PBRU SCIENCE JOURNAL
2022.19(2) : 100-108

การเข้ารหัสเชิงควอนตัม: แนวทางการรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต

Quantum Cryptography: The Way to Encounter Cyber Threat in the Future

ดนัย ปฏิยุทธ
Danai Patiyoot
กองวิชาวิศวกรรมศาสตร์ ฝ่ายศึกษา โรงเรียนนายเรือ ต.ปากน้ำ อ.เมือง จ.สมุทรปราการ 10270
Department of Engineering, Education section, Royal Thai Naval Academy, Paknam, Muang, Samutprakran 10270
*Corresponding author; E-mail: danaipatiyoot@gmailcom
Received: 23 November 2021/Revised: 29 December 2021/Accepted: 24 February 2022

บทคัดย่อ

ในบทความนี้เป็นการกล่าวถึงการเข้ารหัสเชิงควอนตัมโดยได้อธิบายถึงการแจกจ่ายกุญแจเข้ารหัส ซึ่งใช้กลศาสตร์ควอนตัม เรียกว่าการแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัม (Quantum Key Distribution; QKD) การแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัมมีจุดเด่น คือผู้ส่งและผู้รับสามารถตรวจจับได้ว่ากุญแจการเข้ารหัสถูกแอบดังฟังหรือเก็บข้อมูลโดยบุคคลที่สาม และตอนท้ายของบทความได้แสดงให้เห็นถึงการนำการเข้ารหัสเชิงควอนตัมไปใช้งานจริง โดยประเทศต่าง ๆ

คำสำคัญ: การเข้ารหัสเชิงควอนตัม ภัยคุกคามทางไซเบอร์

Abstract

In this article, quantum cryptography is mentioned by explaining of how to distribute the key for encryption, using quantum mechanics, called “Quantum Key Distribution: QKD”. The advantage of the distribution of the encrypted key by quantum cryptography is that the sender and receiver can detect when the key has been intruded by third parties. At the end of the article, it is mentioned of how countries around the world have adopted the quantum cryptography for their uses.

Keywords: Quantum Cryptography, Cyber threat

บทนำ

ในยุคปัจจุบันที่เป็นโลกของการทำธุรกรรม (ระหว่างบุคคล 2 ฝ่าย) เกือบทุกอย่างผ่านอินเทอร์เน็ต ไม่ว่าเป็นการจ่ายบิล การซื้อของ หรือการเล่นสื่อโซเชียลต่าง ๆ และภัยคุกคามต่อการทำธุรกรรมนั้น ๆ นับวันยิ่งเพิ่มมากขึ้นเรื่อย ๆ และหลากหลายรูปแบบ จึงมีความจำเป็นต้องปกป้องข้อมูลส่วนตัวบนโลกอินเตอร์เน็ตด้วยการเข้ารหัสเพื่อปกป้องข้อมูล วิธีการเข้ารหัสข้อมูลมีทั้งแบบสมมาตร (Symmetric key cryptography), แบบอสมมาตร (Public key cryptography) เช่น RSA, one-time pad รวมทั้งการเข้ารหัสเชิงควอนตัม (Quantum cryptography)

ในปัจจุบันการเข้ารหัสกุญแจสาธารณะถือเป็นส่วนสำคัญของการรักษาความปลอดภัยของข้อมูล แต่วิธีการนี้พบอุปสรรคจากกลยุทธ์การโจมตีรูปแบบใหม่ ๆ รวมถึงวิวัฒนาการของคอมพิวเตอร์ควอนตัมที่สุดท้ายแล้วจะทำให้เทคโนโลยีการเข้ารหัสส่วนใหญ่ในปัจจุบันไม่ปลอดภัยอีกต่อไป

การเข้ารหัสเชิงควอนตัมเป็นวิธีเข้ารหัสในการแจกจ่ายกุญแจในการนำไปใช้เข้ารหัสของสองฝ่าย โดยการแจกจ่ายกุญแจนั้นกระทำบนเครือข่ายออปติคัล (Optical) โดยกุญแจในการเข้ารหัสถูก Encode ในรูปของ โฟตอน (ก้อนแสง)(Photon) และการเข้ารหัสแบบควอนตัมมีความปลอดภัยสูง อีกทั้งยังสามารถบอกได้ว่ามีใครแอบดักฟังหรือเก็บข้อมูลโดยอาศัยคุณสมบัติของกลศาสตร์ควอนตัม (คุณสมบัติบางอย่างของอนุภาคคือการที่อนุภาคไม่สามารถวัดได้โดยไม่รบกวนอนุภาคและเปลี่ยนผลลัพธ์ กล่าวคืออนุภาคมีอยู่ในสถานะของการไม่แน่ใจจนกว่าจะทำการวัดบังคับให้เลือกสถานะหนึ่งหรืออื่นใด ดังนั้นหากมีคนทำการวัดอนุภาคมันจะเปลี่ยนแปลงอนุภาคอย่างถาวร เปรียบเช่นเหรียญซึ่งวางตรงๆ บนโต๊ะบนสันเหรียญ ไม่ได้ออกหัวหรือก้อย ถ้าโต๊ะเกิดการสั่นไหว เหรียญจะเปลี่ยนสถานะทันที)

โพลาไรเซชัน (Polarisation)

โมเดลต้นแบบของการสร้างรหัสควอนตัมแบบหนึ่งคือ BB84 เสนอโดย Charles Bennett และ Gilles Brassard ในปี 1984 สิ่งที่จะนำมาใช้ในการสร้างรหัสควอนตัมคือ โฟตอนเดี่ยว (Single photon) ซึ่งเป็นอนุภาคควอนตัมของแสง สมบัติที่สนใจของโฟตอนในที่นี้คือ โพลาไรเซชัน (Polarisation) ซึ่งเลือก 2 เบสิส (Basis) คือ [1]

1. เบสิสปกติ (Rectangular basis) มีแนวดิ่ง (แทนด้วย 0)และแนวราบ (แทนด้วย 1) (Shown in Figure 1)

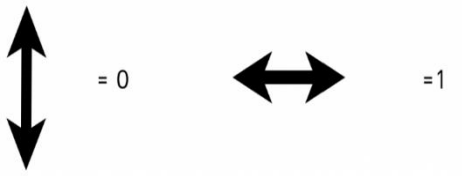

Figure 1. Normal basis

2. เบสิสทแยง (Diagonal basis) แนวทแยงซ้าย (แทนด้วย 0) และทแยงขวา (แทนด้วย 1) (Shown in Figure 2)

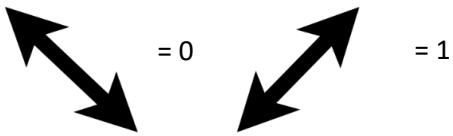

Figure 2. Diagonal basis

3. การวัดทิศของโพลาไรเซชันนั้น สามารถทำได้โดยการส่งโฟตอนผ่านฟิลเตอร์ (Filter)

ซึ่งมีอยู่ 2 แบบตามเบสิสตามแนวทิศของโพลาไรเซชัน (Shown in Figure 3)

Figure 3. Type of filters

4. กรณีที่ 1 หากเลือกฟิลเตอร์ที่สอดคล้องกับทิศของโพลาไรเซชัน จะได้ผลของการวัดที่แน่นอน (เข้าทางซ้ายออกทางขวา) (Shown in Figure 4)

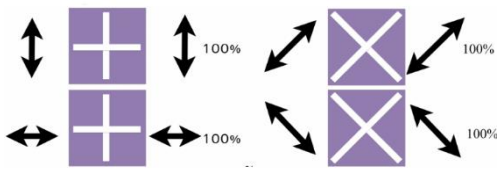

Figure 4. Choosing filter according to direction of polarization

5. กรณีที่ 2 หากเลือกฟิลเตอร์ไม่สอดคล้องกับทิศของโพลาไรเซชัน เช่น (Shown in Figure 5)

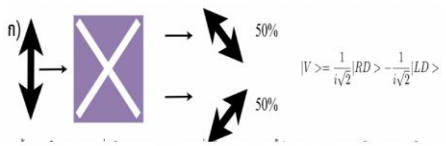

Figure 5. Choosing a filter not according to the direction of polarisation (Diagonal filter & vertical polarisation)

6. นั่นคือมีโอกาส 50% ที่จะได้ทแยงซ้ายและ 50% ที่จะได้ทแยงขวา ซึ่งเป็นผลมาจากหลักความไม่แน่นอนของ

ไฮเซนเบิร์ก (Heisenberg uncertainty principle: การวัดสถานะการโพลาไรเซชันของโฟตอนนั้น ไม่สามารถทำได้โดยไม่รบกวนระบบ) ขอให้ระบุอ้างอิงเพื่อให้งานของผู้วิจัยสมบูรณ์มากยิ่งขึ้น หรืออาจมองได้ว่าเนื่องจากทิศโพลาไรเซชันของโฟตอนแนวดิ่งสามารถเขียนในรูปของสถานะซ้อนทับ (Superposition: สามารถอยู่ในสถานะควอนตัมได้หลายสถานะในเวลาเดียวกันคือเป็นสถานะที่บิตเป็นทั้ง 0 และ 1 ในเวลาเดียวกัน) ระหว่างทิศทแยงซ้ายและทแยงขวา (Shown in Figure 6)

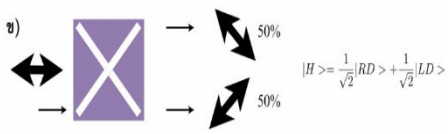

Figure 6. Choosing a filter not according to the direction of polarisation (Diagonal filter & horizontal polarisation)

สำหรับกรณีนี้มีโอกาส 50% ที่จะได้ทแยงซ้ายและ 50% ที่จะได้ทแยงขวา เนื่องจากทิศโพลาไรเซชันของโฟตอนแนวราบสามารถเขียนในรูปของสถานะซ้อนทับ (Superposition) ระหว่างทิศทแยงซ้ายและทแยงขวา (Shown in Figure 7)

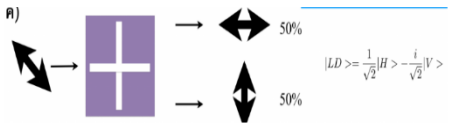

Figure 7. Choosing a filter not according to the direction of polarisation (Normal filter & left diagonal polarisation)

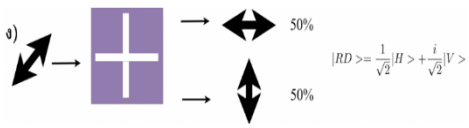

Figure 8. Choosing a filter not according to direction of polarisation (Normal filter & right diagonal polarisation)

สำหรับกรณีนี้ก็มีโอกาส 50% ที่จะได้แนวราบ และ 50% ที่จะได้แนวดิ่ง เนื่องจากทิศโพลาไรเซชันของโฟตอนแนวทแยงซ้ายสามารถเขียนในรูปของสถานะซ้อนทับ (Superposition) ระหว่างทิศแนวดิ่งและแนวราบ (Shown in Figure 8)

สำหรับกรณีนี้มีโอกาส 50% ที่จะได้แนวราบ และ 50% ที่จะได้แนวดิ่ง เนื่องจากทิศโพลาไรเซชันของโฟตอนแนวทแยงขวาสามารถเขียนในรูปของสถานะซ้อนทับ (Superposition) ระหว่างทิศแนวดิ่งและแนวราบ (Shown in Figure 8)

กระบวนการสร้างกุญแจเข้ารหัสและเช็คความปลอดภัยของกุญแจเข้ารหัส

1. กระบวนการสร้างกุญแจเข้ารหัส

สมมุติว่าอลิสและบ๊อบต้องการสื่อสารกันอย่างเป็นความลับ ดังนั้นทั้งสองต้องสร้างรหัส วิธีการก็คืออลิสทำการส่งสายของโฟตอนเดี่ยวที่ไม่มีทิศของโพลาไรเซชันผ่านฟิลเตอร์ 4 แบบ โดยทำการเลือกชนิดของฟิลเตอร์แบบสุ่ม ส่งผลทำให้โฟตอนที่ออกมามีทิศโพลาไรเซชันแบบสุ่มแล้วส่งไปให้บ๊อบผ่านช่องทางควอนตัม (Quantum channel) (Shown in Figure 9) [1]

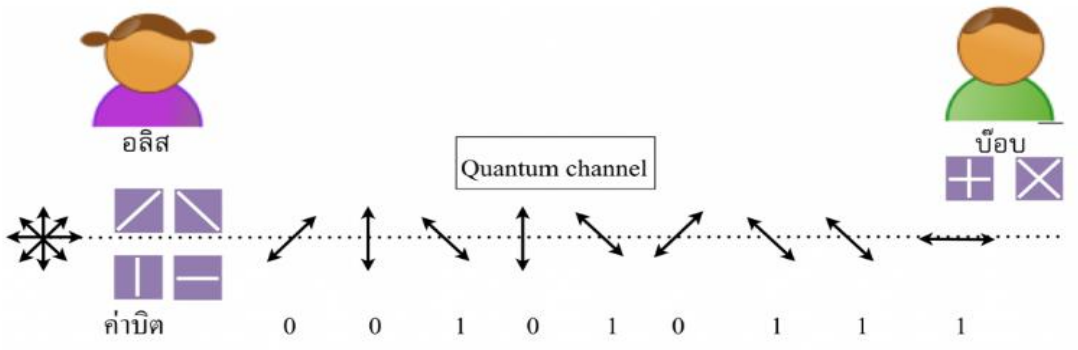

Figure 9. Alice sends single photon that does not have the direction of polarisation through four types of filters

บ๊อบซึ่งไม่รู้ทิศโพราไลเซชันของแต่โฟตอนที่ส่งมาหรือไม่รู้เป็นเบสิสแบบไหน สิ่งที่บ๊อบทำได้คือเลือกฟิลเตอร์ที่มี 2 แบบอย่างสุ่ม เพื่อทำการวัดทิศของโพลาไรเซชัน ดังรูปด้านล่าง ซึ่งมีทั้งตรงและไม่ตรง (Shown in Figure 10)

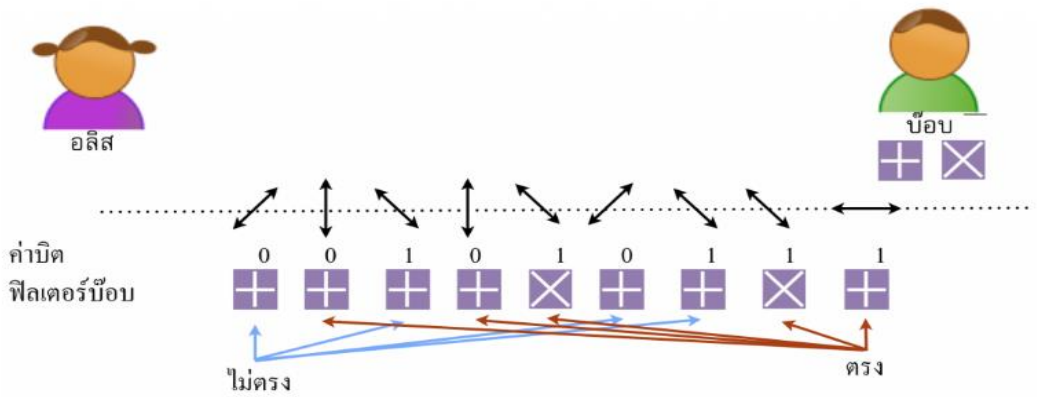

Figure 10. Bob chooses randomly two types of filters

หากบ๊อบเลือกฟิลเตอร์ผิด จะเกิดโอกาส 50% ในการที่จะได้โพราไลเซชันในแต่ละทิศสำหรับเบสิสใหม่ หากเลือกถูกก็จะได้ผลถูกต้อง 100% (Shown in Figure 11)

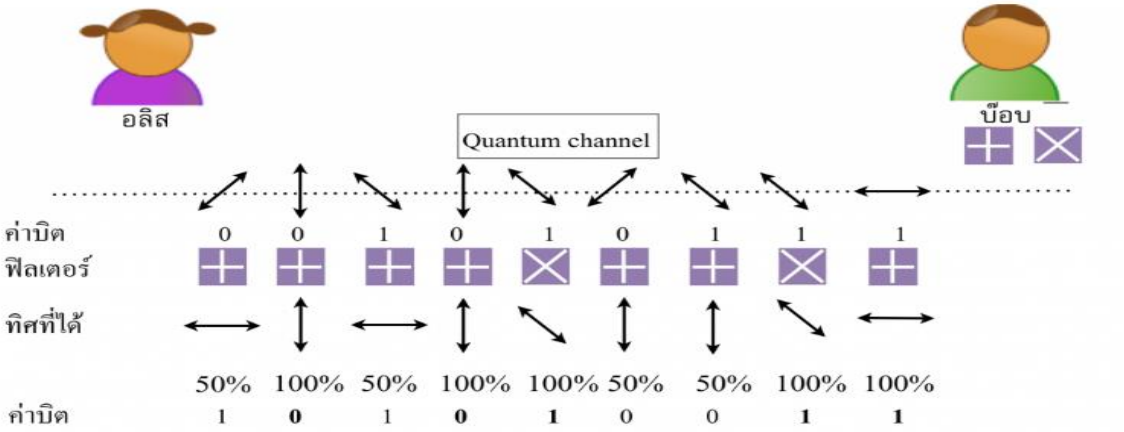

Figure 11. Bob chooses both right and wrong filters

เมื่อบ๊อบวัดเสร็จแล้วจะทำการสื่อสารกับอลิสผ่านช่องทางสาธารณะ (Classical channel) เช่น โทรศัพท์ เพื่อบอกลำดับฟิลเตอร์ที่ใช่ในการวัดทิศของโพลาไรเซชัน(โดยไม่ได้บอกค่าบิตที่ได้) อลิสแค่บอกว่าฟิลเตอร์ไหนถูกต้อง เมื่อบอกหมดแล้วก็ทำการทิ้งค่าบิตที่เกิดจากการวัดที่ฟิลเตอร์ไม่ถูกต้อง แล้วเก็บค่าบิตที่ฟิลเตอร์ตรงกันไว้อย่างเดียว (Shown in Figure 12)

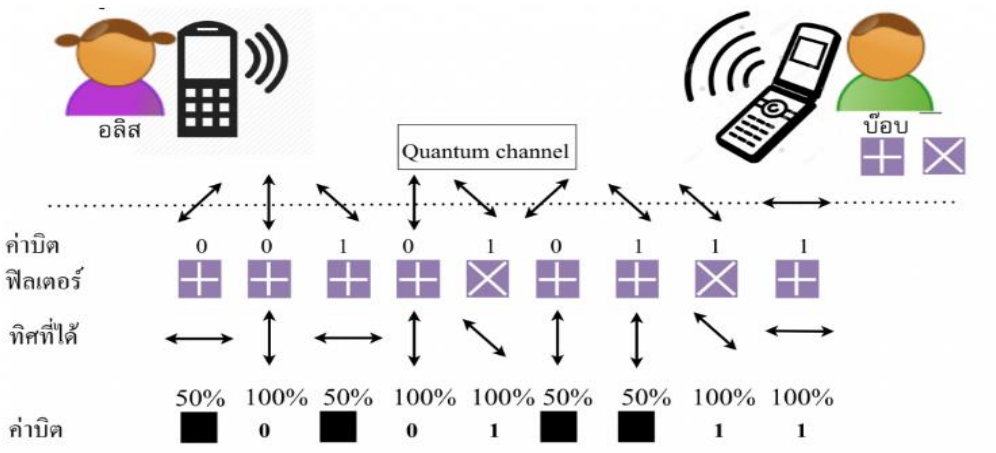

Figure 12. Bob communicates via public network and tells the sequence of filters

ทั้งคู่จะแชร์ลำดับบิต 00111 ซึ่งจะถูกใช้เป็นรหัสในการสื่อสาร ลำดับบิตดังกล่าวสร้างขึ้นมาแบบสุ่ม ซึ่งนำไปใช้ในการเข้ารหัสแบบ One-time pad

นอกจากนั้น ยังสามารถหา Shared secret key ได้อีกวิธีหนึ่งดังนี้ (Shown in Table 1)

Table 1. Methods in finding “Shared secret key”

Alice’s random bit	0	1	1	0	1	0	0	1
Alice’s random bases	+	+	×	+	×	×	×	+
Alice’s polarizations	↑	→	↖	↑	↖	↗	↗	→
Bob’s random bases	+	×	×	×	+	×	+	+
Bob’s measurements	↑	↗	↖	↗	→	↗	→	→
Values kept afterwards	✓		✓			✓		✓
Shared secret key	0		1			0		1

ซึ่งในกรณี Shared secret key คือ 0101

2. กระบวนการเช็คความปลอดภัยของกุญแจเข้ารหัส

หากตอนนี้ถ้าต้องการรู้ว่าทั้งสองพูดคุยอะไรกัน จึงต้องทำการดักเอารหัสในขั้นตอนของการสร้างรหัส สถานการณ์ของบุคคลที่ 3 (C) ก็ไม่ต่างจากบ๊อบ เพราะต้องเลือกฟิลเตอร์แบบสุ่มเหมือนกัน (Shown in Figure 13) [1]

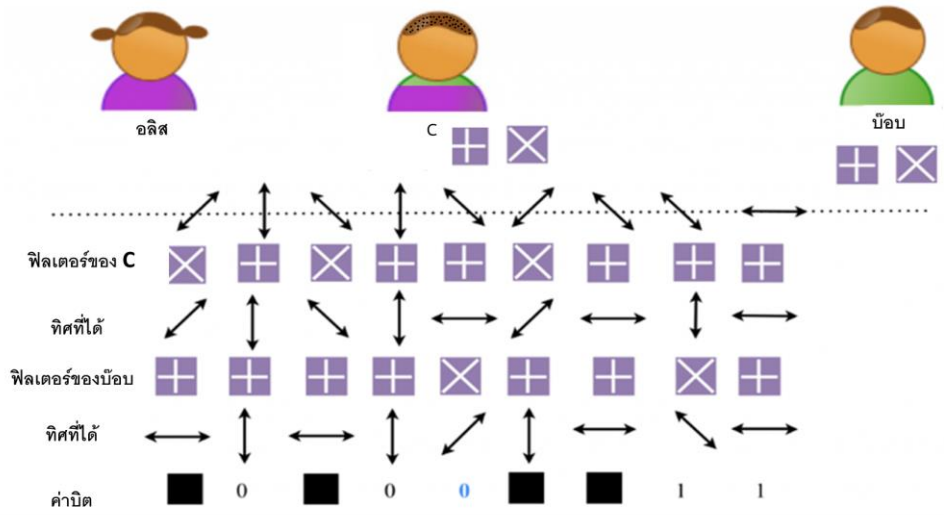

Figure 13. Eavesdropping the conversation between A and B

จะเห็นได้ว่าลำดับของรหัสนั้นเปลี่ยนไปจาก 00111 เป็น 00011 เป็นผลของการที่ C เข้ามาวัดทิศของโพลาไรเซชันซึ่งเลือกฟิลเตอร์ผิดส่งผลทำให้ทิศเปลี่ยนไปเมื่อถึงบ๊อบจึงทำให้ผลการวัดเปลี่ยนไปด้วย ทำให้ทั้งคู่รู้ทันทีว่ามีคนมาดักเอารหัส เมื่ออลิสและบ๊อบรู้ว่ารหัสโดนดักไปแล้วทั้งคู่ก็แค่ทิ้งรหัสชุดนั้นไปแล้วไปสร้างใหม่ยังช่องทางควอนตัมอื่นแทน

1. การนำไปใช้งานจริง

ในปัจจุบันเราเริ่มเห็นเครือข่าย Quantum Key Distribution (QKD) เพิ่มมากขึ้น โดยเครือข่าย QKD ที่ยาวที่สุดอยู่ในประเทศจีน ซึ่งมีเส้นทางเชื่อมโยงภาคพื้นดินระหว่างปักกิ่งและเซี่ยงไฮ้ เป็นระยะทาง 2,032 กิโลเมตร (1,263 ไมล์) และจุดเชื่อมต่อจากภาคพื้นดินสู่ดาวเทียมจำนวน 2 แห่ง ซึ่งสามารถทำการกระจายกุญแจเข้ารหัสเชิงควอนตัม (Quantum Key Distribution: QKD) ระหว่างผู้ใช้มากกว่า 150 รายในระยะทางรวม 4,600 กิโลเมตร

ในฟากฝั่งของอเมริกาก็มีธนาคารและบริษัทการเงินต่าง ๆ ใช้เพื่อส่งข้อมูลแล้ว เช่น สตาร์ทอัพ Quantum Xchange ที่เชื่อมแมนฮัตตันกับรัฐนิวเจอร์ซีย์ในระยะทาง 805 กิโลเมตร (500 ไมล์) [4]

อินเดียสร้างการเชื่อมโยงการสื่อสารระหว่างห้องปฏิบัติการกลาโหมซึ่งมีการป้องกันการเจาะระบบในเดือนธันวาคม พ.ศ. 2563 โดยศูนย์วิจัยอิมราชและห้องปฏิบัติการวิจัยและพัฒนาด้านกลาโหมซึ่งอยู่ห่างกัน 12 กิโลเมตรในไฮเดอราบัด เชื่อมต่อกันด้วยการเชื่อมโยงข้อมูลการกระจายกุญแจเข้ารหัสเชิงควอนตัม ซึ่งเป็นส่วนสำคัญในการพัฒนาเทคโนโลยีการกระจายกุญแจเข้ารหัสเชิงควอนตัม [5]

สมาร์ทโฟน Samsung Galaxy Quantum สัญชาติเกาหลีใต้ โดยมือถือรุ่นนี้ใช้การเข้ารหัสเชิงควอนตัม (Quantum cryptography) (Shown in Figure 14) โดยการใช้ชิป Quantum Random Number Generator (QRNG) ที่มีขนาด 2.5 มม. เท่านั้น ซึ่งจะใช้สำหรับการเข้ารหัสควอนตัมด้วยการนำเสียงที่เกิดจากหน้าจอ LED และเซ็นเซอร์ในกล้อง

อย่าง CMOS Image Sensor ไปใช้ในงานเข้ารหัส ซึ่งการเข้ารหัสแบบนี้จะเป็นการสุ่มการเข้ารหัสอย่างแท้จริง และไม่สามารถคาดเดาได้ (Shown in Figure 14)[3]

Figure 14. Smart phone "Samsung Galaxy Quantum" that uses Quantum cryptography (อ้างอิงภาพจาก [3])

ปัจจุบันมีหลากหลายธนาคารและเซอร์วิสต่าง ๆ ที่รองรับการทำงานร่วมกับการเข้ารหัสเชิงควอนตัม ไม่ว่าจะเป็น T World, T Pass และ T Membership ที่เป็นบริการของ SK Telecom หรือ Shinhan Bank Standard และ Chartered Bank Korea ก็มีบริการที่รองรับ Quantum Cryptography เช่นเดียวกัน [3]

สรุป

ข้อดีของการเข้ารหัสเชิงควอนตัมนั้นอยู่ที่การสร้างรหัสที่สามารถตรวจสอบการเข้ามาของบุคคลที่ 3 ได้ และหากสร้างรหัสสำเร็จก็สามารถนำไปเข้ารหัสข้อความได้ โดยเทคโนโลยีควอนตัมจะเข้ามาสร้างความมั่นคงในเชิงความปลอดภัยของข้อมูล ไม่ว่าจะเป็นข้อมูลทางการทหาร ข้อมูลในเชิงธุรกิจ ช่วยยกระดับการรักษาข้อมูลส่วนบุคคล ทั้งในด้านการสื่อสาร การเงินการธนาคาร และการทำธุรกรรมผ่านอินเทอร์เน็ต เพราะการสื่อสารเชิงควอนตัมสามารถปกป้องข้อมูลให้เป็นความลับผ่านการเข้ารหัสเชิงควอนตัมที่จะไม่สามารถโจรกรรมได้ตัวอย่างการใช้งานที่เป็นรูปธรรมคือการเข้ารหัสเชิงควอนตัมของสมาร์ทโฟนยี่ห้อ Samsung

เอกสารอ้างอิง

1 การเข้ารหัสทางควอนตัม (Quantum Cryptography) [Internet]. 2018 [cited 2021 Oct 7]. Available from: https://www.qute-th.com/2018/11/29/การเข้ารหัสทางควอนตัม-quantum-c/

2 การเข้ารหัสทางควอนตัม (Quantum Cryptography) [Internet]. 2015 [cited 2021 Oct 7]. Available from: https://www.techtalkthai.com/quantum-key-distribution-part-1/

3 Galaxy Quantum 2 ใช้การเข้ารหัสเชิงควอนตัมเพิ่มความปลอดภัยให้แอป โดยเฉพาะกลุ่ม Mobile Banking [Internet]. 2021 [cited 2021 Oct 7]. Available from: https://droidsans.com/

galaxy-quantum-2-equipped-with-qrng-quantum-cryptography-chip/

4 การสื่อสารเชิงควอนตัม (Quantum Communication) คืออะไร [Internet]. 2019 [cited 2021 Oct 7]. Available from: https://www.blockdit.com/posts/5cdbf6e850ad781f982390aa

5 อินเดียใช้การเปลี่ยนแปลงเชิงควอนตัมเพื่อรักษาความปลอดภัยด้านการสื่อสาร [Internet]. 2021 [cited 2021 Oct 7]. Available from: https://ipdefenseforum.com/th/2021/01/อินเดียใช้การเปลี่ยนแป/

6 Federico Grasselli. Quantum Cryptography: From Key Distribution to Conference KeyAgreement. Springer; 2021.