วารสารวิศวกรรมศาสตร์และนวัตกรรม
Journal of Engineering and Innovation

บทความวิจัย

การศึกษาประสิทธิภาพการประมวลผลกำเนิดรหัสลับส่วนหลังในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศแบบพัวพัน

Experimental study of post-processing for key generation in entangled free-space quantum key distribution system

พัชรพงษ์ ตรีวิริยานุภาพ[1]* ปรมินทร์ แสงวงษ์งาม[2]

[1] สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏพระนคร เขตบางเขน กรุงเทพมหานคร 10220

[2] กลุ่มวิจัยอุปกรณ์สเปกโทรสโกปีและเซนเซอร์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ อำเภอคลองหลวง ปทุมธานี 12120

Patcharapong Treeviriyanupab[1]* Paramin Sangwongngam[2]

[1] Department of Information Technology, Faculty of Science and Technology, Phranakhon Rajabhat University, Bangkok 10220

[2] Spectroscopic and Sensing Devices Research Group, National Electronics and Computer Technology Center, Pathum Thani 12120

* Corresponding author.

E-mail: patcharapong@pnru.ac.th; Telephone: 0 2544 8556

วันที่รับบทความ 28 มีนาคม 2566; วันที่แก้ไขบทความ ครั้งที่ 1 31 พฤษภาคม 2566; วันที่ตอบรับบทความ 22 มิถุนายน 2566

บทคัดย่อ

บทความนี้นำเสนอการออกแบบและพัฒนากระบวนการประมวลผลกำเนิดกุญแจรหัสลับส่วนหลังในรูปแบบซอฟต์แวร์ที่สอดคล้องตามหลักปฏิบัติของระบบการกระจายกุญแจรหัสลับเชิงควอนตัม ประกอบด้วยขั้นตอนวิธีทั้งสามส่วนหลัก ได้แก่ 1) การประมาณค่าพารามิเตอร์อัตราความผิดพลาดบิตเชิงควอนตัมโดยอาศัยวิธีการสุ่มตัวอย่างบิต 2) การไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีแบบปรับอัตราเข้ารหัสอย่างเหมาะสมทำงานร่วมกับวิธีการยืนยันความถูกต้องด้วยฟังก์ชันแฮชแบบพหุนาม และ 3) การขยายสภาวะส่วนตัวด้วยฟังก์ชันแฮชเชิงเอกภพที่อาศัยการสุ่มชุดข้อมูลไบนารีตามโครงสร้างของเมทริกซ์แบบโทพลิทซ์ภายใต้เงื่อนไขของอัตราการกำเนิดกุญแจรหัสลับที่ปลอดภัยจากผลการทดสอบประสิทธิภาพร่วมกับระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบพัวพันตามเกณฑ์วิธีการ BBM92 บนช่องสัญญาณเชิงควอนตัมผ่านอากาศในระยะทาง 11 เมตร จำนวน 100 รอบการทำงาน ซึ่งให้กำเนิดกุญแจซิฟท์มีอัตราเร็วเฉลี่ยเท่ากับ 1,109.08 บิตต่อวินาที โดยวิธีการที่นำเสนอมีประสิทธิภาพในการประมวลผลสร้างข้อตกลงร่วมกันระหว่างคู่สื่อสารกำเนิดเป็นกุญแจรหัสลับที่มีค่าถูกต้องตรงกันตามหลักความปลอดภัยทางทฤษฎีสารสนเทศได้ผลลัพธ์ของค่าเฉลี่ยการประมาณค่าอัตราความผิดพลาดบิตเชิงควอนตัมเท่ากับ 2.0127% ค่าเฉลี่ยประสิทธิภาพการไกล่เกลี่ยความผิดพลาดเท่ากับ 1.1919 และค่าเฉลี่ยอัตราการกำเนิดกุญแจรหัสลับสุดท้ายเท่ากับ 428.42 บิตต่อวินาที ขั้นตอนวิธีที่ได้นำเสนอสามารถนำไปปรับค่าพารามิเตอร์อินพุตที่เหมาะสมกับการประมวลผลในแต่ละขั้นตอนเพื่อรองรับการประยุกต์ใช้งานจริงร่วมกับอุปกรณ์การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องโดยเฉพาะอย่างยิ่งกับระบบที่ต้องการความเร็วสูงต่อไป

คำสำคัญ

วิทยาการรหัสลับเชิงควอนตัม การกระจายกุญแจรหัสลับเชิงควอนตัม การประมวลผลกำเนิดรหัสลับเชิงควอนตัมส่วนหลัง หลักความปลอดภัยทางทฤษฎีสารสนเทศ การไกล่เกลี่ยความผิดพลาด การขยายสภาวะส่วนตัว

Abstract

This paper presents the design and development of practical post-processing software for a general quantum key distribution system. The proposed algorithms consist of three main contributions: 1) channel parameter estimation for

quantum bit error rates by a random key sampling method, 2) information reconciliation using rate-adaptive LDPC codes, that collaborate with identical key confirmation by employing a polynomial-based hash function, and 3) privacy amplification performed by a universal hash function, where the binary information is randomly chosen to construct the Toeplitz matrix corresponding to the condition of a secure secret key rate. The proposed post-processing algorithms were implemented and tested in an entangled quantum key distribution experiment based on the BBM92 protocol over a 11-meter free-space quantum channel link. The experiment was conducted over 100 cycles and was able to generate the average sifted key rate of 1,109.08 bits per second. The efficiency of the proposed algorithms enabled two legitimate parties to generate the identical secret key according to the information-theoretic security principles, where the average estimated quantum bit error rate was 2.0127%, the average efficiency of information reconciliation was 1.1919, and the average final secret key rate was 428.42 bits per second. The proposed algorithms could be used in the industrial quantum key distribution systems based on a discrete-variable protocol by optimizing the input parameters of the post-processing procedure, especially for high-speed applications.

Keywords

quantum cryptography; quantum key distribution; QKD post-processing; information-theoretic security; information reconciliation; privacy amplification

1 บทนำ

การพัฒนาเทคโนโลยีการกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum key distribution: QKD) เกิดขึ้นในปี พ.ศ. 2527 [1] โดยอาศัยพื้นฐานสารสนเทศเชิงควอนตัม (Quantum information) มารับประกันความปลอดภัยในการกำเนิดชุดข้อมูลกุญแจรหัสลับภายใต้หลักการคัดลอกไม่ได้ (No-cloning theorem) [2] เมื่อใดที่สถานะควอนตัม (Quantum state) ที่ใช้แทนค่าสารสนเทศถูกคัดลอกหรือวัดค่าจะเป็นผลให้สถานะเกิดการเปลี่ยนแปลงทำให้คู่สื่อสารทราบถึงการดักจับข้อมูลระหว่างการสื่อสาร (Eavesdropping) จากค่าอัตราความผิดพลาดที่สูงขึ้น และสามารถยกเลิกการใช้ชุดข้อมูลนั้นได้ นำไปสู่การเป็นวิธีการรักษาความมั่นคงของข้อมูลแบบไม่มีเงื่อนไขขึ้นกับขีดจำกัดความสามารถของอุปกรณ์การคำนวณใดๆ (Unconditionally security) [3]

ในการพัฒนาเทคโนโลยี QKD สู่การใช้งานจริงเป็นโครงสร้างพื้นฐานการรักษาความปลอดภัยข้อมูลสารสนเทศในระบบการสื่อสาร [4,5] จำเป็นต้องพิจารณาทางเทคนิคในสองส่วนหลัก ดังนี้

1) อุปกรณ์ฮาร์ดแวร์เชิงแสง (Optical hardware devices) สำหรับการกำเนิดและตรวจจับค่าสถานะควอนตัมทั้งในรูปแบบโฟตอนเดี่ยว (Single photon) หรือคู่โฟตอนพัวพัน (Entangled photon pairs) [6] รับส่งผ่านช่องสัญญาณเชิงควอนตัม (Quantum channel) ระหว่างอุปกรณ์คู่สื่อสารภาคส่ง (Alice) กับภาครับ (Bob)

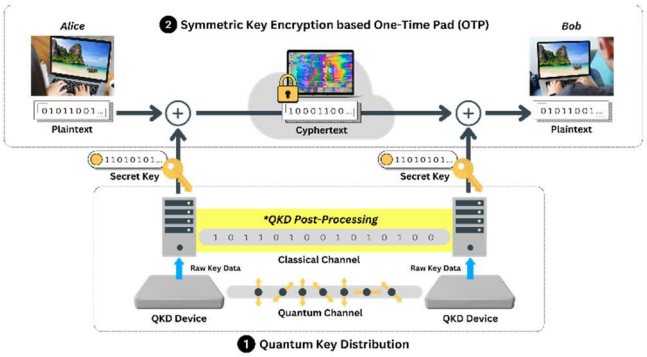
2) การประมวลผลรหัสลับส่วนหลัง (QKD post-processing) เกิดขึ้นบนช่องทางการสื่อสารทั่วไป (Classical channel) อาศัยหลักทฤษฎีข่าวสารสารสนเทศ (Information theory) [7] ในการสร้างข้อตกลงร่วมกันระหว่างคู่สื่อสารเป็นชุดข้อมูลกุญแจรหัสลับ (Secret-key agreement) [8] ที่มีค่าตรงกันโดยสมบูรณ์และมีความปลอดภัยดังตัวอย่างงานวิจัยเชิงทฤษฎีใน [9–12] อีกทั้งการออกแบบและพัฒนาวิธีการ QKD post-processing ประสิทธิภาพสูงจะมีส่วนสำคัญในการเพิ่มขีดความสามารถด้านอัตรากำเนิดกุญแจรหัสลับ (Secret key throughput) จากระบบ QKD ให้เพียงพอต่อการใช้งานจริงร่วมกับเกณฑ์วิธีการเข้ารหัสลับข้อมูลที่เป็นมาตรฐานของระบบการสื่อสารให้มีความมั่นคงปลอดภัยอย่างสูงสุด

งานวิจัยนี้มีวัตถุประสงค์ในการศึกษาประสิทธิภาพตามหลักปฏิบัติของกระบวนการ QKD post-processing [9,11–13] โดยได้นำเสนอการออกแบบขั้นตอนวิธีในการกำเนิดชุดข้อมูลรหัสลับ (Post-processing algorithms) ภายใต้เงื่อนไขความปลอดภัยของระบบ QKD เริ่มต้นจากการนำบิตข้อมูลกุญแจซิฟท์ (Sifted key) ที่ได้จากการแลกเปลี่ยนเวกเตอร์ฐาน (Key sifting) ตามเกณฑ์วิธีการกำเนิดและตรวจจับสถานะเชิงควอนตัมเข้าสู่ขั้นตอนการประมาณค่าหาอัตราความผิดพลาดช่องสัญญาณเชิงควอนตัม (Quantum bit error rate: QBER)

และนำผลของการประมาณค่า QBER ที่ได้มาเป็นพารามิเตอร์ในการออกแบบขั้นตอนการไกล่เกลี่ยความผิดพลาดด้วยวิธีการปรับอัตราเข้ารหัสแอลดีพีซีให้เหมาะสม (Rate-adaptive LDPC codes) [14,15] กับขีดความสามารถในการแก้ไขความผิดพลาดบนเงื่อนไขความปลอดภัยของสารสนเทศ หลังจากนั้นจึงนำชุดข้อมูลกุญแจที่ผ่านการไกล่เกลี่ยความผิดพลาดแล้ว (Reconciled key) เข้าสู่ขั้นตอนการยืนยันความถูกต้อง (Confirmation) โดยการประยุกต์ใช้เทคนิคการเปรียบเทียบรหัสแฮช (Hash) แทนข้อมูล Reconciled key ระหว่างคู่สื่อสารที่ถูกสร้างขึ้นจากฟังก์ชันแฮชแบบพหุนาม (Polynomial hashing function) [16,17] ในส่วนของขั้นตอนการขยายสภาวะส่วนตัว (Privacy amplification) ได้ประยุกต์นำวิธีการสุ่มชุดข้อมูลไบนารีตามรูปแบบของฟังก์ชันแฮชเชิงเอกภพ (Universal hashing function) บนพื้นฐานของเมทริกซ์โทพลิทซ์ (Toeplitz matrix) [9,18] ในการให้กำเนิดข้อมูลกุญแจรหัสลับสุดท้าย (Secret key) ที่ปลอดภัยโดยไม่มีความสัมพันธ์อันใดกับข้อมูลที่ผู้ดักจับ (Eavesdropper: *Eve*) มีโอกาสได้รับทั้งในระหว่างการรับส่งสถานะบนช่องสัญญาณเชิงควอนตัมและสารสนเทศบนช่องสัญญาณการสื่อสารทั่วไป

นอกจากนี้ กระบวนการ QKD post-processing ตามขั้นตอนวิธีที่ได้ออกแบบในงานวิจัยนี้ ถูกนำมาพัฒนาและทดสอบประสิทธิภาพการประมวลผลในรูปแบบซอฟต์แวร์ประสานการทำงานเพื่อรับค่าชุดข้อมูลกุญแจซิฟท์จากการทดสอบบนระบบกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศแบบพัวพัน (Entangled free-space QKD system) ด้วยอุปกรณ์ Einstein–Podolsky–Rosen (EPR) 405 [19,20] พัฒนาขึ้นโดยสถาบันเทคโนโลยีแห่งออสเตรีย (Austrian Institute of Technology: AIT) มาประมวลผลกลั่นกรองข้อมูลเป็นกุญแจรหัสลับที่ปลอดภัย (Secret-key distillation)

เนื้อหาของบทความนี้ ประกอบด้วยส่วนที่ 2 กล่าวถึงหลักการที่เกี่ยวข้องสำหรับการวิจัย ได้แก่ แนวคิดของระบบ QKD และหลักการทำงานของกระบวนการ QKD post-processing ในส่วนที่ 3 นำเสนอการออกแบบขั้นตอนวิธีทั้งหมดของกระบวนการ QKD post-processing และนำเสนอผลการทดสอบประสิทธิภาพการประมวลผลกำเนิดกุญแจรหัสลับส่วนหลังจากระบบ QKD ประเภทคู่โฟตอนพัวพันเป็นเนื้อหาในส่วนที่ 4 และส่วนที่ 5 นำเสนอบทสรุปและข้อเสนอแนะของงานวิจัย



รูปที่ 1 แผนผังของระบบวิทยาการรหัสลับเชิงควอนตัม (Quantum cryptography) โดยแบ่งหลักเกณฑ์การทำงานเป็นสองส่วนหลัก ได้แก่ 1) การกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum key distribution) ประกอบด้วยการรับส่งสถานะบนช่องสัญญาณเชิงควอนตัม (Quantum channel) ประสานการทำงานร่วมกับกระบวนการประมวลผลรหัสลับส่วนหลัง (QKD post-processing) บนช่องทางการสื่อสารทั่วไป (Classical channel) และ 2) การเข้ารหัสลับข้อมูลแบบสมมาตร (Symmetric key encryption) ด้วยอัลกอริทึมเข้ารหัสแบบใช้กุญแจครั้งเดียว (One-time pad: OTP)

2. แนวคิดและหลักการที่เกี่ยวข้อง

เนื้อหาในส่วนนี้กล่าวถึงแนวคิดของระบบ QKD อภิปรายโดยหลักเกณฑ์ของวิทยาการรหัสลับดั้งเดิม และหลักการทำงานของการประมวลผลกำเนิดรหัสลับส่วนหลัง (QKD post-processing)

2.1 แนวคิดของการกระจายกุญแจรหัสลับเชิงควอนตัมโดยหลักเกณฑ์ของวิทยาการรหัสลับแบบดั้งเดิม

วิทยาการรหัสลับที่อาศัยเกณฑ์วิธีการกระจายกุญแจรหัสลับเชิงควอนตัม (QKD) ถูกเรียกว่า วิทยาการรหัสลับเชิงควอนตัม (Quantum cryptography) แสดงได้ดังรูปที่ 1 หากพิจารณาแนวทางการประยุกต์ใช้งานจริงของระบบ QKD บนพื้นฐานหลักเกณฑ์ของวิทยาการรหัสลับแบบดั้งเดิม สามารถอธิบายเป็นสองส่วนหลักดังนี้

2.1.1 หลักเกณฑ์การกระจายกุญแจรหัสลับ (Key distribution protocol)

กระบวนการกำเนิดและแลกเปลี่ยนข้อมูลกุญแจรหัสลับ (Key generation and exchange) หรือโพรโทคอลการกระจายกุญแจรหัสลับ (Key distribution protocol) ที่ใช้งาน

โดย ทั่วไปนั้น ความปลอดภัยของระบบขึ้นกับความยากของปัญหาในการแก้สมการทางคณิตศาสตร์ (Mathematical problems) อาทิ โพรโทคอลอาร์เอสเอ (RSA) [21] ยืนยันความปลอดภัยจากความซับซ้อนในการแยกตัวประกอบ (Integer factorization) โพรโทคอลดิฟฟี่-เฮลแมน (Diffie-Hellman: DH) [22] และโพรโทคอล Elliptic-curve Diffie–Hellman (ECDH) [23] ยืนยันความปลอดภัยจากการแก้ปัญหาของลอการิทึมแบบไม่ต่อเนื่อง (Discrete logarithm) เป็นต้น วิธีการเหล่านี้จึงมีข้อจำกัดด้านความปลอดภัยขึ้นกับความยากในการแก้สมการทางคณิตศาสตร์ (Computational security) ซึ่งมีโอกาสถูกทำลายได้จากอุปกรณ์ประมวลผลประสิทธิภาพสูง เช่น คอมพิวเตอร์ควอนตัม (Quantum computer) [24,25] ที่มีความสามารถในการประมวลผลสารสนเทศเพื่อถอดรหัสข้อมูลภายใต้วิธีการทางคณิตศาสตร์ที่ซับซ้อนได้อย่างรวดเร็ว [26,27]

ดังนั้นวัตถุประสงค์สำคัญของระบบ QKD สามารถนำมาประยุกต์ใช้งานแทนวิธีการแบบดั้งเดิม เพื่อเป็นระบบการกระจายกุญแจรหัสลับที่ไม่ขึ้นกับความสามารถและข้อจำกัดด้านเวลาการประมวลผลของเครื่องคำนวณใดๆ ที่เรียกว่า ความปลอดภัยสารสนเทศแบบไม่มีเงื่อนไข (Unconditional security) [3] โดยอาศัยช่องทางการสื่อสารเฉพาะทางหรือช่องสัญญาณเชิงควอนตัม (Quantum channel) เป็นสื่อกลางระหว่างอุปกรณ์เชิงแสง (QKD Device) ของภาคส่ง (*Alice*) กับภาครับ (*Bob*) ในการรับส่งสถานะควอนตัมแทนด้วยคุณสมบัติของโฟตอน ซึ่งในทางปฏิบัติสามารถแบ่งเทคโนโลยีการให้กำเนิดโฟตอน (Photon sources) เป็นสองระบบ [6] ดังนี้

1) ระบบ QKD แบบการจัดเตรียมแหล่งกำเนิดและการวัดค่าสถานะ (Prepare-and-measure QKD scheme) ที่อาศัยพื้นฐานการกำเนิดและวัดค่าสถานะของโฟตอนเดี่ยว (Single photon) [28] ตัวอย่างเกณฑ์วิธีที่ใช้แทนค่าสถานะในระบบดังกล่าว ได้แก่ โพรโทคอล BB84 [1]

2) ระบบ QKD แบบความพัวพัน (Entanglement-based QKD scheme) อาศัยพื้นฐานของปรากฏการณ์ความพัวพันเชิงควอนตัม (Quantum entanglement) เพื่อให้กำเนิดคู่โฟตอนพัวพันจากแหล่งกำเนิดตัวกลาง (Entangled photon source) [19] และถูกส่งไปวัดค่าสถานะที่ *Alice* และ *Bob* โดยเกณฑ์วิธีในการสร้างข้อตกลงร่วมกันภายใต้ระบบ Entanglement-based QKD ได้แก่ โพรโทคอล E91 [29] และ BBM92 [30]

จากนั้นจึงเข้าสู่กระบวนการ QKD post-processing บนช่องทางการสื่อสารทั่วไป ซึ่งเป็นส่วนหนึ่งภายใต้ระบบ QKD ที่สำคัญในการกลั่นกรองข้อมูลกุญแจดิบ (Raw key data) ตามเกณฑ์วิธีการรับส่งสถานะควอนตัมมาประมวลผลเพื่อกำเนิดเป็นกุญแจรหัสลับ (Secret key) และสามารถออกแบบระบบเพื่อหลีกเลี่ยงการโจมตีแบบคนกลางหรือ Man-in-the-Middle (MITM) attack จากการประเมินค่าอัตราความผิดพลาดบนชุดข้อมูลที่สูงผิดปกติ โดยหลักการและขั้นตอนย่อยของกระบวนการ QKD post-processing ซึ่งเป็นส่วนสำคัญของงานวิจัยในบทความนี้ จะอธิบายในหัวข้อที่ 2.2

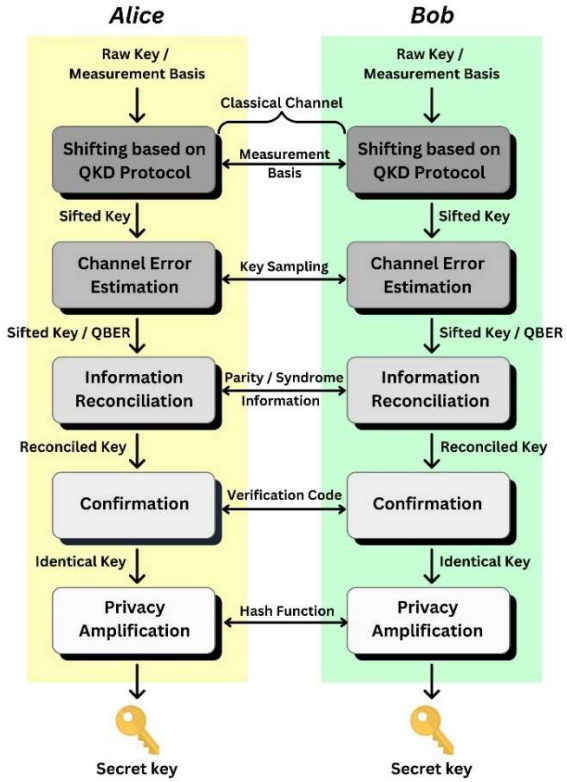
2.1.2 หลักเกณฑ์การเข้ารหัสลับ (Encryption)

การเข้ารหัสเพื่อปกปิดข้อมูลต้นฉบับให้เป็นความลับที่ผู้อื่นไม่สามารถเข้าใจนอกจากคู่สื่อสารตัวจริงเท่านั้น โดยสามารถแบ่งประเภทตามเกณฑ์วิธีการใช้งานชุดกุญแจ [31] ได้แก่ เกณฑ์การเข้ารหัสลับแบบสมมาตร (Symmetric-key algorithms) และแบบอสมมาตร (Asymmetric-key algorithms) โดยทั่วไปวิธีการเข้ารหัสทั้งสองประเภทมีการนำค่าข้อมูลกุญแจมาใช้งานวนซ้ำ (Key reuse) [32] อันเป็นช่องโหว่หนึ่งในการโจมตีเพื่อทำลายความลับของข้อมูลจากพลังการประมวลผลของอุปกรณ์ประสิทธิภาพสูงได้เช่นกัน [24,25]

ดังนั้นการนำเทคโนโลยี QKD มาประยุกต์ใช้เพื่อสร้างระบบวิทยาการรหัสลับให้เกิดความปลอดภัยโดยแท้จริง (Perfect secrecy) [33] ต้องอาศัยเกณฑ์การเข้ารหัสแบบใช้กุญแจครั้งเดียว (One-time pad: OTP) [34] ซึ่งขนาดของชุดกุญแจรหัสลับ K_i ต้องมีความยาวเท่ากับขนาดของข้อความต้นฉบับ (Plaintext) M_i แสดงการเข้ารหัสได้ดังสมการ (1)

$$C_i = M_i \oplus K_i \tag{1}$$

โดยที่ C_i คือ ข้อความไซเฟอร์ (Ciphertext) ขนาด *i* บิต ที่ได้จากการเข้ารหัสโดยการดำเนินการ Exclusive Or (XOR) หรือการบวกเลขฐานสอง (Modulo-2 addition) ระหว่างข้อความต้นฉบับ M_i กับกุญแจรหัสลับ K_i ขนาด *i* บิตเท่ากัน



รูปที่ 2 ลำดับขั้นตอนของกระบวนการประมวลผลกำเนิดรหัสลับส่วนหลัง (QKD post-processing)

จากหลักเกณฑ์การเข้ารหัสลับข้างต้น ระบบ QKD จะมีส่วนสำคัญในการเพิ่มประสิทธิภาพการกำเนิดกุญแจรหัสลับเพื่อรับประกันความปลอดภัยระหว่างการสื่อสารข้อมูลได้โดยสมบูรณ์ (Perfect security) [3,33] สนับสนุนการประยุกต์ใช้งานจริงเป็นโครงสร้างพื้นฐานสำคัญสำหรับระบบการสื่อสารที่ต้องการความมั่นคงปลอดภัยเป็นอย่างสูง เช่น การทำธุรกรรมทางการเงินและการสื่อสารระหว่างสถาบันการเงิน การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานรัฐ ข้อมูลความมั่นคงของชาติ และข้อมูลด้านสุขภาพและการแพทย์ ตลอดจนการเชื่อมโยงการสื่อสารปลอดภัยระหว่างอุปกรณ์เครือข่ายเชิงควอนตัม (Quantum network) เป็นต้น

2.2 หลักการและขั้นตอนการประมวลผลกำเนิดรหัสลับส่วนหลัง (QKD post-processing)

การประมวลผลกำเนิดรหัสลับส่วนหลังสำหรับระบบ QKD ใดๆ อาศัยช่องทางการสื่อสารทั่วไปเป็นสื่อกลางระหว่างคู่สื่อสาร *Alice* กับ *Bob* โดยเริ่มต้นจากการนำข้อมูลกุญแจดิบ (Raw key data) ที่ได้จากการรับส่งสถานะควอนตัมตามเกณฑ์วิธีที่เลือกใช้งานมาประมวลผลจนได้ผลลัพธ์เป็นข้อมูลกุญแจรหัสลับ (Secret key) ที่ผ่านการยืนยันความถูกต้อง (Data integrity) และความปลอดภัย (Secure) บนหลักการความปลอดภัยทางทฤษฎีสารสนเทศ (Information-theoretic security) [35] พร้อมสำหรับนำไปใช้ในกระบวนการเข้าและถอดรหัสลับ (En-/Decryption) ระหว่างคู่สื่อสาร *Alice* กับ *Bob* ตามลำดับ โดยลำดับการทำงานของกระบวนการ QKD post-processing แสดงได้ดังรูปที่ 2 ประกอบด้วยขั้นตอนดังนี้

1) การแลกเปลี่ยนเวกเตอร์ฐาน (Sifting): *Alice* และ *Bob* ทำการแลกเปลี่ยนและเปรียบเทียบข้อมูลเวกเตอร์ฐาน (Basis) โดยขึ้นกับเกณฑ์วิธีการรับส่งสถานะควอนตัม (QKD protocol) ซึ่งในงานวิจัยนี้ ได้ทำการทดสอบประสิทธิภาพร่วมกับระบบ QKD ด้วยอุปกรณ์แบบความพัวพัน EPR 405 ที่อาศัยโพรโทคอล BBM92 [30] ในการสุ่มเวกเตอร์ฐานสำหรับวัดค่าสถานะ (Measurement basis) จากแหล่งกำเนิดตัวกลางที่สามารถสร้างโพลาไรเซชันของคู่โฟตอนพัวพัน (Polarization-entangled photon pairs) แทนด้วย $\langle\Phi_1|$ แสดงดังสมการ (2)

$$\begin{aligned}\langle\Phi_1| &= \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \\ &= \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)\end{aligned} \tag{2}$$

โดย *Alice* และ *Bob* ต่างสุ่มเลือกเวกเตอร์ฐาน (Basis) ที่ตั้งฉากกัน เพื่อทำการวัดค่าสถานะในสองรูปแบบ ดังนี้

- เวกเตอร์ฐานแนวเส้นตรง (Rectilinear basis: ⊕) สามารถวัดค่าโพลาไรเซชันแนวนอน (Horizontal: H) 0° แทนด้วยบิต 0 และแนวตั้ง (Vertical: V) 90° แทนด้วยบิต 1
- เวกเตอร์ฐานแนวทแยงมุม (Diagonal basis: ⊗) สามารถวัดค่าโพลาไรเซชันแนว + ($+45^\circ$) แทนด้วยบิต 0 และแนว − (-45°) แทนด้วยบิต 1

จากปรากฏการณ์ความพัวพันเชิงควอนตัมเป็นผลให้การวัดค่าสถานะระหว่าง *Alice* กับ *Bob* เป็นไปตามหลักปฏิสัมพันธ์ซึ่งกันและกันโดยสมบูรณ์ (Perfect anti-correlation) ในกรณีที่ *Alice* กับ *Bob* สุ่มเลือกเวกเตอร์ฐานแบบเดียวกันในการวัดค่าแล้วผลลัพธ์ที่ได้จะตรงข้ามกัน แสดงเป็นตัวอย่างขั้นตอน Sifting ได้ดังตารางที่ 1 โดยการเลือกค่ากุญแจดิบเฉพาะที่มีเวกเตอร์ฐาน [A] กับ [B] ในการวัดสถานะที่ตรงกัน ได้ผลลัพธ์เป็นบิตข้อมูลไบนารีของ *Alice* กับ *Bob* ที่มีความยาวเท่ากัน เรียกว่า กุญแจซิฟท์ (Sifted Key) K^A_{Sifted} และ K^B_{Sifted} ตามลำดับ

ตารางที่ 1 การแลกเปลี่ยนเวกเตอร์ฐาน (Sifting) ด้วยโพรโทคอล BBM92 โดยเลือกข้อมูลกุญแจดิบ (Raw key) ที่ใช้เวกเตอร์ฐานรูปแบบเดียวกันในการวัดค่าสถานะคู่โฟตอนพัวพันในแต่ละครั้งของ *Alice* กับ *Bob* และทำการแปลงผลลัพธ์ให้เป็นบิตข้อมูลกุญแจซิฟท์ (Sifted key)

ครั้งที่วัดสถานะ	1	2	3	4	5	6
ข้อมูลดิบของภาคส่ง (*Alice*'s raw data)						
การสุ่มเวกเตอร์ฐาน [A] สำหรับวัดค่าสถานะ (Measurement basis)	⊕ (*HV*)	⊗ (+–)	⊗ (+–)	⊕ (*HV*)	⊗ (+–)	⊕ (*HV*)
ผลการวัดสถานะ (Measurement result)	↕ (*V*)	↘↗ (–)	↗↘ (+)	↔ (*H*)	↗↘ (+)	↕ (*V*)
ค่ากุญแจดิบ (Raw Key)	1	1	0	0	0	1
ข้อมูลดิบของภาครับ (*Bob*'s raw data)						
การสุ่มเวกเตอร์ฐาน [B] สำหรับวัดค่าสถานะ (Measurement basis)	⊕ (*HV*)	⊕ (*HV*)	⊗ (+–)	⊕ (*HV*)	⊕ (*HV*)	⊗ (+–)
ผลการวัดสถานะ (Measurement result) *Anti-correlation	↔ (*H*)	↕ (*V*)	↘↗ (–)	↔ (*H*)	↕ (*V*)	↗↘ (+)
ค่ากุญแจดิบ *กลับค่า (Raw Key) *Flip-bit	1	0	0	1	0	1
การแลกเปลี่ยนข้อมูลการสุ่มเวกเตอร์ฐาน (Sifting)						
เปรียบเทียบเวกเตอร์ฐาน [A] กับ [B] ตรงกัน ? (Compatible basis)	✓	×	✓	✓	×	×
กุญแจซิฟท์ของ Alice (K^{A}_{Sifted})	1	-	0	0	-	-
กุญแจซิฟท์ของ Bob (K^{B}_{Sifted})	1	-	0	1 (Error)	-	-

2) การประมาณค่าพารามิเตอร์ช่องสัญญาณ (Channel parameter estimation): คู่สื่อสาร *Alice* กับ *Bob* ดำเนินการประเมินค่าพารามิเตอร์แทนความผิดพลาดจากการรับส่งสถานะบนช่องสัญญาณเชิงควอนตัมที่อาจเกิดขึ้นได้จากการดักจับข้อมูลและ/หรือความไม่สมบูรณ์ของอุปกรณ์ QKD ที่เรียกว่า ค่าอัตราความผิดพลาดบิตเชิงควอนตัม (Quantum bit error rate: *QBER*) ซึ่งโดยทั่วไปใช้วิธีการสุ่มเปิดเผยบิตกุญแจซิฟท์บางส่วน (Key sampling) เป็นข้อมูลตัวอย่างสำหรับเปรียบเทียบเพื่อประเมินค่า *QBER* ซึ่งสามารถบ่งบอกถึงความน่าจะเป็นร่วมกันของสารสนเทศ (Joint probability) ระหว่าง *Alice* กับ *Bob* รวมถึงผู้ดักจับข้อมูล (*Eve*) ที่มีโอกาสได้รับสารสนเทศอันมีความเกี่ยวพันกับกุญแจรหัสลับ ดังนั้นค่าความผิดพลาดบนระบบ QKD สามารถนำมาพิสูจน์อัตรากำเนิดกุญแจรหัสลับที่ปลอดภัย (r_K) จากสารสนเทศร่วมกัน (Mutual information) ระหว่าง *Alice* (*A*) กับ *Bob* (*B*) แทนด้วย $I(A;B)$ และ *Alice* (*A*) กับ *Eve* (*E*) แทนด้วย $I(A;E)$ แสดงความสัมพันธ์ได้ดังสมการ (3) และ (4)

$$r_K = I(A;B) - I(A;E) \tag{3}$$

จะได้

$$r_K = H(A|E) - H(A|B) \tag{4}$$

กำหนดให้ $H(.|.)$ แทนปริมาณข่าวสารตามเงื่อนไขหรือแชนนอนเอนโทรปี (Shannon entropy) [7] ระหว่างสารสนเทศที่มีความสัมพันธ์กัน หากนำค่า *QBER* แทนอัตราความผิดพลาด *e* บนช่องสัญญาณไบนารีแบบสมมาตร (Binary symmetric channel: BSC); $H(e) = -e\log_2 e-(1-e)\log_2(1-e)$ จะได้ผลการพิสูจน์ค่า *QBER* สูงสุดต้องไม่เกิน 11% (*QBER* ≤ 11%) เพื่อให้ได้อัตราการกำเนิดกุญแจรหัสลับ r_K บนเงื่อนไขของหลักความปลอดภัยทางทฤษฎีสารสนเทศ ดังนั้นค่า *QBER* ที่ได้จากขั้นตอนการประมาณค่าพารามิเตอร์ช่องสัญญาณนี้ จะถูกนำมาใช้เป็นตัวชี้วัดความปลอดภัยของระบบ QKD ต่อไป

นอกจากนี้ วิธีการประมาณค่าอัตราความผิดพลาดที่กระทำในระหว่างหรือหลังจากขั้นตอนการไกล่เกลี่ยความผิดพลาดได้มีการนำเสนอใน [36,37] อย่างไรก็ตาม ความแม่นยำในการประมาณค่า *QBER* แต่ละวิธีจะส่งผลกระทบต่อประสิทธิภาพของวิธีการไกล่เกลี่ยความผิดพลาดที่เลือกใช้งาน

3) การไกล่เกลี่ยความผิดพลาด (Information reconciliation): กระบวนการแก้ไขความผิดพลาดบนข้อมูลกุญแจซิฟท์ระหว่าง *Alice* กับ *Bob* จากค่า *QBER* ที่เกิดขึ้น โดยทั่วไปอาศัยวิธีการไกล่เกลี่ยความผิดพลาดแบบทางเดียว (One-way reconciliation) [38] เริ่มต้นจาก *Alice* ทำการสร้างข้อมูลที่มีความสัมพันธ์เกี่ยวข้องกับกุญแจซิฟท์ของตนและส่งผ่านช่องทางการสื่อสารทั่วไปไปยัง *Bob* เพื่อใช้ตรวจสอบและแก้ไขตำแหน่งบิตของกุญแจซิฟท์ที่ผิดพลาดให้มีค่าตรงกัน ได้ผลลัพธ์เป็นชุดกุญแจที่ได้รับการแก้ไขความผิดพลาดแล้วที่เรียกว่า Reconciled key

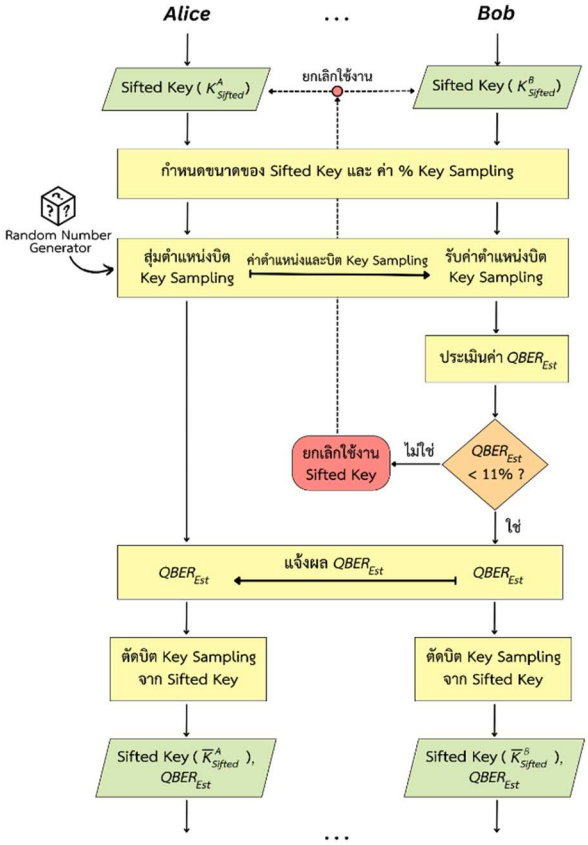
ตัวอย่างวิธีการไกล่เกลี่ยความผิดพลาด ได้แก่ โพรโทคอลคาสเคด (Cascade) [39,40] เป็นอัลกอริทึมการค้นหาแบบไบนารี (Binary searching) ที่เรียบง่าย โดยการแบ่งชุดกุญแจออกเป็นบล็อกตามขนาดที่เหมาะสม และคำนวณหาพาริตี้บิต (Parity bit) พร้อมการเปรียบเทียบในแต่ละบล็อกระหว่างคู่สื่อสาร หากพาริตี้บิตของบล็อกใดมีค่าแตกต่างกันแล้ว จะสามารถค้นหาตำแหน่งบิตที่ผิดพลาดและแก้ไขโดยการวนซ้ำรอบได้ นอกจากนี้มีการประยุกต์นำหลักทฤษฎีรหัสช่องสัญญาณสมัยใหม่ (Modern coding theory) ด้วยเทคนิคของรหัสตรวจสอบพาริตี้แบบความหนาแน่นต่ำหรือแอลดีพีซี (Low-density parity-check code: LDPC) [41,42] มาออกแบบและพัฒนาเพื่อเพิ่มประสิทธิภาพในการแก้ไขความผิดพลาดภายใต้จำนวนบิตเปิดเผยน้อยที่สุดดังตัวอย่างวิธีการที่นำเสนอใน [15,43–45]

4) การยืนยันความถูกต้อง (Confirmation): คู่สื่อสาร *Alice* และ *Bob* ทำการตรวจสอบความถูกต้องบนชุดกุญแจ Reconciled key หลังจากที่ได้รับการไกล่เกลี่ยความผิดพลาดแล้ว โดยทั่วไปอาศัยวิธีการสร้างรหัสขนาดสั้นกำเนิดจากฟังก์ชันแฮช (Hash function) [16] เพื่อแทนค่ากุญแจระหว่างคู่สื่อสาร *Alice* กับ *Bob* และทำการเปรียบเทียบ หากรหัสแฮช (Hash) ที่ได้มีค่าตรงกันแล้ว สามารถยืนยันได้ว่ากุญแจระหว่าง *Alice* กับ *Bob* นั้น มีความสัมพันธ์ตรงกันอย่างสมบูรณ์ (Fully correlation) หรือความน่าจะเป็นของสารสนเทศ A เท่ากับ B มีค่าเท่ากับหนึ่ง ($\Pr[A=B]=1$) และเรียกชุดกุญแจที่ผ่านการยืนยันความถูกต้องนี้ว่า Identical key

5) การขยายสภาวะส่วนตัว (Privacy amplification): การลดความสัมพันธ์ข้อมูลกุญแจที่ผู้ดักจับมีโอกาสได้รับหรือขโมยไปทั้งในช่องสัญญาณเชิงควอนตัมและช่องทางการสื่อสารทั่วไป โดยคู่สื่อสารนำชุดกุญแจที่ผ่านการยืนยันความถูกต้อง (Identical key) จากขั้นตอนก่อนหน้า มาดำเนินการร่วมกับกับเมตริกซ์แบบไบนารีของฟังก์ชันแฮชเชิงเอกภพ (Universal hashing function) เช่น เมทริกซ์แบบโทพลิทซ์ (Toeplitz matrix) [18] เป็นต้น เพื่อกำเนิดเป็นข้อมูลกุญแจรหัสลับสุดท้าย (Final secret key) ที่มีความปลอดภัยสูงสุด โดยตัวอย่างงานวิจัยใน [46,47] ได้นำเสนอหลักการพิสูจน์ขนาดของกุญแจรหัสลับภายใต้เงื่อนไขความปลอดภัยของระบบ QKD

3. การออกแบบขั้นตอนวิธีการประมวลผลรหัสลับส่วนหลังสำหรับระบบการกระจายกุญแจรหัสลับเชิงควอนตัม (QKD post-processing algorithms)

เนื้อหาในส่วนนี้นำเสนอการออกแบบขั้นตอนวิธีการประมวลผลรหัสลับส่วนหลัง (Post-processing algorithms) โดยการรับค่าข้อมูลกุญแจซิฟท์ (Sifted key) ที่ผ่านการรับส่งสถานะเชิงควอนตัมและการแลกเปลี่ยนเวกเตอร์ฐาน (Key sifting) ภายใต้ระบบการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่องใดๆ (Discrete variable quantum key distribution: DV-QKD) [13] มาเป็นอินพุตเข้าสู่การประมวลผลเพื่อกลั่นกรองเป็นกุญแจรหัสลับสุดท้าย (Final secret key) ตามขั้นตอนย่อยที่เป็นหลักปฏิบัติของกระบวนการ QKD post-processing โดยงานวิจัยนี้ ได้แบ่งส่วนของการออกแบบขั้นตอนวิธีเป็น 3 ส่วนหลัก ดังรายละเอียดต่อไปนี้



รูปที่ 3 แผนผังขั้นตอนวิธีการประมาณค่าอัตราความผิดพลาดบิตเชิงควอนตัมด้วยการสุ่มเปิดเผยบิตกุญแจบางส่วน (QBER estimation by key sampling) และการประเมินค่า QBER บนเงื่อนไขความปลอดภัยของระบบ QKD

3.1 ขั้นตอนวิธีการประมาณค่าอัตราความผิดพลาดบิตเชิงควอนตัมและการประเมินเงื่อนไขความปลอดภัยของระบบ

วิธีการประมาณค่าอัตราความผิดพลาดบิตเชิงควอนตัมอาศัยเทคนิคการสุ่มเปิดเผยและเปรียบเทียบตัวอย่างบิตกุญแจซิฟท์บางส่วน (Key sampling) สำหรับประเมินค่า $QBER_{Est}$ เพื่อเป็นพารามิเตอร์ในการตัดสินใจนำข้อมูลที่ได้จากการรับส่งสถานะเชิงควอนตัมเข้าสู่กระบวนการ QKD post-processing กำเนิดเป็นกุญแจรหัสลับต่อไป ซึ่งวิธีการที่นำเสนอแสดงเป็นแผนผังการทำงานได้ดังรูปที่ 3 โดยมีขั้นตอนดังนี้

1) กำหนดขนาดของกุญแจซิฟท์ (Sifted key) และเปอร์เซ็นต์การสุ่มเปิดเผยบิตจากขนาดของกุญแจซิฟท์ทั้งหมด (% Key sampling)

2) *Alice* ดำเนินการสุ่มคัดเลือกตำแหน่งบิตกุญแจที่จะเปิดเผยตามค่า % Key sampling และทำการส่งค่าชุดตำแหน่งและบิตที่เปิดเผยไปยัง *Bob*

3) *Bob* ดำเนินการคัดเลือกบิตกุญแจซิฟท์ตามชุดตำแหน่งที่ได้รับจาก *Alice* และทำการเปรียบเทียบเพื่อประเมินค่า $QBER_{Est}$ คำนวณได้ดังสมการที่ (5)

$$QBER_{Est}[\%] = \frac{n_{error}}{n_{correct} + n_{error}} \times 100 \qquad (5)$$

โดยที่ $n_{correct}$ และ n_{error} แทนจำนวนบิตเปิดเผย (Key sampling) ที่มีค่าตรงกัน และไม่ตรงกันระหว่าง *Alice* กับ *Bob* ตามลำดับ

4) *Bob* ประเมินความปลอดภัยของระบบ QKD จากค่า $\%QBER_{Est}$ ที่คำนวณได้ และแจ้งผลไปยัง *Alice* ซึ่งเป็นไปตามเงื่อนไขขีดจำกัดของอัตรากำเนิดกุญแจรหัสลับที่ปลอดภัยดังสมการ (3) และ (4) โดยสามารถออกแบบเป็นเงื่อนไขการประเมินความปลอดภัยของระบบได้ดังนี้

- กรณี $QBER_{Est} \leq 11\%$; คู่สื่อสาร *Alice* กับ *Bob* ดำเนินการตัดข้อมูลกุญแจซิฟท์ที่เปิดเผยทิ้ง และนำกุญแจซิฟท์ส่วนที่คงอยู่ ($\bar{K}^{A}_{Sifted}$ และ $\bar{K}^{B}_{Sifted}$) เข้าสู่ขั้นตอนต่อไป
- กรณี $QBER_{Est} > 11\%$; ระบบยกเลิกการใช้งานกุญแจซิฟท์ชุดดังกล่าวทั้งหมด

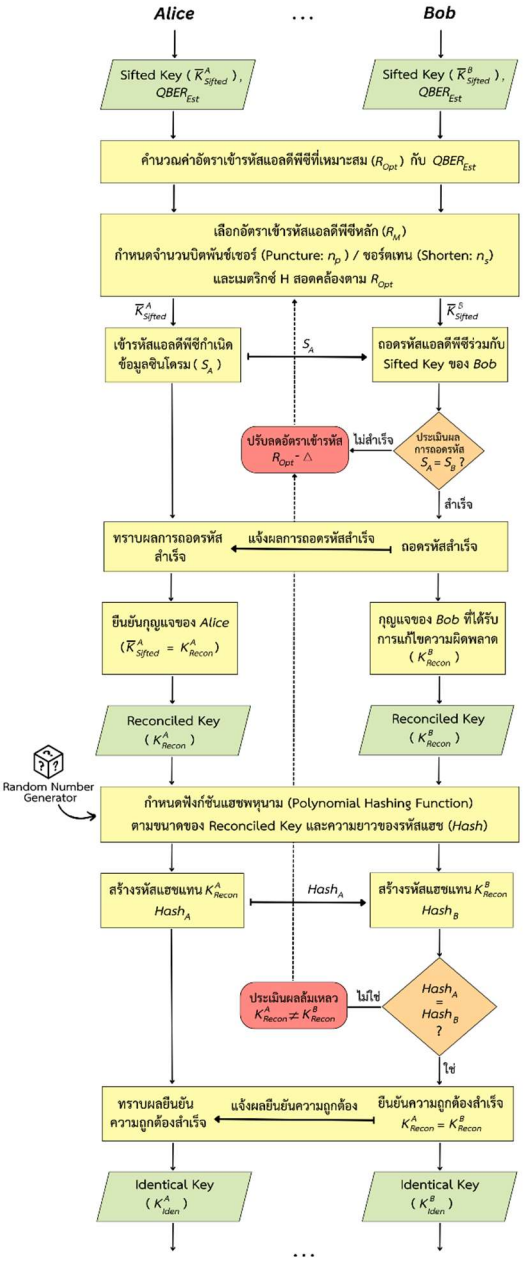
3.2 ขั้นตอนวิธีการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสที่เหมาะสมและการยืนยันความถูกต้อง

วิธีการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสเหมาะสมที่ได้นำเสนอในงานวิจัยนี้ อาศัยการประยุกต์นำเทคนิคของรหัสแอลดีพีซีแบบไม่สม่ำเสมอ (Irregular LDPC codes) [48] มาพัฒนาบนระบบการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารข้างเคียง (Source coding with side information) [49] ระหว่าง *Alice* กับ *Bob* โดยอาศัยเทคนิคพันช์เชอร์ (Puncture) และชอร์ตเทน (Shorten) [50] ทำหน้าที่ปรับอัตราเข้ารหัสแอลดีพีซีให้เหมาะสม (R_{Opt}) ด้วยวิธีการเดนซิตี้อีโวลูชัน (Density evolution) [42] สอดคล้องกับค่า $QBER_{Est}$ ที่ได้จากขั้นตอนก่อนหน้า เพื่อให้ *Alice* สามารถกำเนิดข้อมูลซินโดรม (Syndrome Information: S_A) ที่มีปริมาณเหมาะสมกับความสามารถในการถอดรหัสซินโดรม (Syndrome decoding) เพื่อแก้ไขความผิดพลาดของ *Bob* ภายใต้เงื่อนไขความปลอดภัยของระบบ QKD ซึ่งพิจารณาได้จากปริมาณการเปิดเผยสารสนเทศระหว่างขั้นตอนไกล่เกลี่ยความผิดพลาด (M_{Leak}) ที่มีความสัมพันธ์กับกุญแจซิฟท์ของ *Alice* ($\bar{K}^{A}_{Sifted}$) ในที่นี้คือข้อมูลซินโดรม S_A นั่นเอง ดังนั้นประสิทธิภาพการไกล่เกลี่ยความผิดพลาด (f_{Recon}) สามารถคำนวณได้จากอัตราส่วนระหว่างปริมาณการเปิดเผยข้อมูลซินโดรมจริง M_{Leak} กับปริมาณการเปิดเผยสารสนเทศทางทฤษฎีที่น้อยที่สุด (Minimum information leakage) ในระหว่างกระบวนการไกล่เกลี่ยความผิดพลาด แทนด้วย $H(e)$ แสดงได้ดังสมการ (6)

$$f_{Recon} = \frac{M_{Leak}}{H(e)} = \frac{1 - R_{Opt}}{H(e)} \qquad (6)$$

โดยที่ M_{Leak} มีความสัมพันธ์กับอัตราการเข้ารหัสแอลดีพีซีที่เหมาะสม R_{Opt} ภายใต้เงื่อนไขของการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารข้างเคียง ($M_{Leak} = 1 - R_{Opt}$) และ $H(e)$ แสดงถึงเอนโทรปีของอัตราความผิดพลาด e ระหว่างข้อมูลกุญแจ $\bar{K}^{A}_{Sifted}$ กับ $\bar{K}^{B}_{Sifted}$ ซึ่งสามารถแทนค่า e ด้วยอัตราความผิดพลาดบิตเชิงควอนตัมที่ได้จากการประมาณ ($QBER_{Est}$) โดยค่า f_{Recon} ที่ได้จากสมการ (6) ถือเป็นพารามิเตอร์สำคัญในการพิจารณาถึงประสิทธิภาพการไกล่เกลี่ยความผิดพลาด

สอดคล้องกับปริมาณการเปิดเผยสารสนเทศ M_{Leak} ภายใต้อัตราการเข้ารหัสแอลดีพีซีที่เลือกใช้งานอย่างเหมาะสม R_{Opt}



รูปที่ 4 แผนผังขั้นตอนวิธีการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสแอลดีพีซีที่เหมาะสม (Information reconciliation based on rate-adaptive LDPC codes) และการยืนยันความถูกต้องตรงกัน (Confirmation) บนชุดกุญแจที่ได้รับการไกล่เกลี่ยความผิดพลาดแล้ว

นอกจากนี้ได้มีการประยุกต์นำฟังก์ชันแฮชแบบพหุนาม (Polynomial hashing function) [16,17] มาออกแบบเป็นขั้นตอนการยืนยันความถูกต้อง (Confirmation) ของข้อมูลกุญแจที่ได้รับการไกล่เกลี่ยความผิดพลาดแล้ว (Reconciled key) ระหว่าง *Alice* กับ *Bob* โดยประสานการทำงานเป็นขั้นตอนวิธีร่วมกับการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสที่เหมาะสม แสดงเป็นแผนผังการทำงานได้ดังรูปที่ 4 โดยมีขั้นตอนดังนี้

1) *Alice* นำค่า $QBER_{Est}$ มาคำนวณอัตราเข้ารหัสแอลดีพีซีที่เหมาะสม (R_{Opt}) สอดคล้องกับพารามิเตอร์ f_{Recon} ในสมการ (6)

2) *Alice* กับ *Bob* เลือกเมทริกซ์ตรวจสอบความผิดพลาด (Parity check matrix: H) ของรหัสแอลดีพีซีหลัก (LDPC Mother code: R_M) และดำเนินการกำหนดจำนวนบิตพันช์เชอร์ (n_p) และบิตชอร์ตเทน (n_s) บนชุดข้อมูลกุญแจ $\bar{K}^A_{Sifted}$ และ $\bar{K}^B_{Sifted}$ ตามลำดับ ให้มีค่าสอดคล้องกับ R_{Opt} ร่วมกัน

3) *Alice* ดำเนินการเข้ารหัสกำเนิดข้อมูลซินโดรม $S_A = \bar{K}^A_{Sifted} \cdot \mathrm{H}^T$ ด้วยอัตรา R_{Opt} และส่ง S_A ผ่านช่องทาง การสื่อสารไปยัง *Bob*

4) *Bob* นำ $\bar{K}^B_{Sifted}$ ที่ถูกกำหนดตำแหน่งบิต n_p และ n_s เข้าสู่กระบวนการถอดรหัสแอลดีพีซี (LDPC Decoding) เพื่อแก้ไขตำแหน่งบิตผิดพลาดบน $\bar{K}^B_{Sifted}$ จนกระทั่งสิ้นสุดการถอดรหัส

5) *Bob* ดำเนินการประเมินผลการถอดรหัส โดยการคำนวณซินโดรม S_B จากข้อมูลกุญแจที่ผ่านการแก้ไขความผิดพลาดแล้ว (K^B_{Recon}) จากนั้นจึงดำเนินการเปรียบเทียบกับ S_A และแจ้งผลไปยัง *Alice* ซึ่งสามารถออกแบบเงื่อนไขการประเมินผลการถอดรหัสได้ดังนี้

- กรณี $S_A = S_B$ แสดงผลการถอดรหัสสำเร็จ; *Alice* และ *Bob* นำข้อมูลกุญแจที่ผ่านการไกล่เกลี่ยความผิดพลาดแล้ว K^A_{Recon} และ K^B_{Recon} ตามลำดับ เข้าสู่การขั้นตอนการยืนยันความถูกต้อง
- กรณี $S_A \neq S_B$ แสดงผลการถอดรหัสล้มเหลว; *Alice* และ *Bob* ดำเนินการปรับลดอัตราเข้ารหัส $R_{Opt} - \Delta$ โดยกลับสู่ขั้นตอนที่ 2 เพื่อลดจำนวนบิต n_p และเพิ่มจำนวนบิต n_s แล้วดำเนินการตามขั้นตอนที่ 3 – 5 อีกครั้ง

6) *Alice* และ *Bob* ดำเนินการเข้าสู่ขั้นตอนการยืนยันความถูกต้องตรงกันของ K^A_{Recon} และ K^B_{Recon} โดยเริ่มต้นจากการสร้างฟังก์ชันแฮชแบบพหุนาม (Polynomial hashing function: h_{PolyR}) จากชุดข้อมูลจำนวนสุ่ม s และจำนวนเฉพาะ p โดยที่ $s \in \{0, 1, 2, \ldots, p-1\}$

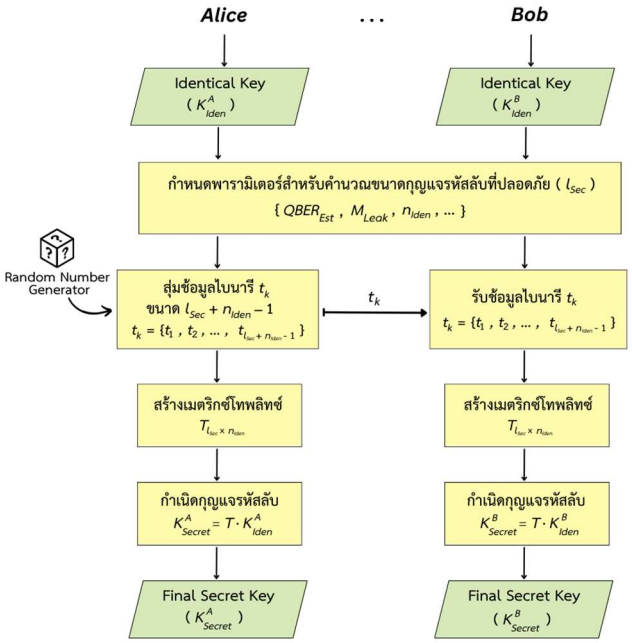
7) *Alice* ดำเนินการคำนวณรหัส $Hash_A$ จาก h_{PolyR} ที่ถูกสร้างขึ้นโดย $Hash_A = h_{PolyR}(K^A_{Recon})$ และส่งข้อความดังกล่าวไปยัง *Bob*

8) *Bob* คำนวณรหัส $Hash_B = h_{PolyR}(K^B_{Recon})$ และดำเนินการเปรียบเทียบกับ $Hash_A$ ที่ได้รับจาก *Alice* ซึ่งสามารถกำหนดผลของการยืนยันความถูกต้องเป็นเงื่อนไขได้ดังนี้

- กรณี $Hash_A = Hash_B$ แสดงผลการยืนยันความถูกต้องสำเร็จ; กุญแจของ *Alice* และ *Bob* มีความถูกต้องตรงกันโดยสมบูรณ์ ($K^A_{Recon} = K^B_{Recon}$) และสามารถนำข้อมูลกุญแจที่ผ่านการยืนยันความถูกต้องแล้ว (K^A_{Iden} และ K^B_{Iden}) เข้าสู่ขั้นตอนถัดไป
- กรณี $Hash_A \neq Hash_B$ แสดงผลการยืนยันความถูกต้องล้มเหลว; กุญแจของ *Alice* และ *Bob* ยังคงเกิดข้อผิดพลาด ($K^A_{Recon} \neq K^B_{Recon}$) จึงต้องกลับสู่ขั้นตอนการปรับลดอัตราเข้ารหัสเพื่อประมวลผลการไกล่เกลี่ยความผิดพลาดและยืนยันความถูกต้องใหม่ในขั้นตอนที่ 2 – 8 อีกครั้ง

3.3 ขั้นตอนวิธีการขยายสภาวะส่วนตัวด้วยฟังก์ชันแฮชเชิงเอกภพแบบเมทริกซ์โทพลิทซ์

การออกแบบวิธีการขยายสภาวะส่วนตัวได้ประยุกต์นำฟังก์ชันแฮชเชิงเอกภพ (Universal hashing function) ที่กำเนิดจากการสุ่มข้อมูลไบนารีตามโครงสร้างของเมทริกซ์โทพลิทซ์ (Toeplitz matrix) [18] มาดำเนินการร่วมกับข้อมูลกุญแจที่ผ่านการยืนยันความถูกต้องแล้ว เพื่อกำเนิดเป็นกุญแจรหัสลับสุดท้าย (Final secret key) ที่ไม่มีความสัมพันธ์ใดๆ กับสารสนเทศของผู้ดักจับข้อมูล ซึ่งวิธีการที่นำเสนอได้อาศัยพารามิเตอร์ที่เกี่ยวข้องจากขั้นตอนก่อนหน้า ได้แก่ค่า $QBER_{Est}$ ที่ได้จากขั้นตอนการประมาณค่าอัตราความผิดพลาด ปริมาณการเปิดเผยสารสนเทศระหว่างขั้นตอนการไกล่เกลี่ยความผิดพลาด (M_{Leak}) และขนาดของกุญแจที่ผ่านการยืนยันความถูกต้อง (n_{Iden}) หลังจากขั้นตอนการยืนยันความถูกต้องเสร็จสิ้น เป็นต้น มาพิจารณาถึงความปลอดภัยของระบบภายใต้เงื่อนไขการคำนวณขนาดของกุญแจรหัสลับสุดท้ายที่ปลอดภัย (l_{Sec}) โดยแผนผังการทำงานตามขั้นตอนวิธีการขยายสภาวะส่วนตัวที่นำเสนอแสดงได้ดังรูปที่ 5 มีรายละเอียดดังนี้



รูปที่ 5 แผนผังขั้นตอนวิธีการขยายสภาวะส่วนตัวด้วยฟังก์ชันแฮชเชิงเอกภพตามโครงสร้างของเมทริกซ์แบบโทพลิทซ์ (Toeplitz matrix)

1) *Alice* นำพารามิเตอร์ที่เกี่ยวข้อง ได้แก่ ค่า $QBER_{Est}$ ปริมาณการเปิดเผยสารสนเทศ M_{Leak} และขนาดของ Identical key (n_{Iden}) มาคำนวณหาขนาดของกุญแจรหัสลับสุดท้าย (l_{Sec}) ภายใต้เงื่อนไขขีดจำกัดความปลอดภัยของอัตราการกำเนิดกุญแจรหัสลับ (Secure secret key rate) [47] แสดงดังสมการ (7)

$$l_{Sec} = [(1 - h(e)) - M_{Leak}] \cdot n_{Iden} - 2\log_2(\frac{1}{\varepsilon_{Sec}}) \qquad (7)$$

โดยที่ ε_{Sec} แทนพารามิเตอร์ของการขยายสภาวะส่วนตัวบนเงื่อนไขของอัตราการกำเนิดกุญแจรหัสลับที่ปลอดภัย

2) *Alice* ดำเนินการสุ่มชุดข้อมูลไบนารี $t_k = \{t_1, t_2, \dots, t_{l_{sec}+n_{Iden}-1}\}$ ขนาด $l_{Sec} + n_{Iden} - 1$ บิต และส่ง t_k ผ่านช่องทางการสื่อสารไปยัง *Bob*

3) *Alice* และ *Bob* นำชุดข้อมูลไบนารี t_k จัดเรียงในรูปแบบเมทริกซ์โทพลิทซ์ ($T_{l_{sec} \times n_{Iden}}$) ตามโครงสร้างดังสมการ (8)

$$T_{l_{sec}\times n_{Iden}}=\begin{bmatrix} t_{l_{sec}} & t_{l_{sec}+1} & \cdots & \cdots & & \cdots & \cdots & t_{l_{sec}+n_{Iden}-2} & t_{l_{sec}+n_{Iden}-1} \\ t_{l_{sec}-1} & t_{l_{sec}} & \ddots & & & & \cdots & t_{l_{sec}+n_{Iden}-3} & t_{l_{sec}+n_{Iden}-2} \\ \vdots & t_{l_{sec}-1} & \ddots & \ddots & & & & \vdots & \vdots \\ t_2 & \vdots & \ddots & t_{l_{sec}} & t_{l_{sec}+1} & & & & t_{n_{Iden}-2} \\ t_1 & t_2 & \cdots & t_{l_{sec}-1} & t_{l_{sec}} & t_{l_{sec}+1} & \cdots & \cdots & t_{n_{Iden}-1} \end{bmatrix}_{l_{Sec}\times n_{Iden}} \quad (8)$$

4) *Alice* และ *Bob* นำข้อมูลกุญแจ K^A_{Iden} และ K^B_{Iden} ของตนเองดำเนินการคูณกับทรานส์โพสของเมทริกซ์ $T_{l_{sec}\times n_{Iden}}$ แสดงดังสมการ (9)

$$K_{Secret_{1\times l_{Sec}}} = K_{Iden_{1\times n_{Iden}}} \cdot T^T_{n_{Iden}\times l_{Sec}} \quad (9)$$

จากสมการ (9) จะได้ข้อมูล K^A_{Secret} และ K^B_{Secret} เป็นกุญแจรหัสลับสุดท้าย (Final secret key) ของคู่สื่อสาร *Alice* กับ *Bob* ตามลำดับ ซึ่งถือเป็นผลลัพธ์จากระบบ QKD หลังจากสิ้นสุดกระบวนการ QKD post-processing ที่ผ่านการสร้างข้อตกลงระหว่างคู่สื่อสารบนชุดข้อมูลกุญแจรหัสลับให้มีค่าตรงกันและมีความปลอดภัยสูงสุดสำหรับการนำไปใช้ในระบบวิทยาการรหัสลับต่อไป

4. ผลการทดสอบ

กระบวนการประมวลผลรหัสลับส่วนหลังสำหรับระบบการกระจายกุญแจรหัสลับเชิงควอนตัม (QKD post-processing) ตามขั้นตอนวิธี (Algorithms) ที่ได้นำเสนอในงานวิจัยนี้ ได้ถูกนำมาพัฒนาในรูปแบบซอฟต์แวร์ด้วยโปรแกรมภาษาซีพลัสพลัส (C++ programming) บนโครงสร้าง (Framework) ของซอฟต์แวร์สำหรับระบบการกระจายรหัสลับเชิงควอนตัมจากสถาบันเทคโนโลยีแห่งออสเตรีย (AIT QKD Software) [51,52] และดำเนินการทดสอบร่วมกับอุปกรณ์ EPR 405 [19,20] บนพื้นฐานของระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบคู่โฟตอนพัวพัน (Entanglement-based QKD system) โดยการตั้งค่าอุปกรณ์รับส่งสถานะจากแหล่งกำเนิดผ่านอากาศ (Free-space) ไปยังภาครับในระยะทาง 11 เมตร และนำผลของชุดข้อมูลกุญแจซิฟท์ (Sifted key) ที่ผ่านการแลกเปลี่ยนเวกเตอร์ฐาน (Sifting) ด้วยโพรโทคอล BBM92 [30] เข้าสู่การประมวลผลตามขั้นตอนของ QKD post-processing ที่ได้ออกแบบและพัฒนาในรูปแบบซอฟต์แวร์ติดตั้งพร้อมประมวลผลบนเครื่องคอมพิวเตอร์ระหว่างภาคส่ง (*Alice*) กับภาครับ (*Bob*) ที่เชื่อมต่อการสื่อสารแบบอีเทอร์เน็ต (Ethernet) ด้วยโพรโทคอลมาตรฐาน TCP/IP โดยรายละเอียดคุณสมบัติของคอมพิวเตอร์ที่ใช้ในการทดสอบประสิทธิภาพและการกำหนดเงื่อนไขของพารามิเตอร์สำหรับขั้นตอนวิธี QKD post-processing ที่นำเสนอในงานวิจัยนี้ แสดงได้ดังตารางที่ 2 และ 3 ตามลำดับ

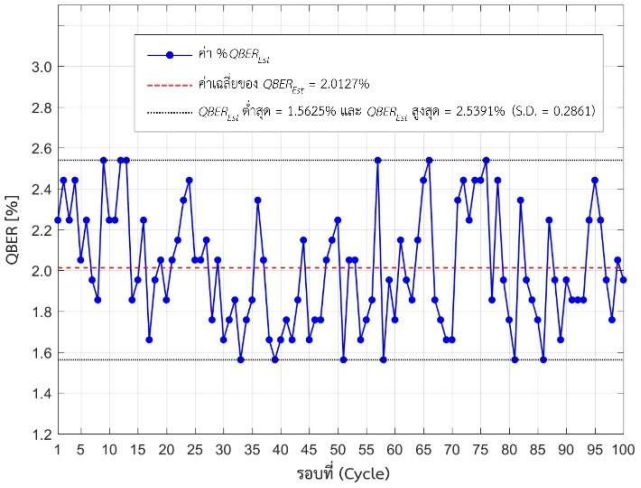
ตารางที่ 2 คุณสมบัติด้านฮาร์ดแวร์และซอฟต์แวร์ของเครื่องคอมพิวเตอร์ที่ใช้ในการทดสอบประสิทธิภาพการประมวลผลกำเนิดรหัสลับส่วนหลัง (QKD post-processing)

คุณสมบัติของระบบคอมพิวเตอร์	
ซีพียู (CPU)	64-bit Intel Xeon Processor X3430 Quad Core / Cache 8MB / 2.40 GHz
หน่วยความจำ (Memory)	16 GB DDR3
ระบบปฏิบัติการ (OS)	Debian GNU/Linux
เวลาตอบสนองระหว่างภาคส่งกับภาครับ (Network Latency)	3 ms

ตารางที่ 3 การกำหนดค่าพารามิเตอร์อินพุตสำหรับขั้นตอนวิธีการประมวลผลกำเนิดรหัสลับส่วนหลัง (Post-processing algorithms) เพื่อการทดสอบประสิทธิภาพร่วมกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศแบบ คู่โฟตอนพัวพัน (Entangled free-space QKD system)

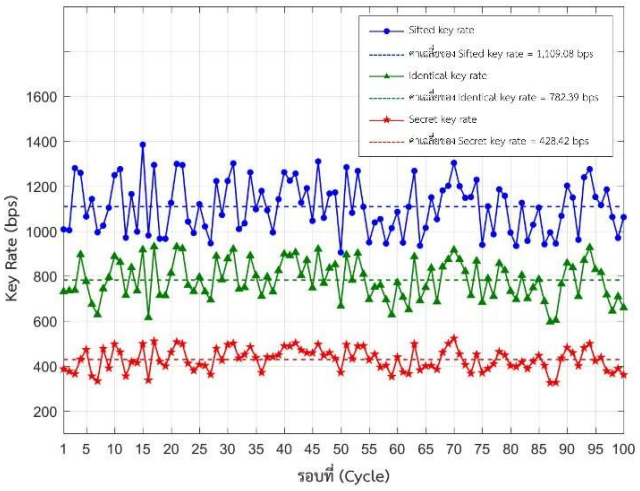
ค่าพารามิเตอร์สำหรับ QKD post-processing algorithms		
1. ขั้นตอนวิธีการประมาณค่าอัตราความผิดพลาด (QBER Estimation)	ขนาดของกุญแจซิฟท์ (Sifted key size) [บิต]	5,120
	เปอร์เซ็นต์การสุ่มตัวอย่างบิต / จำนวนบิตเปิดเผย [%Sampling / บิต]	20% / 1,024
2. ขั้นตอนวิธีการไกล่เกลี่ยความผิดพลาดและยืนยันความถูกต้อง (Information reconciliation and confirmation)	ขนาดบล็อกของรหัสแอลดีพีซี (LDPC block length) [บิต]	4,096
	อัตราเข้ารหัสแอลดีพีซีหลัก (LDPC mother code: R_M)	0.6, 0.7, 0.8
	ผลรวมของจำนวนบิตพันช์เชอร์ (n_p) และบิตชอร์ตเทน (n_s) (d = n_p + n_s) [บิต]	420
	ขนาดของรหัสแฮช (Hash size) [บิต / ไบต์]	64 / 8
3. ขั้นตอนวิธีการขยายสภาวะส่วนตัว (Privacy amplification)	ความปลอดภัยของการขยายสภาวะส่วนตัว (ε_{sec})	2×10^{-20}

การทดสอบประสิทธิภาพในงานวิจัยนี้ ดำเนินการตามกระบวนการที่เป็นหลักปฏิบัติของระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) [6,13] จำนวนทั้งสิ้น 100 รอบ (Cycles) และนำเสนอผลการทดสอบประสิทธิภาพ QKD post-processing ตามขั้นตอนวิธีที่ได้ออกแบบทั้งสามส่วนหลัก เริ่มต้นจากการประมวลผลการประมาณค่าอัตราความผิดพลาดบิตเชิงควอนตัมด้วยวิธีการสุ่มตัวอย่างบิตเปิดเผย (QBER estimation by key sampling) โดยการนำชุดข้อมูลกุญแจซิฟท์ (Sifted key) จำนวน 5,120 บิต มาดำเนินการสุ่มบิตเปิดเผยและเปรียบเทียบค่าระหว่าง *Alice* กับ *Bob* จำนวน 20% จากข้อมูลกุญแจทั้งหมดหรือเท่ากับตัวอย่างบิตจำนวน 1,024 บิต



รูปที่ 6 ผลการประมาณค่าอัตราความผิดพลาดบิตเชิงควอนตัม ($QBER_{Est}$) ด้วยวิธีการสุ่มเปิดเผยและเปรียบเทียบค่าบิตข้อมูลกุญแจซิฟท์ 20% จากจำนวนกุญแจทั้งหมด (20% of key sampling) ดำเนินการทดสอบจำนวน 100 รอบ

ผลของการทดสอบประสิทธิภาพการประมาณค่า $QBER_{Est}$ ในแต่ละรอบการทำงานของระบบการกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศแบบพัวพัน จำนวน 100 รอบ แสดงได้ดังรูปที่ 6 จากผลการทดสอบพบว่า วิธีการประมาณค่า $QBER_{Est}$ ที่ได้นำเสนอจากการคำนวณในสมการ (5) ให้ผลของค่าเฉลี่ย $QBER_{Est}$ เท่ากับ 2.0127% จากจำนวนรอบในการทดลองทั้งหมด โดยมีค่า $QBER_{Est}$ สูงสุดเท่ากับ 2.5391% และค่า $QBER_{Est}$ ต่ำสุดเท่ากับ 1.5625% รวมถึงการนำผลของค่า $QBER_{Est}$ ทั้งหมดมาพิจารณาการกระจายของข้อมูลจากการคำนวณค่าเบี่ยงเบนมาตรฐาน (Standard Deviation: S.D.) ได้เท่ากับ 0.2861 โดยหลังจากสิ้นสุดขั้นตอนการประมาณค่าอัตราความผิดพลาดบิตเชิงควอนตัมแล้ว จำนวนบิตที่เปิดเผยจะถูกตัดทิ้งและนำข้อมูลกุญแจซิฟท์ที่คงเหลือจำนวน 4,096 บิต เข้าสู่การประมวลผลการไกล่เกลี่ยความผิดพลาดในขั้นตอนถัดไป



รูปที่ 7 ผลการทดสอบประสิทธิภาพอัตรากำเนิดกุญแจ (Key rate) ที่เกิดขึ้นในแต่ละขั้นตอนการประมวลผลรหัสลับส่วนหลัง (QKD post-processing) ได้แก่ อัตราเร็วของกุญแจซิฟท์ (Sifted key rate) อัตราเร็วของกุญแจที่ได้รับการยืนยันความถูกต้อง (Identical key rate) และอัตราเร็วของกุญแจรหัสลับ (Secret key rate) ตามลำดับ โดยแสดงผลตามรอบการทำงานของระบบฯ จำนวนทั้งสิ้น 100 รอบ

รูปที่ 7 แสดงผลการทดสอบประสิทธิภาพอัตรากำเนิดกุญแจ (Key rate) ที่เกิดขึ้นในแต่ละขั้นตอน QKD post-processing ตามรอบการทำงานของระบบกระจายกุญแจรหัสลับเชิงควอนตัม จำนวนทั้งสิ้น 100 รอบ โดยเริ่มต้นพิจารณาประสิทธิภาพอัตราเร็วของกุญแจซิฟท์ (Sifted key rate) ที่ได้จากขั้นตอนการรับส่งสถานะเชิงควอนตัมแบบพัวพันผ่านอากาศและการแลกเปลี่ยนเวกเตอร์ฐานตามเกณฑ์วิธี BBM92 มีค่าเฉลี่ยของอัตราเร็วที่ 1,109.08 บิตต่อวินาที (Bits per second: bps) จากนั้นจึงเข้าสู่ขั้นตอนประมวลผลการไกล่เกลี่ยความผิดพลาดบนบิตข้อมูลกุญแจซิฟท์ระหว่างคู่สื่อสารให้มีค่าถูกต้องตรงกัน โดยการออกแบบวิธีการไกล่เกลี่ยความผิดพลาดบนพื้นฐานของรหัสช่องสัญญาณ (Information reconciliation based on channel coding scheme) เพื่อปรับอัตราการเข้ารหัสแอลดีพีซี (Rate-adaptive LDPC

codes) ได้อย่างเหมาะสมกับ $QBER_{Est}$ เป็นผลให้ภาคส่ง (*Alice*) สามารถกำเนิดข้อมูลซินโดรม (Syndrome information) ให้มีปริมาณเหมาะสมกับประสิทธิภาพในการถอดรหัสเพื่อแก้ไขความผิดพลาดบนชุดกุญแจซิฟท์ของภาครับ (*Bob*) ซึ่งปริมาณข้อมูลซินโดรมนี้ถือเป็นสารสนเทศที่เปิดเผยในระหว่างขั้นตอนการไกล่เกลี่ยความผิดพลาด (M_{Leak}) อันมีความสัมพันธ์กับการเลือกใช้อัตราการเข้ารหัสแอลดีพีซีที่เหมาะสม (R_{Opt}) ตามขั้นตอนวิธีที่ได้นำเสนอ และจะถูกนำไปพิจารณาเป็นส่วนหนึ่งของปริมาณสารสนเทศที่ผู้ดักจับ (*Eve*) มีโอกาสได้รับข้อมูลดังกล่าวบนช่องทางการสื่อสารทั่วไป ซึ่งต้องถูกนำไปคำนวณเพื่อตัดลดความสัมพันธ์กับข้อมูลกุญแจรหัสลับสุดท้ายในขั้นตอนการขยายสภาวะส่วนตัวภายใต้เงื่อนไขความปลอดภัยของระบบ QKD ที่ส่งผลต่อค่าอัตราการกำเนิดกุญแจรหัสลับ (Secret key rate) หลังสิ้นสุดกระบวนการ QKD post-processing ในแต่ละรอบของการทดสอบประสิทธิภาพ

จากผลการทดสอบพบว่า วิธีการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสแอลดีพีซีให้เหมาะสม สามารถให้ผลของประสิทธิภาพการไกล่เกลี่ยความผิดพลาด (f_{Recon}) ที่คำนวณได้ดังสมการ (6) มีค่าเฉลี่ยของ f_{Recon} เท่ากับ 1.1919 สอดคล้องกับค่าเฉลี่ยของจำนวนบิตเปิดเผย (M_{Leak}) เท่ากับ 691.96 บิต หรือคิดเป็น 16.89% จากขนาดของกุญแจซิฟท์ที่เข้าสู่การประมวลผลการไกล่เกลี่ยความผิดพลาดจำนวน 4,096 บิต และเมื่อนำข้อมูลกุญแจที่ผ่านการไกล่เกลี่ยความผิดพลาดแล้ว (Reconciled key) เข้าสู่ขั้นตอนการยืนยันความถูกต้อง (Confirmation) ด้วยฟังก์ชันแฮชพหุนาม (Polynomial hashing function) เพื่อกำเนิดรหัสแฮช (Hash) ขนาด 64 บิต แทนข้อมูล Reconciled key ระหว่างภาคส่งกับภาครับแล้วดำเนินการเปรียบเทียบ ซึ่งผลการทดลองพบว่า อัตราความสำเร็จในการยืนยันความถูกต้องตรงกัน (Success rate of confirmation) บนชุดกุญแจระหว่างคู่สื่อสารหลังจากการไกล่เกลี่ยความผิดพลาดในครั้งที่ 1 เท่ากับ 86% และหากนำชุดกุญแจที่มีผลการยืนยันความถูกต้องล้มเหลวในครั้งที่ 1 นี้มาดำเนินการไกล่เกลี่ยความผิดพลาดอีกครั้ง โดยการปรับลดอัตราเข้ารหัสเพื่อเพิ่มปริมาณข้อมูลซินโดรมให้กับภาครับในการแก้ไขบิตข้อมูลที่ผิดพลาดเพิ่มเติมแล้ว สามารถให้ผลสำเร็จการยืนยันความถูกต้องในครั้งที่ 2 เท่ากับ 100% จากการทดลองทั้งหมด 100 รอบ โดยหลังจากสิ้นสุดขั้นตอนการไกล่เกลี่ยความผิดพลาดและการยืนยันความถูกต้อง สามารถให้กำเนิดข้อมูลกุญแจที่ผ่านการยืนยันความถูกต้องแล้วมีอัตราเร็วเฉลี่ย (Identical key rate) ที่ 782.39 บิตต่อวินาที

หลังจากนั้นจึงเข้าสู่ขั้นตอนการขยายสภาวะส่วนตัว ซึ่งเป็นขั้นตอนสุดท้ายของกระบวนการ QKD post-processing โดยอาศัยฟังก์ชันแฮชเชิงเอกภพบนพื้นฐานของเมทริกซ์แบบโทพลิทซ์ (Universal hashing function based on Toeplitz matrix) ในการให้กำเนิดกุญแจรหัสลับ (Secret key) ที่ถูกตัดลดความสัมพันธ์กับข้อมูลที่ผู้ดักจับมีโอกาสได้รับหรือขโมยไปในระหว่างการสื่อสารผ่านช่องสัญญาณเชิงควอนตัมและช่องทางการสื่อสารทั่วไป จากผลการทดสอบพบว่า ขนาดของกุญแจรหัสลับสุดท้าย (l_{Sec}) ที่ได้จากการคำนวณภายใต้เงื่อนไขความปลอดภัยของระบบ QKD ในสมการ (7) มีค่าเฉลี่ยของจำนวนบิต l_{Sec} เท่ากับ 2,409.96 บิตต่อรอบ คิดเป็นค่าเฉลี่ยของจำนวนบิตที่ถูกตัดลดความสัมพันธ์เท่ากับ 34.62% จากขนาดของกุญแจที่เข้าสู่ขั้นตอนการขยายสภาวะส่วนตัว และสามารถให้ผลลัพธ์ของอัตราการกำเนิดกุญแจรหัสลับสุดท้าย (Secret key rate) มีค่าเฉลี่ยเท่ากับ 428.42 บิตต่อวินาที จากจำนวนรอบในการทดลองทั้งหมด

โดยค่าพารามิเตอร์ผลลัพธ์จากการทดสอบประสิทธิภาพตามรายะเอียดของกระบวนการ QKD post-processing ที่ได้ดำเนินการออกแบบ พัฒนา และทดสอบในระบบตัวอย่างการกระจายกุญแจรหัสลับเชิงควอนตัมแบบคู่โฟตอนพัวพันบนอุปกรณ์ EPR 405 แสดงเป็นผลสรุปได้ดังตารางที่ 4

ตารางที่ 4 ค่าพารามิเตอร์ผลลัพธ์ที่ได้จากการทดสอบประสิทธิภาพกระบวนการประมวลผลรหัสลับส่วนหลัง (QKD post-processing) ร่วมกับระบบการกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศแบบคู่โฟตอนพัวพันด้วยอุปกรณ์ EPR 405

พารามิเตอร์การทดสอบประสิทธิภาพ	การประมาณค่า $QBER_{Est}$ ด้วยการสุ่มตัวอย่างบิต		การไกล่เกลี่ยความผิดพลาดด้วยการปรับอัตราเข้ารหัสแอลดีพีซีที่เหมาะสมและยืนยันความถูกต้อง			การขยายสภาวะส่วนตัวด้วยเมทริกซ์แบบโทพลิทซ์	
	อัตราเร็วของกุญแจซิฟท์ (Sifted key rate) [bps]	ค่า $QBER_{Est}$	จำนวนบิตเปิดเผย (M_{Leak}) [บิต (%)]	ประสิทธิภาพการไกล่เกลี่ยความผิดพลาด (f_{Recon})	อัตราเร็วของกุญแจที่ยืนยันความถูกต้อง (Identical key rate) [bps]	ขนาดของกุญแจรหัสลับต่อรอบ (l_{Sec}) [บิต]	อัตรากำเนิดกุญแจรหัสลับ (Secret key rate) [bps]
ค่าต่ำสุด (Minimum value)	905.39	1.5625%	579 (14.14%)	1.1210	595.96	2,165	324.72
ค่าสูงสุด (Maximum value)	1,384.91	2.5391%	846 (20.65%)	1.3619	930.91	2,607	522.78
ค่าเฉลี่ย (Average value)	1,109.08	2.0127%	691.96 (16.89%)	1.1919	782.39	2,409.96	428.42
	ค่าเบี่ยงเบนมาตรฐาน (S.D.) เท่ากับ 0.2861		อัตราความสำเร็จการยืนยันความถูกต้อง (Success rate of confirmation)		ครั้งที่ 1 = 86% ครั้งที่ 2 = 100%	ค่าเฉลี่ยของจำนวนบิตที่ถูกตัดลดความสัมพันธ์ เท่ากับ 34.62%	

5. สรุปผลการศึกษาและข้อเสนอแนะ

วิธีการประมวลผลกำเนิดรหัสลับส่วนหลังจากระบบการกระจายกุญแจรหัสลับเชิงควอนตัม (QKD post-processing) ที่นำเสนอในงานวิจัยนี้ ได้ดำเนินการออกแบบให้สอดคล้องกับหลักปฏิบัติของระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) ประกอบด้วยขั้นตอนวิธีทั้งสามส่วนหลัก ได้แก่ 1) การประมาณค่าพารามิเตอร์ช่องสัญญาณเชิงควอนตัม โดยอาศัยการสุ่มตัวอย่างบิตเปิดเผยและเปรียบเทียบกันระหว่างคู่สื่อสารเพื่อคำนวณหาค่าอัตราความผิดพลาดบิตเชิงควอนตัม (*QBER*) 2) การไกล่เกลี่ยความผิดพลาดด้วยวิธีการปรับอัตราเข้ารหัสแอลดีพีซีให้เหมาะสมกับค่า *QBER* ประสานการทำงานร่วมกับวิธีการยืนยันความถูกต้องด้วยรหัสแฮชแทนชุดข้อมูลกุญแจที่กำเนิดจากฟังก์ชันแฮชแบบพหุนาม และ 3) การขยายสภาวะส่วนตัวด้วยเทคนิคของเมทริกซ์แบบโทพลิทซ์ในรูปแบบของฟังก์ชันแฮชเชิงเอกภพ ซึ่งสามารถประมวลผลเพื่อกำเนิดกุญแจรหัสลับสุดท้ายที่มีขนาดของจำนวนบิตภายใต้ขีดจำกัดด้านความปลอดภัยทางทฤษฎีสารสนเทศ (Information-theoretic security)

วิธีการที่นำเสนอทั้งสามส่วนหลักได้ถูกนำมาพัฒนาในรูปแบบซอฟต์แวร์เชื่อมโยงการทำงานเพื่อรับส่งข้อมูลร่วมกันระหว่างขั้นตอนเป็นกระบวนการ QKD post-processing และดำเนินการทดสอบประสิทธิภาพร่วมกับชุดข้อมูลกุญแจซิฟท์ที่ได้จากระบบการกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศแบบพัวพันตามเกณฑ์วิธี BBM92 ของอุปกรณ์ EPR 405 ในระยะทาง 11 เมตร ให้กำเนิดอัตราเร็วของกุญแจซิฟท์ (Sifted key rate) มีค่าเฉลี่ยเท่ากับ 1,109.08 bps จากผลการทดลองพบว่า ขั้นตอนวิธีตามกระบวนการ QKD post-processing ที่นำเสนอสามารถรับค่าข้อมูลกุญแจซิฟท์ซึ่งเป็นอินพุตของกระบวนการเข้าสู่การประมวลผลเพื่อให้กำเนิดกุญแจรหัสลับสุดท้ายมีค่าเฉลี่ยของอัตราเร็ว (Secret key rate) เท่ากับ 428.42 bps บนอัตราความผิดพลาดบิตเชิงควอนตัมที่ได้จากการประมาณ (QBER estimation) มีค่าเฉลี่ยเท่ากับ 2.0127% ประสิทธิภาพการไกล่เกลี่ยความผิดพลาด (Reconciliation efficiency) มีค่าเฉลี่ยเท่ากับ 1.1919 และขนาดของกุญแจรหัสลับสุดท้ายที่ปลอดภัย (Final secret key length) มีค่าเฉลี่ยเท่ากับ 2,409.96 บิตต่อรอบ จากจำนวนการทดลองทั้งหมด

ในการทดสอบประสิทธิภาพของกระบวนการ QKD post-processing ที่นำเสนอในงานวิจัยนี้ ได้ดำเนินการร่วมกับอุปกรณ์การกระจายกุญแจรหัสลับเชิงควอนตัมแบบพัวพัน (Entanglement-based QKD) ซึ่งมีข้อจำกัดในด้านอุปกรณ์ฮาร์ดแวร์เชิงแสงเพื่อกำเนิดคู่โฟตอนพัวพันจากแหล่งกำเนิดตัวกลาง (Entangled photon source) และถูกส่งไปตรวจวัดค่าสถานะที่คู่สื่อสาร จนได้ผลลัพธ์เป็นชุดข้อมูลกุญแจดิบ

(Raw key) สำหรับประมวลผลการแลกเปลี่ยนเวกเตอร์ฐาน (Sifting) เพื่อกำเนิดกุญแจซิฟท์ที่อัตราเร็ว (Sifted key rate) โดยประมาณเท่ากับ 1 kbps ส่งผลต่อเนื่องกับอัตราการกำเนิดกุญแจรหัสลับสุดท้าย (Secret key rate) หลังจากกระบวนการ QKD post-processing อยู่ในระดับต่ำกว่า 1 kbps หากพิจารณาถึงการพัฒนาเทคโนโลยีการกระจายกุญแจรหัสลับเชิงควอนตัมสู่การใช้งานเป็นโครงสร้างพื้นฐานการรักษาความปลอดภัยสารสนเทศแล้วนั้น การออกแบบและพัฒนากระบวนการ QKD post-processing ให้มีประสิทธิภาพสูงจะเป็นส่วนหนึ่งของการผลักดันศักยภาพด้านอัตราเร็วการกำเนิดกุญแจรหัสลับในระบบ QKD ให้สูงขึ้น โดยขั้นตอนวิธี QKD pot-processing ที่ได้นำเสนอในงานวิจัยนี้ สามารถนำมาประยุกต์ใช้งานร่วมกับอุปกรณ์การกระจายกุญแจรหัสลับเชิงควอนตัมความเร็วสูง (High-speed QKD devices) [53] โดยการปรับค่าพารามิเตอร์อินพุตในแต่ละขั้นตอนให้เหมาะสมกับการประมวลผลชุดข้อมูลกุญแจซิฟท์ในระดับที่สูงกว่า 1 Mbps ยกตัวอย่างเช่น การขยายขนาดการรับจำนวนกุญแจต่อรอบในการประมวลผล และการเพิ่มขนาดบล็อกของรหัสแอลดีพีซี (LDPC block length) และเมทริกซ์ตรวจสอบพาริตี้ (Parity-check matrix) ในระดับตั้งแต่ 100,000 บิตขึ้นไป เป็นต้น ซึ่งจะเพิ่มความสามารถในการแก้ไขความผิดพลาดที่สูงกว่าการเลือกใช้รหัสแอลดีพีซีที่มีบล็อกขนาดสั้น ส่งผลให้ประสิทธิภาพการไกล่เกลี่ยความผิดพลาดมีค่าสูงขึ้นสอดคล้องกับจำนวนบิตเปิดเผยในระหว่างการไกล่เกลี่ยความผิดพลาดมีปริมาณลดลง ดังนั้นอัตราการกำเนิดกุญแจรหัสลับสุดท้ายหลังจากการตัดลดความสัมพันธ์กับสารสนเทศที่เปิดเผยในขั้นตอนการขยายสภาวะส่วนตัวจะมีความเร็วที่สูงขึ้นด้วยเช่นกัน แต่อย่างไรก็ตามการขยายจำนวนบิตเพื่อรองรับปริมาณกุญแจที่มากขึ้นจะส่งผลกระทบต่อความซับซ้อนในคำนวณ (Computational complexity) อันสัมพันธ์กับระยะเวลาการประมวลผล (Computation time) ที่สูงขึ้น ซึ่งปัญหาดังกล่าวจะถูกนำมาพิจารณาเพื่อศึกษาประสิทธิภาพสำหรับเป็นแนวทางการออกแบบและพัฒนากระบวนการ QKD post-processing ทั้งในรูปแบบของซอฟต์แวร์ไลบรารี (Software library) และการพัฒนาต่อยอดสู่ต้นแบบเชิงฮาร์ดแวร์ เช่น อุปกรณ์ลอจิกแบบโปรแกรม (Field programmable gate array: FPGA) เป็นต้น ที่จะสามารถลดเวลาการประมวลผลกระบวนการ QKD post-processing ให้รวดเร็วยิ่งขึ้น สนับสนุนการประยุกต์ใช้งานจริงในระบบเชิงพาณิชย์ที่ต้องการความเร็วสูงต่อไป

กิตติกรรมประกาศ

งานวิจัยนี้ได้รับการสนับสนุนการดำเนินงานจากกองทุนวิจัย สำนักวิจัยและพัฒนา มหาวิทยาลัยราชภัฏพระนคร คณะวิจัยขอขอบคุณศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติที่ให้การสนับสนุนสถานที่และเครื่องมือสำหรับการดำเนินงานวิจัย และขอขอบคุณ Dr. Christoph Pacher, Dr. Andreas Poppe และ Mr. Oliver Maurhart จากสถาบันเทคโนโลยีแห่งออสเตรียที่ให้คำปรึกษาด้านเทคนิคในการพัฒนางานวิจัย

เอกสารอ้างอิง

[1] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. *Proceedings of International Conference on Computers, Systems and Signal Processing; 1984; Bangalore, India*. p. 175–179.

[2] Wootters WK, Zurek WH. A single quantum cannot be cloned. *Nature*. 1982; 299: 802–803.

[3] Cachin C, Maurer U. Unconditional security against memory- bounded adversaries. *Advances in Cryptology– CRYPTO ' 97*. Springer, Berlin, Heidelberg. 1997; 1294: 292–306.

[4] ID Quantique. Clavis XG QKD system. Available from: https: / / www. idquantique. com/ quantum- safe-security/products/clavis-xg-qkd-system/ [Accessed 1 Febuary 2023]

[5] Toshiba Digital Solutions Corporation. Quantum Key Distribution Products. Available from: https: / / www. global. toshiba/ ww/ products-solutions/ security- ict/ qkd/ products. html [Accessed 1 Febuary 2023]

[6] Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. *Reviews of modern physics*. 2020; 92: 025002.

[7] Shannon CE. A mathematical theory of communication. *The Bell System Technical Journal*. 1948; 27(3): 379–423.

[8] Maurer UM. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*. 1993; 39(3): 733–742.

[9] Fung CHF, Ma X, Chau H. Practical issues in quantum-key-distribution postprocessing. P*hysical Review A*. 2010; 81(1): 012318.

[10] Maroy O, Gudmundsen M, Lydersen L, Skaar J. Error estimation, error correction and verification in quantum key distribution. *IET Information Security*. 2014; 8(5): 277–282.

[11] Kiktenko EO, Trushechkin AS, Kurochkin YV, Fedorov AK. Post- processing procedure for industrial quantum key distribution systems, *Journal of Physics: Conference Series*. 2016; 741: 012081.

[12] Lorünser T, Krenn S, Pacher C, Schrenk B. On the security of offloading post-processing for quantum key distribution, *Entropy*. 2023; 25(2): 226.

[13] Scarani V, Pasquinucci HB, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Reviews of Modern Physics*. 2009; 81(3): 1301–1350.

[14] Elkouss D, Martinez-Mateo J, Martin V. Analysis of a rate-adaptive reconciliation protocol and the effect of the leakage on the secret key rate. *Physical Review A*. 2013; 87(4): 042334.

[15] Treeviriyanupab P, Phromsa-ard T, Zhang CM, Li M, Sangwongngam P, Sanevong Na Ayutaya T, et al. Rate-adaptive reconciliation and its estimator for quantum bit error rate. *International Symposium on Communications and Information Technologies; 2014*; Incheon, Korea. 2014. p 351–355.

[16] Wegman MN, Carter JL. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*. 1981; 22(3): 265–279.

[17] Krovetz T, Rogaway P. Fast universal hashing with small keys and no preprocessing: the PolyR construction. *Lecture Notes in Computer Science*. 2015; 73–89.

[18] Gray RM. Toeplitz and circulant matrices: a review. *Foundations and Trends® in Communications and Information Theory*. 2006; 2(3): 155–239.

[19] Poppe A, Fedrizzi A, Hubel H, Ursin R, Zeillinger A. Entangled state quantum key distribution and teleportation. *31st European Conference on Optical Communication*. 2015; Glasgow, Scotland.

[20] Melniczuk D, Jacak M. Testing of the entangled QKD system EPR S405 Quelle (AIT) in commercial 1550 nm fiber network. *International Journal of Communications, Network and System Sciences*. 2014; 7(1): 30–36.

[21] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*. 1978; 21(2): 120 –126.

[22] Diffie W, Hellman ME. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976; 22(6): 644–654.

[23] Strangio MA. Efficient Diffie-Hellmann two-party key agreement protocols based on elliptic curves. *Proceedings of the 2005 ACM symposium on Applied computing; 2005*, *New York, United States*. 2005. p 324–331.

[24] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, et al. Quantum supremacy using a programmable superconducting processor. *Nature*. 2019; 574: 505–511.

[25] IEEE Spectrum. An IBM quantum computer will soon pass the 1000- qubit mark. Available from: https://spectrum.ieee.org/ibm-condor [Aceessed 30 January 2023]

[26] Yan B, Tan Z, Wei S, Jiang H, Wang W, Wang H, et al. Factoring integers with sublinear resources on a superconducting quantum processor. arXiv. Available from: https://arxiv.org/abs/2212.12372 [Aceessed 31 January 2023]

[27] Schneier B. Breaking RSA with a quantum computer. Available from: https: / / www. schneier. com/ blog/ archives/ 2023/ 01/ breaking- rsa- with- a-

quantum- computer. html [Aceessed 31 January 2023]

[28] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat JP, Grangier P. Single photon quantum cryptography. *Physical Review Letters*. 2002; 89: 187901.

[29] Ekert AK. Quantum cryptography based on Bell' s theorem. *Physical Review Letters*. 1991; 67(6): 661-663.

[30] Bennett CH, Brassard G, Mermin D. Quantum cryptography without Bell' s theorem. *Physical Review Letters*. 1992; 68(5): 557-559.

[31] Barker E. Guideline for using cryptographic standards in the federal government: Cryptographic Mechanisms, NIST Special Publication 800-175B, National Institute of Standards and Technology; 2020 March. Available from: https: / / doi. org/ 10. 6028/ NIST. SP. 800- 175Br1 [Aceessed 30 January 2023]

[32] Felsch D, Grothe M, Schwenk J, Czubak A, Szymanek M. The dangers of key reuse: practical attacks on IPsec IKE. *Proceedings of the 27th USENIX Security Symposium; 2018 Aug; Maryland, United States*. 2018. p 567–583.

[33] Shannon CE. Communication theory of secrecy systems. *The Bell System Technical Journal*. 1949; 28(4): 656–715.

[34] Vernam GS. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Transactions of the American Institute of Electrical Engineers*. 1926; 45: 295–301.

[35] Renner R, Gisin N, Kraus B. Information- theoretic security proof for quantum - key- distribution protocols. *Physical Review A*. 2005; 72(1): 012332.

[36] พัชรพงษ์ ตรีวิริยานุภาพ, ธราธร พรมสะอาด. การประมาณค่าช่องสัญญาณด้วยภาวะน่าจะเป็นสูงสุดสำหรับการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสเหมาะสมกับการกระจายกุญแจรหัสลับเชิงควอนตัม. *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*. 2560; 27(1): 169–178.

[37] Kiktenko EO, Malyshev AO, Bozhedarov AA, Pozhar NO, Anufriev MN, Fedorov AK. Error estimation at the information reconciliation stage of quantum key distribution. *Journal of Russian Laser Research*. 2018; 39: 558–567.

[38] Yang L, Dong H, Li Z. One- way information reconciliation schemes of quantum key distribution. *Cybersecurity*. 2019; 2: 16.

[39] Brassard G, Salvail L. Secret- key reconciliation by public discussion. *Advances in Cryptology–EUROCRYPT '93*. 1993, 765: 410–423.

[40] Martinez- Mateo J, Pacher C, Peev M. Demystifying the information reconciliation protocol cascade. *Quantum Information & Computation*. 2015; 15(5–6): 453–477.

[41] Gallager R. *Low- Density Parity- Check Codes* [dissertation] . Massachusetts Institute of Technology; 1963.

[42] Richardson T, Urbanke R. *Modern Coding Theory*. Cambridge University Press; 2008.

[43] Kiktenko EO, Malyshev OA, Fedorov AK. Blind information reconciliation with polar codes for quantum key distribution. *IEEE Communications Letters*. 2021; 25(1): 79–83.

[44] Mao HK, Qiao YC, Li Q. High- efficient syndrome-based LDPC reconciliation for quantum key distribution. *Entropy*. 2021; 23(11): 1440.

[45] Borisov N, Petrov I, Tayduganov A. Asymmetric adaptive LDPC- based information reconciliation for industrial quantum key distribution. *Entropy*. 2023; 25(1): 31.

[46] Scarani V, Renner R. Quantum cryptography with finite resources: unconditional security bound for discrete- variable protocols with one- way postprocessing. *Physical Review Letters*. 2008; 100(20): 200501.

[47] Tomamichel M, Lim CCW, Gisin N, Renner R. Tight finite-key analysis for quantum cryptography. *Nature Communications*. 2012; 3: 634.

[48] Richardson T, Shokrollahi MA, Urbanke R. Design of capacity- approaching irregular low- density parity-check codes. *IEEE Transactions on Information Theory*. 2001; 47(2): 619–637.

[49] Slepian D, Wolf JK. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*. 1973; 19(4): 471–480.

[50] Tian T, Jones CR. Construction of rate compatible LDPC codes utilizing information shortening and parity puncturing. *EURASIP Journal on Wireless Communications and Networking*. 2005; 5: 789–795.

[51] Maurhart O, Petscharnig S, Grafenauer T, Ömer B, Hentschel M, Vogt PS, et al. AIT QKD post processing and network software. *The Annual conference on quantum cryptography (QCrypt) ; 2020 Aug; Amsterdam, The Netherlands*, 2020.

[52] Maurhart O. AIT QKD R10 Software, 2016. Available from: https://github.com/axdhill/ait-qkd [Aceessed 12 March 2022]

[53] Sax R, Boaron A, Boso G, Atzeni S, Crespi A, GrÜnenfelder F, et al. High-speed integrated QKD system. arXiv. Available from: https://arxiv.org/abs/ 2211. 11560 [Aceessed 3 February 2023]