วารสารวิชาการพระจอมเกล้าพระนครเหนือ ปีที่ 27 ฉบับที่ 1 ม.ค.–เม.ย. 2560
The Journal of KMUTNB., Vol. 27, No. 1, Jan.–Apr. 2017

บทความวิจัย

การประมาณค่าช่องสัญญาณด้วยภาวะน่าจะเป็นสูงสุดสำหรับการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสเหมาะสมกับการกระจายกุญแจรหัสลับเชิงควอนตัม

พัชรพงษ์ ตรีวิริยานุภาพ*
สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏพระนคร
ธราธร พรมสะอาด
ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 0-2544-8002 อีเมล: patcharapong@pnru.ac.th DOI: 10.14416/j.kmutnb.2016.04.004
รับเมื่อ 26 ตุลาคม 2558 ตอบรับเมื่อ 8 เมษายน 2559 เผยแพร่ออนไลน์ 1 พฤศจิกายน 2559

บทคัดย่อ

การกระจายกุญแจรหัสลับเชิงควอนตัมถือเป็นหนึ่งในเทคโนโลยีความปลอดภัยด้านการสื่อสาร โดยอาศัยหลักกลศาสตร์ควอนตัมเพื่อกำเนิดและแลกเปลี่ยนข้อมูลกุญแจรหัสลับระหว่างคู่สื่อสารให้มีความปลอดภัยสูงสุดสำหรับระบบวิทยาการรหัสลับ ซึ่งต้องอาศัยกระบวนการไกล่เกลี่ยความผิดพลาดเพื่อจุดประสงค์ในการยืนยันความถูกต้องของข้อมูลกุญแจรหัสลับระหว่างคู่สื่อสารให้มีค่าที่ตรงกัน ในบทความนี้ นำเสนอวิธีการประมาณค่าอัตราความผิดพลาดของช่องสัญญาณเชิงควอนตัมบนพื้นฐานของการประมาณค่าภาวะน่าจะเป็นสูงสุดจากชุดข้อมูลซินโดรมในระหว่างขั้นตอนการไกล่เกลี่ยความผิดพลาดสำหรับการปรับค่าอัตราการเข้ารหัสให้เหมาะสมกับความผิดพลาดของบิตข้อมูลกุญแจเชิงควอนตัมที่เกิดขึ้นในแต่ละช่วงเวลาด้วยรหัสตรวจสอบพาริตี้แบบความหนาแน่นต่ำ ตลอดจนการนำมาประยุกต์ใช้แทนขั้นตอนการเปิดเผยบิตข้อมูลกุญแจบางส่วนที่สูญเสียไปในการประมาณค่าความผิดพลาดแบบดั้งเดิม นำไปสู่ผลลัพธ์ของขนาดบิตข้อมูลกุญแจที่เพิ่มสูงขึ้น โดยจากการวิเคราะห์และทดสอบผลพบว่า วิธีการที่นำเสนอให้ความแม่นยำในการประมาณค่าอัตราความผิดพลาดครอบคลุมเงื่อนไขของการกระจายกุญแจรหัสลับเชิงควอนตัม นำไปสู่การเพิ่มประสิทธิภาพการไกล่เกลี่ยความผิดพลาดที่สูงขึ้นทั้งในด้านความปลอดภัยและอัตราการกำเนิดกุญแจรหัสลับ สนับสนุนการประยุกต์ใช้งานจริงในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมความเร็วสูง

คำสำคัญ: การกระจายกุญแจรหัสลับเชิงควอนตัม, การประมาณค่าโดยภาวะน่าจะเป็นสูงสุด, รหัสตรวจสอบพาริตี้แบบความหนาแน่นต่ำ, การไกล่เกลี่ยความผิดพลาดแบบปรับค่าอัตราเข้ารหัส

การอ้างอิงบทความ: พัชรพงษ์ ตรีวิริยานุภาพ และ ธราธร พรมสะอาด, "การประมาณค่าช่องสัญญาณด้วยภาวะน่าจะเป็นสูงสุดสำหรับการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสเหมาะสมกับการกระจายกุญแจรหัสลับเชิงควอนตัม," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, ปีที่ 27, ฉบับที่ 1, หน้า 169–178, ม.ค.–เม.ย. 2560

วารสารวิชาการพระจอมเกล้าพระนครเหนือ ปีที่ 27 ฉบับที่ 1 ม.ค.–เม.ย. 2560
The Journal of KMUTNB., Vol. 27, No. 1, Jan.–Apr. 2017

Research Article

Channel Estimation Using Maximum-likelihood for Rate-adaptive Reconciliation in Quantum Key Distribution

Patcharapong Treeviriyanupab*
Department of Information Technology, Faculty of Science and Technology, Phranakhon Rajabhat University (PNRU), Bangkok, Thailand

Tharathorn Phromsa-ard
Department of Electrical Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand

* Corresponding Author, Tel. 0-2544-8002, E-mail: patcharapong@pnru.ac.th
DOI: 10.14416/j.kmutnb.2016.04.004
Received 26 October 2015; Accepted 8 April 2016; Published online: 1 November 2016

Abstract

Quantum Key Distribution (QKD), one of the communication security technologies, employs the properties of quantum mechanics to guarantee and exchange the perfectly-secured key generation between two legitimate parties for cryptographic purposes. The reconciliation process is required to correct the transmission error after the distribution of quantum objects. In this paper, the channel parameter estimation is proposed to estimate the error rate in the quantum channel by using the Maximum-Likelihood Estimation (MLE) based on the syndrome information for rate-adaptive reconciliation. The specific Low-Density Parity-Check (LDPC) codes are adapted to optimize their coding rates responding to the possible cases of error in QKD. The proposed method can be applied to avoid wasting sample keys in the traditional channel estimation, and led to increase the final secret key length. The simulation results show an accuracy of the estimated quantum bit error rate (QBER) for covering the range in QKD system. The gain of rate-adaptive reconciliation based on MLE confirms an improvement in the reconciliation efficiency that significantly impacts on the achievable secret key generation rate for high QKD throughput applications.

Keywords: Quantum Key Distribution, Maximum-likelihood Estimation, Low-density Parity-check Codes, Rate-adaptive Reconciliation

Please cite this article as: P. Treeviriyanupab and T. Phromsa-ard, "Channel estimation using maximum-likelihood for rate-adaptive reconciliation in quantum key distribution," *The Journal of KMUTNB.*, vol. 27, no. 1, pp. 169–178, Jan.–Apr. 2017 (in Thai).

1. บทนำ

การกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution: QKD) ถูกคิดค้นขึ้นครั้งแรกในปี พ.ศ. 2527 [1] และได้รับการวิจัยและพัฒนาจนนำมาประยุกต์ใช้งานได้จริงดังตัวอย่างของอุปกรณ์เชิงพาณิชย์ [2]–[4] โดยมีเป้าหมายเพื่อยกระดับความปลอดภัยในระบบการสื่อสารสำหรับสร้างและแลกเปลี่ยนข้อมูลกุญแจรหัสลับให้มีความปลอดภัยสูงสุดแบบไม่มีเงื่อนไข โดยแบ่งส่วนการทำงานออกเป็นห้าขั้นตอนหลัก ดังนี้

1) การรับส่งสถานะเชิงควอนตัม (Quantum Transmission and Reception) บิตข้อมูลกุญแจถูกแทนด้วยหน่วยสารสนเทศเชิงควอนตัมหรือคิวบิต (Qubit) เช่น โพลาไรเซชัน หรือเฟสของโพลาไรเซชัน (Phase-polarization) ของโฟตอนเดี่ยว เป็นต้น ส่งผ่านช่องทางการสื่อสารเชิงควอนตัม จากภาคส่ง (*Alice*) ไปยังภาครับ (*Bob*) ตามลำดับ ผลลัพธ์ที่ได้จากขั้นตอนนี้คือบิตข้อมูลกุญแจดิบ (Raw Key) แบบไบนารีของคู่สื่อสาร *Alice* กับ *Bob*

ในส่วนของขั้นตอนอื่นๆ จะเกิดขึ้นบนช่องสัญญาณทั่วไป หรือที่เรียกว่า การประมวลผลการกำเนิดกุญแจรหัสลับส่วนหลัง (QKD Post-processing) ซึ่งอาศัยเทคนิคการประมวลผลข้อมูลสารสนเทศทั่วไป ภายใต้หลักทฤษฎีข่าวสาร และความปลอดภัยของสารสนเทศ

2) การแลกเปลี่ยนเวกเตอร์ฐาน (Key Sifting) *Alice* และ *Bob* เลือกค่าสถานะของกุญแจดิบเฉพาะที่มีเวกเตอร์ฐาน (Basis) ในการสร้างและวัดค่าสถานะเชิงควอนตัมที่ตรงกันโดยผลลัพธ์ที่ได้คือ บิตข้อมูลไบนารีระหว่าง *Alice* กับ *Bob* ที่มีความยาวเท่ากัน ถูกเรียกว่ากุญแจซิฟท์ (Sifted Key)

3) การประมาณค่าพารามิเตอร์ช่องสัญญาณเชิงควอนตัม (Quantum Channel Parameter Estimation) โดยทั่วไปคู่สื่อสาร (*Alice* กับ *Bob*) ดำเนินการสุ่มเปิดเผยบิตข้อมูลกุญแจซิฟท์บางส่วนเพื่อแลกเปลี่ยนซึ่งกันและกัน (Key Sampling) สำหรับประมาณค่าอัตราความผิดพลาดบนช่องสัญญาณเชิงควอนตัม (Quantum Bit Error Rate: QBER) ที่บ่งบอกถึงความน่าจะเป็นร่วม (Joint Probability) ของข้อมูลกุญแจระหว่าง *Alice* กับ *Bob* และผู้ดักจับข้อมูล (Eavesdropper: *Eve*) โดยข้อมูลกุญแจซิฟท์ที่เปิดเผยต้องถูกตัดทิ้ง และนำข้อมูลกุญแจส่วนที่เหลือเข้าสู่กระบวนการต่อไป หาก QBER มีค่าสูงอย่างผิดปกติ (QBER > 11%) ระบบต้องยกเลิกการใช้งานกุญแจซิฟท์ทั้งหมด

4) การไกล่เกลี่ยความผิดพลาด (Key Reconciliation) ขั้นตอนการแก้ไขความผิดพลาดของข้อมูลซิฟท์ระหว่าง *Alice* กับ *Bob* อันเนื่องมาจากความผิดพลาดจากการรับส่งสถานะผ่านช่องทางการสื่อสารเชิงควอนตัมที่อาจเกิดขึ้นจากสาเหตุของสัญญาณรบกวน (Noise) หรือความไม่เป็นอุดมคติของอุปกรณ์ เป็นต้น ในวิธีการไกล่เกลี่ยความผิดพลาดแบบทางเดียว (One-way Reconciliation) [5] เริ่มต้นจาก *Alice* ทำการสร้างข้อมูลที่มีความสัมพันธ์เกี่ยวข้องกับกุญแจซิฟท์ของตนและส่งไปให้ *Bob* ผ่านช่องสัญญาณแบบทั่วไป เพื่อใช้ตรวจสอบและแก้ไขตำแหน่งบิตของกุญแจซิฟท์ที่ผิดพลาดให้มีค่าตรงกันระหว่างคู่สื่อสาร หรือที่เรียกว่า Reconciled Key

5) การขยายสภาวะส่วนตัว (Privacy Amplification) การลดความสัมพันธ์ข้อมูลกุญแจที่ *Eve* มีโอกาสได้รับหรือขโมยไปทั้งในช่องสัญญาณเชิงควอนตัมและช่องสัญญาณทั่วไป โดยคู่สื่อสารนำกุญแจที่ถูกแก้ไขความผิดพลาด (Reconciled Key) คูณกับเมทริกซ์แบบไบนารีของฟังก์ชันแฮช (Universal Hashing) เพื่อกำเนิดเป็นบิตข้อมูลกุญแจรหัสลับสุดท้าย ที่มีความปลอดภัยสูงสุด [6]

บทความนี้ ให้ความสนใจในการแก้ไขปัญหาขีดจำกัดด้านประสิทธิภาพของขั้นตอนการประมาณค่าพารามิเตอร์ช่องสัญญาณเชิงควอนตัม และการไกล่เกลี่ยความผิดพลาดในระบบ QKD

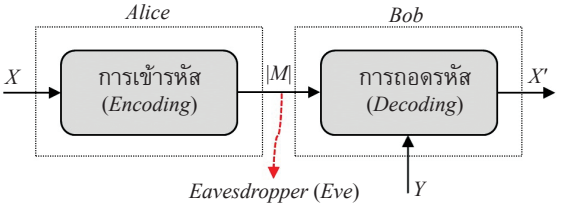
โดยทั่วไปวิธีการไกล่เกลี่ยความผิดพลาดอาศัยพื้นฐานการค้นหาแบบไบนารี และถูกนำมาพัฒนาเป็นโพรโทคอลสำหรับการใช้งานจริงดังตัวอย่างของโพรโทคอลคาสเคด (Cascade) [7] ที่อาศัยการติดต่อสื่อสารระหว่าง *Alice* กับ *Bob* เป็นจำนวนมาก อันส่งผลต่อการประมวลผลที่ล่าช้า ซึ่งยังคงเป็นข้อจำกัดของอัตรา

การกำเนิดกุญแจรหัสลับเชิงควอนตัม

นอกจากนี้ ปัญหาของการไกล่เกลี่ยความผิดพลาดในระบบ QKD ยังได้รับการพัฒนาในแนวทางเช่นเดียวกับเทคโนโลยีของระบบการสื่อสารแบบทั่วไปด้วยทฤษฎีของรหัสช่องสัญญาณ (Channel Coding Theorem) [8] ดังตัวอย่างงานวิจัยที่ได้มีการนำเสนอใน [9]–[12] วิธีการเหล่านี้ใช้หลักการเลือกอัตราการเข้ารหัส (Coding Rate) ที่เหมาะสมกับ QBER (Rate-compatible Reconciliation) ซึ่งจำเป็นต้องอาศัยการประมาณค่า QBER โดยเกณฑ์วิธีแบบดั้งเดิม จากการสุ่มเปิดเผยบิตข้อมูลกุญแจซิฟท์บางส่วน และตัดทิ้งก่อนเข้าสู่กระบวนการไกล่เกลี่ยความผิดพลาดส่งผลต่อขนาดกุญแจรหัสลับที่ลดลง

จากปัญหาของวิธีการต่าง ๆ ที่ได้กล่าวมาข้างต้นจึงนำมาเป็นความมุ่งหมายหลักของการเพิ่มประสิทธิภาพการประมาณค่า QBER และการไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับ โดยบทความนี้ได้นำเสนอและวิเคราะห์ผลการประมาณค่า QBER ด้วยหลักภาวะน่าจะเป็นสูงสุด (Maximum-likelihood Estimation: MLE) บนชุดข้อมูลซินโดรม (Syndrome Information) ที่มีการแลกเปลี่ยนในระหว่างขั้นตอนการไกล่เกลี่ยความผิดพลาด แทนการเปิดเผยและสูญเสียบิตข้อมูลบางส่วนไปในเกณฑ์วิธีแบบดั้งเดิม (Traditional Key Sampling) นำสู่การออกแบบและพัฒนาเป็นวิธีการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสเหมาะสม (Rate-adaptive Reconciliation) สำหรับระบบ QKD ด้วยเทคนิคของรหัสช่องสัญญาณ (Channel Coding) ที่นำมาประยุกต์ใช้คือ รหัสตรวจสอบพาริตี้แบบความหนาแน่นต่ำหรือแอลดีพีซี (Low-Density Parity-Check Code: LDPC) [13] บนโครงสร้างการเข้ารหัสข้อมูลข่าวสารข้างเคียง (Side-information Source Coding)

โดยบทความนี้มีวัตถุประสงค์ในการเพิ่มประสิทธิภาพการประมาณค่าอัตราความผิดพลาดบนช่องสัญญาณเชิงควอนตัม และการไกล่เกลี่ยความผิดพลาดของระบบ QKD ตอบโจทย์ด้านขีดจำกัดของอัตราการกำเนิดกุญแจรหัสลับ (Secret Key Throughput) ให้มีความเร็วสูง



รูปที่ 1 การไกล่เกลี่ยความผิดพลาดบนพื้นฐานของรหัสซลีเพียน-วูล์ฟ

2. ทฤษฎีที่เกี่ยวข้องและการพิสูจน์

เนื้อหาในส่วนนี้ กล่าวถึงหลักการและทฤษฎีที่เกี่ยวข้องตลอดจนการพิสูจน์แนวความคิดการประยุกต์รหัสช่องสัญญาณ สำหรับการไกล่เกลี่ยความผิดพลาดในระบบ QKD

2.1 รหัสซลีเพียน-วูล์ฟ (Slepian-Wolf Coding) และการประยุกต์สำหรับการไกล่เกลี่ยความผิดพลาด

ปัญหาของรหัสซลีเพียน-วูล์ฟเกี่ยวข้องกับการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสาร (Source Coding with Side Information) ตั้งแต่สองแหล่งกำเนิดขึ้นไป [14] ซึ่งนำมาประยุกต์เพื่อแก้ไขปัญหาการไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัมด้วยรหัสช่องสัญญาณดังแผนผังการทำงานในรูปที่ 1 โดยข้อมูลกุญแจของ *Alice* และ *Bob* เขียนแทนด้วยตัวแปรสุ่ม X และ Y ตามลำดับ มีความผิดพลาดเกิดขึ้นภายใต้ ความน่าจะเป็น P_{XY} แสดงเป็นขั้นตอนการทำงานได้ดังนี้

1) การเข้ารหัส *Alice* เข้ารหัสข้อมูล X และส่งผลลัพธ์ $|M|$ ไปยัง *Bob* ผ่านช่องสัญญาณการสื่อสารทั่วไปที่สอดคล้องกับอัตราการบีบอัดข้อมูล (Compression Rate: R_S) ภายใต้เงื่อนไข $R_S \geq H(X|Y)$

2) การถอดรหัส *Bob* ต้องการแก้ไขความผิดพลาดบนข้อมูล Y ให้มีค่าเท่ากับ X โดยการนำข้อมูล Y และ $|M|$ เข้าสู่การถอดรหัสได้ผลลัพธ์ X'

เป้าหมายของการไกล่เกลี่ยความผิดพลาดบนพื้นฐานของรหัสซลีเพียน-วูล์ฟนี้คือ การแปลงข้อมูล X กับ Y ให้มีความสัมพันธ์อย่างสมบูรณ์ โดยที่ความน่าจะเป็น

ของ X เท่ากับ X' มีค่าเท่ากับ 1 ($Prob[X = X'] = 1$) เมื่อพิจารณาถึงข้อมูล $|M|$ ที่ส่งผ่านช่องสัญญาณการสื่อสารทั่วไปในระหว่างการไกลเกลี่ยความผิดพลาด มีโอกาสรั่วไหลไปถึง *Eve* ได้เสมอ ($|M| = Leak_{Recon}$) ดังนั้นประสิทธิภาพของการไกล่เกลี่ยความผิดพลาดต้องขึ้นกับจำนวนบิตข้อมูล $|M|$ สอดคล้องกับปริมาณอัตราการบีบอัด R_S

การนำรหัสช่องสัญญาณมาประยุกต์ใช้งานบนพื้นฐานของระบบซลีเพียน-วูล์ฟ เมื่อให้ X และ Y เปรียบเสมือนกับอินพุตและเอาต์พุตบน GF(2) ที่ได้จากการจำลองการสื่อสารบนช่องสัญญาณสมมาตรแบบไบนารี (Binary Symmetric Channel: BSC) และ C แทนรหัสแบบบล็อกเชิงเส้น ซึ่งมีเมทริกซ์ตรวจสอบพาริตี้ (Parity-Check Matrix) $\mathbf{H}$ ขนาด $M \times N$ ในระบบของซลีเพียน-วูล์ฟ ค่าซินโดรมสามารถคำนวณได้จากการบีบอัดข้อมูลอินพุต X ($S^M = X^N \cdot \mathbf{H}^T$) โดยที่อัตราการบีบอัด R_S คืออัตราส่วนของขนาดข้อมูลซินโดรมกับขนาดของคำรหัส $R_S = M/N$ สอดคล้องกับอัตราการเข้ารหัสช่องสัญญาณใดๆ $R_C = (N - M)/N$ ดังนั้นความสัมพันธ์ระหว่างอัตราการบีบอัดของรหัสซลีเพียน-วูล์ฟ R_S กับอัตราการเข้ารหัสช่องสัญญาณ R_C แสดงได้ดังสมการที่ (1)

$$R_S = 1 - R_C \tag{1}$$

อย่างไรก็ตาม เมื่อนำรหัสช่องสัญญาณมาประยุกต์ใช้เพื่อแก้ไขปัญหาการไกล่เกลี่ยความผิดพลาด อัตราการเข้ารหัสช่องสัญญาณ R_C จำเป็นต้องทำให้มีค่าเหมาะสมที่สุดภายใต้ขอบเขตของรหัสซลีเพียน-วูล์ฟ R_S ดังอสมการที่ (2)

$$\begin{aligned} 1 - R_C &\geq H(X|Y) \\ &\geq H(e) \end{aligned} \tag{2}$$

โดยที่ e คือความน่าจะเป็นแบบมีเงื่อนไขร่วมกันระหว่างข้อมูลกุญแจ X กับ Y ซึ่ง e ในระบบ QKD คืออัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัม (QBER) ที่แสดงถึงความน่าจะเป็นของข้อมูลกุญแจร่วมระหว่าง *Alice Bob* และ *Eve* โดยเอนโทรปี (Entropy) ของ e สามารถคำนวณได้ดังสมการที่ (3)

$$H(e) = -e\log_2 e - (1 - e)\log_2(1-e) \tag{3}$$

2.2 ขอบเขตของความปลอดภัยอัตราการกำเนิดกุญแจรหัสลับเชิงควอนตัม (Bound of Secure Secret Key Rate)

เนื้อหาในส่วนนี้กล่าวถึงขอบเขตความปลอดภัยของกุญแจรหัสลับสุดท้ายที่ได้จากการประมวลผลการกำเนิดกุญแจรหัสลับส่วนหลัง (QKD Post-Processing) ที่ *Eve* มีโอกาสได้รับข้อมูลอันมีความเกี่ยวพันกับกุญแจของ *Alice* บนช่องสัญญาณเชิงควอนตัม และในระหว่างกระบวนการไกล่เกลี่ยความผิดพลาด ($Leak_{Recon}$) โดยขอบเขตเชิงทฤษฎีของความปลอดภัยอัตราการกำเนิดกุญแจรหัสลับ (r) [15] คำนวณได้ดังสมการที่ (4)

$$r = 1 - H(e) - Leak_{Recon} \tag{4}$$

3. การประมาณค่า QBER สำหรับการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราการเข้ารหัสเหมาะสม

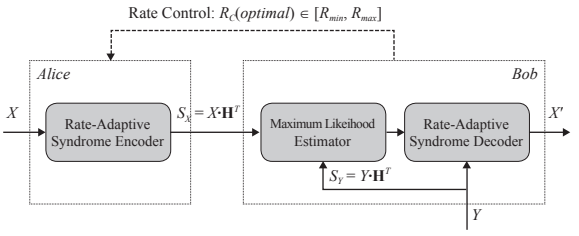
เนื้อหาในส่วนนี้นำเสนอการออกแบบและพัฒนาเทคนิคการประมาณค่าอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัม (QBER) ในระหว่างกระบวนการไกล่เกลี่ยความผิดพลาด เพื่อปรับอัตราการเข้ารหัสให้เหมาะสมกับค่า QBER ที่เป็นไปได้ในระบบ QKD แทนการประมาณค่าความผิดพลาดแบบทั่วไป ที่ทำการสุ่มเปิดเผยและเปรียบเทียบบิตข้อมูลกุญแจบางส่วน เป็นผลให้ต้องสูญเสียบิตข้อมูลในส่วนดังกล่าวทิ้งไป โดยวิธีการประมาณค่า QBER ที่นำเสนอในบทความนี้ มีพื้นฐานการประมาณโดยภาวะน่าจะเป็นสูงสุด กับชุดข้อมูลซินโดรมที่มีการการสื่อสารจาก *Alice* ไปยัง *Bob* ในระหว่างขั้นตอนการไกล่เกลี่ยความผิดพลาด นำไปสู่การใช้ประโยชน์จาก

ข้อมูล QBER ในการหาค่าอัตราเข้ารหัสที่เหมาะสม เพื่อเป้าหมายของการเพิ่มประสิทธิภาพด้านความปลอดภัยและอัตราการกำเนิดกุญแจรหัสลับสุดท้ายที่สูงขึ้น

ในส่วนของวิธีการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราการเข้ารหัสเหมาะสมได้มีการนำเสนอขึ้นด้วยรหัสแอลดีพีซีแบบไม่สม่ำเสมอ (Irregular LDPC Codes) ใช้เทคนิคการสุ่มบิตแบบพันช์เชอร์ (Puncture: p) และชอร์ตเทน (Shorten: s) [16]–[18] เพื่อการปรับเพิ่มหรือลดอัตราการเข้ารหัสให้สอดคล้องกับ QBER ที่เกิดขึ้นบนพื้นฐานของรหัสซลีเพียน-วูล์ฟด้วยการเข้า-/ถอดรหัสซินโดรม (Syndrome En-/Decoding) เพื่อบ่งบอกตำแหน่งและแก้ไขบิตข้อมูลกุญแจที่ผิดพลาดระหว่างคู่สื่อสาร *Alice* กับ *Bob* ให้มีค่าตรงกัน เมื่อกำหนดให้ $\mathbf{H}$ คือเมทริกซ์ตรวจสอบความผิดพลาดของรหัสแอลดีพีซี (Low-Density Parity-Check Matrix) และอัตราการเข้ารหัส $R_C = (k - s) / (n - p - s)$ โดยที่ n คือขนาดบล็อกข้อมูล (Block Length) k คือจำนวนบิตข่าวสาร (Information Bits) p คือจำนวนบิตแบบพันช์เชอร์ และ s คือจำนวนบิตแบบชอร์ต เพื่อปรับเพิ่มหรือลดอัตราเข้ารหัส R_C ตามสัดส่วน $d = p + s$ ซึ่งวิธีการที่นำเสนอแสดงแผนผังการทำงานของระบบได้ดังรูปที่ 2 ประกอบด้วยขั้นตอนต่อไปนี้

1) การเข้ารหัสซินโดรม (Syndrome Encoding) *Alice* เข้ารหัสชุดข้อมูลกุญแจ X เพื่อคำนวณหาค่าซินโดรม $S_X = X \cdot \mathbf{H}^T$ บนพื้นฐานของระบบซลีเพียน-วูล์ฟด้วยอัตราการเข้ารหัสสูงสุด (R_{max}; $p = d$, $s = 0$) และส่งไปยัง *Bob* ผ่านช่องสัญญาณการสื่อสารทั่วไป

2) การประมาณค่า QBER (QBER Estimation) *Bob* นำชุดข้อมูลกุญแจ Y มาคำนวณหาค่าซินโดรม $S_Y = Y \cdot \mathbf{H}^T$ ด้วยอัตราการเข้ารหัสสูงสุด (R_{max}) เช่นเดียวกับ *Alice* และนำ S_Y มาเปรียบเทียบกับ S_X หากเมื่อใดที่ผลการเปรียบเทียบข้อมูลซินโดรมทั้งสองมีความแตกต่างกัน $S_{diff} \neq \{0\}$ ($S_{diff} = S_X \oplus S_Y$; $S_X \neq S_Y$ โดยที่ $\oplus$ แทนตัวดำเนินการ Exclusive Or: XOR) แสดงว่าชุดข้อมูลกุญแจของคู่สื่อสารมีความผิดพลาด และเข้าสู่การประมาณค่า QBER



รูปที่ 2 การไกล่เกลี่ยความผิดพลาดแบบปรับอัตราการเข้ารหัสเหมาะสมกับการประมาณค่า QBER

ต่อไป เริ่มต้นจากการหาค่าจำนวนบิตที่แตกต่างบน S_{diff} ดังสมการที่ (5)

$$q(S_{diff}) = \frac{1}{n-k}\sum_{m=1}^{n-k} S_{diff} \tag{5}$$

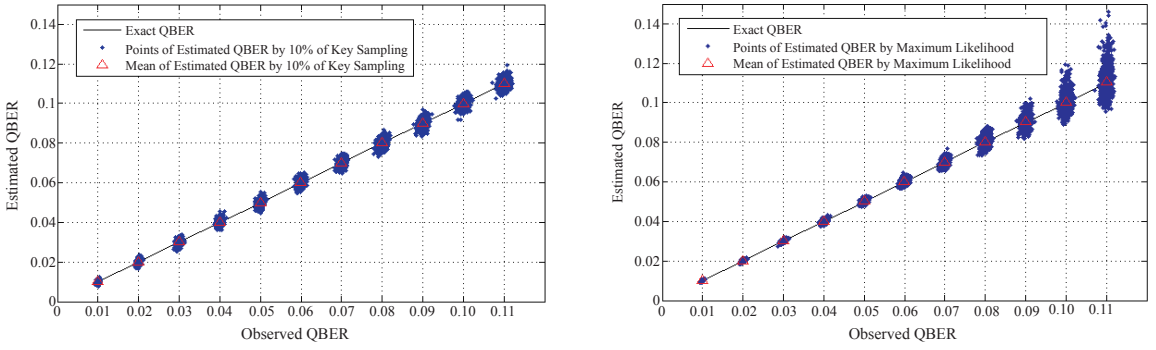
ในการประมาณค่า QBER โดยภาวะน่าจะเป็นสูงสุดสามารถคำนวณได้จากพื้นฐานผลของการแจกแจงทวินาม (Binomial Distribution) [19] ดังสมการที่ (6)

$$q(e) = \sum_{i=1;i\ odd}^{d_c} \binom{d_c}{i} e^i (1-e)^{d_c - i} \tag{6}$$

โดยที่ $q(e)$ แทนฟังก์ชันการแจกแจงทวินามของค่า QBER หรือ e และ d_c คือจำนวนบิตหนึ่งในแถวของเมทริกซ์ $\mathbf{H}$ หรือ Check Node Degree ซึ่งการประมาณค่า e จากข้อมูล S_{diff} แสดงในรูปอินเวอร์สฟังก์ชัน ดังสมการที่ (7)

$$e(S_{diff}) = f^{-1}(q(S_{diff})) = \frac{(1-2q(S_{diff}))^{\frac{1}{d_c}} - 1}{2} \tag{7}$$

3) การปรับค่าอัตราเข้ารหัสเหมาะสม (Rate-adaptive Optimization) ผลของการประมาณค่า QBER จากขั้นตอน 2 จะถูกนำมาใช้เพื่อการคำนวณอัตราเข้ารหัสที่เหมาะสม $R_C(optimal)$ ด้วยอัลกอริธึมเดนซิตี้อีโวลูชัน (Density Evolution) [20] เพื่อสุ่มตำแหน่งพันช์เชอร์จำนวน p บิต และชอร์ตเทนจำนวน s บิต กับชุดข้อมูลกุญแจและเมทริกซ์ $\mathbf{H}$ ให้มีจำนวนสอดคล้องกับ $R_C(optimal)$



(ก) (ข)

รูปที่ 3 ผลการประมาณค่า QBER (Estimated QBER) เทียบกับค่า QBER ที่เกิดขึ้นจริง (Observed QBER) (ก) วิธีสุ่มเปิดเผยบิตข้อมูลกุญแจ 10% ของจำนวนทั้งหมด (10% of Key Sampling) (ข) วิธีประมาณค่าด้วยภาวะน่าจะเป็นสูงสุด (Maximum-Likelihood Estimation: MLE)

ที่มีค่าเข้าใกล้ขอบเขตของ รหัสซลีเพียน-วูล์ฟในอสมการที่ (2) หลังจากนั้น *Alice* ดำเนินการคำนวณ S_X ตามอัตรา $R_C(optimal)$ และส่งไปยัง *Bob* เพื่อทำการถอดรหัสต่อไป

4) การถอดรหัสซินโดรมและยืนยันผล (Syndrome Decoding and Confirmation) *Bob* นำข้อมูล Y เข้าสู่กระบวนการถอดรหัสซินโดรมด้วยอัลกอริธึม Sum-Product บนพื้นฐานของการสืบทอดความเชื่อ (Belief Propagation) เพื่อบ่งบอกตำแหน่งและแก้ไขบิตผิดพลาดบน Y จนกระทั่งสิ้นสุดกระบวนการเมื่อบิตข้อมูลกุญแจที่แก้ไขแล้ว X' มีค่าซินโดรมตรงตามที่ได้รับจาก *Alice* ($S_{X'} = S_X$) ซึ่งเป็นการยืนยันความถูกต้องตรงกันของชุดกุญแจ (Reconciled Key) ระหว่างคู่สื่อสารที่ได้หลังจากการแก้ไขความผิดพลาดแล้ว ($X' = X$) หากการถอดรหัสล้มเหลวจะกลับสู่การประมาณค่า QBER ในขั้นตอนที่ 2 อีกครั้ง กับชุดข้อมูลซินโดรมระหว่างคู่สื่อสารที่ได้จากอัตราเข้ารหัส $R_C(optimal)$

4. ผลการทดสอบ

วิธีการที่นำเสนอได้ถูกออกแบบและพัฒนาเพื่อจำลองผลประสิทธิภาพการประมาณค่า QBER ด้วยภาวะน่าจะเป็นสูงสุดจากข้อมูลซินโดรม และนำมาประยุกต์เป็นส่วนหนึ่งของวิธีการไกล่เกลี่ยความผิดพลาดแบบปรับค่าอัตราการเข้ารหัสให้เหมาะสมกับค่า QBER ที่ประมาณได้เพื่อเปรียบเทียบผลของอัตราการกำเนิดกุญแจรหัสลับร่วมกับโพรโทคอลต่าง ๆ ที่ใช้งานจริง

การจำลองการทดสอบในที่นี้ ข้อมูลกุญแจของ *Alice* กับ *Bob* ถูกสร้างขึ้นในรูปแบบไบนารีขนาด 200,000 บิต สุ่มจากพื้นฐานทางคณิตศาสตร์โดยคอมพิวเตอร์ (Pseudo-Random Number Generator) ให้มีเงื่อนไขความผิดพลาดครอบคลุมค่า QBER ที่เป็นไปได้จริงในระบบ QKD (QBER ตั้งแต่ 1% ถึง 11%) โดยวิเคราะห์ผลจากการทดลองซ้ำ 1,000 ครั้ง แล้วหาค่าเฉลี่ย

รูปที่ 3 แสดงผลการประมาณค่า QBER เทียบกับค่า QBER ที่เกิดขึ้นจริง ตั้งแต่ 1% ถึง 11% บนชุดข้อมูลเดียวกัน ประกอบด้วยวิธีการดั้งเดิมในรูปที่ 3(ก) จากการสุ่มเปิดเผยและเปรียบเทียบค่าบิตข้อมูลกุญแจ 10% ของจำนวนทั้งหมด และวิธีการที่นำเสนอในรูปที่ 3(ข) จากการประมาณค่าด้วยภาวะน่าจะเป็นสูงสุด (MLE) ดังสมการที่ (7) กับชุดข้อมูลซินโดรมที่อัตราการเข้ารหัสสูงสุด ($R_{max} = 0.78$; $p = d = 2 \times 10^4$, $s = 0$) ของรหัสแอลดีพีซีขนาดบล็อคข้อมูลเท่ากับ 2×10^5 บิต โดยมีค่าการกระจายดีกรีบนเมทริกซ์ $\mathbf{H}$ ของโนดตัวแปร $\lambda(x) = 0.1488x^2 + 0.1908x^3 + 0.2664x^6 + 0.0537x^7 + 0.1614x^{18} + 0.1390x^{19} + 0.0399x^{20}$ และโนดตรวจสอบ (Check Nodes) $\rho(x) = 0.000734x^{15} + 0.9986x^{16} + 0.000708x^{17}$ ตามลำดับ

ตารางที่ 1 ผลการวิเคราะห์ประสิทธิภาพการประมาณค่า QBER ด้วยวิธี Key Sampling [รูปที่ 3(ก)] และวิธี Maximum-Likelihood: MLE [รูปที่ 3(ข)]

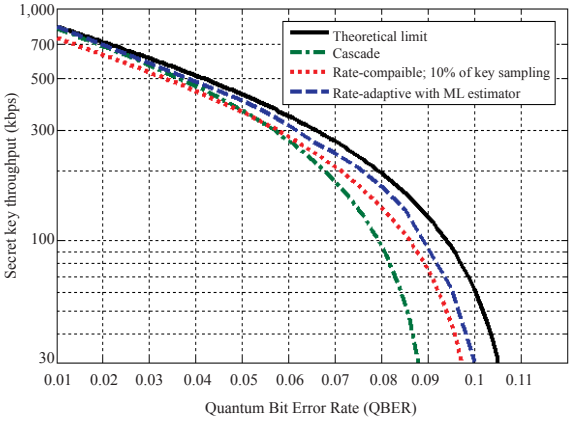
Observed QBER	Estimated QBER by 10% of Key Sampling			Estimated QBER by Maximum-Likelihood (MLE)		
	Mean $\overline{X}$	Standard Deviation (S.D.)	ความแม่นยำเฉลี่ยจากจำนวนครั้งที่ทดลองทั้งหมด (%)	Mean $\overline{X}$	Standard Deviation (S.D.)	ความแม่นยำเฉลี่ยจากจำนวนครั้งที่ทดลองทั้งหมด (%)
0.01	0.0100	0.00069	94.89	0.0100	0.00032	98.11
0.02	0.0200	0.00100	96.33	0.0200	0.00050	98.55
0.03	0.0300	0.00122	96.91	0.0300	0.00062	98.66
0.04	0.0401	0.00144	97.29	0.0400	0.00080	98.70
0.05	0.0500	0.00155	97.68	0.0500	0.00101	98.57
0.06	0.0599	0.00167	97.90	0.0599	0.00128	98.47
0.07	0.0701	0.00175	98.06	0.0701	0.00163	98.21
0.08	0.0800	0.00203	98.15	0.0801	0.00240	97.69
0.09	0.0900	0.00201	98.34	0.0903	0.00331	97.18
0.10	0.1000	0.00209	98.42	0.1003	0.00457	96.45
0.11	0.1099	0.00217	98.48	0.1107	0.00696	95.25
	ค่าเฉลี่ยของความแม่นยำ		97.50	ค่าเฉลี่ยของความแม่นยำ		97.80

จากผลการทดลองในรูปที่ 3 สามารถวิเคราะห์และคำนวณผลแสดงได้ดังตารางที่ 1 ซึ่งพบว่าวิธีการที่นำเสนอ MLE ให้ผลการประมาณค่า QBER ใกล้เคียงกับที่เกิดขึ้นจริงมีผลของค่าความแม่นยำเฉลี่ยสูงกว่าวิธีการ Key Sampling บนช่วง Observed QBER ตั้งแต่ 1% ถึง 7% สอดคล้องกับการกระจายของข้อมูลเมื่อพิจารณาจากค่าเบี่ยงเบนมาตรฐาน (Standard Deviation: S.D.) ในระดับที่น้อยกว่าวิธีการ Key Sampling ภายใต้ช่วง Observed QBER ตั้งแต่ 1% ถึง 7% ด้วยเช่นกัน หากพิจารณาถึงค่าเฉลี่ยของความแม่นยำครอบคลุมช่วง Observed QBER ที่เป็นไปได้ตั้งแต่ 1% ถึง 11% พบว่าวิธีการ MLE ให้ค่าเฉลี่ยที่ 97.80% ซึ่งสูงกว่าวิธีการ Key Sampling ที่ 97.50% จากจำนวนครั้งในการทดลองทั้งหมด อีกทั้งยังสามารถลดการสูญเสียบิตข้อมูลกุญแจบางส่วนจำนวน 10% ที่ต้องถูกตัดทิ้งไปในการประมาณ QBER แบบดั้งเดิมด้วย Key Sampling จึงเหมาะสมสำหรับการนำไปประยุกต์ใช้งานจริงในระบบ QKD

อย่างไรก็ตาม เมื่อ Observed QBER มีค่าสูงขึ้น จะส่งผลให้ค่าความแม่นยำของวิธีการ MLE นั้นลดลง อันเนื่องมาจากข้อมูลซินโดรมที่อัตราการเข้ารหัส $R_C = 0.78$ ให้จำนวนบิตไม่เพียงพอบนความสัมพันธ์ที่เกิดขึ้นกับเมทริกซ์ **H** สำหรับการประมาณจากภาวะน่าจะเป็นสูงสุด ซึ่งสามารถแก้ไขได้โดยการปรับลดอัตราการเข้ารหัสให้ข้อมูลซินโดรมมีจำนวนมากขึ้น หรือการเลือกใช้เมทริกซ์ **H** ขนาดบล็อกที่ใหญ่ขึ้นในการประมวลผล แต่อาจส่งผลกระทบต่อประสิทธิภาพในการไกล่เกลี่ยความผิดพลาดและความซับซ้อนในคำนวณด้วยเช่นกัน

ในส่วนของผลการจำลองประสิทธิภาพอัตราการกำเนิดกุญแจรหัสลับ แสดงได้ดังรูปที่ 4 เมื่อกำหนดให้อัตราการกำเนิดกุญแจรหัสลับในอุดมคติ กรณีไม่มีความผิดพลาดเกิดขึ้น (QBER = 0, $r_{ideal} = 1$) มีความถี่สัญญาณนาฬิกาที่ 1 MHz ดังนั้นอัตราการกำเนิดกุญแจรหัสลับที่เกิดขึ้นจริงจึงมีค่าเท่ากับ ความปลอดภัยของอัตราการกำเนิดกุญแจรหัสลับ (r) ในสมการที่ (4) คูณกับ Clock Rate (Secret Key Throughput = $r \times$ Clock Rate)

โดยผลการจำลองประสิทธิภาพบนเงื่อนไขการทดสอบเดียวกันจะเห็นได้ว่า วิธีการที่นำเสนอ MLE เมื่อมาพัฒนาร่วมกับโพรโทคอล Rate-Adaptive Reconciliation (เส้นประสีน้ำเงิน) ให้ผลของอัตราการกำเนิดกุญแจรหัสลับสูงเข้าใกล้ขีดจำกัดเชิงทฤษฎี (Theoretical Limit) (เส้นทึบสีดำ) มากกว่าโพรโทคอล Cascade (เส้นประสีเขียว) และ Rate-Compatible (เส้นประสีแดง) ที่อาศัยการประมาณค่า QBER ตามเกณฑ์วิธี Key Sampling จำนวน 10% ของ



รูปที่ 4 ประสิทธิภาพอัตราการกำเนิดกุญแจรหัสลับ (Secret Key Throughput) บนเงื่อนไขของ QBER

ขนาดกุญแจซิฟท์ทั้งหมด อีกทั้งยังสามารถขยายขีดจำกัดในการกำเนิดกุญแจรหัสลับที่อัตราความผิดพลาดสูงสุดประมาณ 10% เมื่อเปรียบเทียบกับโพรโทคอลอื่นๆ จากการสำรวจ ได้แก่ Cascade ที่ QBER 8.80% และ Rate-Compatible ที่ QBER 9.75% ตามลำดับ

5. สรุป

วิธีการประมาณค่าอัตราความผิดพลาดบนช่องสัญญาณเชิงควอนตัมจากพื้นฐานภาวะน่าจะเป็นสูงสุดถูกนำเสนอสำหรับการไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสเหมาะสมกับการกระจายกุญแจรหัสลับเชิงควอนตัม แทนการเปิดเผยบิตข้อมูลกุญแจบางส่วนที่ต้องสูญเสียไปในเกณฑ์วิธีการประมาณแบบดั้งเดิม เป็นผลให้กุญแจรหัสลับสุดท้ายที่ได้มีขนาดสูงขึ้น จากผลการทดสอบแสดงให้เห็นว่า วิธีการที่นำเสนอให้ผลการประมาณค่าอัตราความผิดพลาดใกล้เคียงกับที่เกิดขึ้นจริงในระบบ มีผลของค่าความแม่นยำเฉลี่ยที่สูงกว่าวิธีการสุ่มเปิดเผยบิตข้อมูลกุญแจบางส่วนบนช่วงการประมาณค่าอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัมตั้งแต่ 1% ถึง 7% รวมถึงมีการกระจายของข้อมูลอยู่ในระดับที่น้อยกว่าภายใต้ช่วงดังกล่าวเช่นกัน

นอกจากนี้ เมื่อนำมาพัฒนาร่วมกับโพรโทคอลไกล่เกลี่ยความผิดพลาดแบบปรับอัตราเข้ารหัสเหมาะสมด้วยรหัสช่องสัญญาณแอลดีพีซีบนโครงสร้างการเข้ารหัสข้อมูลข่าวสารข้างเคียง สามารถเพิ่มขีดจำกัดของอัตราการกำเนิดกุญแจรหัสลับได้สูงขึ้น จึงเหมาะสำหรับการเป็นโพรโทคอลทางเลือกหนึ่งสนับสนุนการประยุกต์ใช้งานจริงในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมที่ต้องการความเร็วสูง

6. กิตติกรรมประกาศ

งานวิจัยนี้ได้รับสนับสนุนทุนวิจัยจากกองทุนวิจัย สำนักวิจัยและพัฒนา มหาวิทยาลัยราชภัฏพระนคร เลขที่สัญญาโครงการ 26.01/2558

เอกสารอ้างอิง

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE International Conference on Computers*, *Systems and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[2] ID Quantique SA. (2015, October 8). *CERBERIS Quantum Key Distribution (QKD) Server* [Online]. Available: http://www.idquantique.com/

[3] Anhui Qasky Quantum Science and Technology Co. Ltd. (2015, October 10). [Online]. Available: http://www.qasky.com/

[4] SeQureNet SARL. (2015, October 10). *Cygnus: State-of-the-art CVQKD module* [Online]. Available: http://www.sequrenet.com/

[5] R. Renner and S. Wolf, “Simple and tight bounds for information reconciliation and privacy amplification,” in *ASIACRYPT 2005*, Chennai, India, vol. 3788, pp. 199–216, 2005.

[6] C. H. Bennett, G. Brassard, and J. M. Robert. “Privacy amplification by public discussion,” *SIAM Journal on Computing*, vol. 17, no. 2,

pp. 210–229, 1988.

[7] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proceedings Advance in Cryptology EUROCRYPT'93*, vol. 765, pp. 410–423, 1994.

[8] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, October 1948.

[9] D. Elkouss, A. L*eve*rrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proceedings 2009 IEEE International Symposium on Information Theory*, pp. 1879–1883, July 2009.

[10] K. Kasai, T. Tsujimoto, R. Matsumoto, and K. Sakaniwa, "Information reconciliation for QKD with rate-compatible non-binary LDPC codes," in *Proceedings 2010 International Symposium on Information Theory and Its Applications*, pp. 922–927, October 2010.

[11] P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, and O. Sangaroon, "BCH-Based Slepian-Wolf coding with feedback syndrome decoding for quantum key reconciliation," in *Proceedings 2012 International Conference on Electrical Engineering/Electronics*, *Computer*, *Telecommunications and Information Technology*, Thailand, May 2012.

[12] N. Benletaief, H. Rezig, and A. Bouallegue, "Toward efficient quantum key distribution reconciliation," *Journal of Quantum Information Science*, vol. 4, no. 2, pp. 117–128, 2014.

[13] R. Gallager, "Low-density parity-check codes," PhD thesis, Massachusetts Institute of Technology, 1963.

[14] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[15] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[16] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Blind reconciliation," *Quantum Information and Computation*, vol. 12, pp. 791–812, 2012.

[17] P. Treeviriyanupab, T. Phromsa-ard, C.-M. Zhang, M. Li, P. Sangwongngam, T. Sanevong Na Ayutaya, N. Songneam, R. Rattanatamma, C. Ingkavet, W. Sanor, W. Chen, Z.-F. Han, and K. Sripimanwat, "Rate-adaptive reconciliation and its estimator for quantum bit error rate," in *Proceedings 14th International Symposium on Communications and Information Technologies*, Incheon, Korea, 2014, pp. 351–355.

[18] P. Treeviriyanupab, T. Phromsa-ard, J. Wetcharungsri, P. Sangwongngam, C.-M. Zhang, M. Li, W. Chen, and Z.-F. Han, "Efficient rate-adaptive reconciliation in quantum key distribution," in *5th International Conference on Quantum Cryptography*, Tokyo, Japan, 2015.

[19] V. Toto-Zarasoa, A. Roumy, and C. Guillemot, "Maximum likelihood BSC parameter estimation for the Slepian-Wolf problem," *IEEE Communications Letters*, pp. 232–234, vol. 15, 2011.

[20] T. Tian and C. R. Jones, "Construction of rate-compatible LDPC codes utilizing information shortening and parity puncturing," *EURASIP Journal on Wireless Communications and Networking*, pp. 789–795, vol. 5, 2005.