้งศูนย์วิจัยขึ้น ณ มหาวิทยาลัยแห่งชาติ (The National University of Singapore) เมื่อปี พ.ศ.2550 พร้อมงบประมาณ**กว่า 150 ล้านดอลลาร์สิงคโปร์**ในการเป็นศูนย์ความเชี่ยวชาญ Research Centre of Excellence (RCE) และด้วยการลงทุนเชื้อเชิญนักวิจัยที่มีชื่อเสียงระดับโลกเข้าร่วมงาน จึงเป็นจุดเริ่มต้นที่ต่อมาทำให้พัฒนาการของไอทีควอนตัมในประเทศเติบโตและก้าวหน้าแบบเขย่งก้าวกระโดด และเป็นรูปแบบที่แตกต่างจากประเทศอื่น ๆ อย่างชัดเจน

หนึ่งในเอกลักษณ์นั้นคือ การเชิญศาสตราจารย์ อาร์เทอร์ อีเคอร์ท (Artur Ekert) จากมหาวิทยาลัย อ็อกฟอร์ด (Professor of Quantum Physics, Mathematical Institute) ประเทศอังกฤษ หนึ่งในผู้คิดค้นงานการสื่อสารเชิงควอนตัมความพัวพัน (entanglement) มาเป็นผู้อำนวยการของศูนย์เทคโนโลยีควอนตัม (Centre for Quantum Technologies) ซึ่งแน่นอนว่าทั้งศูนย์ฯ มีประชากรส่วนใหญ่เป็นนักวิจัยชาวต่างชาติ ภาพรวมจากผลผลิตและการเติบใหญ่ของศูนย์ฯนี้แสดงให้เห็นถึงการลงทุนโครงสร้างพื้นฐานบ่มเพาะศักยภาพด้านไอทีควอนตัมอย่างเข้มข้น รวมทั้งกำลังเร่งผลักดันตามแผนระยะยาวให้เป็นอีกหนึ่งในหน่วยงานสำคัญหลักของโลกในอนาคตอีกด้วย

หากเน้นกับเฉพาะวิทยาการรหัสลับเชิงควอนตัม ซึ่งถูกบรรจุอยู่ในแผนส่วนของโครงสร้างพื้นฐานทางความมั่นคงปลอดภัยด้านข่าวสาร (Security & Trusted Infocomm Infrastructure) นั้น เป้าหมายของสิงคโปร์จะไปถึงการประยุกต์ใช้ทั้งภาครัฐและภาคการเงินการธนาคาร โดยวางแผนสร้างเครือข่ายสื่อสารรหัสลับเชิงควอนตัมทั่วทั้งเกาะสิงคโปร์ จนทำให้สานะภาพงานด้านไอทีควอนตัมที่มีอยู่บนเกาะขนาดประมาณเพียงแค่ครึ่งเดียวของกทม. แห่งนี้กลับมีความพร้อมมากกว่าหลายประเทศในยุโรปที่เป็นเจ้าวิทยาการไปแล้วเมื่อวัดกันด้วยทั้งสี่ปัจจัยหลักที่พิจารณาถึงนั้น (นโยบาย บุคลากร งบและวิทยาการใหม่ ๆ)

ข้อมูลล่าสุดของศูนย์แห่งนี้ ได้ใช้งบประมาณไปกว่าหนึ่งพันล้านบาทในระยะเวลาสามปี (ค.ศ. 2012-2015) เฉพาะเพื่อการสร้างบุคลากร โดยรับนักศึกษาที่มีศักยภาพเข้าศึกษาและเป็นนักวิจัย โดยมีอัตราส่วนนักศึกษาต่างชาติสูงมากกว่า เมื่อรวมกับ**บุคลากร**ที่เชิญเข้ามาก็ได้มาถ่ายทอด**วิทยาการ**และช่วยสร้างคนในประเทศสิงคโปร์ได้ต่อเอง

สรุป ประเทศสิงคโปร์มี **"นโยบายนำสุดทางกับแผนงานสุดล้ำ งบประมาณพร้อม ที่ขาดคือบุคลากรกับวิทยาการจึงนำเข้าจากต่างประเทศมาทำงานเต็มเวลา"** แม้มีเริ่มต้นแค่สองปัจจัยแต่ในที่สุดได้รวมครบทั้งสี่ปัจจัยหลักแล้ว สิงคโปร์จึงเป็นประเทศตัวอย่างใกล้บ้านที่เน้นย้ำให้เห็นได้ว่า แม้ขาดถึงสองปัจจัยหลักก็ยังทำได้ในช่วงเวลาอันสั้น เพราะการมี**จุดแข็งด้านงบประมาณ**และ**นโยบาย**เป็นที่สุด จึงทำให้อุปสรรคทั้งสองได้รับการชดเชยจนสู่การสร้างผลงานบนเวทีไอทีควอนตัมโลกได้

ข.4 จากปัจจัยเสี่ยงสู่การพัฒนาสร้างรายได้ของเกาหลีใต้และรัสเซีย

(ห้องปฏิบัติการรหัสลับควอนตัม SK telecom)

(ต้นแบบกับการนำเสนอรหัสลับควอนตัม SK telecom)

(ระยะเวลาเพียงสองปี เกาหลีได้สร้างศูนย์กลาง (testbed) ระยะทางรวมกว่าสองร้อยกม.แล้ว[29])

- **เกาหลีใต้**

ข้อมูลจากการประชุมเชิงปฏิบัติการมาตรฐานรหัสลับเชิงควอนตัมโลกครั้งที่ 3 (IQC/ETSI QKD workshop) ต้นเดือนตุลาคม พ.ศ. 2558 ณ กรุงโซล ประเทศเกาหลีใต้ ถึงกับทำให้โลกไอทีได้แปลกใจกับการพลิกโฉมหน้าครั้งใหญ่ของประเทศเกาหลีใต้ ซึ่งเป็นผู้เพิ่งเริ่มกิจกรรมวิจัยสาขานี้มาได้ไม่นาน แต่เนื่องจากเกาหลีใต้ถูกคุกคามจากพี่น้องร่วมเชื้อชาติฝากเหนือต่อระบบอินเทอร์เน็ต จึงต้องหาวิธีสมบูรณ์แบบเพื่อหยุดความเสี่ยงนั้นร่วมกับรหัสลับควอนตัม รวมทั้งแนวทางด้านเศรษฐกิจและศักดิ์ศรีที่ตามหลังเพื่อนบ้านก็มาเป็นตัวขับดันงานด้านไอทีเชิงควอนตัมของประเทศ ทำให้พัฒนาไปได้เร็วมาก จากที่เคยประเมินตนเองว่าวิทยาการของเกาหลีใต้ด้านนี้ไกลห่างจากประเทศแถวหน้าของโลก 2 ถึง 7 ปี

ประเทศเกาหลีใต้นี้เคยได้พลิกโฉมหน้าโลกมาแล้วกับอุตสาหกรรมโทรศัพท์เคลื่อนที่ทั้งกรณีของซัมซุง แอลจี ที่สามารถแข่งขันกับทั้งโนเกีย แอปเปิล โมโตโรลา ฯ จนมาอยู่แถวหน้าของโลก และกำลังประสบผลสำเร็จมากับไอทีควอนตัมอีกเรื่องหนึ่งแล้ว เพียงที่ SK telecom บริษัทผู้ให้บริการโทรคมนาคมใหญ่ที่สุดในประเทศวางแผนทดลองกับเครือข่ายใหม่ที่ติดตั้งแบบจุดต่อจุดในปีค.ศ.2016 โดยโยงระบบจากกรุงโซลไปเมืองซูวอนระยะประมาณ 50 กิโลเมตร แล้วขยายลงไปเมืองทางตอนใต้ต่อไปราว 200 กิโลฯ จะต่อกระจายจากหนึ่งไปหลายจุดจนถึงเป็นโครงข่ายในปีค.ศ. 2018 และค.ศ. 2020 ตามลำดับ และมีต้นแบบเริ่มออกงานเพื่อจำหน่ายทั้งภายในและต่างประเทศแล้วด้วย

29 ข่าว *http://www.businesswire.com/news/home/20160304005490/en/*

โดยรูปแบบการทำงานในประเทศมีการรวมตัวกันเป็นสมาคมทั้งภาครัฐฯ อุตสาหกรรมและวิชาการ (Quantum Information Communication Research Association) เพื่อการขับเคลื่อนภารกิจอนาคตนี้โดยบริษัท SK Telecom นี้ก็เป็นเจ้าภาพร่วมกับอีกสองหน่วยวิจัยหลักของประเทศด้านวิทย์ฯเทคโนฯและความมั่นคงไอที (NSRI, KISTI[30]) รวมตั้งเป็นกลุ่มสหภาพควอนตัม (Quantum Union) อันเป็นแนวทางตัวอย่างที่ดีอีกกรณีหนึ่ง เนื่องจากงานด้านโครงสร้างพื้นฐานที่ลงทุนสูงทั้งด้านบุคลากรและงบประมาณโดยทั่วไปจะต้องเริ่มมาจากภาครัฐ แต่หากต่อยอดโดยอุตสาหกรรมไม่ได้งานเหล่านั้นก็จะจบลงในเวลาอันรวดเร็ว และเป็นการสูญเสียในลักษณะที่เรียกว่า "ตำน้ำพริกละลายแม่น้ำ" (พัฒนาไปไม่ถึงจุดมวลวิกฤติ) อันขยายความได้ว่า จะเป็นเรื่องที่ประสบสำเร็จได้ยากหากให้หน่วยงานรัฐฯ เป็นผู้เริ่มภารกิจเชิงลึกในการวิจัยและพัฒนาเรื่องใหม่ ๆ สำหรับอนาคต เช่น วิทยาการรหัสลับเชิงควอนตัมนี้โดยลำพัง จากกรณีศึกษาของประเทศเกาหลีใต้ ภาคเอกชนด้านสื่อสารโทรคมนาคมหรือ Sktelecom คือ "ผู้เล่น"หลัก มีภารกิจเป้าหมายแคบกว่าภาครัฐ ฯ และมีความสามารถผลักดันจากด้านธุรกิจหรือ "ปลายน้ำ" กระนั้น รัฐบาลที่แม้ต้องดำเนินการครอบคลุมงานอื่นกว้างกว่ามากก็ได้มาเป็นผู้วางโครงสร้างพื้นฐานสนับสนุนอย่างจริงจังให้ จึงเป็นการรวมกลุ่มที่ลงตัวได้ในที่สุด

กระทั่งสี่ปัจจัยพื้นฐานสร้างวิทยาการแห่งอนาคตไอทีควอนตัม ทั้ง"นโยบาย ความรู้ บุคลากรและงบประมาณ"นั้น ประเทศเกาหลีใต้มีครบแล้วโดยที่

นโยบายที่ผลักดันคือทั้ง 1) ด้านเทคโนโลยีภายในประเทศที่เข้มและเกี่ยวเนื่องมาจากระบบเครือข่ายของประเทศเคยโดนนักรบออนไลน์ของเกาหลีเหนือโจมตีเสียหาย และ 2) จากภายนอกคือผลทำนายตลาดและแนวโน้มอุตสาหกรรมทั่วโลก จึงเกิดเป็นแผนที่นำทาง (roadmap) ภายในประเทศต่อมาได้โดยใช้เวลาไม่นาน

วิทยาการ เกาหลีใต้พึ่งพาการซื้อหามาก่อนโดยมีความร่วมมือกับหน่วยงานใหญ่ของโลก เช่น ระบบจากบริษัท idQuantique ฯลฯ นำมาศึกษา สร้างองค์ความรู้เองร่วมด้วยจนสร้างอุปกรณ์ใช้งานเองได้ในที่สุด

กำลังคนที่เป็นทางการเพิ่งเริ่มปีค.ศ. 2014 มีบุคลากรทางด้านสารสนเทศเชิงควอนตัมอยู่ราว 100 ที่ผ่านการฝึกอบรม และจะเพิ่มไปให้ถึง 3,000 คนในปี ค.ศ. 2020 โดยสองปีที่ผ่านมาประสบผลมากแล้ว จึงสามารถคาดการณ์ต่อไปเมื่อถึงระยะเวลาหกปีตามแผน ประเทศเกาหลีคงได้พลิกโฉมหน้าวงการไอทีควอนตัมได้อีกมาก

งบประมาณ รวมงานไอทีควอนตัมเกาหลีช่วงค.ศ.2014 – 2020 มีสูงระดับ 100 ล้านเหรียญหรือเลยสามพันล้าน (~3,500,000,000) บาท

"ปัจจุบัน เกาหลีใต้โดย SK telecom กำลังกลายเป็นผู้ผลิตจำหน่ายในอุตสาหกรรมรหัสลับเชิงควอนตัมแล้ว"

30 *National Security Research Institute และ Korea Institute of Science and Technology Information*

- **รัสเซีย**

เช่นกันจากข้อมูลการประชุมเชิงปฏิบัติการมาตรฐานรหัสลับเชิงควอนตัมโลกครั้งที่ 3 (IQC/ETSI QKD workshop) ต้นเดือนตุลาคม พ.ศ.2558 พบว่าประเทศรัสเซียก็มีการพัฒนาเปลี่ยนแปลงครั้งใหญ่ แนวทางสำคัญประการหนึ่งเป็นผลต่อเนื่องมาจากอดีตที่มีการปฏิรูปโครงสร้างการเมือง เศรษฐกิจและสังคม ตามแนวทางที่ชื่อ"เปเรสตรอยกา (Perestroyka)" ในปีค.ศ.1985 ที่เริ่มหาระบบทุนนิยมเข้าประเทศ เพื่อนำพาประเทศกลับมาสู่เวทีโลกอีกครั้งด้วยสารพันแนวทางการพัฒนาประเทศ หนึ่งในนั้นคือสาขาวิทย์และเทคโนฯ จนให้กำเนิดหน่วยงานด้านเทคโนโลยีควอนตัมด้วยเช่นกัน โดยมีการขับเคลื่อนพันธกิจต่อถึงยุทธศาสตร์สู่การปฏิบัติแล้ว และในไม่กี่ปีต่อมาจึงปรากฏมีโครงการรหัสลับควอนตัมในที่สุดอันเป็นส่วนหนึ่งของศูนย์วิจัยควอนตัมแห่งชาติ (RQC)[31] ที่ก่อตั้งขึ้นเป็นหนึ่งใน 16 กลุ่มภารกิจแรกของมูลนิธิสโคลโกโว (Skolkovo Foundation) องค์กรที่ไม่แสวงกำไรเพื่อการพัฒนาเทคโนโลยีใหม่และการประยุกต์ใช้เชิงพาณิชย์และเป็นกองทุนที่เพิ่งก่อตั้งขึ้นเมื่อปี พ.ศ.2553 มานี้โดยอดีตประธานาธิบดี ดมิตรี เมดเวเดฟ (Dmitry Medvedev)

ศูนย์วิจัย ฯ แห่งนี้ได้เผยพันธกิจและยุทธศาสตร์ที่เข้าหาบุคลากรที่มีชื่อเสียงฝั่งตะวันตกด้วยการเชิญมาให้คำปรึกษา และบริหารจัดการรวมไปถึงบุคลากรชาวรัสเซียที่ไปประสบความสำเร็จอยู่ในต่างประเทศด้วย เสมือนโครงการ "สมองไหลกลับ[32]" ทั่วไป

โดยสรุป จากปัจจัยเสี่ยงต่าง ๆ นำไปสู่การปฏิรูปโครงสร้างหลายด้านของประเทศนั้นก็ได้ขับดันให้แนวทางงานด้านสารสนเทศเชิงควอนตัมของประเทศรัสเซียเกิดมี 1) **นโยบายเข้มข้น** และ 2) **งบประมาณสูง** คล้ายกันกับสิงคโปร์ที่มีคู่ปัจจัยหลักแรกนี้แล้วใช้ไปเหนี่ยวนำเอา 3) **บุคลากรคุณภาพจากต่างชาติ** (รวมทั้งคนรัสเซียในต่างแดน) และสุดท้าย 4) **เพื่อแสวงหาวิทยาการใหม่**เข้าประเทศได้

31 *Russian Quantum Center (RQC): www.rqc.ru*

32 *ประเทศไทยช่วงกว่าสองทศวรรษก่อนหน้า (พ.ศ.2533) ได้มีการเริ่มโครงการ "สมองไหลกลับ (reverse brain drain)" นี้ด้วยเช่นกัน (http://rtxt.nstda.or.th/)*

ข.5 ไอทีควอนตัมไทยกับสี่ปัจจัยพัฒนาสำคัญ

จากแนวทางตัวอย่างที่ได้สำรวจวิเคราะห์ของโครงการที่เกี่ยวข้องในต่างประเทศข้างต้น นำมาสู่การย้อนศึกษาอดีตที่ใกล้เคียงภายในประเทศ เพื่อที่จะได้เชื่อมโยงประสบการณ์ต่าง ๆ สู่การวางแนวทางอนาคตกับวิทยาการรหัสลับเชิงควอนตัมอันเป็นการสื่อสารยุคใหม่ในหัวข้อถัดไป ด้วยตัวอย่างด้านงานวิจัยและพัฒนาดังนี้

ประเทศไทยนอกจากการเป็นผู้บริโภคหรือผู้ซื้อเทคโนโลยี**ด้านสื่อสารโทรคมนาคมหรือไอที**แล้ว อดีต เคยได้พยายามทำการวิจัยและพัฒนาเพื่อยืนได้ด้วยตนเองมากับหลายโครงการแล้ว การศึกษาประวัติศาสตร์ของเรื่องที่เกี่ยวข้องเพื่อการหยั่งรู้แนวโน้มอนาคตเริ่มได้ตั้งแต่ยุคระบบ**โทรเลข** ที่เริ่มนำเข้ามาใช้เป็นทางการที่พ.ศ.2418 กรมไปรษณีย์โทรเลขได้ประกาศให้ใช้รหัสสัญญาณภาษาไทยในการรับส่งภายในประเทศตั้งแต่วันที่ 1 พฤศจิกายน พ.ศ.2455 ต่อมาในปี พ.ศ.2496 ได้มีการประดิษฐ์คิดค้นเครื่อง**โทรพิมพ์ภาษาไทย** (โดย สมาน บุณยรัตพันธุ์) จนถึงปี พ.ศ.2497 จึงได้มีเครื่องโทรพิมพ์ทำงานทั้งสองภาษาในเครื่องเดียวกันมีความเร็ว 357 อักษรต่อนาทีโดยใช้ร่วมกับโทรเลขเรื่อยมา ระบบภาษาจึงเป็นแนวทางหลักที่ทำเองได้เพราะต่างชาติทำแทนได้ยาก ซึ่งจัดได้ว่าเป็นงานวิจัยประยุกต์ชิ้นแรก ๆ ของประเทศ

หลังจากนั้น เรื่องภาษากับการประยุกต์ให้เหมาะสมกับเมืองไทยจึงเป็นแนวทางเด่นชัดที่สุดจนเข้าสู่ช่วงยุคไอทีที่มีคอมพิวเตอร์มาร่วม งานพัฒนาหลักจึงมากับภาษาไทย เช่น รหัสภาษาไทยของ สมอ.และเกษตรฯ การสร้างฟอนท์ (font) และรหัสร่วมสื่อสารจนถึงการแปลภาษา แต่สำหรับงานโครงสร้างทุกระบบหลักยังคงต้องนำเข้าทั้งหมด

กระทั่งมาถึงยุคของระบบสื่อสารโทรศัพท์บ้าน ตั้งแต่อดีตมาจนถึงยุคที่ต้องการขยายไปทั่วประเทศโดยในเขตเมืองหลวงต้องการเพิ่มเติมสองล้านเลขหมายและในภูมิภาคอีกหนึ่งล้าน ซึ่งเข้าใจกันว่าเป็นช่วงที่มีการพัฒนา (ด้านการให้บริการ) ถึงจุดสูงสุด โดยมีผู้ผลิตนำสินค้ามาทดลองระบบพร้อมให้บริการไปด้วย เช่น เอที&ทีแอนด์ที (AT&T) ซีเมนส์ (Siemens) อีริคสัน (Ericsson) หรือเอ็นอีซี (NEC) เป็นต้น ระหว่างนั้นงานวิจัยของไทยที่เกี่ยวข้องขับเคลื่อนไปได้แค่ระบบชุมสายโทรศัพท์สำนักงานและบ้าน (PABX) ขนาดเล็ก ขณะที่เหล่าผู้ผลิตต่างชาติกำลังเปลี่ยนย้ายไปยังเทคโนโลยีโทรศัพท์เคลื่อนที่

และช่วงนั้นเอง ในประเทศไทยอยู่ในช่วงยุค"*สมองไหลกลับ*"ที่บุคลากรไทยในต่างแดนได้รับการสนับสนุนให้กลับมาพัฒนาประเทศช่วงเริ่มหน่วยงานวิจัยและพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีสามทศวรรษที่ผ่านมา และเกิดมี โครงการวิจัยและพัฒนาระบบโทรคมนาคมเพื่อการสื่อสารเคลื่อนที่ยุคที่สาม (3G) ด้วยงบรวมกว่า 20 ล้านบาท และมีโครงการคู่ขนานที่ใหญ่มากร่วมกันระหว่างหน่วยงานด้านกลาโหมกับ สกว. (สำนักงานกองทุนสนับสนุนการวิจัย) งบรวม 100 ล้านเวลาอีก 10 ปีกับโครงการยานบินไร้คนบังคับ (UAV) ซึ่งทั้งสองโครงการร่วมระบบโทรคมนาคมมีผู้เล่นจากหลายสถาบันจำนวนมากแต่มีจุดสิ้นสุดที่ไม่ต่างกัน กลายเป็นประสบการณ์ของประเทศด้านการวิจัยและพัฒนาระบบโทรคมนาคมที่ควรค่าแก่การศึกษาเป็นอย่างยิ่ง รวมไปถึงโครงการขนาดใหญ่ด้านการสื่อสารไร้สายชุมชน (Wireless Local Loop: WLL) ก็อีกหนึ่งงานที่ยังไม่ได้มีการประมาณตัวเลขงบประมาณแต่ไม่สัมฤทธิ์ผลตามความคาดหวังถึงการพึ่งพาตนเองได้ทุกโครงการทั้งหมด (แม้จะได้ผลลัพธ์เชิงวิชาการหรือต้นแบบอื่น ๆ จำนวนมาก)

ดังนั้นก่อนที่จะมีการเริ่มโครงการใหญ่ในอนาคตอีกเช่นโครงการศูนย์ทดสอบฯ (testbed) ด้านรหัสลับเชิงควอนตัมนี้ จึงควรได้เห็นภาพสะท้อนจากอดีตงานวิจัยที่ออกมากับสองคำสำคัญหลักคือ การเข้าจังหวะ (synchronization[35]) ของเทคโนโลยีที่ต่างและบุคลากรที่แตกความถนัด รวมทั้งอัตตลักษณ์ของงานระบบโทรคมนาคมที่เป็นกลุ่มสหสาขาและมีมาตรฐานมาค้ำ (OSI effect[34]) ที่มีความแตกต่างของส่วนงานมากต้องอาศัยการทำงานเป็นทีมที่สามารถรวมความแตกต่างสูงมากทั้งปริมาณ เทคนิค และการบูรณาการอดีตที่ผ่านมา งานวิจัยแบบเดี่ยวชิ้นเล็กในประเทศมีประสบผลสำเร็จในหลายระดับมามากมาย แต่เมื่อเป็นระบบโทรคมนาคมแม้ผลกระทบสูงนั้นแต่ก็มีความแตกต่างมากในชั้นงานที่ไม่สามารถปฏิบัติได้โดยลำพังเช่นงานเดี่ยวขนาดเล็ก โครงการใหญ่ตัวอย่างดังกล่าวคือบทเรียนดียิ่งที่หากทั้งเป้าหมายกับความคาดหวังของผู้สนับสนุนและสังคมผิดไกลไปจากความเข้าใจกันเรื่อง synchronization และ OSI effect ที่มีความหลากหลายแตกต่างและต้องจัดการให้เข้ากันได้นั้น บทสรุปก็อาจเสียของหรือลงทุนเสียเปล่าได้ (*คาดหวังผลจากโครงการใหญ่โทรคมนาคมหลายระดับงานด้วยเกณฑ์เดียวกันกับระดับงานเดี่ยว*) อีกทั้ง เทคโนโลยีโทรคมนาคมอายุไม่ยืนยาว เปลี่ยนแปลงด้วยความรวดเร็ว เช่น วิทยุติดตามตัว โฟนพ้อยท์ (Phone Point) หรืออุปกรณ์สื่อสารยุคใหม่อื่น ๆ ที่แม้ประสิทธิภาพสูงขึ้นแต่กลับตกยุคไวขึ้น จึงเป็นปัจจัยเสี่ยงที่แฝงร่วมอยู่ด้วยเช่นกันกับงานวิจัยและพัฒนาโทรคมนาคม

รวมทั้งเป็นที่น่าเสียดาย หน่วยงานในอดีตที่กำเนิดขึ้นมาเพื่อการรวมกลุ่มสร้างงานเป็นระบบโทรคมนาคมโดยเกี่ยวข้องกับทั้ง synchronization และ OSI effect นั้นคือ TRIDI (สถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.)) ที่ต้องถูกยุบเลิกไปกับภาวะทางการเมืองในอดีต งานวิจัยและพัฒนาแบบทีมโทรคมนาคมในประเทศจึงยังคงไม่มีเกณฑ์เพื่อการเฉพาะต่อไป

บทสรุปที่ผ่านมาของประเทศได้มีบทเรียนงานวิจัยโทรคมนาคมไทยที่ชัดเจนกับเรื่อง"**จุดมวลวิกฤติที่ไปไม่ถึง**"ซึ่งก็ต้องวนกลับมาเริ่มใหม่ซ้ำ ๆ เมื่อดูเหตุปัจจัยพื้นฐานทั้งสี่ ก) บุคลากร ข) งบประมาณ ค) วิทยาการและ ง) นโยบายที่ขาดแคลนยิ่ง จึงจำเป็นต้องจัดซื้อหรือพึ่งพาจากต่างประเทศต่อไป แต่โดยทั้งนี้ มีข้อสังเกตที่สัมพันธ์กับภาคส่วนผู้เกี่ยวข้องกับการพัฒนาระบบโทรคมนาคมดังนี้

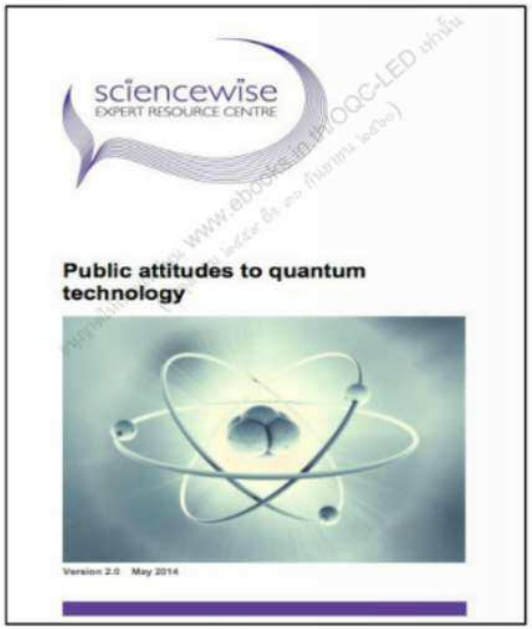
- ***ภาคการศึกษาวิจัยและพัฒนาบุคลากร*** หากมีการประยุกต์กติกาการเรียนการสอน การวิจัยและพัฒนาแบบทั่วไปที่ใช้กับงานเดี่ยวต่อโจทย์ด้านระบบโทรคมนาคมแบบที่เป็นทีม*ต่างระดับขนาดใหญ่และนาน* การลดน้อยถอยลงจึงได้เกิดขึ้นกับทั้งนักศึกษาที่เลือกเรียนสาขานี้ รวมถึงประชากรวิจัย นักวิชาการและผลงานตัวชี้วัดที่จะใช้ยกระดับการแข่งขันของประเทศ โดยหนีเคลื่อนย้ายไปสู่งานประเภทเดี่ยว เล็กหรือเห็นผลได้เร็วแทน ซึ่งภารกิจด้านวิทยาการสาขาใหม่ในอนาคตหรือรหัสลับเชิงควอนตัมของโครงการนี้ก็จะประสบอุปสรรคการขาดแคลนบุคลากรเป็นที่แน่นอน ดังนั้น จึงต้องเร่งรัดชักชวนทุกภาคส่วนทั้งการศึกษาและการวิจัยและพัฒนาให้กลับเข้าร่วมกับแนวทางสำคัญของอนาคตให้มากที่สุดและเป็นการด่วน แนวทางหนึ่งนั้นคือการลงโครงสร้างพื้นฐานโดยเพื่อให้มีสนามการศึกษาและวิจัยรองรับดังเช่นงานสร้างศูนย์ทดสอบฯ (testbed) ของโครงการนี้

---

35 Synchronization คือการเข้าจังหวะรองรับทุกส่วนงานของระบบสื่อสารทั้งฮาร์ดแวร์และซอฟต์แวร์กับความเร็วที่สอดคล้องกัน หากหลุดหรือไม่ซิงค์ การสื่อสารจะเกิดความผิดพลาด กรณีระบบงานของมนุษย์ความหมายคล้ายกันคือ "ขาดความสอดคล้อง"

34 OSI (Open System Interconnection) effect ผลเพื่อนเคียงของเจ็ดระดับงานที่แตกต่างตามมาตรฐานที่ต้องการความสอดคล้องกัน ไม่สามารถทดแทนด้วยการเพิ่มระดับใดโดยลำพัง (เช่น ทีมวิ่งเดี่ยวมีทุกคน มีความถนัดวิ่งในระดับใกล้กันเปลี่ยนตัวทดแทนได้สะดวกกว่า แต่ทีมวอลเลย์บอลทุกคนมีตำแหน่งถนัดและกติกาอื่นที่ต่างไปมาก ไม่สามารถนำเกณฑ์ของทีมวิ่งเดี่ยวมาใช้ได้อย่างมีประสิทธิภาพ) เช่นกัน งานวิจัยด้านโทรคมนาคมที่มีรีโกลหรือยากสูง กำลังคนมากและเวลาร่วมเป็นระบบนาน ตกยุคเร็ว ซึ่งต้องการ "การเข้าจังหวะเจ็ดระดับต่าง" เป็นสำคัญ หากใช้กติกาเดี่ยวก็จะเกิดเช่นเดียวกับงานโครงการวิจัยขนาดใหญ่ในอดีต

- **ภาคอุตสาหกรรม** มีสัญญาส่งมอบคุณภาพการบริการในภาวะธุรกิจที่แข่งขันสูงกับช่วงอายุเทคโนโลยีที่สั้น รวมทั้งรายได้ที่ก็ต้องแข่งกับรายจ่ายสัมปทานที่สูงเช่นกัน ดังนั้น การขอยอมซื้อโดยสมบูรณ์จึงเป็นทางเลือกสุดที่เสี่ยงน้อย งานวิจัยในภาคเอกชนโทรคมนาคมไทยจึงยังคงเป็นเป้าหมายที่ไกลเกิน โดยเรื่องการประมูลระบบโทรศัพท์ยุคที่สาม (3G) ที่ประสบปัญหายาวนานจนถึงยุคที่สี่ (4G) และสัมปทานดิจิทัลทีวี คือตัวอย่างล่าสุดของประเทศผู้ซื้อแบบไทยที่ไม่สามารถพึ่งพาตนเองได้และเป็นเพียงปัญหาของธุรกิจการให้บริการเท่านั้น ไม่มีส่วนใดเกี่ยวข้องกับพัฒนาการหรือความก้าวหน้ามีส่วนพึ่งพาเทคโนโลยีภายในประเทศแต่อย่างใดเลย หากยังไม่มีหน่วยงานที่สามารถเชื่อมโยงภาคอุตสาหกรรมให้เข้าสู่วงการวิจัยได้ด้วยตนเอง (เช่น SK telecom ของประเทศเกาหลี) โอกาสที่จะพึ่งพาตนเองด้านสานสนเทศเชิงควอนตัมในอนาคตก็จะน้อยมากเช่นกัน จะคงเหลือเพียงมุมการศึกษาและติดตามความก้าวหน้าของตัวเทคโนโลยีเองดังข้อสังเกตของ**ภาคการศึกษาวิจัยและพัฒนาบุคลากร** เท่านั้น



ช.6 แนวทางอนาคตที่เหมาะสม: พัฒนาบุคลากรและสนามทดสอบ

จากคาดการณ์อนาคตเทคโนโลยีและแนวทางต่าง ๆ ร่วมกับข้อมูลพัฒนาการของต่างประเทศ และประสบการณ์ที่เกี่ยวข้องในอดีตของประเทศไทยดังที่ได้นำเสนอมาแล้วนั้น จึงจะนำมาสู่การเลือกสรรแนวทางที่เหมาะสมสำหรับรองรับเทคโนโลยีสาขาใหม่ที่มากับวิทยาการรหัสลับเชิงควอนตัม

ซึ่งก่อนการประมวลผลยังมีข้อสังเกตประเด็นใหญ่อีกกรณีหนึ่ง นั่นคือ ภาคสังคมไทยยังได้พบกับเรื่อง "ควอนตัมหลอกลวง" หรือ fraud เช่น *"เครื่องสำอางยี่ห้อควอนตัม กระติกน้ำสะสมพลังงานลึกลับเชิงควอนตัม กิจกรรมกายภาพช่วยรักษาผู้ป่วยด้วยเหรียญควอนตัม จนถึงดาวเทียมควอนตัม (quantum satellite) งานวิชาการของนักวิจัย นักวิทยาศาสตร์แนวประหลาดในหลากสาขาทั้ง วงจรไฟฟ้าควอนตัมตามใจนึก (quantum cost) เก็บกุญแจรหัสควอนตัมไว้ใช้คำนวณงานภายหลัง (quantum key) แม้กระทั่งสถานะควอนตัมขึ้นไปอยู่ในเครือข่ายโทรศัพท์เคลื่อนที่ (quantum key on mobile)"* เป็นต้น ซึ่งทั้งหมดข้างต้นนี้มิได้เกี่ยวข้องอะไรกับกลศาสตร์ควอนตัม (quantum mechanics) ศาสตร์แขนงหนึ่งในสาขาฟิสิกส์อันเป็นวิทยาศาสตร์ที่มนุษย์รู้จักเป็นทางการมาเกือบหนึ่งร้อยปีแล้ว (ค.ศ.1925) ในวงการวิทย์เรื่องเหล่านั้นส่งผลไม่สู้ดี แต่มีมากมายจนเกิดเป็นอุปสรรคที่ต้องแก้ไขกันทั่วโลก และมาจนนำหน้าเรื่องจริงไปไกลแล้ว แม้ในประเทศพัฒนาแล้วแหล่งกำเนิดที่ยุโรปเองก็เกิดทั้งกรณีหลอกลวง (fraud) หรือหลงไปกับคำว่าควอนตัมมากเช่นกัน

แม้ในขณะที่มีสินค้าและข่าวเรื่องสารสนเทศเชิงควอนตัมของจริงปรากฏมากเช่น กูเกิล (Google) แถลงเมื่อปลายปีพ.ศ. 2558 ว่าควอนตัมคอมพิวเตอร์ทำงาน (บางกรณี) ได้เร็วกว่าเครื่องธรรมดาร้อยล้านเท่า หลายบริษัทยักษ์ใหญ่ก็ทุ่มทุนสร้างเร่งแข่งขันกัน ส่วนโครงข่ายการสื่อสารเชิงควอนตัมก็ปรากฏตัวมากขึ้นจากยุโรปสู่ญี่ปุ่น ฯลฯ มีเครื่องมืออุปกรณ์ไอที่ออกมาขายจากหลายผู้ผลิตเป็นทางการ ก็มิได้ทำให้ "ควอนตัมหลอกลวง" ทั้งด้านวิชาการสินค้าและบริการที่เกี่ยวข้องกับชื่อควอนตัมลดลงแต่อย่างใด

ขณะที่ในประเทศไทยก็พบมากเช่นกันทั้ง กรณีวงการศึกษาและวิจัยที่หลงไปจินตนาการเองโดยปราศจากวิชาการรองรับและด้วยเหตุปัจจัยซ่อนเร้น การพลาดจากความเข้าใจผิวเผินแล้วตีความต่อเอง หรือติดหมุกไปกับความเชื่อละทิ้งแนวทางวิทยาศาสตร์ จนถึงการพ่วงชื่อใช้ไปกับสินค้าบริการก็มีมาก[55]

กรณี "ควอนตัมหลอกลวง" ในประเทศเหล่านี้ สอดคล้องกับรายงานหน่วยงาน"Sciencewise" ด้วยการสนับสนุนจากรัฐบาลสหราชอาณาจักร โดยกรมธุรกิจ นวัตกรรม และทักษะงาน (Department for Business, Innovation and Skills: BIS) ซึ่งได้ให้แนวทางที่สอดรับกันดังที่จะสรุปต่อภาคท้ายนี้คือ "Sciencewise" ได้สำรวจความคิดเห็นหรือผลกระทบทางสังคมจริยธรรมและเทคโนโลยีการรับรู้ของเทคโนโลยีนี้ ต่อความเข้าใจอันต่างจากเทคโนโลยีด้านอื่น ๆ ที่ผ่านมา โดยประเมินความคิดเห็นของประชาชนพบว่า การจะปรากฏตัวขึ้นของเครื่องมือควอนตัมขึ้นนปลกใหม่และมีประสิทธิภาพสูงมากในอนาคตนั้น จะมาควบคู่กับความลึกลับที่ยังคงเป็นปริศนาหรือยากต่อความเข้าใจอยู่ต่อไป

55 *http://www.dailynews.co.th/article/DQC_slash_LED (ควอนตัมหลอกลวง)*

ในรายงานยังระบุด้วยว่าการลงทุนของภาครัฐและเอกชนแข็งแกร่งขึ้นอย่างมาก เทคโนโลยีควอนตัมในทางปฏิบัติได้ขยับเข้ามาใกล้ตลาดหรือพร้อมขายกว่าที่เคยเป็น กระนั้น ก็ยังคงมากับรายงานอีกด้านหนึ่งเรื่องความเข้าใจหรือความยุ่งยาก

รายงานนี้ยังมีการคาดการณ์ประเด็นสำคัญที่ได้เสนอต่อรัฐบาล (สหราชอาณาจักร) ไว้ให้คิดทำการต่อด้วยคือ *"ในอนาคตอันใกล้มีโอกาสสูงมากที่เทคโนโลยีควอนตัมจะส่งผลกระทบอย่างมีนัยสำคัญต่อทั้งเรื่อง สุขภาพ การป้องกันความเป็นส่วนตัวในโลกออนไลน์ และผลกระทบกับสิ่งแวดล้อม* ***จึงดูเหมือนว่าจะมีความจำเป็นเร่งด่วนที่จะต้องปรับปรุงความเข้าใจของสาธารณชนจากความหลงใหลที่มีอยู่กับปรากฏการณ์ที่น่าแปลกประหลาด (และน่าทึ่ง) ของทฤษฎีควอนตัม มาสู่คำถามเพื่อการเตรียมพร้อมด้านจริยธรรมและสังคมวิทยา (ethical and sociological) ที่จะตามมา"***

เช่นเดียวกัน แม้ประเทศไทยจะมีฐานความรู้ด้านไอทีควอนตัม (quantum information) ห่างไกลจากต้นกำเนิดมาก ไม่สามารถสร้างผลงานวิจัย ผลิตสินค้าหรือบริการที่เกี่ยวข้องขึ้นได้เองในประเทศอย่างเป็นรูปธรรม แต่ก็สามารถจะป้องกันผลลบ การสูญเสีย หรือทัศนคติที่จะทำให้ความก้าวหน้าด้านนี้ล้าหลังไปกว่าเดิมได้ โดยสามารถช่วยกันสื่อสารอย่างเหมาะสมกับไอทีควอนตัมแนววิทยาศาสตร์จากทั่วโลก เพื่อลดการหลงรู้แต่หลบกลบข้อผิดพลาดและการติดบ่วงห่วงชื่อสินค้าในสังคมไทยโดยสำคัญ และเหตุที่ประเด็น "ควอนตัมหลอกลวง" นี้มีความสำคัญเพราะหากเมื่อใดกลศาสตร์ควอนตัมถูกอ้างอิงหรือแปลงใช้เป็นกิจกรรมทางสังคม วัฒนธรรมหรือประเพณีอันมีความสวยงามทางจิตวิญญาณจนกลายเป็นความเชื่อฝังลึกแบบเรื่องอื่น ๆ ในสังคมไทยไปมากแล้ว ก็จะยิ่งแก้ไขได้ยากเนื่องจาก ***"การกลับมาแก้ไขความเข้าใจที่ผิดทิศทางไปแล้ว จะลำบากมากกว่าการปูพื้นวิทยาศาสตร์ที่ถูกต้องตั้งแต่แรก"***

ทั้งหมดนี้ จึงเป็นเหตุสอดคล้องที่โครงการนี้จะให้ความสำคัญเร่งด่วนกับที่ภาคการศึกษาวิจัยและพัฒนาบุคลากร ดังนั้น แนวทางอนาคตที่เหมาะสมสำหรับประเทศไทยจึงควรมุ่งเป้าดังกล่าวกับกิจกรรมเพื่อการพัฒนาสร้างบุคลากรและการสร้างสนามเพื่อได้ใช้ทดสอบ ทดลอง ศึกษา ดูงาน รวมทั้งเพื่อการเตรียมพร้อมด้านจริยธรรมและสังคมวิทยาดังกล่าวข้างต้น และอื่น ๆ ซึ่งเป็นที่มาของ**พันธกิจ (Mission):**

"สังคมมีความรู้ความเข้าใจ ตระหนักต่อเทคโนโลยีวิทยาการสารสนเทศเชิงควอนตัมและที่เกี่ยวข้อง พร้อมรับกับการเปลี่ยนแปลง"

ข.7 จากแนวทางเดิมสู่ศูนย์ทดสอบฝึกอบรมและถ่ายทอดฯของประเทศ

หากพิจารณารวมทุกกรณีของพัฒนาการวิทยาการรหัสลับควอนตัมโลกบนปัจจัยสำคัญสี่ประการพื้นฐานนั้นแล้ว สามารถสรุปโดยย่อได้ดังนี้คือ

สหรัฐอเมริกา: *"นโยบาย งบประมาณ บุคลากร พร้อมวิทยาการสะสมนำหน้าและพัฒนาต่อเนื่อง"*
ยุโรป: *"รวมนโยบาย รวมงบประมาณ บุคลากรรวมทีมระหว่างประเทศ พร้อมวิทยาการที่ได้สั่งสมมานาน"*
ญี่ปุ่น *"นโยบายนำกับแผนถึงสี่สิบปี งบประมาณพร้อม บุคลากรและวิทยาการก็สั่งสมสร้างเองได้ทั้งหมด"*
จีน: *"นโยบายนำ งบและบุคลากรมาก วิทยาการได้ศึกษาถ่ายทอดจนสามารถพึ่งพาตนเองและก้าวหน้า"*
สิงคโปร์: *"นโยบายนำ งบประมาณพร้อม ส่วนบุคลากรกับวิทยาการนำเข้าจากต่างประเทศ"*
เกาหลีใต้: *"นโยบายนำ งบประมาณพร้อม บุคลากรเร่งสร้าง วิทยาการเรียนรู้จากต่างประเทศ"*

ตัวอย่างทั้งหมดนี้ก็เพื่อชี้เป้าการพัฒนาของต่างประเทศที่มีปัจจัยสำคัญหลักร่วมกันชัดเจนประการหนึ่งคือ "นโยบายที่สนับสนุน" แม้บางประเทศจะขาดหลายปัจจัยอื่น เช่น สิงคโปร์ แต่ก็ขยดเขยได้ด้วยแรงผลักดันเต็มกำลังของหรือนโยบายระดับประเทศที่นำพาไปนั่นเอง

สำหรับการพัฒนาไอทีควอนตัมของไทย โดยรวมยังคงอยู่ในระดับพื้นฐานหรือการเริ่มต้นขาดแคลนทุนปัจจัยดังกล่าว (*งบและคนไม่เพียงพอ วิทยาการตามหลังและขาดนโยบายหรือแผนที่นำทางของประเทศ*) จึงมีความเป็นไปได้แนวทางเดียว นั่นคือ*การศึกษาและพัฒนาบุคลากรเพื่อการติดตามความก้าวหน้าของโลกและการเตรียมตัวเป็นผู้ซื้ออย่างฉลาดในอนาคต* [36] ซึ่งจะสอดคล้องกับภาคสำรวจที่ได้บทสรุปไว้ก่อนหน้าดัง **ข. 6 แนวทางอนาคตที่เหมาะสม: พัฒนาบุคลากรและสนามทดสอบ** ที่ควรมุ่งเป้ากับกิจกรรมเพื่อการพัฒนาสร้างบุคลากรและการสร้างสนามเพื่อได้ใช้ทดสอบ ทดลอง ศึกษา ดูงาน รวมทั้งเพื่อการเตรียมพร้อมด้านจริยธรรมและสังคมวิทยาดังกล่าวนั้น จึงเป็นที่มาของข้อเสนอโครงการ "ศูนย์ทดสอบ ฝึกอบรมและถ่ายทอดเทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัม (Thai Quantum Cryptography Testbed)"[37] [38] นี้

โ ดยที่ผ่านมา เคยได้มีการจัดทำข้อเสนอโครงการ "ศูนย์กลางการทดสอบการใช้งาน การวิจัยและการพัฒนาด้านวิทยาการรหัสลับเชิงควอนตัมของประเทศ" (Thai Quantum Cryptography Testbed) นำเสนอครั้งแรกเมื่อปีพ.ศ.2551 ต่อคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.) ในอดีต โดยได้มีการนำเสนอข้อเสนอโครงการระยะที่ 1 (ภายหลังหลังเหตุการณ์ 19 กันยายน พ.ศ.2549) และแม้ต่อมามีการนำเสนออีกสองครั้งโดยคุณวุฒิและคณะ

36 บทพิจารณ์และข้อเสนอ : สารสนเทศเชิงควอนตัมในประเทศไทย: พัฒนาการด้านวิทยาการรหัสลับ ถดถอยสู่อนาคต (พ.ศ.๒๕๕๗) ISBN 9786163748300

37 อย่าง ข้อมูลเพิ่มเติมเรื่องความสำคัญของการพัฒนาบุคลากรด้วยการสร้างสนามทดสอบงานวิจัยนี้ประเด็นที่น่าสนใจจาก ของ ชี (Solmaz Rhee) รอง ผอ.ด้านงานระบบไซเบอร์และอินเทอร์เน็ตทุกระดับของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (NIST) กล่าวไว้เมื่อปลายปีพ.ศ.2557 ในแนวว่ารัฐบาลหรือผู้กำกับนโยบายสามารถช่วยเหลือกับกิจกรรมใหม่ๆ ในสี่ทางได้ คือ "ปัจจัยที่สาม" ซึ่งก่อให้เกิดบ่วงควบของรัฐฯ เคยกับสองอย่างที่ทำมานานแล้วทั้ง "ให้ทุนวิจัยและกำกับกฎเกณฑ์ต่าง (funding and regulation)" หากเพิ่มโอกาสกับการสร้างสนาม (testbed/ playground) จะทำให้เหล่านักวิจัย วิศวกรทั้งหลายมีช่องทางนำความคิดมาลองสร้างจริงได้ (access to infrastructure is one way to give engineers a true testing ground for their ideas) ซึ่งการนำเข้นแนวคิดที่สามนี้ก็กำลังเห็นผลกับโครงการเน็ตอีซีอะ(ริง)ที่สหรัฐฯ (ฯลฯ) หากรัฐฯ ไม่ลงทุนกับงานฐานรากหรือสนามขนาดใหญ่ เอกชนหรือนักวิจัยและชาวบ้านคงไม่สามารถลงมือทำได้เองเพราะเกินตัวทั้งงบประมาณและความรับผิดชอบ งานวิจัยก็จะเรียบวนกลับไปในสองขั้นตอนเดิม)

38 โดยควอนตัมของรัฐฯ วางกลยุทธ์เพื่อขับเคลื่อนแผนที่นำทางของ"ระบบสารสนเทศเชิงควอนตัม (QIS: Quantum Information System)" ให้สำเร็จตามเป้าหมายที่ตั้งไว้ จากนโยบายการพัฒนาวิทยาศาสตร์และเทคโนฯ ให้นั้น มีปัจจัยหลักหนึ่งคือ ***การจัดตั้งศูนย์ทดสอบ (Testbed)*** พร้อมไปกับการดำเนินงานตามวิสัยทัศน์ของสภาวิทยาศาสตร์และเทคโนโลยี (National Science and Technology Council) ที่ก่อตั้งสภานับของรับใช้เพื่อบริหารจัดการและพัฒนาบุคลากร QIS เหล่านั้นอีกด้วย

กรรมการบริหาร (บอร์ด) กทช. ในขณะนั้นแล้วก็ตาม แต่ในปี พ.ศ.2553 มีการการเปลี่ยนโครงสร้างจาก กทช. เป็น กสทช. (คณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ) รวมกับการเปลี่ยนแปลงภาคการเมืองและนโยบายก่อนหน้าและต่อ ๆ มาตลอดระยะเวลา 8 ปี จึงทำให้โครงการนี้ต้องหยุดชะงักลง อันเป็นการเสียโอกาสของประเทศไปรวมถึงทรัพยากรที่ได้ลงทุนก่อนหน้านั้นแล้วทั้งครุภัณฑ์ บุคลากร เวลา รวมทั้งโอกาสติดตามเทคโนโลยีความก้าวหน้าของโลกซึ่งล้ำลงไปกว่าเดิมมาก โดยทีมงานนักวิจัยและบุคลากรที่เกี่ยวข้องได้พยายามรักษาสถานะภาพ องค์ความรู้และความพร้อมทุกด้านเพื่อให้มีโอกาสฟื้นกลับมาเริ่มต้นใหม่อีกครั้ง

ณ ปัจจุบัน (พ.ศ. 2559) โครงการได้เริ่มกลับมาขับเคลื่อนงานส่วนย่อยด้านการพัฒนาบุคลากรแล้ว ซึ่งยังคงต้องได้รับการผลักดันอย่างต่อเนื่องและการสนับสนุนจากทุกฝ่ายที่เกี่ยวข้องเพื่อให้กลับเข้าสู่การสร้างเป็น "ศูนย์กลางการทดสอบการใช้งาน การวิจัยและการพัฒนาด้านวิทยาการรหัสลับเชิงควอนตัมของประเทศ" (Thai Quantum Cryptography Testbed) ดังวัตถุประสงค์ของโครงการนี้ได้ จึงทำการปรับปรุงและกำหนดวิสัยทัศน์ (Vision) ของข้อเสนอโครงการใหม่อันสอดคล้องกับสภาพปัจจุบัน ดังนี้

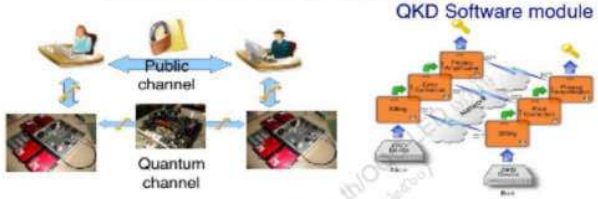
"การเป็นศูนย์กลางการทดสอบ การใช้งาน การวิจัยและพัฒนาด้านการสื่อสารปลอดภัย การสื่อสารเชิงแสง และวิทยาการรหัสลับเชิงควอนตัมของประเทศไทย"

ภาคผนวก ค)

ผลงานหลักในอดีต

QKD based on entangled photon

(ปรากฏการณ์ควอนตัมพื้นฐาน)



ความเข้าใจ การสื่อสารสาธารณะ (Pending 2015)

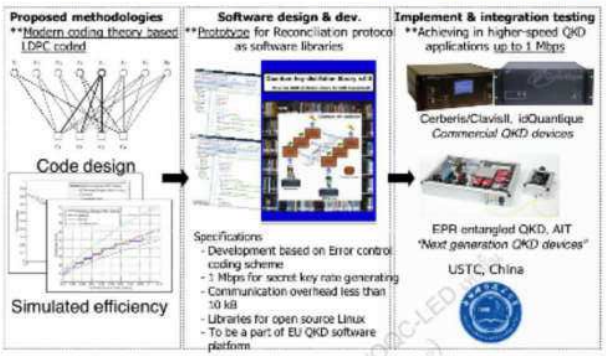
Quantum Random Number Generator & Randomness Testing Service (ThaiRand) platform

Applications:
Scientific Research & Industrial Burst Test
PIN or ID for one time password
SecureCommunications

บริการทั่วไป (Expired 2015)

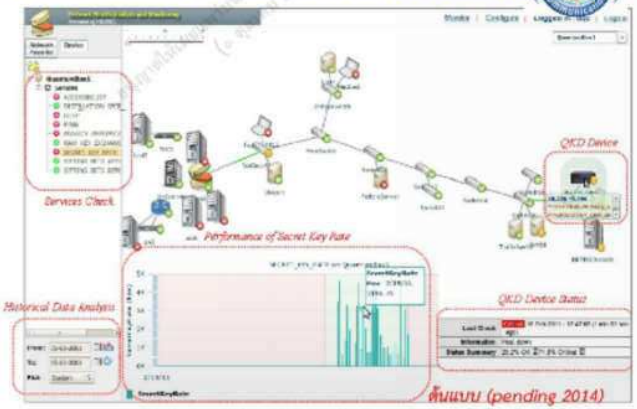
API software platform for reconciliation protocol

Error control coding (Turbo/ LDPC) for QKD



ต้นแบบ (pending 2014)

q-NetHam (Q. Network Monitoring and Analysis)



ต้นแบบ (pending 2014)

สถานระดับประเทศ (Pending 2011)

ค.ศ.2006 (พ.ศ. 2549)
โครงการวิจัย ลำดับที่ 1: การจำลองออกแบบการประมวลผลสัญญาณ สำหรับระบบวิทยาการรหัสลับเชิงควอนตัม (การสาธิตและการติดตั้งอุปกรณ์ระยะแรก) ด้วยทุน AIT's RTG Joint Research Project, Fiscal Year Budget 2004 ผ่านสถาบันเทคโนโลยีแห่งเอเชีย (AIT)

โครงการระบบวิทยาการรหัสลับเชิงควอนตัม : ต้นแบบ ชุดกระจายกุญแจรหัสลับเชิงควอนตัม (QC – BB84) โดยงบประมาณของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สวทช.

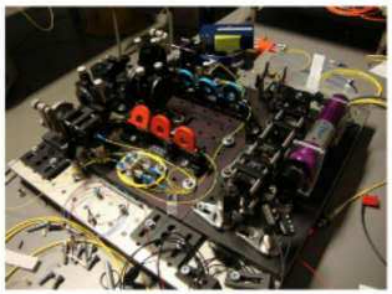
ค.ศ.2008 (พ.ศ. 2551)
นำเสนอโครงการ "ศูนย์กลางวิจัยและพัฒนา ฝึกอบรม และถ่ายทอดเทคโนโลยีระบบวิทยา การรหัสลับเชิงควอนตัม: ระยะที่ 1" (Thai Quantum Cryptography Testbed Center: Phase I) ต่อคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.) - ต่อมา กทช. เปลี่ยนเป็น กสทช. (ไม่ได้รับการแจ้งการดำเนินการต่อใด ๆ)

ค.ศ.2010 (พ.ศ. 2553)
เปิดให้บริการแหล่งกำเนิดจำนวนสุ่มเชิงควอนตัมและการทดสอบ (Web service : Quantum Random Number Generation and Testing Service)

ค.ศ.2013 (พ.ศ. 2556)
โครงการวิจัย การพัฒนาโพรโทคอลใกล้เกลี่ยความผิดพลาดประสิทธิภาพสูง สำหรับระบบกระจายกุญแจรหัสลับเชิงควอนตัม (High Efficiency Key Reconciliation Protocol for Quantum Key Distribution) ทุนอุดหนุนการวิจัยพัฒนา และวิศวกรรมจากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

(ชุดกระจายกุญแจรหัสลับ IDQuantiques)

(ชุดสร้างคู่โฟตอนพัวพัน (BBO Entanglement: EPR)



ภาคผนวก ง)
Thai Quantum Information Forum (Q-Thai.Org)

(version 1.0)

แนวทางการดำเนินงาน

กลุ่มวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย (๒๕๕๙ - ๒๕๖๔)

(Thai Quantum Information Forum 2016 - 2021)

โดย

สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคม และสารสนเทศ (ECTI)

และ

ชมรมไฟฟ้าสื่อสาร (IEEE ComSoc Thailand chapter)
สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE Thailand Section)

สนับสนุนเทคนิค
ศูนย์ความเป็นเลิศด้านฟิสิกส์ (Thailand Excellence Center in Physics)

1. เกริ่นนำ

"สารสนเทศเชิงควอนตัม (quantum information) คือ ศาสตร์ที่ศึกษาและประยุกต์ใช้พฤติกรรมของกลศาสตร์ควอนตัมเพื่องาน สารสนเทศหรือข่าวสาร เพื่อใช้ในการสื่อสาร การคำนวณและอื่น ๆ ให้ได้มาซึ่งรูปแบบใหม่ในการสื่อสาร การคำนวณและอื่น ๆ ที่สอดคล้องซึ่งไม่มีอยู่ในการสื่อสารและการคำนวณแบบดั้งเดิม โดยวิทยาการสารสนเทศควอนตัม (quantum information science) เป็นการรวมความรู้สามสาขาเข้าด้วยกัน ได้แก่ ทฤษฎีสารสนเทศหรือข่าวสาร (information theory) ซึ่งอธิบายขีดจำกัดของการสื่อสารดั้งเดิม วิทยาการคอมพิวเตอร์ที่ใช้อธิบายกระบวนการคำนวณหรือประมวลผล และฟิสิกส์ควอนตัม โดยใช้เพื่ออธิบายพฤติกรรมของอนุภาคที่นำมาใช้เป็นตัวสื่อ"

สารสนเทศเชิงควอนตัม กำเนิดขึ้นจากการนำหลักการของ"กลศาสตร์ควอนตัม (quantum mechanics)" มาประยุกต์ใช้งานกับ"เทคโนโลยีสารสนเทศ (information technology)" โดยมีเป้าประสงค์เพื่อการได้มาซึ่งระบบที่มีขนาดเล็กลง เร็วขึ้น นำมาประยุกต์ใช้ตอบสนองความต้องการของมนุษย์ได้มากขึ้น ดังนั้น สารสนเทศเชิงควอนตัมจะเกี่ยวโยงกับอุปกรณ์ (devices) การสื่อสารข้อมูล (communications) และการประมวลผลของข้อมูล (computing) อันจะเกิดเป็นแขนงวิชาหรือวิทยาการใหม่ เมื่อทั้งสามสาขาย่อยนี้นำมาพัฒนาร่วมกันกับกลศาสตร์ควอนตัมเกิดเป็น อุปกรณ์เชิงควอนตัม (quantum devices) การสื่อสารข้อมูลเชิงควอนตัม (quantum communications) และการคำนวณเชิงควอนตัม (quantum computing) ที่มีประโยชน์กับระบบสารสนเทศยุคใหม่และมีประสิทธิภาพสูงขึ้นอย่างมากซึ่งไม่เคยปรากฏมีมาก่อน

เทคโนโลยีสารสนเทศเชิงควอนตัม (quantum information technology) คือ การประยุกต์ใช้คุณสมบัติเชิงควอนตัมที่สามารถอธิบายปรากฏการณ์ของวัตถุที่มีขนาดเล็กระดับอะตอมเข้ากับสารสนเทศในปัจจุบัน เช่น การสื่อสาร การคำนวณ การเก็บข้อมูล การเข้ารหัสลับ เป็นต้น โดยสารสนเทศเชิงควอนตัมได้รับความสนใจจากทั่วโลกโดยเฉพาะอย่างยิ่งการคำนวณเชิงควอนตัม (quantum computing) และวิทยาการรหัสลับเชิงควอนตัม (quantum cryptography) ซึ่งการคำนวณเชิงควอนตัมเป็นการคำนวณในรูปแบบที่แตกต่างจากเดิม โดยการคำนวณเชิงควอนตัมจะมีข้อมูลแบบบิต "0" และ "1" เกิดได้พร้อมกัน เรียกว่า สถานะซ้อนทับทางตำแหน่ง ซึ่งจากคุณสมบัติการซ้อนทับทางตำแหน่งนี้ สามารถเพิ่มประสิทธิภาพในการประมวลผลในการแก้ไขปัญหาบางอย่างได้ดีกว่าการประมวลผลด้วยคอมพิวเตอร์ในปัจจุบัน ส่วนวิทยาการรหัสลับเชิงควอนตัมนั้นเป็นเทคโนโลยีที่สามารถป้องกันการดักขโมยข้อมูลกุญแจรหัสผ่านช่องสื่อสาร (ผ่านอากาศและเส้นใยนำแสง) ได้อย่างสมบูรณ์โดยการรับรองความปลอดภัยสูงสุดด้วยทฤษฎีพื้นฐานทางควอนตัมฟิสิกส์ เนื่องจากเมื่อมีการลักลอบอ่านข้อมูลผู้ส่งผู้รับจะทราบทันทีและแม้จะได้ข้อมูลไปในทางทฤษฎีแล้ว ข้อมูลนั้นจะไม่สามารถถูกถอดรหัสได้

สำหรับประเทศไทยเอง ได้เคยมีการรวมกลุ่มเฉพาะกิจบุคลากรที่สนใจด้านเทคโนโลยีสารสนเทศเชิงควอนตัมระหว่างสถาบันการศึกษาและสถาบันวิจัย เริ่มต้นเมื่อวันที่ 14 กุมภาพันธ์ พ.ศ. 2547 ภายใต้ชื่อกลุ่ม "กลุ่มวิจัยเทคโนโลยีสารสนเทศเชิงควอนตัมไทย (Thai Quantum Information Forum : Q-TI forum)" เพื่อเป็นศูนย์กลางในการแลกเปลี่ยนองค์ความรู้พื้นฐาน ระดมความคิดเห็น และแลกเปลี่ยนบุคลากรด้านเทคโนโลยีสารสนเทศเชิงควอนตัมและอื่น ๆ ที่เกี่ยวข้อง แต่ได้ลดบทบาทและกิจกรรมลงไปอย่างมากในช่วงถัดมา

ในขณะที่โดยรวม ประเทศไทยยังคงขาดแคลนทุกปัจจัยที่สำคัญของการพัฒนาทั้ง **บุคลากร งบประมาณ วิทยาการพื้นฐาน** และ**น โ ย บ า ย** ซึ่งจากรายงานการสำรวจก่อนหน้าได้ระบุว่าประเทศควรได้เร่งพัฒนาติดตามวิทยาการสาขาใหม่นี้ และแนวทางที่ควรเริ่มต้นให้เร็วที่สุดและสะดวกที่สุดควรเป็นการสื่อสารวิทยาศาสตร์ภาคสาธารณะ รวมทั้งการพัฒนาองค์ความรู้สู่บุคลากรที่มีอยู่ทั่วประเทศ กอปรผลกระทบมุมลบของสังคมที่ได้นำคำ

วิทยาศาสตร์"ควอนตัม"ไปใช้ในทางที่คลาดเคลื่อนอย่างกว้างขวางอันเป็นอุปสรรคอีกประการหนึ่งที่หนักมากต่อการพัฒนาบุคลากรดังกล่าวได้

ดังนั้น สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคม และสารสนเทศ (ECTI) จึงริเริ่มที่จะได้ร่วมกับหน่วยงานพันธมิตร จัดตั้งกลุ่มศึกษาวิจัยและพัฒนาสารสนเทศเชิงควอนตัมไทย (Thai Quantum Information Forum) ขึ้นมาใหม่ โดยได้เริ่มเผยแพร่กิจกรรมสาธารณะแล้ว (Q-Thai.Org) เพื่อสร้างโครงสร้างพื้นฐาน ส่งเสริม และพัฒนาการค้นคว้าวิจัยด้านเทคโนโลยีสารสนเทศเชิงควอนตัม ตลอดจนแสวงหาแนวทางการขยายความร่วมมือด้านบุคลากร การแลกเปลี่ยนเทคโนโลยี และอื่น ๆ กับต่างประเทศ อันจะเป็นการผลักดันงานวิจัยด้านเทคโนโลยีสารสนเทศเชิงควอนตัมในประเทศให้มีความพร้อมมากขึ้น และมีแนวทางการนำไปใช้ประโยชน์ร่วมกับเทคโนโลยีอื่น ๆ อย่างมีบูรณาการและเหมาะสมในอนาคตได้

2. คำสำคัญ (Key words) : *สารสนเทศเชิงควอนตัม กลศาสตร์ควอนตัม การคำนวณและการสื่อสารปลอดภัย แผนที่นำทางเทคโนโลยี และการสื่อสารวิทยาศาสตร์*

3. วัตถุประสงค์โครงการ (Objectives)

3.1 เพื่อติดตามความก้าวหน้าเทคโนโลยีสารสนเทศเชิงควอนตัมโลกเพื่อการวางแผนที่นำทางและแนวทางและการพยากรณ์อนาคตรองรับสำหรับประเทศไทย
3.2 เพื่อสร้างโครงสร้างพื้นฐาน พัฒนาบุคลากร สนับสนุนหลักสูตรการเรียนการสอนและงานวิจัยในประเทศ
3.3 เพื่อรวมกลุ่มและยกระดับการเรียนรู้สารสนเทศเชิงควอนตัมในสู่การวิจัยและพัฒนา และใช้งานสารสนเทศเชิงควอนตัมที่เหมาะสม
3.4 เพื่อส่งเสริม สนับสนุนการสื่อสารวิทยาศาสตร์ พัฒนาคุณภาพการศึกษายกระดับองค์ความรู้และถ่ายทอดองค์ความรู้สู่สังคม และเตรียมความพร้อมและทัศนคติที่ถูกต้องเหมาะสมสำหรับเทคโนโลยีที่จะอุบัติใหม่ในอนาคตของกลศาสตร์ควอนตัมเชิงสาธารณะ
3.5 เพื่อบูรณาการเสริมสร้างความเข้มแข็งและปรับใช้กับวิทยาการสาขาอื่น ๆ หรือด้านที่เกี่ยวข้อง เช่น มาตรวิทยา (quantum metrology) เป็นต้น
3.6 สร้างความร่วมมือระหว่างหน่วยงานต่าง ๆ ในประเทศ ทั้งภาคการศึกษา นโยบายและอุตสาหกรรมที่เกี่ยวข้อง เตรียมพร้อมรับการถ่ายทอดเทคโนโลยีอุบัติใหม่เพื่อสามารถต่อยอดองค์ความรู้สู่งานวิจัยในอนาคต

4. ขอบเขตการดำเนินงาน (Scope)
การบริหารงานในกลุ่มวิจัยร่วมฯดำเนินงานภายใต้**วิสัยทัศน์ (Vision)**

"ประเทศไทยมีเครือข่ายการสื่อสารเชิงควอนตัมระบบแรกใน 5 ปี และระบบการคำนวณเชิงควอนตัมแรกในอีกไม่เกิน 10 ปี"

โดยมีพันธกิจ (Mission)

- Infrastructure: จัดสร้าง ร่วมมือ ระดมทุน แบ่งปันโครงสร้างพื้นฐานและหน่วยปฏิบัติการเพื่อการสื่อสารและการคำนวณเชิงควอนตัม
- Human resource development: พัฒนาบุคลากร จัดหาและจัดสรรทุนการศึกษา งบวิจัย และพัฒนารับการถ่ายทอดเทคโนโลยี ร่วมงานและดึงดูดผู้เชี่ยวชาญจากต่างประเทศ
- Courses/ training/ visiting: ร่วมมือจัดทำหลักสูตร การเรียนการสอน สัมนา ฝึกอบรมและโครงงานวิจัยร่วมกับนักศึกษา นักวิจัย คณาจารย์ และบุคลากรภาคอุตสาหกรรมในประเทศโดยร่วมมือกับต่างประเทศ
- Homemade technology: แสวงหา ผลักดัน พื้นที่หรือมุมมองจุดแข็งงานวิจัยของตนเองให้ได้มีส่วนร่วมหรือบทบาทในระดับนานาชาติ

4.1 ขอบเขตหัวข้อเทคนิคพื้นฐาน

4.1.1 การสื่อสารและรหัสลับเชิงควอนตัม (Quantum Communication & Cryptography)
- การจัดตั้งเครือข่ายการสื่อสารปลอดภัยเชิงควอนตัมเพื่อเป็นสนามทางการวิจัย ทดสอบและพัฒนางานวิจัย (Infrastructure)
- การพัฒนาอุปกรณ์รหัสลับเชิงควอนตัมเพื่อการสื่อสารปลอดภัย
- ความร่วมมือของหน่วยงานภาคการศึกษา วิจัยและด้านความมั่นคง

4.1.2 การส่งถ่ายข่าวสารเชิงควอนตัม (Quantum Teleportation)
- การศึกษาและวิจัยเกี่ยวกับองค์ความรู้พื้นฐานด้านการส่งถ่ายข่าวสารเชิงควอนตัม เช่น คู่โฟตอนหัวพันเพื่อการสื่อสารเชิงควอนตัมและอื่น ๆ ที่เกี่ยวข้อง

4.1.3 การคำนวณเชิงควอนตัม (Quantum Computing)
- การศึกษาและวิจัยองค์ความรู้พื้นฐานด้านการคำนวนเชิงควอนตัม ด้วยแสง (โฟตอน) ควอนตัมดอท รวมทั้งอะตอมเย็น (cold atom) และอื่น ๆ
- การพัฒนาอุปกรณ์และเครื่องมือลดการนำเข้าและชุดทดลองเพื่อการศึกษาสาธารณะ

4.1.4 แผนที่นำทางเทคโนโลยีและการคาดการณ์เทคโนโลยี (Technology roadmap/foresight)
- ศึกษาและวิเคราะห์สถานการณ์ปัจจุบัน และทิศทางการพัฒนาเทคโนโลยีสารสนเทศเชิงควอนตัมของโลกภายในกรอบระยะเวลา 10 ปี
- ศึกษาศักยภาพ การประยุกต์ใช้เทคโนโลยีสารสนเทศเชิงควอนตัมของต่างประเทศในปัจจุบันและอนาคตระยะเวลา 10 ปี
- ศึกษาศักยภาพและสถานภาพ การวิจัยเทคโนโลยีสารสนเทศเชิงควอนตัมของประเทศไทย
- จัดทำแผนที่นำทางเทคโนโลยีสารสนเทศเชิงควอนตัม สำหรับเครือข่ายการสื่อสารยุคใหม่ของประเทศไทยภายใต้กรอบระยะ 2016 -2025

5. หลักการและเหตุผล (Needs and Solution)
สารสนเทศเชิงควอนตัม (quantum information) เป็นองค์ความรู้ใหม่ที่กำลังจะมีผลกระทบต่อเทคโนโลยี

ของโลกในอนาคตอันใกล้ และได้รับความสนใจทั่วโลกในขณะนี้ทั้งในด้านการค้าและการวิจัยเพื่อสร้างองค์ความรู้พื้นฐาน โดยเป็นการนำหลักการของกลศาสตร์ควอนตัมมาประยุกต์ใช้กับเทคโนโลยีสารสนเทศ เพื่อให้การสื่อสารข้อมูล (communications) และการประมวลผลข้อมูล (computing) หรือเทคโนโลยีอื่น ๆ ที่เกี่ยวข้องทำงานได้เร็วขึ้น ขนาดเล็กลง และมีรูปแบบการประยุกต์ใช้ที่หลากหลาย

5.1 โครงสร้างภารกิจและการบริหารงานของกลุ่มความร่วมมือ

ส่วนการบริหารงานประกอบด้วยหัวหน้ากลุ่มวิจัยร่วมฯดำเนินการบริหารและวางนโยบาย ซึ่งมีที่ปรึกษาให้คำแนะนำการบริหารกลุ่มวิจัยร่วมฯ โดยมีการแบ่งส่วนการบริหารภายในออกเป็น 3 กลุ่ม ได้แก่ กลุ่มวิจัยทำหน้าที่ดำเนินการวิจัยตามขอบเขตงานของกลุ่มตามยุทธศาสตร์ กลุ่มนโยบาย/แผนงานทำหน้าที่วางนโยบายร่วมกับหัวหน้ากลุ่มและกำหนดทิศทางการวิจัย และกลุ่มส่งเสริมเครือข่ายรับผิดชอบส่วนของกิจกรรมเผยแพร่ผลงานวิชาการและขยายเครือข่ายความร่วมมือ โดยตลอดทั้งการดำเนินงานจะมีคณะทำงานย่อยของสมาคมฯ ให้การบริการและสนับสนุนกลุ่มวิจัยร่วมฯ

คณะทำงานย่อย/ ฝ่ายบริหารและสนับสนุน

1. กลุ่มวิจัยเทคโนโลยีสารสนเทศควอนตัมไทย (Q-Thai.Org Forum) สมาคมวิชาการไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคม และสารสนเทศ (ECTI)
2. ชมรมไฟฟ้าสื่อสาร (IEEE ComSoc Thailand chapter) สมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE Thailand Section)
3. ศูนย์ความเป็นเลิศด้านฟิสิกส์ (Thailand Excellence Center in Physics)
4. มหาวิทยาลัยและหน่วยงานอื่น ๆ ที่เข้าร่วม

5.2 แนวทางการบริหารงานกลุ่มวิจัยร่วมฯ

5.2.1 ด้านการวิจัยและพัฒนา

- ศึกษาและวิจัยการคำนวณ การสื่อสารและรหัสลับเชิงควอนตัม การส่งถ่ายข่าวสารเชิงควอนตัมและที่เกี่ยวข้อง
- พัฒนาหลักสูตรการเรียนการสอนด้านสารสนเทศเชิงควอนตัม
- พัฒนาและแลกเปลี่ยนบุคลากรร่วมทั้งในกับต่างประเทศในทุกระดับ
- จัดหาและพัฒนาโครงสร้างพื้นฐานสำหรับการศึกษาและงานวิจัย

5.2.2 ด้านนโยบาย/แผนงาน

- จัดหาและระดมทุนเพื่อการสร้างโครงสร้างพื้นฐานและการปฏิบัติงาน
- พัฒนาหลักสูตรการเรียนการสอน การฝึกอบรม
- จัดทำแผนที่นำทางเทคโนโลยีด้านสารสนเทศเชิงควอนตัม สำหรับเป็นแนวทางในการวิจัยและพัฒนาของประเทศ
- จัดทำและปรับปรุงแผนที่นำทางเทคโนโลยีพร้อมการประเมินความก้าวหน้าเป็นระยะ

5.2.3 ด้านการส่งเสริมเครือข่าย

- จัดการประชุม สัมนาเชิงปฏิบัติการ การประชุมวิชาการ รวมกลุ่มวิจัย
- ส่งเสริมและแลกเปลี่ยนบุคลากร และแสวงหาทุนการศึกษาในทุกระดับ
- จัดนิทรรศการ ตีพิมพ์เผยแพร่ผลงาน นิทรรศการและการสื่อสารวิทยาศาสตร์
- สร้างความร่วมมือกับทั้งในและต่างประเทศ

6. เป้าหมายหลักและผลลัพธ์ที่คาดว่าจะได้รับ (Output and Benefit)

6.1 โครงสร้างพื้นฐานเพื่อใช้ในการวิจัยและพัฒนาด้านสารสนเทศเชิงควอนตัม ได้แก่ ห้องปฏิบัติการเฉพาะทางและเครือข่ายการวิจัย และทดสอบด้านการสื่อสารเชิงแสงผ่านเส้นใยนำแสง เป็นต้น

6.2 แผนที่นำทางเทคโนโลยี หลักสูตรการเรียนการสอนด้านสารสนเทศเชิงควอนตัม

6.3 บุคลากรด้านเทคโนโลยีสารสนเทศเชิงควอนตัมจำนวนเพียงพอต่อการพัฒนา

6.4 ประเทศไทยมีเครือข่ายการสื่อสารเชิงควอนตัมแรกในอีก 5 ปี และระบบการคำนวณเชิงควอนตัมในอีกไม่เกิน 10 ปี เพื่อรองรับการประยุกต์ใช้งานจริงกับองค์กรที่สำคัญของประเทศ

6.5 ประเทศไทยมีความพร้อมและทัศนคติที่ถูกต้องเหมาะสม สำหรับเทคโนโลยีที่จะอุบัติใหม่ในอนาคตของกลศาสตร์ควอนตัมเชิงสาธารณะมากขึ้น

6.6 เกิดมีความร่วมมือที่เข้มแข็งระหว่างหน่วยงานในและต่างประเทศ ทั้งภาคการศึกษา นโยบายและอุตสาหกรรมที่เกี่ยวข้อง

(แสง-ควอนตัม-สื่อสาร-แอลอีดี)
OQC.LED.TTKM
(หน้าสุดท้าย)

ประวัติผู้วิจัย

Curriculum Vitae of Suwit Kiravittaya

Contact:

Room: LAB EE 5 (Workshop EE)

Department of Electrical and Computer Engineering,

Faculty of Engineering, Naresuan University,

99 Moo 9, Siharajdachochai Road,

Tambon Taphoo, Amphoe Muang,

Phitsanulok Province

Postcode 65000, THAILAND

Tel.: +66-(0)55-96-4143

Fax: +66-(0)55-96-4005

E-mail: suwitki@ieee.org

Personal Data

Current Research Interests

- Applied Electronics for Various Sensing Systems
- Opto-Electronics: Solar Cells, Photodetectors, LEDs and Lasers
- Molecular Beam Epitaxy and Optical Properties of Semiconductor Nanostructures
- Quantum Information Technology: Computation, Communication and Coding

Education and Work Experience

Jun 1994 - May 1998	Chulalongkorn University, Bangkok, Thailand Bachelor of Electrical Engineering (Second class honor)
Jun 1998 - May 2003	Chulalongkorn University, Bangkok, Thailand Doctoral of Electrical Engineering
Dec 2000 - Jun 2002 (17 months)	Max-Planck-Institute for Solid State Research, Stuttgart, Germany Research on the growth of self-assembled quantum dots based on III-V compound semiconductor by molecular beam epitaxy.
Jun 2003 - Feb 2007	Max-Planck-Institute for Solid State Research, Stuttgart, Germany Post-doctoral fellowship Research on the growth of self-assembled III-V quantum dots on patterned substrates by molecular beam epitaxy.
Mar 2007 - Dec 2008	Max-Planck-Institute for Solid State Research, Stuttgart, Germany Post-doctoral fellowship Theoretical modeling of structural, electronic, and optical properties of semiconductor micro- and nanostructures.
Jan 2009 - Apr 2010	Institute for Integrative Nanosciences, IFW Dresden, Dresden, Germany Scientific Staff Member Theoretical modeling of structural, electronic, and optical properties of semiconductor micro- and nanostructures.
May 2010 - Oct 2011	Institute for Integrative Nanosciences, IFW Dresden, Dresden, Germany Scientific Staff Member Head of Research Group: Strained Nanomembranes for Optical, Electronic, and Fluidic Systems (SNOEFS)
Jan 2012 - Present	Department of Electrical and Computer Engineering, Naresuan University Phitsanulok, Thailand Lecturer

Review Services for Journals

- New Journal of Physics
- Nanotechnology
- Semiconductor Science and Technology
- Journal of Crystal Growth
- Materials Science in Semiconductor Processing
- Nanoscale Research Letters
- Applied Physics Letters
- Journal of Applied Physics
- Physical Review B
- Dataset Papers in Optics (Editorial Board)

Publication

Book

1. Suwit Kiravittaya
   Introduction to Electronics (in Thai)
   February (2014), ISBN 978-616-348-529-8

Book Chapters

5. S. Kiravittaya, A. Rastelli, and O. G. Schmidt
   Quantum dot crystals: Growth and characterization
   in volume 22 of Encyclopedia of Nanoscience and Nanotechnology (edited by H. S. Nalwa), page 23-32 (2011)

4. A. Rastelli, S. Kiravittaya, and O. G. Schmidt
   Growth and control of optically active quantum dots
   in Single Semiconductor Quantum Dots (edited by P. Michler), Springer, Berlin (2009)

3. S. Kiravittaya, H. Heidemeyer, and O. G. Schmidt
   In(Ga)As quantum dot crystals on patterned GaAs(001) substrates
   in Lateral Alignment of Epitaxial Quantum Dots (edited by O. G. Schmidt), Springer, Berlin (2007)

2. G. S. Kar, S. Kiravittaya, M. Stoffel, and O. G. Schmidt
Ordered SiGe island arrays: Long range material distribution and possible device applications
in Lateral Alignment of Epitaxial Quantum Dots (edited by O. G. Schmidt), Springer, Berlin (2007)

1. A. Rastelli, R. Songmuang, S. Kiravittaya, and O. G. Schmidt
Hierarchical self-assembly of lateral quantum-dot molecules around nanoholes
in Lateral Alignment of Epitaxial Quantum Dots (edited by O. G. Schmidt), Springer, Berlin (2007)

International Journals

77. S. L. Li, L. B. Ma, S. Böttner, Y. F. Mei, M. R. Jorgensen, S. Kiravittaya, and O. G. Schmidt
Angular position detection of single nanoparticles on rolled-up optical microcavities with lifted degeneracy
Physical Review A 88, 033833 (2013)

76. P. Boonpeng, S. Kiravittaya, S. Thainoi, S. Panyakeow, and S. Ratanathammaphan
InGaAs quantum-dot-in-ring structure by droplet epitaxy
Journal of Crystal Growth 378, 435 (2013)

75. L. B. Ma, S. L. Li, V. A. Bolanos Quinones, L. C. Yang, W. Xi, M. Jorgensen, S. Baunack, Y. F. Mei, S. Kiravittaya, and O. G. Schmidt
Dynamic molecular processes detected by microtubular opto-chemical sensors self-assembled from prestrained nanomembranes
Advanced Materials 25, 2357 (2013)

74. H. L. Zhen, G. S. Huang, S. Kiravittaya, S. L. Li, Ch. Deneke, Dominic J. Thurmer, Y. F. Mei, O. G. Schmidt, and W. Lu
Light-emitting properties of a strain-tuned microtube containing coupled quantum wells
Applied Physics Letters 102, 041109 (2013)

73. S. Böttner, S. Li, J. Trommer, S. Kiravittaya, and O. G. Schmidt
Sharp whispering-gallery modes in rolled-up vertical SiO2 microcavities with quality factors exceeding 5000
Optics Letters 37, 5136 (2012)

72. S. L. Li, L. B. Ma, H. L. Zhen, M. R. Jorgensen, S. Kiravittaya, and O. G. Schmidt
Dynamic axial mode tuning in a rolled-up optical microcavity
Physical Review B 86, 195421 (2012)

71. V. M. Fomin, S. Kiravittaya, and O. G. Schmidt
Electron localization in inhomogeneous Möbius rings
Physical Review B 86, 195421 (2012)

70. V. A. Bolanos Quinones, L. B. Ma, S. L. Li, M. Jorgensen, S. Kiravittaya, and O. G. Schmidt
Enhanced optical axial confinement in asymmetric microtube cavities rolled up from circular-shaped nanomembranes
Optics Letters 37, 4284 (2012)

69. V. A. Bolanos Quinones, L. B. Ma, S. L. Li, M. Jorgensen, S. Kiravittaya, and O. G. Schmidt
Localized optical resonances in low refractive index rolled-up microtube cavity for liquid-core optofluidic detection
Applied Physics Letters 101, 151107 (2012)

68. S. M. Harazim, V. A. Bolanos Quinones, S. Kiravittaya, S. Sanchez, and O. G. Schmidt
Lab-in-a-tube: on-chip integration of glass optofluidic ring resonators for label-free sensing applications
Lab on a Chip 12, 2649 (2012)

67. A. Rastelli, F. Ding, J. D. Plumhof, S. Kumar, R. Trotta, Ch. Deneke, A. Malachias, P. Atkinson, E. Zallo, T. Zander, A. Herklotz, R. Singh, V. Krapek, J. R. Schröter, S. Kiravittaya, M. Benyoucef, R. Hafenbrak, K. D. Jöns, D. J. Thurmer, D. Grimm, G. Bester, K. Dörr, P. Michler, and O. G. Schmidt
Controlling quantum dot emission by integration of semiconductor nanomembranes onto piezoelectric actuators
Physica Status Solidi B 249, 687 (2012)

66. P. Cendula, S. Kiravittaya, and O. G. Schmidt
Electronic and optical properties of quantum wells embedded in wrinkled nanomembranes
Journal of Applied Physics 111, 043105 (2012)

65. G. Pizzi, M. Virgilio, G. Grosso, S. Kiravittaya, and O. G. Schmidt
Curvature effects on valley splitting and degeneracy lifting: Case of Si/Ge rolled-up nanotubes
Physical Review B 85, 075308 (2012)

64. E. J. Smith, S. Schulze, S. Kiravittaya, Y. F. Mei, S. Sanchez, and O. G. Schmidt
Lab-in-a-tube: detection of individual mouse cells for analysis in flexible split-wall microtube resonator sensors

Nano Letters 11, 4037 (2011)

63. L. B. Ma, S. Kiravittaya, S. L. Li, V. A. Bolanos Quinones, Y. F. Mei, and O. G. Schmidt
Tuning of optical resonances in asymmetric microtube cavities
Optics Letters 36, 3840 (2011)

62. C. Ortix, S. Kiravittaya, O. G. Schmidt, and J. van den Brink
Curvature-induced geometric potential in strain-driven nanostructures
Physical Review B 84, 045438 (2011)

61. S. Kiravittaya, H. S. Lee, L. Balet, L. H. Li, M. Francardi, A. Gerardino, A. Fiore, A. Rastelli, and O. G. Schmidt
Tuning optical modes in slab photonic crystal by atomic layer deposition and laser-assisted oxidation
Journal of Applied Physics 109, 053115 (2011)

60. P. Cendula, S. Kiravittaya, I. Mönch, J. Schumann, and O. G. Schmidt
Directional roll-up of nanomembranes mediated by wrinkling
Nano Letters 11, 236 (2011)

59. Y. F. Mei, S. Kiravittaya, S. Harazim, and O. G. Schmidt
Principles and applications of micro and nanoscale wrinkles
Materials Science and Engineering: R 70, 209 (2010)

58. R. O. Rezaev, S. Kiravittaya, V. M. Fomin, A. Rastelli, and O. G. Schmidt
Engineering self-assembled SiGe islands for robust electron confinement in Si
Physical Review B 82, 153306 (2010)

57. G. S. Huang, V. A. Bolaños Quiñones, F. Ding, S. Kiravittaya, Y. F. Mei, and O. G. Schmidt
Rolled-up optical microcavities with subwavelength wall thicknesses for enhanced liquid sensing applications
ACS Nano 4, 3123 (2010)

56. J. Peng, C. Hermannstädter, M. Witzany, M. Heldmaier, L. Wang, S. Kiravittaya, A. Rastelli, O. G.

Schmidt, P. Michler, and G. Bester
Heterogeneous confinement in laterally coupled InGaAs/GaAs quantum dot molecules under lateral electric fields
Physical Review B 81, 205315 (2010)

55. T. Lutz, T. Suzuki, G. Costantini, L. Wang, S. Kiravittaya, A. Rastelli, O. G. Schmidt, and K. Kern
Reversing the shape transition of InAs/GaAs (001) quantum dots by etching-induced lateral In segregation
Physical Review B 81, 205414 (2010)

54. Ch. Deneke, A. Malachias, S. Kiravittaya, M. Benyoucef, T. H. Metzger, and O. G. Schmidt
Strain states in a quantum well embedded into a rolled-up microtube: X-ray and photoluminescence studies
Applied Physics Letters 96, 143101 (2010)

53. T. Zander, A. Herklotz, S. Kiravittaya, M. Benyoucef, F. Ding, P. Atkinson, S. Kumar, J. D. Plumhof, K. Dörr, A. Rastelli, and O. G. Schmidt
Epitaxial quantum dots in stretchable optical microcavities
Optics Express 17, 22452 (2009)

52. H. S. Lee, S. Kiravittaya, S. Kumar, J. D. Plumhof, L. Balet, L. H. Li, M. Francardi, A. Gerardino, A. Fiore, A. Rastelli, and O. G. Schmidt
Local tuning of photonic crystal nanocavity modes by laser-assisted oxidation
Applied Physics Letters 95, 191109 (2009)

51. Y. F. Mei, D. J. Thurmer, Ch. Deneke, S. Kiravittaya, Y.-F. Chen, A. Dadgar, F. Bertram, B. Bastek, A. Krost, J. Christen, T. Reindl, M. Stoffel, E. Coric, and O. G. Schmidt
Fabrication, self-assembly, and properties of ultrathin AlN/GaN porous crystalline nanomembranes: tubes, spirals, and curved sheets
ACS Nano 3, 1663 (2009)

50. V. A. Bolaños Quiñones, G. S. Huang, J. D. Plumhof, S. Kiravittaya, A. Rastelli, Y. F. Mei, and O. G. Schmidt
Optical resonance tuning and polarization of thin-walled tubular microcavities

Optics Letters 34, 2345 (2009)

49. L. Wang, A. Rastelli, S. Kiravittaya, M. Benyoucef, and O. G. Schmidt
Self-assembled quantum dot molecules
Advanced Materials 21, 2601 (2009)

48. H. S. Lee, A. Rastelli, S. Kiravittaya, P. Atkinson, C. C. Bof Bufon, I. Mönch, and O. G. Schmidt
Selective area wavelength tuning of InAs/GaAs quantum dots obtained by TiO2 and SiO2 layer patterning
Applied Physics Letters 94, 161906 (2009)

47. G. S. Huang, S. Kiravittaya, V. A. Bolanos Quinones, F. Ding, M. Benyoucef, A. Rastelli, Y. F. Mei, and O. G. Schmidt
Optical properties of rolled-up tubular microcavities from shaped nanomembranes
Applied Physics Letters 94, 141901 (2009)

46. S. Kiravittaya, A. Rastelli, and O. G. Schmidt
Advanced quantum dot configurations
Reports on Progress in Physics 72, 046502 (2009)

45. P. Cendula, S. Kiravittaya, Y. F. Mei, Ch. Deneke, and O. G. Schmidt
Bending and wrinkling as competing relaxation pathways for strained free-hanging films
Physical Review B 79, 085429 (2009)

44. A. Malachias, Ch. Deneke, B. Krause, C. Mocuta, S. Kiravittaya, T. H. Metzger, and O. G. Schmidt
Direct strain and elastic energy evaluation in rolled-up semiconductor tubes by x-ray microdiffraction
Physical Review B 79, 035301 (2009)

43. S. Kiravittaya and O.G. Schmidt
Quantum-dot crystal defects
Applied Physics Letters 93, 176109 (2008)

42. P. Atkinson, S. Kiravittaya, M. Benyoucef, A. Rastelli, and O. G. Schmidt

Site-controlled growth and luminescence of InAs quantum dots using in situ Ga-assisted deoxidation of patterned substrates
Applied Physics Letters 93, 101908 (2008)

41. A. Bernardi, S. Kiravittaya, A. Rastelli, R. Songmuang, D. J. Thurmer, M. Benyoucef, and O. G. Schmidt
On-chip Si/SiOx microtube refractometer
Applied Physics Letters 93, 094106 (2008)

40. S. Mendach, S. Kiravittaya, A. Rastelli, M. Benyoucef, R. Songmuang, and O. G. Schmidt
Bidirectional wavelength tuning of individual semiconductor quantum dots in a flexible rolled-up microtube
Physical Review B 78, 035317 (2008)

39. L. Wang, A. Rastelli, S. Kiravittaya, P. Atkinson, F. Ding, C. C. Bof Bufon, C. Hermannstädter, M. Witzany, G. J. Beirne, P. Michler, and O. G. Schmidt
Towards deterministically controlled InGaAs/GaAs lateral quantum dot molecules
New Journal of Physics 10, 043031 (2008)

38. S. Kiravittaya, M. Benyoucef, R. Zapf-Gottwick, A. Rastelli, and O. G. Schmidt
Optical fine structure of single ordered GaAs quantum dots
Physica E 40, 1909 (2008)

37. M. Benyoucef, S. Kiravittaya, Y. F. Mei, A. Rastelli, and O. G. Schmidt
Strongly coupled semiconductor microcavities: A route to couple artificial atoms over micrometric distances
Physical Review B 77, 035108 (2008)

36. Y. F. Mei, D. J. Thurmer, F. Cavallo, S. Kiravittaya, and O. G. Schmidt
Semiconductor sub-micro-/nanochannel networks by deterministic layer wrinkling
Advanced Materials 19, 2124 (2007)

35. Y. F. Mei, S. Kiravittaya, M. Benyoucef, D. J. Thurmer, T. Zander, C. Deneke, F. Cavallo, A. Rastelli, and O. G. Schmidt

Optical properties of a wrinkled nanomembrane with embedded quantum well
Nano Letters 7, 1676 (2007)

34. F. Ding, L. Wang, S. Kiravittaya, E. Müller, A. Rastelli, and O. G. Schmidt
Unveiling the morphology of buried In(Ga)As nanostructures by selective wet chemical etching: From quantum dots to quantum rings
Applied Physics Letters 90, 173104 (2007)

33. T. Merdzhanova, A. Rastelli, M. Stoffel, S. Kiravittaya, and O. G. Schmidt
Island motion triggered by the growth of strain-relaxed SiGe/Si(001) islands
Journal of Crystal Growth 301-302, 319 (2007)

32. A. Rastelli, A. Ulhaq, S. Kiravittaya, L. Wang, A. Zrenner, and O. G. Schmidt
In situ laser microprocessing of single self-assembled quantum dots and optical microcavities
Applied Physics Letters 90, 073120 (2007)

31. S. Kiravittaya, M. Benyoucef, R. Zapf-Gottwick, A. Rastelli, and O. G. Schmidt
Ordered GaAs quantum dot arrays on GaAs(001): Single photon emission and fine structure splitting
Applied Physics Letters 89, 233102 (2006)

30. S. Kiravittaya, A. Rastelli, and O. G. Schmidt
Morphology and photoluminescence of seeded three-dimensional InAs/GaAs(001) quantum-dot crystals
physica status solidi c 3, 3668 (2006)

29. A. Rastelli, A. Ulhaq, Ch. Deneke, L. Wang, M. Benyoucef, E. Coric, W. Winter, S. Mendach, F. Horton, F. Cavallo, T. Merdzhanova, S. Kiravittaya, and O. G. Schmidt
Fabrication and characterization of microdisk resonators with In(Ga)As/GaAs quantum dots
physica status solidi c 3, 3641 (2006)

28. S. Kiravittaya, R. Songmuang, A. Rastelli, H. Heidemeyer, and O. G. Schmidt
Multi-scale ordering in self-assembled InAs/GaAs(001) quantum dots
Nanoscale Research Letters 1, 1 (2006)

27. L. Wang, A. Rastelli, S. Kiravittaya, R. Songmuang, O. G. Schmidt, B. Krause, and T. H. Metzger
Guided self-assembly of lateral InAs/GaAs quantum-dot molecules for single molecule spectroscopy
Nanoscale Research Letters 1, 74 (2006)

26. G. S. Kar, S. Kiravittaya, U. Denker, B.-Y. Nguyen, and O. G. Schmidt
Strain distribution in a transistor using self-assembled SiGe islands in source and drain regions
Applied Physics Letters 88, 253108 (2006)

25. T. Merdzhanova, S. Kiravittaya, A. Rastelli, M. Stoffel, U. Denker, and O. G. Schmidt
Dendrochronology of strain-relaxed islands
Physical Review Letters 96, 226103 (2006)

24. S. Mendach, R. Songmuang, S. Kiravittaya, A. Rastelli, M. Benyoucef, and O. G. Schmidt
Light emission and wave guiding of quantum dots in a tube
Applied Physics Letters 88, 111120 (2006)

23. A. Rastelli, S. Kiravittaya, L. Wang, C. Bauer, and O. G. Schmidt
Micro-photoluminescence spectroscopy of hierarchically self-assembled quantum dots
Physica E 32, 29 (2006)

22. S. Kiravittaya, A. Rastelli, and O. G. Schmidt
Photoluminescence from seeded three-dimensional InAs/GaAs quantum-dot crystals
Applied Physics Letters 88, 043112 (2006)

21. S. Kiravittaya, A. Rastelli, and O. G. Schmidt
Self-assembled InAs quantum dots on patterned GaAs(001) substrates: Formation and shape evolution
Applied Physics Letters 87, 243112 (2005)

20. M. Stoffel, A. Rastelli, S. Kiravittaya, and O. G. Schmidt
Strain mediated lateral SiGe island motion in single and stacked layers
Physical Review B 72, 205411 (2005)

19. B. Krause, T. H. Metzger, A. Rastelli, R. Songmuang, S. Kiravittaya, and O. G. Schmidt
Shape, strain and ordering of lateral InAs quantum dot molecules
Physical Review B 72, 085339 (2005)

18. S. Kiravittaya, H. Heidemeyer, and O. G. Schmidt
Lateral quantum dot replication in three-dimensional quantum-dot crystals
Applied Physics Letters 86, 263113 (2005)

17. S. Kiravittaya and O. G. Schmidt
Comment on "A growth pathway for highly ordered quantum dot arrays"[Appl. Phys. Lett. 85, 5974 (2004)]
Applied Physics Letters 86, 206101 (2005)

16. J. Novák, V. Holý, J. Stangl, G. Bauer, E. Wintersberger, S. Kiravittaya, and O. G. Schmidt
A method for characterization of strain fields in buried quantum dots using x-ray standing waves
Journal of Physics D: Applied Physics 38, A137 (2005)

15. G. S. Kar, S. Kiravittaya, M. Stoffel, and O. G. Schmidt
Material distribution across the interface of random and ordered island arrays
Physical Review Letters 93, 246103 (2004)

14. O. G. Schmidt, A. Rastelli, G. S. Kar, R. Songmuang, S. Kiravittaya, M. Stoffel, U. Denker, S. Stufler, A. Zrenner, D. Grützmacher, B.-Y. Nguyen, and P. Wennekers
Novel nanostructure architectures
Physica E 25, 280 (2004)

13. S. Kiravittaya, H. Heidemeyer, and O. G. Schmidt
Growth of three-dimensional quantum dot crystals on patterned GaAs (001) substrates
Physica E 23, 253 (2004)

12. R. Songmuang, S. Kiravittaya, and O. G. Schmidt
Formation of lateral quantum dot molecules around self-assembled nanoholes
Applied Physics Letter 82, 2892 (2003)

11. R. Songmuang, S. Kiravittaya, and O. G. Schmidt
Shape evolution of InAs quantum dots during overgrowth
Journal of Crystal Growth 249, 416 (2003)

10. R. Songmuang, S. Kiravittaya, M. Sawadsaringkarn, S. Panyakeow, and O. G. Schmidt
Photoluminescence investigation of low-temperature capped self-assembled InAs/GaAs quantum dots
Journal of Crystal Growth 251, 166 (2003)

9. S. Kiravittaya, R. Songmuang, N.Y. Jin-Phillip, S. Panyakeow, and O. G. Schmidt
Self-assembled nanoholes and lateral QD bi-molecules by molecular beam epitaxy and atomically precise in situ etching
Journal of Crystal Growth 251, 258 (2003)

8. O. G. Schmidt, C. Deneke, S. Kiravittaya, R. Songmuang, Y. Nakamura, Y. Zapf-Gottwick, C. Müller, and N.Y. Jin-Phillip
Self-assembled nanoholes, lateral quantum-dot molecules, and rolled-up nanotubes
IEEE Journal of Selected Topics in Quantum Electronics 8, 1025 (2002)

7. O. G. Schmidt, S. Kiravittaya, Y. Nakamura, H. Heidemeyer, R. Songmuang, C. Müller , N.Y. Jin-Phillip, K. Eberl, H. Wawra, S. Christiansen, Gräbeldinger, and H. Schweizer
Self-assembled semiconductor nanostructures: climbing up the ladder of order
Surface Science 514, 10 (2002)

6. Y. Nakamura, O. G. Schmidt, N.Y. Jin-Phillip, S. Kiravittaya, C. Müller, K. Eberl, H. Gräbeldinger, and H. Schweizer
Vertical alignment of laterally ordered InAs and InGaAs quantum dot arrays on patterned (001) GaAs substrates
Journal of Crystal Growth 242, 339 (2002)

5. H. Heidemeyer, S. Kiravittaya, C. Müller, N.Y. Jin-Phillip, and O. G. Schmidt
Closely stacked InAs/GaAs quantum dots grown at low growth rate
Applied Physics Letters 80, 1544 (2002)

4. S. Kiravittaya, Y. Nakamura, and O. G. Schmidt
Photoluminescence linewidth narrowing of InAs/GaAs self-assembled quantum dots
Physica E 13, 224 (2002)

3. R. Songmuang, S. Kiravittaya, S. Thainoi, P. Changmuang, S. Sopitpan, S. Ratanathammaphan, M. Sawadsaringkarn, and S. Panyakeow
Selective growth of InAs/GaAs self-organized quantum dots by shadow mask technique
Journal of Crystal Growth 227-228, 1053 (2001)

2. S. Kiravittaya, R. Songmuang, P. Changmuang, S. Sopitpan, S. Ratanathammaphan, M. Sawadsaringkarn, and S. Panyakeow
InAs/GaAs self-organized quantum dots on (411)A GaAs by molecular beam epitaxy
Journal of Crystal Growth 227-228, 1010 (2001)

1. S. Kiravittaya, U. Manmontri, S. Sopitpan, S. Ratanathammaphan, C. Antarasen, M. Sawadsaringkarn, and S. Panyakeow
AlGaAs/GaAs/InGaAs composite MQW structures for photovoltaic applications
Solar Energy Material and Solar Cells 68, 89 (2001)

International Conference Proceedings

23. Suwit Kiravittaya, Maetee Kunsugsa, Supachok Thainoi, Somchai Ratanathammaphan, and Somsak Panyakeow
Electronic structure calculation of GaSb/GaAs quantum dot
Proceedings of the International Electrical Engineering Congress (iEECON) (2014)

22. Suwit Kiravittaya, Poonyasiri Boonpeng, Wipakorn Jevasuwan, Somchai Ratanathammaphan, and Somsak Panyakeow
Quantum-Dot Ring Formation by Strained Droplet Epitaxy
Abstract Book of the 17th International Conference on Crystal Growth and Epitaxy (ICCGE-17) (2013)

21. Suwit Kiravittaya, Maetee Kunrugsa, Suwat Sopitpan, Somchai Ratanathammaphan, and Somsak Panyakeow
Molecular Beam Epitaxial Growth of GaSb Quantum Dots on Ge Substrates
Abstract Book of the 17th International Conference on Crystal Growth and Epitaxy (ICCGE-17) (2013)

20. Suwit Kiravittaya, Wipakorn Jevasuwan, Somchai Ratanathammaphan, and Somsak Panyakeow
Energetic favorite of quantum dot formation in ring-shaped InP quantum-dot molecules
Proceedings of the Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology Conference (ECTI-CON) (2013)

19. Suwit Kiravittaya, Poonyasiri Boonpeng, Somchai Ratanathammaphan, and Somsak Panyakeow
Simple energetic estimation of electronic states in quantum-dot cellular automata
Proceedings of the International Electrical Engineering Congress (iEECON) (2013)

18. V. M. Fomin, S. Kiravittaya, and O. G. Schmidt
Electronic structure and the Aharonov-Bohm effect in inhomogeneous Möbius ring
Abstract Book of the DPG-Frühjahrstagung (2013)

17. Suwit Kiravittaya, Peter Cendula, and Oliver G. Schmidt
Optical transition in quantum well embedded in wrinkled nanomembrane
Abstract Book of the International Conference on Superlattices, Nanostructures and Nanodevices (ICSNN) (2012)

16. S. Kiravittaya and O. G. Schmidt (Plenary, Invited)
Rolled-up resonators for on-chip applications
Abstract Book of the 5th Conference on Materials Science and Condensed Matter Physics (MSCMP) (2010)

15. P. Cendula, S. Kiravittaya, J. Gabel, and O. G. Schmidt
Control of rolling direction for released strained wrinkled nanomembrane
Proceedings of the COMSOL Conference (2009)

14. S. Kiravittaya, Ch. Deneke, and O. G. Schmidt

Interface inhomogeneity of multilayer rolling up process
Abstract Book of the 12th International Conference on the Formation of Semiconductor Interfaces (ICFSI-12) (2009)

13. S. Kiravittaya, P. Cendula, A. Rastelli, and O. G. Schmidt
Effect of local deformation on the emission energy of quantum dots in a flexible tube
Proceedings of the COMSOL Conference (2008)

12. S. Kiravittaya, A. Bernardi, A. Rastelli, R. Songmuang, D. J. Thurmer, M. Benyoucef, and O. G. Schmidt
Numerical investigation of optical response from rolled-up microtube resonator and its application
Proceedings of the 10th International Conference on Transparent Optical Networks (ICTON) 4, 45 (2008)

11. S. Kiravittaya, M. Benyoucef, R. Zapf-Goettwick, A. Rastelli, and O. G. Schmidt
Fine structure of single ordered GaAs quantum dots
Abstract Book of the 13th International Conference on Modulated Semiconductor Structure (MSS-13) (2007)

10. A. Rastelli, S. Kiravittaya, M. Benyoucef, Y. F. Mei, and O. G. Schmidt
In situ tuning of optical modes in single semiconductor microcavities by laser heating
Proceedings of the 9th International Conference on Transparent Optical Networks (ICTON) 3, 58-60 (2007)

9. S. Kiravittaya, A. Rastelli, and O. G. Schmidt
Photoluminescence investigation of seeded three-dimensional InAs/GaAs quantum-dot crystals
Abstract Book of the 4th International Conference on Quantum Dots (2006)

8. S. Kiravittaya and O. G. Schmidt
Quantum dot defects in quantum dot crystals
Abstract Book of the 12th International Conference on Modulated Semiconductor Structure (MSS-12) (2005)

7. S. Kiravittaya and O. G. Schmidt
Diffusion in and around highly ordered arrays of self-assembled InAs/GaAs quantum dots
Abstract Book of the Quantum Dot Conference (2004)

6. R. Songmuang, S. Kiravittaya, N. Y. Jin-Phillipp, and O. G. Schmidt
Molecular beam epitaxy and in situ etching for nanohole and lateral quantum dot multi-molecule fabrication
Abstract Book of the Low Dimensional Structures and Devices (LDSD) (2002)

5. S. Kamprachum, S. Kiravittaya, R. Songmuang, S. Thainoi, S. Kanjanachuchai, M. Sawadsaringkarn, and S. Panyakeow
Multi-stacked quantum dots with graded dot sizes for photovoltaic applications
Proceedings of the 29th IEEE Photovoltaic Specialists Conference 1055-1057 (2002)

4. S. Kiravittaya, R, Songmuang, and O. G. Schmidt
Self-assembled quantum dots and nanoholes by molecular beam epitaxial growth and atomically precise in situ etching
Proceedings of the Material Research Society Symposium 722: K10.11.1-6. (2002)

3. S. Kiravittaya, Y. Nakamura, and O. G. Schmidt
Photoluminescence linewidth narrowing of InAs/GaAs self-assembled quantum dots
Abstract Book of the 13th International Conference on Modulated Semiconductor Structure (MSS-10) (2001)

2. S. Kiravittaya, R. Songmuang, S. Thainoi, S. Sopitpan, S. Kanjanachuchai, S. Ratanathammaphan, M. Sawadsaringkarn, and S. Panyakeow
Self-assembled composite quantum dots for photovoltaic applications
Proceedings of the 28th IEEE Photovoltaic Specialists Conference 818-821 (2000)

1. S. Kiravittaya, U. Manmontri, S. Sopitpan, S. Ratanathammaphan, C. Antarasen, M. Sawadsaringkarn, and S. Panyakeow
AlGaAs/GaAs/InGaAs composite MQW structures for photovoltaic applications
Proceedings of the 2nd World Conference and Exhibition on Photovoltaic Solar Energy Conversion 3617-3620 (1998)

Domestic Journals

3. Suwit Kiravittaya and Wanwisa Pansak
   Relationship between taken time and examination scores in fundamental of electrical engineering course
   Journal of Education Naresuan University 15 (2): 117-123. (2013)

2. Rudeesun Songmuang, Suwit Kiravittaya, Montri Sawadsaringkarn, and Somsak Panyakeow
   The growth of InAs self-organized quantum dots by molecular beam epitaxy
   Research and Development Journal, The Engineering Institute of Thailand 13: 34-41. (2002)

1. Suwit Kiravittaya, Montri Sawadsaringkarn, and Somsak Panyakeow
   Single electron transistor: Theory and applications
   Research and Development Journal, The Engineering Institute of Thailand 11: 20-27. (2000)

Domestic Conference Proceedings

8. Suwit Kiravittaya, Poonyasiri Boonpeng, Somchai Ratanathammaphan, and Somsak Panyakeow
Effects of structural inhomogeneity on electron confinement in semiconductor quantum rings
Proceedings of the 35th Electrical Engineering Conference (EECON-35) vol. 2 p. 1025-1028. (2012)

7. Suwit Kiravittaya (Invited)
Self-organized nanostructures: quantum dots and nanomembranes
Proceedings of RGJ-Ph.D. Congress XIII S1-L5 p. 73. (2012)

6. Suwit Kiravittaya (Invited)
Homogeneity Improvement of InAs/GaAs Self-Assembled Quantum Dots Grown by Molecular Beam Epitaxy
Proceedings of RGJ-Ph.D. Congress IV S1-L3. (2003)

5. Suwit Kiravittaya, Rudeesun Songmuang, Montri Sawadsaringkarn, and Somsak Panyakeow
Kinetic Monte Carlo simulation of molecular beam epitaxial growth
Proceedings of the 25th Electrical Engineering Conference (EECON-25) EL134-EL138. (2002)

4. Rudeesun Songmuang, Suwit Kiravittaya, Montri Sawadsaringkarn, and Somsak Panyakeow
InAs/GaAs, InGaAs/GaAs, and InAs/InGaAs/GaAs composite quantum dots
Proceedings of the 23rd Electrical Engineering Conference (EECON-23) 685-688. (2000)

3. Suwit Kiravittaya, Rudeesun Songmuang, Montri Sawadsaringkarn, and Somsak Panyakeow
In-situ RHEED investigation of MBE-grown InAs QDs on (0 0 1) GaAs epilayer
Proceedings of the 23rd Electrical Engineering Conference (EECON-23) 689-692. (2000)

2. Suwit Kiravittaya, Montri Sawadsaringkarn, and Somsak Panyakeow
Quantum dots structure for optoelectronic devices
Proceedings of RGJ-Ph.D. Congress I 144. (2000)

1. Suwit Kiravittaya, Suwat Sopitpan, Somchai Ratanathammaphan, Montri Sawadsaringkarn, and Somsak Panyakeow
The study of AlGaAs/GaAs/InGaAs composite quantum well (CQW) structure

Proceedings of the 21st Electrical Engineering Conference (EECON-21) 123-126. (1998)

Reference

1. Prof. Dr. Somsak Panyakeow
   Semiconductor Device Research Laboratory (SDRL)
   Department of Electrical Engineering, Faculty of Engineering,
   Chulalongkorn University,
   Bangkok, THAILAND

2. Prof. Dr. Yongfeng Mei
   Department of Materials Science,
   Fudan University,
   Shanghai, CHINA

3. Prof. Dr. Armando Rastelli
   Institute of Semiconductor and Solid State Physics
   Johannes Kepler Universität,
   Linz, AUSTRIA

4. Prof. Dr. Oliver G. Schmidt
   Director of Institute for Integrative Nanosciences (IIN)
   Leibniz Institute for Solid State and Materials Research (IFW-Dresden)
   Dresden, GERMANY

JUTAPHET WETCHARUNGSRI

home:

Office: 112 NECTEC Thailand Science Park,
Phahonyothin Rd., Klong 1, Klong Luang,
Pathumthani 12120
Thailand
66(0)2-564-6900 Ext 2133
jutaphet.wetcharungsri@nectec.or.th

Education

April 2014 **Thammasat University,**
Master of Engineering, Department of Electrical and Computer Engineering.

April 2007 **King Mongkut's Institute of Technology Ladkrabang,**
Bachelor of Engineering, Department of Telecommunication Engineering.

Publication

Journal

2015
- **J. Wetcharungsri,** N. Buabthong, P. Thuphairo, P. Sangwongngam, K. Sripimanwat, "Design of Multi-Mode Semi-Parallel LDPC Decoders for WiMAX Standards", ***Thammasat International Journal of Science and Technology (TIJSAT)***, pp. 59-72

2014
- P. Kasamechonchung, A. Klamcheun, K. Boonpavanitchakul, N. Supaka, M. Horprathum, W. Kangwansupamonkon, S. Porntheeraphat, **J. Wetcharungsri**, P. Prompinit, A. Somboonkaew, S. Pratontep, 2014, Morphology-controlled seed-assisted hydrothermal ZnO nanowires via critical concentration for nucleation and their photoluminescence properties, ***Physica status solidui a***, null(211), 2200

Proceeding

2014
- **J. Wetcharungsri,** N. Buabthong, P. Thuphairo, P. Sangwongngam, K. Sripimanwat, "Improvement of Flexible Semi-Parallel LDPC Decoders over FPGA for WiMAX Standards", ***The International Conference on Information and Communication Technology for Embedded Systems (ICICTES2014)***, 140, 1-4
- K. Boonpavanitchakul, **J. Wetcharungsri**, T. Wutikhun, P. Kasamechonchung, M. Horprathum, S. Porntheeraphat, A. Klamcheun, A. Somboonkaew, N. Supaka, P. Prompinit, W. Kangwansupamonkon, S. Pratontep, 2014, "Controllability on Morphology of ZnO Nanowire via Critical Concentration for Nucleation and Its Photoluminescence Properties", ***NanoThailand 2014***, 140, 86

2013
- **J. Wetcharungsri,** N. Buabthong, S. Jantarachote, P. Sangwongngam, K.Sripimanwat, "Field-programmable Gate Array Implementation of Low-density Parity-check Codes Decoder and Hardware Testbed,"; ***IEEE TENCON Spring 2013 Conference***, pp.109 -112, 17-19 April 2013.

Proceeding

2012
- T. Phromsa-ard, J. Arpornsiripat, **J. Wetcharungsri**, P. Sangwongngam, K. Sripimanwat and P. Vanichchanunt, "Improved Gradient Descent Bit Flipping Algorithms for LDPC decoding ," in IEEE Proc. The Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Bangkok, Thailand, pp324-328. (16-18 May 2012).

2011
- P. Sangwongngam, **J. Wetcharungsri**, K. Sripimanwat, el al, 2011, "Implementation of Flexible LDPC Decoder for IEEE 802.16e", ***International Conference on Information and Communication Technology for Embedded Systems***, 140, pp. 135-138

2009
- S. Jantarachote, P. Sangwongngam, **J. Wetcharungsri**, K. Sripimanwat, C. Punyasai, 2009, "Implementation of CIDS-BC-LDPC Decoder on FPGA", ***The 24th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2009)***. 119. 177-180

MR. PARAMIN SANGWONGNGAM

home:

office: 112, NECTEC, Phahon Yothin Rd., Klong Nueng, Klong Luang
Pathum Thani 12120
Thailand
66 (0)2-564-6900 Ext. 2133
paramin.sangwongngam@nectec.or.th
http://www.nectec.or.th/en/

EDUCATION

April 2005 — **Chulalongkorn University** — Bangkok, Thailand
Master of Engineering, Department of Electrical Engineering
Focus: Telecommunications.
Thesis: Turbo-coded differential space-time modulaltion for temporally correlated fading channels
Advisor: Prof. Lunchakorn Wuttisittikulkij
Two new techniques for joint iterative decoding of serial concatenation of turbo codes and differential space-time modulation based on unitary space-time group codes are proposed and evaluated, under temporally correlated fading channels, assuming no Channel State Information (CSI) at both of the transmitter and the receiver.

2000 — **Prince of Songkhla University**, — Songkhla, Thailand
Bachelor of Engineering, Department of Electrical Engineering, ***First Class Honors***
Concentration in Communications
Senior project: Non-destructive Detection Method of Translucent Disorder and Internal Gumming of Mangosteens using signal analysis and neural network
Advisor: Assoc. Prof. Dr. Chusak Limsakul
It aims to study an electrical technique for detecting two important threats, namely translucent disorder and gumming, on mangosteen fruit which is one of the most important agricultural products in Thailand's export. The electrical method employed in this work was feature extraction with a spectrum of resonant frequencies.

Summer 1999 (3 months) — **Advanced Info Service (AIS) Corp.**, — Bangkok, Thailand
Internship, Metropolitan Field Engineer Department
Provided preventive and maintenance services for all equipment in assigned GSM base stations and corrected any faults and alarms in the base stations; consequently, learned good planning, problem solving, communication, and teamwork skills.

FELLOWSHIPS AND AWARDS

May 2006 — ***Outstanding Student Award*** from the Thailand Graduate Institute of Science and Technology (TGIST) in 2006 from the National Science and Technology Development Agency (NSTDA)

May 2005–Aug. 2005 — **Department of Electrical Engineering Fellowship** under "Cooperation Project between Department of Electrical Engineering and Private Sector for Research and Development"

Jun. 2002–Sep. 2004 — ***TGIST Scholarship*** from the National Science and Technology Development Agency to pursue the Master's degree

1997–2000 ***University Departmental Full Scholarship*** - for achieving GPA in the top 5% among all Engineering students; exempted from extra-tuition fee for all semesters while pursuing baccalaureate.

RESEARCH EXPERIENCE

Oct. 2013–present **National Electronics and Computer Technology Center (NECTEC), Photonics Technology Laboratory (PTL)**, Pathum Thani, Thailand
Project Manager: Dr. Supanit Porntheeraphat
- "Research and Development of White Light Emitting Diode Based on Zinc Oxide Optoelectronics Material, Phase 1: Method of ZnO-Substrate Fabrication" project.
- Involved in the characterization setup, especially the photoluminescence system.

Feb. 2012–Sep. 2013 **National Electronics and Computer Technology Center (NECTEC), Optical and Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Advisor: Dr. Keattisak Sripimanwat
- "A Development of Visible Light Wireless LAN System" project.
- Surveyed literature and standards on visible light communications.
- Developed and demonstrated a prototype of WLAN system via visible-light communications.
- Examined novel techniques in digital baseband transmission to increase throughput in practical scenarios.
- Led a team of 7 staff under the project.

Feb. 2012–Sep. 2012 **National Electronics and Computer Technology Center (NECTEC), Optical and Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Advisor: Dr. Andreas Poppe, Austrian Institute of Technology
- Invented a novel synchronization for entanglement-based QKD.

Jan. 2011–present **National Electronics and Computer Technology Center (NECTEC), Optical and Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Partners: Dr. Momtchil Peev, AIT, Austrian Institute of Technology
Prof. Ryutaroh Matsumoto, Tokyo Institute of Technology
- "High Efficiency Key Reconciliation Protocol for Quantum Key Distribution" project.
- Investigated and enhanced quantum key reconciliation protocols over hardware platform for high speed key sharing by applying classes of error control coding to quantum key reconciliation protocols.

May. 2010–Dec. 2010 **National Electronics and Computer Technology Center (NECTEC), Optical a nd Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Partners: Dr. W. S. Mohammed (Bangkok University) and Dr. W. Pijitrojana (Thammasart University)
- Experimented on optical concentrator for optical wireless communications.
- Designed the optical concentrator or antenna via ASAP® Optical Software.

Nov. 2010–Oct. 2012 **National Electronics and Computer Technology Center (NECTEC), Optical and Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Advisor: Dr. Keattisak Sripimanwat

- "National Healthcare Information System (NHIS)" project with approximately $ 1,000,000 funded by National Health Security Office (NHSO), Thailand.
- Designed, installed and tested secured communication network over seven nodes covering four distant cities.
- Prepared a report on comparative study of the designs and other commercial solutions to the secretary of NHSO.

Mar. 2010–Nov. 2011 **National Electronics and Computer Technology Center (NECTEC), Optical and Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Advisor: Dr. Keattisak Sripimanwat

- "Error Control Coding for Security" project.
- Proposed weighted bit-flipping decoding attaining better bit error rate performance.
- Experimentally verified and validated the proposed LDPC decoder over real-time FPGA-based baseband tested.

Mar. 2009–Sep. 2010 **National Electronics and Computer Technology Center (NECTEC), Optical and Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Advisor: Dr. Keattisak Sripimanwat

- "Thai Random Number Service (ThaiRand)" project.
- Strengthened randomness property of random number generation via established online web site at http://203.185.132.49/qrngws/index.jsp.

Apr. 2006–Oct. 2009 **National Electronics and Computer Technology Center (NECTEC), Optical and Quantum Communication Laboratory (OQC)**, Pathum Thani, Thailand
Advisor: Dr. Keattisak Sripimanwat

- "Error Control Coding for Next Generation Mobile Communications and Hard Disk Systems" project.
- Designed and implemented Low-density parity-check codes (LDPC) decoder regarding to the combination of Cycle-Invariant Difference Set (CIDS) block-circulant (BC) matrix, and the λ-min decoding algorithm to reduce the complexity area based on the semi-parallel architecture within constraint on trade-off between throughput and complexity area over FPGA chips.
- The architecture is applicable for various applications including 3G mobile communications and magnetic storage.

Sep. 2005–Feb. 2006 **University of Applied Science Northwestern (Fachhochschule Nordwestschweiz or FHNW)**, Olten, Switzerland
Advisor: Prof. Martin Kropp

- The eFitness project.
- Aimed to develop a mobile smart client application for collecting and managing training data of users via mobile phones over different smart phones and two mainstreams of J2ME and .NET framework.
- Designed and developed graphic user interfaces and control modules, and provided specific guidelines for the design and implementation.

May 2005–Aug. 2005 **Chulalongkorn University , Department of Electrical Engineering**, Bangkok, Thailand
Advisor: Prof. Lunchakorn Wuttisittikulkij

- Investigated and implemented OFDM techniques over hardware board.

- Employed various instrument and development boards to perform the experiment.

Jun. 2001–April 2005 **Chulalongkorn University , Department of Electrical Engineering**, Bangkok, Thailand
Advisor: Prof. Lunchakorn Wuttisittikulkij

- "Turbo-coded differential space-time modulaltion for temporally correlated fading channels" research topic.
- Conducted graduate research on iterative decoding, space-time modulation, and bit interleaver.
- Derived the soft-input soft-output demodulator based probabilistic detection theory to achieve better bit error rate performance of mobile communications.

TEACHING EXPERIENCE

Jun. 2005–Aug. 2005 *Teaching Assistant*: Wireless Communications and Networking, CHULALONGKORN UNIVERSITY, Bangkok, Thailand.
- Assisted students individually with assignment and graded their assignments.

GRANTS

Project Leader "A Development of Visible Light Wireless LAN System," National Science and Technology Development Agency (NSTDA), Ministry of Science and Technology (MOST), Thailand
Managed six-month project; supervised two Master's students and two undergraduate assistants; invented and developed a visible light wireless LAN system installed in NECTEC.

Project Leader "Error Control Coding for Security," National Science and Technology Development Agency (NSTDA), Ministry of Science and Technology (MOST), Thailand (duration: 12.03.2010 – 22.12.2011)
Organized a one-year project; supervised two Master's students and one undergraduate assistant.

Project Leader "Error Control Coding for Next Generation Mobile Communications and Hard Disk Systems," National Science and Technology Development Agency (NSTDA), Ministry of Science and Technology (MOST), Thailand (duration: 01.10.2006 – 01.10.2009)
Managed two-year project with about $ 66,000 budget; supervised one Master's student; established collaboration with academic partners

INSTRUMENTATION EXPERIENCE

Electrical and electronic engineering	*Telecommunication engineering*	*Development platform*	*Quantum cryptography*
Oscilloscope Function generator Arbitrary wave generator	Vector signal generator: Agilent modeled E4438C 250 kHz – 6 GHz ESG Network Analyzer: E4445A PSA Spectrum Analyzer, 3 Hz – 13.2 GHz	ADC/DAC: AD9432 Eval ADC/DAC: FMC150 Xilinx ML501 Xilinx ML605	QKD devices: IDQ's Cerberis model QKD devices: IDQ's Clavis II QKD devices: AIT's EPR405 Photon counter: Picoharp

SPECIAL SKILLS

Programming: (*Language*) VHDL, Altium, C/C++, .NET, MATLAB
(*Tool*) Tortoise, CVS, Redmine

PCB design:	Altium, OrCAD SPICE, signal integrity, Sonnet Lite
FPGA design:	Xilinx ISE, ModelSim
Optics design	ASAP® Optical Software
Innovation:	TRIZ methodology for inventive problem solving
Patent tools:	Thomson Innovation, Espacenet

PUBLICATIONS

Journal Articles:

- Muhammad Saadi, Ambar Bajpai, Yan Zhao, **Paramin Sangwongngam**, and Lunchakorn Wuttisittikulkij, "Design and Implementation of Secure and Reliable Communication using Optical Wireless Communication," ***Frequenz***, vol. 68, issue 11-12, pp. 501–509, October 2014.
- Muhammad Saadi, Lunchakorn Wuttisittikulkij, Yan Zhao, **Paramin Sangwongngam**, "A survey on Visible Light Communication: Opportunities, Challenges and Channel Models," ***International Journal of Electronics & Informatics (IJEI)***, ISSN: 2186 – 0114. 2013.
- Pisit Vanichchanunt , **Paramin Sangwongngam**, Suvit Nakpeerayuth, and Lunchakorn Wuttisittikulkij, "Iterative Multiple Symbol Differential Detection for Turbo Coded Differential Unitary Space-Time Modulation," ***Journal Of Communication and Networks***. 2008.

Books and Book Chapters
Three books in Thai as follows.

- ***Laplace Transform***. 2007. ISBN: 978-974-03-1925-2.
- ***MATLAB.*** ISBN: 978-974-03-2309-9.
- ***Channel Coding Theory***. TRIDI. 2009. ISBN: 978-616-73-0511-0

Conference Presentations, Proceedings, and Posters:

- T. Phromsa-ard, **P. Sangwongngam**, K. Sripimanwat, K. Kaemarungsri, P. Vanichchanunt, L. Wuttisittikulkij, "Low-complexity key reconciliation algorithm using LDPC bit-flipping decoding for quantum key distribution," ***the 11th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)***, 2014, vol., no., pp.1–5, 14–17 May 2014.
- M. Saadi, L. Wuttisittikulkij, Yan Zhao, K. Panlek, K. Woradit, **P. Sangwongngam**, "Performance analysis of optical wireless communication system using pulse width modulation***," the 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)***, pp.1–5, 15–17 May 2013.
- M. Saadi, T. Sittivangkul, Y. Zhao, L. Wuttisittikulkij, **P. Sangwongngam,** "A System Demonstration for Visible Light Communication using Adaptive Thershold Detection for Low Data Rate Applications" in ***IEEE International Conference on Electron Devices and Solid State Circuits***, 3–5 Dec., Bangkok, Thailand, 2012.
- (Poster) P. Treeviriyanupab, **P. Sangwongngam**, K. Sripimanwat, "Improved Reconciliation Efficiency with Channel Coding for Quantum Key Distribution" ***the 2nd Annual Conference on Quantum Cryptography (QCRYPT2012)***, 10–14 Sep. 2012, NUS, Singapore.
- T. Lorunser, A. Happe, M. Peev, F. Hipp, D. Melniczuk, P. Cummon, P. Panthong, **P. Sangwongngam** and A. Poppe, "Timing synchronization with photon pairs for quantum communications," ***QCMC2012***, Austria, p. 333.
- (International conference) T. Phromsa-ard, J. Arpornsiripat, J. Wetcharungsri,**P. Sangwongngam,** K. Sripimanwat, and P. Vanichchanunt, "Improved Gradient Descent Bit Flipping Algorithms for LDPC decoding," ***The Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP2012***), 2012.

- M. Pattaranantakul, **P. Sangwongngam** and K. Sripimanwat, "Secure and Efficient Key Management Technique in Quantum Cryptography Network", ***ICUFN 2012***, Phuket, Thailand, Jul. 4–6, 2012.
- P. Treeviriyanupab, **P. Sangwongngam**, K. Sripimanwat, O. Sangaroon, "BCH-Based Slepian-Wolf Coding with Feedback Syndrome Decoding for Quantum Key Reconciliation", ***ECTI-CON 2012***, Hua Hin, Thailand, May 16–18, 2012.
- M. Pattaranantakul, **P. Sangwongngam** and K. Sripimanwat, "Improving VPN Security Performance Based on One-Time Password Technique Using Quantum Keys", ***IC2IT 2012***, Pattaya, Thailand, May 9–10, 2012.
- M. Saadi, **P. Sangwongngam**, S. Nakpeerayuth, P. Vanichchanunt, Y. Zhao, L. Wuttisittikulkij. "Global Efforts in Realizing Visible Light Communication Systems and its Comparison with other Short Range Wireless Communication Networks" ***The NBTC Year End Conference 2011***, Bangkok. 15–16 Dec. 2011.
- M. Pattaranantakul; K. Phodong; C. Issariyapat; **P. Sangwongngam**; R. Kongkachandra "Passive monitoring method for analysis Quantum Key Distribution performance statistics," ***JCSSE 2011***; Nakhon Pathom; 11–13 May 2011.
- M. Pattaranantakul, **P. Sangwongngam** and K. Sripimanwat, "The Design and Implementation of Q-Ti Network and Monitoring System", ***The 2nd International Conferenceon Quantum Information and Technology***, Oct. 21–22, 2010, National Institute of Informatics (NII), Tokyo, Japan.
- **P. Sangwongngam**, J. Wetcharungsri, K. Sripimanwat, *et al*, 2011, "Implementation of Flexible LDPC Decoder for IEEE 802.16e", ***International Conference on Information and Communication Technology for Embedded Systems***, 140, pp. 135–138.
- P. Jarutatsanangkoon, S. Jantarachote, **P. Sangwongngam**, K. Sripimanwat, W. S. Mohammed and W. Pijitrojana, "The Simulations and Experiment of Optical Hemispherical Antenna for Indoor Visible Light Communications," ***National Conference of Optical Applications, NCOA-6, (2010).***
- D. Chumchewkul, **P. Sangwongngam**, and K. Sripimanwat, "Performance Evaluation of Non Line of Sight Ultraviolet Communications", ***The 33th Electrical Engineering Conference (EECON33)***, 140, pp. 1445– 1 448.
- P. Treeviriyanupab, **P. Sangwongngam**, K. Sripimanwat, and O. Sangaroon, "Performance of 1/2-Rate Convolutional Code on Winnow Protocol for Quantum Key Reconciliation", ***2010 10th International Symposium on Communications and Information Technologies (ISCIT2010)***, 115, pp. 550–553
- K. Woradit, N. Wattanamongkhol, **P. Sangwongngam**, L. Wuttisittikulkij, "An alternative state diagram of HDB3," ***ITC-CSCC2009***, 6–8 Jul. 2009.
- S. Jantarachote, J. Wetcharungsri, P. Sikangwan, **P. Sangwongngam**, K. Sripimanwat, C. Punyasai, N. Afzulpurkar, "Implementation of CIDS - BC- LDPC Decoder on FPGA," ***ITC-CSCC2009***, 6–8 Jul. 2009.
- **P. Sangwongngam** and K. Sripimanwat, "Performance evaluation of iterative decoding in application of magnetic recording systems,"***NAC 2007***. 2007.
- P. Vanichchanunt, **P. Sangwongngam**, S. Nakpeerayuth, and L. Wuttisittikulkij, "APP demodulator for turbo coded unitary space-time modulation," ***Proc. IEEE Int. Conf. Commun. (ICC'05)***, South Korea, May 2005.
- **P. Sangwongngam**, P. Vanichchanunt, S. Segkhoonthod, S. Nakpeerayuth, and L. Wuttisittikulkij, "An APP demodulator for iterative decoding of turbo coded differential space-time modulation with unitary group cod es," ***Proc. IEEE TENCON. (TENCON 2004)***, Chiang Mai, Thailand, Nov. 2004.

PATENTS/PETTY PATENTS

All filed in Thailand:

- Patent title: "Reconciliation with Channel Coding for Quantum Key Distribution" (Filing Application). Application Number: 1201005110. Filing Date: 28/09/2012.
  Designed to comply with ETSI standards; invented for high speed QKD in telecommunication network.

- Patent title: "Efficient authentication methods and key management for secured communications" Filing number: 1201000033.
  Improved security level of current top-secret online meetings in both industrial and government sectors; invented key management mechanisms suit to composable security of QKD targeting but not limited to video conference applications.

- Patent title: “Design of a compact low-cost LED driver for visible light communications” Filing number: 1201002990. Filing date: 20/06/2012.
  Improved power conversion efficiency of driving circuits of LEDs in visible light communications; focused on applications of visible light communications.

- Petty patent title: “The generation of entangled photons using linear optical elements” Filing number: 1203000179.
  Invented a linear optical scheme to generate the polarization-entangled photon pairs state that is important to the field of quantum information. It does not depend on the physical mechanism of a non-linear crystal such as BBO and can be used in a wide range of experiments in quantum cryptography and computing.

- Petty patent title: “LDPC decoder for 3G mobile communications”. Filing number: 0903001126.
  The design of the LDPC decoder facilitates the block-circulant property to achieving better trade-offs between an implementation area and a throughput for 3G wireless telecommunications.

EXTRACURRICULAR ACTIVITIES

Exchange student, IAESTE program 2005. Visited Switzerland.
Member, Golf Club, Chulalongkorn University.
Member, Self-Defense Club, Chulalongkorn University.
Member, Electronics and Computer Club, Prince of Songkhla University.

COMMUNITY SERVICE AND INVOLVEMENT

Volunteer, the IEEE Communications Society (as an IEEE Member). Organized numerous seminars and talks by experts in fields of quantum cryptography and communications engineering for local community (including IEEE Distinguished Lecturer Program in Thailand). Co-worked book translation of “the translation version of the IEEE History Center’s Virtual Museum (ISBN: 978-974-88238-7-4)” and “A Brief History of Communications”, distributed to schools and universities libraries nationwide.

Writer, a eulogy on “A Tribute to Punya Thitimajshima: a co-inventor of turbo codes” for an outstanding Thailand's research Prof. Dr. Punya Thitimajshima for IEEE Communication Society.

Active Member, Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology Association of Thailand (ECTI Thailand). Conducted Thai Telecommunications Encyclopedia project for Thais (http://www.thaitelecomkm.org/).

Committee, "Fourteenth National Software Contest (NSC 2012)", Thailand.

Co-organizer, Thai Quantum Information (Q-Ti) forum founded by National Electronics and Computer Technology Center (NECTEC) and other academic institutes to be research and educational community in Thailand.

Social Volunteer, the government's Flood Relief Operations Center, Bangkok, Thailand, 2011.

“ประวัติบุคลากรในโครงการ”

http://www.thaitelecomkm.org/ks/

1. นายเกียรติศักดิ์ ศรีพิมานวัฒน์

ตำแหน่ง กรรมการสายวิชาการเทคโนโลยีสารสนเทศ โทรศัพท์ ๐๒-๕๖๔๗๐๐๐ ต่อ ๕๒๓๓

ประวัติการศึกษา

ปริญญาตรี สาขาฟิสิกส์ มหาวิทยาลัยเชียงใหม่
ปีที่จบการศึกษา พ.ศ. 2532

ปริญญาโท สาขาวิศวกรรมไฟฟ้า สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีที่จบการศึกษา พ.ศ. 2537

ปริญญาเอก สาขาการสื่อสารโทรคมนาคม สถาบันเทคโนโลยีแห่งเอเชีย
ปีที่จบการศึกษา พ.ศ. 2543

ผลงาน/ประสบการณ์

1. รางวัลวิทยานิพนธ์ (ชมเชย) ปี 2544

ชื่อวิทยานิพนธ์ การเข้ารหัสและการปรับแต่งสัญญาณล่วงหน้าแบบใหม่สำหรับช่องสัญญาณที่มีการทับซ้อนของการสื่อสารแบบไร้สาย (Modified Trellis Coded Modulation and Precoding for ISI Channels in Wireless Communication)

2. ที่ปรึกษาด้านการศึกษา

- Communications (System) Laboratory (DSL) ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพมหานครฯ (www.kmitl.ac.th/dslabs)
- โปรแกรมวิชาฟิสิกส์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏ บ้านสมเด็จเจ้าพระยา กรุงเทพมหานครฯ
- คณะกรรมการประจำคณะวิทยาศาสตร์และเทคโนโลยี(คณะกรรมการผู้ทรงคุณวุฒิภายนอก) ด้านการบริหารจัดการ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา กรุงเทพมหานครฯ

3. ประวัติการสอน ณ ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และคณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

4. อาจารย์ควบคุมวิทยานิพนธ์มหาบัณฑิตร่วม ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

5. กิจกรรมอาสาสมัคร/ สมาคมวิชาการ

ECTI: Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology Association of Thailand.

ปีพ.ศ. 2545-2546 กรรมการกลาง (Board Committee)
ปีพ.ศ. 2547-2548 ประชาสัมพันธ์ (Public Relations)
ปีพ.ศ. 2549-2550 เลขาธิการ (General Secretary)
ปีพ.ศ. 2553-2554 กรรมการเทคนิค ด้านโทรคมนาคม (ECTI Technical Chair: Telecommunications)

EECON: Electrical Engineering Conference

ปีพ.ศ. 2550-ปัจจุบัน กรรมการ (Committee)

IEEE Thailand Section -IEEE Communications Society (Thailand Chapters)

ปีพ.ศ. 2550- 2554 ประธานสาขาไฟฟ้าสื่อสาร (Chapter Chair)
ECTI association Thailand: Telecommunications
ปีพ.ศ. 2552- 2554 ประธานสาขาโทรคมนาคม (Chapter Chair)
Thai Telecommunications Encyclopedia:
ปีพ.ศ. 2549- ปัจจุบัน บรรณาธิการ (Editor), Thai Telecommunications Knowledge ManagementI
(www.thaitelecomkm.org/)
6. คณะกรรมการร่วมจัดการประชุมวิชาการ ECTI-Con (ECTI International annual conference)
7. อนุสิทธิบัตร
2554 - อุปกรณ์สำหรับการสร้างคู่โฟตอนพัวพันเชิงโพลาไรซ์
2555 - เครื่องเข้ารหัสและถอดรหัสตรวจสอบพาริตี้ความหนาแน่นต่ำ (Low-Density Parity
- Check: LDPC) สำหรับระบบสื่อสารและโทรคมนาคม ตามมาตรฐาน IEEE802.16e
- วิธีการทดสอบและหาคุณภาพของจำนวนสุ่ม
8. บทความวิชาการ/บทความการประชุมวิชาการ
8.1 บทความวิชาการด้านการสื่อสารด้วยแสงที่มองเห็นได้ (Visible Light Communications) และวิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography) และที่เกี่ยวข้อง
8.2 บทความวิชาการด้านการสื่อสาร (Communications) และอื่น ๆ ที่เกี่ยวข้อง