โพรโทคอลไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับด้วยรหัสพาริตีเช็กความหนาแน่นต่ำสำหรับระบบกระจายกุญแจรหัสลับเชิงควอนตัม

นายธราธร พรมสะอาด

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

KEY RECONCILIATION PROTOCOL WITH LOW-DENSITY PARITY-CHECK CODES FOR QUANTUM KEY DISTRIBUTION

Mr. Tharathorn Phromsa-ard

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Electrical Engineering
Department of Electrical Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2015

หัวข้อวิทยานิพนธ์	โพรโทคอลไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับด้วยรหัสพาริตีเช็กความหนาแน่นต่ำสำหรับระบบกระจายกุญแจรหัสลับเชิงควอนตัม
โดย	นายธราธร พรมสะอาด
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.ลัญฉกร วุฒิสิทธิกุลกิจ
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ดร.กมล เขมะรังษี
	ดร.พิสิฐ วนิชชานันท์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.พสุ แก้วปลั่ง)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.ลัญฉกร วุฒิสิทธิกุลกิจ)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม
(ดร.กมล เขมะรังษี)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม
(ดร.พิสิฐ วนิชชานันท์)

.....กรรมการ
(ผู้ช่วยศาสตราจารย์ สุวิทย์ นาคพีระยุทธ)

.....กรรมการภายนอกมหาวิทยาลัย
(ดร.กำพล วรดิษฐ์)

ธราธร พรมสะอาด : โพรโทคอลไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับด้วยรหัสพาริตีเช็กความหนาแน่นต่ำสำหรับระบบกระจายกุญแจรหัสลับเชิงควอนตัม (KEY RECONCILIATION PROTOCOL WITH LOW-DENSITY PARITY-CHECK CODES FOR QUANTUM KEY DISTRIBUTION) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร.ลัญฉกร วุฒิสิทธิกุลกิจ, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม: ดร.กมล เขมะรังษี, ดร.พิสิฐ วนิชชานันท์, 74 หน้า.

วิทยานิพนธ์นี้นำเสนอวิธีการไกล่เกลี่ยความผิดพลาดซึ่งเป็นหนึ่งในขั้นตอนสำคัญของการกระจายกุญแจรหัสลับเชิงควอนตัมมีจุดประสงค์เพื่อการยืนยันความถูกต้องของข้อมูลกุญแจระหว่างผู้ส่งกับผู้รับตัวจริงให้มีค่าที่ตรงกันสำหรับการนำไปใช้งานในระบบวิทยาการรหัสลับอย่างมีประสิทธิภาพ โดยการออกแบบและพัฒนาวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสพาริตีเช็กความหนาแน่นต่ำหรือรหัสแอลดีพีซีประยุกต์ทำงานร่วมกับการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารข้างเคียง ซึ่งแบ่งวิธีการที่นำเสนอเป็นสามวิธี วิธีการแรกคือ การพัฒนาวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีแบบอัตรารหัสคงที่ด้วยการถอดรหัสแบบบิตฟลิปปิงและซัมโปรดักซินโดรม ซึ่งผลการทดสอบให้ความสามารถในการแก้ไขความผิดพลาดข้อมูลกุญแจรหัสลับที่สูงกว่าโพรโทคอลวินนาวที่มีพื้นฐานมาจากรหัสแฮมมิงและศึกษาวิธีการถอดรหัสและขนาดความยาวรหัสมีผลต่อประสิทธิภาพการไกล่เกลี่ย วิธีการที่สองคือ การพัฒนาวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีแบบปรับอัตรารหัสได้ด้วยผลรวมสะสมของซินโดรม โดยการแบ่งเก็บและส่งเพิ่มข้อมูลซินโดรมบางส่วนให้ภาคถอดรหัสที่เหมาะสมกับอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัม และวิธีการสุดท้ายคือ การพัฒนาวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีที่สามารถปรับค่าอัตรารหัสได้ด้วยวิธีพังเจอร์และชอร์ตเทนให้สอดคล้องกับเงื่อนไขความผิดพลาดกุญแจรหัสลับเชิงควอนตัมที่เกิดขึ้นจากการประเมินอัตราความผิดพลาดของช่องสัญญาณด้วยข้อมูลซินโดรมและประเมินค่าขอบเขตประสิทธิภาพการไกล่เกลี่ยล่วงหน้าเพื่อกำหนดอัตรารหัสที่เหมาะสมสำหรับการไกล่เกลี่ยความผิดพลาด โดยจากวิเคราะห์และเปรียบเทียบผลการทดสอบพบว่า การไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีเหล่านี้ ให้ผลของค่าประสิทธิภาพการไกล่เกลี่ย จำนวนบิตเปิดเผย และการลดทรัพยากรการติดต่อสื่อสารในระหว่างกระบวนการได้ดีกว่าโพรโทคอลดั้งเดิมที่นิยมใช้งาน เช่น โพรโทคอลคาสเคดและวินนาว ดังนั้นจึงเป็นวิธีการทางเลือกหนึ่งซึ่งจะนำไปสู่เป้าหมายของการเพิ่มขีดกำจัดด้านอัตราการกำเนิดกุญแจรหัสลับ สนับสนุนการประยุกต์ใช้งานจริงบนระบบการกระจายกุญแจรหัสลับเชิงควอนตัมประสิทธิภาพสูง

ภาควิชา วิศวกรรมไฟฟ้า	ลายมือชื่อนิสิต .....
สาขาวิชา วิศวกรรมไฟฟ้า	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....
ปีการศึกษา 2558	ลายมือชื่อ อ.ที่ปรึกษาร่วม .....
	ลายมือชื่อ อ.ที่ปรึกษาร่วม .....

5570229821 : MAJOR ELECTRICAL ENGINEERING
KEYWORDS: QUANTUM KEY DISTRIBUTION / LOW-DENSITY PARITY-CHECK CODES / RATE-ADAPTIVE LDPC / KEY RECONCILIATION / SLEPIAN-WOLF CODING

THARATHORN PHROMSA-ARD: KEY RECONCILIATION PROTOCOL WITH LOW-DENSITY PARITY-CHECK CODES FOR QUANTUM KEY DISTRIBUTION. ADVISOR: ASSOC. PROF. LUNCHAKORN WUTTISITTIKULKIJ, Ph.D., CO-ADVISOR: KAMOL KAEMARUNGSI, Ph.D., PISIT VANICHCHANUNT, Ph.D., 74 pp.

In this thesis, a key reconciliation method is proposed as one of the classical part in Quantum Key Distribution (QKD) protocol. The proposed method aims to correct the transmission error after distribution of quantum key objects over a quantum channel. For error correction, Low-Density Parity-Check (LDPC) codes are adopted as the technique of source coding with side information. This study investigates three main proposed methods covering possible cases of error rates in QKD system. The first method is the LDPC code with bit-flipping and sum product syndrome decoding. This technique deploys a fixed code-rate and achieves an error-correcting performance better than Hamming syndrome in Winnow protocol. Furthermore, the relationship of the decoding methods and block-length effect with reconciliation efficiency is investigated. Secondly, rate-adaptive reconciliation based on LDPC accumulate codes is studied. The sequence accumulate syndrome is stored in a buffer and some elements are sent incrementally to the decoder. Finally, rate adaptive LDPC reconciliation method based on puncturing and shortening technique with estimated Quantum Bit Error Rate (QBER) from only syndrome is studied. This method also estimates reconciliation efficiency in advance for determination of an optimal rate. From numerical results, it can be observed that the performance of our proposed schemes in terms of reconciliation efficiency, a number of disclosed bits and interactive communications is superior to conventional Winnow and Cascade protocols. Therefore, gain of these proposed schemes impacts significantly on the achievable secret key generation rate with responding to the high efficiency for discrete-variable QKD applications.

Department:	Electrical Engineering	Student's Signature .....
Field of Study:	Electrical Engineering	Advisor's Signature .....
Academic Year:	2015	Co-Advisor's Signature .....
		Co-Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้จะสำเร็จลุล่วงได้ด้วยดีมิได้หากปราศจากการความช่วยเหลือของท่าน ทั้งหลายดังต่อไปนี้

ขอกราบขอบพระคุณ รศ. ดร.ลัญฉกร วุฒิสิทธิกุลกิจ ดร.กมล เขมะรังษี และ ดร.พิสิฐ วนิชชานันท์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ที่ได้ให้คำแนะนำ ประสิทธิประสาทวิชาความรู้ รวมทั้งข้อคิดเห็นต่างๆ ตลอด ระยะเวลาในการวิจัยมาด้วยดีตลอดมา ตั้งแต่เริ่มศึกษาเล่าเรียนจวบจนจบการศึกษาและการทำงานด้านการวิจัย ณ จุฬาลงกรณ์มหาวิทยาลัยแห่งนี้

ขอขอบคุณ คุณปรมินทร์ แสงวงษ์งาม และ ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์ นักวิจัยแห่งศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนทเทค) ผู้ที่มีความรู้ความเชี่ยวชาญด้านการสื่อสารเชิงแสงและควอนตัม ที่ได้ให้คำปรึกษา ข้อมูลความรู้ และเครื่องมือในการศึกษาทำงานวิจัยนี้

ขอขอบคุณ คุณพัชรพงษ์ ตรีวิริยานุภาพ จากมหาวิทยาลัยราชภัฏพระนครและ Dr.Jesus-Martinez Mateo จากกลุ่มวิจัยคำนวณและสารสนเทศเชิงควอนตัม Technical University of Madrid (UPM) ประเทศสเปน ที่ให้คำปรึกษาและแนะนำด้านการไกล่ความผิดพลาดกุญแจรหัสลับในการทำวิจัยนี้

ขอขอบคุณสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ให้การสนับสนุนทุนการศึกษาและวิจัย ในนามของโครงการทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST) เลขที่ TG-44-09-55-039M ในช่วงปีการศึกษา 2555–2556

สุดท้ายขอกราบขอบพระคุณบิดามารดา และญาติพี่น้องของข้าพเจ้า ที่ได้ให้โอกาส ให้กำลังใจ ให้ความช่วยเหลือห่วงใยมาตลอดซึ่งเป็นส่วนที่สำคัญมากสำหรับช่วยเป็นแรงผลักดันให้ทำงานวิจัยสำตลอดลุล่วงไปด้วยดี

สารบัญ

หน้า

หน้า

หน้า

สารบัญรูป

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหา

โครงสร้างพื้นฐานของระบบการสื่อสารโทรคมนาคมได้เข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตประชาชนในปัจจุบันเพื่อตอบสนองการใช้งานในลักษณะต่างๆ จำเป็นต้องให้การสื่อสารมีประสิทธิภาพยิ่งขึ้นไม่ว่าจะเป็นการส่งข้อมูลข่าวสารผ่านเครือข่ายส่วนตัว (Private network) หรือเครือข่ายสาธารณะ (Public network) เช่น อินเทอร์เน็ต โทรศัพท์เคลื่อนที่ที่มีผู้ใช้งานจำนวนมากขึ้นและการบริการหลายรูปแบบ ทั้งบริการส่งข้อมูลภายใน องค์กรต่างๆ หรือการส่งข้อมูลระหว่างเครือข่ายต่างองค์กร ต่างส่งผลให้เกิดความสะดวก รวดเร็ว ในการส่งข้อมูลข่าวสาร ทำให้การปฏิบัติงานภายในองค์กรดำเนินไปได้อย่างรวดเร็ว ถึงแม้ว่าการส่งข้อมูลผ่านระบบเครือข่ายดังกล่าวจะมีข้อดีอยู่มากมาย แต่ก็มีผู้ประสงค์ร้ายที่แฝงเข้ามาร่วมใช้งานระบบเครือข่าย เพื่อหาประโยชน์ใส่ตนอยู่มากมาย เช่น มีผู้เข้ามาโจมตีระบบ ทำให้ระบบเครือข่ายใช้งานไม่ได้ หรือมีผู้เข้ามาขโมยข้อมูลระหว่างที่มีการรับส่ง เหตุการณ์เหล่านี้กลายเป็นปัญหาสำคัญของการใช้งานระบบเครือข่ายในปัจจุบัน ที่ส่งผลให้เกิดความเสียหายต่อองค์กร เสียหายต่อระบบเศรษฐกิจและความมั่นคงของประเทศตามมา และเพื่อเป็นการป้องกันปัญหาดังกล่าว เทคโนโลยีหนึ่งที่ช่วยให้รักษาความลับของข้อมูลข่าวสารที่ส่งผ่านระบบเครือข่าย เพื่อไม่ให้บุคคลที่สามหรือบุคคลภายนอกรับรู้ข้อมูลระหว่างการส่งคือวิทยาการรหัสลับเชิงควอนตัม (Quantum cryptography) ด้วยวิธีการกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution: QKD) ซึ่งถือได้ว่าเป็นเทคโนโลยีการสื่อสารที่สำคัญเพื่อการสร้างและแลกเปลี่ยนกุญแจรหัสลับ (Secret key) ระหว่างผู้ส่งและผู้รับร่วมกันและให้เป็นความลับจากผู้ดักจับข้อมูลมากที่สุดซึ่งอาศัยคุณสมบัติเชิงควอนตัมของแสง เพื่อใช้เป็นกุญแจรหัสลับและใช้ทฤษฎีกลศาสตร์ควอนตัม (Quantum mechanics) หรือหลักการความไม่แน่นอนของไฮเซนแบร์ก (Heisenberg uncertainly principle) ช่วยยืนยันความปลอดภัยของระบบ ฉะนั้น เมื่อใดที่มีบุคคลที่สามบุกรุกเข้ามาขโมยสถานะควอนตัมของแสง จะทำให้ผู้ส่งและผู้รับทราบได้ทันทีถึงการเข้ามาขโมยกุญแจรหัสลับโดยอัตราความผิดพลาดของกุญแจรหัสลับที่ส่งจะสูงขึ้น ผู้ส่งและผู้รับสามารถยกเลิกการส่งกุญแจรหัสลับได้ทันก่อนจะเกิดความเสียหายตามมา นำไปสู่การเป็นระบบการรักษาความปลอดภัยของข้อมูลแบบไม่มีเงื่อนไข (Unconditionally secure) ดังแตกต่างกับระบบวิทยาการรหัสลับแบบทั่วไปที่ความปลอดภัยของข้อมูลถูกยืนยันได้เพียงขีดความสามารถของอุปกรณ์เครื่องคำนวณ (Secure with computationally bound) เช่น คอมพิวเตอร์ จากคุณสมบัติพิเศษ

ดังกล่าวนี้ระบบการกระจายกุญแจรหัสลับเชิงควอนตัมจึงเข้ามาเป็นส่วนประกอบสำคัญในโครงสร้างพื้นฐานระบบการสื่อสารเพื่อการรักษาความปลอดภัยข้อมูลสารสนเทศ

วิทยาการรหัสลับเชิงควอนตัมเป็นระบบที่ใช้ในการส่งกุญแจรหัสลับ โดยอาศัยคุณสมบัติทางควอนตัมของแสง แต่เนื่องจากสัญญาณรบกวน ความไม่เป็นอุดมคติของอุปกรณ์ทั้งทางภาคส่งและทางภาครับเป็นสาเหตุทำให้กุญแจรหัสลับที่ส่งเกิดความผิดพลาดขึ้นได้ การไกล่เกลี่ยความผิดพลาด (Key reconciliation) เป็นหนึ่งในขั้นตอนสำคัญของการกระจายกุญแจรหัสลับเชิงควอนตัมที่ช่วยแก้ไขความผิดพลาดข้อมูลกุญแจจากสาเหตุดังกล่าวเหมือนระบบการสื่อสารทั่วไป เพื่อการยืนยันความถูกต้องของข้อมูลกุญแจระหว่างผู้ส่งกับผู้รับตัวจริงให้มีค่าที่ตรงกันโดยสมบูรณ์ สำหรับการนำไปใช้ในการเข้าและถอดรหัสข้อมูลในระบบการสื่อสารเพื่อแลกเปลี่ยนข้อมูลจริงได้อย่างมีประสิทธิภาพและมีความปลอดภัยอย่างสูงสุด

โดยทั่วไปวิธีการไกล่เกลี่ยความผิดพลาดจะอาศัยพื้นฐานการค้นหาแบบไบนารี่ ดังตัวอย่างของโพรโทคอลบีบีบีเอสเอส (BBBSS protocol) [1] โพรโทคอลคาสคาด [2] และโพรโทคอลวินนาว (Winnow protocol) [3] เป็นต้น อย่างไรก็ตาม โพรโทคอลเหล่านี้จำเป็นต้องอาศัยการติดต่อสื่อสารระหว่างผู้ส่งและผู้รับอย่างเป็นจำนวนมาก ส่งผลต่อการประมวลผลที่ล่าช้าอันเป็นข้อจำกัดสำคัญของอัตราการกำเนิดกุญแจรหัสลับสำหรับระบบฯ ที่ ต้องการความเร็วสูง และมีความสามารถที่จะแก้ไขความผิดพลาดได้น้อยเพื่อยืนยันความถูกต้องได้ไม่ดีพอ รหัสช่องสัญญาณหรือรหัสแก้ไขความผิดพลาดจึงถูกทำมาประยุกต์ทำงานร่วมกับการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารข้างเคียงเพื่อแก้ปัญหาดังกล่าว หนึ่งในนั้นก็คือรหัสพาริตีเช็กความหนาแน่นต่ำ หรือเรียกโดยย่อว่ารหัสแอลดีพีซี ซึ่งทำหน้าที่ช่วยตรวจวัดและแก้ไขความผิดพลาดที่เกิดขึ้นของข้อมูลที่มีการสื่อสารกันตามช่องทางการสื่อสารต่างๆ ได้ดีมาก เช่น สายโทรศัพท์คลื่นวิทยุผ่านอากาศ และระบบจัดเก็บข้อมูล เป็นต้น ดังจะเห็นได้จากในช่วงหลายปีที่ผ่านมารหัสแอลดีพีซีได้รับความสนใจจากนักวิจัยอย่างมากจากการที่มีบทความที่เกี่ยวข้องทั้งในวารสารวิชาการและการประชุมทางวิชาการจำนวนมาก ในด้านอุตสาหกรรมจะพบผลิตภัณฑ์ที่เกี่ยวข้องกับรหัสนี้จำนวนมากรหัสแอลดีพีซีนั้นมีลักษณะสำคัญคือสามารถถอดรหัสแบบวนซ้ำ (Iterative decoding) ได้ซึ่งมีประโยชน์คือทำให้ลดความซับซ้อนทางการคำนวณในการถอดรหัสลงได้มากแล้วยังให้สมรรถนะอัตราความผิดพลาดบิต(Bit Error Rate: BER) ที่ดีกล่าวคือมี BER ต่ำมากนอกจากนี้ รหัสแอลดีพีซียังมีข้อเด่นคือสามารถสร้างเป็นวงจรดิจิทัลได้มีประสิทธิภาพคือมีความเร็วในการทำงานสูงมีพื้นที่ของวงจรน้อยและมีความยืดหยุ่นในการทำงานสูงนอกจากนี้รหัสแอลดีพีซียังได้รับความน่าเชื่อถือสูงให้ใช้ในมาตรฐานต่างๆมากมายเช่น มาตรฐานระบบโทรทัศน์ดิจิทัลผ่านดาวเทียม DVB-S2 ระบบแพร่ภาพดิจิทัลภาคพื้นดิน DVB-T2 มาตรฐานการสื่อสารไร้สาย WLAN 802.11n, WiMAX 802.16e รวมทั้งมาตรฐานระบบโทรศัพท์เคลื่อนที่ในยุคสามและสี่ (3G/4G)

จากที่ได้กล่าวมาแล้วในข้างต้นได้แสดงให้เห็นถึงที่มาความสำคัญของรหัสแอลดีพีซีและระบบการกระแจกุญแจรหัสลับเชิงควอนตัม จึงเป็นเหตุสำคัญนำมาสู่วัตถุประสงค์ของงานวิทยานิพนธ์นี้คือเพื่อการออกแบบและพัฒนาวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีประยุกต์ทำงานร่วมกับการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารข้างเคียงให้เหมาะสมกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมความเร็วสูง ทำให้สามารถสร้างกุญแจรหัสลับได้อย่างรวดเร็ว และมีประสิทธิภาพสูง

1.2 งานวิจัยที่เกี่ยวข้อง

กระบวนการไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัมต่างมีรูปแบบและวิธีการที่แตกต่างกันไปซึ่งบางวิธีที่ได้รับการจดคุ้มครองเป็นสิทธิบัตรงานประดิษฐ์ และบางวิธีการก็ได้ถูกนำเสนอในเอกสารเชิงวิชาการต่างๆ และต่อมาได้ถูกนำมาพัฒนาเป็นโพรโทคอลฯ สำหรับการใช้งานจริงในระบบการกระจายกุญแจรหัสลับเชิงควอนตัม ในงานวิจัยที่เกี่ยวข้องผู้เขียนขอแบ่งออกได้ 2 รูป คือ แบบแรก ใช้หลักการการค้นหาตำแหน่งบิตข้อมูลกุญแจที่ผิดพลาดด้วยการค้นหาแบบไบนารี (binary search) และแบบที่สอง ใช้รหัสช่องสัญญาณเพื่อช่วยในการแก้ไขความพลาดซึ่งได้มีงานวิจัยที่นำเสนอรูปแบบของรหัสที่ใช้แตกต่างกันไปมากมาย

ตัวอย่างของโพรโทคอลที่ใช้หลักการค้นหาแบบไบนารี่ ได้แก่ โพรโทคอลบีบีบีเอสเอส (BBBSS) นำเสนอโดย Charles H. Bennett และคณะฯ ในปี ค.ศ.1991 จากเอกสารวิชาการเรื่อง “*Experimental Quantum Cryptography*” [1] ซึ่งมีพื้นฐานการแก้ไขความผิดพลาดเริ่มต้นจากคู่สื่อสารแบ่งข้อมูลกุญแจออกเป็นชุด ๆ ตามขนาดของบล็อกที่เหมาะสม และคำนวณหาพาริตีบิตพร้อมการเปรียบเทียบในแต่ละบล็อกนั้นๆ หากบิตพาริตีของบล็อกใดมีค่าแตกต่างกันแล้ว ภาคส่งและภาครับจะดำเนินการค้นหาตำแหน่งบิตข้อมูลกุญแจที่ผิดพลาดด้วยการค้นหาแบบไบนารี (binary search) และดำเนินการแก้ไข โดยโพรโทคอลดังกล่าว จะมีการวนซ้ำรอบ (Iteration) การแก้ไขความผิดพลาดเรื่อยๆ จนกว่าจะสามารถแก้ไขความผิดพลาดได้ทั้งหมด และในเอกสารวิชาการ เรื่อง “*Secret-Key Reconciliation by Public Discussion*” [2] โดย Gilles Brassard และ Louis Salvail ในปี ค.ศ. 1994 ได้มีการพัฒนาโพรโทคอลคาสเคด (Cascade) ที่ได้รับความนิยมในการใช้งานจริงบนระบบการกระจายกุญแจรหัสลับเชิงควอนตัมมากที่สุด ซึ่งมีพื้นฐานการแก้ไขความผิดพลาดด้วยการค้นหาแบบไบนารีเช่นเดียวกับบีบีบีเอสเอส แต่ได้รับการปรับปรุงประสิทธิภาพเพื่อเป้าหมายของการลดจำนวนข้อมูลที่เปิดเผยสู่ช่องสัญญาณในระหว่างกระบวนการ โดยการเพิ่มขั้นตอนการบันทึกข้อมูลกุญแจในแต่ละชุด ซึ่งหากพบความผิดพลาดของบิตข้อมูลใดๆ เกิดขึ้นใหม่แล้ว สามารถทำการตรวจสอบได้โดยการค้นหาแบบย้อนกลับจากข้อมูลที่บันทึกไว้ อันส่งผลให้ปริมาณบิตข้อมูลข่าวสารที่ส่งผ่านช่องสัญญาณมีจำนวนลดลง แต่อย่างไรก็ตามทั้งสองโพรโทคอลที่ได้

กล่าวมาข้างต้น มีพื้นฐานการไกล่เกลี่ยความผิดพลาดโดยการค้นหาแบบไบนารี (binary searching) ดังนั้นจึงจำเป็นต้องอาศัยการติดต่อสื่อสารระหว่างผู้ส่งและผู้รับเป็นจำนวนมาก อันส่งผลต่อการประมวลผลที่ล่าช้าที่ยังคงเป็นข้อจำกัดของอัตราการกำเนิดกุญแจรหัสลับเชิงควอนตัม

ตัวอย่างของโพรโทคอลที่ใช้รหัสช่องสัญญาณ ได้แก่ โพรโทคอลวินนาว (Winnow) นำเสนอโดย W. T. Buttler และคณะฯ จากวารสารวิชาการเรื่อง "*Fast, Efficient Error Reconciliation for Quantum Cryptography*" [3] ในปี ค.ศ. 2003 ที่อาศัยหลักการแก้ไขความผิดพลาดด้วยรหัสแฮมมิง (Hamming code) หนึ่งในประเภทของรหัสแก้ไขความผิดพลาดแทนการค้นหาแบบไบนารี่ ถึงแม้โพโทรคอลวินนาวจะใช้จำนวนครั้งของการสื่อสารระหว่างผู้ส่งและผู้รับที่น้อย ส่งผลให้มีอัตราการประมวลผลที่สูงกว่าทั้งโพรโทคอลบีบีบีเอสเอสและโพรโทรคาสเคด แต่อย่างไรก็ตามประสิทธิภาพของการตรวจสอบและแก้ไขความผิดพลาดยังคงมีขีดจำกัดตามความสามารถของรหัสแฮมมิ่งที่มีประสิทธิภาพต่ำและต่อมาเริ่มใช้รหัสแก้ไขความผิดพลาดร่วมในระบบ เช่น รหัสคอนโวลูชั่น (Convolution codes) [4] รหัสบีซีเอช (BCH codes) [5, 6] การใช้รหัสทั้งสองทำให้ลดการติดต่อระหว่างผู้ส่งและผู้รับลงได้แต่จากความสามารถของรหัสทั้งสองเป็นรหัสแก้ไขความผิดพลาดแบบเก่าซึ่งให้ความสามารถที่ในการแก้ไขที่จำกัดทำให้ประสิทธิภาพในการไกล่เกลี่ยจำกัดลงไปด้วย

ตัวอย่างโพรโทรคอลการไกล่เกลี่ยที่ถูกพัฒนาโดยรหัสช่องสัญญาณที่ให้ประสิทธิภาพที่ดีชนิดหนึ่งคือ รหัสแอลดีพีซี ซึ่งเป็นรหัสที่ได้รับการยอมรับว่ามีความสามารถให้ในการแก้ไขความผิดพลาดเข้าขีดจำกัดของแชนนอน ขอยกตัวอย่าง เช่น บทความวิจัย [7] นำเสนอโดย D. Elkouss, และคณะฯ เสนอวิธีการการแก้ไขความผิดพลาดข้อมูลกุญแจรหัสลับเชิงควอนตัมด้วยรหัสแอลดีพีซีแบบไม่สม่ำเสมอ (Irregular-LDPC code) ประสิทธิสภาพสูงในแต่ละเมทริกซ์พาติเช็กและเลือกอัตราการเข้ารหัสที่เหมาะเฉพาะกับช่วง QBER พร้อมกระบวนการวิเคราะห์ประสิทธิการไกล่เกลี่ยความผิดพลาดแต่วิธีที่นำเสนอยังมีความยาวของรหัสที่สูงพอสมควรมากกว่า 10^7 บิตต่อบล็อกจึงไม่เหมาะสมกับใช้งานในระบบ คณะวิจัยนำโดย J.Martinez-Mateo ได้นำเสนอบทความ ซึ่งนำเสนอปรับค่าการเข้าอัตราในรูปแบบ "Blind Reconciliation" [8-10] ที่อาศัยการวนรอบการทำงานในการปรับลดค่าอัตราการเข้ารหัสเป็นลำดับจนกระทั่งสอดคล้องกับอัตราความผิดพลาดกุญแจรหัสลับที่เกิดขึ้นได้ในระบบฯ และประเมินผลยืนยันความสำเร็จภายใต้การถอดรหัสแบบซินโดรม (Syndrome decoding) อย่างไรก็ตามวิธีการดังกล่าวยังคงต้องใช้จำนวนครั้งในการติดต่อสื่อสารระหว่างคู่สื่อสารขึ้นกับจำนวนครั้งในการวนรอบการทำงานของกระบวนการเข้าและถอดรหัส จึงส่งผลต่ออัตราการประมวลผลที่ล่าช้าในทางปฏิบัติ จากบทความที่ต่อกล่าวมาข้างตนได้นำเสนอวิธีการปรับอัตราการเข้ารหัสที่เหมาะสม ดังนั้น จึงได้มีคณะวิจัยได้วิเคราะห์ประสิทธิการไกล่เกลี่ยและขอบเขตของการทำวิธีการปรับอัตราการเข้ารหัสที่เหมาะสมในแง่ของความปลอดภัยของข้อมูลและจำนวนข้อมูลที่สามารถรั่วไหลได้ในระบบการไกล่เกลี่ย [11, 12]

จากที่ได้กล่าวมาข้างต้นโพรโทคอลจะสามารถแก้ไขปริมาณข้อมูลที่ผิดพลาดในอัตราที่สูง แต่สำหรับการใช้ประยุกต์ใช้งานจริงนั้น วิธีการที่นำเสนอไม่ได้กล่าวถึงส่วนขั้นตอนสำคัญของการวิเคราะห์ปรับค่าอัตราการเข้ารหัสให้เหมาะสมกับสภาพแวดล้อมที่เกิดขึ้นในแต่ละช่วงการทำงานของระบบการกระจายกุญแจรหัสลับเชิงควอนตัม เช่น อัตราความผิดพลาดบิตข้อมูลกุญแจรหัสลับ (quantum bit error rate: QBER) และการประมาณประสิทธิภาพการไกล่เกลี่ยล่วงหน้า (Efficiency) เป็นต้น ดังจะนำเสนอต่อไปในบทที่ 4 ซึ่งจะอาศัยหลักความรู้พื้นฐานความน่าจะเป็นสูงสุด (Maximum likelihood) มาประยุกต์ช่วยในประเมินช่องสัญญาณ [13] โดยอาศัยข้อมูลจากซินโดรมที่ของคู่การสื่อสารที่ต้องส่งผ่านช่องสัญญาณเพื่อไกล่เกลี่ยความผิดพลาดอยู่แล้ว โพรโทคอลการไกล่เกลี่ยความผิดพลาดที่ได้กล่าวมาข้างต้น ต้องอาศัยข้อมูล QBER แสดงถึงความน่าจะเป็นของข้อมูลร่วม (Joint probability) ระหว่างผู้ส่ง ผู้รับ โดยเฉพาะอย่างยิ่งผู้ดักจับข้อมูล อันเป็นตัวแปรสำคัญสำหรับการประมวลผลการแก้ไขความผิดพลาดให้มีประสิทธิภาพสูงสุดโดยทั่วไป QBER ถูกประเมินได้จากการเปิดเผยและเปรียบเทียบบิตข้อมูลกุญแจบางส่วนระหว่างภาคส่งกับภาครับซึ่งกันและกัน และจะถูกตัดทิ้ง เพื่อนำข้อมูลกุญแจส่วนที่เหลือเข้าสู่กระบวนการไกล่เกลี่ยความผิดพลาด ซึ่งเป็นการสูญเสียข้อมูลในส่วนนี้ไป หลังจากที่ได้ค่าจากการประเมินช่องสัญญาณแล้วนำไปประมาณขอบเขตของค่าประสิทธิภาพการไกล่เกลี่ยเพื่อเลือกอัตรารหัสที่เหมาะสมต่อไปได้

การปรับอัตรารหัสที่เหมาะสม (rate adaptive) นั้นต้องอาศัยเทคนิคการหาอัตรารหัสที่เหมาะสมในแต่สภาวะที่แตกต่างกันไป โดยเทคนิคนั้นก็คือการพังเจอร์และเชอร์ตเทน โดยคณะวิจัยนำโดย Ha ในเอกสารอ้างอิง [14, 15] ได้นำเสนอวิธีการพังเจอร์ทั้งบล็อกขนาดใหญ่และขนาดปานกลาง ทั้งแบบสุ่มและไม่สุ่มของรหัสแอลดีพีซีแบบไม่สม่ำเสมอในรหัสบล็อกเชิงเส้น และในทางระบบเสมือนจริงการที่จะเลือกที่ใช้พังเจอร์หรือชอร์ตเทนเพื่อเพิ่มและลดอัตรารหัสได้ทีละแบบนั้นขึ้นกับช่องสัญญาณที่เหมาะสมโดยการเลือกที่จะพังเจอร์หรือชอร์ตเทนที่เหมาะสมด้วย ซึ่งเป็นขีดจำกัดของประสิทธิภาพการแก้ไขด้วยวิธีนี้ ด้วยปัญหาทั้งสองนี้จึงเป็นข้อจำกัดหนึ่งของอัตราการกำเนิดกุญแจรหัสลับในระบบฯ และปัญหาดังกล่าว ยังไม่ได้รับการแก้ไขจากวิธีการไกล่เกลี่ยความผิดพลาดที่ถูกนำเสนอก่อนหน้านี้

1.3 แนวทางของงานวิจัย

งานวิจัยนี้ศึกษาโพรโทคอลไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับในระบบกระจายกุญแจรหัสลับเชิงควอนตัมโดยนำรหัสช่องสัญญาณคือรหัสแอลดีพีซีเป็นหลักเพื่อใช้แก้ไขความผิดพลาดของกุญแจรหัสลับเพื่อพัฒนาประสิทธิภาพการไกล่เกลี่ยข้อมูล อัตราการกำเนิดกุญแจรหัสลับที่สูง ลดการ

ติดต่อสื่อสารระหว่างผู้ส่งและผู้รับซึ่งเหมาะสมกับระบบการกระจายกุญแจรหัสรับที่ต้องการความเร็วสูง ซึ่งนำเสนอวิธีคือ

1.3.1 นำเสนอวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีร่วมกับรหัสซลีเพียน-วูลฟ์ โดยการเลือกอัตราการเข้ารหัสที่เหมาะสม (Rate compatible) ด้วยวิธีการถอดรหัสแบบบิตฟลิปปิง ซึ่งเป็นรูปแบบการถอดรหัสแบบฮาร์ดและซัมโปรดักซินโดรมซึ่งเป็นถอดรหัสแบบซอร์ฟ

1.3.2 นำเสนอวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีร่วมกับรหัสซลีเพียน-วูลฟ์ โดยอัตราการเข้ารหัสที่สามารถปรับตัวเหมาะสมได้ (Rate adaptive) โดยเลือกวิธีการปรับรหัสแบบผลรวมสะสมซินโดรมและการปรับอัตราหรัสแบบพังเจอร์และชอร์ตเทนที่ให้ประสิทธิภาพสูง

1.3.3 นำเสนอวิธีการประเมินความผิดพลาดควอนตัมบิต (QBER) และโดยไม่ต้องสูญเสียบิตเปิดเผยโดยใช้ข้อมูลซินโดรมของผู้ส่งและรับจากที่ส่งผ่านช่องสัญญาณทั่วไปอยู่แล้ว โดยให้มีความใกล้เคียงกับความผิดพลาดแท้จริงและนำเสนอวิธีการประมาณค่าขอบเขตประสิทธิภาพล่วงหน้าเพื่อเลือกอัตรารหัสให้เหมาะสม

1.4 วัตถุประสงค์

1.3.1 เพื่อศึกษารหัสพาริตีเช็กความหนาแน่นต่ำที่ใช้แก้ไขความผิดพลาดที่เกิดจากผลของสัญญาณรบกวนภายในช่องทางการสื่อสารของระบบสื่อสาร

1.3.2 เพื่อศึกษาขั้นตอนการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม เพื่อนำรหัสพาริตีเช็กความหนาแน่นต่ำมาพัฒนาโพรโทคอลการไกล่เกลี่ยความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม

1.3.3 เพื่อออกแบบพัฒนาโพรโทคอลการไกล่เกลี่ยความผิดพลาดโดยใช้รหัสพาริตีเช็กความหนาแน่นต่ำให้เหมาะสมกับระบบกระจายกุญแจรหัสลับความเร็วสูง ทำให้สามารถสร้างกุญแจรหัสลับได้อย่างรวดเร็ว และมีประสิทธิภาพ

1.5 ขอบเขตของงานวิจัย

วิทยานิพนธ์นี้นำเสนอการออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสพาริตีเช็กความหนาหนาแน่นต่ำหรือรหัสแอลดีพีซีแบบไบนารี่เท่านั้น โดยการนำรหัสแอลดีพีซีมาประยุกต์ร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง (Side information) เพื่อพัฒนาโพรโทคอลแก้ไขความผิดพลาดให้เหมาะสมกับระบบกระจายกุญแจรหัสลับความเร็วสูง สามารถลดจำนวนรอบการติดต่อสื่อสารระหว่างผู้ส่ง *Alice* และผู้รับ *Bob* ในขั้นตอนการแก้ไขความผิดพลาด และพัฒนาโพรโทคอลให้สามารถใช้ร่วมกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง

1.6 ขั้นตอนและวิธีการดำเนินงาน

1) ศึกษาระบบวิทยาการรหัสลับเชิงควอนตัม การส่งกุญแจรหัสลับและการประยุกต์ระบบวิทยาการรหัสลับเชิงควอนตัม

2) ศึกษากระบวนการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม การทำงานของโพรโทคอลไกล่เกลี่ยความผิดพลาดที่ใช้ในระบบกระจายรหัสลับเชิงควอนตัม

3) ศึกษาขั้นตอนการทำงาน กระบวนการเข้ารหัสและกระบวนการถอดรหัสของรหัสแก้ไขความผิดพลาดพาริตีเช็กความหนาแน่นต่ำหรือรหัสแอลดีพีซี

4) นำรหัสแอลดีพีซีมาประยุกต์ร่วมกับโพรโทคอลไกล่เกลี่ยความผิดพลาดแอลดีพีซีจากการกระจายกุญแจรหัสลับเชิงควอนตัมเพื่อพัฒนาโพรโทคอลให้เหมาะสมกับระบบกระจายกุญแจรหัสลับประสิทธิภาพสูง

5) ออกแบบโปรแกรมและจำลองการทำงานโพรโทคอลไกล่เกลี่ยความผิดพลาดแอลดีพีซีที่ได้พัฒนาขึ้น

6) ทดสอบและวิเคราะห์ประสิทธิภาพระบบที่ได้ออกแบบไว้

7) รวบรวมและตรวจสอบข้อมูล เพื่อจะทำเล่มวิทยานิพนธ์

1.7 ประโยชน์ที่คาดว่าจะได้รับ

ได้วิธีการออกแบบโพรโทคอลกระบวนการไกล่เกลี่ยความผิดพลาดด้วยรหัสพาริตีความหนาแน่นต่ำสำหรับระบบกระจายกุญแจรหัสลับเชิงควอนตัมที่มีค่าสัมประสิทธิ์ประสิทธิภาพการไกล่เกลี่ยที่ดีเข้าใกล้ทฤษฎี ลดการติดต่อสื่อสารระหว่างผู้ส่งและผู้รับ เหมาะสำหรับระบบกระจายกุญแจรหัสลับที่ต้องการความเร็วสูงและให้อัตราการกำเนิดกุญแจรหัสลับที่สูง

1.8 ประมวลวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้แบ่งเนื้อหาออกเป็นทั้งหมด 6 บทดังต่อไปนี้

บทที่ 1 บทนำ: มีเนื้อหาเกี่ยวกับความเป็นมาและความสำคัญของปัญหาของงานวิจัยนี้ในวิทยานิพนธ์ของรายละเอียดที่เกี่ยวกับเป้าหมายสำคัญของระบบการกระจายกุญแจรหัสเชิงควอนตัม ปัญหาที่ประสบและงานวิจัยที่เกี่ยวข้องกับวิทยานิพนธ์นอกจากนี้ยังกล่าวถึงแนวคิดที่เสนอวัตถุประสงค์เป้าหมายและขอบเขตของวิทยานิพนธ์ขั้นตอนและวิธีการดำเนินงานและสุดท้ายเป็นประโยชน์ที่คาดว่าจะได้รับจากงานวิจัย

บทที่ 2 ระบบการกระจายกุญแจรหัสลับเชิงควอนตัม: กล่าวถึงหลักการและทฤษฎีเบื้องต้นที่ควรทราบเกี่ยวกับระบบการกระจายกุญแจรหัสลับเชิงควอนตัม การไกล่เกลี่ยความผิดพลาดของกุญแจรหัสลับที่เกิดขึ้นระหว่างการสื่อสาร โพรโทคอลที่ใช้ในการไกล่เกลี่ยความผิดพลาดของกุญแจรหัสลับ

บทที่ 3 ทฤษฎีข่าวสารสนเทศและรหัส : กล่าวถึงหลักการและทฤษฎีเบื้องต้นของทฤษฎีข่าวสารสนเทศ ที่นำมาวิเคราะห์ผสมผสานกับระบบกระจายกุญแจรหัสลับเชิงควอนตัม รหัสช่องสัญญาณที่ใช้แก้ไขความผิดพลาด ขั้นตอนวิธีเข้าและถอดรหัสแอลดีพี การประยุกต์รหัสซลีเพียน-วูฟล์กับรหัสช่องสัญญาณ

บทที่ 4 โพรโทคอลไกล่เกลี่ยความผิดพลาดรหัสลับที่นำเสนอ : กล่าวถึงโครงสร้างโพรโทคอลการไกล่เกลี่ยความผิดพลาดของระบบพร้อมทั้งหมดการวิเคราะห์ประสิทธิภาพของระบบที่เสนอ

บทที่ 5 ผลการทดสอบโพรโทคอลไกล่เกลี่ยความผิดพลาดรหัสลับที่นำเสนอ: ในบทนี้จะเป็นการแสดงผลการจำลองแบบ (Simulation results) ของระบบที่ใช้วิธีการดั้งเดิมและวิธีการที่เสนอด้วยคอมพิวเตอร์เพื่อเปรียบเทียบสมรรถนะรวมถึงผลกระทบจากพารามิเตอร์ของระบบที่นำเสนอ

บทที่ 6 สรุป: บทนี้จะเป็นการสรุปผลการวิจัยที่ได้ศึกษาทั้งหมดของวิทยานิพนธ์และเสนอแนะแนวทางการทำวิจัยต่อจากงานวิจัยนี้ในอนาคต

บทที่ 2
การกระจายกุญแจรหัสลับเชิงควอนตัม

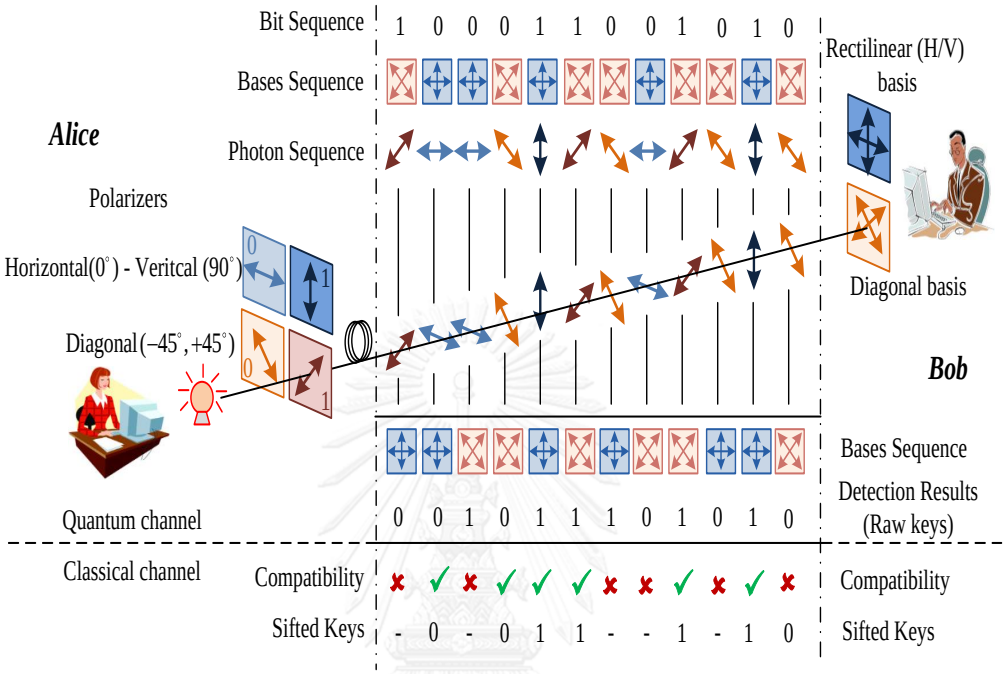
2.1 พื้นฐานระบบกระจายกุญแจรหัสลับเชิงควอนตัม

การกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution: QKD) [16] ถือเป็นหนึ่งในสาขาของเทคโนโลยีสารสนเทศเชิงควอนตัม (Quantum information technology) ที่ได้รับการวิจัยและพัฒนาจนสามารถนำมาประยุกต์ใช้งานได้จริงดังตัวอย่างของระบบฯ เชิงพาณิชย์ในปัจจุบัน [17] โดยมีเป้าหมายเพื่อยกระดับความปลอดภัยในระบบการสื่อสารที่สำคัญ สำหรับการสร้างและแลกเปลี่ยนข้อมูลกุญแจรหัสลับร่วมกันของคู่สื่อสารให้เป็นความลับจากผู้ดักจับข้อมูลมากที่สุด ซึ่งสามารถยืนยันความปลอดภัยด้วยหลักทฤษฎีทางกลศาสตร์เชิง ควอนตัมหรือหลักการความไม่แน่นอนของไฮเซนแบร์ก (Heisenberg uncertainly principle) [18] นำไปสู่การเป็นระบบรักษาความปลอดภัยของข้อมูลแบบไม่มีเงื่อนไข (unconditionally secure) ภายใต้ทฤษฎีการเข้ารหัสด้วยอัลกอริธึม One-time Pads กับชุดข้อมูลกุญแจรหัสลับที่เป็นจำนวนสุ่มที่แท้จริง (True random) ซึ่งในที่นี้คือ กุญแจรหัสลับเชิงควอนตัม โดยระบบฯ ดังกล่าวสามารถสร้างและรับประกันความปลอดภัยของข้อมูลได้เหนือกว่าระบบวิทยาการรหัสลับแบบทั่วไป ที่ความปลอดภัยถูกยืนยันได้เพียงภายใต้ขีดข้อจำกัดความสามารถของอุปกรณ์เครื่องคำนวณ (Secure with computationally bound) เช่น คอมพิวเตอร์ในปัจจุบัน

การกระจายกุญแจรหัสลับเชิงควอนตัมจะอาศัยสองช่องสัญญาณสำคัญ ได้แก่ ช่องสัญญาณเชิงควอนตัม (Quantum channel) และช่องสัญญาณแบบทั่วไปที่ได้รับการยืนยันตัวตนคู่การสื่อสาร (Classical authenticated channel) เพื่อการกำเนิดเป็นกุญแจรหัสลับแบบสมมาตรความปลอดภัยสูงสำหรับคู่สื่อสารทั้งผู้ส่ง (*Alice*) และผู้รับ (*Bob*) โดยเกณฑ์วิธีการรับส่งกุญแจรหัสลับเชิงควอนตัมที่เป็นพื้นฐานรู้จักกันดีภายใต้โพรโทคอลบีบี 84 (BB84) ดังรูปที่ 2.1 ซึ่งบิตข้อมูลกุญแจรหัสลับจะถูกแทนหน่วยสารสนเทศเชิงควอนตัมหรือคิวบิต (Qubit) ได้แก่ สถานะโพลาไรเซชันของแสง (Polarization) หรือเฟสของโพลาไรเซชัน (Phase-polarization) ของโฟตอนเดี่ยวเป็นต้น โดยทั่วไปการกระจาย กุญแจรหัสลับเชิงควอนตัมสามารถแบ่งย่อยเป็นขั้นตอนการทำงานได้ดังรูปที่ 2.2 ซึ่งมีรายละเอียดต่อไปนี้

ขั้นตอนที่ 1 การรับส่งกุญแจรหัสลับผ่านช่องทางการสื่อสารเชิงควอนตัม (Quantum transmission and reception)

เริ่มต้นจากผู้ส่ง (*Alice*) สุ่มข้อมูลบิตกุญแจรหัสลับตามรูปแบบของการสุ่มอย่างแท้จริงจำนวน N บิต $X=\{X_1,X_2,...,X_N\}$ แล้วแทนค่าในรูปแบบการสุ่มหนึ่งในสอง

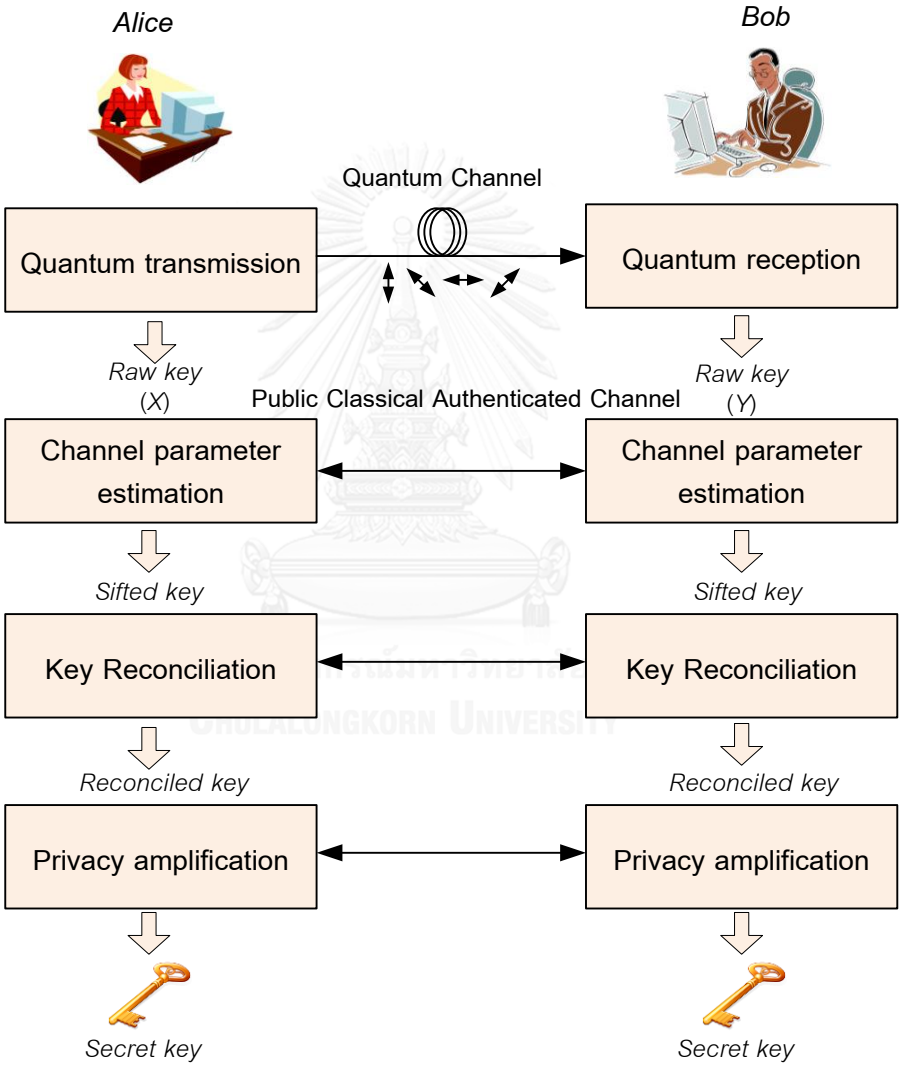


รูปที่ 2.1 การรับส่งกุญแจรหัสลับเชิงควอนตัมของโพรโทคอล BB84

ของสถานะเชิงควอนตัมด้วยของเวกเตอร์ฐาน (Basis) ที่ตั้งฉากซึ่งกันและกัน ได้แก่ เวกเตอร์ฐานเชิงเส้นตรง (Rectilinear basis)แทนโพลาไรเซชัน 90 องศา (↑) และ 0 องศา (→)และเวกเตอร์ฐานเชิงทแยงมุม (Diagonal basis) แทนโพลาไรเซชัน 45 องศา (↗) และ -45 (↘) องศาจากนั้นเข้ารหัสด้วยการใช้โพลาไรเซชันของโฟตอนเดี่ยว (Single photon) สี่สถานะเพื่อแทนบิตสุ่มหรือกุญแจรหัสลับบิตที่ต้องการส่งเช่น บิต “1”แทนด้วยโพลาไรเซชัน 90 องศา (↑) หรือ 45 องศา (↗) และบิต “0”แทนด้วยโพลาไรเซชัน 0 องศา (→) หรือ -45 องศา (↘)และ *Alice* ทำการสุ่มโพลาไรเซชันหนึ่งในสี่สถานะแล้วส่งไปยัง *Bob* ผ่านช่องทางการสื่อสารเชิงควอนตัมเช่น อากาศ (Free space) หรือเส้นใยนำแสง (Fiber optic) จากนั้นผู้รับจึงใช้หลักทฤษฎีการวัดทางควอนตัม (Quantum measurement) ด้วยการสุ่มเวกเตอร์ฐานจากหนึ่งในสองรูปแบบ เพื่อใช้รับโพลาไรเซชันแล้วแปลงจากสถานะเชิงควอนตัมที่รับได้เป็นบิตข้อมูลกุญแจ $Y=\{Y_1,Y_2,...,Y_N\}$ โดยผลลัพธ์ที่ได้จาก

กระบวนการนี้คือ บิตข้อมูลกุญแจดิบ X และ Y ในรูปแบบทั่วไป (Raw keys) ของผู้ส่งกับผู้รับตามลำดับดังรูปที่ 2.1

โดยขั้นตอนอื่นๆ นอกเหนือจากการรับส่งกุญแจรหัสลับผ่านช่องทางการสื่อสารเชิงควอนตัม จะเกิดขึ้นในส่วนช่องสัญญาณแบบทั่วไปหรือที่เรียกว่า QKD post processing ซึ่งอาศัยหลักทฤษฎีข่าวสารสารสนเทศในการประมวลผลเป็นกุญแจรหัสลับสุดท้ายที่มีความปลอดภัยสูงสุด



รูปที่ 2.2 ภาพรวมขั้นตอนพื้นฐานการกระจายกุญแจรหัสลับเชิงควอนตัม

ขั้นตอนที่ 2 การประมาณความผิดพลาดบนช่องสัญญาณเชิงควอนตัม (Channel parameter estimation)

ผู้ส่งและผู้รับอาศัยกระบวนการแลกเปลี่ยนเวกเตอร์ฐาน (Key sifting) โดยการเลือกค่าสถานะของกุญแจดิบเฉพาะที่มีเวกเตอร์ฐานระหว่างผู้ส่งและผู้รับที่ตรงกัน โดยผลลัพธ์ที่ได้คือ บิตข้อมูลไบนารีระหว่างผู้ส่งและผู้รับที่มีความยาวเท่ากันหรือที่เรียกว่า กุญแจซิฟย์ (Sifted key) หลังจากนั้นผู้ส่งและผู้รับจะการเปิดเผยข้อมูลกุญแจซิฟย์บางส่วนซึ่งกันและกัน เพื่อการประเมินค่าอัตราความผิดพลาดที่เกิดขึ้นบนช่องสัญญาณเชิงควอนตัมหรือ Quantum Bit Error Rate (QBER) ซึ่งค่าดังกล่าวแสดงถึงความน่าจะเป็นของข้อมูลร่วม (Joint probability) ระหว่างผู้ส่งและผู้รับ โดยเฉพาะอย่างยิ่งผู้ดักจับข้อมูล (Eavesdropper: *Eve*) ที่ไม่อาจทราบได้ในระบบกระจายกุญแจรหัสลับแบบทั่วไป (Classical key agreement) ถ้าหาก QBER มีค่าสูงอย่างผิดปกติ ผู้ส่งและผู้รับสามารถคาดเดาได้ว่าอาจมีผู้บุกรุกเข้ามายุ่งเกี่ยวกับระบบฯ และดำเนินการยกเลิกการรับส่งกุญแจหรือยกเลิกการใช้งานกุญแจรหัสลับที่มีอัตราความผิดพลาดสูงได้ทันที โดยข้อมูลกุญแจซิฟย์ดังกล่าวที่ถูกเปิดเผยแล้ว จะถูกตัดทิ้ง และนำข้อมูลกุญแจส่วนที่เหลือเข้าสู่กระบวนการต่อไป

ขั้นตอนที่ 3 การไกล่เกลี่ยความผิดพลาด (Key reconciliation)

เนื่องจากอาจมีความผิดพลาดจากการรับส่งข้อมูลกุญแจรหัสลับผ่านช่องทางการสื่อสารเชิงควอนตัม ที่เกิดขึ้นได้จากสาเหตุของสัญญาณรบกวน (Noise) หรือความไม่เป็นอุดมคติของอุปกรณ์ฯ เป็นต้น จึงจำเป็นต้องมีขั้นตอนการแก้ไขความผิดพลาดของข้อมูลซิฟย์ระหว่างผู้ส่งและผู้รับ โดยวิธีการแก้ไขผิดพลาดแบบทั่วไป เริ่มต้นจากผู้ส่งทำการสร้างข้อมูล $\boldsymbol{M}$ ที่มีความสัมพันธ์เกี่ยวข้องกับกุญแจซิฟย์ของตน และส่ง $\boldsymbol{M}$ ไปให้ผู้รับผ่านช่องสัญญาณแบบทั่วไป จากนั้นผู้รับจะใช้ข้อมูล $\boldsymbol{M}$ ดังกล่าว ประมวลผลเพื่อตรวจสอบและแก้ไขความถูกต้องกับกุญแจซิฟย์ของตน เพื่อให้มีค่าที่ตรงกันระหว่างผู้ส่งกับผู้รับ ซึ่งเรียกขั้นตอนนี้ว่าการไกล่เกลี่ยความผิดพลาด และกุญแจซิฟย์ที่ถูกแก้ไขแล้ว (Reconciled key) จะถูกส่งเข้าสู่กระบวนการการขยายสภาวะส่วนตัวเพื่อกำเนิดเป็นกุญแจรหัสลับสุดท้าย

ขั้นตอนที่ 4 การขยายสภาวะส่วนตัว (Privacy amplification)

การขยายสภาวะส่วนตัวเป็นขั้นตอนการเพิ่มความปลอดภัยของข้อมูลกุญแจด้วยการลดความสัมพันธ์ข้อมูลที่ผู้ดักจับมีโอกาสได้รับไปในระหว่าง

กระบวนการต่างๆ ทั้งในช่องสัญญาณเชิงควอนตัมและช่องสัญญาณทั่วไปให้น้อยที่สุด โดยผู้ส่งและผู้รับนำกุญแจที่ถูกแก้ไขความผิดพลาดแล้ว (Reconciled key) คูณกับเมทริกซ์แบบไบนารี่ของฟังก์ชันแฮชเชิงเอกภพ (Universal hashing) เพื่อกำเนิดเป็นบิตข้อมูลกุญแจรหัสลับ (Secret key) ที่ไม่มีความสัมพันธ์กับข้อมูลของผู้ดักจับสำหรับการนำไปใช้งานระบบวิทยาการรหัสลับต่อไป [19]

โดยทั่วไปแล้ว สองขั้นตอนสุดท้ายของการกระจายกุญแจรหัสลับเชิงควอนตัม ได้แก่ การไกล่เกลี่ยความผิดพลาด และการขยายสภาวะส่วนตัว มีพื้นฐานการทำงานเช่นเดียวกับเทคนิคการสร้างข้อตกลงร่วมกันของข้อมูลกุญแจรหัสลับระหว่างสองฝั่งคู่สื่อสาร (Classical secret-key agreement) [20] หรือที่เรียกว่า การกลั่นกรองกุญแจรหัสลับ (Secret-key distillation) ที่มีการทำงานเกิดขึ้นบนช่องสัญญาณการสื่อสารโดยทั่วไป มีเป้าหมายหลักเพื่อการกำเนิดเป็นชุดข้อมูลของคู่สื่อสารระหว่างภาคส่งกับภาครับที่ได้รับการยืนยันความถูกต้องและความปลอดภัยจากผู้ไม่ประสงค์ดีโดยสมบูรณ์

2.2 การไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัม

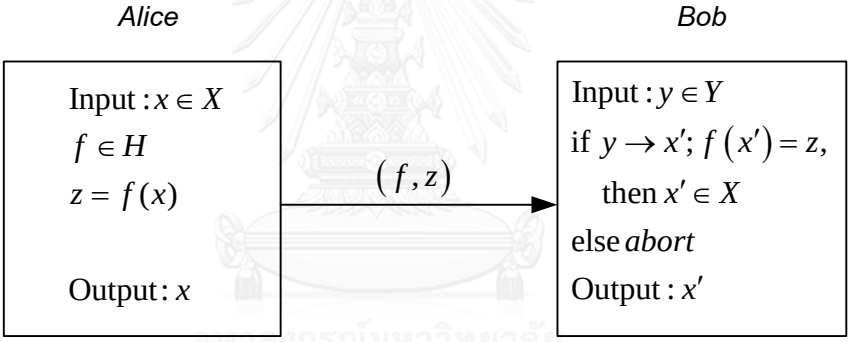
การไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัม (Quantum key reconciliation)ถือเป็นขั้นตอนหนึ่งที่สำคัญในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมเพื่อการแก้ไขความผิดพลาดและยืนยันความถูกต้องของข้อมูลกุญแจรหัสลับระหว่างผู้ส่งและผู้รับตัวจริงให้มีความปลอดภัยได้อย่างสูงสุด โดยอาศัยระบบการสื่อสารเพื่อแลกเปลี่ยนข้อมูลกันระหว่างผู้ส่งและผู้รับบนช่องสัญญาณแบบทั่วไปในปริมาณที่น้อยที่สุดเท่าที่คู่สื่อสารทั้งสองจะสามารถยืนยันความถูกต้องตรงกันของข้อมูลกุญแจรหัสลับได้

โดยเนื้อหาในส่วนนี้ จะกล่าวถึงนิยามรูปแบบของเทคนิคการไกล่เกลี่ยความผิดพลาดโดยทั่วไปภายใต้หลักพื้นฐานทางทฤษฎีข่าวสารสารสนเทศ ได้แก่ การไกล่เกลี่ยความผิดพลาดแบบทางเดียว (One-way reconciliation scheme) และการไกล่เกลี่ยความผิดพลาดบนพื้นฐานของการเข้ารหัสช่องสัญญาณ (Reconciliation scheme based on channel coding) ที่มีความสามารถในการแก้ไขความผิดพลาดได้ดีและสามารถนำมาประยุกต์ใช้งานในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (Discrete Variable Quantum Key Distribution: DV-QKD) ซึ่งเป็นระบบฯ ที่ได้รับการพัฒนาจนสามารถใช้งานได้จริงในปัจจุบัน

2.2.1 การไกล่เกลี่ยความผิดพลาดแบบทางเดียว

การไกล่เกลี่ยความผิดพลาดแบบทางเดียว (One-way reconciliation scheme) โดยทั่วไปมีเป้าหมายเพื่อให้ *Alice* ส่งข้อมูลที่มีความสัมพันธ์ร่วมกับกุญแจรหัสลับของตนที่น้อยที่สุดเท่าที่ *Bob* จะสามารถแก้ไขความผิดพลาดบนข้อมูลกุญแจรหัสลับให้มีค่าตรงกับของ *Alice* ได้ ซึ่งสามารถแสดงเป็นแบบจำลองการทำงานของระบบฯ ได้ดังรูปที่ 2.3 สมมติให้ *Alice* และ *Bob* มีข้อมูลกุญแจรหัสลับที่เกิดข้อผิดพลาดกัน เขียนแทนด้วยตัวแปร $x \in X$ และ $y \in Y$ ตามลำดับ และ H แทนฟังก์ชัน two-universal family of hash เพื่อการแปลง X ไปเป็น Z โดยที่ $f \in H$ จากข้อกำหนดข้างต้นสามารถแสดงเป็นขั้นตอนการไกล่เกลี่ยความผิดพลาดดังแผนผังดังนี้

ขั้นตอนที่ 1 *Alice* นำข้อมูล x มาประมวลผลด้วยฟังก์ชัน f เพื่อหาข้อมูลความสัมพันธ์ร่วมกับกุญแจรหัสลับ $z\left(z \in f(x)\right)$โดยที่ $z \in Z$ หลังจากนั้น *Alice* จึงส่งทั้ง f และผลลัพธ์ z ไปยัง *Bob*



รูปที่ 2.3 แบบจำลองการการไกล่เกลี่ยความผิดพลาดแบบทางเดียว

ขั้นตอนที่ 2 *Bob* นำข้อมูลทั้ง f และ z มาประมวลผลร่วมกับ y เพื่อคำนวณหาเอาท์พุต $x'\left(x' \in X\right)$ ที่เปรียบเสมือนเป็นข้อมูลกุญแจรหัสลับของ *Bob* ที่ได้รับการแก้ไขความผิดพลาดแล้ว โดยแบบจำลองดังกล่าวสามารถตรวจสอบความสำเร็จในการยืนยันความตรงกันของข้อมูล x' กับ x ได้เมื่อผลลัพธ์ของฟังก์ชัน $f(x') = z$ ถ้าไม่เช่นนั้น ระบบฯ จะล้มเหลวและยุติการแก้ไขความผิดพลาดดังกล่าว

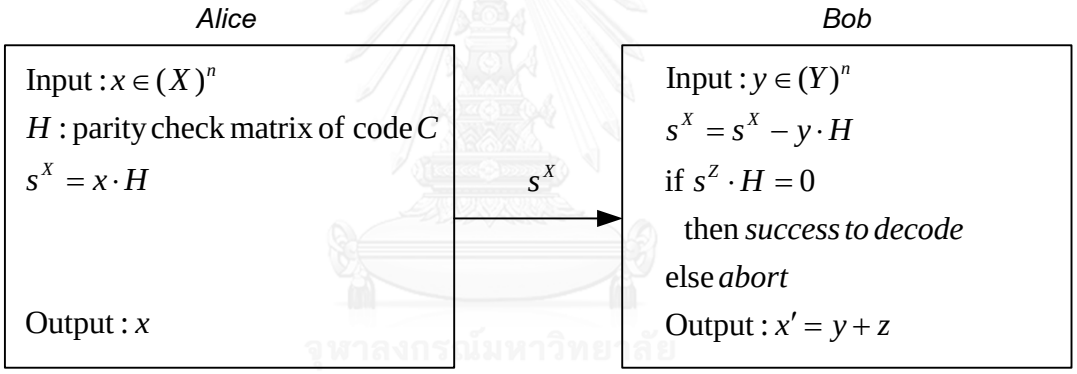
อย่างไรก็ตาม เนื่องจาก z เป็นข้อมูลที่มีความสัมพันธ์ร่วมกับกุญแจรหัสลับของทั้ง *Alice* และ *Bob* และมีโอกาสรั่วไหลไปยังผู้ดักจับข้อมูล *Eve* ได้ หากช่องสัญญาณการสื่อสารไม่มีความปลอดภัยโดยสมบูรณ์ ดังนั้น *Alice* จำเป็นต้องส่งข้อมูลไปยัง *Bob* ในปริมาณที่เหมาะสมเพียงพอสำหรับการแก้ไขความผิดพลาดได้ ซึ่งปริมาณข้อมูลที่รั่วไหลน้อยที่สุด จะสอดคล้องกับปริมาณค่าความสัมพันธ์ระหว่าง x กับ y หรือปริมาณข่าวสารตามเงื่อนไขร่วมกันสูงสุด (Maximum joint

entropy) $H_{\max}^{\phi}(X|Y)$ โดยที่ ϕ จะปลอดภัยได้ต้องขึ้นกับความน่าจะเป็นร่วมกันระหว่าง x กับ y หรือดังแสดงเป็นขอบเขตปริมาณข้อมูลที่รั่วไหลน้อยที่สุดบนการไกล่เกลี่ยความผิดพลาดแบบทางเดียวได้ตามอสมการที่ 2.1 [21]

$$leak_{\mathrm{Recon\{A,B\}}} \le H_{\max}\left(P_{XY}(x,y)|Y\right) + \log(2/\phi). \qquad (2.1)$$

2.2.2 การไกล่เกลี่ยความผิดพลาดบนพื้นฐานของการเข้ารหัสช่องสัญญาณ

รหัสช่องสัญญาณ (Channel coding) จะใช้เทคนิครหัสควบคุมความผิดพลาด (Error Control Coding: ECC) หรือรหัสแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correction: FEC) เพื่อการป้องกันและแก้ไขความผิดพลาดของข้อมูลในระบบการสื่อสารดิจิทัล ซึ่งในที่นี้ จะถูกนำมาประยุกต์ใช้งานเพื่อเป็นทางเลือกหนึ่งของกระบวนการไกล่เกลี่ยความผิดพลาดภายใต้พื้นฐานทางทฤษฎีข่าวสารสารสนเทศแบบทั่วไป โดยแสดงเป็นแบบจำลองของระบบฯ ได้ดังรูปที่ 2.4



รูปที่ 2.4 แบบจำลองการการไกล่เกลี่ยความผิดพลาดบนพื้นฐานของการเข้ารหัสช่องสัญญาณ

สมมติให้ *Alice* และ *Bob* มีชุดข้อมูลกุญแจรหัสลับที่เกิดข้อผิดพลาดกัน $x = \{x_1, x_2, ..., x_n\}$ และ $y = \{y_1, y_2, ..., y_n\}$ ตามลำดับ โดยที่ระบบฯ นี้ จะมีความปลอดภัยได้เมื่อ x และ y สอดคล้องกับเงื่อนไขของปริมาณความน่าจะเป็น $P_{xy}(x,y)$ เมื่อ C แทนรหัสควบคุมความผิดพลาดแบบบล็อกเชิงเส้น (Linear block code) ซึ่งมี เมทริกซ์ตรวจสอบความผิดพลาด H บน GF(q) (GF แทน *Galois Field*) จากข้อกำหนดข้างต้นสามารถแสดงเป็นขั้นตอนหลักของการไกล่เกลี่ยความผิดพลาดด้วยรหัสช่องสัญญาณดังนี้

ขั้นตอนที่ 1 การเข้ารหัส (Encoder) *Alice* เข้ารหัส เพื่อคำนวณหาค่าที่แสดงถึงลักษณะความผิดพลาดที่เกิดขึ้นกับชุดของข้อมูล หรือที่เรียกว่า ซินโดรม (Syndrome: s) โดยที่ หลังจากนั้นจึงส่งไปยัง Bob

ขั้นตอนที่ 2 การถอดรหัส (Decoder) Bob คำนวณหาค่าความแตกต่างระหว่างซินโดรมของชุดข้อมูล x และ y หรือ s^Z ได้โดย $s^Z = s^X - yH$ หาก $s^Z H = 0$ แสดงว่าการถอดรหัสทำได้สำเร็จ จากนั้น *Bob* จึงคำนวณหา z ได้จากการตรวจสอบหาตำแหน่งข้อผิดพลาด (Error pattern estimator) ภายใต้ C ผลลัพธ์ที่ได้คือ ข้อมูลกุญแจรหัสลับ x' ของ *Bob* ที่ได้รับการแก้ไขความผิดพลาดแล้วจาก $x' = z + y$

อย่างไรก็ตาม ข้อมูล s^X ในที่นี้ ถือเป็นข้อมูลที่มีความสัมพันธ์ร่วมกับกุญแจรหัสลับของทั้ง *Alice* และ *Bob* และถูกส่งผ่านช่องสัญญาณการสื่อสาร ซึ่งอาจรั่วไหลไปถึง *Eve* ได้เช่นกัน จากทฤษฎีการเข้ารหัสช่องสัญญาณ ปริมาณของ s^X ที่เหมาะสม เพื่อยืนยันความตรงกันระหว่างข้อมูล x' กับ x ต้องอยู่ภายใต้ขีดจำกัดของปริมาณข่าวสารร่วม (Mutual information , $I(X;Y)$) บิตต่อช่องสัญญาณหรือที่เรียกว่า "*ความจุของช่องสัญญาณ* (Channel capacity)"

เมื่อกำหนดให้ P_{XY} แทนปริมาณความน่าจะเป็นและ $\varphi > 0$ แล้วปริมาณข้อมูลที่รั่วไหลน้อยที่สุดภายใต้การไกล่เกลี่ยความผิดพลาดบนพื้นฐานของการเข้ารหัสช่องสัญญาณสามารถคำนวณได้ดังสมการที่ 2.2

$$leak_{\mathrm{Recon}\{C\}} = H\left(X \mid Y\right) + \varphi \tag{2.2}$$

2.3 ตัวอย่างโพรโทคอลการไกล่เกลี่ยความผิดพลาด

กระบวนการไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัมต่างมีรูปแบบและวิธีการที่แตกต่างกันไป ซึ่งบางวิธีการได้ถูกพัฒนาเป็นโพรโทคอลไกล่เกลี่ยความผิดพลาด (Reconciliation protocol) ที่ใช้งานได้จริงในระบบ QKD โดยตัวอย่างโพรโทคอลการไกล่เกลี่ยความผิดพลาดที่นิยมใช้งานจริงในระบบ DV-QKD เมื่อ *Alice* และ *Bob* ต่างมีข้อมูลกุญแจแบบไบนารี X และ Y จำนวน n บิต สามารถแสดงรายละเอียดและภาพรวมการทำงานได้ดังนี้

2.3.1 โพรโทคอลบีบีบีเอสเอส

โพรโทคอลบีบีบีเอสเอส (BBBSS Protocol) เป็นโพรโทคอลการไกล่เกลี่ยความผิดพลาดข้อมูลไบนารีชนิดแรก นำเสนอโดยชาร์ล เบนเนท (Charles H. Bennett) และคณะฯ ในปี ค.ศ.1991 จากบทความ "*Experimental Quantum Cryptography*" [1] ซึ่งมีพื้นฐานการแก้ไขความผิดพลาดเริ่มต้นจาก *Alice* และ *Bob* แบ่งข้อมูลกุญแจออกเป็นชุดๆ ตามขนาดของบล็อกที่เหมาะสม และคำนวณหาพาริตีบิตพร้อมการเปรียบเทียบในแต่ละบล็อกนั้นๆ หากบิตพาริตีของบล็อกใดมีค่าแตกต่างกันแล้ว *Alice* และ *Bob* จะค้นหาตำแหน่งบิตข้อมูลกุญแจที่ผิดพลาดด้วยการค้นหาแบบ

ไบนารี (Binary search) และดำเนินการแก้ไข โดยโพรโทคอลดังกล่าว จะมีการวนซ้ำรอบ (Iteration) การแก้ไขความผิดพลาดเรื่อยๆ เมื่อพิจารณาการแก้ไขความผิดพลาดในรอบที่ *i Alice* และ *Bob* จะเปิดเผยบิตพาริตีของแต่ละบล็อก $B_j^{(i)}$ ดังสมการที่ 2.3

$$Par_{X,j}^{(i)} = \sum_{t \in \Gamma_j^i} X_t, \text{ และ } Par_{Y,j}^{(i)} = \sum_{t \in \Gamma_j^i} Y_t, \tag{2.3}$$

ตามลำดับ ถ้าพาริตีของบล็อก $B_j^{(i)}$ มีค่าแตกต่างกันอัน $Par_{X,j}^{(i)} \neq Par_{Y,j}^{(i)}$ หมายถึงมีบิตกุญแจที่ผิดพลาดเป็นจำนวนคี่เกิดขึ้นในบล็อก $B_j^{(i)}$ หลังจากนั้นการค้นหาความผิดพลาดแบบไบนารีจะเริ่มต้นขึ้น (Binary search) และแก้ไขด้วยการกลับบิตผิดพลาดดังกล่าว โดยโพรโทคอลฯ นี้ จะมีการวนซ้ำรอบการแก้ไขความผิดพลาดไปจนกระทั่งมีการเปิดเผยจำนวนบิตพาริตีในปริมาณที่เพียงพอต่อการแก้ไขความผิดพลาดที่เกิดขึ้นในระบบ QKD อันสอดคล้องกับค่าอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัม (QBER) แต่อย่างไรก็ตามโพรโทคอลนี้พาริตีบิตสามารถตรวจสอบพบเพียงเมื่อมีความผิดพลาดเกิดขึ้นเป็นจำนวนคี่แต่จะไม่สามารถที่ตรวจพบความผิดพลาดเมื่อมีความผิดพลาดเกิดขึ้นเป็นจำนวนคู่ ดังนั้นหากต้องการทราบตำแหน่งกุญแจรหัสลับบิตที่ผิด ผู้ส่งและผู้รับจะแบ่งบล็อกกุญแจรหัสลับที่มีพาริตีบิตแตกต่างกันออกเป็นสองบล็อกแล้วเปรียบเทียบพาริตีบิตของบล็อกเหล่านั้นใหม่พร้อมกับตัดกุญแจรหัสลับบิตตำแหน่งสุดท้ายของบล็อกออกเพื่อลดข้อมูลเกี่ยวกับกุญแจรหัสลับที่บุคคลที่สามได้ไประหว่างการแก้ไขความผิดพลาด ซึ่งผู้ส่งและผู้รับจะทำเช่นนี้จนกว่าจะทราบตำแหน่งกุญแจรหัสลับที่ผิด

2.3.2 โพรโทคอลคาสเคด

โพรโทคอลคาสเคด (Cascade Protocol) เป็นหนึ่งในโพรโทคอลการแก้ไขความผิดพลาดข้อมูลไบนารีที่ได้รับความนิยม และถูกในมาประยุกต์ใช้งานจริงในระบบ QKD มากที่สุด พัฒนาขึ้นโดยกิลเลสบราสซาร์ด (Gilles Brassard) และหลุยส์ ซัลเวีย (Louis Salvail) ในบทความ “*Secret-Key Reconciliation by Public Discussion*” ปี 1994 [2] ซึ่งเป็นโพรโทคอลที่มีพื้นฐานการแก้ไขความผิดพลาดด้วยการค้นหาแบบไบนารีเช่นเดียวกับบีบีบีเอสเอส แต่มีการปรับปรุงระหว่างกระบวนการแก้ไขความผิดพลาด เนื่องจากในระหว่างกระบวนการแก้ไขความผิดพลาดของโพรโทคอลบีบีบีเอสเอส นี้จะทำการตัดกุญแจรหัสลับบิตในตำแหน่งสุดท้ายของแต่ละบล็อกออก การตัดกุญแจรหัสลับบิตเหล่านี้ออกส่งผลให้โพรโทคอลบีบีเอสเอสนี้มีความปลอดภัย สามารถลดข้อมูลเกี่ยวกับกุญแจรหัสลับบิตที่ *Eve* จะได้จากการเข้ามาขโมยระหว่างการแก้ไขความผิดพลาด แต่จะส่งผลต่อประสิทธิภาพในการแก้ไขความผิดพลาดของโพรโทคอลและจำนวนกุญแจรหัสลับบิตที่เหลือภายหลังจากการแก้ไขความผิดพลาด โพรโทคอลคาสเคดนี้จะไม่ทำการตัดกุญแจรหัสลับบิตใน

ตำแหน่งสุดท้ายของแต่ละบล็อกออก เพื่อเพิ่มประสิทธิภาพการแก้ไขความผิดพลาด และยังปรับปรุงประสิทธิภาพเพื่อเป้าหมายของการลดจำนวนข้อมูลที่เปิดเผยสู่ช่องสัญญาณในระหว่างกระบวนการ โดยการเพิ่มขั้นตอนการบันทึกข้อมูลกุญแจในแต่ละชุด ซึ่งหากพบความผิดพลาดของบิตข้อมูลใดๆ เกิดขึ้นใหม่แล้ว สามารถทำการตรวจสอบได้โดยการค้นหาแบบย้อนกลับจากข้อมูลที่บันทึกไว้ อันส่งผลให้ปริมาณบิตข้อมูลข่าวสารที่ส่งผ่านช่องสัญญาณมีจำนวนลดลง นอกจากนี้โพรโทคอลคาสคาดยังได้รับการปรับปรุงประสิทธิภาพดังตัวอย่างของงานวิจัย [22] ที่บล็อกของกุญแจในแต่ละรอบถูกทำให้มีขนาดที่เหมาะที่สุด เพื่อเป้าหมายของการเพิ่มประสิทธิภาพการแก้ไขความผิดพลาดไปสู่การใช้จำนวนบิตที่เปิดเผยในปริมาณที่ใกล้เคียงกับขอบเขตเชิงทฤษฎีให้มากที่สุด

2.3.3 โพรโทคอลวินนาว

โพรโทคอลวินนาว (Winnow Protocol) นี้มีพื้นฐานการแก้ไขความผิดพลาดเช่นเดียวกับบีบีบีเอสเอสและคาสเคด ถูกพัฒนาขึ้นในปี ค.ศ. 2003 โดยมีบัตเลอร์ (W. T. Buttler) และคณะเป็นผู้พัฒนาภายใต้การตีพิมพ์ในวารสารวิชาการ “*Fast, Efficient Error Reconciliation for Quantum Cryptography*” [3] ถึงแม้วินนาวจะอาศัยการเริ่มต้นด้วยการใช้พาริตีบิตในการตรวจสอบความผิดพลาดของชุดข้อมูลกุญแจในแต่ละบล็อกที่เกิดขึ้น แต่อัลกอริธึมในการค้นหาตำแหน่งและแก้ไขความผิดพลาดจะแตกต่างกับบีบีบีเอสเอสและคาสเคดที่อาศัยการค้นหาแบบไบนารีจึงทำให้มีการติดต่อการสื่อสารระหว่าง *Alice* กับ *Bob* เป็นจำนวนมาก ส่งผลให้เกิดความล่าช้าไม่เหมาะสมกับระบบฯ ที่ต้องการความเร็วสูง ด้วยเหตุนี้ วินนาวจึงนำหลักการของรหัสแฮมมิง (Hamming code) หนึ่งในประเภทของรหัสควบคุมความผิดพลาดชนิดหนึ่ง แทนการค้นหาตำแหน่งบิตผิดพลาดแบบไบนารี โดยเมื่อใดที่พบพาริตีของชุดกุญแจในแต่ละบล็อกระหว่าง *Alice* กับ *Bob* มีค่าไม่ตรงกันแล้ว การหาค่าแฮมมิงซินโดรม (Hamming syndrome) ของคู่สื่อสารทั้งสองจะเกิดขึ้นดังสมการที่ 2.4

$$S^X = \left(\sum_{j=1}^{N_h} X_i h_{i,j}^{(m)} \right) (mod\, 2) \in \{0,1\}^m \text{ และ } S^Y = \left(\sum_{j=1}^{N_h} Y_i h_{i,j}^{(m)} \right) (mod\, 2) \in \{0,1\}^m \quad (2.4)$$

ตามลำดับ โดยที่ $h_{i,j}^{(m)}$ คือ เมทริกซ์ตรวจสอบพาริตีของรหัสแฮมมิง (Parity check matrix) เมื่อใดที่ซินโดรมของ *Alice* กับ *Bob* มีความแตกต่างกันแล้ว $\left(S^{diff} = S^X \oplus S^Y \neq \{0\} \right)$ การค้นหาตำแหน่งบิตผิดพลาดจะถูกบ่งบอกได้จากค่าความแตกต่างของซินโดรม S^{diff} ดังกล่าว

นอกจากนี้ โพรโทคอลวินนาวยังมีขั้นตอนการรักษาความเป็นส่วนตัวด้วยการตัดบิตข้อมูลกุญแจรหัสลับเฉพาะบล็อกที่มีการแก้ไขความผิดพลาดแล้วเท่านั้นในตำแหน่ง 2^k โดยที่ k มีค่า

เท่ากับ $0,1,...,m-1$ โดยขนาดกุญแจรหัสที่ได้จากการแก้ไขความผิดพลาดด้วยวินนาวจะมีขนาดสั้นลงกว่ากุญแจดั้งเดิม

อย่างไรก็ตาม จากหลักการของรหัสแฮมมิงที่การแก้ไขความผิดพลาดทำเพียงเฉพาะบิตผิดพลาดจำนวนเพียงหนึ่งบิตในแต่ละบล็อก ดังนั้นวินนาวจึงมีโอกาสเกิดความล้มเหลวเมื่อใดก็ตามที่อัตราความผิดพลาดสูงเกินขีดความสามารถของรหัสแฮมมิง ซึ่งในงานวิจัยของ [23] ได้นำเสนอการวิเคราะห์ขนาดของบล็อกที่เหมาะสมเพื่อโอกาสของความสำเร็จในการไกล่เกลี่ยความผิดพลาดบนเงื่อนไขของอัตราความผิดพลาดกุญแจรหัสลับระดับต่างๆ ที่เป็นไปได้ในระบบ QKD

บทที่ 3
ทฤษฎีข่าวสารสนเทศและรหัส

3.1 ทฤษฎีข่าวสารสนเทศ

การส่งข้อมูลผ่านระบบสื่อสารเพื่อให้การส่งมีประสิทธิภาพสูงสุด ข้อมูลข่าวสารที่ต้องการส่งจะถูกบีบอัดเพื่อให้ปริมาณข่าวสารที่ส่งมีขนาดเล็กที่สุดที่ภาคเข้ารหัสแหล่งกำเนิด ซึ่งการที่จะศึกษาเรื่องของการเข้ารหัสแหล่งกำเนิดจะต้องศึกษาในส่วนของแหล่งกำเนิดข่าวสาร และปริมาณข่าวสารที่สร้างจากแหล่งกำเนิด ตามทฤษฎีข่าวสาร (Information Theory) ที่เสนอโดย C. Shannon [24] ซึ่งรายละเอียดมีดังต่อไปนี้

ปริมาณข่าวสารและปริมาณข่าวสารเฉลี่ย

กำหนดให้แหล่งกำเนิดข่าวสารแหล่งหนึ่งมีการสร้างข้อมูลข่าวสารออกมา M สัญลักษณ์ (Symbol) โดยข้อมูลแต่ละสัญลักษณ์ $\{x_1, x_2, .., x_M\}$ และความน่าจะเป็นในการเกิดข้อมูลข่าวสารในแต่ละสัญลักษณ์มีดังต่อไปนี้

$$P(X = x_i) = p_i \qquad \text{โดยที่ } i = 1, 2, 3, .., M$$

p_i คือความน่าจะเป็นที่แหล่งกำเนิดข่าวสารสร้างสัญลักษณ์ x_i
จากกฎความน่าจะเป็นผลรวมของความน่าจะเป็นของเหตุการณ์ที่เกิดขึ้นทั้งหมดมีค่าเท่ากับหนึ่ง ดังต่อไปนี้

$$\sum_{i=1}^{M} p_i = 1$$

โดยปริมาณข่าวสารที่สร้างจากแหล่งกำเนิดข่าวสารจะมีความสัมพันธ์กับ ความน่าจะเป็นในการเกิดข่าวสารนั้น เช่น หากภาคส่งทำการส่งข้อมูลข่าวสารชุดเดิมซ้ำกัน จะทำให้ภาครับได้รับปริมาณข่าวสารน้อยเนื่องจากความน่าจะเป็นในการเกิดข่าวสารนี้มีค่ามาก แต่หากภาครับได้รับข้อมูลข่าวสารชุดที่มีโอกาสในการส่งมาน้อย หรือข้อมูลข่าวสารที่ไม่เคยได้รับมาก่อนจะทำให้ภาครับได้รับปริมาณข่าวสารมาก เนื่องจากความน่าจะเป็นในการเกิดข่าวสารนั้นมีค่าน้อย ซึ่งปริมาณข่าวสารแสดงได้ดังสมการที่ (3.1)

$$I(x_i) = \log_a \frac{1}{p_i} \quad \text{โดยที่ } i = 1, 2, 3, ..., M \tag{3.1}$$

I คือปริมาณข่าวสารที่สร้างจากแหล่งกำเนิดข่าวสารเมื่อ a คือ ฐาน (base) ของฟังก์ชั่นลอการิทึม และถ้า $a=2$ ปริมาณข่าวสารมีหน่วยเป็นบิต (bit) จะได้ $I(x_k)=\log_2(1/p_k)=-\log_2(p_k)$ บิต หากพิจารณาแหล่งกำเนิดข่าวสารหนึ่งในแต่ละเวลาจะพบว่าปริมาณข่าวสารที่แหล่งกำเนิดนั้นสร้างขึ้น จะมีปริมาณข่าวสารที่ไม่เท่ากัน ส่งผลให้การออกแบบระบบสื่อสารให้มีประสิทธิภาพทำได้ด้วยความยากลำบาก ดังนั้นผู้ออกแบบจึงนิยมใช้ปริมาณข่าวสารเฉลี่ยมาใช้ในการวิเคราะห์และออกแบบระบบสื่อสาร ซึ่งปริมาณข่าวสารเฉลี่ยหรือเอนโทรปี (Entropy) สามารถแสดงได้ดังต่อไปนี้

$$\begin{aligned} H(X) &= E[I_i] \\ &= \sum_{i=1}^{M} p_i I(x_i) \\ &= \sum_{i=1}^{M} p_i \log_2\left(\frac{1}{p_i}\right) \\ &= -\sum_{i=1}^{M} p_i \log_2(p_i) \end{aligned} \tag{3.2}$$

$H(X)$ คือปริมาณข่าวสารเฉลี่ยที่สร้างจากแหล่งกำเนิด มีหน่วยเป็นบิตต่อสัญลักษณ์ (bit per symbol)

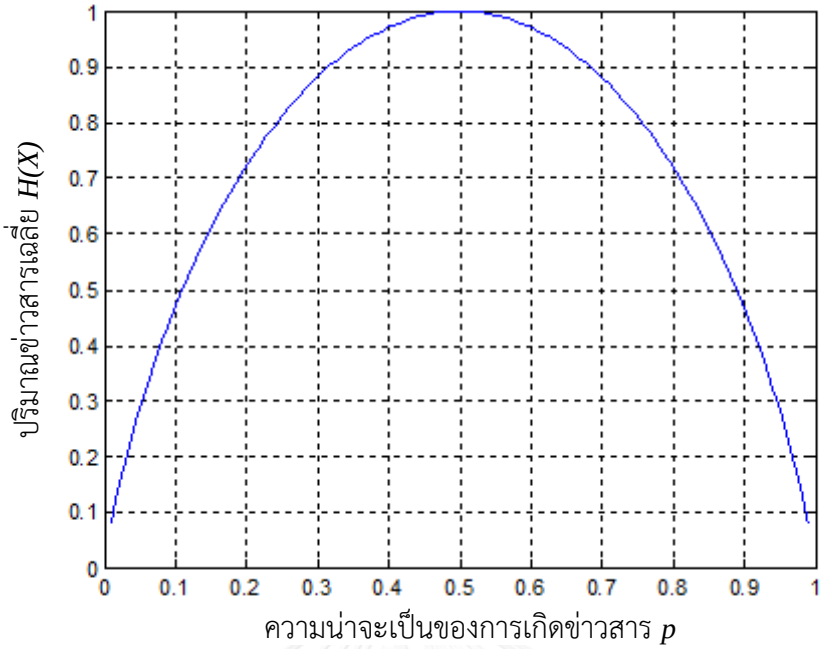
ในกรณีที่แหล่งกำเนิดข่าวสาร สร้างข่าวสารที่มีความน่าจะเป็นในการเกิดเท่ากันทุกสัญลักษณ์ จะทำให้ปริมาณข่าวสารเฉลี่ยจะมีค่ามากที่สุดเช่น กำหนดให้แหล่งกำเนิดสร้างข้อมูลข่าวสารสองชนิดที่มีความน่าจะเป็นในการเกิดข้อมูลข่าวสารชนิดแรกเท่ากับ p และความน่าจะเป็นในการเกิดข้อมูลข่าวสารชนิดที่สองเท่ากับ $1-p$ ปริมาณข่าวสารเฉลี่ยแสดงได้ดังนี้

$$H(X) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{3.3}$$

ซึ่งปริมาณข่าวสารเฉลี่ยของแหล่งกำเนิดนี้แสดงได้ดังรูปที่ 3.1 โดยจากรูปสามารถสรุปได้ว่าปริมาณข่าวสารเฉลี่ยของแหล่งกำเนิดใดๆ จะมีค่ามากที่สุดก็ต่อเมื่อข้อมูลข่าวสารที่สร้างจากแหล่งกำเนิดนั้นมีความน่าจะเป็นในการเกิดเท่ากันทั้งหมดทุกสัญลักษณ์ ดังนั้นค่าปริมาณข่าวสารเฉลี่ยจะมีคุณสมบัติดังต่อไปนี้

$$0 \le H(X) \le \log_2(M) \tag{3.4}$$

M คือจำนวนข่าวสารที่แหล่งกำเนิดนั้นสร้างขึ้น



รูปที่ 3.1 ปริมาณข่าวสารเฉลี่ยของแหล่งกำเนิดข้อมูลข่าวสารสองสัญลักษณ์

3.2 รหัสช่องสัญญาณ

การส่งข้อมูลดิจิทัลในระบบการสื่อสารทั่วไปนั้นมักเกิดการรบกวนของข้อมูลจากช่องสัญญาณทำให้การส่งข้อมูลนั้นเกิดความผิดพลาดได้เสมอ เพื่อที่จะต้องการให้ระบบการสื่อสารมีความถูกต้องน่าเชื่อถือจึงมีการคิดค้นการเข้ารหัสช่องสัญญาณเกิดขึ้นเพื่อใช้ในการตรวจจับข้อผิดพลาดโดยวิธีการเข้ารหัสช่องสัญญาณนั้นสามารถแบ่งได้ 2 ประเภทคือการแก้ไขความผิดพลาดแบบส่งซ้ำอัตโนมัติ (Automatic repeat request : ARQ) และการแก้ไขข้อผิดพลาดแบบข้างหน้า (Forward Error Correction : FEC) ซึ่งทั้ง 2 แบบที่ว่ามานี้จะมีการเพิ่มจำนวนบิตที่เรียกว่าพาริตีบิตที่ใช้ในการตรวจสอบข้อผิดพลาด แต่ที่ต่างกันคือ การเข้ารหัสข้อมูลแบบ ARQ เป็นการนำคุณสมบัติของการตรวจจับความผิดพลาดของรหัสมาใช้งาน ระบบที่ใช้หลักการนี้มีการนำคำรหัสที่รับได้มาทำการตรวจจับความผิดพลาดที่เกิดขึ้น หากพบว่าข้อมูลที่ถอดรหัสได้เกิดความผิดพลาด ก็จะดำเนินการขอ(Request) ให้ส่งข้อมูลดังกล่าวมาอีกครั้งหนึ่งรูปแบบของการรับและส่งข้อมูลมีหลายรูปแบบ (Protocol) เช่น แบบหยุดและรอ (Stop & Wait) แบบถอยหลัง (Go-Back-N) และแบบเลือกส่ง (Selective repeat) การเข้ารหัสในลักษณะนี้เหมาะการการใช้ในระบบประเภทที่ต้องการความถูกต้องของข้อมูลสูงและค่าการประวิงเวลาไม่เป็นเรื่องสำคัญ เช่น ระบบการสื่อสา ข้อมูลคอมพิวเตอร์

เป็นต้น ส่วนการเข้ารหัสข้อมูลแบบ FEC นั้น เป็นการนำคุณสมบัติ ในการแก้ไขความผิดพลาดมาใช้งานมีการนำคำรหัส ที่รับได้ที่ภาครับมาประมวลผลเพื่อกำเนิดบิตข่าวสาร พร้อมทั้งทำการแก้ไขบิตข่าวสารได้เองที่คาดว่าเกิดความผิดพลาดขึ้น การแก้ไขความผิดพลาดแบบล่วงหน้านิยมแบ่งออกเป็นสองประเภท ได้แก่ รหัสแบบบล็อก (Block code) และรหัสคอนโวลูชัน (Convolution code) สำหรับรหัสแบบบล็อกเป็นรหัสที่นำบิตข่าวสารมาแบ่งเป็นบล็อกย่อยๆ ซึ่งมีขนาดเท่ากันเพื่อนำมาเข้าหรือถอดรหัส ผลลัพธ์ที่ได้จากการทำงาน ของภาคเข้าหรือถอดรหัส ณ เวลาใด ๆ จะขึ้นอยู่กับรูปแบบ ของข้อมูลที่ป้อนเข้าสู่วงจร ณ ขณะนั้น รหัสแต่ละประเภทมีรูปแบบการเข้าและถอดรหัสรวมทั้งมีขีดความสามารถของการป้องกันความผิดพลาดที่แตกต่างกัน สำหรับรหัสแบบคอนโวลูชันเป็นการเข้ารหัสข้อมูล ในลักษณะต่อเนื่องมากกว่ารหัสแบบบล็อก มีการนำอุปกรณ์ประเภทหน่วยความจำมาใช้ที่ภาคเข้ารหัสเพื่อให้สามารถนำบิตข่าวสารที่ถูกป้อนเข้าสู่วงจร ณ ในอดีตมาคำนวณร่วมกับข้อมูลที่ป้อนเข้ามา ณ ปัจจุบันการเข้ารหัสแบบ FEC นี้เหมาะสมสำหรับการสื่อสารข้อมูลที่ต้องการความต่อเนื่อง เช่น ระบบโทรศัพท์เคลื่อนที่ และฮาร์ดดิสก์เป็นต้น

3.2.1 รหัสช่องสัญญาณแบบบล็อกเชิงเส้น

รหัสบล็อกเชิงเส้นจัดว่าเป็นรหัสที่ได้รับความนิยมอย่างสูงในทฤษฎีช่องสัญญาณ โดยมีคุณสมบัติคือเมื่อนำคำรหัส 2 คำใด ๆ มาทำการบวกแบบมอดูโล (modulo) จะได้คำรหัสอีกคำรหัสจากชื่อที่ถูกเรียกว่ารหัสบล็อกนั้นมาจากการเข้ารหัสข้อมูลที่ต้องการส่งออกจะถูกแบ่งออกเป็นบล็อกที่มีจำนวนบิตเท่า ๆ กันสมมติให้มีจำนวน k บิตจากนั้นจึงทำการเข้ารหัสแต่ละบล็อกของข้อมูลให้เป็นคำรหัสที่มีจำนวน n บิต เท่า ๆ กัน ซึ่งมีจำนวนมากกว่าจำนวนบิตข้อมูลของแต่ละบล็อกสมมติให้มีจำนวน $n > k$ บิต เนื่องจากจำนวนบิตที่เพิ่มขึ้นย่อมหมายถึงการใช้พลังงานในการส่งสัญญาณเพิ่มขึ้นจึงต้องมีการระบุอัตราของการเข้ารหัสซึ่งคืออัตราส่วนระหว่างจำนวนสัญลักษณ์ข้อมูลหนึ่งบล็อกต่อจำนวนสัญลักษณ์ของคำรหัสในที่นี้เท่ากับ $R = k / n$ นั่นเองโดยอัตราของการเข้ารหัสนี้จะต้องนำไปชดเชยค่าอัตราสวนของสัญญาณระหวางสัญญาณที่ต่องการกับสัญญาณรบกวน(Signal to Noise Ratio : SNR) ที่สามารถลดลงได้ในตอนคำนวณอัตรารหัสเพื่อให้อัตรารหัสที่คำนวณได้เป็นประโยชน์ที่ได้รับอย่างแท้จริง

3.2.2 รหัสแอลดีพีซี

รหัสแอลดีพีซีจัดเป็นรหัสบล็อกเชิงเส้น (linear block code) ประเภทหนึ่ง ที่ถูกค้นพบขึ้นเมื่อปี ค.ศ. 1960 โดยโรเบิร์ต กัลลาเกอร์ [25] แต่ในเวลานั้นรหัสชนิดนี้ยังไม่ได้รับความสนใจเท่าใด

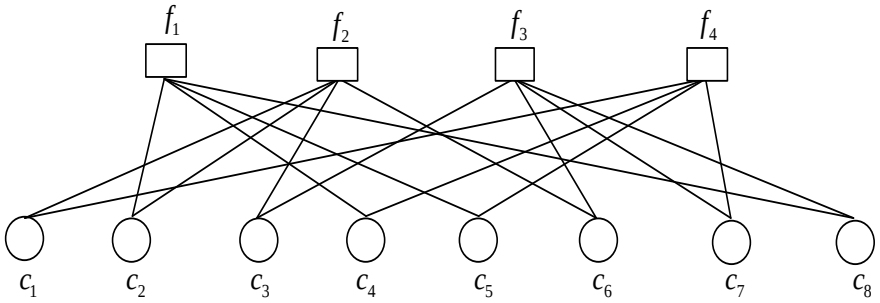
นัก เพราะเทคโนโลยีทางฮาร์ดแวร์ยังมีข้อจำกัดอยู่มาก อีกทั้งในเวลาที่ไล่เลี่ยกันนั้นได้มีการการค้นพบรหัสรีดโซโลมอน (Reed Solomon) ซึ่งมีคุณสมบัติที่ดีและเหมาะสมกับการประยุกต์ใช้งานในทางปฏิบัติมากกว่า จนกระทั่งประมาณ 30 ปีถัดมา จอห์น แมคเคย์และคณะฯ [28] ได้นำรหัสแอลดีพีซีมาพัฒนาต่อ จนทำให้รหัสชนิดนี้ได้รับความสนใจอย่างมากในปัจจุบัน

3.2.2.1 คุณลักษณะพื้นฐานของรหัสแอลดีพีซี

คุณลักษณะพื้นฐานที่สำคัญของรหัสแอลดีพีซีคือเป็นรหัสบล็อกเชิงเส้นที่เมทริกซ์พาริตี (Parity check matrix) $\mathbf{H}$ ที่มีตัวเลข 1 หรือในกรณีนอนไบนารี่มากกว่าหรือเท่ากับ 1 (ไม่ใช่ศูนย์)อยู่จำนวนน้อย (มีความหนาแน่นต่ำ) เมื่อเทียบกับเลข 0 การแสดงรหัสแอลดีพีซีนั้นสามารถทำได้ 2 แบบ คือ

1. การแสดงด้วยเมทริกซ์ $\mathbf{H}=\left(h_{ij}\right)_{m\times n}$ ที่มีขนาด $m\times n$ โดย m คือจำนวนบิตข้อมูล และ n คือจำนวนบิตของคำรหัส
2. การแสดงด้วยกราฟแทนเนอร์ (Tanner graph) ซึ่งเป็นกราฟที่ประกอบด้วยโนดตัวแปร (variable node) จำนวน n ตัวและโนดตรวจสอบ (check node) จำนวน m ตัว โดยมีเส้นเชื่อมต่อระหว่างโนดทั้งสองชนิด

$$\mathbf{H}=\begin{bmatrix}0&1&0&1&1&0&0&1\\1&1&1&0&0&1&0&0\\0&0&1&0&0&1&1&1\\1&0&0&1&1&0&1&0\end{bmatrix} \tag{3.5}$$



รูปที่ 3.2 การเชื่อมต่อของโนดตัวแปรและโนดตรวจสอบของรหัสแอลดีพีซี

เมทริกซ์พาริตีเช็ก (สมการที่ 3.5) สามารถแสดงแทนได้ด้วยกราฟแทนเนอร์ซึ่งอยู่ในรูปกราฟไบพาร์ไทร์ (bipartite graph) หมายถึง โนดสองโนดมีการแลกเปลี่ยนข้อมูลระหว่างกันสองโนดเท่านั้น ได้แก่โนดตัวแปร (c_node) และโนดตรวจสอบ (f_node) (รูปที่ 3.3) ซึ่งจะทำการแลกเปลี่ยนข้อมูลระหว่างกันเพื่อตรวจสอบความผิดพลาดของข้อมูลที่ส่ง โดยการแลกเปลี่ยนข้อมูลจะสิ้นสุดเมื่อข้อมูลมีความถูกต้องทั้งหมด หรือครบจำนวนการวนรอบที่ระบุไว้

โดยแต่ละแถวในเมทริกซ์พาริตีเช็กแทนโนดตราจสอบหรือสมการตรวจสอบ $f_i \mid i \in \{1,2,...,m\}$ และแต่ละหลักในเมทริกซ์พาริตีเช็กแทนโนดตัวแปร $c_j \mid j \in \{1,2,...,n\}$ ตัวอย่างแถวแรกของเมทริกซ์ $\mathbf{H}$.ในสมการที่ 3.5 คือสมการตรวจสอบ $f_1 = c_2 \oplus c_4 \oplus c_5 \oplus c_8$ กราฟแทนเนอร์จะเชื่อมต่อกันก็ต่อเมื่อโนดตรวจสอบ i เชื่อมต่อกับโนดตัวแปร j ที่ไม่เท่ากับ 0 $(h_{ij} \neq 0)$ วงลูบ (cycles) ของกราฟแทนเนอร์คือเส้นทางเดิน (path) ของโนดตัวแปรจุดเริ่มต้นกับจุดสุดท้ายเป็นจุดเดียวกัน เช่น ในรูป 3.2 $c_3 \rightarrow f_2 \rightarrow c_6 \rightarrow f_3 \rightarrow c_3$ แสดงเส้นทางเดินของวงลูบที่น้อยที่สุดหรือเรียกว่าเกิร์ธ (girth) ในที่นี้มีค่าเท่ากับ 4 และรหัสแอลดีพีซีนั้นถ้าจะให้ได้ประสิทธิภาพที่ดีควรหลีกเลี่ยงเกิร์ธเท่ากับ 4

3.2.2.2 ประเภทของรหัสแอลดีพีซี

รหัสแอลดีพีซีสามารถแบ่งออกได้เป็น 2 ประเภท คือ

1. รหัสแอลดีพีซีแบบสม่ำเสมอ (regular LDPC codes) รหัสประเภทนี้จะมีจำนวน 1 ในเมทริกซ์ $\mathbf{H}$ ในแต่ละแถวเท่ากัน และจำนวน 1 ในแต่ละคอลัมน์ จะมีค่าเท่ากับ จำนวน 1 ในแต่ละแถวคูณด้วย (n/m)
2. รหัสแอลดีพีซีแบบไม่สม่ำเสมอ (irregular LDPC codes) รหัสประเภทนี้จะมีจำนวน 1 ในเมทริกซ์ $\mathbf{H}$ ในแต่ละแถวไม่เท่ากัน

3.2.2.3 เข้ารหัสแอลดีพีซี

พิจารณาการเข้ารหัสข้อมูล $\mathbf{m} = [m_1, m_2, m_3 ..., m_k]$ จำนวน k บิต แล้วได้คำรหัส $\mathbf{c} = [c_1, c_2, ..., c_n]$ จำนวน n บิต โดยจะมีโครงสร้างดังสมการ[26, 27]

$$\mathbf{c} = [m_1, m_2, ..., m_k, p_1, p_2, ..., p_{n-k}] \tag{3.6}$$

โดยมีบิตส่วนเกินที่เพิ่มเข้ามาเรียกว่า พาริตีบิต คือ $\mathbf{p} = [p_1, p_2, ..., p_{n-k}]$ จำนวน $n-k$ บิต ซึ่งรหัสแบบนี้จะถูกเรียกว่า รหัสแบบมีระบบ (systematic code) และอัตราส่วนของจำนวนบิต

ข้อมูลกับจำนวนบิตคำรหัสจะเรียกว่า อัตรารหัส (code rate) มีค่าเท่ากับ $R=\frac{k}{n}$ และ $0<R\leq 1$ เสมอ

การเข้ารหัสแอลดีพีซีนั้นสามารถกระทำได้ 2 แบบคือ การเข้ารหัสด้วยเมทริกซ์พาริตี $\mathbf{H}$ และการเข้ารหัสด้วยเมทริกต์กำเนิด $\mathbf{G}$ ดังนั้นเมื่อใช้รหัสแบบมีระบบ และต้องการเข้ารหัสข้อมูลสิ่งที่ต้องทำคือการหาบิตพาริตี $\mathbf{p}$ มาต่อกับบิตข้อมูล $\mathbf{m}$ ก็จะได้คำรหัส $\mathbf{c}$ ที่ต้องการ

การเข้ารหัสด้วยเมทริกซ์พาริตี $\mathbf{H}$

โดยทั่วไปแล้วรหัสแอลดีพีซีจะถูกกำหนดด้วยเมทริกซ์พาริตีเช็ก $\mathbf{H}$ ขนาด $m\times n$ ดังนั้นหาบิตพาริตี $\mathbf{p}$ จากเมทริกซ์พาริตี $\mathbf{H}$ โดยอาศัยความสัมพันธ์ดังนี้

$$\mathbf{H}_{m\times n}(\mathbf{c}_{1\times n})^{\mathrm{T}}=\mathbf{0}_{m\times 1} \tag{3.7}$$

เมื่อ $\mathbf{0}_{m\times 1}$ คือเวกเตอร์ศูนย์ จัดรูปเมทริกซ์ $\mathbf{H}$ ใหม่จะได้

$$\mathbf{H}=[\mathbf{H}_1\,|\,\mathbf{H}_2] \tag{3.8}$$

เมื่อ $\mathbf{H}_1$ มีขนาด $m\times k$ และ $\mathbf{H}_2$ มีขนาด $m\times(n-k)$ ดังนั้นแทนค่าสมการ (3.8) และสมการ (3.6) ลงในสมการ (3.7) จะได้

$$[\mathbf{H}_1\mathbf{H}_2]\begin{bmatrix}\mathbf{m}^{\mathrm{T}}\\ \mathbf{p}^{\mathrm{T}}\end{bmatrix}=\mathbf{0}$$

$$\mathbf{H}_1\mathbf{m}^{\mathrm{T}}+\mathbf{H}_2\mathbf{p}^{\mathrm{T}}=\mathbf{0}$$

$$\mathbf{p}^{\mathrm{T}}=(\mathbf{H}_2)^{-1}\mathbf{H}_1\mathbf{m}^{\mathrm{T}} \tag{3.9}$$

เนื่องจาก $\mathbf{H}_2$ เป็นเมทริกซ์จัสตุรัสจึงสามารถหาค่าผกผันได้ ($m=n-k$)

การเข้ารหัสด้วยเมทริกซ์กำเนิด $\mathbf{G}$

การสร้างคำรหัสจากเมทริกซ์กำเนิด $\mathbf{G}$ สามารถกระทำได้โดยง่ายดังนี้ นำบิตข้อมูล $\mathbf{m}$ จำนวน k บิต คูณด้วยเมทริกซ์กำเนิด $\mathbf{G}$ (Generator matrix) ซึ่งมีขนาดเป็น $k\times n$ โดยการคูณหรือบวกทั้งหมดจะกระทำแบบมอดูโล 2 แล้วจึงได้ผลคูณที่มี n สมาชิกเกิดเป็นคำรหัส

$$\mathbf{c}=\mathbf{m}_k\mathbf{G}_{k\times n}=[c_1,c_2,c_3,...,c_n]=[m_1,m_2,...,m_k,p_1,p_2,...,p_{n-k}] \tag{3.10}$$

ในกรณีของรหัสมีระบบ n แถวแรกของ Generator matrix จะต้องประกอบกันเป็นเมทริกซ์เอกลักษณ์

$$\mathbf{G}=[\mathbf{I}_k\,|\,\mathbf{G}_1]^{\mathrm{T}} \tag{3.11}$$

โดย $\mathbf{G}_1$ แทนสมาชิกอีก $k\times(n-k)$ แถวที่เหลือหรือกล่าวอีกนัยหนึ่งก็ $\mathbf{G}_1$ คือเมทริกซ์ของบิตพาริตีที่เพิ่มเข้ามา

$$\mathbf{G}_1=[\mathbf{p}_{k\times(n-k)}]=\begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} & \cdots & p_{1,(n-k)} \\ p_{2,1} & p_{2,2} & p_{2,3} & \cdots & p_{2,(n-k)} \\ p_{3,1} & p_{3,2} & p_{3,3} & \cdots & p_{3,(n-k)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k,1} & p_{k,2} & p_{k,3} & \cdots & p_{k,(n-k)} \end{bmatrix} \tag{3.12}$$

จากที่ได้กล่าวมาแล้วรหัสแอลดีพีซีจะถูกกำหนดด้วยเมทริกซ์พาริตีเช็ก $\mathbf{H}$ ดังนั้นจึงต้องมีการแปลงเมทริกซ์พาริตีเช็ก $\mathbf{H}$ ให้เป็นเมทริกซ์กำเนิด $\mathbf{G}$ โดยการทำ Gaussian Elimination ทั่วไปซึ่งมีคุณสมบัติ $\mathbf{HG}=0$

อย่างไรก็ตามในขั้นตอนการคูณเวคเตอร์สัญลักษณ์ข้อมูลด้วย Generator matrix นั้นสามารถลดปริมาณการคำนวณลงได้เนื่องจากสมาชิก k ตัวแรกของคำรหัสจะเป็นสัญลักษณ์ข้อมูลตามเวคเตอร์สัญลักษณ์ข้อมูลอยู่แล้วจึงคำนวณการคูณเฉพาะสมาชิก $n-k$ ตัวหลังเท่านั้น

3.2.2.4 การถอดรหัสแอลดีพีซี

การถอดรหัสแอลดีพีซีสามารถแบ่งออกได้ 3 แบบ คือ การถอดรหัสแบบฮาร์ด (hard decoding) คือ การตัดสินใจแบบหยาบข้อมูลที่ใช้ในการคำนวณจะเป็นแบบลอจิกหรือเลขจำนวนเต็ม เช่น bit flipping algorithm, majority logic การถอดรหัสแบบซอฟต์ (soft decoding) คือ การตัดสินใจแบบละเอียดโดยอาศัยความน่าจะเป็นข้อมูลที่ใช้ในการคำนวณจะละเอียดขึ้นคือเป็นเลขจำนวนจริงเช่น belief propagation algorithm, sum produce algorithm และการถอดรหัสแบบผสม (hybrid decoding) คือ การรวมกันทั้งทั้งการตัดสินใจทั้งสองแบบข้างต้น เช่น modified bit flipping algorithm [25][26]

การถอดรหัสไบนารีแอลดีพีซีโดยการตัดสินใจแบบซอฟต์

การถอดรหัสโดยการตัดสินใจแบบซอฟต์ (soft-decision) [28] นั้นมีพื้นฐานมาจากแนววิธี belief propagation algorithm (BPA) โดยจะอาศัยข่าวสารหรือความเชื่อจากช่องสัญญาณแต่ละบิต เป็นข่าวสารตั้งต้นสำหรับกระบวนการถอดรหัส อัลกอริทึม BPA จะทำการส่งผ่านหรือกระจายข่าวสารของแต่ละบิตดังกล่าวไปตามเส้นทางบนกราฟแทนเนอร์ (Tanner's graph) จนกว่าคำรหัสที่ถูกถอดรหัสจะทำให้ทุกสมการตรวจสอบ (parity check equation) เป็นจริง ซึ่งก็คือ

$f_i = 0 | i \in \{1,2,...,m\}$ ซึ่งการถอดรหัสแบบนี้ให้ผลที่ดี ก่อนที่จะแสดงถึงอัลกอริทึมของการตัดสินใจแบบซอฟต์ จะกำหนดนิยามของตัวแปรต่าง ๆ ดังนี้

- $P_j(1) = P_r(c_j = 1 | r_j) | j \in \{1,2,...,n\}$ และ $P_j(0) = P_r(c_j = 0 | r_j) | j \in \{1,2,...,n\}$ คือ ความน่าจะเป็นที่จะเป็นบิต 1 และบิต 0 ของคำรหัส c_j เมื่อรู้ค่าข้อมูลที่รับได้ r_j

  โดย $P_r(c_j = 1 | r_j) = 1/(1+e^{-2ar_j/\sigma^2})$ ในช่องสัญญาณสื่อสารที่มีสัญญาณรบกวนเกาส์เซียนสีขาวแบบบวก หรือ AWGN (additive white Gaussian noise) เมื่อ a คือ แอมปลิจูด (amplitude) และ σ^2 คือความแปรปรวน (variance) ของสัญญาณหรือ

  $P_r(c_j = 1 | r_j) = 1 - e$ ในช่องสื่อสารแบบสมมาตรไบนารี (Binary Symmetric Channel: BSC) เมื่อ e ความน่าจะเป็นตัดข้าม (Crossover probability)

- q_{ij} คือข่าวสารที่ถูกส่งโดยโนดตัวแปร c_j ไปยังโนดตรวจสอบ f_i ทุกๆ ข่าวสารจะประกอบด้วย $q_{ij}(0)$ และ $q_{ij}(1)$ ซึ่งขึ้นอยู่กับความเชื่อที่ว่า r_j เป็น 0 หรือ 1

- r_{ij} คือข่าวสารที่ถูกส่งจากโนดตรวจสอบ f_i ไปยังโนดบิต c_j เช่นกัน r_{ij} ก็จะประกอบด้วย $r_{ij}(0)$ และ $r_{ij}(1)$ ที่ระบุค่าความเชื่อว่า c_n เป็น 0 หรือ 1

สำหรับลำดับขั้นตอนของอัลกอริทึมการตัดสินใจแบบซอฟต์มีดังนี้

1. โนดตัวแปรทุกโนดตัวแปรจะส่งข่าวสาร q_{ij} โดยจะมีค่าเป็นไปได้ทั้งสองกรณีคือ $q_{ij}(1) = P_j(1)$ และ $q_{ij}(0) = 1 - P_j(1) = P_j(0)$ และกำหนดจำนวนรอบสูงสุดที่ใช้ในการถอดรหัส
2. โนดตรวจสอบคำนวณข่าวสารใหม่ : โนดตรวจสอบจะทำการคำนวณและส่งข่าวสารตอบกลับ r_{ij} โดย

$$r_{ij}(0) = \frac{1}{2} + \frac{1}{2} \prod_{j' \in V_i \setminus j} (1 - 2q_{ij'}(1)) \tag{3.13}$$

และ

$$r_{ij}(1) = 1 - r_{ij}(0) \tag{3.14}$$

สมการข้างต้นเป็นการคำนวณค่าความน่าจะเป็นที่จำนวนของโนดตัวแปรที่เป็น 1 (ยกเว้น c_j) เป็นเลขคู่ ค่าความน่าจะเป็นดังกล่าวนี้มีค่าเท่ากับความน่าจะเป็น $r_{ij}(0)$ นั่นคือเมื่อบิต c_j มีค่าเป็น 0 ข่าวสารที่คำนวณได้นี้ถูกส่งคืนกลับไปที่โนดตัวแปร c_j

โดย $V_i = \{ j \in \{1,2,...,n\} \mid h_{ij} \neq 0 \}$ แทนเซตของโนดตัวแปรที่เชื่อมต่อกับโนดตรวจสอบ f_i หรือเซตของสมาชิกในแถวที่ i ใน $\mathbf{H}$ ที่ไม่เป็นศูนย์เช่น $V_1 = \{2,4,5,8\}$ ดังในรูปที่ 3.3

$V_{i\setminus j} = \{ j \in \{1,2,...,n\} \mid h_{ij} \neq 0 \} \setminus \{ j \}$ แทนเซตของโนดตัวแปรที่เชื่อมต่อกับโนดตรวจสอบ f_i ยกเว้นตัวโนดตัวแปร c_j หรือเซตของสมาชิกในแถวที่ i ยกเว้นหลักที่ j ใน $\mathbf{H}$ ที่ไม่เป็นศูนย์ เช่น $V_{1\setminus 2} = \{4,5,8\}$

3. โนดบิตคำนวณข่าวสารของตนเองใหม่ : โนดบิตจะคำนวณข่าวสารของตนเองใหม่ ด้วยการผนวกรวมข่าวสารล่าสุดที่ได้จากโนดตรวจสอบเข้ากับข่าวสารตั้งต้นดั้งเดิมของตนเองที่รับได้จากช่องสัญญาณ ผลที่ได้ส่งกลับไปยังโนดตรวจสอบโดยใช้สมการดังนี้

$$q_{ij}(0) = K_{ij}(1-P_j) \prod_{i' \in C_{j\setminus i}} r_{i'j}(0) \tag{3.15}$$

และ

$$q_{ij}(1) = K_{ij}(P_j) \prod_{i' \in C_{j\setminus i}} r_{i'j}(1) \tag{3.16}$$

โดย $C_j = \{ i \in \{1,2,...,m\} \mid h_{ij} \neq 0 \}$ แทนเซตของโนดตรวจสอบที่เชื่อมต่อกับโนดตัวแปร c_j หรือเซตของสมาชิกในหลักที่ j ใน $\mathbf{H}$ ที่ไม่เป็นศูนย์ $C_1 = \{2,4\}$

$C_{j\setminus i} = \{ i \in \{1,2,...,m\} \mid h_{ij} \neq 0 \} \setminus \{ i \}$ แทนเซตของโนดตรวจสอบที่เชื่อมต่อกับโนดตัวแปร c_j ยกเว้นตัวโนดตรวจสอบ f_i หรือเซตของสมาชิกในหลักที่ j ยกเว้นแถวที่ i ใน $\mathbf{H}$ ที่ไม่เป็นศูนย์ เช่น $C_{1\setminus 2} = \{4\}$

ด้วยเหตุนี้ค่าคงที่ K_{ij} จะถูกเลือกเพื่อที่จะทำให้ $q_{ij}(0) + q_{ij}(1) = 1$

ในการคำนวณค่าประมาณของบิตโนด c_j หรือ $\hat{c}_j$ นั้น ทำได้โดยการคำนวณความน่าจะเป็นของบิต c_j ว่าจะเป็น 0 หรือ 1 และจะทำการเลือกค่าที่เป็นไปได้มากกว่า โดยใช้สมการดังต่อไปนี้

$$Q_j(0) = K_j(1-P_j(1)) \prod_{i \in C_j} r_{ij}(0) \tag{3.17}$$

และ

$$Q_j(1) = K_j P_j(1) \prod_{i \in C_j} r_{ij}(1) \tag{3.18}$$

โดยเลือกค่า K_j เพื่อให้ $Q_j(0) + Q_j(1) = 1$

สังเกตว่าการคำนวณมีความคล้ายคลึงกับการคำนวณค่า $q_{ij}(b) \mid b \in \{0,1\}$ แต่ต่างกันที่ $Q_j(b)$ จะคำนวณจากข่าวสาร ของทุก ๆ โนดตรวจสอบที่ใช้ และขั้นตอนสุดท้ายคำนวณคำรหัสที่จะได้ด้วยการตัดสินใจอย่างหยาบคือ

$$\hat{c}_j = \begin{cases} 1 & \text{if } Q_j(1) > Q_j(0) \\ 0 & \text{if } Q_j(1) < Q_j(0) \end{cases} \tag{3.19}$$

ในกรณีที่ $Q_j(0) = Q_j(1)$ ให้สุ่มเลือกค่า $\hat{c}_j$ ให้เป็น 0 หรือ 1 ด้วยความน่าจะเป็นที่เท่ากัน ถ้าการประมาณค่าคำรหัสมีความถูกต้องตามสมการตรวจสอบ $\mathbf{H}\hat{\mathbf{c}}^{\mathrm{T}} = \mathbf{0}$ หรือจำนวนรอบการวนซ้ำเกินค่าสูงสุดที่ได้ตั้งไว้ ก็จะสิ้นสุดกระบวนการถอดรหัส

4. กลับไปยังขั้นตอนที่ 2

จากที่ได้กล่าวไปแล้วข้างต้นการถอดรหัสโดยใช้การตัดสินใจแบบซอฟต์ BPA จะเห็นได้ว่าเกิดการคูณกันของค่าความน่าจะเป็นหลายครั้ง เนื่องจากการคูณกันของค่าที่น้อยกว่า 1 หลายครั้งจะทำให้ผลลัพธ์ที่ได้มีค่าเข้าใกล้ศูนย์ ซึ่งจะส่งผลต่อเสถียรภาพเชิงตัวเลขในการคำนวณ เมื่อใช้รหัสที่มีความยาวของบล็อกสูง ๆ และรอบการคำนวณที่สูงขึ้น ปัญหาในจุดนี้สามารถแก้ไขได้ด้วยการเปลี่ยนจากการคูณเป็นการบวกแทน ด้วยวิธีจัดรูปขั้นตอนการถอดรหัสให้อยู่ในรูปของอัตราสวนของความน่าจะเป็นในเทอมของล็อก (Log Likelihood Ratio: LLR) และขั้นตอนแบบนี้มักจะถูกเรียกว่าซัมโปรดักอัลกอรีทึม (Sum Product Algorithm :SPA) ซึ่งสรุปได้ดังต่อไปนี้

1. กำหนดค่าเริ่มต้น

$\eta_{ij} = 0$ เมื่อ η_{ij} คือ ข่าวสารที่ส่งจากโนดตรวจสอบที่ i ไปยังโนดบิตที่ j

L_c คือวามน่าเชื่อถือของช่องสัญญาณ (channel reliability)

$L_c = \frac{2}{\sigma^2}$ สำหรับช่องสัญญาณ AWGN และ

$L_c = \log((1-e)/e)$ สำหรับช่องสัญญาณ BSC

$L_j = L_c r_j$ เมื่อ L_j คือ อัตราส่วนความน่าจะเป็นลอการึทึม (LLR) ของบิตข้อมูลตัวที่ j

2. โนดตรวจสอบคำนวณข่าวสารใหม่ :โนดตรวจสอบจะทำการคำนวณและส่งข่าวสารตอบกลับ η_{ij} โดย

$$\eta_{ij} = -2\tanh^{-1}\left\{\prod_{j \in V_i \setminus j} \tanh\left(\frac{-(L_j - \eta_{ij'})}{2}\right)\right\} \tag{3.20}$$

3. โนดตัวแปรคำนวณข่าวสารของตนเองใหม่ : โนดบิตจะคอยคำนวณข่าวสารที่จะตอบกลับไปยังโนดตรวจสอบอยู่เสมอ ด้วยการผนวกรวมข่าวสารล่าสุดที่ได้จากโนดตรวจสอบเข้ากับข่าวสารตั้งต้นดั้งเดิมของตนเองที่รับได้จากช่องสัญญาณ ผลที่ได้ส่งกลับไปยังโนดตรวจสอบ ซึ่งมีการคำนวณตามสมการ

$$L_j = L_c r_j + \sum_{i \in C_j} \eta_{ij} \tag{3.21}$$

คำนวณข้อมูลถอดรหัสจากทุกๆ โนดตัวแปรจากความสัมพันธ์คือ

$$\hat{c}_j = \begin{cases} 1 & \text{if } L_j > 0 \\ 0 & \text{if } L_j < 0 \end{cases} \tag{3.22}$$

ในกรณีที่ $L_j(0) = L_j(1)$ ให้สุ่มเลือกค่า $\hat{c}_j$ ให้เป็น 0 หรือ 1 ด้วยความน่าจะเป็นที่เท่ากัน ถ้าการประมาณค่าคำรหัสมีความถูกต้องตามสมการตรวจสอบ $\mathbf{H}\hat{\mathbf{c}}^{\mathrm{T}} = \mathbf{0}$ หรือจำนวนรอบการวนซ้ำครบตามค่าสูงสุดที่ได้ตั้งไว้ ก็จะสิ้นสุดกระบวนการถอดรหัส

4. กลับไปยังขั้นตอนที่ 2

3.3. รหัสซลีเพียน-วูลฟ์

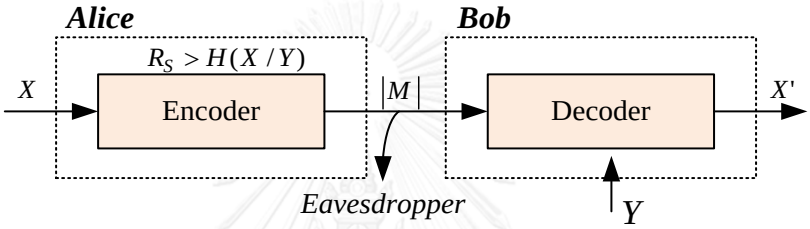
ปัญหาของรหัสซลีเพียน-วูลฟ์ (Slepian-Wolf Coding) เกี่ยวข้องกับการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารของสองแหล่งหรือมากกว่าถูกเรียกโดยทั่วไปว่า *"การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างเคียง(Source coding with side information)"* [29] ซึ่งรหัสซลีเพียน-วูลฟ์นี้ เป็นหลักสำคัญสำหรับการนำมาประยุกต์เพื่อแก้ไขปัญหาการไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัมโดยรหัสควบคุมความผิดพลาดได้เป็นอย่างดี

โดยเนื้อหาในส่วนนี้ จะกล่าวถึงนิยามโดยทั่วไปของรหัสซลีเพียน-วูลฟ์ และโครงสร้างของการแก้ไขปัญหาการไกล่เกลี่ยความผิดพลาดด้วยรหัสดังกล่าว รวมถึงความสัมพันธ์ระหว่างการเข้ารหัสซลีเพียน-วูลฟ์กับรหัสช่องสัญญาณ (Channel coding) สำหรับการนำรหัสควบคุมความผิดพลาดมาประยุกต์ใช้งานบนพื้นฐานการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างเคียง เพื่อวัตถุประสงค์ของการปรับปรุงประสิทธิภาพการไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัมต่อไป

เมื่อพิจารณาแหล่งกำเนิดจำนวนสองแหล่ง (ภาคส่งและภาครับ) ที่มีข้อมูล X ความสัมพันธ์กับข้อมูลข่าวสารข้างเคียง Y บนความน่าจะเป็น ตามลำดับ โดยที่ภาคส่งไม่ทราบข้อมูล Y ใดๆ ของภาครับ โดยกระบวนการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างเคียงเริ่มต้นจากภาคส่งทำการเข้ารหัสด้วยการบีบอัด (compression) ข้อมูล X ของตน โดยผลลัพธ์ที่ได้คือ ข้อมูลที่มี

ความสัมพันธ์กับ Y ในที่นี้เขียนแทนด้วย $|M|$ แล้วจึงส่ง $|M|$ ผ่านช่องสัญญาณการสื่อสารไปยังภาครับ ซึ่งขนาดของ $|M|$ จะสอดคล้องกับอัตราการบีบอัดข้อมูล ภายใต้เงื่อนไข ต่อจากนั้น ภาครับจะนำข้อมูล $|M|$ มาผ่านกระบวนการถอดรหัสร่วมกับข้อมูลข่าวสารข้างเคียง Y ของตน เพื่อกำหนดเป็นข้อมูลใหม่ของภาครับที่ได้รับการแก้ไขความผิดพลาดแล้ว เขียนแทนด้วย X' โดยสิ่งสำคัญที่ต้องพิ่งพิจารณาในการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างเคียงนี้คือ ปริมาณข้อมูลข่าวสารตามทฤษฎีที่ภาครับต้องการจากภาคส่ง เพื่อการแก้ไขความผิดพลาดบนข้อมูล Y ต้องมีค่าภายใต้ขอบเขตของรหัสซลีเพียน-วูลฟ์ ดังอสมการที่ 3.23

$$R_S \geq H\left(X \mid Y\right) \tag{3.23}$$



รูปที่ 3.3 การไกล่เกลี่ยความผิดพลาดบนพื้นฐานของรหัสซลีเพียน-วูลฟ์

โดยที่ภาคส่งทราบเพียงแค่ปริมาณความน่าจะเป็นของข้อมูลร่วม (Joint probability) ระหว่าง X กับ Y เท่านั้น และปริมาณข่าวสารตามเงื่อนไขร่วมกันระหว่าง $H(X \mid Y)$ คำนวณได้ดังสมการที่ 3.24

$$H(X \mid Y) = -e\log 2 - (1-e)\log(1-e) \tag{3.24}$$

ปัญหาของการไกล่เกลี่ยความผิดพลาดสามารถแก้ไขได้โดยรหัสซลีเพียน-วูลฟ์ ดังแสดงเป็นแผนผังการทำงานของระบบได้ในรูปที่ 3.3 โดยกุญแจรหัสลับของภาคส่ง (*Alice*) และภาครับ (*Bob*) เขียนแทนด้วยตัวแปรสุ่ม X และ Y ตามลำดับ มีความผิดพลาดเกิดขึ้นภายใต้ความน่าจะเป็น ซึ่งแสดงเป็นลำดับขั้นตอนการทำงานได้ดังนี้

ขั้นตอนที่ 1 การเข้ารหัส: *Alice* เข้ารหัสข้อมูล X และส่งผลลัพธ์ $|M|$ ไปยัง *Bob* ผ่านช่องสัญญาณการสื่อสารทั่วไป

ขั้นตอนที่ 2 การถอดรหัส: *Bob* ต้องการแก้ไขความผิดพลาดบนข้อมูล Y ให้มีค่าเท่ากับ X โดยการนำข้อมูล Y และ $|M|$ เข้าสู่กระบวนการถอดรหัส

โดยเป้าหมายของการไกล่เกลี่ยความผิดพลาดบนพื้นฐานของรหัสซลีเพียน-วูลฟ์นี้ คือ การแปลงข้อมูล X กับ Y ให้มีความสัมพันธ์อย่างสมบูรณ์ (Fully correlation) โดยที่ความน่าจะเป็นของ X เท่ากับ X' มีค่าเท่ากับ 1 $\{\Pr(X = X') = 1\}$ อย่างไรก็ตาม ข้อมูลที่ส่งผ่านช่องสัญญาณการสื่อสารทั่วไปในระหว่างการไกลเกลี่ยความผิดพลาด ในที่นี้คือ ข้อมูล $|M|$ มีโอกาสรั่วไหลไปถึงผู้ดักจับ (*Eve*) ได้เสมอ ดังนั้นประสิทธิภาพการไกล่เกลี่ยความผิดพลาดต้องขึ้นกับจำนวนบิตข้อมูล $|M|$ นี้ด้วย ซึ่งสอดคล้องกับปริมาณอัตราการเข้ารหัสซลีเพียน-วูลฟ์

เมื่อพิจารณาถึงการนำรหัสช่องสัญญาณหรือรหัสควบคุมความผิดพลาดมาประยุกต์ใช้งานบนพื้นฐานของระบบซลีเพียน-วูลฟ์ดังตัวอย่างการประยุกต์ใช้งานในเครือข่ายเซ็นเซอร์ไร้สายหรือระบบมัลติมีเดีย เป็นต้น จะเห็นได้ว่ารหัสซลีเพียน-วูลฟ์มีความสัมพันธ์เกี่ยวเนื่องกับรหัสช่องสัญญาณ โดยเมื่อให้ X และ Y เปรียบเสมือนกับอินพุตและเอาท์พุตบน GF(2) ที่ได้จากการจำลองการสื่อสารบนช่องสัญญาณแบบ BSC และ C แทนรหัสแบบบล็อกเชิงเส้นซึ่งมีเมทริกซ์ตรวจสอบพาริตี H ขนาด $M \times N$ ในระบบของซลีเพียน-วูลฟ์ ค่าซินโดรมสามารถคำนวณได้จากการบีบอัดข้อมูลอินพุต X คือ $S^M = X_N \mathbf{H}^T_{M \times N}$ โดยที่อัตราการบีบอัด $R_S = M / N$ คือ R_S อัตราส่วนของข้อมูลซินโดรมกับคำรหัสสามารถแสดงแทนได้ด้วย $R_c = (N - M) / N$ ซึ่งจะสอดคล้องกับอัตราการเข้ารหัสช่องสัญญาณ C ใดๆ เขียนแทนด้วย ดังนั้นความสัมพันธ์ระหว่างอัตราการบีบอัดของรหัสซลีเพียน-วูลฟ์กับอัตราการเข้ารหัสช่องสัญญาณแสดงได้ดังสมการที่ 3.25

$$R_S = 1 - R_C \tag{3.25}$$

อย่างไรก็ตาม เมื่อนำรหัสควบคุมความผิดพลาดมาประยุกต์ใช้งานเพื่อแก้ไขปัญหาการไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับเชิงควอนตัม อัตราการเข้ารหัสช่องสัญญาณ จำเป็นต้องทำให้มีค่าที่เหมาะสมที่สุดภายใต้ขอบเขตของรหัสซลีเพียน-วูลฟ์ $R_S \geq H(X \mid Y)$ ดังอสมการต่อไปนี้

$$\begin{aligned} 1 - R_C &\geq H(X \mid Y) \\ &\geq H(e) \end{aligned} \tag{3.26}$$

โดยที่ e คือ ความน่าจะเป็นแบบมีเงื่อนไขร่วมกันระหว่างข้อมูลกุญแจ X กับ Y ซึ่ง e ในระบบ QKD จะสอดคล้องกับอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัม (QBER) ที่แสดงถึงความน่าจะเป็นของข้อมูลร่วมระหว่าง *Alice Bob* และ *Eve* โดย สามารถคำนวณได้ดังสมการที่ 3.26

$$H(X \mid Y) = -e \log 2 - (1 - e) \log(1 - e) \tag{3.27}$$

3.4 การประเมินค่าอัตราการกำเนิดกุญแจรหัสลับเชิงควอนตัมและประสิทธิภาพการไกล่เกลี่ยความผิดพลาด

จากทฤษฎีข่าวสารสนเทศ (information & coding theorem) สามารถพิสูจน์เงื่อนไขความปลอดภัยบนอัตราการกำเนิดกุญแจรหัสลับที่ได้จากระบบ QKD โดยเนื้อหาในส่วนนี้ จะกล่าวถึงการพิสูจน์ถึงขอบเขตความปลอดภัยของกุญแจรหัสลับเมื่อผ่านกระบวนการไกล่เกลี่ยความผิดพลาดเสร็จสมบูรณ์ ที่ผู้ดักจับ (*Eve*) มีโอกาสได้รับข้อมูลอันมีความเกี่ยวพันกับกุญแจของภาคส่ง (*Alice*) และภาครับ (*Bob*) บนช่องสัญญาณเชิงควอนตัม และในระหว่างกระบวนการการไกล่เกลี่ยความผิดพลาด

โดยในการไกล่เกลี่ยความผิดพลาดแบบสมบูรณ์ อัตราการกำเนิดกุญแจรหัสลับเชิงทฤษฎีที่ได้หลังจากการไกล่เกลี่ยความผิดพลาดที่ปลอดภัย (secure reconciled key rate:) สามารถคำนวณได้ดังสมการที่ 3.28

$$\begin{aligned} r_{th} &= I\left(X;Y\right) - I(X:Z), \\ &= H(X) - H(X\,|\,Y) - \{H(X) - H(X\,|\,Z)\} \\ &= H\left(X\,|\,Z\right) - H(X\,|\,Y) \end{aligned} \tag{3.28}$$

โดยที่ $H(\cdot\,|\,\cdot)$ หมายถึง ปริมาณข่าวสารฟอนนอยมานน์ร่วมแบบมีเงื่อนไข (conditional Von Neumann entropy) ของ สารสนเทศเชิงควอนตัม แต่เนื่องจากการไกล่เกลี่ยความผิดพลาดเกิดขึ้นบนช่องสัญญาณแบบทั่วไป ดังนั้นปริมาณข่าวสารฟอนนอยมานน์ในที่นี้ เปรียบเสมือนปริมาณข่าวสารร่วมหรือแชนนอนแอนโทรปีในทฤษฎีข่าวสารสารสนเทศแบบทั่วไป โดย $H\left(X\,|\,Z\right)$ คือ ปริมาณข่าวสารร่วมแบบมีเงื่อนไขระหว่าง *Eve* ที่มีความสัมพันธ์กับข้อมูลกุญแจของ *Alice* และ $H(X\,|\,Y)$ แทนปริมาณข่าวสารที่ *Bob* ต้องการเพื่อการแก้ไขความผิดพลาดบนกุญแจของตนเอง

หากพิจารณาถึง ระบบการไกล่เกลี่ยความผิดพลาดที่เกิดขึ้นจริงนั้น ในเทอมของ $H(X\,|\,Y)$ จะสอดคล้องกับอัตราการบีบอัดของรหัสซลีเพียน-วูลฟ์ $(R_S \geq H(X\,|\,Y))$ ที่สามารถยืนยันความตรงกันของข้อมูลกุญแจระหว่าง *Alice* กับ *Bob* หลังเสร็จสิ้นกระบวนการไกล่เกลี่ยความผิดพลาดได้ $H(X\,|\,Y)$ จึงอาจมีค่ามากกว่าเชิงทฤษฎีในสมการที่ 3.28 ดังนั้นอัตราการกำเนิดกุญแจรหัสลับจริง (Actual secure reconciled key rate:) สามารถคำนวณได้ดังสมการที่ 3.29

$$r_{real} = H\left(X\,|\,Z\right) - f \cdot H(X\,|\,Y) \tag{3.29}$$

โดยที่ f คือ พารามิเตอร์แสดงประสิทธิภาพการไกล่เกลี่ยความผิดพลาด (Reconciliation efficiency) ซึ่งสามารถใช้เพื่อการประเมินค่าความสามารถการไกล่เกลี่ยความผิดพลาดแต่ละรูปแบบ

ได้เป็นอย่างดี โดยหากการไกล่เกลี่ยความผิดพลาดทำได้สมบูรณ์ ในที่นี้ f จะมีค่าเท่ากับ 1 และอัตราความผิดพลาดบิตในระบบ QKD (QBER) สูงสุดต้องมีค่าไม่เกิน 11% จึงจะทำให้ได้อัตราการกำเนิดกุญแจรหัสลับมีค่าเป็นบวกแสดงถึงความปลอดภัยภายใต้เงื่อนไขของทฤษฎีข่าวสารสนเทศดังรูปที่ 3.4 โดย $H(X|Z)=1-H(X|Y)$ [16] และสามารถพิสูจน์หาขอบเขตได้ดังนี้

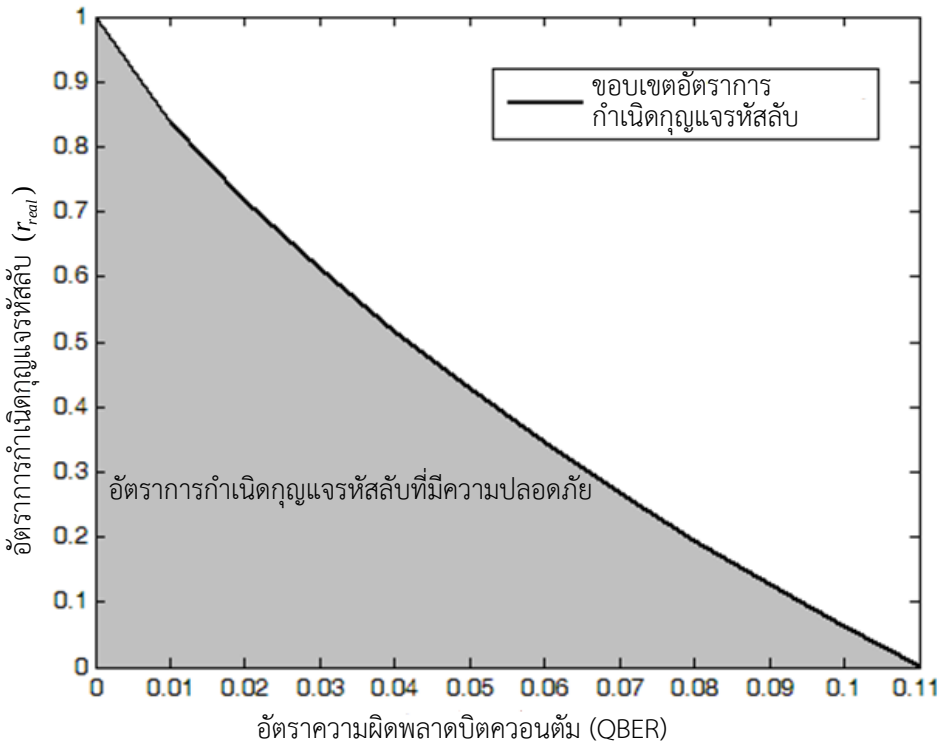
$$\begin{aligned} r_{real} &= H(X|Z) - f \cdot H(X|Y) \\ &= 1 - H(X|Y) - f \cdot H(X|Y) \\ &= 1 - (1+f) \cdot H(X|Y) \end{aligned} \tag{3.30}$$

เมื่อ $f=1$ และ $r_{real} \geq 0$ จะได้

$$\begin{aligned} 0 &\leq 1 - 2 \cdot H(X|Y) \\ H(X|Y) &\leq \frac{1}{2} \\ H(e) &\leq \frac{1}{2} \\ e &\leq 0.11\,(11\%) \end{aligned} \tag{3.31}$$

โดยประสิทธิภาพการไกล่เกลี่ยความผิดพลาดเมื่อนำรหัสควบคุมความผิดพลาดมาประยุกต์ใช้งาน สามารถคำนวณหาค่า ได้จากสมการที่ 3.29

$$f = \frac{R_S}{H(X|Y)} = \frac{1-R_C}{H(X|Y)} \tag{3.32}$$



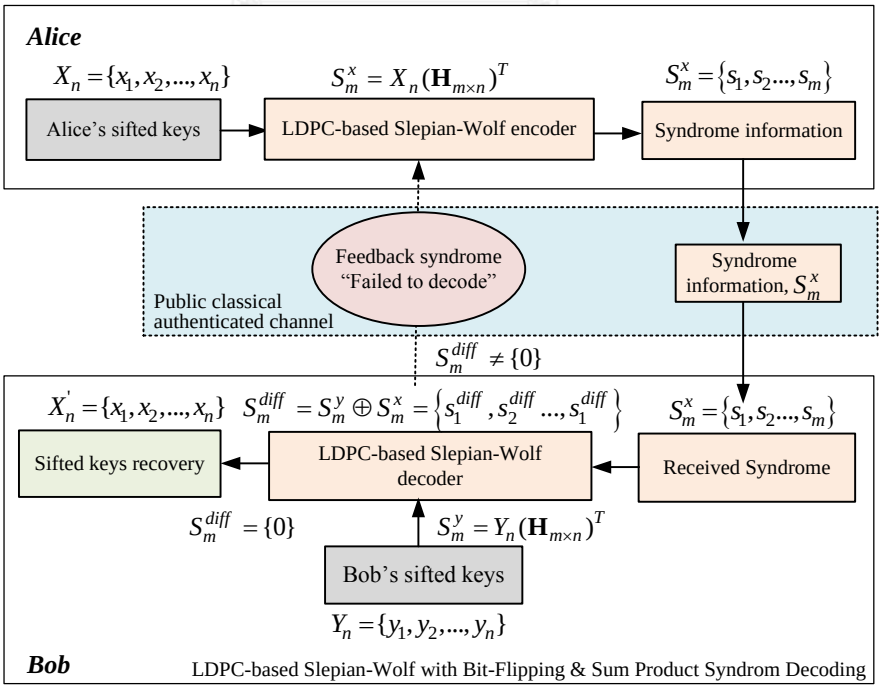
รูปที่ 3.4 ขอบเขตอัตราการกำเนิดกุญแจรหัสลับกับอัตราความผิดพลาดบิตควอนตัม

บทที่ 4
โพรโทคอลไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับที่นำเสนอ

ในบทนี้จะนำเสนอโพรโทคอลไกล่เกลี่ยความผิดพลาดด้วยรหัสแก้ไขความผิดพลาดแอลดีพีซีร่วมกับประกอบด้วยวิธีการดังต่อไปนี้ หัวข้อ 4.1 จะกล่าวถึงขั้นตอนวิธีการไกล่เกลี่ยความผิดพลาดความซับซ้อนต่ำโดยใช้การถอดรหัสแอลดีพีซีแบบบิตฟลิปปิงและแบบซัมโปรดักซินโดรม หัวข้อ 4.2 จะกล่าวถึงขั้นตอนการไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวได้ด้วยผลรวมของซินโดรม หัวข้อ 4.3 จะกล่าวถึงขั้นตอนการไกล่เกลี่ยความผิดพลาดอัตรารหัสแอลดีพีซีแบบปรับตัวได้โดยอาศัยเทคนิคการสุ่มบิตตำแหน่งพังเจอร์และชอร์ตเทนร่วมกับการประเมินช่องสัญญาณในที่นี้คือการประมาณความผิดพลาดกุญแจรหัสลับบิต (QBER) และการประมาณประสิทธิภาพการไกล่เกลี่ยความผิดพลาด

4.1 การไกล่เกลี่ยความผิดพลาดความซับซ้อนต่ำด้วยการถอดรหัสแอลดีพีซีแบบบิตฟลิปปิงและซัมโปรดักซินโดรม

ในหัวข้อนี้จะกล่าวถึงการประยุกต์ใช้การถอดรหัสแอลดีพีซี 2 แบบ คือแบบบิตฟลิปปิง (Bit-Flipping) ซึ่งเป็นการถอดรหัสแบบฮาร์ดและแบบซัมโปรดัก (Sum product) ซินโดรมซึ่งเป็นการถอดรหัสแบบซอร์ฟ แผนภาพแสดงการขั้นตอนการไกล่เกลี่ยความผิดพลาดดังรูปที่ 4.1



รูปที่ 4.1 วิธีการไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบบิตฟลิปปิงและซัมโปรดักซินโดรม

4.1.1 การไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบบิตฟลิปปิง

1. กำเนิดกุญแจรหัสลับ : *Alice* และ *Bob* กำเนิดกุญแจซิฟย์ที่มีความสัมพันธ์กัน X_n และ Y_n ตามลำดับ

2. การเข้ารหัส : *Alice* นำข้อมูลทั้งหมดลำดับ X_n เข้ารหัสซินโดรม $S_m^x = X_n(\mathbf{H}_{m\times n})^T$ แล้วส่งข้อมูลซินโดรม S_m^x ไปยัง Bob ผ่านช่องทางสัญญาณสื่อสารสาธารณะ

3. การเปรียบเทียบซินโดรม : *Bob* นำข้อมูลกุญแจซีฟคำนวณซินโดรม $S_m^Y = Y_n(\mathbf{H}_{m\times n})^T$ แล้วนำไปเปรียบเทียบกับซินโดรม S_m^x ที่ได้รับจาก *Alice* ผ่านทางช่องสัญญาณสาธารณะ

$$S_m^{diff} = S_m^x \oplus S_m^y. \tag{4.1}$$

กระบวนการไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบบิตฟลิปปิงเมื่อ $S_m^{diff} \neq \{0\}_m$ แต่ถ้าเมื่อ $S_m^{diff} = \{0\}_m$ ก็จะแสดงว่า *Alice* และ *Bob* มีกุญแจซิฟย์ที่มีค่าตรงกัน

4. การถอดรหัส : ถ้าซินโดรมมีความแตกต่างกันที่ได้จากขั้นตอนที่ 3 คือ $S_m^{diff} \neq \{0\}_m$ แล้ว Bob จะเข้ากระบวนการถอดรหัสโดยการหาตำแหน่งที่ไม่มีความน่าเชื่อจากโนดตรวจสอบ (check node) ของเมทริกซ์ $\mathbf{H}$ เพื่อจัดรูปแบบของความผิดพลาดของ *Bob* วิธีการถอดรหัสแบบบิตฟลิปปิงมีรายละเอียดอย่างง่ายดังนี้ [30, 31]

4.1 กำหนดค่าเริ่มต้น $l = 1$ รอบที่ใช้ในการถอดรหัส

4.2 รับข้อมูลแบบฮาร์ด $Y_n = (y_1, y_2, ..., y_n)$ เมื่อ Y_n คือกุญแจซิพท์ของ *Bob* และ $S_m^x = X_n(\mathbf{H}_{m\times n})^T$ เมื่อ S_m^x คือข้อมูลซินโดรมจากภาคส่ง

4.3 เปรียบเทียบซินโดรม กำหนดให้ $S_m^y = Y_n(\mathbf{H}_{m\times n})^T$ ถ้า $S_m^{diff} = S_m^x \oplus S_m^y = 0$ จะได้ Y_n เป็นข้อมูลที่ไม่มีความผิดพลาดและหยุดกระบวนการถอดรหัส

4.4 บิตฟลิปปิง

กำหนดให้ $E_j = \sum_{m\in C_j} (2\cdot S_m^{diff} - 1),\ j \in \{1,2,...,n\}$ ค่า E_j คือค่าความไม่น่าเชื่อถือที่ส่งผลกระทบต่อโดยตรวจสอบ

4.4.1 หาตำแหน่งที่ไม่น่าเชื่อของโนดตัวแปร ถ้า $\{j \mid (E_j > \theta)\} \neq \{\}$ เมื่อค่า θ ค่าขีดเริ่มต้น (Threshold) แล้วฟลิป (กลับ) ตำแหน่งบิตในเซตดังกล่าวทั้งหมด (โหมดหลายบิต)

4.4.2 ถ้า $j = \arg\max_{j\in\{1,2,...,n\}} E_j$ หาตำแหน่งที่มีความน่าไม่เชื่อถือมากที่สุดแล้วฟลิป (กลับ) บิตตรงตำแหน่งนั้น (โหมดบิตเดียว)

ขั้นตอนสุดท้ายถ้า $S_m^{diff} = 0$ สิ้นสุดกระบวนการถอดรหัสแต่ $S_m^{diff} \neq 0$ แจ้งกลับความล้มแล้วไปยังภาคส่งเพื่อแก้ไขใหม่อีกครั้ง การโดยการเลือกอัตราเข้ารหัสแอลดีพีซีลำดับถัดไปที่มีค่าลดลง

เพื่อให้มีการส่งค่าซินโดรมใหม่ไปมากขึ้น จนกระทั่งสามารถแก้ไขความผิดพลาดของข้อมูลกุญแจในบล็อกนั้นๆ ได้ดังแสดงไว้ที่รูปที่ 4.1

ตัวอย่างการถอดรหัสแอลดีพีซีอย่างง่ายแบบบิตฟลิปปิง

กำหนดให้กุญแจรหัส X_n และ Y_n มีค่าแตกต่างกันตำแหน่งที่ 8

$X_n = [0\ 1\ 1\ 0\ 1\ 1\ 0\ \underline{1}]$ $Y_n = [0\ 1\ 1\ 0\ 1\ 1\ 0\ \underline{0}]$

โดยใช้เมทริกซ์พารีตีเช็ก $\mathbf{H}$ ในรูปที่ 2.3

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

คำนวณค่าซินโดรมต่าง ๆ ได้ดังนี้

$S_m^x = X_n(\mathbf{H}_{m\times n})^T = [1\ 1\ 1\ 1]$ $S_m^y = Y_n(\mathbf{H}_{m\times n})^T = [0\ 1\ 0\ 1]$ และ $S_m^{diff} = [1\ 0\ 1\ 0]$

หาค่าความไม่น่าเชื่อของโนดตัวแปรที่มีผลกระทบต่อซินโดรม

$$E_j = \sum_{m\in C_j} (2\cdot S_m^{diff} - 1),\ j \in \{1,2,...,n\}$$

$= [-2\ 0\ 0\ 0\ 0\ 0\ 0\ 2]$

หาตำแหน่งที่มีความไม่น่าเชื่อมากที่สุดซึ่งก็คือตำแหน่ง 8 กลับบิตนั้นคือ $Y_8 = [1]$

4.1.2 การไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบซัมโปรดักซินโดรม

การไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบซัมโปรดักอัลกอริทึมเป็นการถอดรหัสแบบซอร์ฟที่มีความซับซ้อนต่ำซึ่งปรับปรุงมาจากการถอดรหัสแบบ belief propagation algorithm แสดงขั้นตอนการไกล่เกลี่ยความผิดพลาดดังรูป 4.1 และรายละเอียดดังนี้

1. กำเนิดกุญแจรหัสลับ : *Alice* และ *Bob* กำเนิดกุญแจซิฟย์ที่มีความสัมพันธ์กัน X_n และ Y_n ตามลำดับ กำหนดให้ $\Pr(X \neq Y) = e$ เมื่อ e อัตราความผิดพลาดควอนตัมบิต (QBER)

2. การเข้ารหัส : *Alice* นำข้อมูลทั้งหมดลำดับ X_n เข้ารหัสซินโดรม $S_m^x = X_n(\mathbf{H}_{m\times n})^T$ แล้วส่งข้อมูลซินโดรม S_m^x ไปยัง Bob ผ่านช่องทางสัญญาณสื่อสารสาธารณะ

3. การถอดรหัส : *Bob* นำข้อมูลซินโดรม S_m^x จาก Alice มาใช้แก้ไขความผิดพลาดร่วมกับข้อมูล Y_n ที่ *Bob* ซึ่งมีอยู่ก็คือข้อมูลข่าวสารข้างเคียง (side information) ข้อมูลนำเข้าของ Bob จะเป็นข้อมูลแบบซอร์ฟเพื่อนำสู่กระบวนการถอดรหัสคือ $L_c = \log((1-e)/e)(2Y_n - 1)$ ซึ่งหมายถึงการมอดูเลตแบบ Binary phase sift keying (BPSK) เปลี่ยนข้อมูล 0 เป็นร่วม -1 และ 1 เป็น 1 ก่อนเข้าสู่กระบวนการถอดรหัสแบบซัมโปรดักดังในหัวข้อ 3.2.2.4

ขั้นตอนสุดท้ายถ้า $S_m^{diff} = 0$ สิ้นสุดกระบวนการถอดรหัสแต่ $S_m^{diff} \neq 0$ แจ้งกลับความล้มแล้วไปยังภาคส่งเพื่อแก้ไขใหม่อีกครั้ง โดยการเลือกอัตราเข้ารหัสแอลดีพีซีที่มีค่าลดลงในลำดับถัดไป

การปรับปรุงการถอดรหัสชัมโปรดักซินโดรมแอลดีพีซี

การถอดรหัสซินโดรมแอลดีพีซีถูกนำมาประยุกต์ในการแก้ไขความความผิดพลาดร่วมรหัสซลีเพียน-วูลฟ์หรือรหัสข่าวสารข้างเคียงโดยได้มีการปรับปรุงขั้นตอนการถอดรหัสในส่วนของโนดตรวจสอบในสมการ (3.19) คือ [32]

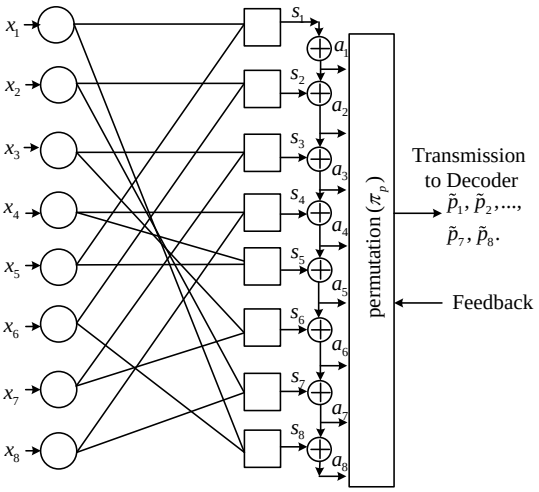
$$\eta_{ij} = (-1)^{S_m} \left\{ -2\tanh^{-1} \left\{ \prod_{j \in V_i \setminus j} \tanh\left(\frac{-(L_j - \eta_{ij'})}{2} \right) \right\} \right\} \quad (4.2)$$

เมื่อ S_m คือซินโดรมจากภาคส่ง และตรวจสอบกระบวนการสิ้นสุดการถอดรหัสเมื่อซินโดรมจากการถอดรหัสแล้วเท่ากับซินโดรมของภาคส่ง $\Pr(S^x = S^{x'}) = 1$

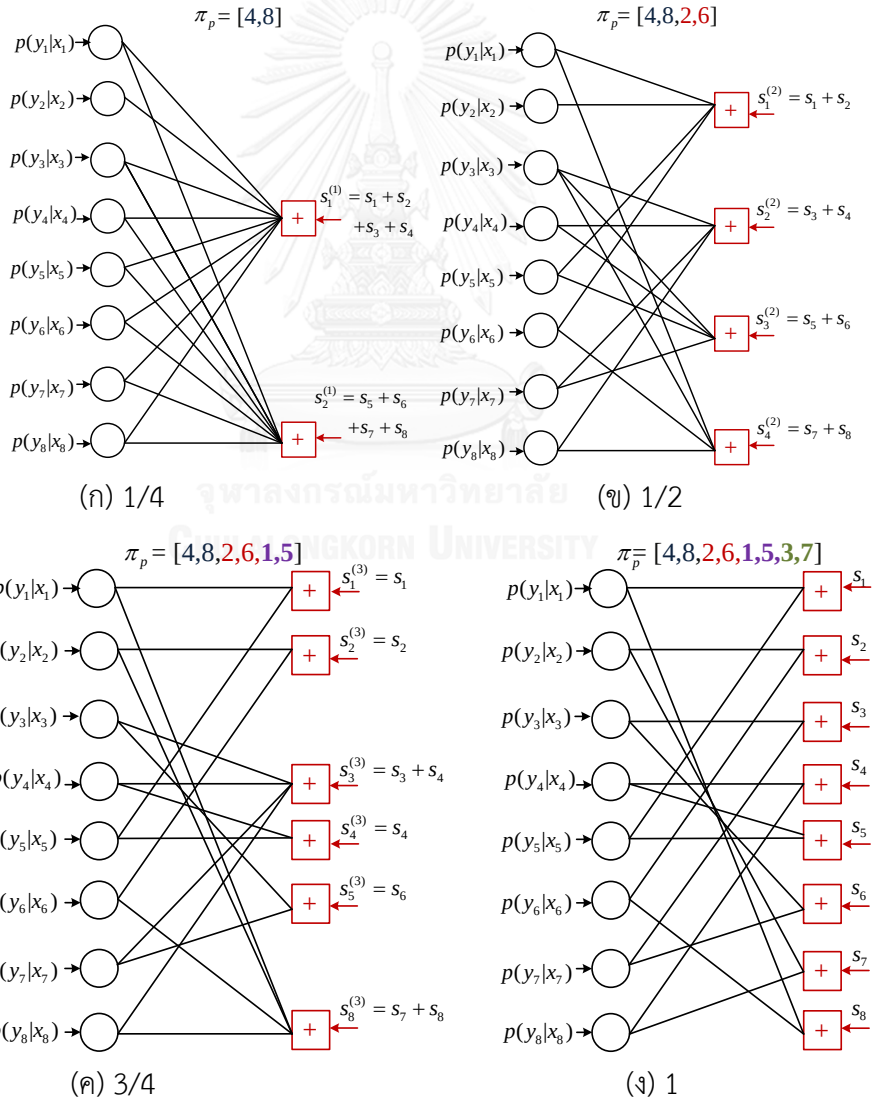
4.2 การไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวได้โดยผลรวมสะสมของซินโดรม

การไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวได้โดยผลรวมของซินโดรมเป็นวิธีแก้ไขความผิดพลาดแบบปรับอัตราการเข้ารหัสได้โดยอาศัยการเพิ่มผลรวมของข้อมูลซินโดรมของภาคส่งไปให้ภาครับเรื่อย ๆ จนกว่าจะแก้ไขความผิดพลาดได้ ที่ภาคการเข้ารหัสจะนำข้อมูล $\mathbf{x}$ มาคำนวณข้อมูลซินโดรม $s = \mathbf{x}\mathbf{H}^T = [s_1, s_2, ..., s_n]$ เมื่อ $\mathbf{H}$ คือพาริชีเช็กเมตริกร์ขนาด $n \times n$ มีอัตรารหัสเท่า 1 จากนั้นจะคำนวณผลรวมสะสมของซินโดรมจากข้อมูลทั้งหมด $\mathbf{a} = [a_1, a_2, ..., a_n]$ เมื่อ $a_j = \sum_{i=1}^{j} s_i \mid j \in \{1, 2, ..., n\}$ และทำการสลับตำแหน่งของ $\mathbf{a}$ ด้วยพารามิเตอร์สลับตำแหน่ง π จะได้ข้อมูลใหม่ $\tilde{\mathbf{p}} = [\tilde{p}_1, \tilde{p}_2, ..., \tilde{p}_n]$ แบ่งข้อมูลเก็บไว้บางส่วนและจะส่งข้อมูล $\tilde{\mathbf{p}}$ บางส่วนไปที่ภาครับดังตัวอย่างในรูปที่ 4.2 กำหนดให้มีจำนวนบิตทั้งหมด 8 บิตและมีพารามิเตอร์สลับตำแหน่งคือ $\pi_p = [4, 8, 2, 6, 1, 5, 3, 7]$ และกำหนดอัตรารหัสที่เป็นไปได้คือ $k = 4$ ดังนั้นข้อมูลที่จะส่งจะเพิ่มทีละ $l = n/k = 2.$ บิตส่งไปให้ภาครับจนกว่าจะแก้ไขได้ [33, 34]

ภาครับจะรับข้อมูลผลรวมสะสมของซินโดรมโดยเริ่มที่อัตรารหัสบีบอัดต่ำที่สุดคือ $1/4$ โดยการับข้อมูล $\tilde{\mathbf{p}} = [\tilde{p}_1, \tilde{p}_2]$ จากภาคส่งจากนั้นทำสลับตำแหน่งจะได้ $\mathbf{a} = [a_4, a_8]$ เข้ากระบวนถอดรหัสแอลดีพีซี ถ้าที่อัตรารหัสบีบอัด $1/4$ การถอดรหัสล้มเหลวภาครับก็จะร้องขอให้ภาคส่งข้อมูลมาเพิ่มเติมซึ่งก็คือ $[\tilde{p}_3, \tilde{p}_4]$ และภาครับจะมารวมกับข้อมูลเดิม $\tilde{\mathbf{p}} = [\tilde{p}_1, \tilde{p}_2, \tilde{p}_4, \tilde{p}_4,]$ และทำสลับตำแหน่งใหม่ $\mathbf{a} = [a_2, a_4, a_6, a_8]$ เพื่อเข้ากระบวนการถอดรหัสใหม่อีกครั้งซึ่งอัตราการบีดอัดจะเพิ่มเป็น $1/2$ แต่ถ้าการถอดรหัสยังล้มเหลวอีกภาครับจะร้องขอไปยังภาคส่งให้ส่งข้อมูลเพิ่มเติมมาอีกและภาครับจะรวมกับข้อมูลเดิมที่ส่งมาก่อนหน้าจะอีกจนการถอดสำเร็จจะสำเร็จดังแสดงกราฟที่ภาครับรูปที่ 4.3 เมื่อ $p(y_n \mid x_n)$ คือความน่าจะเป็นข้อมูลที่ที่ภาครับได้เมื่อรู้ค่า y_n และต้องการประมาณค่า x_n และสรุปขั้นตอนการไกล่เกลี่ยความผิดพลาดแสดงไว้ดังรูปที่ 4.4 [35]



รูปที่ 4.2 ตัวอย่างการเข้ารหัสแบบผลรวมซินโดรมของรหัสแอลดีพีซี



รูปที่ 4.3 ตัวอย่างการถอดรหัสแบบผลรวมซินโดรมของรหัสแอลดีพีซีด้วยอัตราการบีบอัดต่าง ๆ

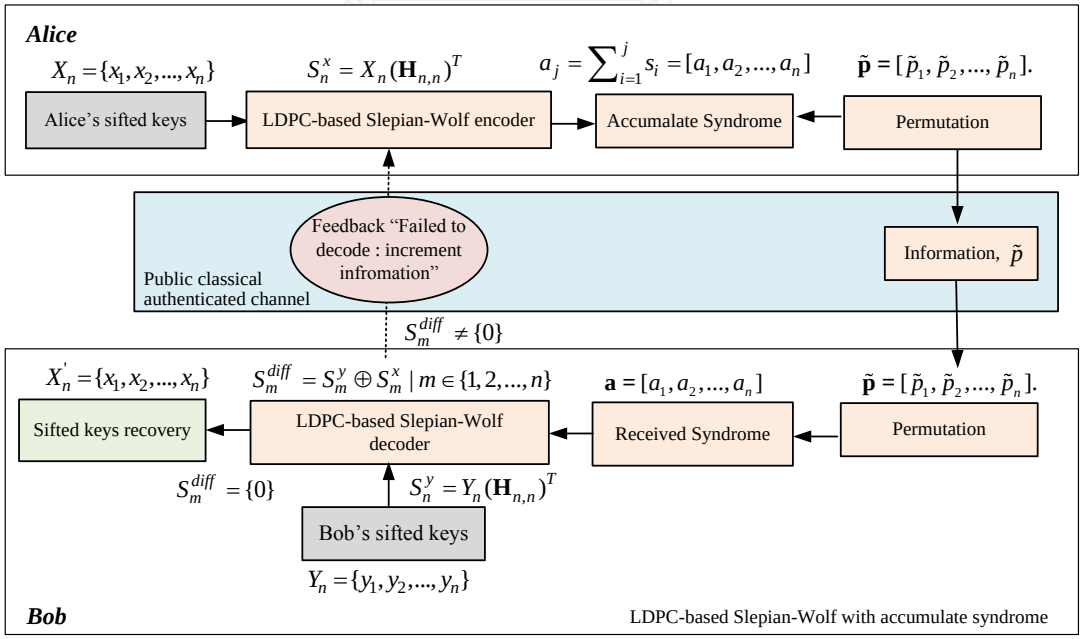
ขั้นตอนกระบวนแก้ไขความผิดพลาดด้วยรหัสแอลดีพีซีของผลรวมสะสมซินโดรมร่วมกับรหัสซลีเพียน-วูลฟ์

1. กำเนิดกุญแจรหัสลับ : *Alice* และ *Bob* กำเนิดกุญแจซิฟย์ที่มีความสัมพันธ์กัน X_n และ Y_n ตามลำดับ กำหนดให้ $\Pr(X \neq Y) = e$ เมื่อ e อัตราความผิดพลาดควอนตัมบิต (QBER)

2. การเข้ารหัส : *Alice* นำข้อมูลทั้งหมดลำดับ X_n เข้ารหัสซินโดรม $S_m^x = X_n(\mathbf{H})^T$ แล้วจากนั้นจะคำนวณผลรวมสะสมของซินโดรม $\mathbf{a} = [a_1, a_2, ..., a_n]$ เมื่อ $a_j = \sum_{i=1}^{j} s_i \mid j \in \{1, 2, ..., n\}$ และทำการสลับตำแหน่งของ $\mathbf{a}$ ด้วยพารามิเตอร์สลับตำแหน่ง π_p จะได้ข้อมูลใหม่ $\tilde{\mathbf{p}} = [\tilde{p}_1, \tilde{p}_2, ..., \tilde{p}_n]$. แบ่งข้อมูลเก็บไว้บางส่วนและจะส่งข้อมูล $\tilde{\mathbf{p}}$ ไปยัง Bob ผ่านช่องทางสัญญาณสื่อสารสาธารณะ

3. การถอดรหัส : *Bob* นำข้อมูล $\tilde{\mathbf{p}}$ ซึ่งก็ของซินโดรมสะสม $\mathbf{a}$ ของซินโดรม S^x จาก *Alice* มาใช้แก้ไขความผิดพลาดร่วมกับข้อมูล Y_n ที่ Bob ซึ่งมีอยู่ก็คือข้อมูลข่าวสารข้างเคียง (Side information) ข้อมูลนำเข้าของ *Bob* จะเป็นข้อมูลแบบซอร์ฟเพื่อนำสู่กระบวนการถอดรหัสแบบซัมโปรดัก คือ $L_c = \log((1-e)/e)(2Y_n - 1)$ ซึ่งหมายถึงการมอดูเลตแบบ BPSK เปลี่ยนข้อมูล 0 เป็น ร่วม -1 และ 1 เป็น 1

ขั้นตอนสุดท้ายถ้า $S^{diff} = 0$ สิ้นสุดกระบวนการถอดรหัสแต่ $S^{diff} \neq 0$ แจ้งกลับความล้มแล้วไปยังภาคส่งเพื่อแก้ไขใหม่อีกครั้ง โดยการร้องขอให้ *Alice* ส่งเพิ่มข้อมูลซินโดรมสะสม $\tilde{\mathbf{p}}$ มาให้และ *Bob* จะนำข้อมูลมารวมกับข้อมูลเดิมก่อนหน้านี้เข้าสู่กระบวนการถอดรหัสแอลดีพีซีจนกว่าจะแก้ไขความผิดพลาดได้ทั้งหมดดังที่ได้กล่าวมาแล้วก่อนหน้านี้



รูปที่ 4.4 วิธีการไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีโดยผลรวมสะสมของซินโดรม

4.3 การไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวเหมาะสมและการประเมินช่องสัญญาณ

4.3.1 การประเมินช่องสัญญาณ

การประเมินช่องสัญญาณในที่นี้จะกล่าวถึงเฉพาะช่องสัญญาณแบบสมมาตรไบนารี (BSC) ซึ่งในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมก็คือการประเมินค่าอัตราความผิดพลาดกุญแจรหัสลับ (QBER) ในระหว่างกระบวนการไกล่เกลี่ยความผิดพลาดซึ่งจะใช้วิธีจากความรู้พื้นฐานความน่าจะเป็นสูงสุด (Maximum likelihood) เริ่มต้นด้วยการนำชุดข้อมูลซินโดรมของคู่สื่อสารมาดำเนินการเปรียบเทียบ $S_{Z_{n-k}} = S_{X_{n-k}} \oplus S_{Y_{n-k}}$ โดยที่ $S_{X_{n-k}} = x_n(\mathbf{H}_{(n-k)\times n})^T$ และ $S_{Y_{n-k}} = y_n(\mathbf{H}_{(n-k)\times n})^T$ และหาค่าจำนวนเฉลี่ยบิตที่มีความแตกต่างกันบน $S_{Z_{n-k}}$ ดังสมการที่ 4.3

$$\hat{q}(S_{Z_{n-k}}) = \frac{1}{n-k}\sum_{m=1}^{n-k} S_z^{n-k} a \tag{4.3}$$

จากนั้นจึงเข้าสู่กระบวนการประเมินค่าอัตราความผิดพลาด QBER จากความน่าจะเป็นสูงสุดซึ่งสามารถคำนวณได้จากพื้นฐานผลของการแจกแจงไบโนเมียล (Binomial distribution) จากเมทริกซ์พาริตีเช็กแบบความหนาแน่นต่ำหรือเมทริกซ์ $\mathbf{H}$ ของรหัสแอลดีพีซี ดังสมการที่ 4.4

$$\hat{q}(e) = \sum_{i=1, i\,odd}^{d_c} \binom{d_c}{i} e^i (1-\mathrm{e})^{d_c-1} \tag{4.4}$$

โดยที่แทนฟังก์ชันการแจกแจงไบโนเมียลของค่าอัตราความผิดพลาด e (QBER) และ d_c คือจำนวนบิตหนึ่งในแถวของเมทริกซ์ $\mathbf{H}$ หรือ ดีกรีของโนดตรวจสอบ ซึ่งการประเมินค่าอัตราความผิดพลาด e จากข้อมูลซินโดรมเปรียบเทียบ $S_{Z_{n-k}}$ สามารถคำนวณได้จากอินเวอร์สฟังก์ชันของสมการที่ 4.5 ดังนี้

$$\hat{e}(S_{Z_{n-k}}) = f^{-1}(\hat{\mathrm{q}}(S_{Z_{n-k}})) = \frac{1-(1-2\hat{q}(S_{Z_{n-k}}))^{1/d_c}}{2} \tag{4.5}$$

การประมาณช่องสัญญาณรอบแรกของภาคถอดรหัสผลของการประเมินค่าอัตราความผิดพลาด QBER ในที่นี้ จะถูกนำมาใช้เพื่อการคำนวณค่าอัตราเข้ารหัสที่เหมาะสม $R_C(optimal)$ บนพื้นฐานอัลกอริธึมการหาค่าประมาณขอบเขตประสิทธิภาพการไกล่เกลี่ย $f(n,\varepsilon,e)$ ที่เป็นฟังก์ชันสอดคล้องกับค่าความยาวของคำรหัส n อัตราความสามารถแก้ไขความผิดพลาด ε และประสิทธิภาพของรหัสแอลดีพีซี หลังจากนั้นจึงเข้าสู่ขั้นตอนการกำหนดตำแหน่งพังเจอร์ (Puncture)

จำนวน p บิต และชอร์ตเทน (Shorten) จำนวน s บิตของชุดข้อมูลกุญแจรหัสลับและเมทริกซ์ H ให้มีจำนวนสอดคล้องกับอัตราเข้ารหัสที่เหมาะสม $R_C(optimal)$ ภายใต้ขอบเขตของรหัซลีเพียน-วูลฟ์ ดังจะกล่าวขั้นตอนวิธีในหัวข้อถัดไป

จากเทคนิคการประเมินค่า QBER ที่นำเสนอนี้ ถูกใช้แทนการประเมินความผิดพลาด (Channel estimation) แบบทั่วไป ที่จำเป็นต้องสูญเสียบิตเปิดเผยบางส่วน นำไปสู่เป้าหมายของการเพิ่มขนาดของกุญแจรหัสลับสุดท้าย

4.3.2 การปรับตัวอัตรารหัสที่เหมาะสม

ในกระบวนการแก้ไขความผิดพลาดที่เหมาะสมในระบบการสื่อสารที่มีความไม่แน่นอนนั้น อัตราการเข้ารหัสจึงจำเป็นพิจารณาให้เหมาะสมต่อสภาวะนั้นๆ รหัสแอลดีพีซีเป็นที่รู้จักกันอยู่ว่าไม่ใช่รหัสที่ให้อัตราการเข้ารหัสที่เหมาะสมกับสภาวะได้หลายๆ อย่าง แต่ก็มีบางเทคนิคช่วยให้รหัสแอลดีพีซีสามารถให้อัตราการเข้ารหัสที่หลากหลายเหมาะสมกับช่องสัญญาณได้ คือ เทคนิคการพังเจอร์ (puncture) หรือชอร์ตเทน (shorten) กระบวนการปรับตัวของอัตราการเข้ารหัสนี้เรียกว่าการมอดูเลตอัตรารหัส (rate modulate) ดังจะกล่าวแบบย่อดังต่อไปนี้

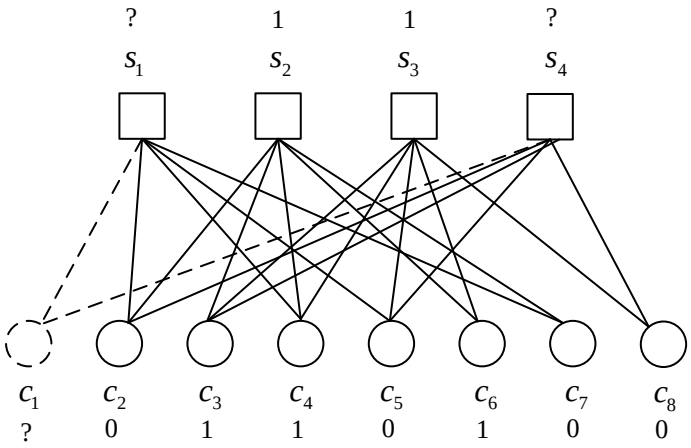
4.3.2.1 พังเจอร์ริง

โดยทั่วไปเป็นที่รู้จักดีว่าการพังเจอร์ริง (puncturing) เป็นการมอดูเลตรหัสของรหัสแบบเชิงเส้นโดยการตัดทิ้ง p บิตจากคำรหัสโดยที่ $p<n$ และจากโครงสร้างของคำรหัสเดิมคือ $C(n,k)$ ก็จะกลายเป็น $C(n-p,k)$ จะได้อัตรารหัสที่เพิ่มขึ้นคือ

$$R_c = \frac{k}{n-p} = \frac{R_0}{1-\pi} \tag{4.6}$$

เมื่อ $R_0 = k/n$ คือ อัตรารหัสดั้งเดิม และ $\pi = p/n$ คือ สัดส่วนจำนวนบิตที่พังเจอร์โดยที่ $\pi<1$

จากรูปที่ 4.5 แสดงตัวอย่างของกราฟแทนเนอร์ที่ประยุกต์ใช้พังเจอร์ในรหัสบล็อกเชิงเส้นโดยรหัสโครงสร้างเดิมคือ $C(8,4)$ และมีอัตรารหัสดั้งเดิมคือ $R_0 = (8-4)/8 = 1/2$ แล้วโดยพังเจอร์ด้วยการตัดทิ้งออก 1 บิตจากคำรหัสทั้งหมด ดังนั้นจะมีโครงสร้างรหัสคือ คือ $C(7,4)$ และมีอัตรารหัสใหม่ที่เพิ่มขึ้นคือ $R_0 = (8-4)/(8-1) = 4/7$

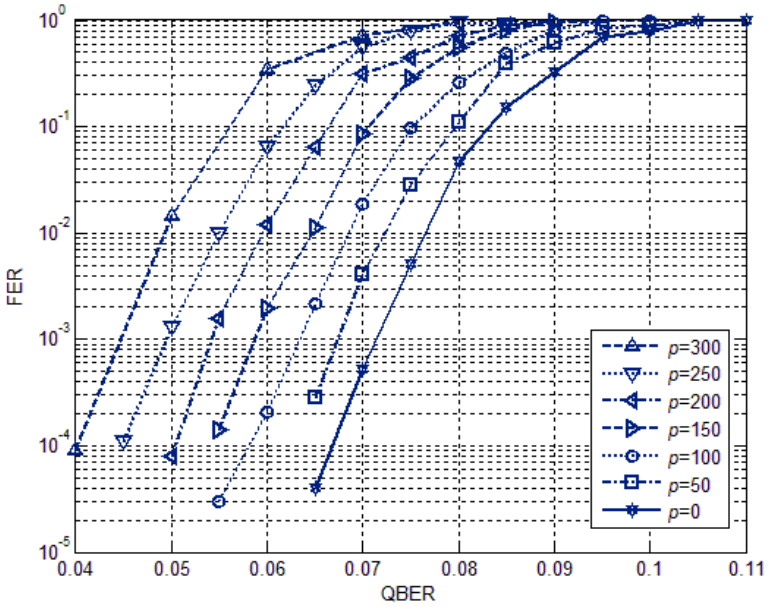


รูปที่ 4.5 ตัวอย่างกราฟแทนเนอร์จำนวนบิตที่พังเจอร์ในรหัสบล็อคเชิงเส้น

รูปที่ 4.6 จากผลจำลองสมรรถนะแสดงให้เห็นว่าเมื่อให้จำนวนบิตพังเจอร์ที่แตกต่างกันก็จะให้ค่าประสิทธิการแก้ไขความผิดพลาดที่แตกต่างกันด้วย จากการทดลองกำหนดพาริตีเช็กเมทริกซ์ H มีขนาด 1000×2000 เพราะฉะนั้น $R_0 = 1/2$ และจากการกำหนดบิตพังเจอร์ในสัดส่วนที่แตกต่างกันก็จะได้อัตรารหัสรหัสที่แตกต่างกันด้วยกล่าวคือในที่นี้ถ้าเพิ่มจำนวนบิตพังเจอร์ก็จะได้อัตรารหัสเพิ่มขึ้นด้วยดังตารางที่ 4.1 ซึ่งจะเห็นได้ว่าเมื่อเพิ่มจำนวนบิตพังเจอร์ประสิทธิภาพในการแก้ไขความผิดพลาดจะลดลงไปด้วย

ตารางที่ 4.1 การปรับอัตรารหัสด้วยพังเจอร์

จำนวนบิตพังเจอร์ p	**สัดส่วนพังเจอร์** $\pi = p/n$	**อัตรารหัสใหม่** R
0	0	0.5000
50	0.025	0.5128
100	0.050	0.5263
150	0.075	0.5405
200	0.100	0.5556
250	0.125	0.5714
300	0.150	0.5882



รูปที่ 4.6 ผลการจำลองสมรรถนะการแก้ไขความผิดพลาดด้วยรหัสแอลดีพีซีของสัดส่วนพังเจอร์

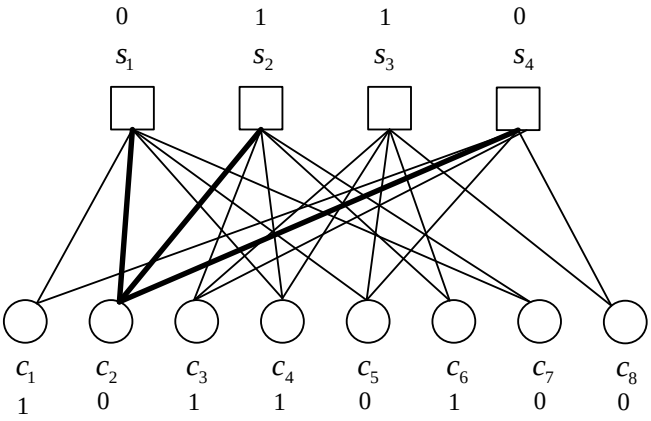
4.3.2.2 ชอร์ตเทนนิง

พังเจอร์ริงเป็นการเพิ่มอัตรารหัสโดยการการลดซินโดรมหรือบิตตรวจสอบ ในทางตรงกันข้าม ชอร์ตเทนนิง (shortening) เป็นการลดอัตรารหัสโดยเพิ่มซินโดรมหรือบิตตรวจสอบ

การมอดูเลตรหัสของรหัสแบบเชิงเส้นโดยการตัดทิ้ง s บิตจากคำรหัสโดยที่ $s<n$ และจากโครงสร้างของคำรหัสเดิมคือ $C(n,k)$ ก็จะเปลี่ยนเป็น $C(n-s,k-s)$ จะได้อัตรารหัสที่เพิ่มขึ้นคือ

$$R_c = \frac{k-s}{n-s} = \frac{R_0-\sigma}{1-\sigma} \tag{4.7}$$

เมื่อ $R_0 = k/n$ คือ อัตรารหัสดั้งเดิม และ $\sigma = s/n$ คือ สัดส่วนจำนวนบิตที่ชอร์ตเทนโดยที่ $\sigma<1$



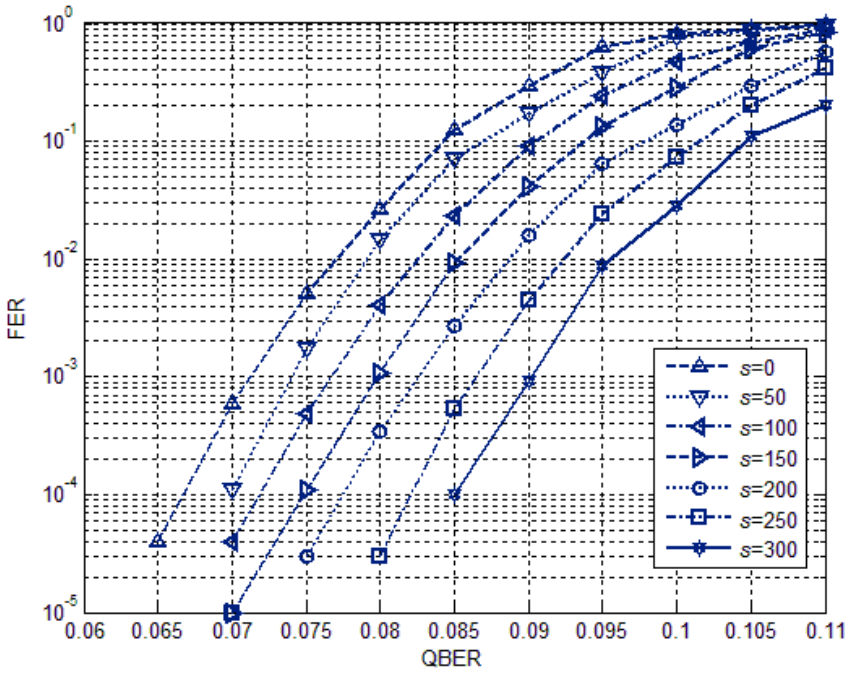
รูปที่ 4.7 ตัวอย่างกราฟแทนเนอร์จำนวนบิตที่ชอร์ตเทนในรหัสบล็อคเชิงเส้น

จากรูปที่ 4.7 แสดงตัวอย่างของกราฟแทนเนอร์ที่ประยุกต์ใช้ชอร์ตเทนในรหัสบล็อกเชิงเส้น โดยรหัสโครงสร้างเดิมคือ $C(8,4)$ และมีอัตรารหัสดั้งเดิมคือ $R_0 = (8-4)/8 = 1/2$ แล้วโดยชอร์ตเทนด้วยการกำหนดบิตที่จะชอร์ตเทนให้มีข้อมูลตรงตำแหน่งเป็นศูนย์จำนวน 1 ตำแหน่งจากคำรหัสทั้งหมด ดังนั้นจะมีโครงสร้างรหัสใหม่คือ คือ $C(7,3)$ และมีอัตรารหัสใหม่ที่ลดลงคือ $R = (8-4-1)/(8-1) = 3/7$

รูปที่ 4.8 จากผลจำลองสมรรถนะแสดงให้เห็นว่าเมื่อให้จำนวนบิตชอร์ตเทนที่แตกต่างก็จะให้ค่าประสิทธิการแก้ไขความผิดพลาดที่แตกต่างกันด้วย จากการทดลองกำหนดพาริตีเช็กเมทริกซ์ H มีขนาด 1000×2000 เพราะฉะนั้น $R_0 = 1/2$ และจากการกำหนดบิตชอร์ตเทนในสัดส่วนที่แตกต่างกันก็จะได้อัตรารหัสรหัสที่แตกต่างกันกล่าวคือในที่นี้เมื่อเพิ่มจำนวนบิตชอร์ตเทนก็จะได้อัตรารหัสลดลงด้วยดังตารางที่ 4.2 ซึ่งจะเห็นได้ว่าเมื่อเพิ่มจำนวนบิตชอร์ตเทนประสิทธิภาพในการแก้ไขความผิดพลาดก็จะเพิ่มขึ้นไปด้วย

ตารางที่ 4.2 การปรับอัตรารหัสด้วยชอร์ตเทน

จำนวนบิตชอร์ตเทน s	**สัดส่วนชอร์ตเทน** $\sigma = s/n$	**อัตรารหัสใหม่** R
0	0	0.5000
50	0.025	0.4872
100	0.050	0.4737
150	0.075	0.4595
200	0.100	0.4444
250	0.125	0.4286
300	0.150	0.4118



รูปที่ 4.8 ผลการจำลองสมรรถนะการแก้ไขความผิดพลาดด้วยรหัสแอลดีพีซีของสัดส่วนชอร์ตเทน

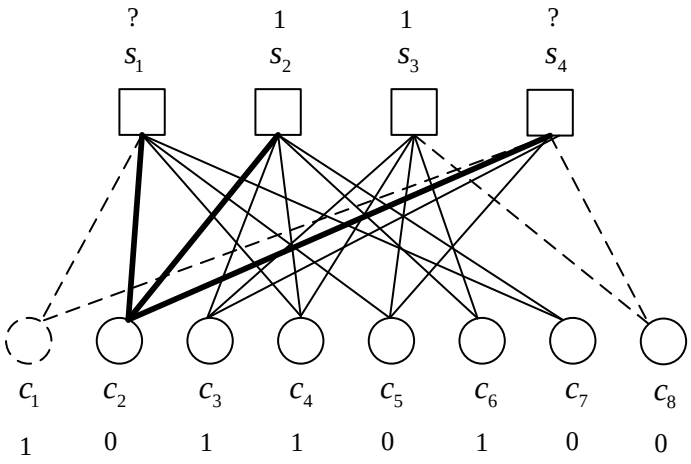
4.3.2.3 พังเจอร์ริงและชอร์ตเทนนิง

ในหัวนี้จะกล่าวถึงการปรับตัวที่เหมาะสมของอัตรารหัสด้วยเทคนิค 2 อย่างด้วยกัน คือ พังเจอร์ริงและชอร์ตเทนนิง การมอดูเลตรหัสของรหัสแบบเชิงเส้นโดยการตัดทิ้ง p และ s บิตจากคำรหัสโดยที่ $d<n$ เมื่อ $d=p+s$ และจากโครงสร้างของคำรหัสเดิมคือ $C(n,k)$ ก็จะเปลี่ยนเป็น $C(n-p-s,k-s)$ จะได้อัตรารหัสที่เพิ่มขึ้นคือ

$$R_c=\frac{k-s}{n-p-s}=\frac{R_0-\sigma}{1-\delta} \tag{4.8}$$

เมื่อ $R_0=k/n$ คือ อัตรารหัสดั้งเดิม และ $\delta=d/n$ คือ สัดส่วนจำนวนบิตที่พังเจอร์และชอร์ตเทน โดยที่ $\delta<1$ และ $\delta=\pi+\sigma$

จากรูปที่ 4.9 แสดงตัวอย่างของกราฟแทนเนอร์ที่ประยุกต์ใช้พังเจอร์และชอร์ตเทนในรหัสบล็อกเชิงเส้น โดยรหัสโครงสร้างเดิมคือ $C(8,4)$ และมีอัตรารหัสดั้งเดิมคือ $R_0=(8-4)/8=1/2$ แล้วโดยพังเจอร์และชอร์ตเทนด้วยการกำหนดบิตที่จะพังเจอร์ 2 บิตและบิตชอร์ตเทนให้มีข้อมูลตรงตำแหน่งเป็นศูนย์จำนวน 1 ตำแหน่งจากคำรหัสทั้งหมด ดังนั้นจะมีโครงสร้างรหัสใหม่คือ คือ $C(5,3)$ และมีอัตรารหัสใหม่ที่ลดลงคือ $R=(8-4-1)/(8-2-1)=3/5$

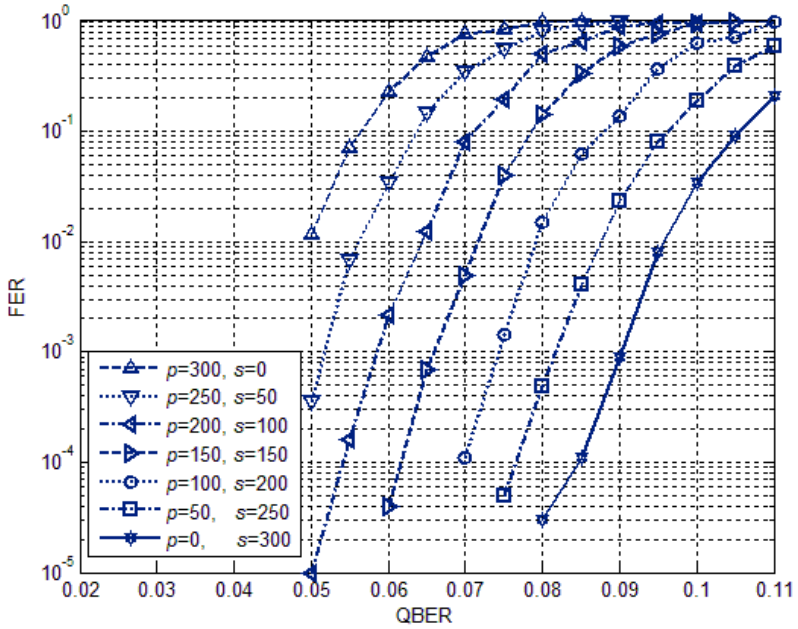


รูปที่ 4.9 ตัวอย่างกราฟแทนเนอร์จำนวนบิตที่พังเจอร์และชอร์ตเทนในรหัสบล็อคเชิงเส้น

รูปที่ 4.9 จากผลจำลองสมรรถนะแสดงให้เห็นว่าเมื่อให้จำนวนบิตพังเจอร์และชอร์ตเทนที่แตกต่างก็จะให้ค่าประสิทธิการแก้ไขความผิดพลาดที่แตกต่างกันด้วย จากการทดลองกำหนดเมทริกซ์พาริตีเช็ก $\mathbf{H}$ มีขนาด 1000×2000 เพราะฉะนั้น $R_0=1/2$ กำหนดบิตพังเจอร์และชอร์ตเทน $d=p+s=300$ อัตรามอดูเลท $\delta=d/n=0.150$ และจากกำหนดบิตพังเจอร์และชอร์ตเทนในสัดส่วนที่แตกต่างกันก็จะได้อัตรารหัสรหัสที่แตกต่างกันกล่าวคือในที่นี้เมื่อลดบิตพังเจอร์จะได้จำนวนบิตชอร์ตเทนเพิ่มขึ้นและอัตรารหัสลดลงด้วยดังตารางที่ 4.3 ซึ่งจะเห็นได้ว่าเมื่อลดบิตพังเจอร์และเพิ่มบิตชอร์ตเทนประสิทธิภาพในการแก้ไขความผิดพลาดก็จะเพิ่มขึ้นไปด้วย

ตารางที่ 4.3 การปรับอัตรารหัสด้วยพังเจอร์และชอร์ตเทน

จำนวนบิตพังเจอร์ p	**จำนวนบิตชอร์ตเทน** s	**สัดส่วนพังเจอร์** $\pi=p/n$	**สัดส่วนชอร์ตเทน** $\sigma=s/n$	**อัตรารหัสใหม่** R
300	0	0.150	0	0.5882
250	50	0.125	0.025	0.5588
200	100	0.100	0.050	0.5294
150	150	0.075	0.075	0.5000
100	200	0.050	0.100	0.4706
50	250	0.025	0.125	0.4412
0	300	0	0.150	0.4118



รูปที่ 4.10 ผลการจำลองสมรรถนะการแก้ไขความผิดพลาดรหัสแอลดีพีซีของสัดส่วนพังเจอร์และชอร์ตเทน

ขั้นตอนการไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวเหมาะสมและการประเมินช่องสัญญาณ

การบวนการไกล่เกลี่ยความผิดพลาดนั้นค่าประสิทธิภาพการไกล่เกลี่ยความผิดพลาดจะเป็นฟังก์ชันหรือขึ้นอยู่กับพารามิเตอร์ที่ใช้ดังนี้คือ จำนวนบิตทั้งที่ใช้ อันตราความผิดพลาดบิตควอนตัม และเป้าหมายอัตราการไกล่เกลี่ยความผิดพลาด ซึ่งสามารถคำนวณค่าขอบเขตของประสิทธิภาพการไกล่เกลี่ยได้ดังนี้[36]

$$f(n,\varepsilon,e)=\eta_{LDPC}(1+\frac{1}{\sqrt{n}}\frac{\sqrt{v(e)}}{h(e)}\Phi^{-1}(1-\varepsilon)) \tag{4.9}$$

โดยที่

e คือ ค่าอัตราความผิดพลาดควอนตัมบิตที่ได้จากการประเมินช่องสัญญาณ QBER

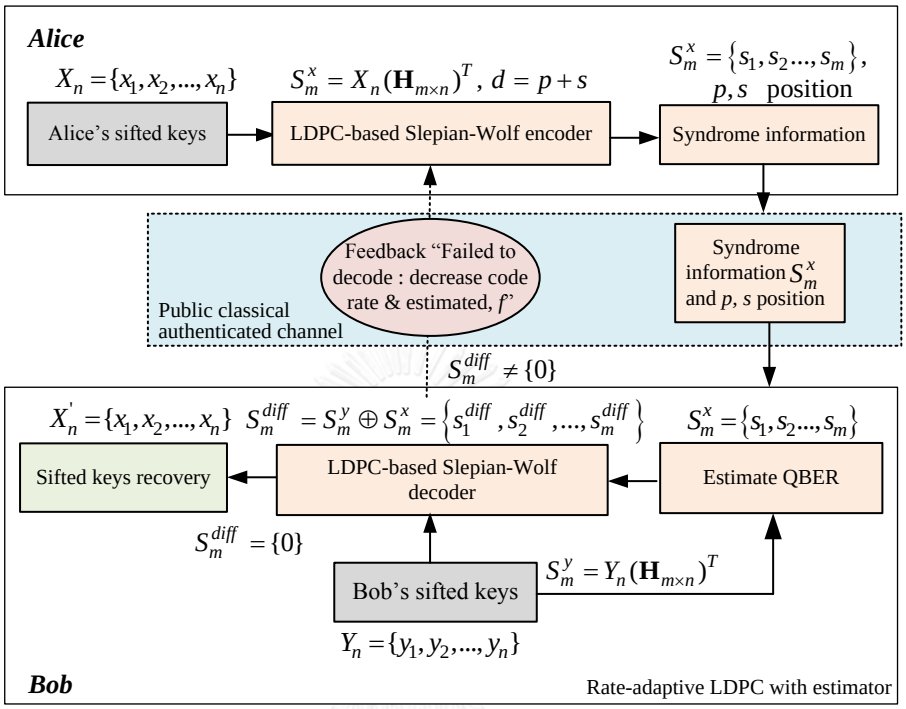
ε คือ ค่าอัตราการไกล่เกลี่ยความผิดพลาด หรือในที่นี้คือ FER (Frame Error Rate)

$h(e)=-e\log_2 e-(1-e)\log_2(1-e)$ คือฟังก์ชันปริมาณข่าวสารเฉลี่ยแบบมีเงื่อนไข (conditional entropy)

$v(e)=e(1-e)(\log_2(e/(1-e)))^2$ คือฟังก์ชันความแปรปรวนข่าวสารแบบมีเงื่อนไข (conditional entropy variance)

Φ คือฟังก์ชั่นความน่าจะเป็นแจกแจงสะสม (cumulative standard normal distribution)

η_{LDPC} คือประสิทธิการแก้ไขความผิดพลาดของรหัสแอลดีพีซี $\eta_{LDPC} \geq 1$



รูปที่ 4.11 วิธีการไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบปรับอัตรารหัสเหมาะสมและประเมินค่าล่วงหน้า

ขั้นตอนวิธีการไกล่เกลี่ยความผิดพลาดแสดงไว้ดังรูปที่ 4.11 และสามารถอธิบายได้ดังนี้

1. กำเนิดกุญแจรหัสลับและค่าเริ่มต้น : *Alice* และ *Bob* กำเนิดกุญแจซิฟย์ที่มีความสัมพันธ์กัน X_l และ Y_l ตามลำดับ $l = n - d$ โดยที่ $d = p + s, \delta = d / n$ จำนวนบิตพังเจอร์และชอร์ตเทนที่เพิ่มเข้ามา กำหนดให้ $\Pr(X \neq Y) = e$ เมื่อ e อัตราความผิดพลาดควอนตัมบิต (QBER) ซึ่งได้จากการประเมินความผิดพลาดในหัวข้อ 4.3.2 ตั้งค่าเป้าหมายการไกล่เกลี่ยความผิดพลาด (FER) ε และค่าจำนวนบิตทั้งหมด n เพื่อนำไปสู้การประมาณค่าขอบเขตประสิทธิภาพที่เป็นไปได้

2. การเข้ารหัส : *Alice* นำข้อมูลทั้งหมดลำดับ X_n เข้ารหัสซินโดรม $S_m^x = X_n(\mathbf{H}_{m\times n})^T$ เมื่อ *Alice* รู้ค่าประสิทธิภาพเริ่มต้น $f(n, \varepsilon, e)$ จากสมการ 4.8 ก็จะมาสามารถหาค่าอัตรารหัสที่เหมาะสมเพื่อกำหนดจำนวนบิตสุ่มพังเจอร์และชอร์ตเทนได้คือ

$$R = 1 - f(n, \varepsilon, e)h(e) \tag{4.10}$$

$$s = (R_0 - R(1-\delta))n \tag{4.11}$$

$$p = d - s \tag{4.12}$$

จากนั้นส่งข้อมูลซินโดรม S_m^x และตำแหน่งของ p และ s ไปยัง Bob ผ่านช่องทางสัญญาณสื่อสารสาธารณะ

3. การถอดรหัส : *Bob* นำข้อมูลซินโดรม S_m^x จาก Alice มาใช้แก้ไขความผิดพลาดร่วมกับข้อมูล Y_n ที่ *Bob* ซึ่งมีอยู่ก็คือข้อมูลข่าวสารข้างเคียง (Side information) ข้อมูลนำเข้าของ *Bob* จะเป็นข้อมูลแบบซอร์ฟเพื่อนำสู่กระบวนการถอดรหัสคือ $L_c = \log((1-e)/e)(2Y_n - 1)$ ซึ่งหมายถึงการมอดูเลตแบบ (BPSK) เปลี่ยนข้อมูล 0 เป็นร่วม -1 และ 1 เป็น 1 ก่อนเข้าสู่กระบวนการถอดรหัสแบบซัมโปรดักดังในหัวข้อ 3.2.2.4

ขั้นตอนสุดท้ายถ้า $S_m^{diff} = 0$ สิ้นสุดกระบวนการถอดรหัสแต่ $S_m^{diff} \neq 0$ แจ้งกลับความล้มแล้วไปยังภาคส่งเพื่อแก้ไขใหม่อีกครั้ง โดยการเลือกอัตราเข้ารหัสแอลดีพีซีลำดับถัดไปที่มีค่าลดลงโดยการลดจำนวนพังเจอร์และเพิ่มจำนวนชอร์ตเทน

บทที่ 5
ผลการทดสอบโพรโทคอลไกล่เกลี่ยความผิดพลาดกุญแจรหัสลับที่นำเสนอ

ในบทนี้จะนำเสนอผลทดสอบของโพรโทคอลไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีแบบต่าง ๆ ที่นำเสนอทั้งในแง่ของสมรรถนะการแก้ไขความผิดพลาดหรืออัตราความผิดพลาดบิต ประสิทธิภาพการไกล่เกลี่ย (Reconciliation efficiency) จำนวนบิตเปิดเผย (Disclose bit) และอัตราการให้กำเนิดรหัสกุญแจรหัสลับ ประกอบด้วยหัวข้อดังต่อไปนี้ หัวข้อ 5.1 จะกล่าวถึงผลการจำลองวิธีการไกล่เกลี่ยความผิดพลาดความซับซ้อนต่ำโดยใช้การถอดรหัสแอลดีพีซีแบบบิตฟลิปปิงและแบบซัมโปรดักซินโดรม หัวข้อ 5.2 จะกล่าวถึงผลการจำลองระบบการไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวได้ด้วยผลรวมสะสมของซินโดรม หัวข้อ 5.3 จะกล่าวถึงผลการจำลองการไกล่เกลี่ยความผิดพลาดอัตรารหัสแอลดีพีซีแบบปรับตัวได้โดยอาศัยเทคนิคการสุ่มบิตตำแหน่งพังเจอร์และชอร์ตเทนร่วมกับการประเมินช่องสัญญาณในที่นี้คือการประมาณความผิดพลาดกุญแจรหัสลับบิต (QBER) และการประมาณประสิทธิภาพการไกล่เกลี่ยความผิดพลาด

5.1 ผลการจำลองการไกล่เกลี่ยความผิดพลาดความซับซ้อนต่ำด้วยการถอดรหัสแอลดีพีซีแบบบิตฟลิปปิงและซัมโปรดักซินโดรม

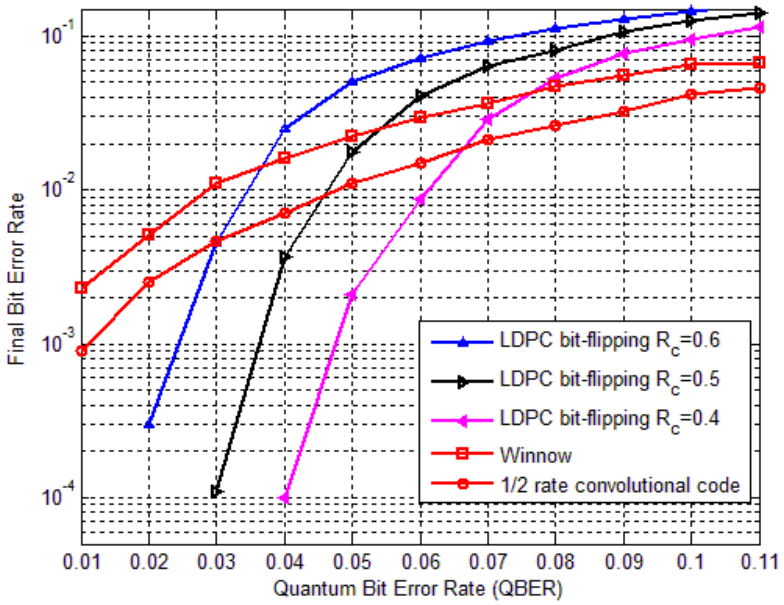
ในหัวนี้จะกล่าวถึงผลการทดลองประสิทธิภาพการไกล่เกลี่ยความผิดพลาดของการถอดแอลดีพีซี 2 แบบคือแบบบิตฟลิปปิงซึ่งเป็นแบบฮาร์ดมีความซับซ้อนต่ำและการถอดรหัสแอลดีพีซีแบบซัมโปรดักซินโดรมซึ่งเป็นแบบซอร์ฟแสดงผลการทอลองในเทอมของสมรรถนะอัตราการแก้ไขความผิดพลาดบิต

5.1.1 ผลการจำลองการไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบบิตฟลิปปิง

จากขั้นตอนที่นำเสนอในหัวข้อที่ 4.4.1 กำหนดพารามิเตอร์ที่ใช้ในการทดลองดังต่อไปนี้

- กำเนิดกุญแจรหัสที่ใช้มากกว่า 100,000 บิต โดยใช้เมทริกซ์พาริตีเช็กขนาดความยาว $N = 1,000$ บิต สร้างจากอัลกอรึทึม PEG (Progressive Edge Grown) [37] จำนวนรอบที่ใช้ในการวนซ้ำถอดรหัส 100 รอบ

ผลการจำลองในรูปที่ 5.1 แสดงถึงสมรรถนะในไกล่เกลี่ยความผิดพลาดด้วยการถอดรหัสแอลดีพีซีแบบบิตฟลิปปิงอย่างง่ายโดยมีความซับซ้อนต่ำเหมาะสำหรับการจัดทำสร้างฮาร์ดแวร์ได้ง่าย โดยให้อัตราความผิดพลาดบิตสุดท้าย (Final Bit Error Rate) ได้ดีในช่วง QBER ต่ำ-ปานกลาง เมื่อเทียบกับรหัสก่อนหน้านี้เช่นวินนาวและคอนวูโลชั่น แต่ก็ยังใช้อัตราที่สูงกว่าและยังแก้ไขความผิดพลาดไม่ดีพอเท่าที่ควร ในหัวข้อนี้จะเป็นการศึกษาขั้นตอนวิธีการไกล่เกลี่ยความผิดพลาดอย่างง่าย



รูปที่ 5.1 สมรรถนะการแก้ไขความผิดพลาดด้วยการถอดรหัสแลดีพีซีแบบบิตฟลิปปิง

5.1.2 ผลการจำลองการไกล่เกลี่ยความด้วยการถอดรหัสแอลดีพีซีแบบชัมโปรดักชินโดรม

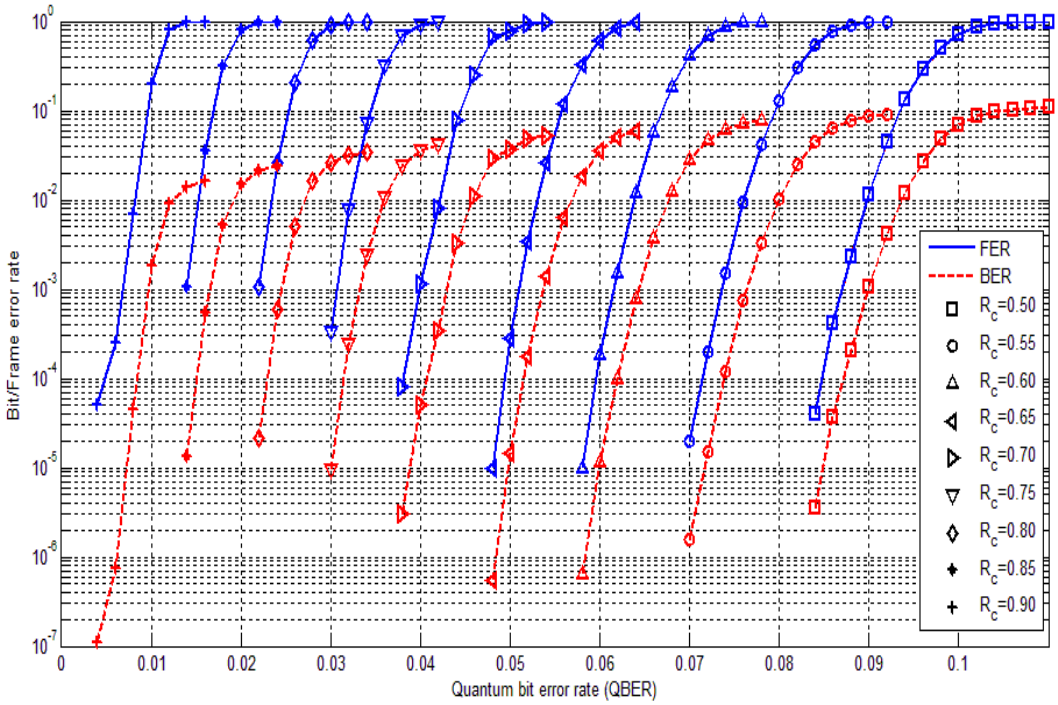
จากขั้นตอนที่นำเสนอในหัวข้อ 4.1.2 กำหนดพารามิเตอร์ที่ใช้ในจำลองผลการทำงานดังนี้

- กำเนิดกุญแจรหัสมากกว่า 100,000 บล็อก โดยใช้เมทริกซ์ขนาดความยาว $N=10,000$ และ $N=100,000$ บิต สร้างจากอัลกอรึทึม PEG จำนวนรอบที่ใช้ในการวนซ้ำถอดรหัส 100 รอบ

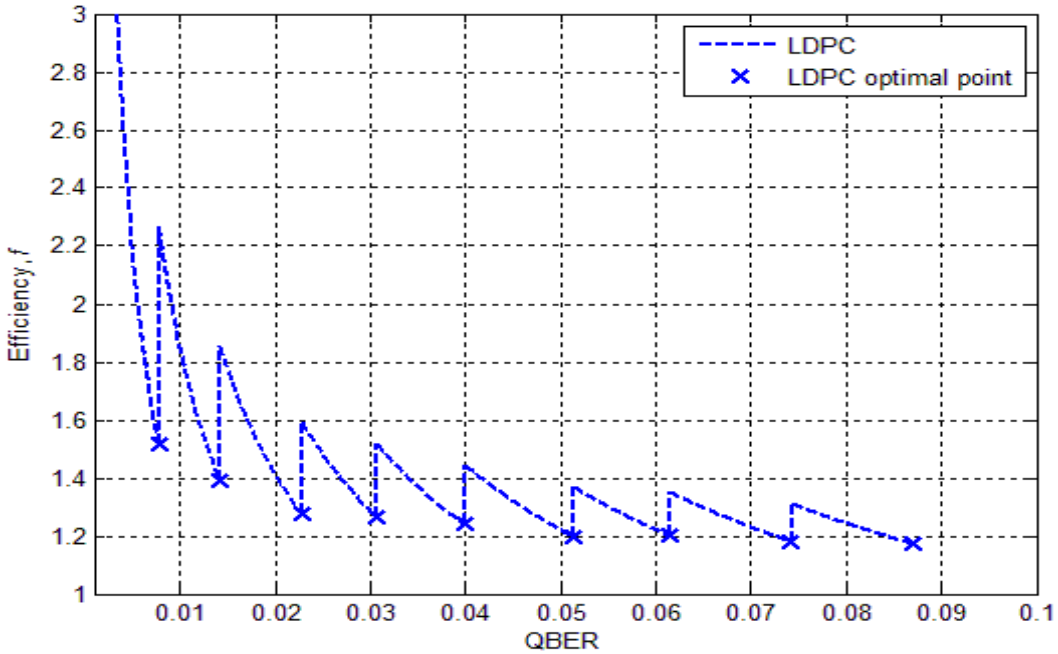
ผลการจำลองประสิทธิการไกล่เกลี่ยความผิดพลาดขนาดความยาวรหัส $N=10,000$ โดยใช้อัตรารหัสได้ $R_c=\{0.90\ \ 0.85\ \ 0.80\ \ 0.75\ \ 0.70\ \ 0.65\ \ 0.60\ \ 0.55\ \ 0.50\}$ ในรูปของอัตราการแก้ไขความผิดพลาดบิต (Bit Error Rate : BER) และเฟรมหรือบล็อก (Frame error rate : FER) ต่ออัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัม (QBER) ดังรูปที่ 5.2 ซึ่งจะเห็นได้ว่าเมื่อใช้อัตรารหัสที่ต่างกัน ประสิทธิภาพการไกล่เกลี่ยที่ได้จะได้ต่างกันด้วย เมื่อใช้อัตรารหัสที่สูงความสามารถในการแก้ไขความผิดพลาดก็จะน้อยกว่าอัตรารหัสที่ต่ำกว่า ดังนั้นการเลือกใช้อัตรารหัสก็มีผลต่อประสิทธิการไกล่เกลี่ยความผิดพลาดด้วยกล่าวคือเมื่อช่วง QBER ต่ำก็จะเลือกใช้อัตรารหัสที่สูงก็เพียงพอต่อการแก้ไขความผิดพลาดได้แล้วไม่ต้องใช้อัตราที่ต่ำกว่านี้ซึ่งก็จะหมายจะต้องเปิดเผยจำนวนบิตเพิ่มขึ้นตามมาด้วย

รูปที่ 5.3 แสดงประสิทธิการไกล่ความผิดพลาดของขนาดความยาวรหัส $N=10,000$ ซึ่งคำนวณได้จากสมการ 3.32 คือ $f=R_S/H(X|Y)=(1-R_C)/H(X|Y)$ โดยเลือกจุดค่า QBER ที่

สามารถแก้ไขอัตราความผิดพลาดได้ $\mathrm{FER}=10^{-3}$ จากกราฟในรูปที่ 5.2 ผลจากการทดลองที่ได้จะเป็นจุดที่เหมาะสมกับช่วงของ QBER ในแต่ล่ะค่าดังที่ในตารางที่ 5.1 ด้วย



รูปที่ 5. 2 ผลการจำลองสมรรถนะการแก้ไขความผิดพลาดของรหัสแอลดีพีซี $N=10,000$ อัตรารหัสต่างๆ

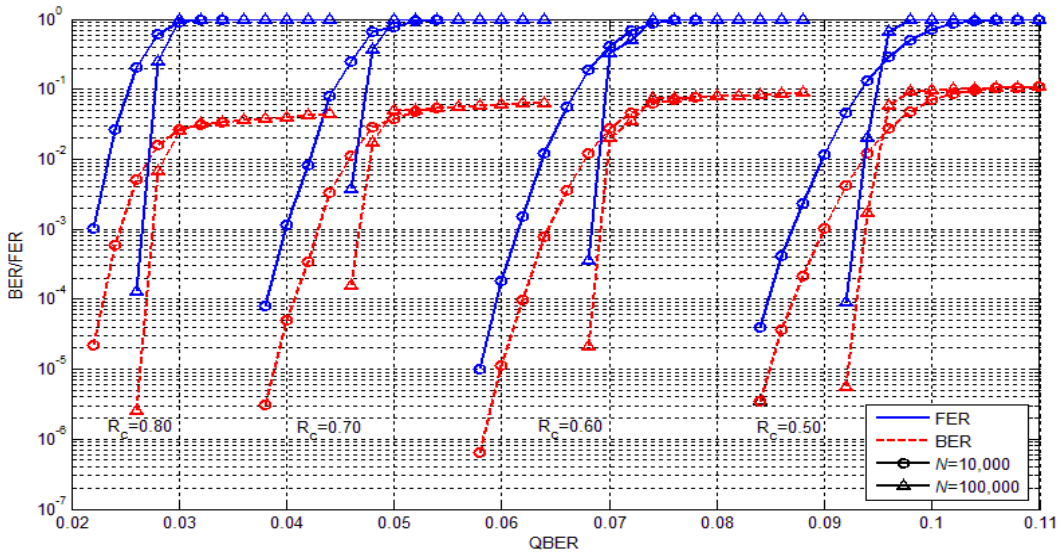


รูปที่ 5.3 ผลการจำลองประสิทธิภาพการไกล่เกลี่ยของรหัสแอลดีพีซี $N=10,000$ อัตรารหัสต่างๆ

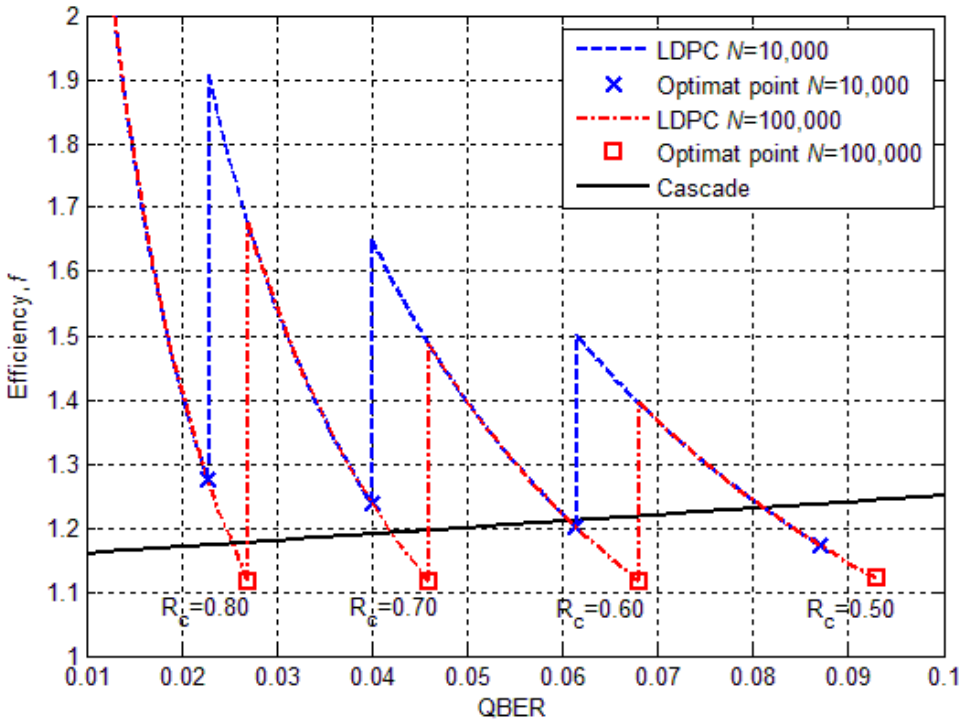
รูปที่ 5.4 แสดงผลการจำลองการเปรียบเทียบการทำงานของอัตราการแก้ไขบิตผิดพลาดสุดท้าย BER และ FER ในแต่ละอัตรารหัสของ $N=10,000$ บิตและ $N=100,000$ บิต จากกราฟจะเห็นได้ว่ารหัสที่มีความยาวบิตมากกว่าจะให้อัตราการแก้ไขบิตผิดพลาดที่ดีกว่าเมื่ออัตรารหัสเดียวกัน

รูปที่ 5.5 แสดงผลการจำลองการเปรียบเทียบประสิทธิการไกล่ความผิดพลาดของ $N=10,000$ และ $N=100,000$ ในแต่ละอัตรารหัสที่เท่ากัน โดยคำนวณค่าประสิทธิภาพการไกล่เกลี่ยได้จากสมการที่ 3.32 โดยเลือกจุดที่สามารถแก้ไขได้ที่ $\mathrm{FER}=10^{-3}$ ของรูปที่ 5.4 และจากการทดสอบจะเห็นได้ว่าเมื่อใช้รหัสบิตที่มียาวเพิ่มขึ้นจะให้ค่าประสิทธิดีกว่าเข้าใกล้ค่าทฤษฎีมากขึ้น $f=1$ โดยให้ค่าประมาณ 1.11 และประสิทธิภาพดีกว่าโพรโทคอลคาสเคดที่นำเสนอมาก่อนหน้านี้

ตารางที่ 5.1 ตารางสรุปค่าการเปรียบเทียบที่ได้จากการจำลองผลการทำงานของระบบตั้งแต่รูปที่ 5.2-5.5 ทั้งหมดในรูปของอัตรารหัส ความยาวของรหัส ค่า QBER ที่เหมาะสม และประสิทธิภาพการไกล่เกลี่ย



รูปที่ 5. 4 ผลการจำลองเปรียบเทียบสมรรถนะการแก้ไขความผิดพลาดของรหัสแอลดีพีซี $N=10,000$ และ $N=100,000$ อัตรารหัสต่างๆ



รูปที่ 5. 5 ผลการจำลองประสิทธิภาพการไกล่เกลี่ยของรหัสแอลดีพีซี $N=10,000$ และ $N=100,000$

ตารางที่ 5.1 เปรียบเทียบประสิทธิภาพการไกล่เกลี่ยและจุดทำงานที่เหมาะสม QBER ของแต่ละอัตรารหัส

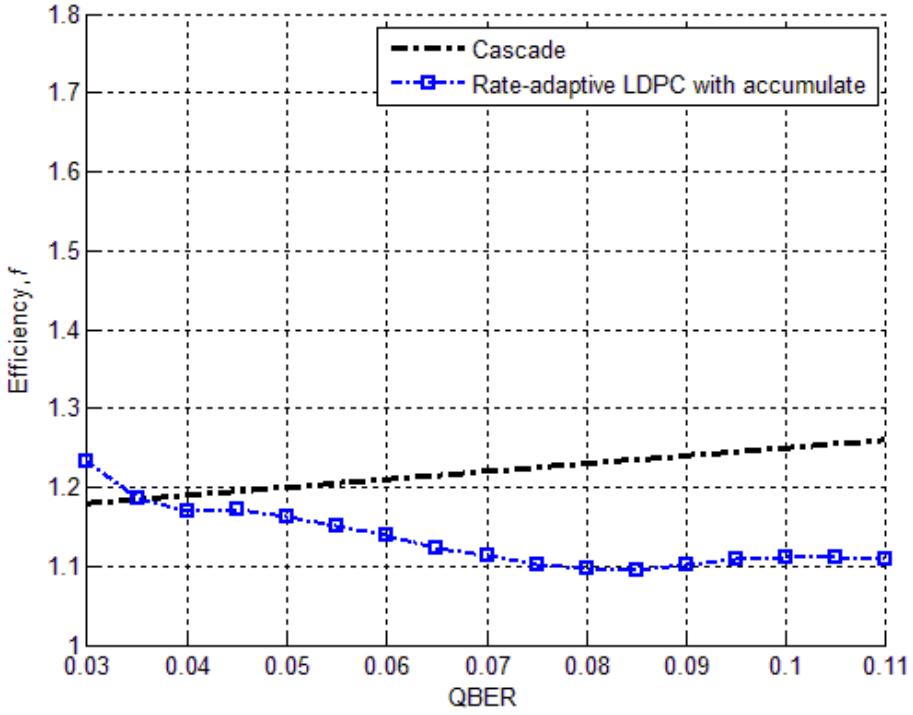
อัตรารหัส R_c	**จำนวนบิตต่อบล็อก** N	**จุด QBER ทำงานเหมาะสมที่** FER=10^{-3}	**ประสิทธิภาพการไกล่เกลี่ย** f
0.09	10,000	0.0079	1.5191
	100,000	-	-
0.85	10,000	0.0143	1.3908
	100,000	-	-
0.80	10,000	0.0229	1.2754
	100,000	0.0270	1.1160
0.75	10,000	0.0307	1.2647
	100,000	--	-
0.70	10,000	0.0400	1.2402
	100,000	0.0460	1.1146
0.65	10,000	0.0514	1.1973
	100,000	-	-
0.60	10,000	0.0614	1.2009
	100,000	0.0680	1.1160
0.55	10,000	0.0743	1.1795
	100,000	-	-
0.50	10,000	0.0871	1.1719
	100,000	0.0935	1.1201

5.2 ผลการจำลองการไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวได้ด้วยผลรวมสะสมของซินโดรม

ผลการจำลองด้วยวิธีการที่นำเสนอนี้จะพิจารณาเปรียบเทียบในเทอมของประสิทธิภาพการไกล่เกลี่ยความผิดพลาดและจำนวนบิตเปิดเผยกับโพรโทคอลที่นำเสนอมาก่อนหน้านี้ และจากขั้นตอนที่นำเสนอในหัวข้อ 4.2 กำหนดพารามิเตอร์ที่ใช้ในจำลองผลการทำงานดังนี้

- เมทริกซ์พาริตีเช็กขนาดความยาว $N = 12,672$ บิต สร้างจากอัลกอรึทึม PEG โดยใช้ขั้นตอนการถอดรหัสแอลดีพีซีแบบชัมโปรดักซินโดรม จำนวนรอบที่ใช้ในการวนซ้ำถอดรหัส 100 รอบ จำนวนครั้งเฉลี่ยที่ใช้ในการทดลอง 1,000 ครั้ง

รูปที่ 5.7 แสดงถึงประสิทธิภาพการไกล่เกลี่ยของระบบคำนวณได้จากสมการ 3.32 จะเห็นได้ว่าสามารถให้ประสิทธิภาพที่กว่าระบบที่นิยมใช้อยู่ตั้งแต่ QBER = 0.035 ขึ้นไป และช่วงระหว่าง QBER = 0.07 ขึ้นค่าประสิทธิภาพการไกล่เกลี่ยจะเริ่มคงที่คือประมาณ 1.11 ซึ่งเข้าใกล้เส้นทฤษฎีมากขึ้น อย่างไรก็ตามสามารถเพิ่มขนาดความยาวรหัสของเมทริกซ์พาริตีเช็ก เพื่อจะได้ประสิทธิภาพที่ดีขึ้นแต่ก็ต้องแลกมาด้วยพื้นที่เก็บเมทริกซ์พาริตีเช็กที่ใช้สำหรับปรับค่าอัตรารหัสมากขึ้นตามไปด้วย

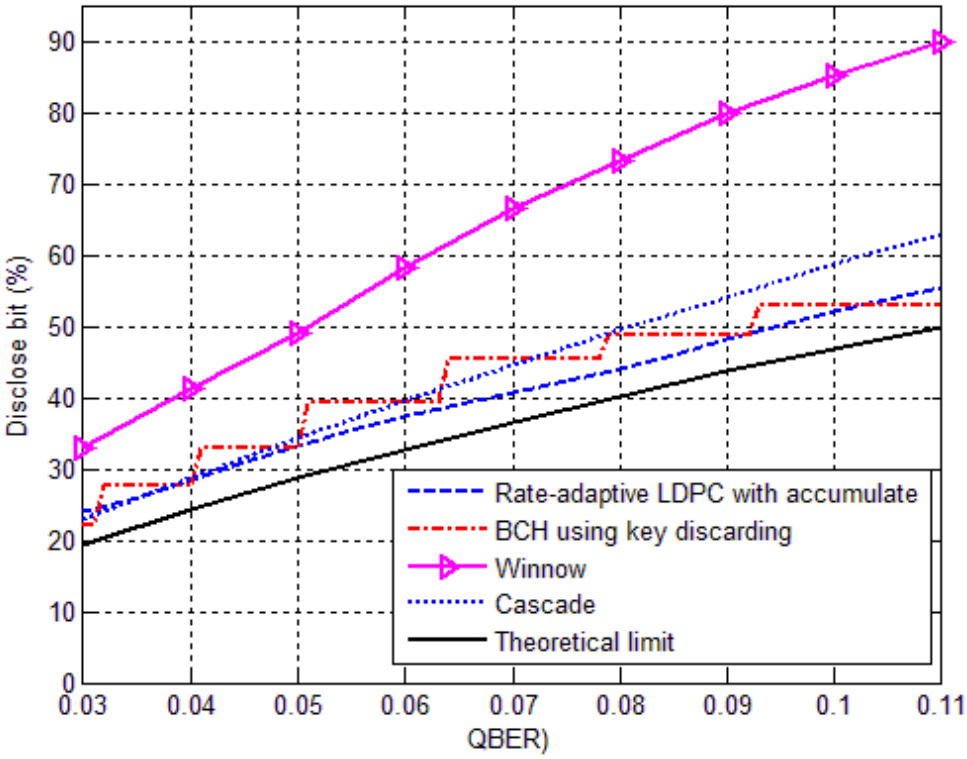


รูปที่ 5.6 ผลการจำลองประสิทธิภาพการไกล่เกลี่ยรหัสแอลดีพีซีด้วยผลรวมสะสมของซินโดรม

รูปที่ 5.6 แสดงจำนวนบิตเปิดเผยระหว่างกระบวนการไกล่เกลี่ยความผิดพลาดจากการทดลองจะเห็นได้ว่าระบบที่นำเสนอสามารถให้ขีดจำกัดทฤษฎีกว่าระบบอื่นๆ ช่วงระหว่าง QBER ที่ 0.03 – 0.11 ได้แก่โพรโทคอลที่ใช้รหัสบีซีเอช โพรโทคอลวินนาว โพรโทคอลคาสเคด โดยค่าทฤษฎีบิตเปิดเผยสามารถคำนวณได้ดังสมการ

$$d_{th} = 1 - I(e), \tag{5.1}$$

เมื่อ e คือ QBER และ $I(e) = 1 + e\log_2 e + (1-e)\log_2(1-e).$



รูปที่ 5.7 ผลการจำลองจำนวนบิตเปิดเผยระหว่างกระบวนการไกล่เกลี่ยด้วยรหัสแอลดีพีซีด้วยผลรวมสะสมของซินโดรม

5.3 ผลการจำลองการไกล่เกลี่ยความผิดพลาดด้วยอัตรารหัสแอลดีพีซีแบบปรับตัวเหมาะสมและการประเมินช่องสัญญาณ

ผลการจำนวนของระบบที่นำเสนอไว้ในหัวข้อที่ 4.3 จะแบ่งออกเป็น 2 ส่วนคือที่เป็นค่าประเมินความผิดพลาดของช่องสัญญาณและส่วนที่เกี่ยวกับประสิทธิของไกล่เกลี่ยความผิดพลาดของระบบ กำหนดพารามิเตอร์ที่ใช้ในการทดลองดังนี้

- เมทริกซ์พาริตีเช็กขนาดความยาว $N = 200,000$ บิตสร้างจากอัลกอริทึม PEG ใช้การถอดรหัสแอลดีพีซีแบบซัมโปรดักซินโดรม จำนวนรอบที่ใช้ในการวนถอดรหัส 100 รอบ จำนวนครั้งเฉลี่ยที่ใช้ในการทดลอง 100 ครั้ง ค่ามอดูเลทพังเจอร์และชอร์ตเทนที่ใช้ $\delta = 0.1$ อัตรารหัส $R_0 = \{0.80, 0.70, 0.60, 0.50\}$

5.3.1 ผลการจำลองการประเมินความผิดพลาดของช่องสัญญาณ

ผลการจำลองจากที่นำเสนอไว้ในหัวข้อ 4.3.1 เป็นการประเมินช่องสัญญาณแบบ BSC ซึ่งในที่นี้ก็คือการประเมินความผิดพลาดควอนตัม (QBER) เพื่อจะเป็นกำหนดขอบเขตของประสิทธิภาพของการไกล่เกลี่ยความผิดพลาดเริ่มต้นได้จะช่วยลดรอบการติดต่อระหว่าง *Alice* และ *Bob* ระหว่างกระบวนการไกล่เกลี่ยและเพิ่มกุญแจรหัสลับสุดท้าย

จากรูปที่ 5.8 และรูปที่ 5.9 แสดงผลการทดลองของความยาว $N = 100,000$ และ $N = 200,000$ ตามลำดับ โดยอัตรารหัสให้เหมาะสมกับช่วงของการทำงานแต่ละช่วง QBER ดังตารางที่ 5.2 โดยคำนวณได้จาก

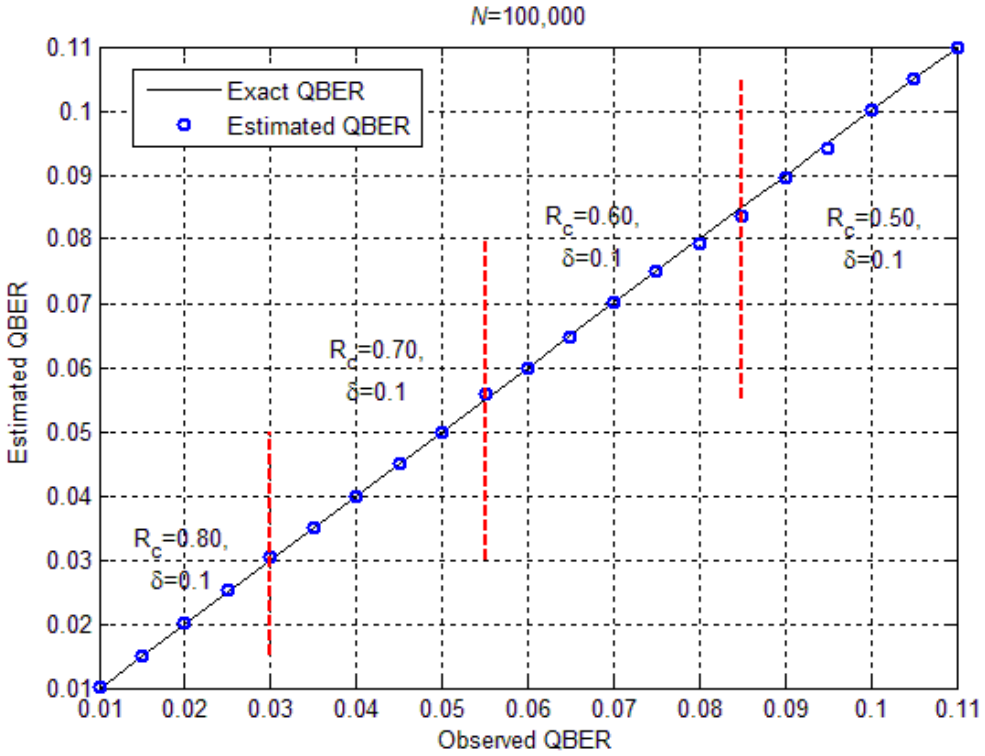
$$R_{\min} = \frac{R_0 - \delta}{1-\delta} \le R \le \frac{R_0}{1-\delta} = R_{\max}$$

และอยู่ในขอบเขตที่จะสามารถแก้ไขความผิดพลาดได้ $R_{\min} \le 1 - h(e_2)$ และ $R_{\max} \ge 1 - h(e_1)$

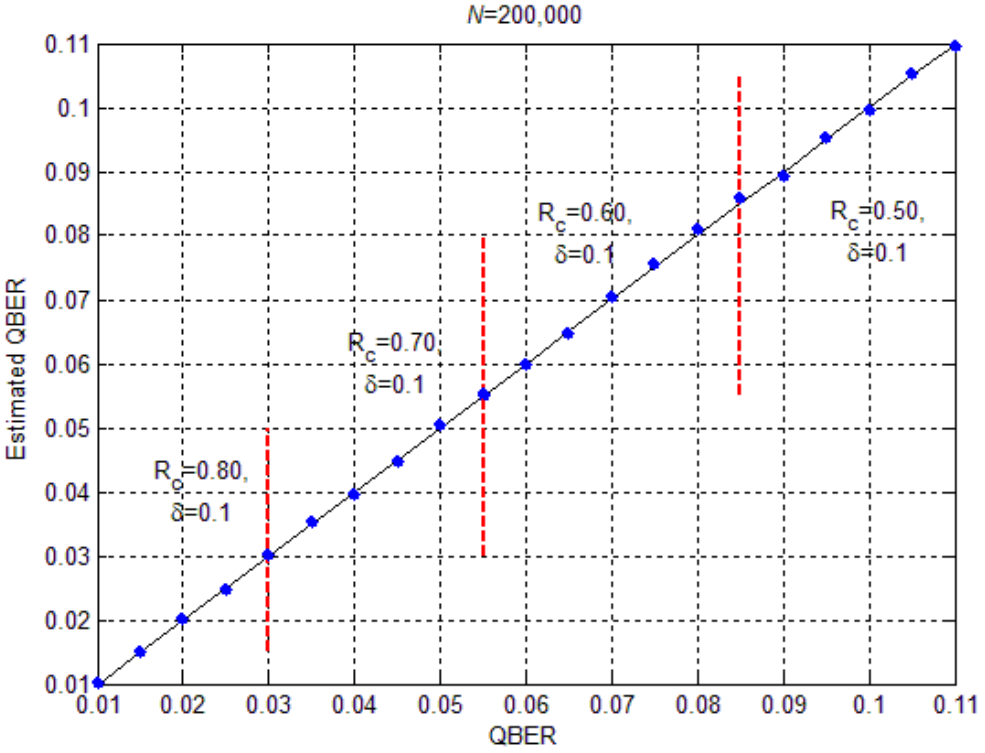
จากรูปผลทดลองทั้งสองจะเห็นได้ว่าค่า QBER ที่ได้จากการประมาณได้มีค่าใกล้เคียงกับค่าจริงมาก

ตารางที่ 5.2 อัตรารหัสแอลดีพีซีใช้อัตรามอดูเลทเท่ากับ 0.1

R_0	$R_{\max}$	$R_{\min}$	$[e_{\min}, e_{\max}]$
0.80	0.8889	0.0778	[0.01, 0.03]
0.70	0.7778	0.6667	[0.035, 0.055]
0.60	0.6667	0.5556	[0.06, 0.85]
0.50	0.5556	0.4444	[0.90, 0.11]



รูปที่ 5.8 ผลการประเมินค่า QBER เทียบกับค่าจริง $N = 100,000$

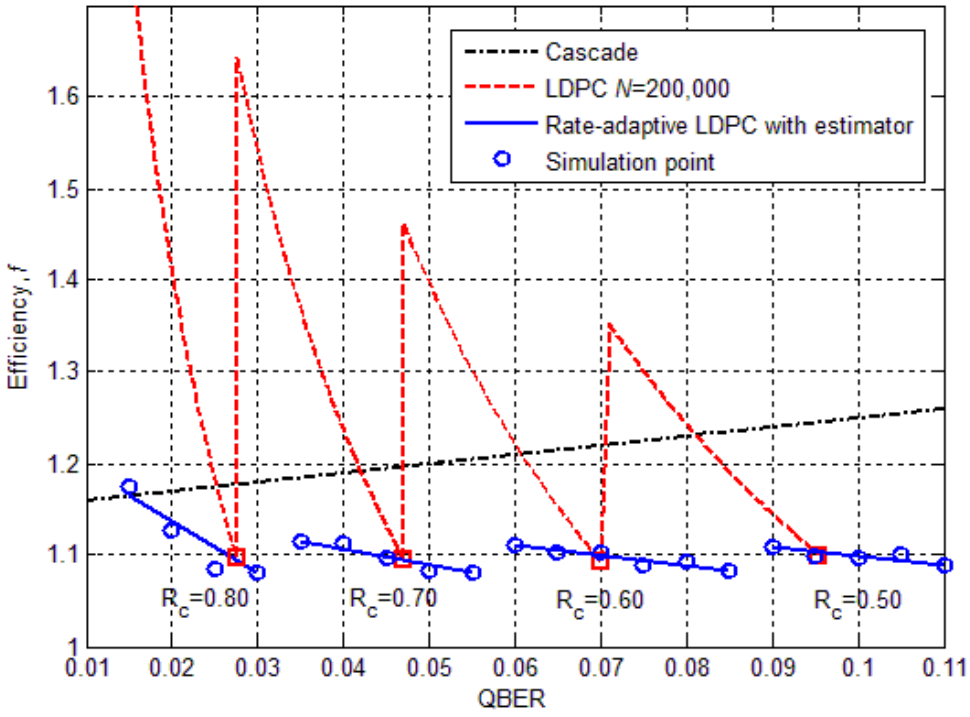


รูปที่ 5.9 ผลการประเมินค่า QBER เทียบกับค่าจริง $N = 200,000$

5.3.2 ผลการจำลองประสิทธิภาพการไกล่เกลี่ยความผิดพลาดและบิตเปิดเผย

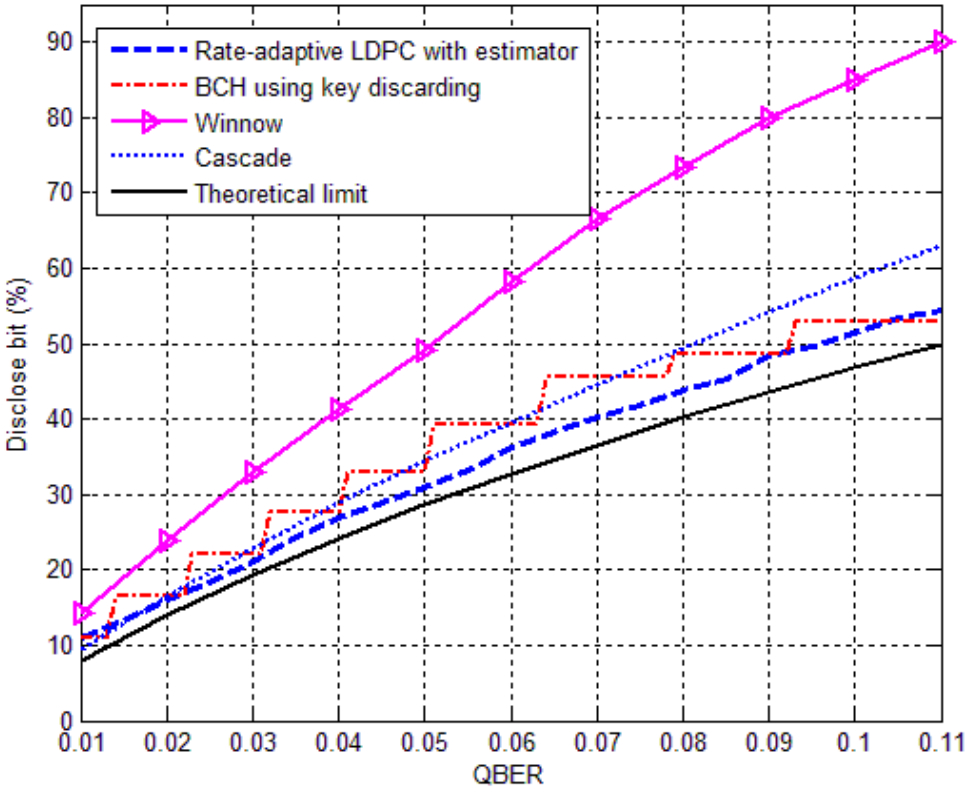
ผลการจำลองจากที่นำเสนอไว้ในหัวข้อ 4.3 ในเทอมของประสิทธิภาพไกล่ความผิดพลาดและจำนวนบิตเปิดเผย โดยวิธีการกระบวนการไกล่เกลี่ยความผิดพลาดรหัสแอลดีพีซีแบบปรับตัวเหมาะสมและการประเมินช่องสัญญาณและประสิทธิการไกล่เกลี่ยล่วงหน้าดังต่อไปนี้

รูปที่ 5.10 แสดงถึงประสิทธิภาพการไกล่เกลี่ยของระบบคำนวณได้จากสมการ 3.32 จะเห็นได้ว่าสามารถให้ประสิทธิภาพที่ดีกว่าระบบที่นิยมใช้อยู่สามารถครอบคลุมค่า QBER เกือบทั้งหมดใช้เมทริกซ์พาริตีเช็กเพียง 4 ตัวเท่านั้น ค่าประสิทธิภาพที่ได้ก็เข้าค่าทฤษฎีมากขึ้น



รูปที่ 5.10 ผลการจำลองประสิทธิการไกล่เกลี่ยรหัสแอลดีพีซีด้วยอัตรารหัสแบบปรับตัวเหมาะสมและการประเมินช่องสัญญาณ

รูปที่ 5.10 แสดงจำนวนบิตเปิดเผยระหว่างกระบวนการไกล่เกลี่ยความผิดพลาดจากการทดลองจะเห็นได้ว่าระบบที่นำเสนอสามารถให้ขีดจำกัดทางทฤษฎีกว่าระบบอื่นๆ ช่วงระหว่าง QBER เกือบทั้งหมดได้แก่โพรโทคอลที่ใช้รหัสบีซีเอช โพรโทคอลวินนาว และโพรโทคอลคาสเคด โดยค่าทฤษฎีบิตเปิดเผยสามารถคำนวณในสมการ 5.1



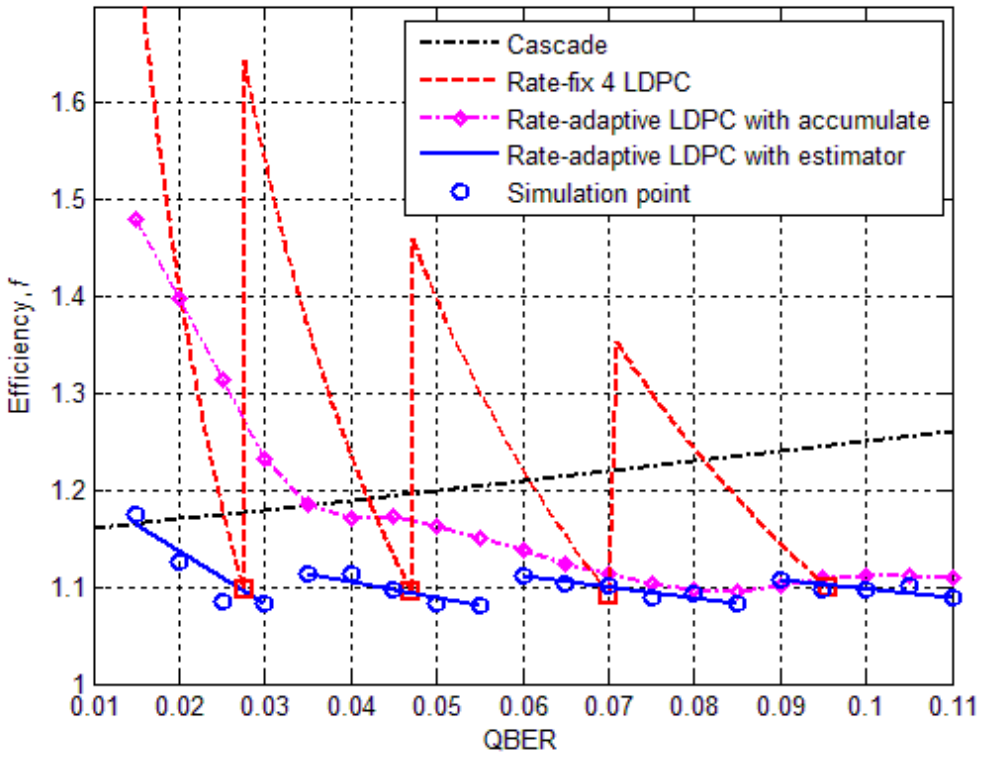
รูปที่ 5.11 ผลการจำลองจำนวนบิตเปิดเผยของรหัสแอลดีพีซีด้วยอัตรารหัสแบบปรับตัวเหมาะสมและการประเมินช่องสัญญาณ

5.4 การเปรียบเทียบผลการจำลองการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซี

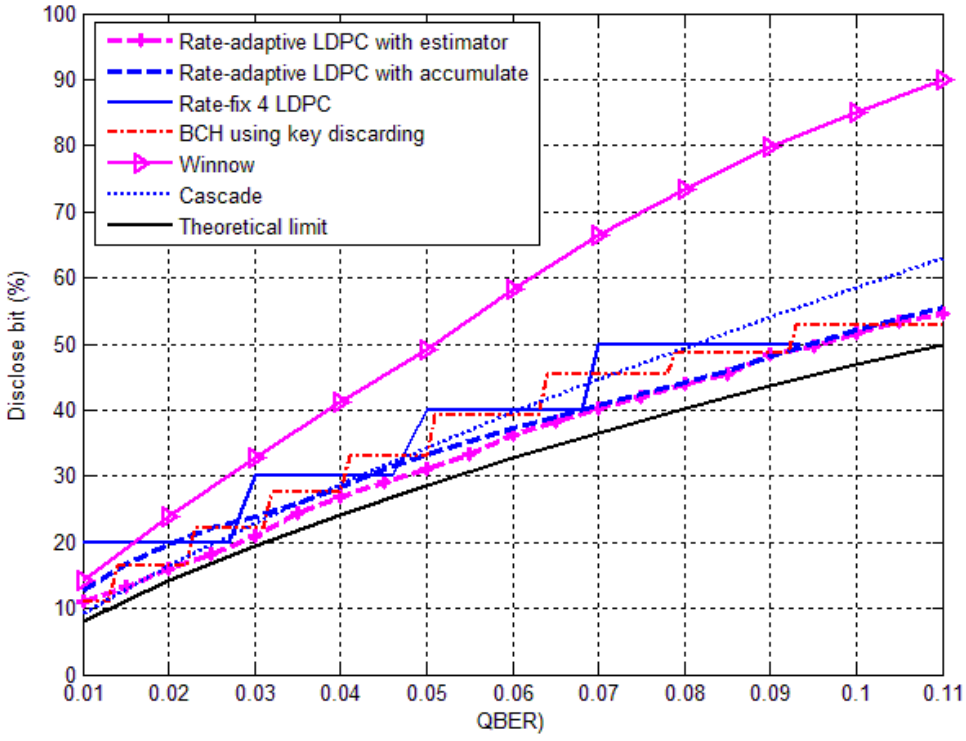
ในหัวข้อนี้จะเสนอผลการเปรียบเทียบระบบที่นำเสนอมาทั้งหมดในเทอมของค่าประสิทธิภาพการไกล่เกลี่ยความผิดพลาด จำนวนบิตเปิดเผย และอัตราการให้กำเนิดกุญแจรหัสลับ

รูปที่ 5.12 แสดงค่าประสิทธิภาพการไกล่เกลี่ยความผิดพลาดของวิธีการที่นำเสนอจะได้ว่าวิธีการไกล่เกลี่ยด้วยรหัสแอลดีพีซีแบบปรับตัวเหมาะสมร่วมกับการประเมินอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัมและค่าประสิทธิภาพการไกล่เกลี่ยล่วงหน้าให้ประสิทธิภาพที่ดีกว่าวิธีอื่นเข้าใกล้เคียงขีดจำกัดทางทฤษฎีซึ่งใช้เมทริกซ์พาริตีเช็กเพียง 4 ตัว เมื่อเปรียบเทียบกับการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีด้วยผลรวมสะสมของซินโดรม การไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีแบบอัตรารหัสคงที่ และระบบที่ใช้งานจริงในปัจจุบันโพรโทคอลคาสเคด ตามลำดับ

รูปที่ 5.13 แสดงค่าการเปรียบเทียบจำนวนบิตเปิดเผยที่ใช้ในระหว่างกระบวนการไกล่เกลี่ยจะเห็นได้ว่าระบบที่นำเสนอจะให้จำนวนบิตเปิดเผยจำนวนน้อยกว่าเข้าใกล้ค่าทางทฤษฎีมากกว่าระบบอื่นที่นำเสนอมาก่อนหน้านี้



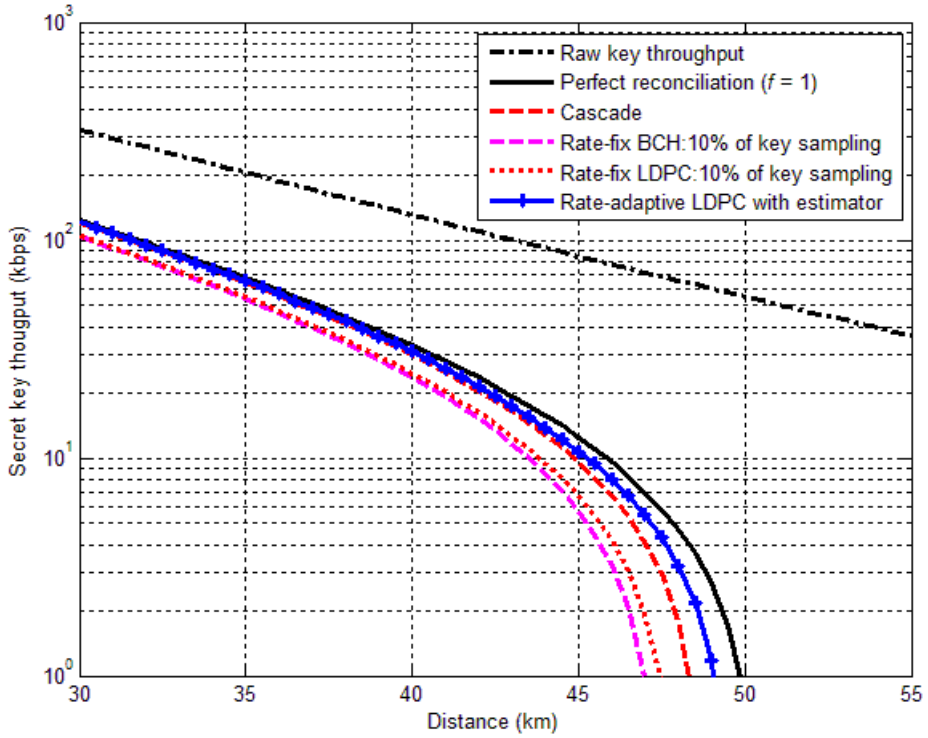
รูปที่ 5.12 ผลการเปรียบเทียบประสิทธิภาพการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซี



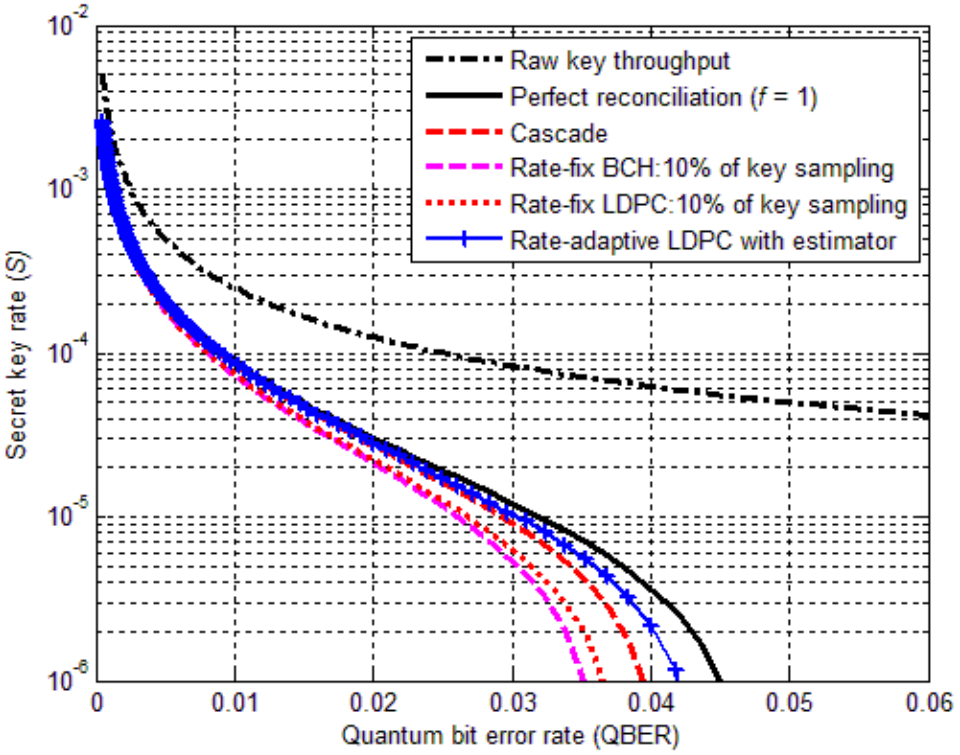
รูปที่ 5.13 ผลการเปรียบเทียบจำนวนบิตเปิดเผยการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซี

จากวิธีการที่นำเสนอสามารถแสดงเป็นขั้นตอนการไกล่เกลี่ยความผิดพลาดข้อมูลกุญแจรหัสลับด้วยรหัสแอลดีพีซีแบบปรับตัวรหัสเหมาะสมได้ในหัวข้อ 4.3 โดยผลการจำลองประสิทธิภาพการไกล่เกลี่ยความผิดพลาดตามหลักการที่ได้นำเสนอนี้ ถูกคำนวณและเปรียบเทียบกับโพรโทคอลที่ได้รับความนิยมใช้งานจริงบนตัวอย่างต้นแบบระบบการกระจายกุญแจรหัสลับเชิงควอนตัมความเร็วสูง ซึ่งแสดงเป็นกราฟความสัมพันธ์ระหว่างอัตราการกำเนิดกุญแจรหัสลับสุดท้าย (Secret key throughput) กับระยะทางในระดับการรับส่งสถานะเชิงควอนตัมผ่านเส้นใยนำแสงในรูปที่ 5.14 และอัตราการกำเนิดกุญแจรหัสลับกับค่าความผิดพลาดกุญแจรหัสลับเชิงควอนตัม (QBER) ในรูปที่ 5.15 บนเงื่อนไขของระบบฯ จริงภายใต้โพรโทคอลบีบี 84 (BB84) [38, 39] ที่ความถี่แหล่งกำเนิดสัญญาณ 1 GHz บนเส้นใยนำแสงแบบทั่วไปที่มีค่าความสูญเสีย (optical loss) 0.2 dB/km และประสิทธิภาพการตรวจรับสัญญาณ (detection efficiency) ที่ 20% บนความน่าจะเป็นของอัตราความผิดเพี้ยน (Dark counts probability) เท่ากับ 10^{-5}

ในรูปที่ 5.14 แสดงผลการเปรียบเทียบประสิทธิภาพอัตราการกำเนิดกุญแจรหัสลับสุดท้าย (Secret key throughput) ของการไกล่เกลี่ยความผิดพลาดระหว่างวิธีการที่นำเสนอคือการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีแบบปรับอัตรารหัสเหมาะสมได้พร้อมกับการประเมินอัตราความผิดพลาดกุญแจรหัสลับ (QBER) และการประเมินค่าประสิทธิภาพการไกล่เกลี่ย $f(n,\varepsilon,e)$ ล่วงหน้ากับโพรโทคอลคาสเคด (Cascade) และการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีและบีซีเอชแบบอัตรารหัสคงที่เหมาะสม จากการเปิดเผยและเปรียบเทียบบิตข้อมูลกุญแจ (key sampling) 10% ของขนาดกุญแจทั้งหมด โดยจากผลการจำลองประสิทธิภาพพบว่า วิธีการนำเสนอสามารถปรับปรุงประสิทธิภาพการไกล่เกลี่ยความผิดพลาดได้ดีกว่าโพรโทคอลที่ใช้งานจริง ดังเห็นได้จากเส้นกราฟอัตราการกำเนิดกุญแจรหัสลับของวิธีการที่นำเสนอมีค่าเข้าใกล้ขีดข้อจำกัดเชิงทฤษฎี (Perfect reconciliation) กว่าวิธีการอื่นๆ นำไปสู่การได้ระยะทางในการรับส่งสถานะเชิงควอนตัมสูงสุดและบนเงื่อนไขการให้กำเนิดอัตรากุญแจรหัสกับอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัมที่สูงกว่าดังในรูปที่ 5.15



รูปที่ 5.14 ผลการเปรียบเทียบประสิทธิภาพอัตราการกำเนิดกุญแจรหัสลับสุดท้ายกับระยะทางที่ส่ง



รูปที่ 5.15 ผลการเปรียบเทียบประสิทธิภาพอัตราการกำเนิดกุญแจรหัสลับกับ QBER

บทที่ 6
บทสรุปและข้อเสนอแนะ

บทนี้กล่าวถึงบทสรุปที่ได้จากการออกแบบและพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยการนำรหัสแอลดีพีซีมาใช้ในการพัฒนาโพรโทคอลไกล่เกลี่ยความผิดพลาดทั้งหมดและยังกล่าวถึงข้อเสนอแนะและแนวทางในการทำวิจัยต่อไปในอนาคต

6.1 บทสรุป

งานวิจัยนี้ได้ศึกษาการนำรหัสพาริตีเช็กความหนาแน่นต่ำหรือรหัสแอลดีพีซีมาประยุกต์ใช้ร่วมกับรหัสซลีเพียน-วูลฟ์หรือรหัสแหล่งกำเนิดข่าวสารข้างเคียงเพื่อแก้ไขปัญหาความผิดพลาดกุญแจรหัสลับที่เกิดจากการกระจายกุญแจรหัสลับเชิงควอนตัม โดยการออกแบบและพัฒนาโพรโทคอลเพื่อลดจำนวนรอบการติดต่อระหว่างผู้ส่งและผู้รับ เพิ่มประสิทธิภาพการไกล่เกลี่ยความผิดพลาด ให้เหมาะสมกับในแต่ล่ะช่วงของอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัม และเหมาะสำหรับนำมาใช้ในการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง เนื่องจากกุญแจรหัสลับอยู่ในรูปแบบข้อมูลไบนารี ผลการจำลองการทำงานมีรายละเอียดดังต่อไปนี้

การพัฒนาโพรโทคอลด้วยแอลดีพีซีความซับซ้อนต่ำด้วยการถอดรหัสแบบบิตฟลิปปิงและซัมโปรดักซินโดรม โพรโทคอลที่ได้พัฒนานี้สามารถลดจำนวนรอบการติดต่อระหว่างผู้ส่งและผู้รับโดยอัตรารหัสของรหัสแอลดีพีซีขึ้นอยู่กับอัตราความผิดพลาดจากการส่งกุญแจรหัสลับทางช่องสื่อสารเชิงควอนตัม (QBER) โดยผู้รับแจ้งกลับความล้มเหลวแก่ผู้ส่งถ้าหากการถอดรหัสเปรียบเทียบซินโดรมล้มเหลว จากผลการทดลองการถอดรหัสแบบบิตฟลิปปิงอย่างง่ายสามารถแก้ไขความผิดพลาดช่วง QBER ต่ำ ๆ แต่มีซับซ้อนต่ำเหมาะสำหรับจัดทำพัฒนาเป็นชุดอุปกรณ์ฮาร์ดแวร์ในขณะที่การถอดรหัสแบบซัมโปรดักให้สมรรถนะการแก้ไขความผิดพลาดที่ดีกว่า มีความซับซ้อนต่ำกว่าแบบ belief propagation algorithm แต่ก็ยังมีความซับซ้อนมากกว่าแบบบิตฟลิปปิง ในหัวนี้ได้ศึกษาอัตรารหัสและความยาวคำรหัสมีผลต่อประสิทธิภาพการไกล่เกลี่ยความผิดพลาด

การพัฒนาโพรโทคอลแก้ไขความผิดพลาดด้วยรหัสแอลดีพีซีแบบปรับตัวได้ด้วยผลรวมสะสมซินโดรม โดยปรับอัตรารหัสด้วยการส่งเพิ่มข้อมูลซินโดรมเพิ่มให้เหมาะสมกับทุกช่วง QBER ตั้งแต่ค่าน้อยสุด โดยการเข้าอัตรารหัสบีบอัดซินโดรมแบ่งเก็บไว้และส่งไปยังภาคถอดรหัสบางส่วนเรื่อยๆ จนกว่าจะแก้ไขได้สำเร็จ เมื่อทำการเปรียบเทียบผลการจำลองการกับโพรโทคอลที่มีมาก่อนหน้านี้ เช่น โพรโทคอลที่ใช้รหัสบีซีเอช โพรโทคอลวินนาว โพรโทคอลคาสเคด เป็นต้น วิธีการที่เสนอนี้จะเปิดเผยข้อมูลเกี่ยวกับกุญแจรหัสลับน้อยกว่าและมีประสิทธิภาพการไกล่เกลี่ยที่เข้าขีดจำกัดทางทฤษฎีมากกว่า

การพัฒนาโพรโทคอลด้วยรหัสแอลดีพีซีแบบปรับตัวเหมาะสมโดยการสุ่มบิตพังเจอร์และชอร์ตเทน และการประเมินความผิดพลาดกุญแจรหัสลับเชิงควอนตัมจากข้อมูลซินโดรมที่ส่งผ่านช่องสัญญาณ รวมถึงการประเมินค่าประสิทธิภาพการไกล่เกลี่ยล่วงหน้าเพื่อกำหนดค่าอัตรารหัสที่เหมาะสม โดยจากผลการทดสอบวิธีการที่นำเสนอให้ประสิทธิภาพการไกล่เกลี่ยที่ดีกว่าโดยเข้าใกล้ 1 ทางทฤษฎีด้วยจำนวนบิตเปิดเผยที่น้อยกว่า และอัตราการให้กำเนิดรหัสลับสุดท้ายที่สูงกว่าเพราะไม่ต้องสูญเสียบิตที่ต้องใช้ในการประเมินความผิดพลาดกุญแจรหัสลับเชิงควอนตัมก่อนหน้านี้และยังช่วยลดจำนวนรอบในการสื่อสารระหว่างผู้ส่งและผู้รับเพราะสามารถประมาณค่าขอบเขตประสิทธิภาพที่จะสามารถแก้ไขความผิดพลาดได้ล่วงหน้า

6.2 ข้อเสนอแนะ

หัวข้อวิจัยที่ศึกษาต่อคือการไกล่เกลี่ยความผิดพลาดในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (Continuous Variable Quantum Key Distribution: CV-QKD) เป็นระบบกระจายกุญแจรหัสลับเชิงควอนตัมรูปแบบใหม่ที่มีการส่งกุญแจกระจายตัวแบบเกาส์ ซึ่งจะทำให้สามารถส่งกุญแจรหัสลับได้ระยะทางไกลขึ้น ออกแบบและพัฒนารหัสแอลดีพีซีแบบนอนไบนารี่ (Non-binary LDPC) ประยุกต์ใช้งานร่วมในกระบวนการไกล่เกลี่ยความผิดพลาดซึ่งจะให้ประสิทธิภาพที่ดีกว่าแบบไบนารี่แต่ก็แลกมาด้วยความซับซ้อนที่เพิ่มขึ้นรวมทั้งศึกษาพารามิเตอร์ต่างๆ ที่เกี่ยวข้อง สุดท้ายนำวิธีการที่ออกแบบไว้พัฒนาเป็นซอร์ฟแวร์ที่ใช้งานในระดับห้องปฏิบัติการจริงซึ่งมีอุปกรณ์กระจายกุญแจรหัสลับและเกิดเป็นระบบกระจายกุญแจรหัสลับที่จะใช้งานติดต่อสื่อสารได้จริงในอนาคตอันใกล้นี้

รายการอ้างอิง

[1] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology,* vol. 5, pp. 3-28, 1992.

[2] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," *presented at the Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, Lofthus, Norway, 1994.

[3] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A,* vol. 67, p. 052303, 2003.

[4] P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, and O. Sangaroon, "Performance of 1/2-rate convolutional code on Winnow protocol for quantum key reconciliation," in *International Symposium on Communications and Information Technologies (ISCIT)*, pp. 550-553, 2010.

[5] W. Traisilanun, K. Sripimanwat, and O. Sangaroon, "Secret key reconciliation using BCH code in quantum key distribution," in *International Symposium on Communications and Information Technologies (ISCIT '*07*)*, pp. 1482-1485, 2007.

[6] P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, and O. Sangaroon, "BCH-based Slepian-Wolf coding with feedback syndrome decoding for quantum key reconciliation," in *International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp. 1-4, 2012.

[7] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *IEEE International Symposium on Information Theory, ISIT* 2009. pp. 1879-1883, 2009.

[8] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Interactive reconciliation with low-density parity-check codes," in *International Symposium on Turbo Codes and Iterative Information Processing (ISTC),* pp. 270-274*,* 2010,.

[9] D. Elkouss Coronas, J. Martinez Mateo, and V. Martín Ayuso, "Information reconciliation for quantum key distribution," *Quantum Information and Computation,* vol. 11, pp. 226-238, 2011.

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

[11] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Analysis of a rate-adaptive reconciliation protocol and the effect of leakage on the secret key rate," *Physical Review A,* vol. 87, no. 4, p. 042334, 2013.

[12] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Secure rate-adaptive reconciliation," in 2010 *International Symposium on Information Theory and its Applications (ISITA)*, pp. 179-184, 2010.

[13] V. Toto-Zarasoa, A. Roumy, and C. Guillemot, "Maximum Likelihood BSC Parameter Estimation for the Slepian-Wolf Problem," *Communications Letters, IEEE,* vol. 15, pp. 232-234, 2010,

[14] J. Ha, J. Kim, and S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Transactions on Information Theory,* vol. 50, pp. 2824-2836, 2004.

[15] J. Ha, J. Kim, D. Klinc, and S. W. McLaughlin, "Rate-compatible punctured low-density parity-check codes with short block lengths," *IEEE Transactions on Information Theory,* vol. 52, pp. 728-738, 2006.

[16] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE International Conference on computers, Systems & Signal Processing*, Bangalore, India, pp. 175-179, December 1984,.

[17] ID Quantique SA. A fast and secure solution: high speed encryption combined with quantum key distribution [Online].

[18] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," *Zeitschrift für Physik,* vol. 43, pp. 172-198, 1927.

[19] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.,* vol. 17, pp. 210-229, 1988.

[20] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory,* vol. 39, pp. 733-742, 1993.

[21] R. Renner, "Security of Quantum Key Distribution," Ph.D., ETH Zurich (Swiss Federal Institute of Technology), 2005.

[22] T. Sugimoto and K. Yamazaki, "A Study on Secret Key Reconciliation Protocol "Cascade," *IEICE TRANSACTIONS on Fundamentals of Electronics Communications and Computer Sciences,* vol. E83-A, pp. 1987-1991, 2000.

[23] Y. Hao, P. Xiang, L. Xiaxiang, J. Wei, L. Tian, and H. Guo, "Efficiency of Winnow Protocol in Secret Key Reconciliation," in *WRI World Congress on Computer Science and Information Engineering,* , pp. 238-242, 2009.

[24] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal, The,* vol. 27, pp. 379-423, 1948.

[25] R. G. Gallager, "Low-density parity-check codes," *Information Theory, IRE Transactions on,* vol. 8, pp. 21-28, 1962.

[26] พ. วนิชชานันท์, ทฤษฎีรหัสช่องสัญญาณ *"Channel coding theory",* . กรุงเทพฯ: สถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม (สพท), 2009.

[27] ป. โควินท์ทวีวัฒน์, การประมวลผลสัญญาณสำหรับการจัดเก็บข้อมูลดิจิทัล เล่ม3: การออกแบบวงจรภาครับขั้นฟ vol. 3. นครปฐม: โปรแกรมวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏนครปฐม, 2011.

[28] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Transactions on Information Theory,* vol. 47, pp. 599-618, 2001.

[29] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory,* vol. 19, pp. 471-480, 1973.

[30] T. Phromsa-ard, P. Sangwongngam, K. Sripimanwat, K. Kaemarungsri, P. Vanichchanunt, and L. Wuttisittikulkij, "Low-complexity key reconciliation algorithm using LDPC bit-flipping decoding for quantum key distribution," in *International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON),* pp. 1-5, 2014.

[31] T. Phromsa-ard, J. Arpornsiripat, J. Wetcharungsri, P. Sangwongngam, K. Sripimanwat, and P. Vanichchanunt, "Improved Gradient Descent Bit Flipping algorithms for LDPC decoding," in *Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP)*, pp. 324-328, 2012.

[32] A. D. Liveris, X. Zixiang, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Communications Letters,* vol. 6, pp. 440-442, 2002.

[33] D. Varodayan, A. Aaron, and B. Girod, "Rate-adaptive codes for distributed source coding," *Signal Processing,* vol. 86, pp. 3123-3130, 2006.

[34] C. Yu and G. Sharma, "Improved low-density parity check accumulate (LDPCA) Codes," *IEEE Transactions on Communications,* vol. 61, pp. 3590-3599, 2013.

[35] T. Phromsa-ard, P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, K. Kaemarungsi, P. Vanichchanunt*, et al.*, "Efficient rate-adaptive reconciliation based on LDPC accumulate Codes for Quantum Key Distribution," in *International Technical Conference on Circuits/Systems, Computers and Communication (ITC-CSCC* 2015*),* Seoul, Korea, pp. 89-92, 2015

[36] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, "Fundamental finite key limits for information reconciliation in quantum key distribution," in 2014 *IEEE International Symposium on Information Theory (ISIT)*, pp. 1469-1473*,* 2014

[37] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Transactions on Information Theory,* vol. 51, pp. 386-398, 2005.

[38] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in. *Proceedings. International Symposium on Information Theory, ISIT* 2004 , p. 136, 2004.

[39] 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, p. 1301, 2009.

ประวัติผู้เขียนวิทยานิพนธ์

นายธราธร พรมสะอาด เกิดวันที่ 20 สิงหาคม พ.ศ. 2531 ที่จังหวัดอุบลราชธานี ได้เข้ารับการศึกษาในหลักสูตรวิศวกรรมศาสตรบัณฑิต คณะวิศวกรรมศาสตร์ มหาวิทยาลัยอุบลราชธานี ในปีการศึกษา 2550 และสำเร็จการศึกษาปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้า เกียรตินิยมอันดับสอง ในปีการศึกษา 2553 จากนั้นจึงได้เข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2555