การพัฒนาคุณภาพจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสแก้ไขความผิดพลาด

SECRET KEY RECONCILIATION IN QUANTUM KEY DISTRIBUTION WITH FORWARD ERROR CORRECTING CODE

วุฒิกรณ์ ตรัยศิลานันท์

WUTHIGORN TRAISILANUN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2551

KMITL-2008-EN-M-230-133

การพัฒนาคุณภาพจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสแก้ไขความผิดพลาด

SECRET KEY RECONCILIATION IN QUANTUM KEY DISTRIBUTION WITH FORWARD ERROR CORRECTING CODE

วุฒิกรณ์ ตรัยศิลานันท์

WUTHIGORN TRAISILANUN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2551

KMITL–2008–EN–M–230–133

SECRET KEY RECONCILIATION IN QUANTUM KEY DISTRIBUTION WITH FORWARD ERROR CORRECTING CODE

WUTHIGORN TRAISILANUN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN INFORMATION ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2008

KMITL–2008–EN–M–230–133

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การพัฒนาคุณภาพจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสแก้ไขความผิดพลาด

Secret Key Reconciliation in Quantum Key Distribution With Forward Error Correcting Code

นักศึกษา นายวุฒิกรณ์ ตรัยศิลานันท์

รหัสประจำตัว 48061016

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมสารสนเทศ

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.อรลาภ แสงอรุณ

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.กนก	เจนจิระพงศ์เวช	
รศ.ดร.ชวลิต	เบญจางคประเสริฐ	
ดร.เกียรติศักดิ์	ศรีพิมานวัฒน์	
รศ.นภพินทุ์	อนันตรศิริชัย	
รศ.อรลาภ	แสงอรุณ	

วัน / เดือน/ ปี ที่สอบ 6 มีนาคม 2551 เวลา 13.30-15.30 น.

สถานที่สอบ ณ ห้องประชุม 1 ชั้น 3 อาคาร A

บัณฑิตวิทยาลัยรับรองแล้ว

(รศ.ดร.รวีวรรณ ชินะตระกูล)

คณบดีบัณฑิตวิทยาลัย

วันที่ 14 **เดือน** มีนาคม **พ.ศ.** 2551

หัวข้อวิทยานิพนธ์	การพัฒนาคุณภาพจากการกระจายกุญแจรหัสลับเชิงควอนตัม ด้วยรหัสแก้ไขความผิดพลาด
นักศึกษา	นายวุฒิกรณ์ ตรัยศิลานันท์
รหัสนักศึกษา	48061016
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
พ.ศ.	2551
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.อรลาภ แสงอรุณ
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์

บทคัดย่อ

วิทยาการรหัสลับเชิงควอนตัมเป็นระบบที่ใช้ในการส่งกุญแจรหัสลับ โดยอาศัยคุณสมบัติทางควอนตัมของแสง แต่เนื่องจากสัญญาณรบกวน ความไม่เป็นอุดมคติของอุปกรณ์ทั้งทางภาครับและทางภาคส่งเป็นสาเหตุทำให้กุญแจรหัสลับที่ส่งเกิดความผิดพลาดขึ้นได้ วิทยานิพนธ์นี้นำเสนอการนำรหัสบีซีเอชและรหัสคอนโวลูชันมาประยุกต์ร่วมกับ การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง (Side Information) และการนำรหัสบีซีเอชมาประยุกต์พัฒนาโพรโทคอลฟุรุคาวาเพื่อใช้แก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม ซึ่งผลการจำลองการทำงานการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) เมื่อพิจารณาอัตราความผิดพลาดที่เหลือจากการแก้ไขความผิดพลาดน้อยกว่า 10^{-3} เมื่อนำรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างและนำรหัสบีซีเอชมาพัฒนาโพรโทคอลฟุรุคาวา วิธีการที่นำเสนอนี้จะมีการการติดต่อระหว่างผู้ส่ง (*Alice*) และผู้รับ (*Bob*) เพียงหนึ่งรอบ สามารถแก้ไขความผิดพลาดที่อัตราความผิดพลาดของกุญแจรหัสลับทางช่องสื่อสารเชิงควอนตัม (QBER) น้อยกว่า 8% และ 10% ตามลำดับ เมื่อเปรียบเทียบกับโพรโทคอลคาสเคดและโพรโทคอลวินนาว ที่ใช้จำนวนรอบในการติดต่อระหว่างผู้ส่งและผู้รับมากกว่า แต่วิธีการที่นำเสนอนี้จะมีปริมาณข้อมูล ที่ส่งผ่านช่องสื่อสารสาธารณะสูงกว่า การนำรหัสคอนโวลูชันมาใช้แก้ไขความผิดพลาดร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง ผลการจำลองการทำงานพบว่าที่ค่า Constraint Length เท่ากับสามและอัตราการเข้ารหัสเท่ากับ 1/2 หลักการที่นำเสนอนี้สามารถลดจำนวนรอบการติดต่อระหว่างผู้ส่งและผู้รับลงได้ แต่จะให้ประสิทธิภาพการแก้ไขความผิดพลาดที่ต่ำและปริมาณข้อมูลที่ส่งผ่านช่องสื่อสารสาธารณะสูงขึ้นเมื่อเปรียบเทียบกับโพรโทคอลวินนาวและโพรโทคอลฟุรุคาวา ทั้งนี้วิธีการที่นำเสนอนี้สามารถนำไปประยุกต์ใช้เพื่อแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD) ร่วมกับการแก้ไขข้อผิดพลาดแบบสไลซ์ได้ด้วย

Thesis Title	Secret Key Reconciliation in Quantum Key Distribution with Forward Error Correcting Code
Student	Mr. Wuthigorn Traisilanun
Student ID.	48061016
Degree	Master of Engineering
Program	Information Engineering
Year	2008
Thesis Advisor	Assoc. Prof. Ornlarp Saengaroon
Co-Thesis Advisor	Dr.Keattisak Sripimanwat

ABSTRACT

Quantum cryptography is the advanced method to send the secret key. Generally, its principle form is to encrypt via the quantum state of light. However, many factors such as in the noisy quantum channel cause the uncorrelated key and affect to the system performance. This thesis presents applications of forward error correcting codes of BCH codes and convolutional code for an error correcting protocol in the process of quantum key distribution. First, BCH code is applied on the problem of side-information source coding. Next, BCH code with Furukawa's protocol in order to reduce interactivities between *Alice* and *Bob,* is studied. Simulation results in the case of discrete variable quantum key distribution (DV-QKD) show that these proposed methods can reduce interactivities between *Alice* and *Bob* with quantum bit error rate less than 8% and 10%, respectively. However, both methods reveal the amount of secret key information more than those of the CASCADE and Winnow protocol. Alternatively, another case of convolution code with side-information source coding is done comparatively. Although this higher potential coding scheme reduces the number of interactivity, it obtains lower performance on error and reveals the number of secret key information more than those of protocols (Winnow and Furukawa).In addition, all proposed methods can be used to correct the error in continuous variable quantum key distribution (CV-QKD) with slice error correction.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้เป็นอย่างดี ด้วยความช่วยเหลือและสนับสนุนจากหลายๆ ฝ่ายด้วยกัน โดยผู้เขียนขอขอบพระคุณดังต่อไปนี้

ขอขอบคุณ รศ.อรลาภ แสงอรุณ อาจารย์ผู้ควบคุมวิทยานิพนธ์ ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังและ ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์ อาจารย์ผู้ควบคุมวิทยานิพนธ์ร่วมและนักวิจัยจากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ในการให้ความรู้ คำแนะนำและคำปรึกษาที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์เล่มนี้ ผู้เขียนรู้สึกซาบซึ้งในความอนุเคราะห์และขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบคุณภาควิชาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังที่ประสิทธิประสาทวิชาความรู้ ที่เป็นพื้นฐานในการทำวิทยานิพนธ์เล่มนี้

ขอขอบคุณศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ อุทยานวิทยาศาสตร์ประเทศไทย ในการใช้สถานที่เพื่อทำวิจัยในวิทยานิพนธ์เล่มนี้

ขอขอบพระคุณทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST) ที่สนับสนุนทุนการศึกษาระหว่างปีการศึกษา 2547 ถึง 2550 เพื่อทำการวิจัยในวิทยานิพนธ์เล่มนี้

ขอขอบพระคุณทีมงานทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST) ที่ให้ความช่วยเหลือเป็นอย่างดีตลอดระยะเวลาการรับทุน

ขอขอบคุณทีมงานผู้ช่วยนักวิจัย หน่วยปฏิบัติการวิจัยการสื่อสารเชิงแสงและควอนตัม (OQC) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ที่ให้ความรู้ ความร่วมมือและความช่วยเหลือเกี่ยวกับวิทยาการรหัสลับเชิงควอนตัมเป็นอย่างดี

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ทางผู้จัดทำขอมอบแด่ผู้มีพระคุณทุกท่านไว้ ณ โอกาสนี้

วุฒิกรณ์ ตรัยศิลานันท์

สารบัญ

หน้า

บทคัดย่อภาษาไทย I

บทคัดย่อภาษาอังกฤษ II

กิตติกรรมประกาศ III

สารบัญ IV

สารบัญรูป IX

สารบัญตาราง XI

รายการคำย่อ XII

รายการสัญลักษณ์ XIII

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 2

1.2 ความมุ่งหมายและวัตถุประสงค์ของงานวิจัย 5

1.3 ขอบเขตงานวิจัย 5

1.4 ขั้นตอนการวิจัย 6

1.5 รายละเอียดวิทยานิพนธ์ 6

บทที่ 2 ระบบสื่อสารดิจิตอลและรหัสแก้ไขความผิดพลาด 8

2.1 ระบบสื่อสารดิจิตอล 8

2.2 ภาคเข้ารหัสแหล่งกำเนิด 9

2.2.1 ปริมาณข่าวสารและปริมาณข่าวสารเฉลี่ย 9

2.2.2 การเข้ารหัสแหล่งกำเนิด 13

2.3 ช่องสัญญาณและสัญญาณรบกวน 15

2.3.1 ซ็อตนอยส์ 15

2.3.2 สัญญาณรบกวนเนื่องจากอุณหภูมิ 16

2.4 การเข้ารหัสช่องสัญญาณ 17

2.4.1 การแก้ไขความผิดพลาดของข้อมูลในระบบสื่อสารดิจิตอล 18

2.4.2 รหัสแก้ไขความผิดพลาดล่วงหน้า 18

2.5 ตัวอย่างรหัสแก้ไขความผิดพลาดล่วงหน้า 19

2.5.1 รหัสแบบบล็อกเชิงเส้น 19

2.5.1.1 ความสามารถในการตรวจจับและแก้ไขความผิดพลาด 20

สารบัญ (ต่อ)

หน้า

2.5.1.2 การเข้ารหัสแบบบล็อกเชิงเส้น 20

2.5.1.3การถอดรหัสแบบบล็อกเชิงเส้น 21

2.5.2 รหัสแฮมมิง 21

2.5.2.1 การเข้ารหัสแฮมมิง 22

2.5.2.2การถอดรหัสแฮมมิง 22

2.5.3 รหัสบีซีเอช 27

2.5.3.1 พหุนามกำเนิดรหัสบีซีเอช 27

2.5.3.2 การเข้ารหัสบีซีเอช 28

2.5.3.3 การถอดรหัสบีซีเอช 28

2.5.4 รหัสคอนโวลูชัน 28

2.5.4.1การเข้ารหัสคอนโวลูชัน 29

2.5.4.2การถอดรหัสคอนโวลูชัน 31

2.5.4.3 การถอดรหัสคอนโวลูชันด้วยวิธีไวเทอร์บี 31

บทที่ 3 วิทยาการรหัสลับเชิงควอนตัม 33

3.1 ประวัติวิทยาการรหัสลับเชิงควอนตัม 35

3.2 วิทยาการรหัสลับเชิงควอนตัม 36

3.2.1 การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง 37

3.2.2 การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง 40

3.3 กระบวนการกลั่นกุญแจรหัสลับ 43

3.3.1 การไกล่เกลี่ยความผิดพลาด 43

3.3.2 การขยายสภาวะส่วนตัว 43

3.4 การประยุกต์ระบบวิทยาการรหัสลับเชิงควอนตัม 44

3.4.1 การประยุกต์ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง 44

3.4.1.1 การส่งกุญแจรหัสลับบิตด้วยโพลาไรเซชันของโฟตอนเดี่ยว 45

3.4.1.2 การส่งกุญแจรหัสลับบิตด้วยเฟสของโพลาไรเซชัน 47

3.4.2 การประยุกต์ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง 51

3.5 การเปรียบเทียบระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่องและแบบต่อเนื่อง 53

สารบัญ (ต่อ)

หน้า

3.5.1 ความแตกต่างของแหล่งกำเนิด 53
3.5.2 ความแตกต่างด้านอุปกรณ์ตรวจจับแสง 55
3.5.3 ความแตกต่างของกุญแจรหัสลับ
และกระบวนการไกล่เกลี่ยความผิดพลาด 55

บทที่ 4 กระบวนการไกล่เกลี่ยความผิดพลาดของกุญแจรหัสลับ 58
4.1 การวัดปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับ 59
4.1.1ปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับในระบบ DV-QKD 60
4.1.2 ปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับในระบบ CV-QKD 61
4.2 ข้อจำกัดของแชลนอนในระบบกระจายกุญแจรหัสลับเชิงควอนตัม 66
4.3 อัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัม 67
4.4 ตัวอย่างโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม 67
4.4.1 โพรโทคอล BBBSS 68
4.4.1.1หลักการพื้นฐานของพาริตี้บิต 68
4.4.1.2 การทำงานของโพรโทคอล BBBSS 69
4.4.2 โพรโทคอล CASCADE 71
4.4.3 โพรโทคอล Winnow 75
4.4.3.1 การเปรียบเทียบพาริตี้บิต 75
4.4.3.2 การแก้ไขความผิดพลาดด้วยโพรโทคอล Winnow 76
4.4.4 การแก้ไขความผิดพลาดด้วยรหัสบล็อกเชิงเส้นตามวิธีของฟุรุคาวา 80
4.5 การแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง 83
4.5.1 การแก้ไขข้อผิดพลาดแบบสไลซ์ 83
4.5.2 การประมาณค่าจากจำนวนจริงเป็นตัวเลขแบบไบนารี 84
4.5.2.1 การประมาณค่ากุญแจรหัสลับบิตของ *Alice* 87
4.5.2.2 การประมาณค่ากุญแจรหัสลับบิตของ *Bob* 88

บทที่ 5 วิธีการออกแบบและจำลองการทำงาน 92
5.1 การออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาด 92
5.1.1 รหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 93

สารบัญ (ต่อ)

หน้า

5.1.1.1 การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 93

5.1.1.2 พื้นฐานรหัสบีซีเอช 94

5.1.1.3 การพัฒนาโพรโทคอลด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 95

5.1.2 การพัฒนาการแก้ไขความผิดพลาดวิธีฟุรุคาวาด้วยรหัสบีซีเอช 99

5.1.3 การพัฒนาโพรโทคอลด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 102

5.2 การจำลองการทำงานกระบวนการรับส่งกุญแจรหัสลับเชิงควอนตัม 103

5.2.1 การจำลองการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง 104

5.2.2 การจำลองการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง 106

5.3 การจำลองการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม 106

5.3.1 การจำลองการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง 107

5.3.2 การจำลองการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง 116

บทที่ 6 ผลการจำลองการทำงาน 119

6.1 การแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง 119

6.1.1 กระบวนการแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 119

6.1.2 การนำรหัสบีซีเอชมาพัฒนาโพรโทคอลของฟุรุคาวา 122

6.1.3 กระบวนการแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 125

6.2 การแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง 127

บทที่ 7 สรุปและข้อเสนอแนะ 130

7.1 สรุปผลการวิจัย 130

7.2 ปัญหาและอุปสรรคที่พบในงานวิจัย 132

7.3 ข้อเสนอแนะในการพัฒนา 132

สารบัญ (ต่อ)

หน้า

เอกสารอ้างอิง 133
ภาคผนวก ก พื้นฐานทฤษฎีความน่าจะเป็นกับวิทยาการรหัสลับเชิงควอนตัม 137
ภาคผนวก ข อุปกรณ์เชิงแสงสำหรับระบบวิทยาการรหัสลับเชิงควอนตัม 152
บัญชีศัพท์ 154
ประวัติผู้เขียน 158

สารบัญรูป

รูปที่ หน้า

1.1 การทำงานของระบบวิทยาการรหัสลับเชิงควอนตัม 3

2.1 ไดอะแกรมองค์ประกอบพื้นฐานของระบบสื่อสารดิจิตอล 9

2.2 ปริมาณข่าวสารเฉลี่ยของแหล่งกำเนิดข้อมูลข่าวสารสองสัญลักษณ์ 12

2.3 การทำงานของรหัสฮัฟแมน 14

2.4 คุณสมบัติของสัญญาณรบกวนแบบขาว 17

2.5 ตัวอย่างวงจรเข้ารหัสคอนโวลูชันแบบสมมาตร 30

2.6 ตัวอย่างวงจรเข้ารหัสคอนโวลูชันแบบอสมมาตร 30

3.1 การทำงานของวิทยาการรหัสลับ 34

3.2 กระบวนการกระจายกุญแจรหัสลับเชิงควอนตัม 42

3.3 โครงสร้างพื้นฐานระบบวิทยาการรหัสลับเชิงควอนตัมใช้สถานะโพลาไรเซชัน 46

3.4 พื้นฐานระบบวิทยาการรหัสลับเชิงควอนตัมใช้ Mach-Zehnder Interferometer 46

3.5 ระบบวิทยาการรหัสลับเชิงควอนตัมใช้ Mach-Zehnder Interferometer สองระบบ 49

3.6 ลักษณะสัญญาณพัลส์ที่ภายใน Mach-Zehnder Interferometer 49

3.7 การรวมกันของสัญญาณพัลส์ก่อนถึงตัวตรวจจับที่ *Bob* 49

3.8 พื้นฐานระบบวิทยาการรหัสลับเชิงควอนตัมแบบแบบปรับเปลี่ยนเฟสอัตโนมัติ 51

3.9 พื้นฐานระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องด้วยโคฮีเรนต์ของแสง 52

3.10 ความน่าจะเป็นในการพบโฟตอนภายในพัลส์แสง 54

3.11 การกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง 56

3.12 การกระจายกุญแจรหัสลับแบบต่อเนื่อง 56

4.1 ช่องสัญญาณแบบไบนารี 61

4.2 ความสัมพันธ์ระหว่างประสิทธิภาพและการสูญเสียภายในช่องสื่อสารเชิงควอนตัม 63

4.3 ความสัมพันธ์ระหว่างสัญญาณรบกวนในสถานะพื้นและประสิทธิภาพของช่องสื่อสาร 64

4.4 ปริมาณข่าวสารสุทธิระหว่าง *Bob* และ *Eve* ที่ความแปรปรวนเท่ากับสาม กรณีการไกล่เกลี่ยความผิดพลาดย้อนกลับ 64

4.5 ปริมาณข่าวสารสุทธิระหว่าง *Bob* และ *Eve* ที่ความแปรปรวนเท่ากับสาม กรณีการไกล่เกลี่ยความผิดพลาดทางตรง 66

4.6 ตัวอย่างการทำงานของโพรโทคอล BBBSS 70

4.7 ตัวอย่างการทำงานของโพรโทคอล CASCADE 72

4.8 การแบ่งบล็อกกุญแจรหัสลับและการหาพาริตี้บิตของโพรโทคอล Winnow 78

สารบัญรูป (ต่อ)

รูปที่ หน้า

4.9 การแบ่งฟังก์ชันการกระจายแบบเกาส์ออกเป็น 4 ส่วนคือ $\tau_0 \le x < \tau_1$, $\tau_1 \le x < \tau_2$, $\tau_2 \le x < \tau_3$ และ $\tau_3 \le x < \tau_4$ 85

4.10 ตัวอย่างการกำหนดค่าไบนารีเมื่อจำนวนสไลซ์เท่ากับสอง 88

4.11 การประมาณค่าบิตของ *Bob* เมื่อจำนวนสไลซ์เท่ากับสอง 90

5.1 การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 94

5.2 วิธีการแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 96

5.3 การแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 101

5.4 แผนภาพการจำลองการสร้างกุญแจรหัสลับแบบไม่ต่อเนื่อง 105

5.5 แผนภาพการสร้างกุญแจรหัสลับที่กระจายตัวแบบเกาส์ 107

5.6 กระบวนการหาพาริตี้บิตของรหัสบีซีเอชทางด้าน *Alice* 109

5.7 กระบวนการสร้างคำรหัสใหม่และแก้ไขความผิดพลาดของ *Bob* 110

5.8 การแก้ไขความผิดพลาดด้วยรหัสบีซีเอชทาง *Alice* 112

5.9 การแก้ไขความผิดพลาดด้วยรหัสบีซีเอชทาง *Bob* 113

5.10 กระบวนการหาพาริตี้บิตของรหัสคอนโวลูชันทางด้าน *Alice* 115

5.11 กระบวนการสร้างคำรหัสคอนโวลูชันใหม่และแก้ไขความผิดพลาดของ *Bob* 116

5.12 แผนภาพการทำงานการแก้ไขความผิดพลาดแบบสไลซ์ 118

6.1 การเปรียบเทียบความสามารถในการแก้ไขความผิดพลาดรหัสบีซีเอชที่อัตราความสามารถในการแก้ไขความผิดพลาดเท่ากับหนึ่ง 120

6.2 การเปรียบเทียบประสิทธิภาพการแก้ไขความผิดพลาดของรหัสบีซีเอชที่อัตราความสามารถในการแก้ไขความผิดพลาดต่างกัน 120

6.3 การเปรียบเทียบจำนวนพาริตี้บิตที่ส่ง 122

6.4 การเปรียบเทียบประสิทธิภาพของรหัสบีซีเอชเมื่อนำมาใช้ในการพัฒนาวิธีฟุรุคาวา 123

6.5 ประสิทธิภาพการนำรหัสคอนโวลูชันมาใช้ในการแก้ไขความผิดพลาด 126

สารบัญตาราง

ตารางที่ หน้า

2.1 การเข้ารหัสแฮมมิง 23

2.2 การเข้ารหัสแฮมมิงด้วยบิตข้อมูลขนาด 4 บิต ("1010") 23

2.3 การตรวจสอบความผิดพลาดเมื่อเกิดการผิดของบิต 23

3.1 สัญลักษณ์และสถานะโพลาไรเซชันของกุญแจรหัสลับบิตของโพรโทคอลBB84 39

3.2 ความสัมพันธ์ระหว่างมุมเฟสกับโพลาไรเซชันในโพรโทคอล BB84 39

3.3 สัญลักษณ์และการส่งกุญแจรหัสลับบิตด้วยเฟสของโพลาไรเซชันของโฟตอนเดี่ยว 39

3.4 สัญลักษณ์และการส่งกุญแจรหัสลับบิตด้วยโพรโทคอล GG02 42

4.1 ตัวอย่างการหาพาริตี้บิตของข้อมูลขนาด 7 บิต 68

4.2 ความน่าจะเป็นของจำนวนบิตผิดในบล็อกและการกระจายแบบปัวส์ซอง 72

6.1 การจำลองการแก้ไขความผิดพลาด ที่ค่าอัตราการผิดของบิต 0.01 (1%) และจำนวน
กุญแจรหัสลับ 10,200 บิต 124

6.2 การจำลองการแก้ไขความผิดพลาด ที่ค่าอัตราการผิดของบิต 0.1 (10%) และจำนวน
กุญแจรหัสลับ 10,200 บิต 124

6.3 การจำลองการแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัส
แหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง 126

6.4 ค่าจำนวนจริงที่แบ่งช่วงบนฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ 128

6.5 ผลการจำลองการทำงานการแก้ไขข้อผิดพลาดแบบสไลซ์ 128

6.6 การแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูล
ข่าวสารข้างในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง 129

รายการคำย่อ

ARQ	Automatic Retransmission Query หรือ Automatic Repeat Request
BCP	Binary Correcting Protocol
BER	Bit Error Rate
BS	Beam Splitter
BSC	Binary Symmetric Channel
CV-QKD	Continuous Variable Quantum Key Distribution
DMC	Discrete Memoryless Channel
DV-QKD	Discrete Variable Quantum Key Distribution
FEC	Forward Error Correcting Code
FSK	Frequency Shift Keying
GF	Galois Field
HWP	Haft-Wave Plate
K	Constraint Length
LED	Light Emitting Diode
PBS	Polarizing Beam Splitter
PD	Photodiode
PM	Phase Modulator
PSK	Phase Shift Keying
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
SEC	Slice Error Correction
SNR	Signal to Noise Ratio

รายการสัญลักษณ์

ขนาดของข้อมูล (บิต)	k
ขนาดของบล็อก (บิต)	N
ขนาดของบล็อกคำรหัส (บิต)	n
ความยาวทั้งหมดของกุญแจรหัสลับ	l
ความสามารถในการแก้ไขความผิดพลาด (บิต)	t
คำรหัส	C
ซินโดรม	S
ปริมาณข่าวสาร (บิตต่อสัญลักษณ์)	I
ปริมาณข่าวสารเฉลี่ย (บิตต่อสัญลักษณ์)	H
ปริมาณข่าวสารร่วมระหว่าง X และ Y (บิตต่อสัญลักษณ์)	$I(X;Y)$
โพลาไรเซชันมุม 0 องศา	$\rightarrow$
โพลาไรเซชันมุม 45 องศา	$\nearrow$
โพลาไรเซชันมุม -45 องศา	$\searrow$
โพลาไรเซชันมุม 90 องศา	$\uparrow$
เฟสของสถานะโคฮีเรนต์	P
มุมเฟสของโพลาไรเซชัน (องศาหรือเรเดียน)	θ
เมทริกซ์กำเนิด	G
เมทริกซ์ตรวจสอบพาริตี้	H
ระยะห่างแฮมมิ่งต่ำสุด	$d_{\min}$
เวกเตอร์ฐานที่แทนโพลาไรเซชันมุม 45 องศา และ โพลาไรเซชันมุม -45 องศา	$\otimes$
เวกเตอร์ฐานที่แทนโพลาไรเซชันมุม 90 องศา และ โพลาไรเซชันมุม 0 องศา	$\oplus$
แอมพลิจูด	A
อัตราความผิดพลาด	e

บทที่ 1
บทนำ

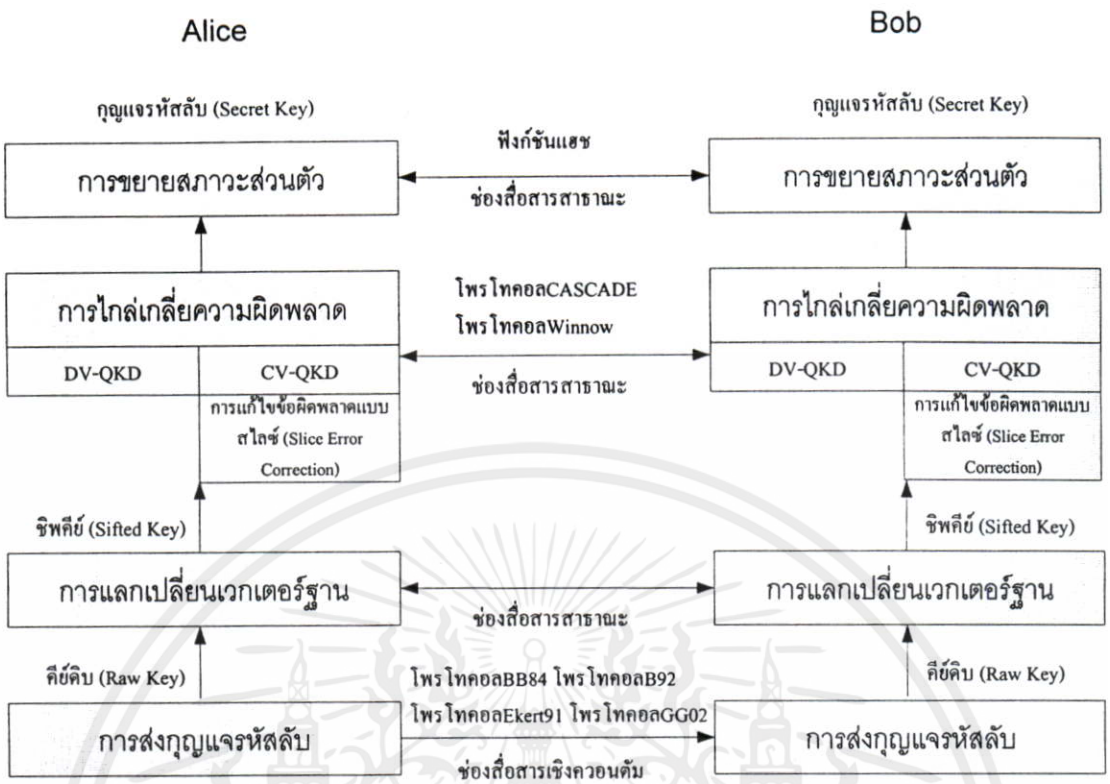
ปัจจุบันการส่งข้อมูลข่าวสารผ่านเครือข่ายส่วนตัว (Private Network) หรือเครือข่ายสาธารณะเช่น อินเตอร์เน็ต มีผู้ใช้งานเป็นจำนวนมาก และให้บริการได้หลายรูปแบบ ทั้งบริการส่งข้อมูลภายใน องค์กรต่างๆ หรือการส่งข้อมูลระหว่างเครือข่ายต่างองค์กร ต่างส่งผลให้เกิดความสะดวก รวดเร็ว ในการส่งข้อมูลข่าวสาร ทำให้การปฏิบัติงานภายในองค์กรดำเนินไปได้อย่างรวดเร็ว ถึงแม้ว่าการส่งข้อมูลผ่านระบบเครือข่ายดังกล่าวจะมีข้อดีอยู่มากมาย แต่ก็มีผู้ประสงค์ร้ายที่แฝงเข้ามาร่วมใช้งานระบบเครือข่าย เพื่อหาประโยชน์ใส่ตนอยู่มากมาย เช่น มีผู้เข้ามาโจมตีระบบทำให้ระบบเครือข่ายใช้งานไม่ได้ หรือมีผู้เข้ามาขโมยข้อมูลระหว่างที่มีการรับส่ง เหตุการณ์เหล่านี้กลายเป็นปัญหาสำคัญของการใช้งานระบบเครือข่ายในปัจจุบัน ที่ส่งผลให้เกิดความเสียหายต่อองค์กร เสียหายต่อระบบเศรษฐกิจและความมั่นคงของประเทศตามมา และเพื่อเป็นการป้องกันปัญหาดังกล่าว วิทยาการรหัสลับจึงถูกนำมาใช้เพื่อรักษาความลับของข้อมูลข่าวสารที่ส่งผ่านระบบเครือข่าย เพื่อไม่ให้บุคคลที่สามหรือบุคคลภายนอกรับรู้ข้อมูลระหว่างการส่ง วิทยาการรหัสลับที่ใช้กันในปัจจุบัน มีหลายแบบ อาทิเช่น วิทยาการรหัสลับแบบสมมาตร (Systematic Cryptography) เป็นวิทยาการที่ใช้กุญแจรหัสลับชุดเดียวกันทั้งการเข้ารหัสและการถอดรหัสลับ ดังนั้นความปลอดภัยของวิทยาการรหัสลับนี้ จะขึ้นอยู่กับความปลอดภัยของกุญแจรหัสลับชุดนั้น ส่วนวิทยาการรหัสลับแบบอสมมาตร (Asymmetric Cryptography)ก็เป็นอีกวิทยาการหนึ่งที่อาศัยความซับซ้อนในการคำนวณ เพื่อป้องกันและรักษาความลับของข้อมูลข่าวสารที่ส่ง แต่ในอนาคต เมื่อเทคโนโลยีการคำนวณมีความก้าวหน้ามากขึ้นอีก เช่น มีการพัฒนาควอนตัมคอมพิวเตอร์ (Quantum Computer) ที่สามารถประมวลผลได้เร็วกว่าคอมพิวเตอร์ที่ใช้อยู่ในปัจจุบัน จนเป็นเหตุให้วิทยาการรหัสลับที่ใช้อยู่ในนั้น ไม่สามารถป้องกัน และรักษาความลับข้อมูลได้อีกต่อไป จึงมีการพัฒนาวิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography)ขึ้น เพื่อใช้ในการส่งกุญแจรหัสลับ (Secret Key)ระหว่างผู้ส่งและผู้รับ ก่อนจะนำกุญแจรหัสลับนั้นมาใช้ร่วมกับวิทยาการรหัสลับแบบสมมาตรในปัจจุบัน ตัวอย่างเช่น วิธีของเวอร์แนม (Vernam Cipher)

การส่งกุญแจรหัสลับในระบบวิทยาการรหัสลับเชิงควอนตัม อาศัยคุณสมบัติเชิงควอนตัมของแสง เพื่อใช้แทนกุญแจรหัสลับ และใช้ทฤษฎีกลศาสตร์ควอนตัม (Quantum Mechanics) ช่วยยืนยันความปลอดภัยของระบบ ฉะนั้น เมื่อใดที่มีบุคคลที่สามบุกรุกเข้ามาขโมยสถานะควอนตัมของแสง จะทำให้ผู้ส่งและผู้รับทราบทันที ถึงการเข้ามารบกวนระบบ ผู้ส่งและผู้รับสามารถยกเลิกการส่งกุญแจรหัสลับได้ทันก่อนจะเกิดความเสียหายตามมา

1.1 ความเป็นมาและความสำคัญของปัญหา

วิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography) หรือ การกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution) นำเสนอครั้งแรกในปี ค.ศ. 1984 เรียกว่าโพรโทคอล BB84 [1] ซึ่งเป็นแนวคิดในการส่งกุญแจรหัสลับโดยอาศัยหลักการโพลาไรเซชัน (Polarization) ของโฟตอนเดี่ยวที่ไม่ตั้งฉากกันสองเวกเตอร์ฐาน (Basis) แทนกุญแจรหัสลับบิต ตามระบบสื่อสารแบบดิจิตอล (บิต "0" และ บิต "1") ในปี ค.ศ. 1992 C.H. Bennett และคณะ ได้แสดงระบบวิทยาการรหัสลับระบบแรกขึ้นโดยใช้โพรโทคอล BB84นี้ ในการส่งกุญแจรหัสลับผ่านอากาศ (Free Space)ได้สำเร็จ โดยสามารถส่งได้เป็นระยะทาง 32 เซนติเมตร ด้วยอัตราเร็วในการส่งกุญแจรหัสลับ 10 บิตต่อวินาที [2] จากนั้นวิทยาการรหัสลับเชิงควอนตัม กลายเป็นที่สนใจของนักวิจัยทั่วโลก โดยมีการวิจัยและพัฒนา เพื่อให้ระบบวิทยาการรหัสลับเชิงควอนตัมสามารถส่งกุญแจรหัสลับได้ระยะทางไกลขึ้น มีอัตราเร็วในการส่งกุญแจรหัสลับสูงขึ้น และสามารถใช้ร่วมกับระบบเครือข่ายสื่อสารดิจิตอลในปัจจุบันได้ มีหน่วยงานที่สำคัญของโลกหลายหน่วยงาน เช่น MIT นิตยสาร PC Magazine และ RAND ได้จัดให้วิทยาการรหัสลับเชิงควอนตัมเป็นหนึ่งในเทคโนโลยีที่น่าจับตามองในอนาคต ตัวอย่างหน่วยงานวิจัยเกี่ยวกับระบบวิทยาการรหัสลับเชิงควอนตัมที่สำคัญของโลก ได้แก่ หน่วยงาน Defense Advanced Research Projects Agency (DARPA) ซึ่ง เป็นหน่วยงานสังกัดกระทรวงกลาโหมของประเทศสหรัฐอเมริกาได้ให้ทุนสนับสนุนงานวิจัยเกี่ยวกับระบบเครือข่ายวิทยาการรหัสลับเชิงควอนตัม เรียกว่า "DARPA Quantum Network" โดยแรกเริ่มเป็นความร่วมมือระหว่างมหาวิทยาลัยบอสตัน (Boston University) มหาวิทยาลัยฮาร์วาด (Harvard University) และ BBN Technology ได้สร้างระบบเครือข่ายวิทยาการรหัสลับเชิงควอนตัมระบบแรกของโลกเมื่อปี ค.ศ. 2003 [3] [4] จากนั้นในปี ค.ศ. 2005 บริษัท QinetiQ ได้เข้าร่วมงานการวิจัยเพื่อสร้างเครือข่ายวิทยาการรหัสลับเชิงควอนตัมด้วย [5] นอกจากนี้สหภาพยุโรปมีโครงการวิจัยเกี่ยวกับวิทยาการรหัสลับเชิงควอนตัมที่ชื่อว่า Development of a Global Network for Secure Communication based on Quantum Cryptography (SECOQC) โดยเป็นความร่วมมือจากสถาบันวิจัยต่างๆภายในสหภาพ ยุโรปซึ่งลงทุนประมาณ 11 ล้านยูโร เพื่อดำเนินการกำหนดมาตรฐานระบบวิทยาการรหัสลับเชิงควอนตัมและบังคับใช้ภายในระยะเวลา 4 ปี [6] เป็นต้น

วิทยาการรหัสลับเชิงควอนตัม หรือ การกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution: QKD) แบ่งการทำงานได้เป็นสองกระบวนการคือการส่งกุญแจรหัสลับทางช่องสื่อสารเชิงควอนตัม (Quantum Channel) เช่น โพรโทคอลBB84[1] โพรโทคอลB92[7] โพรโทคอลEkert91[8] โพรโทคอลGG02 [9] และ กระบวนการกลั่นกุญแจรหัสลับ (Secret Key Distillation) ซึ่งประกอบด้วย



รูปที่ 1.1 การทำงานของระบบวิทยาการรหัสลับเชิงควอนตัม

กระบวนการไกล่เกลี่ยความผิดพลาด (Reconciliation) เป็นการแก้ไขความผิดพลาดจากการส่งกุญแจรหัสลับ เนื่องมาจาก สัญญาณรบกวน (Noise) ความไม่เป็นอุดมคติของอุปกรณ์ และการเข้ามาขโมยสถานะควอนตัมของบุคคลที่สาม ตัวอย่างของโพรโทคอลแก้ไขความผิดพลาด คือ โพรโทคอลCASCADE และ โพรโทคอล Winnow ฯลฯ กระบวนการต่อมา เรียกว่าการขยายสภาวะส่วนตัว (Privacy Amplification) เป็นกระบวนการลดความสามารถในการทำสำเนากุญแจรหัสลับขึ้นมาใหม่ของบุคลที่สาม ซึ่งจะทำการลดขนาดของกุญแจรหัสลับลงโดยอาศัยฟังก์ชันแฮช (Hash Function) รูปแบบการทำงานของการกระจายกุญแจรหัสลับเชิงควอนตัมแสดงดังรูปที่ 1.1

ปัจจุบันวิทยาการรหัสลับนี้ มีการพัฒนาอย่าง กว้างขวาง รวดเร็ว ทั้งกระบวนการกระจายกุญแจรหัสลับ และกระบวนการกลั่นกุญแจรหัสลับ (Secret Key Distillation) โดยการกระจายกุญแจรหัสลับแบ่งออกเป็นสองประเภท[10] คือ การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (Discrete Variable Quantum Key Distribution: DV-QKD) ซึ่งเป็นการกระจายกุญแจรหัสลับเชิงควอนตัมรูปแบบเดิมที่อาศัยหลักการโพลาไรเซชัน หรือ การเปลี่ยนเฟส(Phase) ของการโพลาไรของโฟตอนเดี่ยวหรือคู่โฟตอนพัวพัน (Entangled Photon) แทนค่ากุญแจรหัสลับบิต และการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง(Continuous Variable Quantum Key Distribution: CV-QKD) ซึ่งเป็นระบบวิทยาการรหัสลับเชิงควอนตัมรูปแบบใหม่ที่อาศัยคุณสมบัติของแสงเช่น

Squeezed State หรือ สถานะโคฮีเรนต์ของแสง (Coherent State) มาแทนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ ซึ่งคุณสมบัติทางควอนตัมของแสงเหล่านี้ จะช่วยให้ระบบวิทยาการรหัสลับเชิงควอนตัมสามารถส่งกุญแจรหัสลับได้ด้วยอัตราเร็วมากและสามารถส่งไปด้วยระยะทางที่ไกลกว่าระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง ในส่วนของความปลอดภัยของระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องนี้ ยังคงใช้กฎความไม่แน่นอน (Uncertainty Principle) ของไฮเซนแบร์ก (Heisenberg) ช่วยยืนยันความปลอดภัยเช่นเดียวกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง[11] จึงทำให้มั่นใจได้ว่ากุญแจรหัสลับที่ส่ง จะมีความปลอดภัยเสมอ และสามารถตรวจพบบุคคลที่สามที่ เข้ามาขโมยสถานะควอนตัมของแสงภายในช่องทางการสื่อสารเชิงควอนตัม(Quantum Channel)ได้ทุกครั้ง

การส่งสถานะควอนตัมของแสงแทนกุญแจรหัสลับ เช่นโพลาไรเซชันหรือเฟสของการโพลาไร ผ่านช่องทางการสื่อสารเชิงควอนตัมในตัวกลางที่เป็นอากาศ (Free Space) หรือ เส้นใยแก้วนำแสง (Fiber Optic) นั้น อาจจะมีปัจจัยอื่นๆ เช่น สัญญาณรบกวนภายในช่องสื่อสารเชิงควอนตัม การลดทอนความเข้มของแสง และการบุกรุกเข้ามาขโมยสถานะควอนตัมของแสงของบุคคลที่สาม (โดยทั่วไปเรียกว่า *Eve*) ความไม่เป็นอุดมคติของอุปกรณ์ อันเป็นสาเหตุหลักที่ทำให้สถานะควอนตัมของแสงเกิดการเปลี่ยนแปลง ส่งผลให้กุญแจรหัสลับระหว่างผู้ส่ง (โดยทั่วไปเรียกว่า *Alice*) และผู้รับ (โดยทั่วไปเรียกว่า *Bob*) เกิดความผิดพลาดตามไปด้วย ดังนั้น เมื่อนำกุญแจรหัสลับเหล่านี้ไปใช้รักษาความลับและความปลอดภัยของข้อมูล โดยใช้วิทยาการรหัสลับแบบสมมาตรที่ใช้อยู่ในปัจจุบัน อาจจะทำให้ *Bob* ไม่สามารถถอดรหัสลับข้อมูลที่ *Alice* ส่งมาได้อย่างถูกต้อง เป็นสาเหตุให้การสื่อสารเกิดความผิดพลาดตามมา ดังนั้นกระบวนการไกล่เกลี่ยความผิดพลาด (Reconciliation) หรือกระบวนการทำให้กุญแจรหัสลับของ *Alice* และ *Bob* เหมือนกัน จึงเป็นสิ่งสำคัญในระบบวิทยาการรหัสลับเชิงควอนตัม โพรโทคอลแก้ไขความผิดพลาด ที่นำมาประยุกต์ใช้งานในระบบวิทยาการรหัสลับเชิงควอนตัม ได้แก่ โพรโทคอลCASCADE [12] หรือ โพรโทคอล BBBSS [2] ต่างอาศัยพาริตี้บิต (Parity Bit) เพื่อตรวจสอบความผิดพลาดของกุญแจรหัสลับ ซึ่งพาริตี้บิตสามารถบอกได้เพียงมีความผิดพลาดที่เกิดขึ้นภายในบล็อกกุญแจรหัสลับเท่านั้น ไม่สามารถบอกตำแหน่งความผิดพลาดได้ และเพื่อแก้ไขกุญแจรหัสลับบิตที่ผิด โพรโทคอลเหล่านี้จะแบ่งบล็อกกุญแจรหัสลับที่มีพาริตี้บิตแตกต่างกันออกเป็นครึ่งหนึ่ง จากนั้นหาพาริตี้บิตใหม่แล้วจึงเปรียบเทียบพาริตี้บิตกันอีกครั้ง จนกว่าจะทราบตำแหน่งกุญแจรหัสลับบิตที่ผิด ซึ่งจะทำให้การแก้ไขความผิดพลาดที่เกิดขึ้นนี้มีการติดต่อระหว่าง *Alice*และ *Bob*หลายครั้งมาก ขบวนการการแก้ไขความผิดพลาดจะล่าช้า ไม่เหมาะที่จะนำมาใช้ในระบบกระจายกุญแจรหัสลับความเร็วสูง [13] และทำให้กระบวนการสร้างกุญแจรหัสลับไม่มีประสิทธิภาพเท่าที่ควร

1.2 ความมุ่งหมายและวัตถุประสงค์ของงานวิจัย

รหัสแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correcting Code: FEC) เป็นเทคนิคหนึ่งที่ใช้ในระบบสื่อสารดิจิตอลปัจจุบัน เพื่อลดผลกระทบจากสัญญาณรบกวน (Noise) ที่เป็นสาเหตุหนึ่งที่ทำให้ข้อมูลที่ส่งผ่านระบบสื่อสารเกิดความผิดพลาด การนำรหัสแก้ไขความผิดพลาดล่วงหน้าไปใช้งาน เช่น ใช้ในระบบเครือข่ายโทรศัพท์เคลื่อนที่ ระบบการสื่อสารดาวเทียม ฯลฯ จะช่วยให้ข้อมูลที่ส่งมีความผิดพลาดลดลง ใช้เวลาในการส่งข้อมูลน้อยลง และทำให้การส่งข้อมูลมีประสิทธิภาพเพิ่มขึ้น

วิทยานิพนธ์นี้เสนอการนำรหัสแก้ไขความผิดพลาดล่วงหน้ามาประยุกต์พัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม ให้กระบวนการสร้างกุญแจรหัสลับเหมาะสมกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมความเร็วสูง เช่น ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) เพื่อลดจำนวนรอบการติดต่อระหว่าง *Alice* และ *Bob* รวมทั้งสามารถนำวิธีการแก้ไขความผิดพลาดที่ได้ออกแบบนี้ ไปใช้ได้ทั้งในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (Discrete Variable Quantum Key Distribution: DV-QKD) และระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (Continuous Variable Quantum Key Distribution: CV-QKD) โดยวัตถุประสงค์ของงานวิจัยมีดังต่อไปนี้

- เพื่อศึกษารหัสแก้ไขความผิดพลาดล่วงหน้าที่ใช้ลดความผิดพลาดที่เกิดจากผลของสัญญาณรบกวนภายในช่องทางการสื่อสารของระบบสื่อสาร
- เพื่อศึกษาขั้นตอนการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม เพื่อนำรหัสแก้ไขความผิดพลาดล่วงหน้ามาพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม
- เพื่อออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาด ให้เหมาะสมกับระบบกระจายกุญแจรหัสลับความเร็วสูง ทำให้สามารถสร้างกุญแจรหัสลับได้อย่างรวดเร็ว
- เพื่อพัฒนาโพรโทคอลแก้ไขความผิดพลาดให้สามารถใช้แก้ไขความผิดพลาดได้ทั้งในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องและแบบไม่ต่อเนื่อง

1.3 ขอบเขตงานวิจัย

วิทยานิพนธ์นี้นำเสนอการออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสบีซีเอช (Bose Ray-Chaudhuri และ Hocquenghem: BCH) โดยการนำรหัสบีซีเอช มาประยุกต์ร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง (Side Information) และ การนำรหัสบีซีเอช มาพัฒนาโพรโทคอลฟุรุคาวา (Furukawa) [14] เพื่อพัฒนาโพรโทคอลแก้ไขความผิดพลาดให้เหมาะสมกับระบบกระจายกุญแจรหัสลับความเร็วสูง

สามารถลดจำนวนรอบการติดต่อสื่อสารระหว่าง *Alice* และ *Bob* ในขั้นตอนการแก้ไขความผิดพลาด และพัฒนาโพรโทคอลให้สามารถใช้ร่วมกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง และระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องได้อีกด้วย

1.4 ขั้นตอนการวิจัย

การนำรหัสบีซีเอชมาใช้พัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม มีขั้นตอนการทำงานดังต่อไปนี้

- ศึกษาระบบวิทยาการรหัสลับเชิงควอนตัม การส่งกุญแจรหัสลับและการประยุกต์ระบบวิทยาการรหัสลับเชิงควอนตัม
- ศึกษากระบวนการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม การทำงานของโพรโทคอลแก้ไขความผิดพลาดในระบบวิทยาการรหัสลับเชิงควอนตัม
- ศึกษาขั้นตอนการทำงาน กระบวนการเข้ารหัสและกระบวนการถอดรหัสของรหัสแก้ไขความผิดพลาดล่วงหน้า
- นำรหัสบีซีเอชและรหัสคอนโวลูชันมาประยุกต์ร่วมกับโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมเพื่อพัฒนาโพรโทคอลให้เหมาะสมกับระบบกระจายกุญแจรหัสลับความเร็วสูง
- ออกแบบโปรแกรมและจำลองการทำงานโพรโทคอลแก้ไขความผิดพลาดที่ได้พัฒนาขึ้น

1.5 รายละเอียดวิทยานิพนธ์

วิทยานิพนธ์เล่มนี้แบ่งเนื้อหาออกเป็น 7 บท ซึ่งรายละเอียดของแต่ละบทมีดังต่อไปนี้

บทที่ 1 แสดงความเป็นมาและความสำคัญของปัญหาที่วิจัยวัตถุประสงค์การทำวิจัย ขอบเขตการวิจัย และ ขั้นตอนการวิจัย

บทที่ 2 แสดงพื้นฐานของระบบสื่อสารดิจิตอล และรหัสแก้ไขความผิดพลาดล่วงหน้า

บทที่ 3 แสดงพื้นฐานวิทยาการรหัสลับเชิงควอนตัม โพรโทคอลที่ใช้ในการส่งกุญแจรหัสลับ ระบบวิทยาการรหัสลับเชิงควอนตัม และการทำงานของระบบรวมทั้งอุปกรณ์ที่ใช้ในการส่งและรับกุญแจรหัสลับในระบบวิทยาการรหัสลับเชิงควอนตัม

บทที่ 4 แสดงการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม โพรโทคอลแก้ไขความผิดพลาดในระบบวิทยาการรหัสลับเชิงควอนตัม การทำงานของโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม

บทที่ 5 เสนอการออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสบีซีเอชและรหัสคอนโวลูชัน ที่สามารถนำมาใช้ร่วมกับระบบการ

กระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) และนำไปประยุกต์ใช้ในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD)

บทที่ 6 แสดงผลการออกแบบและผลการทดสอบการพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสบีซีเอชและรหัสคอนโวลูชัน

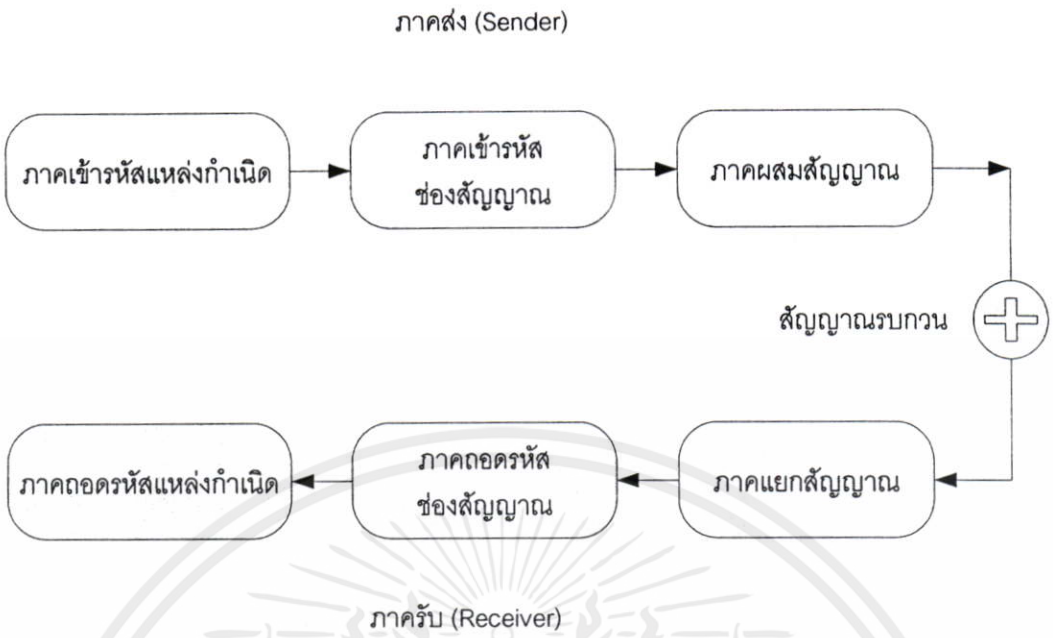
บทที่ 7 เสนอ บทสรุปของงานวิจัย ปัญหาที่เกิดขึ้นจากการวิจัย และข้อเสนอแนะในการพัฒนา

บทที่ 2
ระบบสื่อสารดิจิตอลและรหัสแก้ไขความผิดพลาด

สำหรับการส่งข้อมูลผ่านระบบสื่อสาร ข้อมูลที่ส่งอาจถูกรบกวนโดยสัญญาณรบกวนที่เกิดขึ้นภายในช่องสัญญาณในระบบสื่อสาร ซึ่งสัญญาณรบกวนนี้เป็นสาเหตุสำคัญที่ทำให้ข้อมูลที่ส่งผ่านระบบสื่อสารเกิดความผิดพลาด เพื่อลดผลกระทบของสัญญาณรบกวนที่มีผลต่อความผิดพลาดของข้อมูลที่ส่งผ่านระบบสื่อสาร รหัสแก้ไขความผิดพลาดจึงถูกนำมาใช้เพื่อป้องกันหรือทำให้ความผิดพลาดที่เกิดขึ้นระหว่างการส่งข้อมูลข่าวสารลดน้อยลง โดยในบทนี้จะกล่าวถึงพื้นฐานระบบสื่อสารดิจิตอลและรหัสแก้ไขความผิดพลาดเพื่อใช้เป็นพื้นฐานการพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมต่อไป

2.1 ระบบสื่อสารดิจิตอล

ระบบสื่อสารทั่วไปประกอบด้วยภาคส่ง (Sender) ภาครับ (Receiver) และช่องสัญญาณการสื่อสาร (Channel) ในการส่งข้อมูลข่าวสารผ่านระบบสื่อสารดิจิตอล ภาคส่งจะนำข้อมูลข่าวสารที่สร้างจากแหล่งกำเนิด (Information Source) มาผ่านเข้าสู่ภาคเข้ารหัสแหล่งกำเนิด (Source Encoder) เพื่อทำให้ขนาดของข้อมูลข่าวสารที่ต้องการส่งมีขนาดลดลง หากข้อมูลที่ส่งเป็นสัญญาณแบบอนาล็อก เช่น ระดับสัญญาณแรงดันไฟฟ้าที่ได้จากไมโครโฟน เป็นต้น ภาคเข้ารหัสแหล่งกำเนิดจะทำการเปลี่ยนสัญญาณเหล่านี้ให้อยู่ในรูปแบบสัญญาณดิจิตอล จากนั้นข้อมูลดิจิตอลเหล่านี้จะถูกส่งผ่านเข้าสู่ภาคเข้ารหัสช่องสัญญาณ (Channel Encoder) เพื่อป้องกันความผิดพลาดที่อาจเกิดขึ้นในระหว่างการส่งข้อมูลผ่านระบบสื่อสาร จากนั้นข้อมูลจะถูกผสมสัญญาณ (Modulate) ร่วมกับสัญญาณพาห์ซึ่งจะทำให้สัญญาณที่ส่งเกิดการเปลี่ยนรูปแบบตามสัญญาณข้อมูลข่าวสาร เช่น การผสมสัญญาณทางเฟส (Phase Shift Keying: PSK) การผสมสัญญาณทางความถี่ (Frequency Shift Keying: FSK) เป็นต้น การผสมสัญญาณนี้เป็นสิ่งจำเป็นในระบบสื่อสาร เพื่อทำให้ข้อมูลข่าวสารที่จะส่งมีความเหมาะสมกับช่องสัญญาณนั้น ส่งผลให้ข้อมูลข่าวสารที่ต้องการส่งสามารถส่งได้ระยะทางไกลยิ่งขึ้น และทำให้ความผิดพลาดระหว่างการส่งลดน้อยลงเนื่องมาจากสัญญาณที่ส่งเมื่อผ่านช่องสัญญาณ สัญญาณรบกวนอาจทำให้สัญญาณที่ส่งเกิดความผิดเพี้ยนและทำให้ข้อมูลข่าวสารเกิดความผิดพลาดตามไปด้วย การเลือกรูปแบบการผสมสัญญาณจะช่วยลดระดับความผิดพลาดเหล่านี้และทำให้ข้อมูลข่าวสารที่ส่งเกิดความผิดพลาดลดลง การทำงานขององค์ประกอบที่ภาครับจะสอดคล้องกับทางภาคส่ง โดยสัญญาณที่รับได้ถูกแยกสัญญาณ (Demodulate) เพื่อให้ได้สัญญาณข้อมูลกลับคืนมา ซึ่งข้อมูลที่รับได้นี้อาจมีความผิดพลาดรวมเข้ามาด้วยข้อมูลที่ได้จากการแยกสัญญาณจะถูกถอดรหัสช่องสัญญาณ



รูปที่ 2.1 ไดอะแกรมองค์ประกอบพื้นฐานของระบบสื่อสารดิจิตอล

เพื่อแก้ไขความผิดพลาดที่เกิดขึ้นระหว่างการส่ง โดยภาคถอดรหัสช่องสัญญาณ (Channel Decoder) จากนั้นข้อมูลที่ได้จากภาคถอดรหัสช่องสัญญาณจะถูกเปลี่ยนให้เป็นข้อมูลข่าวสารกลับคืนมา โดยภาคถอดรหัสแหล่งกำเนิด (Source Decoder) ซึ่งไดอะแกรมองค์ประกอบพื้นฐานของระบบสื่อสารดิจิตอลแสดงดังรูปที่ 2.1

2.2 ภาคเข้ารหัสแหล่งกำเนิด

การส่งข้อมูลผ่านระบบสื่อสารเพื่อให้การส่งมีประสิทธิภาพสูงสุด ข้อมูลข่าวสารที่ต้องการส่งจะถูกบีบอัดเพื่อให้ปริมาณข่าวสารที่ส่งมีขนาดเล็กที่สุดที่ภาคเข้ารหัสแหล่งกำเนิด ซึ่งการที่จะศึกษาเรื่องของการเข้ารหัสแหล่งกำเนิดจะต้องศึกษาในส่วนของแหล่งกำเนิดข่าวสาร และปริมาณข่าวสารที่สร้างจากแหล่งกำเนิด ตามทฤษฎีข่าวสารที่เสนอโดย C. Shannon [15] ซึ่งรายละเอียดมีดังต่อไปนี้

2.2.1 ปริมาณข่าวสารและปริมาณข่าวสารเฉลี่ย

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

$$P(X = x_k) = p_k \qquad \text{โดยที่ } k = 1,2,3,..,M$$

p_k คือความน่าจะเป็นที่แหล่งกำเนิดข่าวสารสร้างสัญลักษณ์ x_k

จากกฎความน่าจะเป็น ผลรวมของความน่าจะเป็นของเหตุการณ์ที่เกิดขึ้นทั้งหมดมีค่าเท่ากับหนึ่ง ดังต่อไปนี้ (รายละเอียดดังในภาคผนวก ก.)

$$\sum_{k=1}^{M} p_k = 1$$

โดยปริมาณข่าวสารที่สร้างจากแหล่งกำเนิดข่าวสารจะมีความสัมพันธ์กับ ความน่าจะเป็นในการเกิดข่าวสารนั้น เช่น หากภาคส่งทำการส่งข้อมูลข่าวสารชุดเดิมซ้ำกัน จะทำให้ภาครับได้รับปริมาณข่าวสารน้อยเนื่องจากความน่าจะเป็นในการเกิดข่าวสารนี้มีค่ามาก แต่หากภาครับได้รับข้อมูลข่าวสารชุดที่มีโอกาสในการส่งมาน้อย หรือข้อมูลข่าวสารที่ไม่เคยได้รับมาก่อนจะทำให้ภาครับได้รับปริมาณข่าวสารมาก เนื่องจากความน่าจะเป็นในการเกิดข่าวสารนั้นมีค่าน้อย ซึ่งปริมาณข่าวสารแสดงได้ดังสมการ [16]

$$I(x_k) = \log_2 \frac{1}{p_k} \qquad \text{โดยที่ } p_k = 1,2,3,...,M \tag{2.1}$$

I คือปริมาณข่าวสารที่สร้างจากแหล่งกำเนิดข่าวสาร

หากพิจารณาแหล่งกำเนิดข่าวสารหนึ่งในแต่ละเวลาจะพบว่าปริมาณข่าวสารที่แหล่งกำเนิดนั้นสร้างขึ้น จะมีปริมาณข่าวสารที่ไม่เท่ากัน ส่งผลให้การออกแบบระบบสื่อสารให้มีประสิทธิภาพทำได้ด้วยความยากลำบาก ดังนั้นผู้ออกแบบจึงนิยมใช้ปริมาณข่าวสารเฉลี่ยมาใช้ในการวิเคราะห์และออกแบบระบบสื่อสาร ซึ่งปริมาณข่าวสารเฉลี่ยหรือเอนโทรปี (Entropy) สามารถแสดงได้ดังต่อไปนี้ (รายละเอียดดังภาคผนวก ก)

$$
\begin{aligned}
H(X) &= E[I_k] \\
&= \sum_{k=1}^{M} p_k I(x_k) \\
&= \sum_{k=1}^{M} p_k \log_2\left(\frac{1}{p_k}\right) \\
&= -\sum_{k=1}^{M} p_k \log_2(p_k)
\end{aligned}
\tag{2.2}
$$

$H(X)$ คือปริมาณข่าวสารเฉลี่ยที่สร้างจากแหล่งกำเนิด

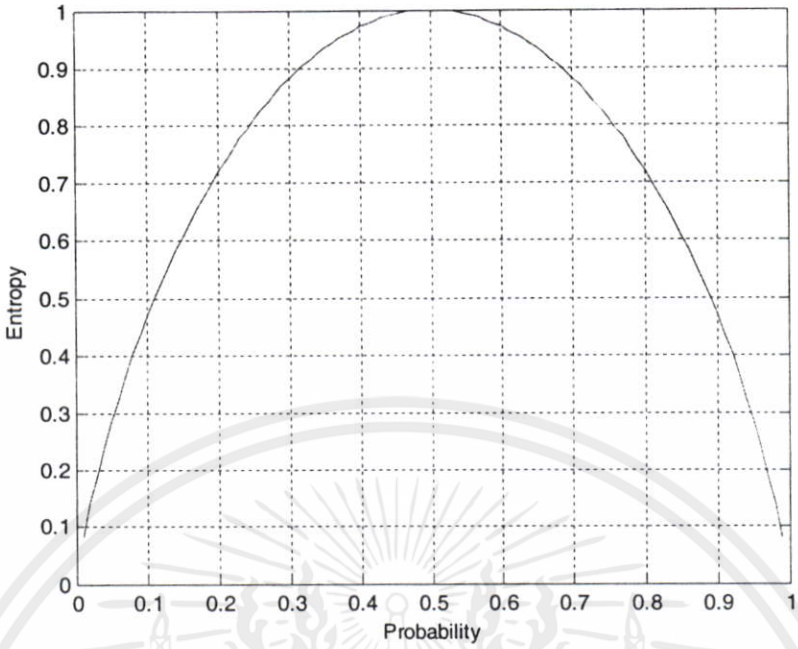
ตัวอย่างการหาปริมาณข่าวสารและปริมาณข่าวสารเฉลี่ยหากแหล่งกำเนิดข่าวสารสร้างข่าวสาร ณ เวลาหนึ่งที่เป็นอักษรภาษาอังกฤษคำว่า "quantum" ปริมาณข่าวสารจากแหล่งกำเนิดข่าวสาร ณ เวลานี้สามารถหาได้ดังต่อไปนี้ $P(X=q)=\frac{1}{26}$ $P(X=u)=\frac{2}{26}$ $P(X=a)=\frac{1}{26}$ $P(X=n)=\frac{1}{26}$ $P(X=t)=\frac{1}{26}$ $P(X=m)=\frac{1}{26}$ ดังนั้นปริมาณข่าวสารสามารถหาได้โดย (รายละเอียดดังภาคผนวก ก)

$$
\begin{aligned}
I &= \log_2\left(\frac{1}{1/26}\right)+\log_2\left(\frac{2}{1/26}\right)+\log_2\left(\frac{1}{1/26}\right)+\log_2\left(\frac{1}{1/26}\right)+\log_2\left(\frac{1}{1/26}\right)+\log_2\left(\frac{1}{1/26}\right) \\
&= 27.2026
\end{aligned}
$$

และปริมาณข่าวสารเฉลี่ยสามารถหาได้ดังต่อไปนี้

$$
\begin{aligned}
H(X) = &-\frac{1}{26}\log_2\left(\frac{1}{26}\right)-\frac{2}{26}\log_2\left(\frac{2}{26}\right)-\frac{1}{26}\log_2\left(\frac{1}{26}\right) \\
&-\frac{1}{26}\log_2\left(\frac{1}{26}\right)-\frac{1}{26}\log_2\left(\frac{1}{26}\right)-\frac{1}{26}\log_2\left(\frac{1}{26}\right)-\frac{1}{26}\log_2\left(\frac{1}{26}\right) \\
= &\ 1.1886
\end{aligned}
$$

ปริมาณข่าวสารเฉลี่ยที่แหล่งกำเนิดสร้างขึ้นมานี้มีค่าเท่ากับ 1.1886 บิตต่อสัญลักษณ์ (bit/symbol)



รูปที่ 2.2 ปริมาณข่าวสารเฉลี่ยของแหล่งกำเนิดข้อมูลข่าวสารสองสัญลักษณ์

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

$$H(X) = -p\log_2(p) - (1-p)\log_2(1-p) \qquad (2.2ก)$$

ซึ่งปริมาณข่าวสารเฉลี่ยของแหล่งกำเนิดนี้แสดงได้ดังรูปที่ 2.2 โดยจากรูปสามารถสรุปได้ว่าปริมาณข่าวสารเฉลี่ยของแหล่งกำเนิดใดๆ จะมีค่ามากที่สุดก็ต่อเมื่อข้อมูลข่าวสารที่สร้างจากแหล่งกำเนิดนั้นมีความน่าจะเป็นในการเกิดเท่ากันทั้งหมดทุกสัญลักษณ์ ดังนั้นค่าปริมาณข่าวสารเฉลี่ยจะมีคุณสมบัติดังต่อไปนี้

$$0 \le H(X) \le \log_2(M) \qquad (2.2ข)$$

M คือจำนวนข่าวสารที่แหล่งกำเนิดนั้นสร้างขึ้น

2.2.2 การเข้ารหัสแหล่งกำเนิด

การเข้ารหัสแหล่งกำเนิดจะเป็นการแทนสัญลักษณ์ของชุดข่าวสารที่สร้างจากแหล่งกำเนิดนั้น ด้วยชุดของคำรหัสที่ประกอบด้วยตัวเลขไบนารี (บิต "0" และ บิต "1") เพื่อใช้ในการรับส่งข่าวสารจริงผ่านระบบสื่อสารดิจิตอล เรียกกระบวนการแทนสัญลักษณ์ข่าวสารด้วยตัวเลขไบนารีนี้ว่าการเข้ารหัสแหล่งกำเนิด (Source Coding) โดยตัวแปรหนึ่งที่สำคัญในการเข้ารหัสแหล่งกำเนิด คือ ความยาวเฉลี่ยของคำรหัสหรือจำนวนบิตเฉลี่ยที่ต้องใช้ในการแทนตัวเลขไบนารีในแต่ละสัญลักษณ์ โดยความยาวเฉลี่ยของคำรหัสนี้สามารถหาได้ดังต่อไปนี้ กำหนดให้แหล่งกำเนิดข่าวสารสร้างข่าวสารทั้งหมดจำนวน M สัญลักษณ์คือ $\{x_1, x_2, ..., x_M\}$ ที่มีความน่าจะเป็นในการเกิดสัญลักษณ์เท่ากับ $\{p_1, p_2, ..., p_M\}$ ความยาวของบิตเฉลี่ยที่ใช้แทนสัญลักษณ์ที่แหล่งกำเนิดนี้สร้างขึ้นแสดงดังสมการ

$$\overline{L} = \sum_{i=1}^{M} p_k I_k \tag{2.3}$$

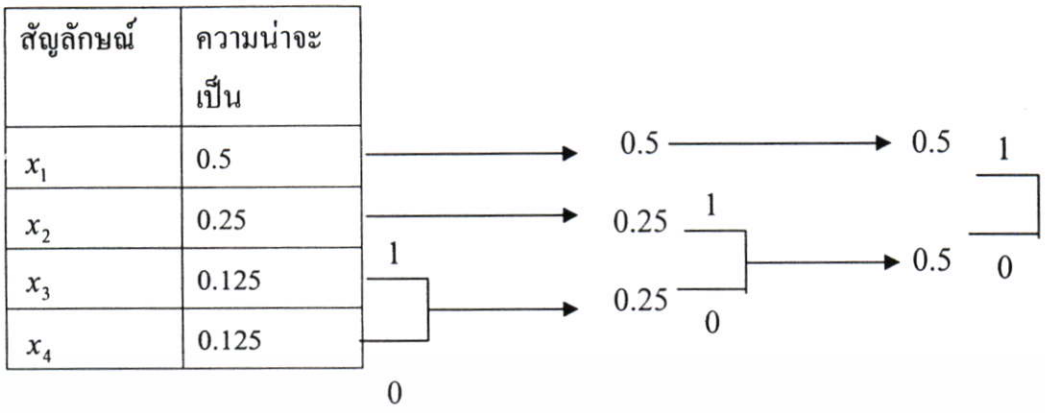
$\overline{L}$ คือ ความยาวของบิตเฉลี่ย

ซึ่งถ้าแหล่งกำเนิดสร้างข่าวสารด้วยปริมาณข่าวสารเฉลี่ยเท่ากับ $H(X)$ ความยาวของบิตเฉลี่ยที่จะใช้ในการแทนสัญลักษณ์ที่สร้างจากแหล่งกำเนิดนี้ จะต้องมีค่ามากกว่าหรือเท่ากับค่าปริมาณข่าวสารเฉลี่ย ตัวอย่างการเข้ารหัสแหล่งกำเนิด เช่น การเข้ารหัสแหล่งกำเนิดด้วยรหัสฮัฟแมน (Huffman Code) [16] ซึ่งการทำงานของรหัสฮัฟแมนมีดังต่อไปนี้

ขั้นตอนที่ 1 เรียงลำดับสัญลักษณ์และความน่าจะเป็นโดยให้สัญลักษณ์ที่มีความน่าจะเป็นในการเกิดมากที่สุดอยู่บน และสัญลักษณ์ที่มีความน่าจะเป็นในการเกิดน้อยที่สุดอยู่ด้านล่าง

ขั้นตอนที่ 2 พิจารณาเฉพาะสัญลักษณ์ที่มีความน่าจะเป็นต่ำที่สุดสองตัวล่างโดยกำหนดบิต "0" ให้กับสัญลักษณ์ที่มีความน่าจะเป็นมากกว่า โดยจะกำหนดบิต "1" ให้กับสัญลักษณ์ที่มีความน่าจะเป็นน้อยกว่า จากนั้นจะทำการสร้างสัญลักษณ์ใหม่จากสัญลักษณ์ทั้งสองโดยความน่าจะเป็นของการเกิดสัญลักษณ์ใหม่นี้มีค่าเท่ากับผลรวมของความน่าจะเป็นของสัญลักษณ์ทั้งสอง

ขั้นตอนที่ 3 เริ่มขั้นตอนที่ 1 และขั้นตอนที่ 2 ใหม่จนกว่าจะเหลือสัญลักษณ์เพียงสองสัญลักษณ์สุดท้าย



รูปที่ 2.3 การทำงานของรหัสฮัฟแมน

ตัวอย่างการเข้ารหัสแหล่งกำเนิดด้วยรหัสฮัฟแมนกำหนดให้แหล่งกำเนิดสร้างสัญลักษณ์สี่สัญลักษณ์ ด้วยความน่าจะเป็นในการเกิดแต่ละสัญลักษณ์มีดังต่อไปนี้ สัญลักษณ์ x_1 มีความน่าจะเป็นเท่ากับ $1/2$ สัญลักษณ์ x_2 มีความน่าจะเป็นเท่ากับ $1/4$ สัญลักษณ์ x_3 มีความน่าจะเป็นเท่ากับ $1/2$ สัญลักษณ์ x_4 มีความน่าจะเป็นเท่ากับ $1/8$ การทำงานของรหัสฮัฟแมนแสดงดังรูปที่ 2.3 ผลที่ได้จากการเข้ารหัสฮัฟแมนมีดังต่อไปนี้ สัญลักษณ์ x_4 จะถูกแทนด้วยตัวเลขไบนารี "000" สัญลักษณ์ x_3 จะถูกแทนด้วยตัวเลขไบนารี "001" สัญลักษณ์ x_2 จะถูกแทนด้วยตัวเลขไบนารี "01" สัญลักษณ์ x_1 จะถูกแทนด้วยตัวเลขไบนารี "1" และจากสมการที่ (2.3) ความยาวเฉลี่ยของคำรหัสที่ได้จากการเข้ารหัสฮัฟแมนแสดงดังต่อไปนี้

$$\begin{aligned}\overline{L} &= \sum_{i=1}^{M} p_k I_k \\ &= 0.5\times 1 + 0.25\times 2 + 0.125\times 3 + 0.125\times 3 \\ &= 1.75 \text{ บิตต่อสัญลักษณ์}\end{aligned}$$

และปริมาณข่าวสารเฉลี่ยแสดงดังต่อไปนี้

$$H(X) = -0.5\times\log_2(0.5) - 0.25\times\log_2(0.25) - 0.125\times\log_2(0.125) - 0.125\times\log_2(0.125)$$

$$= 1.75 \text{ บิตต่อสัญลักษณ์}$$

จากตัวอย่างปริมาณข่าวสารเฉลี่ยและความยาวเฉลี่ยของคำรหัสมีค่าเท่ากันที่ 1.75 บิตต่อสัญลักษณ์

2.3 ช่องสัญญาณและสัญญาณรบกวน

ช่องสัญญาณเป็นสื่อกลางที่ใช้ในการส่งข้อมูลข่าวสารจากภาคส่งไปยังภาครับ โดยสื่อกลางนี้แยกออกเป็นสองประเภทคือ สื่อกลางแบบใช้สายเช่น สายทองแดง และสื่อกลางแบบไร้สาย (Wireless) โดยทั่วไปสัญญาณที่ส่งจากทางภาคส่งไปยังภาครับเมื่อผ่านช่องสัญญาณ สัญญาณที่ส่งอาจจะเกิดความผิดเพี้ยนอันเนื่องมาจากสาเหตุต่างๆ เช่น สัญญาณไปสะท้อนที่ตึกหรืออาคารแล้วเกิดการหักล้างหรือแทรกสอดกับสัญญาณเดิมทำให้ลักษณะหรือรูปร่างของสัญญาณเกิดความเปลี่ยนแปลง ส่งผลให้ภาครับได้รับข้อมูลที่ผิดพลาดตามไปด้วย หรือสัญญาณรบกวนที่เกิดขึ้นภายในช่องสัญญาณเช่น สัญญาณจากแหล่งกำเนิดที่อยู่ข้างเคียง สัญญาณรบกวนที่มาจากดวงอาทิตย์และสัญญาณรบกวนที่เกิดขึ้นภายในอุปกรณ์ภาครับและภาคส่ง ซึ่งสัญญาณรบกวนนี้เป็นสาเหตุทำให้ระดับสัญญาณข้อมูลข่าวสารที่ภาครับได้รับเกิดความแต่ต่างจากระดับสัญญาณเฉลี่ยส่งผลให้ภาครับได้รับข้อมูลข่าวสารที่ผิดพลาด ตัวอย่างสัญญาณรบกวน (Noise) ที่เกิดขึ้นภายในวงจรของภาคส่งและภาครับโดยทั่วไปเช่น ช็อตนอยส์ (Shot Noise) และสัญญาณรบกวนเนื่องจากอุณหภูมิ (Thermal Noise)

2.3.1 ช็อตนอยส์

ช็อตนอยส์ (Shot Noise) เป็นสัญญาณรบกวนที่มักเกิดขึ้นเสมอในวงจรอิเล็กทรอนิกส์ ทั้งอุปกรณ์ภาครับและภาคส่งในระบบสื่อสารหรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆของอุปกรณ์ไฟฟ้า ซึ่งช็อตนอยส์นี้ส่วนใหญ่จะเกิดขึ้นกับอุปกรณ์แอ็กทีฟ (Active Device) ตัวอย่างอุปกรณ์แอ็กทีฟเช่น ไดโอดหรือทรานซิสเตอร์ เป็นต้น สัญญาณรบกวนนี้เกิดเนื่องมาจากการที่อิเล็กตรอน (Electron) หรือ โฟตอน (Photon) ภายในอุปกรณ์แอ็กทีฟเคลื่อนที่ทำให้เกิดการไหลของกระแสไฟฟ้าหรือแรงดันไฟฟ้าซึ่งการเคลื่อนที่ของอิเล็กตรอนหรือโฟตอนนี้โดยปกติจะมีจำนวนที่ไม่แน่นอน ณ ช่วงเวลาใดเวลาหนึ่ง ทำให้กระแสไฟฟ้าหรือแรงดันไฟฟ้า (Voltage) ในช่วงเวลานั้นเกิดขึ้นในลักษณะแบบสุ่มตามไปด้วย เช่น ตัวตรวจจับแสง (Photodiode) กระแสไฟฟ้าที่ไหลภายในวงจรของตัวตรวจจับแสงนี้จะเกิดขึ้นตลอดเวลาเนื่องมาจากอิเล็กตรอนที่ถูกปล่อยออกมาจากขั้วแคโทดนั้นจะไหลไปยังขั้วแอโนด เนื่องมาจากแสงหรือโฟตอนที่เข้ามาตกกระทบตัวตรวจจับแสง ซึ่งจำนวนของอิเล็กตอนที่ถูกปล่อยหรือหลุดออกมาจะมีลักษณะแบบสุ่ม ส่งผลให้เกิดการไหลของกระแสแบบสุ่มด้วยเช่นกัน ดังนั้นเมื่อกระแสไฟฟ้าหรือแรงดันไฟฟ้านี้เข้าไปรวมกับกระแสไฟฟ้าหรือแรงดันไฟฟ้าที่ใช้แทนข้อมูลข่าวสารในระบบสื่อสารหรืออุปกรณ์อิเล็กทรอนิกส์ ซึ่งจะทำให้สัญญาณภายในระบบเกิดการเปลี่ยนแปลง ส่งผลทำให้การทำงานของอุปกรณ์อิเล็กทรอนิกส์เกิดความผิดพลาด โดยจำนวนโฟตอนหรืออิเล็กตรอนที่เกิดขึ้นภายในอุปกรณ์อิเล็กทรอนิกส์จะมีรูปแบบการกระจายโอกาสแบบปัวส์ซอง [17] ดังสมการ (รายละเอียดแสดงในภาคผนวก ก.)

$$P(v=k)=\frac{(\lambda)^k}{k!}e^{-\lambda} \tag{2.4}$$

λ คือค่าเฉลี่ยในการพบโฟตอนหรืออิเล็กตอน

k คือ จำนวนอิเล็กตอน หรือ โฟตอน ซึ่ง $k=1,2,3....$

2.3.2 สัญญาณรบกวนเนื่องจากอุณหภูมิ

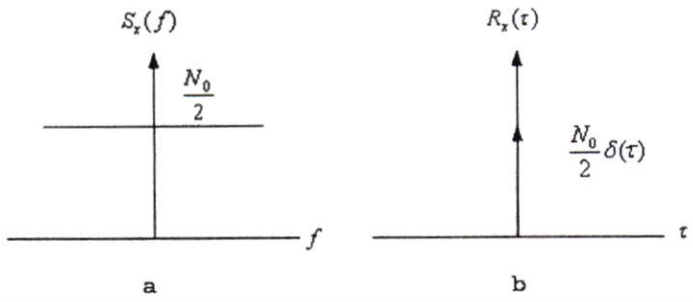
สัญญาณรบกวนเนื่องจากอุณหภูมิ (Thermal Noise) หรือสัญญาณรบกวนไนควิส (Nyquis Noise) เป็นสัญญาณรบกวนที่พบมากในวงจรอิเล็กทรอนิกส์โดยเฉพาะอุปกรณ์อิเล็กทรอนิกส์ประเภทพาสซีส (Passive Devise) เช่น ตัวต้านทาน (Resistor) สัญญาณรบกวนที่เกิดจากอุณหภูมินี้เกิดจากการเคลื่อนที่ของอิเล็กตรอนภายในตัวต้านทาน เนื่องมาจากผลของการเปลี่ยนแปลงอุณหภูมิภายในตัวต้านทาน หากอุณหภูมิภายในตัวต้านทานสูงขึ้น จะส่งผลให้อิเล็กตรอนภายในตัวต้านทานมีพลังงานสูงขึ้นตามไปด้วย อิเล็กตรอนบางตัวจะมีพลังงานมากกว่าระดับพลังงานในสถานะพื้น ซึ่งจะทำให้เกิดกระแสไหลผ่านตัวต้านทานส่งผลให้แรงดันไฟฟ้าที่ตัวต้านทางเกิดการเปลี่ยนแปลงตามไปด้วย ถ้าหากการเคลื่อนที่ของอิเล็กตรอนในตัวต้านทานมีปริมาณมากและอิเล็กตรอนแต่ละตัวเคลื่อนที่ได้อย่างอิสระจากทฤษฎีเซ็นทรัลลิมิต (Central Limit Theorem) สามารถพิสูจน์ว่า สัญญาณรบกวนที่เกิดจากอุณหภูมิจะมีการกระจายแบบเกาส์ด้วยค่าเฉลี่ยเท่ากับศูนย์ [17] ดังสมการ

$$f(x)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{-(x-m_x)^2/2\varsigma^2} \tag{2.5}$$

m_x คือค่าเฉลี่ย และ σ^2 คือค่าความแปรปรวนของการกระจายแบบเกาส์

ในการวิเคราะห์สัญญาณรบกวนที่เกิดขึ้นในการจำลองการทำงานของระบบสื่อสารส่วนใหญ่จะใช้สัญญาณรบกวนขาว (White Noise) ซึ่งสัญญาณรบกวนขาวนี้เป็นสัญญาณรบกวนที่เกิดขึ้นแบบอุดมคติ โดยมีคุณสมบัติความหนาแน่นของแถบกำลังงานจะคงที่ทุกช่วงความถี่ดังแสดงดังรูปที่ 2.4 และดังสมการต่อไปนี้

$$S_x(f)=\frac{N_0}{2} \qquad ;f=[-\infty,\infty] \tag{2.6}$$



รูปที่ 2.4 คุณสมบัติของสัญญาณรบกวนแบบขาว
a) ความหนาแน่นของแถบกำลังงาน และ b) ออโตคอร์รีเลชัน ฟังก์ชัน

ค่าออโตคอร์รีเลชันฟังก์ชันของสัญญาณรบกวนขาวแสดงดังสมการต่อไปนี้

$$R_x(\tau) = \delta(\tau)N_0/2 \tag{2.7}$$

จากค่าออโตคอร์รีเลชันของสัญญาณรบกวนขาว (White Noise) จะมีค่าเท่ากับศูนย์เมื่อ τ ไม่เท่ากับศูนย์ และจะมีค่าเท่ากับ $N_0/2$ เมื่อ τ มีค่าเท่ากับศูนย์ ซึ่งแสดงถึงลักษณะของสัญญาณรบกวนแบบขาวที่เกิดขึ้นในแต่ละเวลาที่ต่างกันจะไม่มีความสัมพันธ์ระหว่างกันเลย [17]

ในการจำลองการทำงานของระบบสื่อสาร (Communication System) รูปแบบช่องสัญญาณที่ใช้ในการจำลองการทำงานระบบสื่อสารส่วนใหญ่จะนิยมใช้ช่องสัญญาณขาวแบบบวก Additive White Gaussian Noise (AWGN) ซึ่งคำว่า

"Additive"หมายถึงสัญญาณที่ภาครับได้รับเกิดจากสัญญาณที่ภาคส่งรวมกับสัญญาณรบกวนภายในช่องสัญญาณ

"White"หมายถึงสัญญาณรบกวนนี้เป็นสัญญาณรบกวนแบบขาวที่มีค่าความหนาแน่นของแถบกำลังงาน (Power Spectrum Density) คงที่

"Gaussian"หมายถึงสัญญาณรบกวนนี้มีโอกาสเกิดขึ้นอยู่กับการกระจายโอกาสแบบเกาส์

2.4 การเข้ารหัสช่องสัญญาณ

ในระหว่างการส่งข้อมูลข่าวสารผ่านระบบสื่อสาร สัญญาณที่ส่งผ่านช่องทางการสื่อสารอาจจะถูกรบกวนจากสัญญาณที่เกิดขึ้นภายในช่องสัญญาณ ทำให้เมื่อสัญญาณเหล่านี้ เมื่อเดินทางไปถึงยังภาครับ สัญญาณที่ภาครับได้รับจะเกิดความผิดเพี้ยน ส่งผลให้ข้อมูลข่าวสารที่ส่งเกิดความผิดพลาดตามไปด้วย เพื่อลดผลกระทบจากสัญญาณรบกวนภายในระบบสื่อสารหลักการของการเข้ารหัสช่องสัญญาณ จะถูกนำมาใช้เพื่อแก้ไขความผิดพลาดที่เกิดขึ้น โดยจะทำการเพิ่มข้อมูลหรือ

เรียกว่ารีดันแดนซี จากข้อมูลที่ต้องการส่งเพื่อใช้ในการตรวจสอบและแก้ไขความผิดพลาดหากตรวจพบความผิดพลาดเกิดขึ้น ซึ่งรายละเอียดของการเข้ารหัสช่องสัญญาณมีดังต่อไปนี้

2.4.1 การแก้ไขความผิดพลาดของข้อมูลในระบบสื่อสารดิจิตอล

วิธีที่ใช้ในการป้องกันหรือแก้ไขความผิดพลาดจากการส่งข้อมูลในระบบสื่อสารดิจิตอลในส่วนของการเข้ารหัสช่องสัญญาณนั้นแบ่งได้เป็นสองประเภทคือ วิธีการส่งซ้ำอัตโนมัติ (Automatic Retransmission Query หรือ Automatic Repeat Request: ARQ) และรหัสแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correcting Code: FEC) [16] วิธีการทำงานของวิธีการส่งซ้ำอัตโนมัติเมื่อภาครับตรวจสอบได้ว่าข้อมูลที่รับได้เกิดความผิดพลาด ภาครับจะทำการร้องขอให้มีการส่งข้อมูลนั้นใหม่อีกครั้ง จะเห็นได้ว่าวิธีการส่งซ้ำอัตโนมัติหากระบบสื่อสารมีความผิดพลาดระหว่างการส่งสูงจะทำให้ระบบสื่อสารมีประสิทธิภาพต่ำ การส่งข้อมูลจะทำได้อย่างล่าช้าแต่วิธีการส่งซ้ำอัตโนมัติจะให้การส่งข้อมูลข่าวสารมีความถูกต้องสูง ในส่วนของรหัสแก้ไขความผิดพลาดล่วงหน้า เมื่อภาครับตรวจพบว่าข้อมูลที่รับได้เกิดความผิดพลาด ภาครับจะแก้ไขความผิดพลาดให้ข้อมูลกลับมาถูกต้องโดยไม่จำเป็นต้องทำการส่งข้อมูลนั้นใหม่อีกครั้ง โดยความสามารถในการแก้ไขความผิดพลาดของรหัสแก้ไขความผิดพลาดล่วงหน้า จะขึ้นอยู่กับชนิดของรหัสแก้ไขความผิดพลาดนั้น ซึ่งเมื่อเปรียบเทียบการทำงานของวิธีการส่งซ้ำอัตโนมัติและรหัสแก้ไขความผิดพลาดล่วงหน้า วิธีการส่งซ้ำอัตโนมัติจะมีการทำงานที่ง่ายและใช้รีดันแดนซีบิตน้อยกว่ารหัสแก้ไขความผิดพลาดล่วงหน้า แต่อัตราเร็วในการส่งข้อมูลจะไม่แน่นอนเนื่องจากต้องส่งข้อมูลใหม่อีกครั้งเมื่อภาครับตรวจพบความผิดพลาดของข้อมูล ส่วนรหัสแก้ไขความผิดพลาดล่วงหน้านั้นมีความซับซ้อนมากกว่าแต่วิธีการนี้จะให้การรับส่งข้อมูลทำได้อย่างรวดเร็ว ดังนั้นในส่วนของการใช้งานจึงขึ้นอยู่กับการประยุกต์ใช้งาน (Application) เช่น เมื่อต้องการความถูกต้องของข้อมูลสูงและไม่จำกัดด้านเวลาที่ต้องการส่งเช่น ข้อมูลเกี่ยวกับรูปภาพทางการแพทย์ การส่งข้อมูลนี้จึงนิยมใช้การแก้ไขความผิดพลาดด้วยวิธีการส่งซ้ำอัตโนมัติ ในส่วนการส่งข้อมูลที่ต้องการความรวดเร็วในการส่งเช่น เสียง การส่งข้อมูลแบบเวลาจริง (Real Time) เป็นต้น การส่งข้อมูลแบบนี้จึงนิยมใช้รหัสแก้ไขความผิดพลาดล่วงหน้า

2.4.2 รหัสแก้ไขความผิดพลาดล่วงหน้า

รหัสแก้ไขความผิดพลาดล่วงหน้าเป็นหนึ่งในเทคนิคที่ใช้ลดผลความผิดพลาดจากการส่งข้อมูล อันเนื่องมาจากสัญญาณรบกวนที่เป็นสาเหตุทำให้ข้อมูลข่าวสารที่ส่งผ่านระบบสื่อสารเกิดความผิดพลาด ซึ่งการทำงานของรหัสแก้ไขความผิดพลาดล่วงหน้า เริ่มจากนำข้อมูลที่ต้องการส่งมาผ่านเข้าสู่วงจรเข้ารหัส (Encoder) ซึ่งจะทำให้ได้ข้อมูลใหม่เรียกว่าคำรหัส (Codeword) โดยคำรหัสนี้ประกอบด้วยส่วนข้อมูลที่เพิ่มขึ้นมาเรียกว่ารีดันแดนซีบิต (Redundancy Bit) และข้อมูลเดิมที่

ผ่านเข้าสู่วงจรเข้ารหัสเช่น นำข้อมูลขนาด k บิต มาผ่านเข้าสู่วงจรเข้ารหัสจะได้คำรหัสขนาด n บิต ซึ่งคำรหัสนี้ประกอบด้วยข้อมูลข่าวสารเดิมขนาด k บิต และส่วนของข้อมูลที่เพิ่มขึ้นขนาด $r = n - k$ บิต หากพิจารณาคำรหัสที่ได้จากวงจรเข้ารหัสทำให้สามารถแบ่งรหัสแก้ไขความผิดพลาดล่วงหน้าออกเป็นสองประเภทคือ

- **รหัสแก้ไขความผิดพลาดล่วงหน้าแบบสมมาตร (Systematic Code)**

รหัสแก้ไขความผิดพลาดล่วงหน้าแบบสมมาตรเป็นรูปแบบของรหัสแก้ไขความผิดพลาดล่วงหน้าซึ่งคำรหัสที่ได้จากวงจรเข้ารหัสจะแยกส่วนระหว่างข้อมูลที่เข้ารหัสและส่วนของรีดันแดนซีอย่างชัดเจนหรือคำรหัสที่ได้จากวงจรเข้ารหัสประกอบด้วยข้อมูลอินพุตที่เข้าสู่วงจรเข้ารหัสและข้อมูลในส่วนของรีดันแดนซีบิต

- **รหัสแก้ไขความผิดพลาดล่วงหน้าแบบอสมมาตร (Nonsystematic Code)**

รหัสแก้ไขความผิดพลาดล่วงหน้าแบบอสมมาตรเป็นอีกหนึ่งรูปแบบของรหัสแก้ไขความผิดพลาดล่วงหน้าซึ่งวงจรเข้ารหัสจะสร้างคำรหัสใหม่ที่ไม่มีส่วนใดในคำรหัสมีข้อมูลหรือมีรูปแบบข้อมูลเดิมที่ใช้ในการเข้ารหัสนั้นอยู่

2.5 ตัวอย่างรหัสแก้ไขความผิดพลาดล่วงหน้า

รหัสแก้ไขความผิดพลาดล่วงหน้าที่ใช้อยู่ในปัจจุบันแบ่งออกเป็นสองชนิดได้แก่ รหัสแบบบล็อก (Block Code) เช่น รหัสแฮมมิง (Hamming Code) รหัสวน (Cyclic Code) รหัสบีซีเอช รหัส RS เป็นต้น และแบบคอนโวลูชัน (Convolutional Code) เช่น รหัสคอนโวลูชัน (Convolution Code) รหัสเทอร์โบ (Turbo Code) เป็นต้น ซึ่งตัวอย่างของรหัสแบบบล็อกและรหัสแบบคอนโวลูชันมีดังต่อไปนี้

2.5.1 รหัสแบบบล็อกเชิงเส้น

รหัสแบบบล็อกเชิงเส้น (Linear Block Code) เป็นหนึ่งในเทคนิคที่ใช้แก้ไขความผิดพลาดที่เกิดขึ้นระหว่างการส่งข้อมูลผ่านระบบสื่อสารดิจิตอล ซึ่งรหัสประเภทนี้ถูกเรียกว่ารหัสแบบบล็อกเนื่องมาจาก ข้อมูลที่นำมาเข้ารหัสจะถูกแบ่งออกเป็นชุดหรือบล็อกย่อยๆ ซึ่งความสามารถในการตรวจหาและแก้ไขความผิดพลาดของรหัสแบบบล็อกขึ้นอยู่กับระยะแฮมมิงน้อยที่สุด (Minimum Hamming Distance) ของคำรหัสที่สร้างได้จากรหัสบล็อกเชิงเส้นแต่ละชนิด หากระยะแฮมมิงน้อยที่สุดมีค่ามากจะทำให้รหัสแบบบล็อกนี้มีความสามารถในการตรวจหาและแก้ไขความผิดพลาดสูง ตัวอย่างรหัสแบบบล็อกเชิงเส้นเช่น รหัสแบบแฮมมิง รหัสวน รหัสบีซีเอช และรหัส RS เป็นต้น

2.5.1.1 ความสามารถในการตรวจจับและแก้ไขความผิดพลาด

ความสามารถที่จะตรวจหาและแก้ไขความผิดพลาดของรหัสแก้ไขความผิดพลาดล่วงหน้าเป็นสิ่งบ่งชี้ถึงประสิทธิภาพของรหัสนั้น โดยการวิเคราะห์คุณสมบัติของรหัสแก้ไขความผิดพลาดล่วงหน้าแต่ละชนิดต้องมีการพิจารณาถึงองค์ประกอบหลายส่วน เช่น น้ำหนักแฮมมิง (Hamming Weight) และระยะแฮมมิง (Hamming Distance) สำหรับค่าน้ำหนักแฮมมิ่งหรือ $w(U)$ นั้นหมายถึงจำนวนบิตของข้อมูลที่ไม่เท่ากับ "0" ภายในบล็อกคำรหัสนั้นหรือจำนวนบิต "1" ที่เกิดขึ้นทั้งหมดภายในบล็อกคำรหัสนั้น สำหรับค่าระยะแฮมมิงหมายถึงจำนวนความแตกต่างระหว่างบิตในคำรหัสตำแหน่งเดียวกันระหว่างคำรหัสสองคำรหัส เช่น คำรหัส U และ V จะมีความแตกต่างของคำรหัสคือ $d(U,V)$ ซึ่งระยะแฮมมิงของคำรหัสทั้งสองสามารถหาได้ดังต่อไปนี้ [18]

$$d(U,V) = \sum_{i=1}^{n} U_i \oplus V_i \tag{2.8}$$

คำรหัสที่สร้างจากรหัสแก้ไขความผิดพลาดล่วงหน้านั้นอาจจะมีค่าระยะแฮมมิงเท่ากันหรือแตกต่างกันขึ้นอยู่กับการนำคำรหัสใดมาเปรียบเทียบ แต่ในการวิเคราะห์การทำงานเพื่อหาประสิทธิภาพของรหัสแบบบล็อกจะพิจารณาเพียงค่าระยะแฮมมิงน้อยที่สุด (Minimum Hamming Distance) หรือ $d_{\min}$ โดย $d_{\min}$ นี้จะถูกนำไปใช้ในการคำนวณความสามารถในการแก้ไขความผิดพลาดของรหัสนั้น ซึ่งจำนวนบิตที่มากที่สุดที่เกิดความผิดพลาดแล้วรหัสแบบบล็อกยังสามารถแก้ไขให้ถูกต้องได้ (t) ดังสมการ

$$t = \left[\frac{d_{\min} - 1}{2} \right] \tag{2.9}$$

ส่วนจำนวนบิตผิดมากที่สุดที่รหัสแก้ไขความผิดพลาดล่วงหน้านั้นสามารถตรวจพบ ได้ว่าเกิดความผิดพลาดขึ้น (Error Detecting Capability) แสดงดังสมการ

$$E = d_{\min} - 1 \tag{2.10}$$

E คือ ความสามารถในการตรวจพบความผิดพลาดของรหัสแก้ไขความผิดพลาดล่วงหน้า

2.5.1.2 การเข้ารหัสแบบบล็อกเชิงเส้น

การเข้ารหัสแบบบล็อกเชิงเส้นมีขั้นตอนการทำงานคือ นำข้อมูลที่ต้องการเข้ารหัสมาแบ่งเป็นชุดหรือแบ่งเป็นบล็อก ซึ่งแต่ละบล็อกนั้นมีขนาดเท่ากับ k บิต ในการเข้ารหัสแบบบล็อก

เชิงเส้นข้อมูลที่ต้องการเข้ารหัสจะถูกคูณเข้ากับเมตริกกำเนิด (Generator Metric) เพื่อสร้างคำรหัส ดังสมการ

$$U = mG \tag{2.11}$$

U คือคำรหัสจากการเข้ารหัสแบบบล็อกเชิงเส้น m คือข้อมูลที่นำมาเข้ารหัสขนาด k บิต

G คือเมตริกซ์กำเนิด (Generator Metric)

2.5.1.3การถอดรหัสแบบบล็อกเชิงเส้น

การตรวจหาความผิดพลาดที่เกิดขึ้นจากการส่งข้อมูลของรหัสแบบบล็อกที่ภาครับนั้น มีวิธีการตรวจหาความผิดพลาดโดยนำคำรหัสที่รับได้มาคูณกับเมทริกตรวจสอบพาริตี้ (Parity Check Metric: H) ซึ่งผลลัพธ์ที่ได้จากการคูณจะเรียกว่าค่าซินโดรม (Syndrome: S) ซึ่งเป็นค่าแสดงถึงลักษณะความผิดพลาดของข้อมูลที่เกิดขึ้นกับข้อมูลบล็อกนั้น [18] โดยหากค่าซินโดรมมีค่าเท่ากับศูนย์ ทางภาครับจะทราบทันทีว่าข้อมูลที่ส่งมามีความถูกต้องแต่หากค่าซินโดรมมีค่าไม่เท่ากับศูนย์ ทางภาครับจะทราบตำแหน่งของบิตผิดภายในบล็อกนั้นจากค่าซินโดรมหรือความผิดพลาดที่เกิดขึ้นกับข้อมูลภายในบล็อก (ขึ้นอยู่กับความสามารถในการแก้ไขความผิดพลาดของรหัสแต่ละชนิด) ซึ่งค่าซินโดรมสามารถหาได้โดย กำหนดให้คำรหัสที่ได้จากวงจรเข้ารหัสคือ U เมื่อคำรหัสนี้ถูกส่งผ่านช่องทางการสื่อสารมายังภาครับ ภาครับจะได้รับคำรหัสใหม่ (V) ที่อาจจะเกิดความผิดพลาดอันเนื่องจากสัญญาณรบกวนโดยที่ $V = U + e$ โดยที่ e คือความผิดพลาดระหว่างการส่งข้อมูลผ่านระบบสื่อสาร ดังนั้นซินโดรมที่ภาครับแสดงดังสมการ

$$S = (U + e)H^T \tag{2.12}$$

S คือซินโดรม และ H คือเมทริกซ์ตรวจสอบพาริตี้

ซึ่งเมทริกซ์ตรวจสอบพาริตี้จะมีความสัมพันธ์กับเมทริกซ์กำเนิด (G) โดยจะทำให้ UH^T มีค่าเป็นศูนย์ ดังนั้นค่าซินโดรมที่ได้นั้นมีค่าเท่ากับ

$$S = eH^T \tag{2.13}$$

2.5.2 รหัสแฮมมิง

รหัสแฮมมิง (Hamming Code) เป็นหนึ่งในรหัสแบบบล็อกเชิงเส้นที่เสนอโดย R. Hamming ในปี ค.ศ. 1950 ซึ่งรหัสแฮมมิงสามารถแก้ไขความผิดพลาดได้หนึ่งบิตต่อบล็อก ซึ่ง

ข้อมูลที่จะนำมาเข้ารหัสจะถูกแบ่งออกเป็นบล็อกขนาด k บิต $m_1, m_2, ..., m_k$ และเมื่อข้อมูลนี้ผ่านเข้าสู่วงจรเข้ารหัสแฮมมิงจะได้คำรหัสประกอบด้วยข้อมูลเดิมขนาด k บิตและส่วนของพาริตี้บิตหรือรีดันแดนซีบิต (Redundancy Bit) ขนาด $n-k$ บิต $p_1, p_2, ..., p_{n-k}$ เมื่อนำข้อมูลและรีดันแดนซีมารวมเป็นคำรหัส (Codeword) จะได้คำรหัสขนาด n บิต $c_1, c_2, ..., c_n$ จากที่กล่าวมานี้เป็นคุณสมบัติพื้นฐานของรหัสแบบบล็อกโดยทั่วไป ซึ่งหลักการทำงานของรหัสแฮมมิงมีดังต่อไปนี้

2.5.2.1 การเข้ารหัสแฮมมิง

จากที่ได้กล่าวถึงส่วนประกอบของรหัสแฮมมิงที่ประกอบด้วย ส่วนของข้อมูลขนาด k บิต และส่วนของพาริตี้บิตขนาด $n-k$ บิตซึ่งการหาค่าพาริตี้บิตเป็นสิ่งที่มีความสำคัญสำหรับสร้างคำรหัสของรหัสแฮมมิงเพื่อใช้บ่งบอกความผิดพลาดและแก้ไขความผิดพลาดที่เกิดขึ้นภายในบล็อกข้อมูล ขั้นตอนการเข้ารหัสแฮมมิงเริ่มจากการเรียงลำดับคำรหัสจากลำดับที่ $1,2,3,...,n$ ซึ่งตำแหน่งของบิตตรวจสอบจะถูกวางไว้ในตำแหน่ง $2^0, 2^1, 2^2, ...$ โดยค่าไบนารีในแต่ละตำแหน่งของบิตตรวจสอบสามารถหาได้จากผลรวมของข้อมูลที่อยู่ในตำแหน่งของบิตตรวจสอบนั้นมีอยู่เช่นข้อมูลตำแหน่งที่ "6" ในบล็อกคำรหัสเกิดจากตำแหน่งของบิตตรวจสอบ "$2 = 2^1$" รวมกับตำแหน่งที่ "$4 = 2^2$" เป็นต้น ตัวอย่างตำแหน่งของบิตข้อมูลและบิตตรวจสอบของรหัสแฮมมิง (7,4) แสดงดังตารางที่ 2.1 และตารางที่ 2.2 แสดงการเข้ารหัสแฮมมิงโดยข้อมูลที่นำมาเข้ารหัส คือ "1010"

2.5.2.2การถอดรหัสแฮมมิง

การถอดรหัสแฮมมิงเป็นการอาศัยบิตตรวจสอบที่ถูกสร้างขึ้นจากผลรวมของบิตข้อมูลในตำแหน่งต่างๆ เพื่อบ่งบอกตำแหน่งของบิตที่ผิดภายในบล็อกโดยสามารถบอกตำแหน่งบิตผิดและแก้ไขความผิดพลาดให้ถูกต้องได้หนึ่งตำแหน่ง จากตารางที่ 2.2 เมื่อนำข้อมูล "1010" มาผ่านเข้าสู่วงจรเข้ารหัสแฮมมิงคำรหัสที่ได้คือ "1010010" เมื่อส่งคำรหัสนี้ผ่านช่องสัญญาณที่มีสัญญาณรบกวนอยู่อาจทำให้เกิดความผิดพลาดขึ้นภายในบล็อกคำรหัสนี้ เช่นภาครับได้รับข้อมูลได้เป็น "1<u>1</u>10010" ภาครับจะตรวจหาความผิดพลาดและแก้ไขความผิดพลาดโดยการหาค่าซินโดรมที่แสดงดังตาราง 2.3 ซึ่งค่าซินโดรมที่หาค่าได้คือ "110" จะแสดงตำแหน่งของบิตผิดที่เกิดขึ้นภายในบล็อกรหัส ทำให้ภาครับสามารถแก้ไขความผิดพลาดที่เกิดขึ้นในตำแหน่งนั้นให้ได้ข้อมูลที่ถูกต้อง นอกจากนี้การเข้ารหัสแฮมมิงและถอดรหัสแฮมมิงยังสามารถแสดงให้อยู่ในรูปเมทริกซ์ (Metric)ซึ่งจากตัวอย่างที่ผ่านมาจะเห็นว่าค่าพาริตี้บิตที่ใช้ในการตรวจสอบความผิดพลาดเกิดจากผลรวมของข้อมูลในตำแหน่งต่างๆ ซึ่งแสดงได้ดังต่อไปนี้

$$p_i = b_{i,2}m_2 + b_{i,2}m_2 + ... + b_{i,k}m_k \quad \text{โดยที่ } i = 1,2,3,...,n-k \tag{2.14}$$

โดยสัมประสิทธิ์ $b_{i,j}$ เป็นสัมประสิทธิ์ที่ประกอบด้วยบิต "0" หรือบิต "1" ซึ่งขึ้นอยู่กับความต้องการให้ข้อมูลในตำแหน่งนั้นมีความสัมพันธ์หรือไม่

ตารางที่ 2.1 การเข้ารหัสแฮมมิง [16]

7	6	5	4	3	2	1	ตำแหน่งบิตของคำรหัส
D4	D3	D2	P3	D1	P2	P1	คำรหัสขนาด 7 บิต
D4	-	D2	-	D1	-	P1	บิตตรวจสอบ
D4	D3	-	-	D1	P2	-	บิตตรวจสอบ
D4	D3	D2	P3	-	-	-	บิตตรวจสอบ

D คือบิตข้อมูล และ *P* คือบิตตรวจสอบ

ตารางที่ 2.2 การเข้ารหัสแฮมมิงด้วยบิตข้อมูลขนาด 4 บิต ("1010")

7	6	5	4	3	2	1	ตำแหน่งของคำรหัส
D4	D3	D2	P3	D1	P2	P1	คำรหัสขนาด 7 บิต
1	0	1	0	0	1	0	คำรหัส
1	-	1	-	0	-	0	บิตตรวจสอบ (P1) = 0
1	0	-	-	O	1	-	บิตตรวจสอบ (P2) = 1
1	0	1	0	-	-	-	บิตตรวจสอบ (P3) = 0

ตารางที่ 2.3 การตรวจสอบความผิดพลาดเมื่อเกิดการผิดของบิต

7	6	5	4	3	2	1	
D4	D3	D2	P3	D1	P2	P1	คำรหัสขนาด 7 บิต
1	**1**	1	0	0	1	0	คำรหัส
1	-	1	-	0	-	0	บิตตรวจสอบ (P1) = 0
1	**1**	-	-	0	1	-	บิตตรวจสอบ (P2) = 1
1	**1**	1	0	-	-	-	บิตตรวจสอบ (P3) = 1

ถ้าต้องการให้ข้อมูลนั้นมีความสัมพันธ์กันค่า $b_{i,j}$ จะเท่ากับ "1" และถ้าต้องการให้ข้อมูลไม่มีความสัมพันธ์ค่า $b_{i,j}$ จะมีค่าเท่ากับ "0"

$$p = \begin{bmatrix} b_{1,1}\ b_{1,2}\ \ldots\ldots\ b_{1,k} \\ b_{2,1}\ b_{2,2}\ldots\ldots\ b_{2,k} \\ .\quad .\quad \ldots\ldots\ . \\ b_{n-k,1}\ b_{n-k,2}\ldots\ b_{n-k,k} \end{bmatrix} \tag{2.15}$$

จากคำรหัส C ประกอบด้วย

$$\begin{aligned} C &= [m_1\ m_2\ \ldots..\ m_k \mid p_1\ p_2\ \ldots.\ p_{n-k}] \\ &= [M \mid MP] \\ &= M[I \mid P] \end{aligned} \tag{2.16}$$

M คือเมทริกซ์ข้อมูล I คือเมทริกซ์เอกลักษณ์และ P คือเมทริกซ์ตรวจสอบ

ถ้ากำหนดให้เมทริกซ์ $[I \mid P] = G$ จะได้

$$C = MG \tag{2.17}$$

G คือเมทริกซ์กำเนิด (Generator Matrix)

ตัวอย่างเมทริกซ์กำเนิดของรหัสแฮมมิง (7,4) มีดังต่อไปนี้

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{2.18}$$

และถ้ากำหนดให้เมทริกซ์ H มีค่าดังสมการ

$$H = [A^t \mid I] \tag{2.19}$$

เมทริกซ์ H นี้จะถูกเรียกว่าเมทริกซ์ตรวจสอบพาริตี้ (Parity Check Metric) โดยคุณสมบัติอย่างหนึ่งของเมทริกซ์ตรวจสอบพาริตี้นี้คือผลคูณระหว่าง H' และ G จะมีค่าเท่ากับศูนย์ดังสมการ

$$H'G = 0$$

และค่าซินโดรม (Syndrome: S) ของรหัสแฮมมิงแสดงได้ดังสมการ

$$S = H * C \tag{2.20}$$

ซึ่งค่าซินโดรมจะใช้บอกถึงตำแหน่งของความผิดพลาดที่เกิดขึ้นกับข้อมูลที่ภาครับได้รับ ถ้าข้อมูลที่ภาครับไม่เกิดความผิดพลาดค่าซินโดรมที่คำนวณได้จะมีค่าเท่ากับ “0” และถ้าข้อมูลที่ภาครับได้รับเกิดความผิดพลาดค่าซินโดรมจะมีค่าไม่เท่ากับศูนย์ ตัวอย่างเมื่อต้องการเข้ารหัสข้อมูล “1001” ด้วยรหัสแฮมมิง (7,4) โดยคำรหัสที่สร้างขึ้นใช้เมทริกซ์กำเนิดที่ได้จากสมการที่ (2.17) และ (2.18) คำรหัสที่สร้างได้มีดังต่อไปนี้

$$C = MG$$

$$= [1\,0\,0\,1] \times \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$= 1\,0\,0\,1\,0\,0\,1$$

เมื่อคำรหัสนี้ถูกส่งไปยังภาครับ ภาครับจะคำนวณหาค่าซินโดรมเพื่อตรวจสอบความถูกต้องข้อข้อมูลที่รับได้หรือหาตำแหน่งของบิตที่ผิดเมื่อข้อมูลที่รับได้เกิดความผิดพลาดขึ้น ในกรณีของข้อมูลที่รับได้ไม่เกิดความผิดพลาดค่าซินโดรมจะมีค่าเท่ากับศูนย์ดังนี้

$$S = H * C$$

$$= \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

ในกรณีเกิดความผิดพลาดขึ้นหนึ่งบิตภายในบล็อกคำรหัส ภาครับได้รับคำรหัสคือ“1011001” ค่าซินโดรมที่ภาครับคำนวณได้มีดังต่อไปนี้

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

ซึ่งค่าซินโดรมที่หาได้จะเท่ากับ “101” โดยค่าซินโดรมจะบอกถึงตำแหน่งของบิตคำรหัสที่เกิดความผิดพลาดขึ้น โดยในตัวอย่างนี้คือตำแหน่งที่ “5” ดังนั้นทางผู้รับสามารถแก้ไขความผิดพลาดที่เกิด ขึ้นและได้รับข้อมูลที่ถูกต้องกลับมา ในกรณีเกิดความผิดพลาดมากกว่าหนึ่งบิตในบล็อกคำรหัส เช่นมีบิตผิดภายในบล็อกคำรหัสสองบิตหากภาครับใช้ค่าซินโดรมเพื่อแก้ไขความผิดพลาดจะส่งผลให้เกิดการผิดของบิตภายในบล็อกเพิ่มขึ้นเป็นสามบิต เช่น คำรหัสที่ภาครับได้รับโดยไม่เกิดความผิดพลาดคือ “1001001” หากเกิดความผิดพลาดขึ้นสองบิตในบล็อกคำรหัสนี้คำรหัสที่ภาครับได้รับอาจเป็น “1011011” (มีการผิดในตำแหน่งที่ “2” ตำแหน่งที่ “5”) โดยจากสมการที่ (2.20) ค่าซินโดรมชี้ตำแหน่งบิตผิดนี้สามารถแสดงได้ดังต่อไปนี้

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

ซึ่งค่าซินโดรมจะชี้ตำแหน่งการผิดไปที่ตำแหน่งที่ "7" หากทำการแก้ไขบิตผิดภายในบล็อกที่ตำแหน่งที่ "7" จะส่งผลให้เกิดการผิดของบิตเพิ่มขึ้นเป็นสามบิตคือในตำแหน่งที่ "2" "5" และตำแหน่งที่ "7" เป็นต้น

2.5.3 รหัสบีซีเอช

รหัสบีซีเอช (รหัส BCH) เป็นหนึ่งในรหัสบล็อกเชิงเส้นโดยจัดอยู่ในกลุ่มรหัสประเภทรหัสวน (Cyclic Code) แบบไบนารีเนื่องจากรหัสชนิดนี้มีขนาดคำรหัสและอัตราการเข้ารหัส (Code Rate) ที่แตกต่างกันซึ่งคุณสมบัติของรหัสบีซีเอชมีดังต่อไปนี้

ความยาวบล็อก $n = 2^m - 1$

ความยาวของข้อมูล $k \geq n - mt$

ระยะแฮมมิงน้อยที่สุด $d_{\min} = 2t + 1$

จากคุณสมบัตินี้ทำให้รหัสบีซีเอชสามารถแก้ไขบิตผิดพลาดภายในบล็อกคำรหัสขนาด $n = 2^m - 1$ บิตได้เท่ากับหรือน้อยกว่า t บิต

2.5.3.1 พหุนามกำเนิดรหัสบีซีเอช

การหาค่าพหุนามกำเนิด (Generator Polynomial) ของรหัสบีซีเอชสามารถหาได้โดยกำหนดให้ α เป็นพริมีทีฟอีลีเมนต์ (Primitive Element) บนฟิลด์กาลัว 2^m หรือ $GF(2^m)$ โดยพหุนามกำเนิดของรหัสบีซีเอชที่มีความยาวคำรหัส $n = 2^m - 1$ บิตและความสามารถในการแก้ไขความผิดพลาด t บิตจะมีพหุนามดีกรีต่ำสุดดังต่อไปนี้ $\alpha, \alpha^2, \alpha^3, ..., \alpha^{2t}$ กำหนดให้ $m_i(x)$ เป็นพหุนามต่ำสุด (Minimum Polynomial) ของ α^i ดังนั้นพหุนามกำเนิดสามารถหาได้จากค่าผลคูณร่วมน้อย (Least Common Multiple: LCM) ของ $m_1(X), m_2(X), ..., m_{2t}(X)$ ทั้งหมดดังสมการ

$$g(X) = LCM\left(m_1(X), m_2(X), ..., m_{2t}(X)\right) \tag{2.21}$$

$\alpha, \alpha^2, \alpha^3, ..., \alpha^{2t}$ เป็นรากของ g(X) และ $g(\alpha^i) = 0$ สำหรับ i=1, 2,..., 2t

ดังนั้นกำลังคู่และกำลังคี่ของ α จะมีพหุนามต่ำสุดเหมือนกันทำให้ผลลัพธ์พหุนามกำเนิดของรหัสบีซีเอชลดลงเหลือ

$$g(X) = LCM\left(m_1(X), m_3(X), ..., m_{2t-1}(X)\right) \tag{2.22}$$

เนื่องจากพหุนามทุกตัวจะมีดีกรีไม่เกิน m ดังนั้นผลคูณของพหุนามต่ำสุดลำดับของพหุนามทั้งหมด t ตัวจะเท่ากับหรือน้อยกว่า $m \times t$ เสมอทำให้พาริตี้บิตของรหัสบีซีเอชจะมีความยาว $n-k$ บิตและจะมีความยาวไม่เกิน $m \times t$ บิตด้วยเช่นกัน

2.5.3.2 การเข้ารหัสบีซีเอช

การเข้ารหัสบีซีเอชสามารถทำได้โดยนำข้อมูล $u(X)$ มาสร้างพหุนามดีกรี $n-k$ และทำการมอดุโล (Modulo) ด้วยพหุนามกำเนิดดังสมการ

$$b(X) = X^{n-k}u(X) \text{ มอดุโล 2 ด้วย } g(X) \tag{2.23}$$

ดังนั้นคำรหัสที่ได้จากการเข้ารหัสบีซีเอชจะได้เป็น

$$v(X) = X^{n-k}u(X) + b(X) \tag{2.24}$$

2.5.3.3 การถอดรหัสบีซีเอช

กำหนดให้ $v(X)=v_0+ v_1X+ v_2X^2+\ldots+ v_{n-1}X^{n-1}$ เป็นพหุนามคำรหัสที่ได้จากการเข้ารหัสบีซีเอชและกำหนดให้ $r(X)==r_0+ r_1X+ r_2X^2+\ldots+ r_{n-1}X^{n-1}$ เป็นพหุนามคำรหัสได้ที่ภาครับได้รับซึ่งรูปแบบความผิดพลาดภายในพหุนามที่ภาครับได้รับมีดังต่อไปนี้

$$r(X) = v(X) + e(X) \tag{2.25}$$

กระบวนการถอดรหัสบีซีเอชแบ่งออกเป็นสามขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 คำนวณหาค่าของซินโดรม $S = S_1, S_2S_3,\ldots,S_{2t}$ จากพหุนามที่ภาครับได้รับ $r(X)$ ซึ่งรหัสบีซีเอชที่มีความสามารถในการแก้ไขความผิดพลาดได้ t บิตต่อบล็อกจะมีค่าซินโดรมทั้งสิ้น $2t$

ขั้นตอนที่ 2 หาค่าของพหุนาม $\alpha(X)$ ของตำแหน่งที่ผิดภายในพหุนามคำรหัสจากค่าซินโดรมที่คำนวณได้จากขั้นตอนที่ 1

ขั้นตอนที่ 3 หาตำแหน่งที่เกิดการผิดพลาดและแก้ไขความผิดพลาดที่เกิดขึ้น

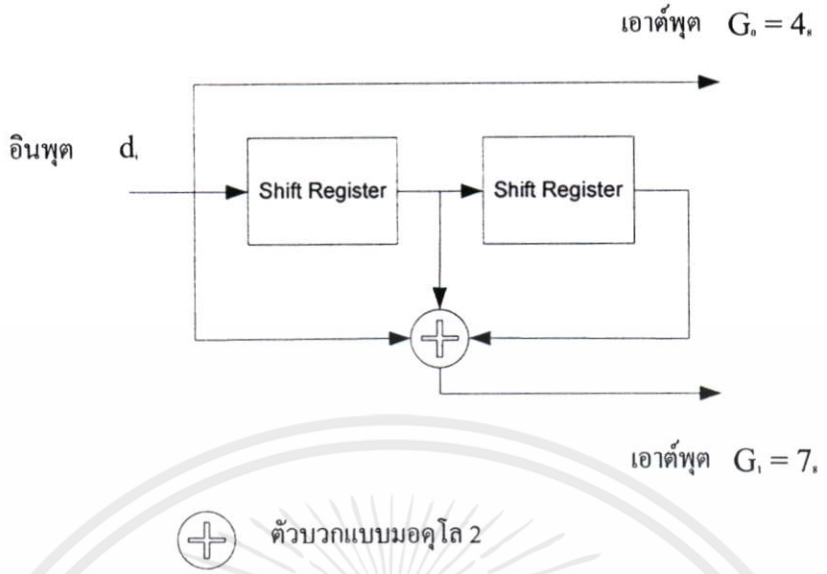
2.5.4 รหัสคอนโวลูชัน

รหัสคอนโวลูชัน (Convolution Code) เป็นหนึ่งในรหัสแก้ไขความผิดพลาดล่วงหน้าซึ่งเสนอในปี ค.ศ.1955 โดย P. Elias การเข้ารหัสคอนโวลูชันเป็นการหาความสัมพันธ์ของกลุ่มข้อมูล

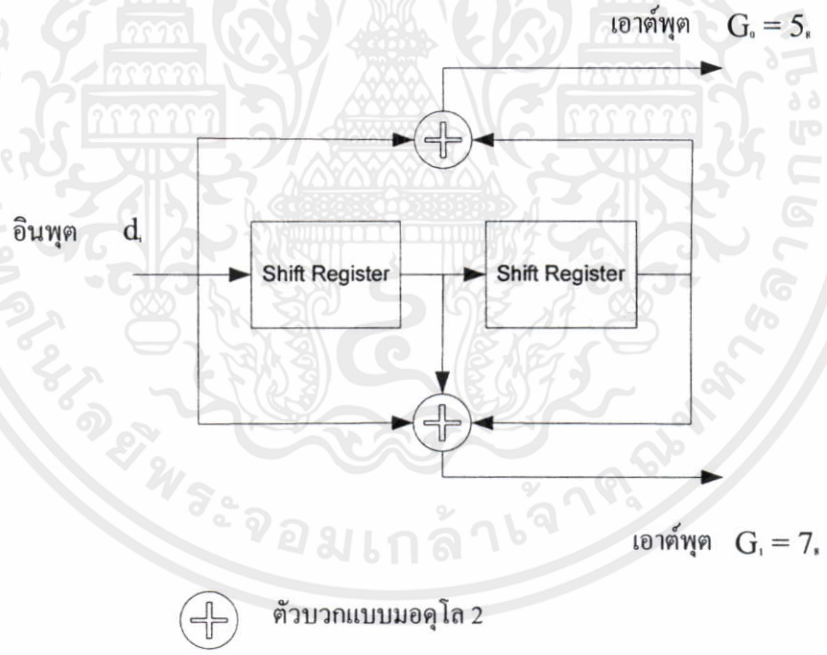
ที่นำมาเข้ารหัสอย่างต่อเนื่อง [18] โดยวงจรเข้ารหัสคอนโวลูชันประกอบด้วยชิพเรจิสเตอร์ (Shift Register) และตัวบวกแบบมอดุโล 2 (Modulo-2 Adder) ส่วนวิธีการถอดรหัสคอนโวลูชันจะมีอยู่หลายวิธีด้วยกันเช่น การถอดรหัสด้วยวิธีตามลำดับ (Sequential Decoding) การถอดรหัสด้วยวิธีย้อนกลับ (Feedback Decoding) การถอดรหัสด้วยวิธีไวเทอร์บี (Viterbi Decoding) เป็นต้น ซึ่งการเข้ารหัสรหัสคอนโวลูชันและวิธีการถอดรหัสคอนโวลูชันมีดังต่อไปนี้

2.5.4.1การเข้ารหัสคอนโวลูชัน

การเข้ารหัสคอนโวลูชันจะนำข้อมูลที่ต้องการเข้ารหัสขนาด k บิตผ่านเข้าสู่วงจรเข้ารหัสคอนโวลูชัน ซึ่งเป็นการเข้ารหัสแบบต่อเนื่องเพื่อหาความสัมพันธ์ของข้อมูล โดยข้อมูลเอาต์พุต (Output) ของการเข้ารหัสคอนโวลูชันขนาด n บิต เกิดจากการนำข้อมูลอินพุตและข้อมูลภายในชิพเรจิสเตอร์มาบวกแบบมอดุโล 2 (Modulo 2) ซึ่งจำนวนข้อมูลไบนารีที่จะนำมาหาความสัมพันธ์กันจะขึ้นอยู่กับค่า Constraint Length (K) ของรหัสคอนโวลูชันโดยค่า Constraint Length เป็นค่าที่แสดงจำนวนข้อมูลอินพุตและข้อมูลสูงสุดในชิพเรจิสเตอร์ที่นำมาบวกแบบมอดุโล 2 เพื่อหาค่าคำรหัส ส่วนค่าอัตราการเข้ารหัส (R) เป็นอัตราส่วนระหว่างจำนวนข้อมูลอินพุตต่อจำนวนเอาต์พุตหรือ (k/n) โดยจำนวนเอาต์พุตของการเข้ารหัสคอนโวลูชันมีจำนวนมากกว่าอินพุตซึ่งรูปแบบของการเข้ารหัสคอนโวลูชันแบ่งออกได้เป็นสองรูปแบบได้แก่ รหัสคอนโวลูชันแบบสมมาตรและรหัสคอนโวลูชันแบบอสมมาตร โดยผลลัพธ์หรือคำรหัสที่ได้จากการเข้ารหัสคอนโวลูชันแบบสมมาตรจะยังคงมีข้อมูลส่วนหนึ่งที่ยังคงมีลักษณะเหมือนข้อมูลที่นำมาเข้ารหัสอยู่ ตัวอย่างของวงจรเข้ารหัสคอนโวลูชันแบบสมมาตรที่อัตราการเข้ารหัสเท่ากับ 1/2 และค่า K เท่ากับสามแสดงดังรูปที่ 2.5 ในส่วนการเข้ารหัสคอนโวลูชันแบบอสมมาตรนั้น คำรหัสที่ได้จากวงจรเข้ารหัสจะไม่มีส่วนใดเลยที่เหมือนกับข้อมูลที่นำมาเข้ารหัส ซึ่งตัวอย่างวงจรเข้ารหัสคอนโวลูชันแบบอสมมาตรที่อัตราการเข้ารหัสเท่ากับ 1/2 และค่า K เท่ากับสามแสดงดังรูปที่ 2.6



รูปที่ 2.5 ตัวอย่างวงจรเข้ารหัสคอนโวลูชันแบบสมมาตร



รูปที่ 2.6 ตัวอย่างวงจรเข้ารหัสคอนโวลูชันแบบอสมมาตร

2.5.4.2การถอดรหัสคอนโวลูชัน

การถอดรหัสคอนโวลูชันนั้นมีขั้นตอนที่ซับซ้อนกว่าวิธีการเข้ารหัสมากซึ่งการตัดสินใจเพื่อให้ได้ข้อมูลที่ถูกต้องมีรูปแบบการตัดสินใจทั้งหมดสองวิธี คือการตัดสินใจแบบหยาบ (Hard Decision) และการตัดสินใจแบบละเอียด (Soft Decision) ซึ่งรายละเอียดของแต่ละวิธีมีดังต่อไปนี้

- **การตัดสินใจแบบหยาบ**

การทำงานของวงจรถอดรหัสจะทำการตัดสินใจตามข้อมูลอินพุตที่รับจากส่วนของการแยกสัญญาณ (Demodulator) ที่ถูกจัดระดับเป็นสองระดับคือ "0" และ "1" ต่ออินพุตหนึ่งบิตโดยการตัดสินใจแบบหยาบนี้เหมาะสำหรับใช้ในช่องสัญญาณแบบไบนารี (Binary Symmetric Channel: BSC) หรือ Discrete Memoryless Channel

- **การตัดสินใจแบบละเอียด**

การตัดสินใจแบบละเอียดจะทำการตัดสินใจโดย ข้อมูลอินพุตที่รับจากภาคแยกสัญญาณสัญญาณที่รับได้จากช่องสัญญาณการสื่อสารจะถูกจัดระดับมากกว่าสองระดับต่ออินพุตหนึ่งอินพุต เช่น 4 ระดับ (2 บิต) หรือ 8 ระดับ (3 บิต) เป็นต้น การตัดสินใจแบบละเอียดมีการทำงานที่ซับซ้อนกว่าแบบหยาบแต่ให้ค่า Coding Gain ที่มากกว่า

2.5.4.3 การถอดรหัสคอนโวลูชันด้วยวิธีไวเทอร์บี

การถอดรหัสคอนโวลูชันโดยวิธีไวเทอร์บี (Viterbi Decoding) เป็นหนึ่งในวิธีการถอดรหัสคอนโวลูชันที่มีความซับซ้อนน้อย เนื่องจากวิธีนี้จะลดความเป็นไปได้ของเส้นทางที่เป็นไปได้ตามแผนภาพเทรลลิส ซึ่งการถอดรหัสโดยวิธีนี้อาศัยระยะแฮมมิงที่เป็นค่าความแตกต่างระหว่างบิตข้อมูลที่รับได้และบิตข้อมูลบนแผนภาพเทรลลิส ณ เวลานั้น ในการถอดรหัสคอนโวลูชันโดยวิธีไวเทอร์บีมีขั้นตอนการทำงานทั้งสิ้นสาม ขั้นตอน [19] ดังต่อไปนี้

ขั้นตอนที่ 1 Branch Metric Generation

ขั้นตอนนี้เป็นการคำนวณหาค่า Branch Metric จากข้อมูลอินพุตที่รับเข้ามา r กับค่าเอาต์พุตของการเข้ารหัส C การคำนวณหาค่า Branch Metric ต้องคำนวณทุกๆ สาขาหรือ Branch ตามสถานะโดยจำนวน Branch เท่ากับ 2^K การคำนวณหาค่า Branch Metric ดังสมการ [19]

$$BM_{i,j,n} = (r_n - C_{i,j})^2 \tag{2.26}$$

BM แทนค่า Branch Metric ระหว่างสถานะ i ไปยังสถานะ j ณ เวลา n

r แทนค่า ข้อมูลอินพุตที่รับเข้ามา ณ เวลา n

C แทนค่าเอาต์พุตของการเข้ารหัสระหว่างสถานะ i ไปยังสถานะ j ณ เวลา n

ขั้นตอนที่ 2 Survivor Path and Path Metric Update

ขั้นตอนนี้เป็นการคำนวณหาค่า Survivor Path และ Path Metric จากจำนวนสถานะ การทำงานทั้งหมดโดยค่า Path Metric ที่เลือกไว้เพื่อใช้ในการหาค่า Path Metric ครั้งต่อไป (Update) ส่วนค่า Survivor Path เป็นค่าที่ใช้ในการตัดสินใจหาค่าเอาต์พุตโดยการคำนวณหาค่า Survivor path และ Path Metric นั้นค่าของ Branch Metric และ Path Metric จะถูกรวมเข้าด้วยกันซึ่งผลการรวมนั้นมีสองค่าที่เข้ามาในแต่ละจุดเชื่อมต่อของแผนภาพเทรลลิส โดยค่า Path Metric เป็นค่าที่เลือกจากค่าผลบวกที่น้อยกว่าส่วนค่า Survivor Path เป็นสถานะ การทำงานที่น้อยกว่าจากการเลือก Path Metric ดังสมการ

$$PM_{j,n} = min(PM_{i,n-1} + BM_{i,j,n}, PM_{i+1,n-1} + BM_{i+1,j,n}) \qquad (2.27)$$

PM แทน Path Metric ระหว่างสถานะ i ไปยังสถานะ j ณ เวลา n

BM แทนค่า Branch Metric ระหว่างสถานะ i ไปยังสถานะ j ณ เวลา n

ขั้นตอนที่ 3 Optimum Paths Trace Back

ขั้นตอนนี้เป็นขั้นตอนการตัดสินใจหาค่าเอาต์พุตหรือข้อมูลที่ภาคส่งได้ส่งมายังภาครับโดยใช้ค่า Survivor Path ในแต่ละสถานะที่บันทึกไว้มาตัดสินใจเลือกเส้นทางข้อมูลโดยอาศัยการตัดสินใจหาเส้นทางของข้อมูลจะเริ่มจาก Survivor Path ในอดีต (Trace Back) ย้อนกลับไปยังตำแหน่งเริ่มต้น

บทที่ 3
วิทยาการรหัสลับเชิงควอนตัม

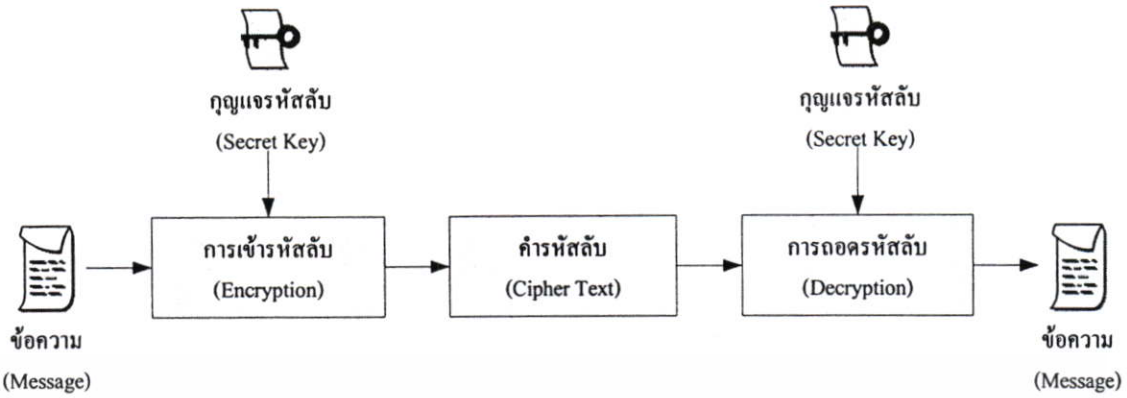
การส่งข้อมูลข่าวสารผ่านระบบเครือข่ายทั้งเครือข่ายภายในองค์กรหรือเครือข่ายสาธารณะ เช่น อินเตอร์เน็ต ข้อมูลบางประเภทไม่สามารถเปิดเผยให้บุคคลอื่นรับรู้ได้เช่น ข้อมูลทางการเงิน รหัสบัตรเครดิต ข้อมูลลับทางการทหาร ข้อมูลลับของแต่ละบริษัท ห้างร้านหรืออื่นๆ เป็นต้น ข้อมูลเหล่านี้มีความจำเป็นที่ต้องส่งผ่านเครือข่ายเพื่อความสะดวก รวดเร็วในการติดต่อสื่อสารระหว่างผู้ส่งและผู้รับ ดังนั้นการส่งข้อมูลผ่านเครือข่ายเหล่านี้ อาจทำให้ข้อมูลถูกเปิดเผยสู่สาธารณชนหรือบุคคลที่ไม่พึงประสงค์ ถ้าหากไม่รักษาความปลอดภัยของข้อมูลเหล่านี้ก่อนทำการส่ง ซึ่งจะส่งต่อระบบเศรษฐกิจและความมั่นคงของประเทศตามมาเพื่อรักษาความปลอดภัยของข้อมูลสำคัญเหล่านี้ วิทยาการรหัสลับ (Cryptography) เป็นวิธีการหนึ่งที่นำมาใช้ซ่อนความหมายหรือเปลี่ยนแปลงรูปแบบของข้อมูลที่ส่ง เพื่อทำให้บุคคลที่สามหรือ *Eve* ไม่สามารถรู้ความหมายของข้อมูลเหล่านี้ โดยผู้ส่งจะนำข้อมูลที่ต้องการส่งมาผ่าน "การเข้ารหัสลับ" (Encryption) โดยอาศัยกุญแจรหัสลับ (Secret Key) ข้อมูลที่ผ่านการเข้ารหัสลับจะถูกเรียกว่า "คำรหัสลับ" (Cipher Text) ซึ่งจะเป็นข้อความในรูปแบบใหม่ที่ไม่มีบุคคลใดทราบความหมายและเมื่อข้อความนี้ส่งมาถึงยังผู้รับ ผู้รับจะนำคำรหัสลับมาผ่านกระบวนที่เรียกว่า "การถอดรหัสลับ" (Decryption) โดยอาศัยกุญแจรหัสลับเพื่อเปลี่ยนคำรหัสลับให้กลับมาเป็นข้อมูลจริงที่ผู้ส่งได้ส่งมา ซึ่งกระบวนการทำงานของวิทยาการรหัสลับแสดงดังรูปที่ 3.1 ตัวอย่างวิทยาการรหัสลับที่ใช้ในปัจจุบันเช่น

- **วิทยาการรหัสลับแบบสมมาตร**

วิทยาการรหัสแบบสมมาตร (Systematic Cryptography) เป็นวิทยาการรหัสลับที่ใช้กุญแจรหัสลับในการเข้ารหัสลับและถอดรหัสลับชุดเดียวกัน ซึ่งวิทยาการรหัสลับนี้สามารถเข้าและถอดรหัสลับได้อย่างรวดเร็ว ตัวอย่างรหัสลับแบบสมมาตรได้แก่ รหัสลับแบบ One-Time Pad รหัสลับ Advanced Encryption Standard (AES) รหัสลับ Data Encryption Standard (DES) รหัสลับ 3DES (Triple DES) เป็นต้น สิ่งสำคัญของวิทยาการรหัสลับนี้เกิดเนื่องมาจากการเข้าและถอดรหัสลับของวิทยาการรหัสลับนี้ใช้กุญแจรหัสลับชุดเดียวกัน ดังนั้นการกระจายกุญแจรหัสลับหรือการส่งกุญแจรหัสลับจึงเป็นปัญหาที่สำคัญที่สุดที่ทำอย่างไรจะทำให้กุญแจรหัสลับส่งไปยังผู้รับได้อย่างถูกต้องและปลอดภัยที่สุด

- **วิทยาการรหัสลับแบบอสมมาตร**

วิทยาการรหัสลับแบบอสมมาตร (Asystematic Cryptography หรือ Public Key Cryptography) เป็นวิทยาการรหัสลับที่อาศัยกุญแจรหัสลับที่บุคคลใดก็สามารถนำกุญแจรหัสลับนี้



รูปที่ 3.1 การทำงานของวิทยาการรหัสลับ

มาใช้ทำการเข้ารหัสลับเรียกกุญแจรหัสลับนี้ว่า "*กุญแจรหัสลับสาธารณะ (Public Key)*" โดยผู้ส่งจะต้องใช้กุญแจรหัสลับสาธารณะให้ตรงกับกุญแจรหัสลับสาธารณะของผู้รับ การถอดรหัสลับผู้รับจะใช้กุญแจรหัสลับที่เรียกว่า "*กุญแจรหัสลับส่วนตัว (Private Key)*" โดยกุญแจรหัสลับส่วนตัวนี้มีเฉพาะเพียงผู้ที่เป็นเจ้าของหรือผู้รับเท่านั้น หลักการที่นำมาใช้เพื่อป้องกันและรักษาความลับข้อมูลข่าวสารของวิทยาการรหัสลับแบบอสมมาตรนี้อาศัยการแยกตัวประกอบจำนวนเฉพาะ (Prime Number) ซึ่งการทำงานจะอาศัยฟังก์ชันทางเดียว (One-way Function) ซึ่งเป็นฟังก์ชันที่ดำเนินการคำนวณเพื่อหาผลลัพธ์นั้นจะทำได้ง่ายแต่หากนำผลลัพธ์มาคำนวณย้อนกลับเพื่อหาข้อมูลต้นฉบับจะคำนวณได้ยากและมีความซับซ้อนสูงซึ่งด้วยเทคโนโลยีด้านการคำนวณเช่น คอมพิวเตอร์ที่ใช้อยู่ในปัจจุบัน การที่บุคคลที่สามหรือบุคคลที่ไม่พึงประสงค์ (โดยทั่วไปจะเรียกว่า "*Eve*") จะสามารถแยกตัวประกอบจำนวนเฉพาะจำนวนมากเหล่านี้ เพื่อหาผลลัพธ์นี้ได้อาจจะใช้เวลาหลายปีหรืออาจจะใช้เวลาหลายร้อยปี จึงทำให้เชื่อได้ว่าวิทยาการรหัสลับนี้สามารถรักษาความลับข้อมูลได้แต่รหัสลับนี้ยังไม่สามารถยืนยันได้อย่างสมบูรณ์ว่าข้อมูลที่ส่งจะไม่มีผู้ลักลอบดักจับและทราบข้อมูลลับนั้น

เมื่อพิจารณาถึงคุณสมบัติของวิทยาการรหัสลับทั้งสองประเภทพบว่าวิทยาการรหัสลับแบบสมมาตรโดยเฉพาะวิธีของเวอร์แนม (Vernam Cipher) เป็นรหัสลับที่มีความปลอดภัยสูงสุดโดยบุคคลที่สามหรือ *Eve* ไม่สามารถถอดรหัสลับได้เลยหากไม่ทราบกุญแจรหัสลับที่ใช้ในการเข้ารหัสลับในแต่ละครั้ง ซึ่งกุญแจรหัสลับที่ใช้ในการเข้าและถอดรหัสลับนี้จะถูกเปลี่ยนเสมอ ปัญหาส่วนใหญ่ที่พบในระบบวิทยาการรหัสลับนี้คือทำอย่างไรจะสามารถส่งกุญแจรหัสลับไปยังผู้รับได้อย่างปลอดภัย ปัจจุบันสามารถใช้วิทยาการรหัสลับแบบอสมมาตรเพื่อรักษาความลับของกุญแจรหัสลับนี้ แต่เมื่อพิจารณาถึงหลักการพื้นฐานที่ใช้ในวิทยาการรหัสลับแบบอสมมาตรที่อาศัยการแยกตัวประกอบจำนวนเฉพาะที่มีค่าจำนวนมาก เมื่อเทคโนโลยีด้านการคำนวณมีความก้าวหน้าเช่น ควอนตัมคอมพิวเตอร์ (Quantum Computer) การแยกตัวประกอบจำนวนเฉพาะที่คอมพิวเตอร์

ในปัจจุบันสามารถทำได้โดยใช้ระยะเวลานาน ควอนตัมคอมพิวเตอร์จะใช้เวลาเพียงเล็กน้อยในการแยกตัวประกอบจำนวนเฉพาะดังกล่าว ทำให้วิทยาการรหัสลับแบบที่ใช้อยู่ปัจจุบันอาจไม่สามารถรักษาความลับได้อีกต่อไป กระบวนการส่งกุญแจรหัสลับรูปแบบใหม่ที่ไม่อาศัยความซับซ้อนทางการคำนวณหรือคุณสมบัติของจำนวนเฉพาะถูกเสนอขึ้นโดยอาศัยคุณสมบัติทางควอนตัมของแสงเพื่อส่งกุญแจรหัสลับ กระบวนการส่งกุญแจรหัสลับนี้เรียกว่า "*รหัสลับเชิงควอนตัม* (Quantum Cryptography)" หรือการกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution: QKD) ซึ่งวิทยาการรหัสลับเชิงควอนตัมใช้ทฤษฎีกลศาสตร์ควอนตัม (Quantum Mechanics) ช่วยยืนยันความปลอดภัยของระบบถ้าหากมีผู้บุกรุกเข้ามาขโมยกุญแจรหัสลับระหว่างการส่ง ผู้ส่งหรือ *Alice* และผู้รับหรือ *Bob* จะรับทราบได้ทันทีถึงการเข้ามาขโมยกุญแจรหัสลับโดยอัตราความผิดพลาดของกุญแจรหัสลับที่ส่งจะสูงขึ้นและทำให้ *Alice* และ *Bob* สามารถยกเลิกการส่งกุญแจรหัสลับนั้นทันทีทำให้ระบบส่งกุญแจรหัสลับมีความปลอดภัยสูง

3.1 ประวัติวิทยาการรหัสลับเชิงควอนตัม

วิทยาการรหัสลับเชิงควอนตัมเริ่มต้นจาก ในปี ค.ศ. 1983 Stephen Weisner นำเสนอการส่งข้อมูลไบนารีรูปแบบใหม่โดยใช้โพลาไรเซชัน (Polarization) ของแสงที่ตั้งฉากกันแทนบิต "1" และ บิต "0" ตามรูปแบบการสื่อสารระบบดิจิตอล [20] ซึ่งแนวความคิดนี้ได้กลายเป็นพื้นฐานในการนำโพลาไรเซชันของแสงมาใช้ในการส่งกุญแจรหัสลับบิตในระบบวิทยาการรหัสลับ โดยในปี ค.ศ. 1984 C.H. Bennett และ G. Brassard ได้เสนอโพรโทคอลในการส่งกุญแจรหัสลับบิตที่แทนด้วยสถานะควอนตัมของแสงหรือเรียกว่า คิวบิต (Qubit) เพื่อใช้แทนกุญแจรหัสลับในระบบวิทยาการรหัสลับผ่านทางช่องสื่อสารเชิงแสงขึ้นเป็นโพรโทคอลแรกเรียกว่า โพรโทคอลBB84"[1] ในปี ค.ศ. 1991 A.K. Ekert ได้เสนอแนวความคิดที่ใช้คู่โฟตอนพัวพัน (Entangled Photon) เพื่อแทนกุญแจรหัสลับที่ต้องการส่งเรียกรูปแบบการส่งนี้ว่าโพรโทคอลEkert91[8] หลังจากโพรโทคอลแรกที่ได้นำเสนอ ในปี ค.ศ. 1992 C.H.Bennett G.Brassard และคณะ ได้แสดงระบบวิทยาการรหัสลับเชิงควอนตัมที่สามารถใช้ในการส่งกุญแจรหัสลับจริงเป็นระบบแรกของโลกโดยใช้โพรโทคอลBB84 สามารถส่งกุญแจรหัสลับผ่านอากาศเป็นระยะทาง 32 เซนติเมตรด้วยอัตราเร็วในการส่ง 10 บิตต่อวินาที [2] และในปีเดียวกัน C.H. Bennett ได้นำเสนอรูปแบบการส่งกุญแจรหัสลับใหม่ที่ใช้โพลาไรเซชันของโฟตอนเดี่ยวเพียงสองสถานะที่ไม่ตั้งฉากกัน เรียกว่าโพรโทคอลB92 [7] โดยเป็นการพัฒนารูปแบบการส่งมาจากโพรโทคอลBB84 เพื่อที่จะลดความซับซ้อนของการจัดเรียงอุปกรณ์การสื่อสารเชิงแสงและเพื่อลดความผิดพลาดที่เกิดขึ้นระหว่างการส่ง หลังจากนั้นในปี ค.ศ. 1999 T.C. Ralph ได้เสนอรูปแบบการส่งกุญแจรหัสลับใหม่นอกเหนือจากการใช้โฟตอนเดี่ยว โดยอาศัยสถานะ Squeezed State ที่ประกอบด้วยจำนวนโฟตอนที่มากกว่าหนึ่งหน่วยเพื่อเป็นสื่อกลางในการส่งกุญแจรหัสลับเรียกรูปแบบการส่งกุญแจรหัสลับนี้ว่า การกระจายกุญแจรหัสลับ

แบบต่อเนื่อง (CV-QKD) [21] ในปี ค.ศ. 2000 M.D. Reid ได้แสดงแนวความคิดในการส่งกุญแจรหัสลับในระบบกระจายกุญแจรหัสลับแบบต่อเนื่องด้วยคู่โฟตอนพัวพัน (Entangled Photon) [22] และในปี ค.ศ. 2002 F.Grosshans และ Ph. Grangier ได้เสนอรูปแบบการส่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์ในระบบกระจายกุญแจรหัสลับแบบต่อเนื่องด้วยสถานะโคฮีเรนต์ของแสง โดยระบบที่นำเสนอสามารถส่งกุญแจรหัสลับได้เร็วถึง 1.7 Mbps ในช่องสื่อสารที่ไม่มีการสูญเสียและ 75 kbps ในการส่งผ่านช่องสื่อสารที่มีการสูญเสีย 3.1 dB [9] จากการพัฒนารูปแบบและเทคนิคที่ใช้ในการส่งกุญแจรหัสลับ ระบบวิทยาการรหัสลับเชิงควอนตัมได้พัฒนาให้สามารถส่งกุญแจรหัสลับได้ระยะทางไกลและมีอัตราเร็วที่สูงขึ้น ซึ่งในปัจจุบันวิทยาการรหัสลับเชิงควอนตัมสามารถส่งผ่านอากาศระยะทาง 144 กิโลเมตร โดยใช้โพรโทคอล BB84 ด้วยอัตราเร็วในการส่ง 12 bps ซึ่งการวิจัยพัฒนาระบบวิทยาการรหัสลับเชิงควอนตัมนี้เป็นการรวมกลุ่มของนักวิจัยจากหลายประเทศ เช่น ประเทศเยอรมนี ออสเตรีย สิงคโปร์ และสหราชอาณาจักร [23] นอกจากนี้กลุ่มนักวิจัยจาก NTT (NTT Basic Research Laboratories) จากประเทศญี่ปุ่น National Institute of Standard and Technologies (NIST) และ Stanford University ประเทศสหรัฐอเมริกา ได้ทำการพัฒนาระบบวิทยาการรหัสลับเชิงควอนตัมผ่านเส้นใยนำแสง (Fiber Optic) ที่ความยาวคลื่น 1550 นาโนเมตร ระยะทาง 105 กิโลเมตร ด้วยอัตราเร็ว 17 kbps และที่ระยะทาง 200 กิโลเมตร ด้วยอัตราเร็วในการส่ง 12.1 bps [24]

3.2 วิทยาการรหัสลับเชิงควอนตัม

วิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography) หรือการกระจายกุญแจรหัสลับเชิงควอนตัม (Quantum Key Distribution: QKD) เป็นระบบในการส่งกุญแจรหัสลับผ่านช่องทางการสื่อสารเชิงควอนตัม (Quantum Channel) เช่น เส้นใยนำแสง (Fiber Optic) และอากาศ (Free Space) โดยกุญแจรหัสลับจะถูกแทนด้วยสถานะทางควอนตัมของแสงเช่น โพลาไรเซชัน เฟสของโพลาไรเซชัน เป็นต้น และใช้กฎทางควอนตัมฟิสิกส์ช่วยยืนยันความปลอดภัยของระบบที่สามารถตรวจพบผู้ที่เข้ามาลักลอบขโมยสถานะควอนตัมทางช่องทางการสื่อสารเชิงควอนตัมได้เสมอ

ระบบวิทยาการรหัสลับเชิงควอนตัมแบ่งการทำงานเป็นสองขั้นตอนคือ การส่งกุญแจรหัสลับผ่านช่องทางการสื่อสารเชิงควอนตัม (Quantum Channel) และการกลั่นกุญแจรหัสลับ (Secret Key Distillation) ซึ่งการกลั่นกุญแจรหัสลับนี้แบ่งการทำงานเป็นสองกระบวนการย่อยได้แก่ กระบวนการไกล่เกลี่ยความผิดพลาด (Reconciliation) เป็นกระบวนการแก้ไขความผิดพลาดของกุญแจรหัสลับที่แตกต่างกันระหว่าง *Alice* และ *Bob* ให้กลับมาเหมือนกันโดย *Alice* จะทำการส่งข้อมูลบางอย่างเกี่ยวกับกุญแจรหัสลับของตนไปให้ *Bob* ผ่านทางช่องสื่อสารสาธารณะ (Public Channel) และ *Bob* จะใช้ข้อมูลนี้ร่วมกับกุญแจรหัสลับของตนเพื่อแก้ไขกุญแจรหัสลับที่แตกต่างให้เหมือนกุญแจรหัสลับของ *Alice* เรียกว่าการไกล่เกลี่ยทางตรง (Direct Reconciliation) นอกจากนี้

Bob สามารถที่จะส่งข้อมูลบางอย่างเกี่ยวกับกุญแจรหัสลับของตนไปให้ *Alice* เพื่อให้ *Alice* ทำการเปลี่ยนกุญแจรหัสลับของตนให้เหมือนกับ *Bob* เรียกว่าการไกล่เกลี่ยย้อนกลับ (Reverse Reconciliation) [25] และกระบวนการขยายสภาวะส่วนตัว (Privacy Amplification) เป็นกระบวนการลดความสำคัญของข้อมูลเกี่ยวกับกุญแจรหัสลับที่บุคคลที่สามหรือ *Eve* ซึ่ง *Eve* อาจจะเข้ามาขโมยสถานะทางควอนตัมของแสงระหว่างการส่งกุญแจรหัสลับทางช่องทางการสื่อสารเชิงควอนตัมและได้ข้อมูลเกี่ยวกับกุญแจรหัสลับไปเพียงเล็กน้อย และข้อมูลเกี่ยวกับกุญแจรหัสลับระหว่างกระบวนการไกล่เกลี่ยความผิดพลาด จากการเข้ามาขโมยทางช่องสื่อสารสาธารณะ หาก *Eve* ได้รับข้อมูลเกี่ยวกับกุญแจรหัสลับมากเกินไปอาจทำให้ *Eve* สามารถทำสำเนากุญแจรหัสลับใหม่ขึ้นมาได้ ซึ่งจะทำให้ระบบเกิดความไม่ปลอดภัย ดังนั้น *Alice* และ *Bob* จำเป็นต้องลดความสามารถในการสร้างกุญแจรหัสลับใหม่ของ *Eve* ด้วยขั้นตอนการขยายสภาวะส่วนตัว ปัจจุบันวิทยาการรหัสลับเชิงควอนตัมแบ่งออกเป็นสองระบบดังนี้

3.2.1 การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง

การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (Discrete Variable Quantum Key Distribution: DV-QKD) เป็นรูปแบบการกระจายกุญแจรหัสลับเชิงควอนตัมรูปแบบแรก ระบบนี้จะทำการส่งกุญแจรหัสลับบิตจาก *Alice* ไปให้ *Bob* ผ่านทางช่องสื่อสารเชิงควอนตัม โดยการแทนกุญแจรหัสลับบิตที่ต้องการส่งด้วยโพลาไรเซชันหรือเฟสของโพลาไรเซชันของโฟตอนเดี่ยว (Single Photon) เช่นโพรโทคอลBB84 [1] โพรโทคอลB92 [7] โพรโทคอลEkert91 [8] เป็นต้น ความปลอดภัยของระบบกระจายกุญแจรหัสลับรูปแบบนี้อาศัยกฎความไม่แน่นอน (Uncertainly Principle) ของไฮเซนแบร์ก (Heisenberg) หาก *Eve* เข้ามาขโมยสถานะควอนตัมของโฟตอนเดี่ยวภายในช่องทางการสื่อสารเชิงควอนตัมจะทำให้คุณสมบัติทางควอนตัมของโฟตอนเดี่ยวเปลี่ยนไป ส่งผลให้กุญแจรหัสลับบิตที่ *Alice* ส่งไปให้ *Bob* จะเกิดความผิดพลาดตามไปด้วย ซึ่งจะทำให้ *Alice* และ *Bob* ทราบถึงการเข้ามาขโมยกุญแจรหัสลับของ *Eve* และ *Alice* และ *Bob* จะยกเลิกการส่งกุญแจรหัสลับนั้นโดยทันที ทำให้ระบบการส่งกุญแจรหัสลับนั้นมีความปลอดภัย ตัวอย่างการทำงานโพรโทคอลในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องมีดังต่อไปนี้

- **โพรโทคอลBB84**

โพรโทคอลBB84 เป็นวิธีการส่งกุญแจรหัสลับบิตวิธีแรกในระบบวิทยาการรหัสลับเชิงควอนตัมที่เสนอโดย C.H. Bennett และ G. Brassard ในปี 1984 [1] โพรโทคอลนี้ใช้โพลาไรเซชันของโฟตอนเดี่ยว (Single Photon) สี่สถานะเพื่อแทนบิตสุ่มหรือกุญแจรหัสลับบิตที่ต้องการส่งเช่น บิต “1” แทนด้วยโพลาไรเซชัน 90 องศา (↑) หรือ 45 องศา (↗) และบิต “0” แทนด้วยโพลาไรเซชัน 0 องศา (→) หรือ -45 องศา (↘) และกำหนดเวกเตอร์ฐานเพื่อใช้แทนและใช้เรียกโพลาไรเซชันที่ตั้งฉากซึ่งกัน โดยเวกเตอร์ฐาน ⊕ แทนโพลาไรเซชัน 90 องศา (↑) และ 0 องศา (→) และ

เวกเตอร์ฐาน ⊗ แทนโพลาไรเซชัน 45 องศา (↗) และ -45 องศา (↘) การทำงานของโพรโทคอล BB84 มีดังต่อไปนี้

ลำดับที่ 1 *Alice* ทำการสุ่มโพลาไรเซชันหนึ่งในสี่สถานะแล้วส่งไปยัง *Bob* ผ่านช่องทางการสื่อสารเชิงควอนตัมเช่น อากาศ (Free Space) หรือเส้นใยนำแสง (Fiber Optic)

ลำดับที่ 2 *Bob* ทำการสุ่มเวกเตอร์ฐานจากหนึ่งในสองเวกเตอร์ฐานเพื่อใช้รับโพลาไรเซชันที่ *Alice* ส่งมาโดยค่าที่รับได้ทั้งหมดจะถูกเก็บไว้และเรียกว่าคีย์ดิบ (Raw Key)

ลำดับที่ 3 *Bob* บอก *Alice* เวกเตอร์ฐานที่ตนใช้ในการตรวจรับโพลาไรเซชันผ่านทางช่องสื่อสารสาธารณะเช่น เครือข่ายอินเตอร์เน็ต เป็นต้น

ลำดับที่ 4 *Alice* บอก *Bob* เวกเตอร์ฐานใดบ้างที่ *Bob* ใช้วัดอย่างถูกต้องหรือตรงกับที่ *Alice* ส่งมา ดังนั้นเมื่อถึงกระบวนการนี้ *Alice* และ *Bob* จะมีกุญแจรหัสลับบิตที่เหมือนกันเรียกกุญแจรหัสลับบิตเหล่านี้ว่า "ชิฟคีย์" (Sifted Key) และเรียกกระบวนการนี้ว่า "*Sifting*" โดยขั้นตอนการทำงานของโพรโทคอล BB84 ทั้งหมดแสดงได้ดังตารางที่ 3.1

นอกจากสถานะโพลาไรเซชันแล้วเฟสของโพลาไรเซชันของโฟตอนเดี่ยวยังสามารถใช้แทนกุญแจรหัสลับบิตได้เช่นเดียวกัน การส่งโพลาไรเซชันผ่านเส้นใยนำแสงโพลาไรเซชันของโฟตอนเดี่ยวจะเกิดการเปลี่ยนแปลงเนื่องจากการสะท้อนของแสงภายในเส้นใยนำแสงทำให้การควบคุมโพลาไรเซชันทำได้ยาก เฟสของโพลาไรเซชันของโฟตอนเดี่ยวจึงถูกนำมาใช้ในการส่งกุญแจรหัสลับผ่านเส้นใยนำแสงโดยรูปแบบการทำงานจะเหมือนกับการใช้โพลาไรเซชันของโฟตอนเดี่ยวเช่นกำหนดให้เฟส "0" เรเดียน (Radian) และ "π" เรเดียน แทนเวกเตอร์ฐานที่หนึ่ง เฟส "$\pi/2$"เรเดียน และ "$3\pi/2$" เรเดียน แทนเวกเตอร์ฐานที่สองและกำหนดให้ เฟส "0" เรเดียน และ "$\pi/2$"เรเดียน แทนด้วยบิต "0" และเฟส "π" เรเดียน และ "$3\pi/2$"เรเดียน แทนด้วยบิต "1" การทำงานของวิธีการนี้มีดังต่อไปนี้

ลำดับที่ 1 *Alice* สุ่มเฟสหนึ่งในสี่เฟส (θ_A) ของโพลาไรเซชันของโฟตอนเดี่ยวแล้วส่งไปยัง *Bob* ผ่านช่องทางการสื่อสารเชิงควอนตัม

ลำดับที่ 2 *Bob* สุ่มเวกเตอร์ฐานหรือ θ_B ที่ประกอบด้วย เฟส "0" เรเดียน หรือ "$\pi/2$" เรเดียน มารับเฟสของโฟตอนเดี่ยวที่ *Alice* ส่งมาโดยหากเฟสที่ทำการวัดได้มีความแตกต่างกันศูนย์เรเดียน *Bob* จะเก็บค่าบิต "0" และเฟสที่ทำการวัดได้มีความแตกต่างกัน "π" เรเดียน *Bob* จะเก็บค่าบิต "1" เป็นค่าชิฟคีย์ หากความแตกต่างของเฟสเป็น "$\pi/2$"เรเดียนหรือ "$3\pi/2$"เรเดียน แสดงว่าเวกเตอร์ฐานที่ *Alice* ใช้ส่งและเวกเตอร์ฐานที่ *Bob* ใช้รับแตกต่างกันดังนั้น *Alice* และ *Bob* จะทิ้งค่ากุญแจรหัสลับบิตที่รับมาได้ทั้งหมด

ตารางที่ 3.1 สัญลักษณ์และสถานะโพลาไรเซชันของกุญแจรหัสลับบิตของโพรโทคอลBB84

เวกเตอร์ฐาน / Alice	⊕	⊗	⊕	⊕	⊕
บิต	0	1	0	0	1
สถานะโพลาไรเซชัน	→	↗	→	→	↑
เวกเตอร์ฐาน / Bob	⊕	⊕	⊗	⊕	⊕
คีย์ดิบ	0	1	1	0	1
ชิฟคีย์	0	-	-	0	1

ตารางที่ 3.2 ความสัมพันธ์ระหว่างมุมเฟสกับโพลาไรเซชันในโพรโทคอล BB84

เฟสของโพลาไรเซชัน (เรเดียน)	โพลาไรเซชัน (องศา)	ค่าบิต	เวกเตอร์ฐาน /โพลาไรเซชัน	เวกเตอร์ฐาน /เฟส
0	0	"0"	⊕	0
π	90	"1"	⊕	0
$\pi/2$	45	"1"	⊗	$\pi/2$
$3\pi/2$	-45	"0"	⊗	$\pi/2$

ตารางที่ 3.3 สัญลักษณ์และการส่งกุญแจรหัสลับบิตด้วยเฟสของโพลาไรเซชันของโฟตอนเดี่ยว [12]

Alice / บิต	0	0	1	1	0	0	1	1
เฟสของ*Alice* (θ_A)	0	0	π	π	$\pi/2$	$\pi/2$	$3\pi/2$	$3\pi/2$
เฟสของ *Bob* (θ_B)	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
θ_A-θ_B	0	$3\pi/2$	π	$\pi/2$	$\pi/2$	0	$3\pi/2$	π
ชิฟคีย์	0	-	1	-	-	0	-	1

การเปรียบเทียบการกระจายกุญแจรหัสลับโดยอาศัยเฟสของโพลาไรเซชันของโฟตอนเดี่ยวและโพลาไรเซชันของโฟตอนเดี่ยวที่ใช้ในโพรโทคอล BB84 แสดงดังตารางที่ 3.2 และโพรโทคอล BB84 ที่ใช้เฟสของโพลาไรเซชันของโฟตอนเดี่ยวแสดงการรับส่งกุญแจรหัสลับบิตตามตารางที่ 3.3

3.2.2 การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง

การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (Continuous Variable Quantum Key Distribution: CV-QKD) เป็นระบบกระจายกุญแจรหัสลับเชิงควอนตัมรูปแบบใหม่นอกเหนือจากการใช้โฟตอนเดี่ยว เนื่องจากเทคโนโลยีในปัจจุบันยังไม่สามารถที่จะสร้างโฟตอนเดี่ยวเพื่อใช้ในวิทยาการรหัสลับเชิงควอนตัมแต่จะอาศัยกานลดทอนความเข้มของแสงจนเหลือความเข้มของแสงอ่อน เพื่อจะประมาณค่าเป็นโฟตอนเดี่ยว ซึ่งจะทำให้ระยะทางในการส่งสั้น พัลส์แสงจำนวนมากไม่มีโฟตอนอยู่ดังนั้นการส่งกุญแจรหัสลับจะทำได้อย่างล้าช้า นอกจากนี้บางพัลส์แสงยังมีโฟตอนมากกว่าหนึ่งหน่วยซึ่งจะส่งผลต่อความปลอดภัยของระบบ ดังนั้นระบบวิทยาการรหัสลับนี้จึงถูกพัฒนาขึ้นโดยอาศัยโฟตอนมากกว่าหนึ่งหน่วยเป็นสื่อกลางในการส่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์ ซึ่งจะทำให้สามารถส่งกุญแจรหัสลับได้ระยะทางไกลขึ้น และนอกจากนี้ทุกสัญญาณพัลส์แสงยังมีข้อมูลเกี่ยวกับกุญแจรหัสลับอยู่ ทำให้สามารถส่งกุญแจรหัสลับได้ด้วยอัตราเร็วสูงกว่า โดยระบบกระจายกุญแจรหัสลับแบบต่อเนื่องนี้เริ่มจากการทดลองในเรื่องของการส่งข่าวสารเชิงควอนตัม (Quantum Teleportation) ซึ่งเป็นการส่งข่าวจากสถานที่หนึ่งไปยังอีกสถานะที่หนึ่งด้วยคุณสมบัติทางควอนตัมของแสง เช่นการใช้คู่โฟตอนพัวพัน เมื่อโฟตอนหนึ่งของคู่โฟตอนพัวพันเดินทางมาถึงยังภาคส่ง ผู้ส่งจะใส่ข้อมูลให้กับโฟตอนนี้ ซึ่งจะทำให้โฟตอนอีกหนึ่งอนุภาคที่พัวพันกันมีข้อมูลตามที่ผู้ส่งได้ทำการส่งเข้าไป ดังนั้นหากโฟตอนนี้เดินทางมาถึงยังภาครับ ผู้รับจะทราบทันทีว่าข้อมูลที่ผู้ส่ง ส่งมานั้นคืออะไร จากหลักการนี้ A. Furusawa ได้เสนอการส่งข่าวสารเชิงควอนตัมใหม่ด้วยคุณสมบัติความเป็นโคฮีเรนต์ของแสงแทนการใช้คู่โฟตอนพัวพัน (Entangled Photon) [26] ในบทความเรื่อง "*การส่งถ่ายข่าวสารเชิงควอนตัม*" ทำให้เกิดความสนใจในเรื่องการส่งข้อมูลโดยใช้คุณสมบัติโคฮีเรนต์ของแสงเป็นสื่อกลางช่วยในการส่งกุญแจรหัสลับ ส่งผลให้เกิดรูปแบบการกระจายกุญแจรหัสลับเชิงควอนตัมรูปแบบใหม่นอกเหนือจากการใช้โฟตอนเดี่ยว เรียกว่า "การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง" และใช้ทฤษฎี No-Cloning Theorem [27] ช่วยยืนยันความปลอดภัยของระบบซึ่งจะทำให้การกระจายกุญแจรหัสลับ สามารถจะพบบุคคลที่สามเสมอหากบุคคลที่สามเข้ามาขโมยกุญแจรหัสลับระหว่างการส่งเช่นเดียวกับระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง ตัวอย่างการโพรโทคอลในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องมีดังต่อไปนี้

- **โพรโทคอล GG02**

โพรโทคอล GG02 เสนอโดย F. Grosshans และ P. Grangier [9] เป็นโพรโทคอลที่ใช้ในการส่งกุญแจรหัสลับที่กระจายแบบเกาส์ในระบบ CV-QKD โดยกุญแจรหัสลับจะแทนด้วยสถานะโคฮีเรนต์ของแสง การทำงานของโพรโทคอลนี้อาศัยโพลาไรเซชันและความเข้มของพัลส์แสงโคฮีเรนต์ทั้งแกนของแอมพลิจูด (Amplitude: A) และแกนเฟส (Phase: P) เพื่อใช้แทนกุญแจรหัสลับที่กระจายแบบเกาส์ ที่ภาครับจะใช้การตรวจจับโฟตอนแบบโฮโมไดน์ (Homodyne Detector) ซึ่งจะมีประสิทธิภาพในตัวจับโฟตอนดีกว่าอะวัลลันซ์โฟโตไดโอด (Avalanche Photodiode) [28] เพื่อใช้ตรวจจับแอมพลิจูดหรือเฟสของโคฮีเรนต์ของแสงขั้นตอนการทำงานของโพรโทคอล GG02 มีดังต่อไปนี้

ขั้นตอนที่ 1 *Alice* สร้างสถานะโคฮีเรนต์ของแสงทั้งในแนวแกนของแอมพลิจูดและมุมเฟส (Phase)ของโพลาไรเซชัน โดยจะทำการสุ่มกุญแจรหัสลับที่ต้องการส่งจากการกระจายตัวแบบเกาส์ (Gaussian Distribution) ที่ค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวน (Variance) เท่ากับ VN_0 ซึ่งโคฮีเรนต์ที่สร้างได้จะแทนด้วย $|A+iP\rangle$ โดยที่ A คือ แอมพลิจูดและ P คือ เฟสหรือ $\left|\sqrt{n}e^{j\theta}\right\rangle$ โดยที่ n คือ ความเข้มของพัลส์แสง (Intensity) และ $n>0$ หลังจากนั้น *Alice* จะทำการส่งโพลาไรเซชันนี้ไปยัง *Bob* ผ่านทางช่องทางการสื่อสารเชิงควอนตัม

ขั้นตอนที่ 2 *Bob* ทำการสุ่มแกน A หรือ P เพื่อมาใช้วัดสถานะโคฮีเรนต์ของแสงที่ส่งมาโดย *Alice* ซึ่งค่าที่รับได้จะมีทั้งค่าในแนวแกนแอมพลิจูดและแนวแกนเฟสของโพลาไรเซชันของโคฮีเรนต์ของแสง

ขั้นตอนที่ 3 *Alice* และ *Bob* ทำการตกลงเลือกแกนที่ใช้ในการส่งและรับโคฮีเรนต์แสงที่เหมือนกัน เมื่อแลกเปลี่ยนแกนแอมพลิจูด (A) หรือเฟส (P) แล้ว *Bob* และ *Alice* จะเก็บเฉพาะค่ากุญแจรหัสลับที่ใช้แกนในการรับและส่งเหมือนกันเท่านั้นและจะทิ้งค่าที่ใช้แกนในการวัดและส่งที่แตกต่างกัน ตัวอย่างการรับส่งกุญแจรหัสลับที่กระจายแบบเกาส์ด้วยโพรโทคอล GG02 กำหนดให้ A_A และ P_A เป็นแอมพลิจูดและเฟสของโคฮีเรนต์แสงที่ *Alice* สุ่มจากฟังก์ชันการกระจายโอกาสแบบเกาส์ที่ค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวนเท่ากับ VN_0 หลังจาก *Alice* ทำการสร้างสถานะโคฮีเรนต์ของแสง $|A_A+iP_A\rangle$ และส่งไปให้ยัง *Bob* ผ่านทางช่องทางการสื่อสารเชิงควอนตัมแล้ว สถานะโคฮีเรนต์ที่ *Bob* ได้รับคือ $|A_B+iP_B\rangle$ *Bob* จะทำการสุ่มวัดสถานะโคฮีเรนต์ของแสงนี้ทั้งในแกนของแอมพลิจูด (A) หรือเฟส (P) จากนั้นทั้ง *Alice* และ *Bob* จะทำการแลกเปลี่ยนแกนของแอมพลิจูดและเฟสที่ใช้ในการวัดและส่งหาก *Bob* ทำการสุ่มวัดในแกนของแอมพลิจูด ดังนั้น *Alice* จะทำการทิ้งข้อมูลในส่วนของแกนเฟส ซึ่งจะทำให้ทั้ง *Alice* และ *Bob* มีข้อมูลที่มีการกระจายแบบเกาส์ของแกนแอมพลิจูดที่ใกล้เคียงกันดังแสดงในตารางที่ 3.4

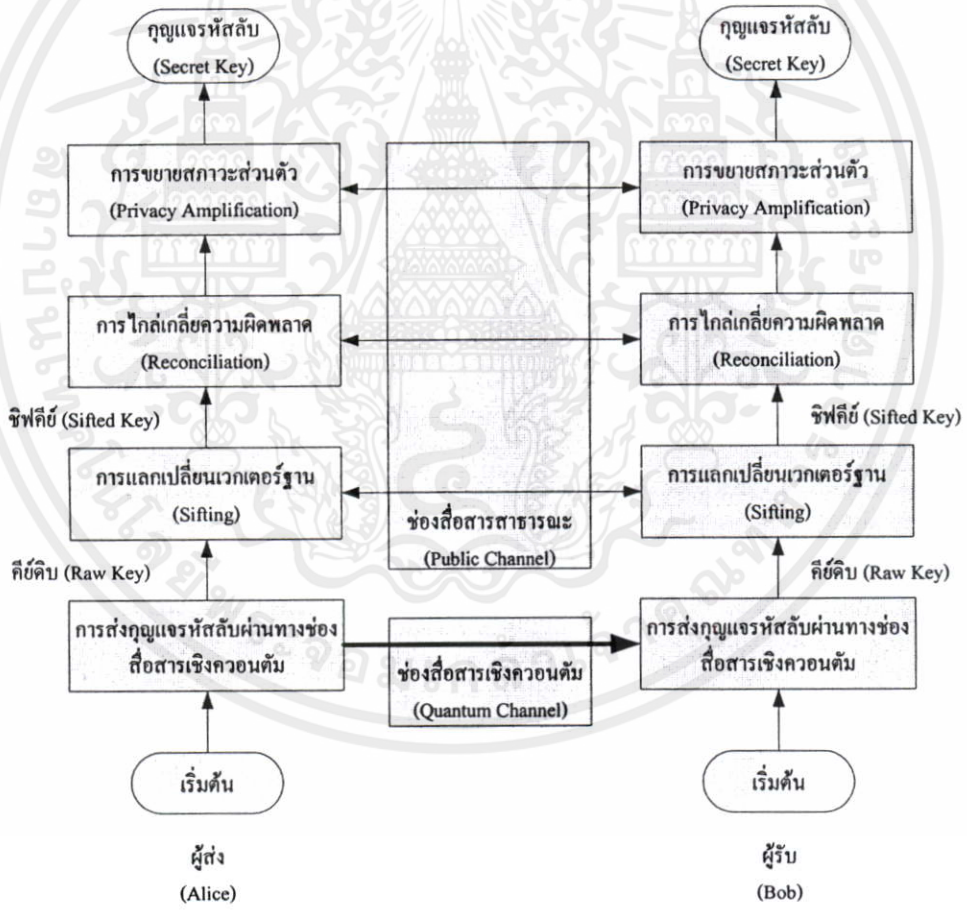
ตารางที่ 3.4 สัญลักษณ์และการส่งกุญแจรหัสลับบิตด้วยโพรโทคอล GG02

สถานะโคฮีเรนต์ของ *Alice*	$\|A_1 + P_1\rangle$	$\|A_2 + P_2\rangle$	$\|A_3 + P_3\rangle$	$\|A_4 + P_4\rangle$	$\|A_5 + P_5\rangle$
การสุ่มตรวจจับของ *Bob*	X^+	X^+	X^-	X^+	X^-
ค่ากุญแจรหัสลับที่ *Bob* ได้รับ	$A_1 + N$	$A_2 + N$	$P_3 + N$	$A_4 + N$	$P_5 + N$
ค่ากุญแจรหัสลับที่ *Alice*	A_1	A_2	P_3	A_4	P_5

โดยที่ X^+ คือการสุ่มวัดสถานะโคฮีเรนต์ของแสงในแนวแกนแอมพลิจูด

X^- คือการสุ่มวัดสถานะโคฮีเรนต์ของแสงในแนวแกนเฟส

N คือสัญญาณรบกวนภายในช่องทางการสื่อสารเชิงควอนตัม



รูปที่ 3.2 กระบวนการกระจายกุญแจรหัสลับเชิงควอนตัม

3.3 กระบวนการกลั่นกุญแจรหัสลับ

วิทยาการรหัสลับเชิงควอนตัมนอกจากจะใช้ทฤษฎีกลศาสตร์ควอนตัมมาช่วยยืนยันความปลอดภัยของระบบการส่งกุญแจรหัสลับแล้วนั้นยัง ยังใช้ทฤษฎีข่าวสารมาช่วยในกระบวนการสร้างกุญแจรหัสลับอีกด้วย โดยการนำทฤษฎีข่าวสารมาใช้ในระบบวิทยาการรหัสลับเชิงควอนตัม อันเนื่องมาจากสัญญาณรบกวนภายในช่องทางการสื่อสารเชิงควอนตัม การเข้ามารบกวนระบบของ *Eve* การลดทอนความเข้มของแสงและความไม่เป็นอุดมคติของอุปกรณ์ทั้งภาคส่งและภาครับ ล้วนเป็นสาเหตุสำคัญที่ทำให้กุญแจรหัสลับของ *Bob* เกิดความแตกต่างจากกุญแจรหัสลับของ *Alice* ดังนั้นหลักการทางทฤษฎีข่าวสารดังกล่าวจึงนำมาใช้เพื่อแก้ไขความผิดพลาดที่เกิดขึ้นนี้เพื่อให้กุญแจรหัสลับมีความผิดพลาดเหลืออยู่น้อยที่สุดและ เพื่อลดข้อมูลเกี่ยวกับกุญแจรหัสลับของ *Eve* ให้เหลือน้อยที่สุดทำให้ *Eve* ไม่สามารถนำข้อมูลส่วนนี้ไปใช้สร้างหรือทำสำเนากุญแจรหัสลับขึ้นมาใหม่ โดยกระบวนการสร้างกุญแจรหัสลับในระบบวิทยาการรหัสลับเชิงควอนตัมทั้งหมดมีขั้นตอนการทำงานดังรูปที่ 3.2 ซึ่งกุญแจรหัสลับที่ได้จะถูกนำไปใช้ในการเข้ารหัสลับและถอดรหัสลับต่อไป

3.3.1 การไกล่เกลี่ยความผิดพลาด

การไกล่เกลี่ยความผิดพลาดเป็นการแก้ไขความผิดพลาดที่เกิดขึ้นจากการส่งกุญแจรหัสลับผ่านทางช่องทางการสื่อสารเชิงควอนตัมซึ่งสัญญาณรบกวนภายในช่องทางการสื่อสารเชิงควอนตัม การเข้ามาขโมยสถานะควอนตัมของบุคคลที่สามและการลดทอนความเข้มของแสง เป็นสาเหตุทำให้สถานะควอนตัมเกิดความผิดเพี้ยนส่งผลให้กุญแจรหัสลับเกิดความผิดพลาดตามไปด้วย เพื่อทำให้กุญแจรหัสลับระหว่าง *Alice* และ *Bob* เหมือนกัน และเพื่อลดความผิดพลาดระหว่างการส่ง โดยการไกล่เกลี่ยความผิดพลาดจะแบ่งการทำงานออกเป็นสองประเภทคือ การไกล่เกลี่ยทางตรง (Direct Reconciliation) เป็นการแก้ไขกุญแจรหัสลับที่ผิดของ *Bob* ให้เหมือนกับของ *Alice* โดย *Alice* จะส่งข้อมูลเกี่ยวกับกุญแจรหัสลับของตนไปให้ยัง *Bob* ผ่านทางช่องสื่อสารสาธารณะ หรือเครือข่ายต่างๆ เพื่อให้ *Bob* แก้ไขกุญแจรหัสลับของตนให้เหมือนกับ *Alice* และ การไกล่เกลี่ยย้อนกลับ (Reverse Reconciliation) เป็นการแก้ไขกุญแจรหัสลับของ *Alice* ให้เหมือนกับกุญแจรหัสลับของ *Bob* โดย *Bob* จะส่งข้อมูลเกี่ยวกับกุญแจรหัสลับของตนไปให้ยัง *Alice* ผ่านทางช่องสื่อสารสาธารณะ หรือเครือข่ายต่างๆ เพื่อให้ *Alice* แก้ไขกุญแจรหัสลับของตนให้เหมือนกับ *Bob*

3.3.2 การขยายสภาวะส่วนตัว

การขยายสภาวะส่วนตัว (Privacy Amplification) เป็นกระบวนทำงานภายหลังจากการไกล่เกลี่ยความผิดพลาดเพื่อลดข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* มีอยู่ทำให้ *Eve* ไม่สามารถจะนำ

ข้อมูลส่วนนี้ไปสร้างหรือทำสำเนากุญแจรหัสลับใหม่ขึ้นมาได้ ซึ่งข้อมูลเกี่ยวกับกุญแจรหัสลับนี้ *Eve* ได้มาจากการเข้าไปขโมยสถานะควอนตัมจากทางช่องทางการสื่อสารเชิงควอนตัมซึ่งหาก *Eve* ทำการขโมยสถานะควอนตัมของแสงมากเกินไปจะทำให้ *Alice* และ *Bob* ทราบทันทีถึงการเข้ามาขโมยสถานะควอนตัมของ *Eve* จากอัตราความผิดพลาดของกุญแจรหัสลับที่เพิ่มมากขึ้นแต่หาก *Eve* เข้ามาขโมยสถานะควอนตัมของแสงเพียงเล็กน้อยจะทำให้ *Alice* และ *Bob* ไม่ทราบการเข้ามาขโมยของ *Eve* เนื่องจากความผิดพลาดของกุญแจรหัสลับที่เกิดขึ้นอาจจะสอดคล้องกับผลความผิดพลาดที่เกิดจากสัญญาณรบกวนภายในช่องทางการสื่อสารเชิงควอนตัมส่งผลให้ *Eve* ได้ข้อมูลส่วนหนึ่งเกี่ยวกับกุญแจรหัสลับไป นอกจากนี้ *Eve* ยังสามารถที่จะเข้ามาขโมยข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Alice* และ *Bob* เปิดเผยระหว่างกระบวนการไกล่เกลี่ยความผิดพลาดทำให้ *Eve* ได้รับข้อมูลเกี่ยวกับกุญแจรหัสลับเพิ่มมากขึ้น หาก *Eve* ได้ข้อมูลเกี่ยวกับกุญแจรหัสลับไปมาก *Eve* อาจจะสามารถสร้างกุญแจรหัสลับใหม่ขึ้นมาได้ การขยายสภาวะส่วนตัวจึงถูกนำมาใช้งานเพื่อลดความสำคัญของข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* มีอยู่ ซึ่งจะทำให้ *Eve* ไม่สามารถสร้างกุญแจรหัสลับใหม่ขึ้นมาได้เช่น การนำกุญแจรหัสลับบิตที่ติดกันสองตำแหน่งมารวมกันแบบมอดุโล 2 (Modulo 2) เนื่องจากข้อมูลที่ *Eve* มีอยู่นั้นจะเป็นข้อมูลที่ขาดหายไปบางส่วนเช่น หากนำบิตตำแหน่งที่หนึ่งและตำแหน่งที่สองมามอดุโล 2 จะได้ผลลัพธ์เป็นกุญแจรหัสลับบิตใหม่ขนาดหนึ่งบิตถ้าหากว่า *Eve* มีข้อมูลเพียงบิตตำแหน่งที่สองเท่านั้นกุญแจรหัสลับบิตที่ *Eve* จะได้หลังจากกระบวนการนี้จะมีความน่าจะเป็นระหว่างบิต “1” และบิต “0” อย่างละ 50% ดังนั้นกุญแจรหัสลับบิตที่ *Eve* สามารถสร้างได้จะมีโอกาสเป็นกุญแจรหัสลับบิตที่ผิดค่อนข้างสูง

3.4 การประยุกต์ระบบวิทยาการรหัสลับเชิงควอนตัม

วิทยาการรหัสลับเชิงควอนตัมเป็นการนำทฤษฎีข่าวสารเชิงควอนตัม (Quantum Information Theory) มาประยุกต์ใช้งานจริงได้เป็นระบบแรกด้วยเทคโนโลยีที่มีอยู่ในปัจจุบัน ซึ่งแนวความคิดเริ่มมาจาก โพรโทคอลBB84 ที่เสนอโดย C.H. Bennett และ G. Brassard [1] หลังจากนั้นอีกแปดปี C.H. Bennett และคณะ นำระบบวิทยาการรหัสลับเชิงควอนตัมเป็นระบบแรกในปี ค.ศ. 1992 สามารถส่งกุญแจรหัสลับได้อัตราเร็ว 10 bps [2] ซึ่งหลังจากนั้นระบบวิทยาการรหัสลับเชิงควอนตัม กลายเป็นที่สนใจสำหรับนักวิจัยที่จะพัฒนาระบบให้สามารถส่งกุญแจรหัสลับได้ระยะทางไกลยิ่งขึ้นและสามารถส่งกุญแจรหัสลับด้วยอัตราเร็วในการส่งสูง ซึ่งการประยุกต์ใช้งานวิทยาการรหัสลับเชิงควอนตัมในปัจจุบันมีตัวอย่างดังต่อไปนี้

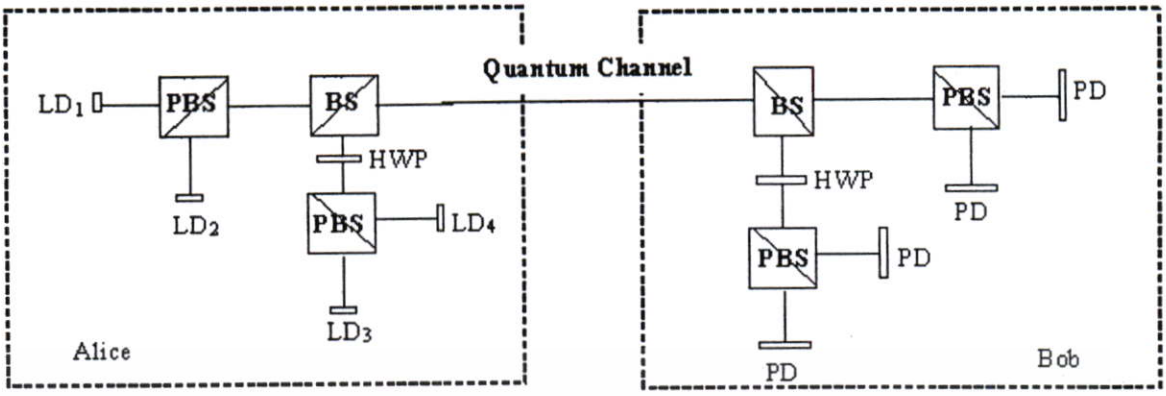
3.4.1 การประยุกต์ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง

ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องเป็นการประยุกต์การส่งกุญแจรหัสลับด้วยโพรโทคอลต่างๆ เช่น โพรโทคอลBB84 โพรโทคอลB92 หรือ โพรโทคอลEkert91

เป็นต้น เพื่อนำกระบวนการส่งกุญแจรหัสลับนี้มาสร้างระบบขึ้นเพื่อใช้งานจริง ซึ่งปัจจุบันมีการพัฒนาวิธีการเพื่อสร้างระบบวิทยาการรหัสลับเชิงควอนตัมให้สามารถส่งกุญแจรหัสลับได้ระยะทางไกล และให้ระบบมีความผิดพลาดระหว่างการส่งน้อย ซึ่งระบบวิทยาการรหัสลับเชิงควอนตัมในปัจจุบันมีการทำงานในหลากหลายวิธีการด้วยกัน โดยในที่นี้จะกล่าวถึงรูปแบบการนำโพรโทคอลBB84 มาประยุกต์ใช้งานเพื่อส่งกุญแจรหัสลับบิตผ่านช่องทางการสื่อสารเชิงควอนตัมเช่น อากาศ (Free Space) หรือ เส้นใยนำแสง (Optical Fiber) ดังรายละเอียดดังต่อไปนี้

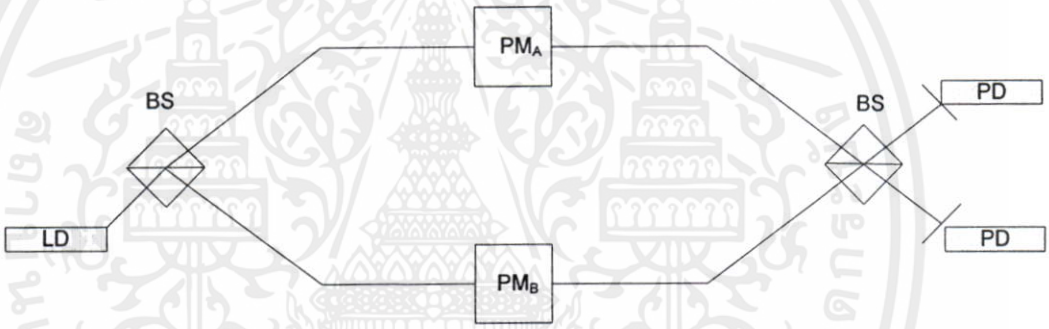
3.4.1.1 การส่งกุญแจรหัสลับบิตด้วยโพลาไรเซชันของโฟตอนเดี่ยว

การนำโพลาไรเซชันของโฟตอนเดี่ยวมาใช้แทนกุญแจรหัสลับบิตเป็นรูปแบบการแทนกุญแจรหัสลับบิตที่นำมาประยุกต์สร้างระบบวิทยาการรหัสลับเชิงควอนตัมอย่างแพร่หลายเช่น ระบบวิทยาการรหัสลับเชิงควอนตัมที่ C. H. Bennett และ G. Brassard เสนอในปี 1992 [2] ซึ่งเป็นระบบวิทยาการรหัสลับเชิงควอนตัมระบบแรกโดยการแทนกุญแจรหัสลับบิตใช้สถานะโพลาไรเซชันทั้งสิ้นสี่สถานะประกอบไปด้วย โพลาไรเซชัน“0” องศา (→)โพลาไรเซชัน “90” องศา (↑) โพลาไรเซชัน “45” องศา (↗)โพลาไรเซชัน “-45” องศา (↘) โดยโพลาไรเซชันของโฟตอนเดี่ยวในระบบนี้สร้างจากไดโอดเปล่งแสงหรือแอลอีดี (Light Emitting Diode: LED) โดยผ่านแสงที่ได้เข้าสู่ตัวลดทอนความเข้มของแสงเพื่อสร้างโฟตอนเดี่ยว จากนั้นจะเลือกโพลาไรเซชันของโฟตอนเดี่ยวที่ต้องการส่งด้วย Pocket Cell โดยเปลี่ยนระดับแรงดันไฟฟ้าตามกุญแจรหัสลับที่ได้จากการสุ่มจากแหล่งกำเนิดจำนวนสุ่มเชิงควอนตัม (Quantum Random Number Generator: QRNG) เป็นต้น ปัจจุบันระบบวิทยาการรหัสลับเชิงควอนตัมที่นำโพลาไรเซชันของโฟตอนเดี่ยวมาใช้ในการส่งกุญแจรหัสลับจะสร้างจากแหล่งกำเนิดแสงเลเซอร์ไดโอด (Laser Diode: LD) สี่ชุดซึ่งแต่ละชุดจะสร้างโพลาไรเซชันของโฟตอนเดี่ยวในมุมที่แตกต่างกันไป โดยลำแสงโพลาไรเซชันที่ตั้งฉากซึ่งกันและกันเช่น โพลาไรเซชัน .0” องศา และโพลาไรเซชัน “90” องศา หรือโพลาไรเซชัน “45” องศา และโพลาไรเซชัน “-45” องศา จะถูกรวมเข้าด้วยกันด้วยกระจกแยกลำแสงโพลาไรเซชัน (Polarization Beam Splitter: PBS) ก่อนลำแสงทั้งหมดจะรวมเข้าด้วยกันโดยใช้กระจกแยกลำแสง (Beam Splitter: BS) และส่งผ่านช่องทางการสื่อสารเชิงควอนตัมไปยังภาครับหรือ *Bob* ดังรูปที่ 3.3 [29] ส่วนทางภาครับจะใช้กระจกแยกลำแสง (BS) เพื่อทำการสุ่มเวกเตอร์ฐานขึ้นมาเพื่อใช้รับโพลาไรเซชันของโฟตอนเดี่ยว โดยแสงที่ผ่านกระจกแยกลำแสงจะเดินทางเข้าสู่ตัวตรวจจับแสงตามโพลาไรเซชัน ซึ่งโพลาไรเซชัน “0” องศา และโพลาไรเซชัน “90” องศา จะเดินทางเข้าสู่ตัวตรวจจับ (Detector)โดยอาศัยกระจกแยกลำแสงโพลาไรเซชัน (PBS) ในการตรวจจับลำแสงแสงโพลาไรเซชัน “45” องศาและ “-45” องศา อาศัย Haft-Wave Plate (HWP) เพื่อเปลี่ยนโพลาไรเซชันมุม “45” องศาและ “-45” องศา เป็นโพลาไรเซชัน “0” และ “90” องศา ก่อนเข้าสู่ตัวตรวจจับแสงดังรูปที่ 3.3 ข้อดีของการประยุกต์วิทยาการรหัสลับเชิงควอนตัมด้วยวิธีนี้คือ กรจัดเรียงอุปกรณ์ทางแสงทำได้ง่าย ระบบไม่มีความซับซ้อน



LD คือแหล่งกำเนิดแสงเลเซอร์ PBS คือกระจกแยกลำแสงโพลาไรเซชัน BS คือกระจกแยกลำแสง PD คือตัวตรวจจับแสงและ HWP คือ Haft Wave Plate

รูปที่ 3.3 โครงสร้างพื้นฐานระบบวิทยาการรหัสลับเชิงควอนตัมใช้สถานะโพลาไรเซชัน [29]



PM คืออุปกรณ์สัญญาณทางเฟส BS คือกระจกแยกลำแสงโพลาไรเซชัน LD คือแหล่งกำเนิดแสงเลเซอร์และ PD คือตัวตรวจจับแสง

รูปที่ 3.4 พื้นฐานระบบวิทยาการรหัสลับเชิงควอนตัมใช้ Mach-Zehnder Interferometer [30]

ข้อเสียของระบบนี้คือในกรณีของการส่งโพลาไรเซชันของโฟตอนเดี่ยวผ่านเส้นใยนำแสง (Optical Fiber) ภาครับจะต้องอาศัยอุปกรณ์บางอย่างเช่น ตัวควบคุมโพลาไรเซชัน (Polarization Control) เพื่อชดเชยหรือป้องกันโพลาไรเซชันของโฟตอนเดี่ยวที่จะเปลี่ยนแปลงอันเนื่องมาจากการสะท้อนของแสงภายในเส้นใยนำแสงและการที่อุณหภูมิภายในเส้นใยนำแสงเกิดการเปลี่ยนแปลงจะมีผลทำให้โพลาไรเซชันของโฟตอนเดี่ยวเกิดการเปลี่ยนแปลงตามไปด้วยเช่นกัน ในกรณีของการส่งโพลาไรเซชันของโฟตอนเดี่ยวผ่านอากาศ โพลาไรเซชันของโฟตอนเดี่ยวที่ส่งจะไม่เกิดการเปลี่ยนแปลงดังเช่นที่เกิดขึ้นภายในเส้นใยนำแสง แต่แสงจากภายนอกโดยเฉพาะแสงจากดวงอาทิตย์ในเวลากลางวันและแสงจากหลอดไฟฟ้า แสงจากดวงจันทร์ในเวลากลางคืนเป็นสาเหตุหลักที่เข้ามา

รบกวนระบบซึ่งอาจจะทำให้ภาครับได้รับข้อมูลที่ผิดพลาด ดังนั้นระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้โพลาไรเซชันของโฟตอนเดี่ยวผ่านอากาศจึงต้องใช้อุปกรณ์ตรวจจับที่อยู่ในช่วงของความยาวคลื่นแสงเฉพาะ ใช้อุปกรณ์เพื่อกรองแสงจากภายนอก เช่น Spatial Filter เป็นต้น และใช้อุปกรณ์ตรวจจับโฟตอนเดี่ยวที่ทำงานในช่วงเวลาที่จำกัด เพื่อตรวจจับแสงในแต่ละพัลส์แสงลดผลกระทบของแสงจากภายนอกไม่ให้เข้ามารบกวนระบบทำให้ระบบลดความผิดพลาดระว่างการรับส่งกุญแจรหัสลับลงได้

3.4.1.2 การส่งกุญแจรหัสลับบิตด้วยเฟสของโพลาไรเซชัน

นอกจากโพลาไรเซชันของโฟตอนเดี่ยวที่ใช้ในการแทนกุญแจรหัสลับบิตแล้วเฟสของโพลาไรเซชันของโฟตอนเดี่ยวยังถูกนำมาใช้เพื่อส่งกุญแจรหัสลับบิตเช่นเดียวกับโพลาไรเซชันของโฟตอนเดี่ยว โดยการสร้างเฟสของโพลาไรเซชันของโฟตอนเดี่ยวในวิทยาการรหัสลับเชิงควอนตัมปัจจุบันนั้นสร้างจาก Mach-Zehnder Interferometer ซึ่งแบ่งออกเป็นสองระบบย่อยคือ ระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้ Mach-Zehnder Interferometer และระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้ระบบ Plug and Play เพื่อส่งกุญแจรหัสลับดังรายละเอียดดังต่อไปนี้

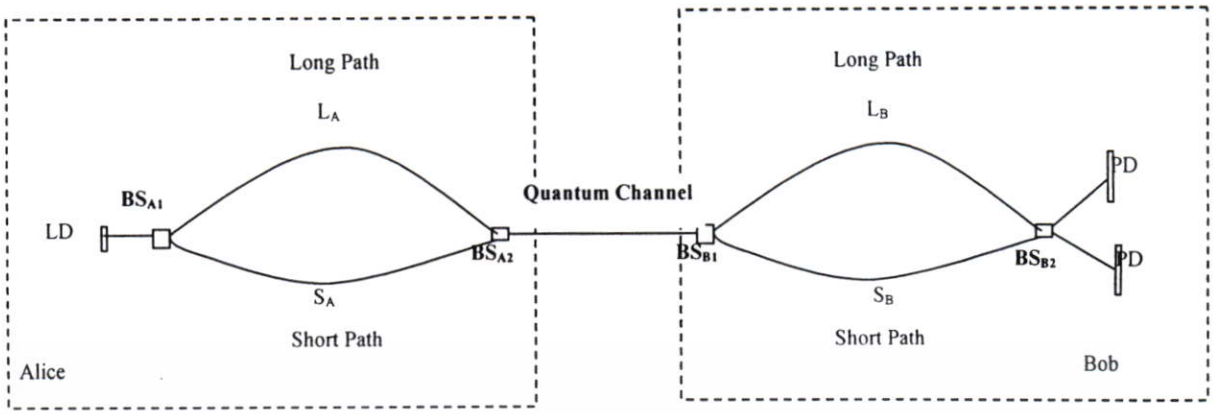
- **การส่งกุญแจรหัสลับด้วย Mach-Zehnder interferometer**

การใช้ Mach-Zehnder Interferometer เพื่อส่งกุญแจรหัสลับในวิทยาการรหัสลับเชิงควอนตัมเป็นการแทนกุญแจรหัสลับด้วยเฟสของโพลาไรเซชันของโฟตอนเดี่ยวซึ่งสร้างโดยการแทรกสอดของโพลาไรเซชันของแสงภายในพัลส์แสงที่เดินทางภายใน Mach-Zehnder Interferometer ทั้งทางภาคส่งและภาครับดังรูปที่ 3.4 ระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้ Mach-Zehnder Interferometer นี้ โพลาไรเซชันของโฟตอนเดี่ยวที่ภาคส่งจะสร้างจากแหล่งกำเนิดเลเซอร์ไดโอด (LD) จากนั้นพัลส์แสงจะผ่านเข้าสู่กระจกแยกลำแสง (BS) เพื่อแยกลำแสงออกเป็นสองเส้นทาง โดยเส้นทางด้านบนของ Mach-Zehnder Interferometer โพลาไรเซชันของโฟตอนเดี่ยวจะถูกเปลี่ยนเฟสโดยใช้ Polarization Modulator: PM_Aของ *Alice* และเส้นทางด้านล่างของ Mach-Zehnder Interferometer เฟสของโพลาไรเซชัน "0" เรเดียน หรือ "π" เรเดียน (Radian) จะถูกสุ่มขึ้นเพื่อเลือกรับเฟสของโพลาไรเซชันที่ส่งมาโดย *Alice* โดยใช้ Polarization Modulator: PM_B ของ *Bob* ก่อนที่เฟสของโพลาไรเซชันของแสงทั้งสองจะมาแทรกสอดกันที่กระจกแยกลำแสง (BS) และเข้าสู่ตัวตรวจจับ (PD) ค่าไบนารีหรือกุญแจรหัสลับบิตที่ *Bob* ได้รับจะขึ้นอยู่กับความต่างเฟสระหว่างโพลาไรเซชันของ *Alice* และ *Bob* [30] ดังสมการ

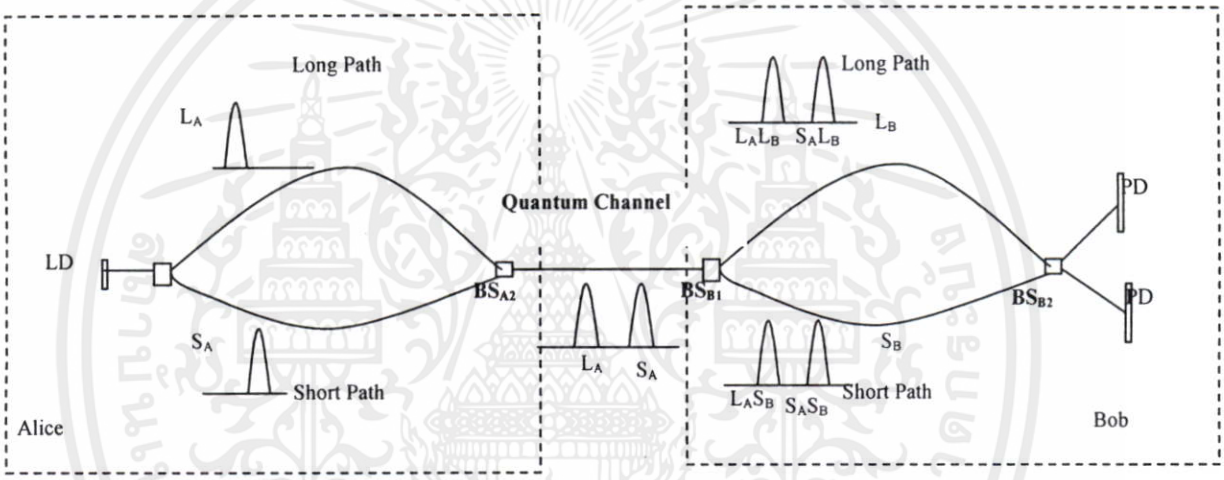
$$\theta = \theta_A - \theta_B \tag{3.1}$$

θ_A เฟสที่ *Alice* ทำการส่งและ θ_B คือเฟสที่ *Bob* ใช้ในการวัดเฟสของโพลาไรเซชัน

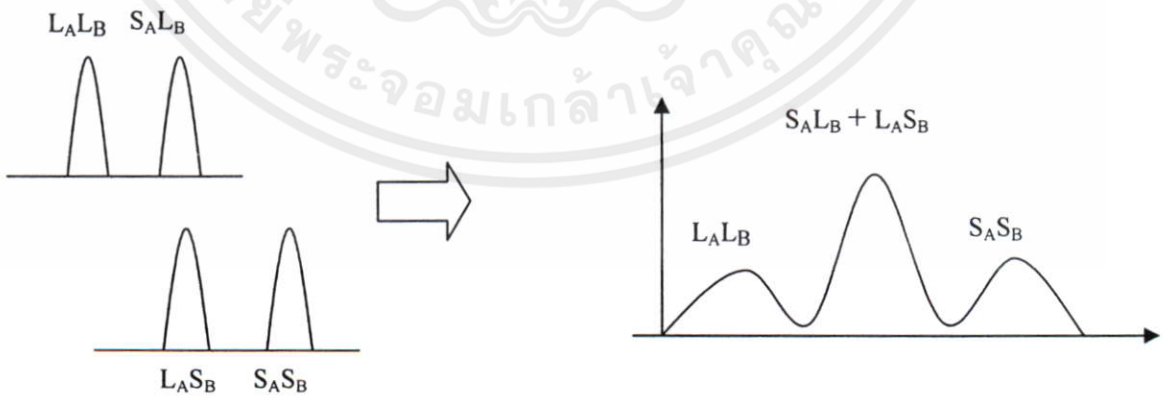
โดยเฟสที่ *Alice* ใช้ส่งจะประกอบด้วยสี่เฟสดังนี้ เฟส "0" เรเดียน เฟส "$\frac{\pi}{2}$" เรเดียน เฟส "π" เรเดียน และเฟส "$\frac{3\pi}{2}$" เรเดียน เฟสเหล่านี้จะตรงกับโพลาไรเซชันของโฟตอนเดี่ยวที่ใช้ส่งกุญแจรหัสลับบิตตามโพรโทคอล BB84 ดังตารางที่ 3.2 และการส่งกุญแจรหัสลับบิตด้วยเฟสของโพลาไรเซชันของโฟตอนเดี่ยวตามรูปแบบโพรโทคอลBB84 ดังตารางที่ 3.3 รูปแบบการส่งกุญแจรหัสลับบิตด้วยเฟสของโพลาไรเซชันของโฟตอนเดี่ยวส่วนใหญ่จะนำไปใช้ในการประยุกต์การส่งกุญแจรหัสลับบิตผ่านเส้นใยนำแสง เนื่องจากการสะท้อนของแสงภายในเส้นใยนำแสงจะทำให้โพลาไรเซชันของแสงเกิดการเปลี่ยนแปลงและควบคุมได้ยาก ดังนั้นการส่งกุญแจรหัสลับบิตผ่านเส้นใยนำแสงส่วนใหญ่จึงอาศัยเฟสของโพลาไรเซชันแทนกุญแจรหัสลับบิตที่ต้องการส่ง ถ้าระบบกระจายกุญแจรหัสลับเชิงควอนตัมใช้ Mach-Zehnder Interferometer เพียงชุดเดียว เพื่อใช้ทั้งการส่งและรับกุญแจรหัสลับบิตดังรูป 3.4 ระบบจะยังคงประสบปัญหาหลายอย่างเช่น ความยาวของเส้นใยนำแสงที่ผิดพลาดเพียงเล็กน้อยจะทำให้เฟสของโพลาไรเซชันเกิดการเปลี่ยนแปลงทำให้การส่งเกิดความผิดพลาดตามมา [30] ดังนั้นการที่จะป้องกันปัญหาที่เกิดขึ้นเหล่านี้ระบบวิทยาการรหัสลับเชิงควอนตัมส่วนใหญ่จะใช้ Mach-Zehnder Interferometer สองชุดในการสร้างเฟสของโพลาไรเซชันของแสงซึ่ง Mach-Zehnder Interferometer ชุดแรกจะอยู่ที่ทาง *Alice* และ Mach-Zehnder Interferometer ชุดที่สองจะอยู่ทาง *Bob* ซึ่ง Mach-Zehnder Interferometer ทั้งสองชุดนี้จะเหมือนกันทุกอย่าง ทั้งความยาวของเส้นใยนำแสงภายใน Mach-Zehnder Interferometer และส่วนประกอบอื่นๆ เพื่อให้การส่งและรับเฟสของโพลาไรเซชันมีความถูกต้องที่สุด [30][3] การทำงานระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้ Mach-Zehnder Interferometer ทั้งสองชุดเพื่อสร้างเฟสของโพลาไรเซชันของโฟตอนเดี่ยวที่ใช้แทนกุญแจรหัสลับนี้ มีการทำงานดังรูปที่ 3.5 รูปที่ 3.6 แสดงการเดินทางของสัญญาณพัลส์แสงภายใน Mach-Zehnder Interferometer ทั้งของ *Alice* และ ของ *Bob* โดยพัลส์แสงที่ออกจากเลเซอร์ไดโอด (LD) ของ *Alice* จะถูกแยกออกเป็นสองเส้นทางโดยกระจกแยกลำแสง (BS_{A1}) จากนั้นพัลส์แสงจะเดินทางไปตามเส้นทางที่ยาวกว่าภายใน Mach-Zehnder Interferometer จะเรียกว่า "L_A" และพัลส์แสงที่เดินทางตามเส้นทางที่สั้นกว่าจะเรียกว่า "S_A" โดยพัลส์แสงทั้งสองจะเดินทางผ่านช่องสื่อสารเชิงควอนตัมไปยัง *Bob* โดยพัลส์แสง S_A จะเดินทางนำหน้าพัลส์แสง L_A เพียงเล็กน้อยเนื่องจากระยะทางเดินทางของแสงที่ไม่เท่ากันภายใน Mach-Zehnder Interferometer จากนั้นเมื่อพัลส์แสงทั้งสองเดินทางมาถึงยัง *Bob* พัลส์แสงทั้งสองจะถูกแยกอีกครั้งโดยกระจกแยกลำแสง (BS_{B1}) ซึ่งจะแยกตามเส้นทางภายใน Mach-Zehnder Interferometer โดยพัลส์แสง S_AL_B และ L_AL_B จะเป็นพัลส์แสงที่เดินทางตามเส้นทางที่ยาวกว่าภายใน Mach-Zehnder Interferometer ของ *Bob* และพัลส์แสง S_AS_B และ L_AS_B จะเป็นพัลส์แสงที่เดินทางตามเส้นทางที่สั้นกว่าภายใน Mach-Zehnder Interferometer และจากนั้นพัลส์แสงทั้งหมดจะรวมเข้าด้วยกันอีกครั้งด้วยกระจกแยกลำแสงโพลาไรเซชัน (BS_{B2}) โดยพัลส์แสง S_AL_B



รูปที่ 3.5 ระบบวิทยาการรหัสลับเชิงควอนตัมใช้ Mach-Zehnder Interferometer สองระบบ [3]



รูปที่ 3.6 ลักษณะสัญญาณพัลส์ที่ภายใน Mach-Zehnder Interferometer [3]

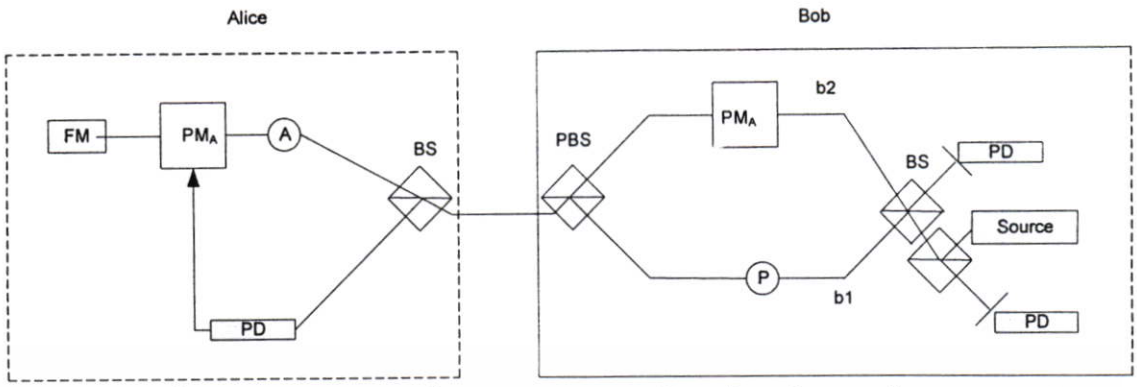


รูปที่ 3.7 การรวมกันของสัญญาณพัลส์ก่อนถึงตัวตรวจจับที่ *Bob* [3]

พัลส์แสง L_AS_B จะถูกรวมเข้าด้วยกันซึ่งการแทรกสอดของทั้งสองพัลส์แสงนี้จะให้ข้อมูลเกี่ยวกับกุญแจรหัสลับแก่ *Bob* ในส่วนพัลส์แสงที่ไม่ได้เกิดการแทรกสอดทั้งพัลส์แสง S_AS_B และ L_AL_A จะไม่มีข้อมูลเกี่ยวกับกุญแจรหัสลับ รูปที่ 3.7 แสดงการแทรกสอดของสัญญาณพัลส์แสงที่ Mach-Zehnder Interferometer ของ *Bob* ที่เกิดขึ้นภายในกระจกแยกลำแสง BS_{B2} ซึ่งเฟสที่แทรกสอดจะอยู่ภายในสัญญาณพัลส์แสงกลาง

- **ระบบวิทยาการรหัสลับเชิงควอนตัมแบบปรับเปลี่ยนเฟสอัตโนมัติ**

ระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้เฟสของโพลาไรเซชันของโฟตอนเดี่ยวนอกจากระบบที่ใช้ Mach-Zehnder Interferometer เพื่อส่งกุญแจรหัสลับแล้วระบบวิทยาการรหัสลับเชิงควอนตัมแบบปรับเปลี่ยนเฟสอัตโนมัติ ซึ่งทางคณะวิจัยจากมหาวิทยาลัยเจนิวา ประเทศสวิตเซอร์แลนด์ได้นำเสนอระบบวิทยาการรหัสลับในรูปแบบปรับเปลี่ยนเฟสอัตโนมัติ โดยสามารถส่งได้ไกล 23 กิโลเมตรผ่านเส้นใยนำแสง [31] เป็นอีกหนึ่งระบบที่ใช้เฟสของโพลาไรเซชันของโฟตอนเดี่ยวเพื่อส่งกุญแจรหัสลับ แต่ระบบนี้แตกต่างจากการระบบที่ใช้ Mach-Zehnder Interferometer คือระบบนี้จะทำการปรับเปลี่ยนเฟสที่เปลี่ยนแปลงจากการส่งอัตโนมัติ เนื่องจากการส่งเฟสของโพลาไรเซชันอาจจะมีการเปลี่ยนแปลงระบบนี้จะทำปรับเปลี่ยนเฟสอัตโนมัติเพื่อให้เฟสที่ส่งมีความถูกต้อง โดยแหล่งกำเนิดแสงจะอยู่ที่ภาครับหรือ *Bob* หาก *Bob* ทำการส่งเฟสของโพลาไรเซชันที่แน่นอนมายังภาคส่งหรือ *Alice* จะทำให้ *Alice* ทราบทันที่ถึงความผิดเพี้ยนที่เกิดขึ้นกับเฟสโพลาไรเซชันที่ *Bob* ส่งมาและจะทำการชดเชยเฟสของโพลาไรเซชันนั้นเพื่อให้เฟสของโพลาไรเซชันที่กลับไปถึง *Bob* มีความถูกต้องโดยการทำงานของระบบวิทยาการรหัสลับเชิงควอนตัมแบบปรับเปลี่ยนเฟสอัตโนมัติแสดงได้ดังรูปที่ 3.8 ซึ่ง *Bob* จะสร้างสัญญาณพัลส์แสงความเข้มแสงสูงก่อนส่งผ่านเข้าสู่ Mach-Zehnder Interferometer ไปยัง *Alice* โดยจากรูปสัญญาณพัลส์ที่สร้างขึ้นจะแยกออกเป็นสองเส้นทางด้วยกระจกแยกลำแสง (BS) ที่ติดอยู่ที่ Mach-Zehnder Interferometer โดยสัญญาณพัลส์แสง b2 จะเคลื่อนที่เข้าสู่เส้นทางด้านบนของ Mach-Zehnder Interferometer ณ เวลานี้อุปกรณ์เปลี่ยนเฟสของโพลาไรเซชัน (Phase Modulator) จะยังไม่ทำงาน ดังนั้นสัญญาณพัลส์ b2 จะยังไม่มีข้อมูลหรือกุญแจรหัสลับอยู่ภายในพัลส์แสงส่วนสัญญาณพัลส์แสง b1 จะเคลื่อนเข้าสู่เส้นทางด้านล่างของ Mach-Zehnder Interferometer ซึ่งจะมีการปรับโพลาไรเซชันเป็น 90 องศาโดยอาศัย Polarizer (P) ก่อนพัลส์แสงทั้งสองจะเคลื่อนที่เข้าสู่กระจกแยกลำแสงโพลาไรเซชัน (PBS) และเดินทางเข้าสู่ช่องทางการสื่อสารเชิงควอนตัมต่อไป (พัลส์แสง b1 นี้จะเคลื่อนที่นำหน้าพัลส์แสง b2 เล็กน้อยเนื่องจากระยะทาง b1 ภายใน Mach-Zehnder Interferometer จะสั้นกว่า b2) เมื่อสัญญาณพัลส์ตามเส้นทาง b1 เคลื่อนที่มาถึง *Alice* สัญญาณพัลส์แสงจะแยกเป็นสองสัญญาณพัลส์โดยกระจกแยกลำแสง (BS) และสัญญาณพัลส์ b1 ที่เคลื่อนที่ไปยังเส้นทางด้านบนของ Mach-Zehnder Interferometer ของ *Alice* จะเคลื่อนผ่านอุปกรณ์ Phase Modulator เพื่อให้เตรียมพร้อมที่จะทำงานเพื่อแทนกุญแจรหัสลับบิตจากนั้นพัลส์แสงจะเคลื่อนที่เข้าสู่



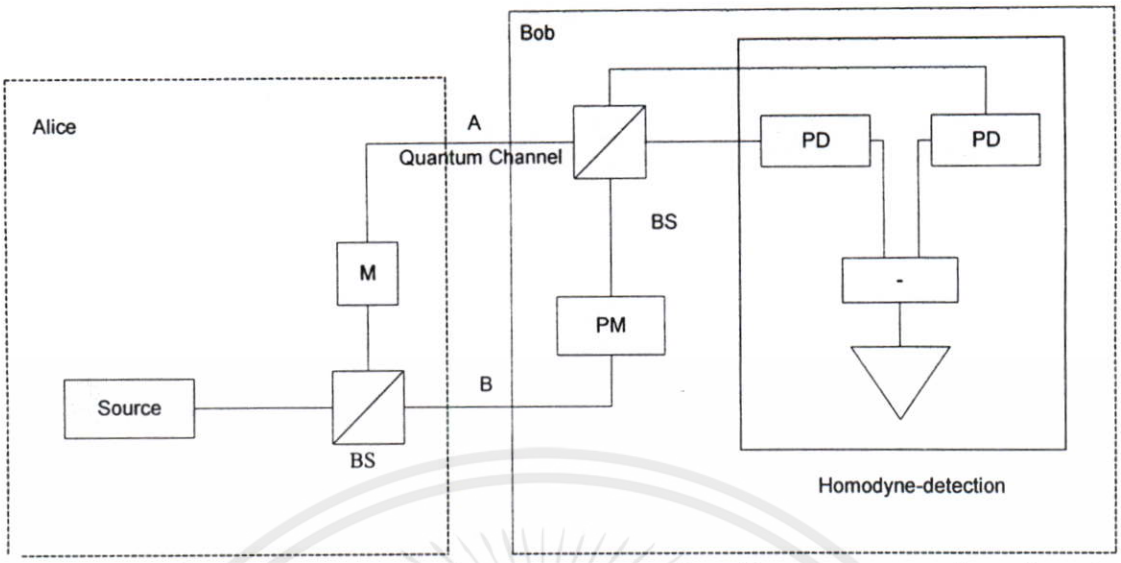
PM คืออุปกรณ์สัญญาณทางเฟส BS คือกระจกแยกลำแสงโพลาไรเซชัน PBS คือกระจกแยกลำแสงโพลาไรเซชัน Source คือแหล่งกำเนิดแสงเลเซอร์ PD คือตัวตรวจจับแสงและ P คือ Polarizer

รูปที่ 3.8 พื้นฐานระบบวิทยาการรหัสลับเชิงควอนตัมแบบแบบปรับเปลี่ยนเฟสอัตโนมัติ [32]

Faraday Mirror (FM) เพื่อปรับมุมโพลาไรเซชันเพิ่มขึ้น 90 องศา และสะท้อนกลับไปยังช่องทางการสื่อสารเชิงควอนตัม ในส่วนสัญญาณพัลส์ตามเส้นทาง b1 ที่เคลื่อนที่ลงด้านล่างสัญญาณพัลส์จะเคลื่อนเข้าสู่ตัวตรวจจับแสง (Photo Diode: PD) เพื่อให้เตรียมความพร้อมที่จะรับสัญญาณพัลส์จากเส้นทาง b2 เมื่อสัญญาณพัลส์จากเส้นทาง b2 เคลื่อนที่มาถึงพัลส์แสงจะแยกเป็นสองเส้นทางโดยเส้นทางด้านบนจะถูกเปลี่ยนเฟสตามที่ *Alice* ได้เลือก (θ_A) และพัลส์แสงนี้จะถูกลดทอนความเข้มเพื่อสร้างโฟตอนเดี่ยว (Single Photon) ก่อนสะท้อนกลับเข้าสู่ช่องทางการสื่อสารเชิงควอนตัม ในส่วนพัลส์แสงที่เคลื่อนที่ลงด้านล่างจะถูกตรวจจับโดยตัวตรวจจับแสงทำให้สัญญาณนี้จะกลายเป็นสัญญาณ Synchronize ระหว่าง *Alice* และ *Bob* เมื่อสัญญาณพัลส์ทั้งสองเคลื่อนที่มาถึงยัง *Bob* สัญญาณพัลส์จะถูกแยกโดยกระจกแยกลำแสงโพลาไรเซชัน (PBS) สัญญาณ b1 จะเคลื่อนที่ขึ้นด้านบนเนื่องจากสถานะโพลาไรเซชันที่ถูกเปลี่ยนโดย Faraday Mirror (FM) ที่ *Alice* และพัลส์นี้จะถูกเปลี่ยนเฟสโดย *Bob* (θ_B) และสัญญาณพัลส์ b2 จะเคลื่อนที่ลงด้านล่าง จากนั้นพัลส์แสงทั้งสองจะเข้ารวมกันที่กระจกแยกลำแสง (BS) ก่อนที่จะตรวจจับการเปลี่ยนเฟสที่ตัวตรวจจับ (PD) ของ *Bob* [30] [32]

3.4.2 การประยุกต์ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง

ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง เป็นวิทยาการรหัสลับเชิงควอนตัมรูปแบบใหม่ที่พัฒนาขึ้นนอกเหนือจากการใช้โฟตอนเดี่ยวในการส่งกุญแจรหัสลับ โดยการประยุกต์วิทยาการรหัสลับในรูปแบบนี้เป็นครั้งแรกโดย F. Grosshans และคณะ ได้นำเสนอการประยุกต์การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง ซึ่งเป็นการนำโพรโทคอล GG02 มาประยุกต์ใช้งาน โดยสามารถส่งกุญแจรหัสลับได้ในอัตราเร็ว 75 kbps



PM คืออุปกรณ์สัญญาณทางเฟส BS คือกระจกแยกลำแสงโพลาไรเซชัน Source คือแหล่งกำเนิดแสงเลเซอร์ PD คือตัวตรวจจับแสงและ M คืออุปกรณ์ผสมสัญญาณทางเฟสและแอมพลิจูด

รูปที่ 3.9 พื้นฐานระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องด้วยโคฮีเรนต์ของแสง [9]

ผ่านเส้นใยนำแสงที่มีการสูญเสีย (Loss) 3.1 dB และอัตราเร็ว 1.7 Mbps ผ่านเส้นใยนำแสงที่ไม่มีการสูญเสีย [9] โดยการทำงานของระบบแสดงดังรูป 3.9 จากรูป *Alice* จะทำการสร้างสถานะโคฮีเรนต์ของแสงความเข้มสูง โดยสถานะโคฮีเรนต์นี้จะถูกส่งผ่านกระจกแยกลำแสง (Beam Splitter: BS) ที่มีอัตราในการแยกลำแสงที่ไม่เท่ากันโดยเส้นทางของแสงความเข้มน้อย (เส้นทาง "A") จะทำการส่งกุญแจรหัสลับไปพร้อมกับสัญญาณพัลส์แสงนี้ ซึ่งกุญแจรหัสลับนี้จะถูกแทนด้วยแอมพลิจูดและเฟสของโคฮีเรนต์ของแสงที่ได้จากการสุ่มจากการกระจายแบบเกาส์ โดยใช้อุปกรณ์ผสมสัญญาณ (Modulator: M) ซึ่งจะเรียกสัญญาณพัลส์แสงที่ใช้ในการส่งกุญแจรหัสลับนี้ว่า "Signal" จากนั้นสัญญาณพัลส์แสง "Signal" จะถูกส่งเข้าสู่ช่องทางการสื่อสารเชิงควอนตัม (Quantum Channel) เพื่อไปยังภาครับต่อไปต่อไป ในส่วนของสัญญาณพัลส์แสงความเข้มสูงที่ได้จากกระจกแยกลำแสงตามเส้นทาง "B" ซึ่งพัลส์แสงนี้จะมีความเข้มสูงกว่าพัลส์แสง "Signal" มาก โดยจะเรียกว่าพัลส์แสงนี้ว่า "Local Oscillator: LO" โดยพัลส์แสง "Local Oscillator" นี้จะถูกส่งมายัง *Bob* ผ่านเส้นทางอีกหนึ่งเส้นทางหนึ่งนอกจากช่องทางการสื่อสารเชิงควอนตัม โดยอาจจะเป็นเส้นใยนำแสง (Fiber Optic) หรืออากาศ (Free Space) เพื่อใช้เป็นสัญญาณการอ้างอิงเฟสของโคฮีเรนต์ของแสงของพัลส์แสง "Signal" ให้แก่ *Bob* เมื่อลำแสงนี้เดินทางมาถึงยัง *Bob* พัลส์แสง "Local Oscillator" นี้จะผ่านเข้าสู่อุปกรณ์ผสมสัญญาณเฟส (Phase Modulator: PM) เพื่อเป็นการปรับเฟสที่จะใช้ในการตรวจจับเฟสของโคฮีเรนต์ของ *Bob* ก่อน จากนั้นทั้งพัลส์แสง "Signal" และ "Local Oscillator" จะรวมกันที่กระจกแยกลำแสง (BS) ซึ่งจะทำให้ *Bob* สามารถเลือกรับแอมพลิจูดหรือ

เฟสของโคฮีเรนต์ของแสงได้และจะได้กุญแจรหัสลับที่กระจายตัวแบบเกาส์ตามที่ *Alice* ได้ทำการส่ง

3.5 การเปรียบเทียบระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่องและแบบต่อเนื่อง

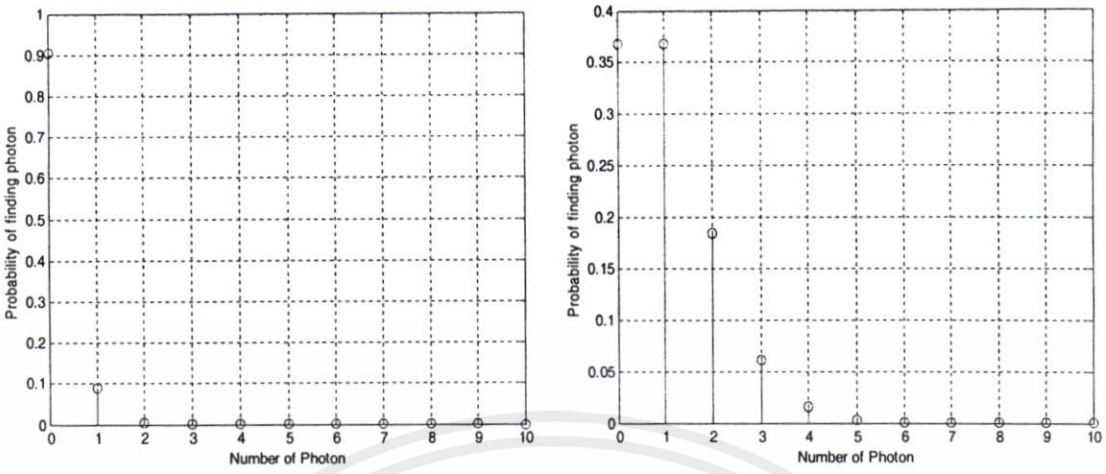
จากระบบวิทยาการรหัสลับเชิงควอนตัมที่พัฒนาขึ้นในปัจจุบัน ทั้งระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง และระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบแบบไม่ต่อเนื่อง ทั้งสองระบบนี้มีความแตกต่างกันในด้านของอุปกรณ์ที่ใช้ในการประยุกต์ รูปแบบของกุญแจรหัสลับและกระบวนการสร้างกุญแจรหัสลับ โดยสามารถสรุปได้ดังต่อไปนี้

3.5.1 ความแตกต่างของแหล่งกำเนิด

การสร้างโฟตอนเดี่ยวที่ใช้ในการส่งกุญแจรหัสลับในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง ในปัจจุบันระบบส่วนใหญ่นิยมใช้การลดทอนความเข้มของแสงเพื่อให้พัลส์แสงเหลือความเข้มแสงต่ำ (Weak Pulse) ซึ่งการลดทอนความเข้มแสงจะทำโดยผ่านพัลส์แสงที่แคบ เข้าสู่ตัวลดทอนความเข้มแสงซึ่งผลที่ได้จะเหลือพัลส์แสงความเข้มต่ำเปรียบเสมือนพัลส์แสงนั้นเป็นโฟตอนเดี่ยว โดยแหล่งกำเนิดแสงที่นิยมใช้ในระบบวิทยาการรหัสลับเชิงควอนตัมคือเลเซอร์ไดโอด (Laser Diode: LD) และไดโอดเปล่งแสงหรือแอลอีดี (Light Emitting Diode: LED) ซึ่งในระบบวิทยาการรหัสลับเชิงควอนตัมปัจจุบัน นิยมใช้แหล่งกำเนิดแสงจากเลเซอร์ไดโอด เนื่องจากช่วงของความยาวคลื่นแสงที่ไดโอดเปล่งแสงปล่อยออกมาจะมีช่วงของความยาวคลื่นแสงมากกว่าช่วงความยาวคลื่นแสงที่สร้างจากเลเซอร์ไดโอด ซึ่งจะทำให้อัตราการส่งพัลส์แสงทำได้ช้ากว่าพัลส์แสงที่สร้างจากเลเซอร์ไดโอดและส่งผลทำให้การส่งกุญแจรหัสลับทำได้ล่าช้าตามไปด้วย โดยจำนวนโฟตอนที่เหลืออยู่ภายในพัลส์แสงภายหลังจากการลดทอนความเข้มของแสง จะมีโอกาสพบจำนวนโฟตอนตามการกระจายโอกาสแบบปัวส์ซอง (Poisson Distribution) ดังสมการ [30] (รายละเอียดแสดงในภาคผนวก ก)

$$P(n) = \frac{\varepsilon^{t}}{t!} e^{-\varepsilon} \tag{3.2}$$

t คือจำนวนโฟตอนในพัลส์แสง และ ε คือค่าเฉลี่ยของจำนวนโฟตอน



ก ข

รูปที่ 3.10 ความน่าจะเป็นในการพบโฟตอนภายในพัลส์แสง

จากรูปที่ 3.10ก และ 3.1ข โอกาสในการพบจำนวนโฟตอนภายในพัลส์แสงที่ค่าเฉลี่ย 0.1 และ 1 หน่วย ตามลำดับ จะเห็นได้ว่าจำนวนโฟตอนที่เกิดขึ้นภายในพัลส์แสงที่ค่าเฉลี่ยเท่ากับ 1 หน่วย นี้จะมีโอกาสไม่พบโฟตอนภายในพัลส์แสงและมีโอกาสในการพบโฟตอนจำนวนหนึ่งหน่วยภายในพัลส์แสงที่ใกล้เคียงกัน นอกจากนี้ยังมีโอกาสพบโฟตอนมากกว่าหนึ่งหน่วยด้วยเช่นเดียวกัน ซึ่งในการเกิดจำนวนโฟตอนมากกว่าหนึ่งหน่วยในพัลส์แสงนี้ จะส่งผลต่อความปลอดภัยของระบบวิทยาการรหัสลับเชิงควอนตัม หากมีบุคคลที่สามเข้ามาตรวจจับพัลส์แสงนี้เพียงบางส่วนและส่งส่วนที่เหลือไปให้ยังภาครับ ซึ่งจะทำให้ผู้ส่งและผู้รับไม่ทราบถึงการเข้ามาขโมยข้อมูลเกี่ยวกับกุญแจรหัสลับของบุคคลที่สามและจะทำให้บุคคลที่สามได้ข้อมูลบางส่วนเกี่ยวกับกุญแจรหัสลับไป หากทำการลดค่าเฉลี่ยของจำนวนโฟตอนภายในพัลส์แสงเท่ากับ 0.1 หน่วย จะเห็นได้ว่าโอกาสที่จะไม่พบโฟตอนจะมีค่ามากกว่าโอกาสที่จะพบโฟตอนหนึ่งหน่วยภายในพัลส์แสง และมีโอกาสน้อยมากที่จะพบโฟตอนมากกว่าหนึ่งหน่วยภายในพัลส์แสง จะเห็นได้ว่าหากระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้สัญญาณพัลส์แสงความเข้มต่ำ (Weak Pulse) หากใช้ค่าเฉลี่ยของโฟตอนภายในพัลส์แสงน้อย เช่น 0.1 หน่วย จะมีข้อดีคือกุญแจรหัสลับในระบบวิทยาการรหัสลับเชิงควอนตัมนี้จะมีความปลอดภัยสูงกว่าระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้ค่าเฉลี่ยของโฟตอนสูงกว่า แต่จะมีข้อด้อยคือระบบวิทยาการรหัสลับเชิงควอนตัมนี้จะมีอัตราเร็วในการส่งกุญแจรหัสลับที่ต่ำตามไปด้วยเนื่องจากพัลส์แสงส่วนใหญ่จะไม่มีโฟตอนอยู่เลย ในส่วนของระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) จะใช้คุณสมบัติทางควอนตัมของที่ต่างจากระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องเช่น ใช้แอมพลิจูดหรือความเข้มของแสงและเฟสของโคฮีเรนต์ของแสงเลเซอร์แทนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ในแต่ละพัลส์แสง ซึ่งทำให้การส่งกุญแจรหัสลับรูปแบบนี้ใช้ความเข้มของแสงที่สูงกว่าระบบกระจายกุญแจรหัสลับแบบไม่

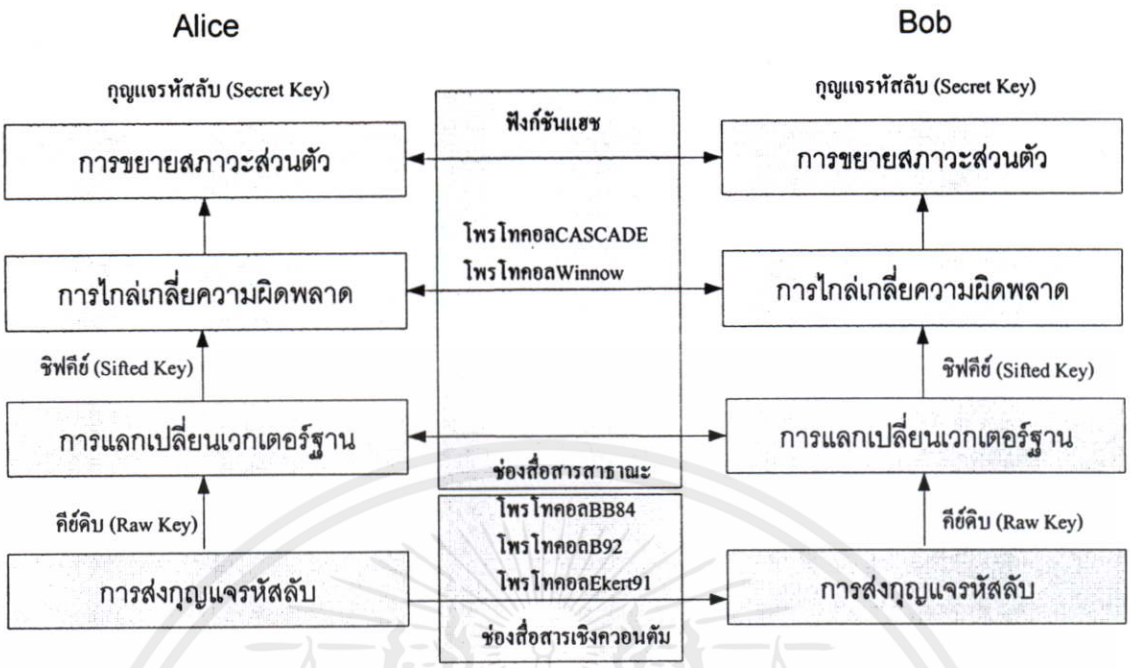
ต่อเนื่องส่งผลให้ระบบสามารถส่งกุญแจรหัสลับได้ไกลและส่งกุญแจรหัสลับได้รวดเร็วกว่าระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง

3.5.2 ความแตกต่างด้านอุปกรณ์ตรวจจับแสง

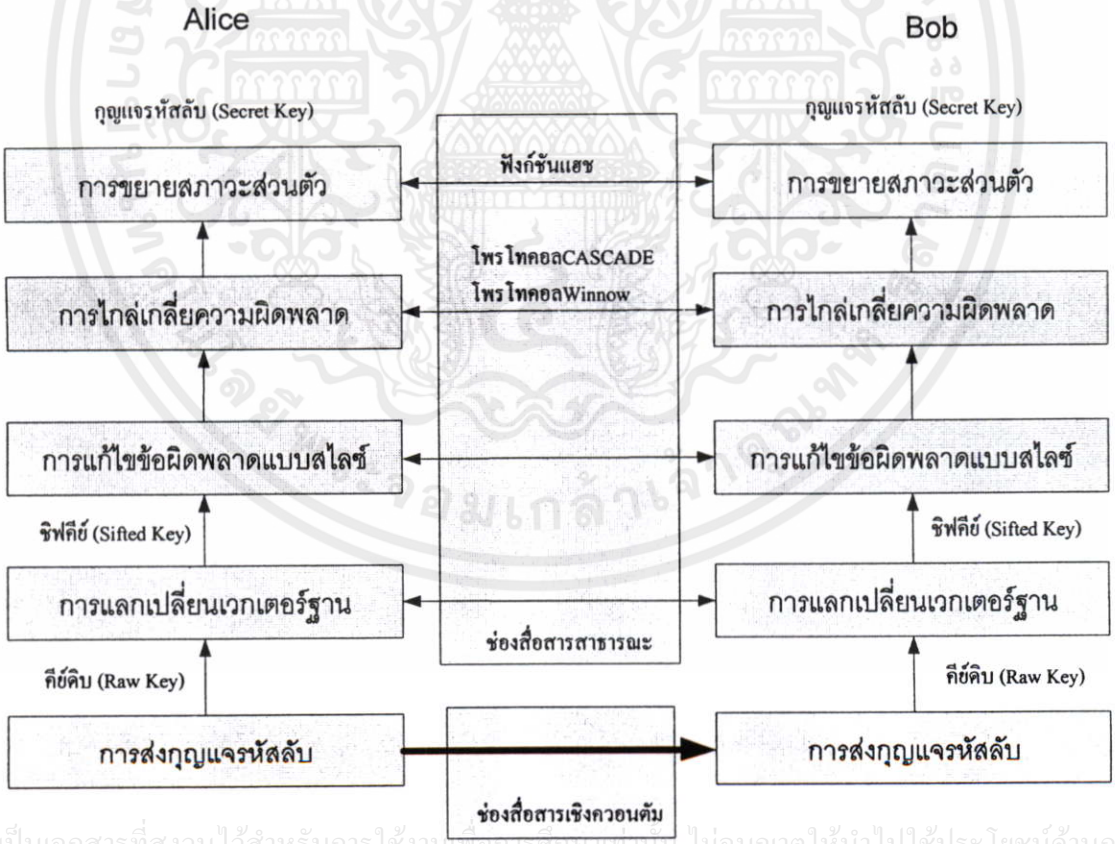
การตรวจจับแสงของระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องนิยมใช้อะวัลลันซ์โฟโตไดโอด (Avalanche Photo Diode: APD) ที่ทำงานใน Geiger Mode ซึ่งมีความสามารถในการตรวจจับแสงที่ความเข้มต่ำได้ดี การใช้อะวัลลันซ์โฟโตไดโอดจะเลือกให้เหมาะสมกับช่วงความยาวคลื่นของแหล่งกำเนิดและช่องทางการสื่อสารเชิงควอนตัมเช่น การสื่อสารผ่านเส้นใยนำแสงสำหรับความยาวคลื่น 830 นาโนเมตร นิยมใช้อะวัลลันซ์โฟโตไดโอดที่สร้างจากสารกึ่งตัวนำซิลิกอน (Si) เนื่องจากมีความสามารถในการตรวจจับโฟตอนเดี่ยวได้มากกว่า 50% [28] แต่ในการสื่อสารผ่านเส้นใยนำแสงสำหรับความยาวคลื่น 1300 นาโนเมตร อะวัลลันซ์โฟโตไดโอดที่สร้างจากสารกึ่งตัวนำซิลิกอนจะตรวจจับแสงที่ช่วงความยาวคลื่นเหล่านี้ได้ไม่มีประสิทธิภาพ จึงจำเป็นต้องเปลี่ยนประเภทของตัวตรวจจับแสงเป็นอะวัลลันซ์โฟโตไดโอดที่สร้างจาก GaAlAs แต่ข้อเสียที่สำคัญของอะวัลลันซ์โฟโตไดโอดที่สร้างจาก GaAlAs นี้คือประสิทธิภาพของการตรวจจับแสงความเข้มต่ำหรือโฟตอนเดี่ยวจะลดลงเหลือประมาณ 10-30% และมีราคาที่ค่อนข้างสูง [28] ในส่วนระบบกระจายกุญแจรหัสลับแบบต่อเนื่องจะใช้ตัวตรวจจับแบบโฮโมไดน์ (Homodyne Detector) ในการตรวจจับแสงซึ่งจะมีประสิทธิภาพดีกว่าอะวัลลันซ์โฟโตไดโอด มีความเร็วในการตรวจจับที่สูงกว่าที่อุณภูมิห้อง นอกจากนี้การจับจับโฟตอนด้วยตัวตรวจจับแบบโฮโมไดน์ จำเป็นต้องมีสัญญาณพัลส์แสงความเข้มสูงเป็นสัญญาณซิงโครไนเซชัน (Synchronization) ซึ่งจะทำให้การตรวจจับสามารถตรวจจับเฟสของโคฮีเรนต์ของแสงเป็นเป็นสัญญาณนาฬิกาในการส่งข้อมูลระหว่างผู้ส่งและผู้รับด้วย [28]

3.5.3 ความแตกต่างของกุญแจรหัสลับและกระบวนการไกล่เกลี่ยความผิดพลาด

การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องเป็นการส่งกุญแจรหัสลับในรูปแบบของตัวเลขไบนารีที่ประกอบด้วยบิต “1” และบิต “0” โดยแทนด้วยสถานะควอนตัมของโฟตอนเดี่ยวเช่น โพลาไรเซชันหรือเฟสของโพลาไรเซชัน เป็นต้น ข้อดีของการส่งกุญแจรหัสลับในรูปแบบไบนารีนี้ คือหากมีความผิดพลาดเกิดขึ้นในระหว่างการส่งกุญแจรหัสลับผู้ส่งและผู้รับจะใช้เทคนิคการแก้ไขความผิดพลาดให้กุญแจรหัสลับที่ผิดมีความถูกต้องและกุญแจรหัสลับนี้ สามารถที่จะนำไปใช้ร่วมกับระบบสื่อสารดิจิตอลเพื่อเข้าและถอดรหัสลับด้วยวิทยาการรหัสลับในปัจจุบันได้ ซึ่งทำให้กระบวนการกระจายกุญแจรหัสลับในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่องมีขั้นตอนในการทำงานดังรูปที่ 3.11



รูปที่ 3.11 การกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง



รูปที่ 3.12 การกระจายกุญแจรหัสลับแบบต่อเนื่อง

ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องเป็นการส่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์ โดยแทนกุญแจรหัสลับด้วยเฟสหรือแอมพลิจูดของสถานะโคฮีเรนต์ของแสง ซึ่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์นี้ จะถูกรบกวนจากสัญญาณรบกวนภายในช่องทางการสื่อสารเชิงควอนตัมได้ง่ายกว่ากุญแจรหัสลับแบบไบนารีและถ้าเกิดความผิดพลาดขึ้น ผู้ส่งและผู้รับยากที่จะแก้ไขความผิดพลาดให้กุญแจรหัสลับที่ส่งมีความถูกต้อง ดังนั้นการแก้ไขความผิดพลาดที่เกิดขึ้นจากการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง ผู้ส่งและผู้รับจะเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิต โดยใช้การแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) ซึ่งเมื่อผู้ส่งและผู้รับได้กุญแจรหัสลับบิตแล้วนั้น ผู้ส่งและผู้รับสามารถที่จะใช้เทคนิคการแก้ไขความผิดพลาดเพื่อทำให้กุญแจรหัสลับที่ส่งมีความถูกต้อง [33] เช่นเดียวกับระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง โดยการทำงานของการกระจายกุญแจรหัสลับแบบต่อเนื่องจะมีขั้นตอนที่ซับซ้อนกว่าการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่องดังรูปที่ 3.12

บทที่ 4
กระบวนการไกล่เกลี่ยความผิดพลาดของกุญแจรหัสลับ

กระบวนการไกล่เกลี่ยความผิดพลาด (Reconciliation) ซึ่งเป็นการแก้ไขความผิดพลาดของกุญแจรหัสลับบิตที่แตกต่างกันระหว่าง *Alice* และ *Bob* ให้กลับมามีกุญแจรหัสลับบิตที่เหมือนกัน โดยสาเหตุที่ทำให้เกิดความผิดพลาดระหว่างการส่งกุญแจรหัสลับบิตเหล่านี้เช่น ในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง บุคคลที่สามหรือ *Eve* เข้ามาขโมยสถานะควอนตัมของแสงภายในช่องทางการสื่อสารเชิงควอนตัมซึ่งการเข้ามาขโมยนี้ของ *Eve* จะเป็นการรบกวนระบบส่งผลให้สถานะควอนตัมเกิดการเปลี่ยนแปลงและส่งผลให้กุญแจรหัสลับเกิดความผิดพลาดตามไปด้วย สัญญาณรบกวน (Noise) ภายในช่องทางการสื่อสารเชิงควอนตัมและความไม่เป็นอุดมคติของอุปกรณ์ภายในภาคส่งและภาครับเป็นอีกสาเหตุที่ทำให้กุญแจรหัสลับบิตเกิดความผิดพลาด ส่วนในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง สัญญาณรบกวนและความไม่เป็นอุดมคติของอุปกรณ์ทั้งทางภาคส่งและภาครับ เป็นสาเหตุสำคัญที่ทำให้กุญแจรหัสลับที่กระจายตัวแบบเกาส์เกิดความผิดพลาด ส่งผลให้การเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตโดยการแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) เกิดความผิดพลาดตามไปด้วย กระบวนการไกล่เกลี่ยความผิดพลาดและการขยายสภาวะส่วนตัว เป็นกระบวนการที่นำมาใช้เพื่อแก้ไขความผิดพลาดที่เกิดขึ้นระหว่างกระบวนการส่งกุญแจรหัสลับและลดความสามารถในการสร้างกุญแจรหัสลับของ *Eve* เพื่อให้กุญแจรหัสลับที่จะนำมาใช้รักษาความปลอดภัยของข้อมูลมีความปลอดภัยมากที่สุด การไกล่เกลี่ยความผิดพลาดแบ่งเป็นสองประเภท [25] คือ

- การไกล่เกลี่ยความผิดพลาดทางตรง (Direct Reconciliation) มีการทำงานโดย *Alice* จะส่งข้อมูลเกี่ยวกับกุญแจรหัสลับของตน เช่น พาริตี้บิตหรือซินโดรมไปให้ *Bob* ผ่านทางช่องสื่อสารสาธารณะเพื่อให้ *Bob* แก้ไขกุญแจรหัสลับบิตที่ผิดให้เหมือนกับกุญแจรหัสลับบิตของ *Alice*
- การไกล่เกลี่ยความผิดพลาดย้อนกลับ (Reverse Reconciliation) มีการทำงานโดย *Bob* จะทำการส่งข้อมูลเกี่ยวกับกุญแจรหัสลับของตน เช่น พาริตี้บิตหรือซินโดรมไปให้ *Alice* ผ่านทางช่องสื่อสารสาธารณะเพื่อให้ *Alice* แก้ไขความผิดพลาดของกุญแจรหัสลับบิตของตนให้มีกุญแจรหัสลับบิตเหมือนกับ *Bob* [25]

เมื่อพิจารณาความปลอดภัยของกุญแจรหัสลับจากการไกล่เกลี่ยความผิดพลาดย้อนกลับและการไกล่เกลี่ยความผิดพลาดทางตรงจะเห็นได้ว่า การไกล่เกลี่ยความผิดพลาดย้อนกลับจะมีความปลอดภัยมากกว่าการไกล่เกลี่ยความผิดพลาดทางตรง เนื่องจากในการส่งกุญแจรหัสลับผ่านช่องทางการสื่อสารเชิงควอนตัม *Alice* จะส่งกุญแจรหัสลับโดยแทนด้วยสถานะควอนตัมของแสง

ผ่านช่องทางการสื่อสารเชิงควอนตัมไปยัง *Bob* ซึ่งบุคคลที่สาม (*Eve*) สามารถที่จะเข้ามาขโมยสถานะควอนตัมแสง ทำให้ *Eve* ได้ข้อมูลเกี่ยวกับกุญแจรหัสลับไป ในกรณีที่ *Alice* และ *Bob* ใช้การไกล่เกลี่ยความผิดพลาดทางตรง โดย *Alice* จะทำการเปิดเผยข้อมูลบางส่วนเกี่ยวกับกุญแจรหัสลับที่ตนมีอยู่ไปให้แก่ *Bob* เพื่อให้ *Bob* ทำการแก้ไขกุญแจรหัสลับบิตของตนให้เหมือนกับ *Alice* ซึ่ง *Eve* สามารถที่จะเข้ามาขโมยข้อมูลเกี่ยวกับกุญแจรหัสลับเหล่านี้ เมื่อ *Eve* นำข้อมูลและนำไปรวมกับข้อมูลเกี่ยวกับกุญแจรหัสลับที่ได้จากการเข้ามาขโมยทางช่องทางการสื่อสารเชิงควอนตัม ทำให้ *Eve* อาจจะสามารถสร้างหรือทำสำเนากุญแจรหัสลับขึ้นมาใหม่ได้ แต่เมื่อพิจารณากรณีการไกล่เกลี่ยความผิดพลาดย้อนกลับ *Bob* จะส่งข้อมูลเกี่ยวกับกุญแจรหัสลับของตนไปให้ *Alice* เพื่อให้ *Alice* แก้ไขความผิดพลาดให้กุญแจรหัสลับเหมือนกับ *Bob* ซึ่งข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Bob* ส่งไปให้ *Alice* นี้เป็นข้อมูลที่กุญแจรหัสลับของ *Bob* ร่วมกับความผิดพลาดระหว่างการส่งสถานะควอนตัมของแสงผ่านช่องทางการสื่อสารเชิงควอนตัม หาก *Eve* เข้ามาขโมยสถานะควอนตัมจากช่องสื่อสารเชิงควอนตัมข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* ได้รับจะแตกต่างจากกุญแจรหัสลับที่ *Bob* มีอยู่ ซึ่งเมื่อ *Eve* เข้ามาขโมยข้อมูลเกี่ยวกับกุญแจรหัสลับระหว่างการแก้ไขความผิดพลาด และนำข้อมูลส่วนนี้มารวมกับข้อมูลเกี่ยวกับกุญแจรหัสลับ ที่ขโมยได้ระหว่างการส่งสถานะควอนตัมทางช่องทางการสื่อสารเชิงควอนตัมจะเห็นได้ว่าข้อมูลที่ *Eve* ได้ไป จะไม่มีส่วนช่วยให้ *Eve* สามารถสร้างหรือทำสำเนากุญแจรหัสลับขึ้นมาใหม่ได้ [33] จึงสามารถสรุปได้ว่าการการไกล่เกลี่ยความผิดพลาดย้อนกลับจะให้กุญแจรหัสลับมีความปลอดภัยมากกว่าการไกล่เกลี่ยความผิดพลาดทางตรง

4.1 การวัดปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับ

การวัดปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Bob* ได้รับจาก *Alice* เพื่อเปรียบเทียบกับปริมาณข่าวสารที่ *Eve* ได้จากการเข้ามาขโมยข้อมูลเกี่ยวกับกุญแจรหัสลับในช่องทางการสื่อสารเชิงควอนตัมนี้เพื่อเป็นการทดสอบความปลอดภัยในขั้นตอนการส่งกุญแจรหัสลับทางช่องสื่อสารเชิงควอนตัม ซึ่งจะทำให้ผู้ส่งและผู้รับมั่นใจว่าระบบการส่งกุญแจรหัสลับนี้มีความปลอดภัยสามารถนำกุญแจรหัสลับที่ได้มาผ่านกระบวนการกลั่นกุญแจรหัสลับและไม่ทำให้ *Eve* ได้ข้อมูลเกี่ยวกับกุญแจรหัสลับมากเกินไปจนสามารถจะทำสำเนาหรือสร้างกุญแจรหัสลับใหม่ ขั้นตอนการวัดปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับระหว่างการส่งสามารถหาได้ดังนี้ กำหนดให้ *Alice* ทำการสร้างกุญแจรหัสลับที่ต้องการส่งโดยแทนด้วยตัวแปรสุ่ม X และที่ภาครับ *Bob* รับกุญแจรหัสลับที่ *Alice* ส่งมาโดยแทนด้วยตัวแปรสุ่ม Y และในระหว่างการส่ง *Eve* สามารถที่จะเข้ามาขโมยกุญแจรหัสลับภายในช่องทางการสื่อสารเชิงควอนตัมได้ซึ่งข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* ขโมยได้แทนด้วยตัวแปรสุ่ม Z ดังนั้นความปลอดภัยในการส่งกุญแจรหัสลับนี้จะต้องเป็นไปตามเงื่อนไขดังสมการ [30]

$$\Delta I = I(X,Y) - I(X,Z) \text{ หรือ } I(X,Y) - I(Y,Z) \tag{4.1}$$

ถ้าระบบกระจายกุญแจรหัสลับเชิงควอนตัมใช้การไกล่เกลี่ยความผิดพลาดทางตรง เพื่อการแก้ไขความผิดพลาด กุญแจรหัสลับที่ส่งโดยระบบกระจายกุญแจรหัสลับเชิงควอนตัมนี้จะมีความปลอดภัยก็ต่อเมื่อปริมาณข่าวสารเฉลี่ยที่ *Bob* ได้รับจาก *Alice* มีค่ามากกว่าปริมาณข่าวสารเฉลี่ยที่ *Eve* ได้รับจาก *Alice* นั่นคือ เมื่อปริมาณข่าวสารสุทธิมีค่ามากกว่าศูนย์ ($\Delta I > 0$) ส่วนระบบกระจายกุญแจรหัสลับที่ใช้การไกล่เกลี่ยความผิดพลาดย้อนกลับ กุญแจรหัสลับในระบบกระจายกุญแจรหัสลับจะมีความปลอดภัย เมื่อ *Alice* มีข้อมูลเกี่ยวกับกุญแจรหัสลับมากกว่า *Eve* โดยที่ $I(X,Y)$ เท่ากับ $I(Y,X)$ ถ้า $\Delta I < 0$ แล้ว *Eve* จะมีปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับมากกว่า *Bob* ในกรณีการไกล่เกลี่ยทางตรงหรือ *Alice* ในกรณีการไกล่เกลี่ยย้อนกลับซึ่งจะทำให้เมื่อนำกุญแจรหัสลับเหล่านี้มาผ่านกระบวนการไกล่เกลี่ยความผิดพลาดแล้วจะเป็นการเพิ่มข้อมูลเกี่ยวกับกุญแจรหัสลับให้แก่ *Eve* ทำให้ *Eve* อาจจะสามารถสร้างหรือทำสำเนากุญแจรหัสลับขึ้นมาใหม่ได้ ดังนั้นในกรณีดังกล่าว ทั้ง *Alice* และ *Bob* จะทำการทิ้งกุญแจรหัสลับที่ทำการส่งนี้ทั้งหมดแล้วทำการส่งกุญแจรหัสลับใหม่แทน

4.1.1ปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับในระบบ DV-QKD

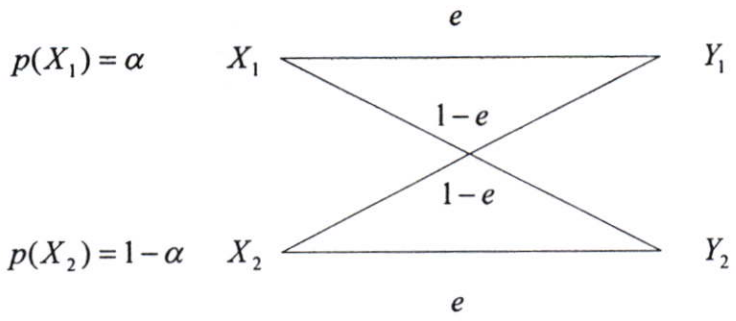
การวัดปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับ หลังจากส่งกุญแจรหัสลับในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องสามารถหาได้ โดยกำหนดให้ระบบกระจายกุญแจรหัสลับเชิงควอนตัมมีรูปแบบการส่งตามช่องสื่อสารแบบไบนารี (Binary Symmetric Channel: BSC) ดังรูปที่ 4.1 โดยปริมาณข่าวสารร่วม (Mutual Information) ระหว่าง *Alice* และ *Bob* เมื่อไม่มีผู้บุกรุกเข้ามาขโมยสถานะควอนตัมของโฟตอนเดี่ยวแสดงดังสมการ

$$I(X;Y) = H(X) - H(X \mid Y) \tag{4.2}$$

โดยที่ปริมาณข่าวสารเฉลี่ย (Entropy) ของ *Alice* สามารถหาได้จาก

$$\begin{aligned} H_X &= -\sum_{i=1}^{2} p(x_i)\log_2 p(x_i) \\ &= -\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha) \end{aligned} \tag{4.3}$$

ปริมาณข่าวสารเฉลี่ยแบบมีเงื่อนไข $H(X \mid Y)$ สามารถคำนวณจาก



รูปที่ 4.1 ช่องสัญญาณแบบไบนารี

$$H(X \mid Y) = \sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log_2 \frac{1}{p(y_j \mid x_i)}$$

$$= -\alpha e \log_2 e - \alpha(1-e)\log_2(1-e) - (1-\alpha)e\log_2 e - (1-\alpha)(1-e)\log_2(1-e)$$
$$= -e\log_2 e - (1-e)\log_2(1-e) \qquad (4.4)$$

ดังนั้นหากแหล่งกำเนิดสร้างตัวเลขไบนารีที่มีความน่าจะเป็นในการเกิดที่เท่ากันจะได้

$$I(X;Y) = 1 + e\log_2 e + (1-e)\log_2(1-e) \qquad (4.5)$$

ดังนั้นหลังจากที่ทำการส่งกุญแจรหัสลับทางช่องทางการสื่อสารเชิงควอนตัมแล้วนั้น *Alice* และ *Bob* จะมีปริมาณข่าวสารร่วมกันมีค่าเท่ากับ $I(X;Y)$ หรือ I_{AB}

4.1.2 ปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับในระบบ CV-QKD

ระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง เป็นระบบวิทยาการรหัสลับเชิงควอนตัมที่ใช้สถานะโคฮีเรนต์ (Coherent) หรือ Squeezed State แทนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ (Gaussian Distribution) ซึ่งระบบนี้ มีการพิจารณาความปลอดภัยระหว่างการส่งกุญแจรหัสลับหรือการตรวจจับผู้บุกรุกที่เข้ามาขโมยสถานะควอนตัมแตกต่างจากการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) โดยการตรวจสอบผู้บุกรุกในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่องนี้ จะเปรียบเทียบปริมาณข่าวสารที่ผู้รับจากช่องทางการสื่อสารเชิงควอนตัม โดยจากทฤษฎีข่าวสารที่นำเสนอโดย C. Shannon [15] อัตราการส่งข้อมูลผ่านช่องสื่อสารจะมีปริมาณสูงสุด เมื่อข่าวสารนั้นมีความน่าจะเป็นในการเกิดที่กระจายโอกาสแบบเกาส์ ดังนั้นถ้า *Alice* ส่งข้อมูลที่กระจายตัวแบบเกาส์ผ่านช่องสื่อสารเชิงควอนตัมมายัง *Bob* หาก *Bob* รับปริมาณข่าวสารได้น้อยกว่าครึ่งหนึ่งที่ *Alice* ส่งมาให้ แสดงว่า *Bob* จะได้ข้อมูลเกี่ยวกับกุญแจรหัสลับน้อย

กว่า *Eve* ซึ่ง *Alice* และ *Bob* จะยกเลิกการส่งกุญแจรหัสลับทั้งหมดและทำการส่งกุญแจรหัสลับใหม่ โดยปริมาณข่าวสารที่ *Bob* ได้รับจาก *Alice* แสดงดังสมการ

$$\begin{aligned} I(A;B) &= \frac{1}{2}\log_2(1+SNR) \\ &= \frac{1}{2}\log_2(1+\frac{V_{Signal}}{V_{Noise}}) \end{aligned} \tag{4.6}$$

SNR คืออัตราส่วนของกำลังงานของสัญญาณต่อกำลังงานของสัญญาณรบกวน (Signal to Noise Ratio: SNR)

V_{Signal} คือความแปรปรวนของสัญญาณที่ภาครับได้รับ

V_{Noise} คือความแปรปรวนของสัญญาณรบกวนที่เกิดขึ้นภายในช่องสัญญาณ

ในการพิจารณาความปลอดภัยของระบบกระจายกุญแจรหัสลับเชิงควอนตัม ΔI จะต้องมีค่ามากกว่าศูนย์ ซึ่งแสดงว่า *Bob* มีปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับมากกว่า *Eve* โดยจากสมการที่ (4.6) $I(A;B)$ หรือ $I(B;A)$ และ $I(B;E)$ แสดงดังนี้ [9]

$$I(A;B) = \frac{1}{2}\log_2\left[\frac{V_B}{(V_{B|A})_{coh}}\right] \tag{4.7}$$

และ

$$I(B;E) = \frac{1}{2}\log_2\left[\frac{V_B}{(V_{B|E})_{\min}}\right] \tag{4.8}$$

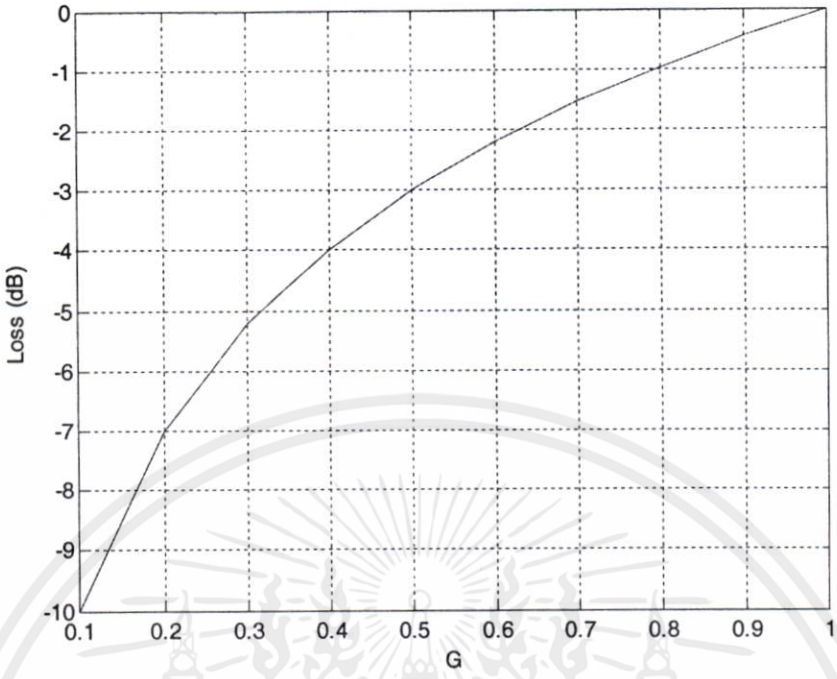
$V_B = < x_B^2 > = < p_B^2 > = G(V+\chi)N_0$

$< x_B^2 >$ คือขนาดของแอมพลิจูดของสถานะโคฮีเรนต์ทางด้าน *Bob*

$< p_B^2 >$ คือขนาดของเฟสของสถานะโคฮีเรนต์ทางด้าน *Bob*

G คือประสิทธิภาพของช่องสื่อสารเชิงควอนตัมถ้า G มีค่าเท่ากับหนึ่ง แสดงว่าไม่มีการสูญเสียภายในช่องสื่อสารเชิงควอนตัม ถ้า G มีค่าเท่ากับ 0.5 แสดงว่ามีการสูญเสียภายในช่องสื่อสารเชิงควอนตัมเท่ากับ 3.1 *dB* เป็นต้น ซึ่งความสัมพันธ์ระหว่างประสิทธิภาพของช่องสื่อสารเชิงควอนตัมและการสูญเสียภายในช่องสื่อสารเชิงควอนตัมแสดงดังรูปที่ 4.2 [9]

V คือความแปรปรวนของสัญญาณซึ่งจะมีค่าเท่ากับ $V = V_A + 1$ โดยที่ V_A คือความแปรปรวนของการกระจายแบบเกาส์ที่ *Alice* ใช้สร้างกุญแจรหัสลับ



รูปที่ 4.2 ความสัมพันธ์ระหว่างประสิทธิภาพและการสูญเสียภายในช่องสื่อสารเชิงควอนตัม

χ คือสัญญาณรบกวนในสถานะพื้น (Vacuum Noise) โดยความสัมพันธ์ระหว่างสัญญาณรบกวนในสถานะพื้น (χ) และประสิทธิภาพของช่องสื่อสาร (G) มีค่าเท่ากับ $\chi = \frac{1-G}{G}$ แสดงดังรูปที่ 4.3

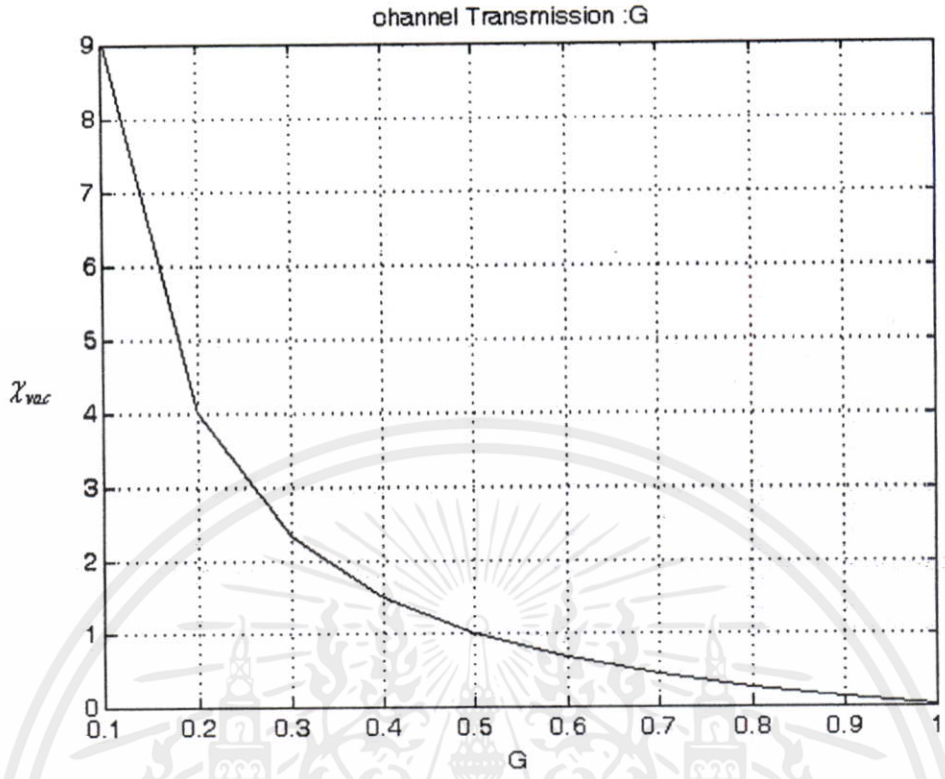
$(V_{B|A})_{coh}$ คือความแปรปรวนแบบมีเงื่อนไขของสถานะโคฮีเรนต์ของ *Bob* เมื่อทราบความแปรปรวนของสถานะโคฮีเรนต์ของ *Alice* แสดงได้ดังนี้ [9]

$$(V_{B|A})_{coh} = (V_{x_B|x_A})_{coh} = (V_{p_{B|}p_A})_{coh} = G(\chi+1)N_0 \tag{4.9}$$

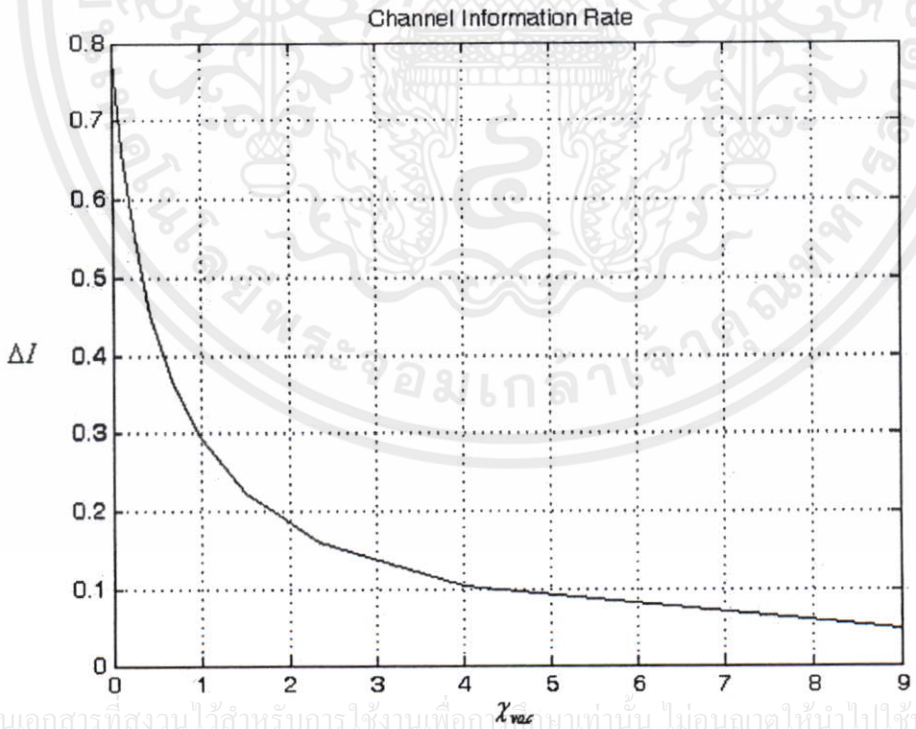
$(V_{B|E})_{\min}$ คือความแปรปรวนแบบมีเงื่อนไขน้อยที่สุดของสถานะโคฮีเรนต์ของ *Bob* เมื่อทราบความแปรปรวนของสถานะโคฮีเรนต์ของ *Eve* แสดงได้ดังนี้ [9]

$$(V_{B|E})_{\min} = (V_{x_B|x_E})_{\min} = (V_{p_{B|}p_E})_{\min} = \frac{N_0}{G(\chi+V^{-1})} \tag{4.10}$$

จากสมการที่ (4.7-4.10) ปริมาณข่าวสารสุทธิแสดงดังสมการ



รูปที่ 4.3 ความสัมพันธ์ระหว่างสัญญาณรบกวนในสถานะพื้นและประสิทธิภาพของช่องสื่อสาร



รูปที่ 4.4 ปริมาณข่าวสารสุทธิระหว่าง *Bob* และ *Eve* ที่ความแปรปรวนเท่ากับสามกรณีการไกล่เกลี่ยความผิดพลาดย้อนกลับ

$$\begin{aligned}\Delta I &= I_{AB} - I_{BE} \\ &= \frac{1}{2}\log_2\left[\frac{1}{G^2(1+\chi)(V^{-1}+\chi)}\right]\end{aligned} \tag{4.11}$$

ΔI คือปริมาณข่าวสารสุทธิ

ความสัมพันธ์ระหว่างสัญญาณรบกวนในสถานะพื้น ประสิทธิภาพของช่องสื่อสารและปริมาณข่าวสารสุทธิระหว่าง *Alice* และ *Bob* แสดงดังรูปที่ 4.4 ซึ่งแม้จะมีการสูญเสียหรือสัญญาณรบกวนเกิดขึ้นระหว่างการส่งปริมาณเท่าใดก็ตามแต่ ปริมาณข่าวสารที่ *Bob* รับได้ยังคงมีค่ามากกว่าปริมาณข่าวสารที่ *Eve* ได้รับหมายความว่า ข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* ขโมยได้จะมีปริมาณที่น้อยกว่า *Bob* ซึ่งจะทำให้ *Alice* และ *Bob* สามารถนำกุญแจรหัสลับนี้ไปผ่านกระบวนการแก้ไขความผิดพลาด ซึ่งเป็นกระบวนการถัดไปได้โดยกุญแจรหัสลับที่ส่งยังคงมีความปลอดภัยอยู่

ในกรณีของการไกล่เกลี่ยความผิดพลาดทางตรงนั้น ปริมาณข่าวสารสุทธิแสดงดังสมการ

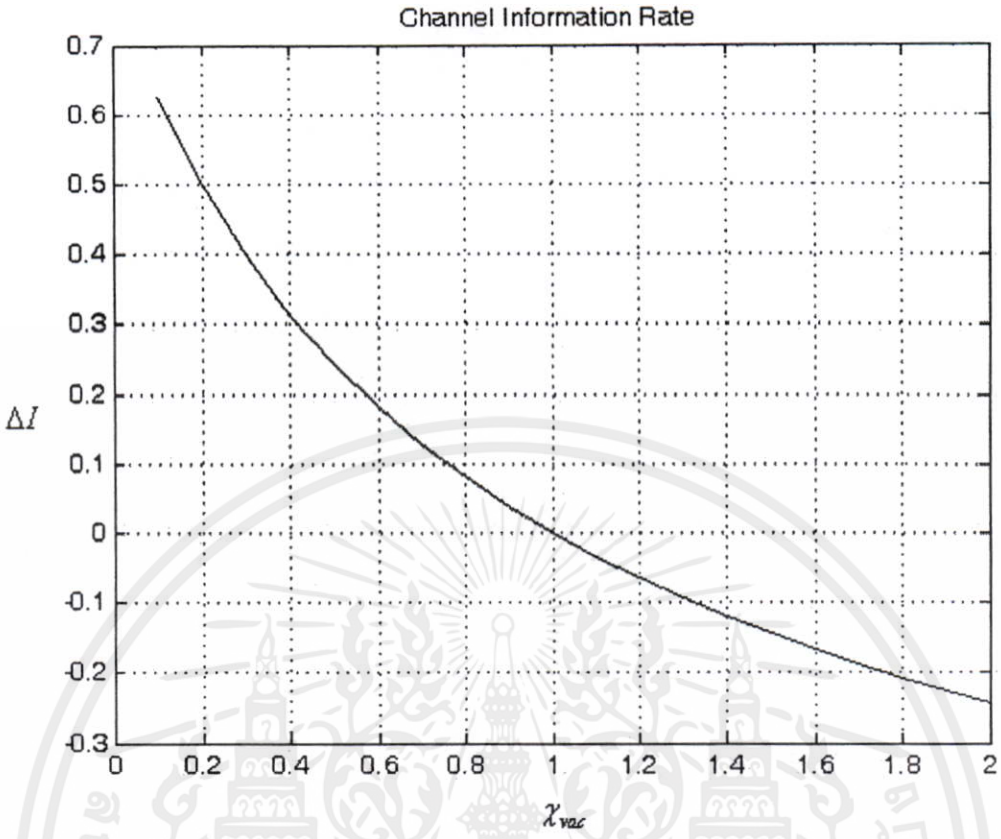
$$\Delta I = I(A;B) - I(A;E) \tag{4.12}$$

โดยที่ $I(A;B)$ แสดงดังสมการที่ (4.8) และ $I(A;E)$ สามารถหาค่าได้จาก [10]

$$I(A;E) = \frac{1}{2}\log_2\left[\frac{V+1/x}{1+1/x}\right] \tag{4.13}$$

$$\Delta I = \frac{1}{2}\log_2\left[\frac{V+x}{1+Vx}\right] \tag{4.14}$$

ซึ่งปริมาณข่าวสารสุทธิในกรณีของการไกล่เกลี่ยความผิดพลาดทางตรง เมื่อเปรียบเทียบกับปริมาณสัญญาณรบกวนที่เกิดขึ้นแสดงได้ดังรูปที่ 4.5 จะเห็นได้ว่ากุญแจรหัสลับจะมีความปลอดภัยก็ต่อเมื่อปริมาณสัญญาณรบกวนมีค่าน้อยกว่าหนึ่ง $(\chi < 1)$ หรือประสิทธิภาพของช่องสื่อสารเชิงควอนตัม $G > \frac{1}{2}$ หากช่องสื่อสารเชิงควอนตัมมีปริมาณสัญญาณรบกวนสูง $\chi > 1$ ปริมาณข่าวสารที่ *Eve* ได้รับจะมีมากกว่า *Bob* ถ้าหาก *Alice* และ *Bob* ยังคงที่จะดำเนินการไกล่เกลี่ยความผิดพลาดอีก ซึ่งจะเป็นการเปิดเผยข้อมูลเกี่ยวกับกุญแจรหัสลับให้ *Eve* อีก อาจจะส่งผลทำให้ *Eve* สามารถที่จะสร้างหรือทำสำเนากุญแจรหัสลับขึ้นมาใหม่ได้ ดังนั้นเมื่อปริมาณข่าวสารที่ *Bob* ได้รับมีค่าน้อยกว่า *Eve* ทั้ง *Alice* และ *Bob* จะทิ้งกุญแจรหัสลับที่รับส่งทั้งหมด แล้วทำการส่งกุญแจรหัสลับใหม่



รูปที่ 4.5 ปริมาณข่าวสารสุทธิระหว่าง *Bob* และ *Eve* ที่ความแปรปรวนเท่ากับสามกรณีการไกล่เกลี่ยความผิดพลาดทางตรง

4.2 ข้อจำกัดของแชลนอนในระบบกระจายกุญแจรหัสลับเชิงควอนตัม

การไกล่เกลี่ยความผิดพลาดเป็นกระบวนการทำให้กุญแจรหัสลับของ *Alice* และ *Bob* มีความเหมือนกัน จากทฤษฎีข่าวสาร (Information Theory) ของแชลนอน (C. Shannon) [15] ปริมาณข้อมูลน้อยที่สุด ที่ *Alice* จะส่งให้ *Bob* เพื่อให้ *Bob* สามารถแก้ไขความผิดพลาดที่เกิดขึ้นเมื่ออัตราความผิดพลาดระหว่างการส่งกุญแจรหัสลับผ่านช่องทางการสื่อสารเชิงควอนตัมเท่ากับ e แสดงได้ดังนี้

$$n_{\min} = 1 - I_s(e) \tag{4.15}$$

e คืออัตราการผิดของกุญแจรหัสลับบิตที่ส่งผ่านช่องทางการสื่อสารเชิงควอนตัมและ $I_s(e)$ เท่ากับ $1 + e\log_2 e + (1-e)\log_2(1-e)$

4.3 อัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัม

อัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัม (Quantum Bit Error Rate: QBER) เป็นอัตราที่ใช้อธิบายถึงจำนวนความผิดพลาดที่เกิดขึ้นทั้งหมดจากการกระจายกุญแจรหัสลับบิตผ่านทางช่องสื่อสารเชิงควอนตัม (Quantum Channel) ในการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง อัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านทางช่องสื่อสารเชิงควอนตัมนี้จะบอกถึงการเข้ามาขโมยกุญแจรหัสลับของบุคคลที่สาม (*Eve*) หากบุคคลที่สามเข้ามาขโมยกุญแจรหัสลับ โดยการขโมยสถานะควอนตัมของโฟตอนเดี่ยวจะทำให้ผู้ส่งและผู้รับทราบทันที เนื่องจากผู้รับไม่ได้รับสถานะควอนตัมของโฟตอนเดี่ยว แต่หากบุคคลที่สามเข้ามาขโมยสถานะควอนตัมของโฟตอนเดี่ยวและทำการสถานะควอนตัมของโฟตอนเดี่ยวขึ้นมาใหม่ ก่อนจะส่งไปให้ผู้รับผ่านทางช่องสื่อสารเชิงควอนตัม ผู้ส่งและผู้รับจะทราบทันทีถึงการเข้ามาขโมยสถานะควอนตัมของบุคคลที่สามเช่นเดียวกัน เนื่องจากอัตราความผิดพลาดของกุญแจรหัสลับที่เพิ่มสูงขึ้นจากปกติ ในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง อัตราความผิดพลาดจากการกระจายกุญแจรหัสลับ จะบอกถึงอัตราความผิดพลาดที่เกิดขึ้นในกระบวนการแก้ไขความผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) โดยอัตราความผิดพลาดที่เกิดขึ้นจากการกระจายกุญแจรหัสลับ หาได้จาก *Alice* และ *Bob* ทำการสุ่มกุญแจรหัสลับของตนขึ้นบางตำแหน่งที่เหมือนกัน ก่อนจะส่งมาเปรียบเทียบกันผ่านทางช่องสื่อสารสาธารณะ (Public Channel) หลังจากนั้นกุญแจรหัสลับที่ถูกสุ่มขึ้นมาทั้งหมดนี้จะถูกทิ้งไป โดอัตราความผิดพลาดจากการกระจายกุญแจรหัสลับสามารถแสดงได้ดังต่อไปนี้

$$\text{อัตราความผิดพลาด } (e) = \text{จำนวนบิตที่ผิด} / \text{จำนวนบิตทั้งหมด} \qquad (4.16)$$

4.4 ตัวอย่างโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม

การส่งกุญแจรหัสลับผ่านทางช่องสื่อสารเชิงควอนตัม สาเหตุต่างๆ เช่น สัญญาณรบกวนภายในช่องสื่อสารเชิงควอนตัม การเข้ามาขโมยสถานะควอนตัมของบุคคลที่สาม ความไม่เป็นอุดมคติของอุปกรณ์ทั้งทางภาคส่งและทางภาครับ ล้วนเป็นสาเหตุทำให้กุญแจรหัสลับที่ส่งเกิดความผิดพลาด ดังนั้นทางผู้ส่งและผู้รับจึงต้องแก้ไขความผิดพลาดที่เกิดขึ้นก่อนที่จะนำกุญแจรหัสลับเหล่านี้ไปใช้ในการเข้ารหัสและถอดรหัสลับ โดยการแก้ไขความผิดพลาดความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) ซึ่งเป็นการส่งกุญแจรหัสลับบิตผ่านทางช่องสื่อสารเชิงควอนตัม หากเกิดความผิดพลาดขึ้นระบบกระจายกุญแจรหัสลับในรูปแบบนี้สามารถใช้โพรโทคอลแก้ไขความผิดพลาดมาใช้ในการแก้ไขความผิดพลาดที่เกิดขึ้นนี้ได้ โดยตัวอย่างโพรโทคอลแก้ไขความผิดพลาดที่ใช้ในการแก้ไขความผิดพลาดพลาด ที่เกิดขึ้นในระหว่างการส่งกุญแจรหัสลับบิตมีตัวอย่างดังต่อไปนี้

ตารางที่ 4.1 ตัวอย่างการหาพาริตี้บิตของข้อมูลขนาด 7 บิต

ข้อมูล (k) ขนาด 7 บิต	พาริตี้คู่ (Even Parity)	พาริตี้คี่ (Odd Parity)
0000000	**0**0000000	**1**0000000
0101010	**1**0101010	**0**0101010
1010101	**0**1010101	**1**1010101
1111111	**1**1111111	**0**1111111

4.4.1 โพรโทคอล BBBSS

โพรโทคอล BBBSS เป็นโพรโทคอลแรกที่ใช้ในการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมสำหรับระบบวิทยาการรหัสลับที่เสนอไว้โดย C.H. Bennett และ G. Brassard ในปี ค.ศ. 1992 [2] ซึ่งการทำงานของโพรโทคอลนี้อาศัยพาริตี้บิตเพื่อใช้ในการตรวจหาตำแหน่งกุญแจรหัสลับบิตที่ผิดและแก้ไขความผิดพลาดที่เกิดขึ้นกับกุญแจรหัสลับบิตนั้น โดยพาริตี้บิตสามารถตรวจสอบพบเพียงความผิดพลาดที่เกิดขึ้นเมื่อมีความผิดพลาดเกิดขึ้นเป็นจำนวนคี่ แต่จะไม่สามารถที่ตรวจพบความผิดพลาดเมื่อมีความผิดพลาดเกิดขึ้นเป็นจำนวนคู่ ดังนั้นหากต้องการทราบตำแหน่งกุญแจรหัสลับบิตที่ผิด ผู้ส่งและผู้รับจะแบ่งบล็อกกุญแจรหัสลับที่มีพาริตี้บิตแตกต่างกันออกเป็นสองบล็อกแล้วเปรียบเทียบพาริตี้บิตของบล็อกเหล่านั้นใหม่พร้อมกับตัดกุญแจรหัสลับบิตตำแหน่งสุดท้ายของบล็อกออกเพื่อลดข้อมูลเกี่ยวกับกุญแจรหัสลับที่บุคคลที่สามได้ไประหว่างการแก้ไขความผิดพลาด ซึ่งผู้ส่งและผู้รับจะทำเช่นนี้จนกว่าจะทราบตำแหน่งกุญแจรหัสลับที่ผิด โดยหลักการพื้นฐานและการทำงานของโพรโทคอล BBBSS มีดังต่อไปนี้

4.4.1.1หลักการพื้นฐานของพาริตี้บิต

พาริตี้บิตเป็นหนึ่งในหลักการที่ใช้ในระบบสื่อสารแบบดิจิตอลเพื่อตรวจสอบความผิดพลาดที่เกิดขึ้นระหว่างการส่งข้อมูลผ่านระบบสื่อสาร ซึ่งพาริตี้บิตคือบิตที่ถูกเพิ่มขึ้นมาอีกหนึ่งในบล็อกข้อมูลที่ต้องการส่งโดยบิตที่เพิ่มขึ้นมานี้จะเป็นบิต “0” หรือ บิต “1” ขึ้นอยู่กับจำนวนของบิต “1” ในบล็อกข้อมูลนั้น พาริตี้บิตแบบเป็นสองประเภทดังนี้

- **พาริตี้คี่ (Odd Parity)** คือพาริตี้บิตที่ถูกเพิ่มขึ้นซึ่งอาจจะเป็นบิต “1” หรือบิต “0” เพื่อให้จำนวนบิต “1” ในบล็อกข้อมูลและบิตพาริตี้บิตมีผลรวมแล้วเป็นจำนวนคี่

- **พาริตี้คู่ (Even Parity)** คือพาริตี้บิตที่ถูกเพิ่มขึ้นซึ่งอาจจะเป็นบิต “1” หรือบิต “0” เพื่อให้จำนวนบิต “1” ในบล็อกข้อมูลและบิตพาริตี้บิตมีผลรวมแล้วเป็นจำนวนคู่

การตรวจสอบความผิดพลาดโดยใช้พาริตี้บิตผู้ส่งจะเพิ่มพาริตี้บิตเข้าไปในบล็อกข้อมูลที่ต้องการส่งเมื่อผู้รับได้รับข้อมูลชุดนั้นจะทำการหาค่าพาริตี้บิตเพื่อเปรียบเทียบกับพาริตี้บิตที่ได้จากผู้ส่ง ถ้าหากพาริตี้บิตมีความแตกต่างกันผู้รับจะทราบทันทีว่าเกิดความผิดพลาดขึ้นภายในบล็อก

ข้อมูลนั้นเป็นจำนวนคี่ แต่ผู้รับจะไม่ทราบตำแหน่งบิตที่ผิดและไม่สามารถแก้ไขบิตที่ผิดให้กลับมาถูกต้องได้ ถ้าพาริตี้บิตที่ผู้รับและผู้ส่งมีความเหมือนกันข้อมูลที่ผู้รับได้รับอาจจะมีความถูกต้องหรือเกิดความผิดพลาดขึ้นเป็นจำนวนคู่โดยที่ผู้รับจะทราบทันทีเลยว่ามีการผิดเกิดขึ้นกับข้อมูลชุดนั้นหรือไม่ โดยตัวอย่างของพาริตี้บิตแสดงได้ดังตารางที่ 4.1

4.4.1.2 การทำงานของโพรโทคอล BBBSS

การทำการแก้ไขความผิดพลาดของโพรโทคอล BBBSS นี้แสดงดังรูปที่ 4.6 ซึ่งขั้นตอนการทำงานทั้งหมดมีดังต่อไปนี้

ขั้นตอนที่ 1 *Alice* และ *Bob* แบ่งกุญแจรหัสลับบิตของตนออกเป็นบล็อกโดยขนาดของบล็อกจะขึ้นอยู่กับปริมาณความผิดพลาดที่เกิดขึ้นระหว่างการส่งทางช่องทางการสื่อสารเชิงควอนตัม (Quantum Bit Error Rate: QBER) และความน่าจะเป็นของการเกิดความผิดพลาดภายในบล็อกข้อมูลซึ่งความน่าจะเป็นในการเกิดการผิดของบิต k บิต ภายในบล็อกขนาด N บิตแสดงดังสมการ [34]

$$P_k(N) = \binom{N}{k} e^k (1-e)^{N-1} \tag{4.17}$$

$P_k(N)$ คือความน่าจะเป็นที่เกิดความผิดพลาดจำนวน k บิตในบล็อกขนาด N บิต โดยขนาดของบล็อกที่เลือกใช้ในกระบวนการแก้ไขความผิดพลาดขึ้นอยู่กับประสิทธิภาพของการแก้ไขความผิดพลาดดังสมการ

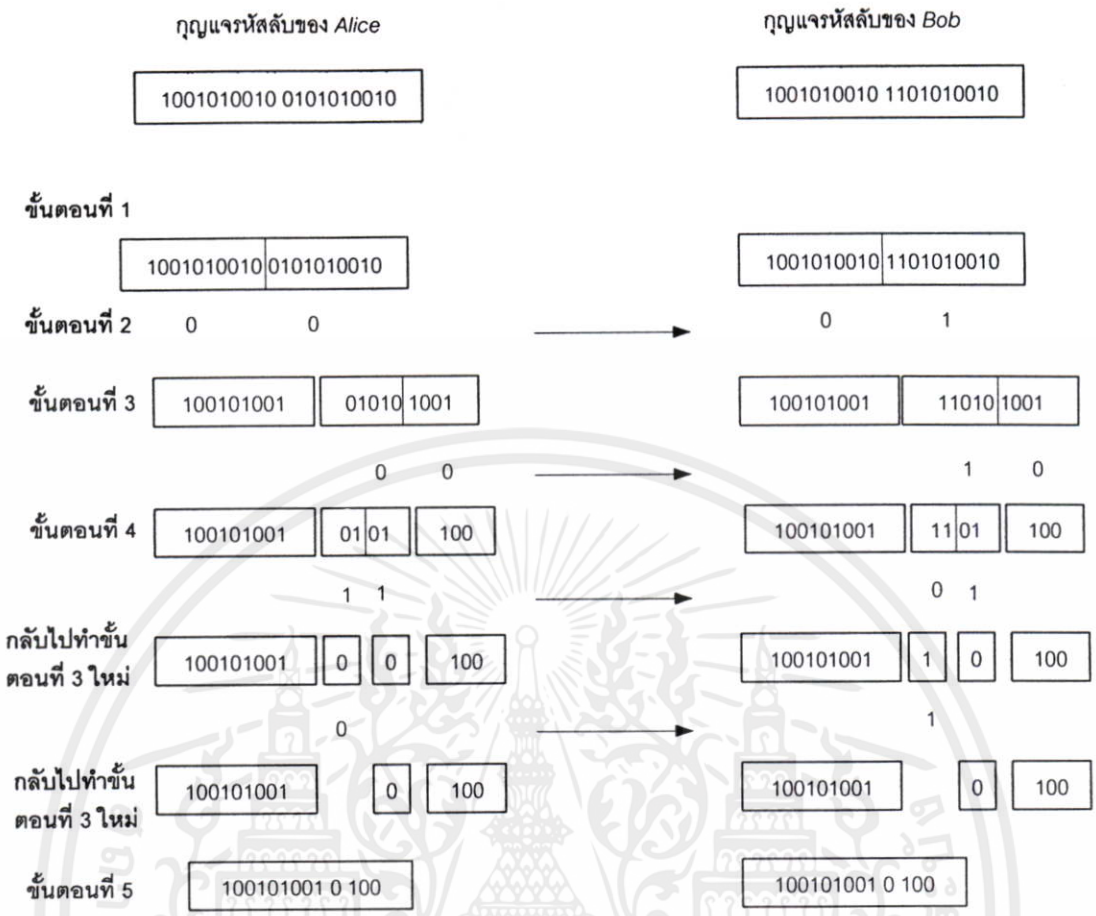
$$\eta(N) = \frac{(1-P_1(N))(N-1)}{N} \tag{4.18}$$

η คือประสิทธิภาพของการแก้ไขความผิดพลาด

N คือขนาดของบล็อก

$P_1(N)$ คือความน่าจะเป็นของการเกิดความผิดพลาดขึ้นหนึ่งบิตภายในบล็อกขนาด N บิต

ขั้นตอนที่ 2 *Alice* และ *Bob* หาพาริตี้บิตในแต่ละบล็อกและทำการเปรียบเทียบพาริตี้บิตเหล่านี้ เมื่อพบพาริตี้บิตที่แตกต่างกัน *Alice* และ *Bob* จะทราบทันที่ว่ากุญแจรหัสลับบิตที่ตนมีอยู่เกิดความผิดพลาด หากผลการเปรียบเทียบพาริตี้บิตมีความเหมือนกัน *Alice* และ *Bob* จะเก็บกุญแจรหัสลับบิตเหล่านั้นไว้พร้อมกับทิ้งกุญแจรหัสลับบิตในตำแหน่งสุดท้ายของทุกบล็อกทิ้งไป เพื่อลดข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* อาจจะได้รับระหว่างกระบวนการเปรียบเทียบพาริตี้บิต จากนั้นจะทำการเพิ่มขนาดของบล็อกและเปลี่ยนตำแหน่งของกุญแจรหัสลับบิต แล้วเริ่มดำเนินการตามขั้นตอนที่ 1 ใหม่



รูปที่ 4.6 ตัวอย่างการทำงานของโพรโทคอล BBBSS

ขั้นตอนที่ 3 หาก *Alice* และ *Bob* พบข้อผิดพลาดที่เกิดขึ้นภายในบล็อกกุญแจรหัสลับแล้ว ทั้ง *Alice* และ *Bob* จะทำการแบ่งบล็อกกุญแจรหัสลับนั้นออกเป็นสองส่วนเท่าๆ กัน จากนั้นจะทำการหาพาริตี้บิตของบล็อกที่ได้แบ่ง พร้อมกับนำพาริตี้บิตมาเปรียบเทียบกันใหม่อีกครั้ง เพื่อหากุญแจรหัสลับที่ผิดอยู่ในบล็อกย่อยใด หลังจากนั้น *Alice* และ *Bob* จะตัดกุญแจรหัสลับบิตตำแหน่งสุดท้ายของแต่ละบล็อกทิ้งไป

ขั้นตอนที่ 4 *Alice* และ *Bob* จะทำตามขั้นตอนที่ 3 จนกว่าจะพบตำแหน่งกุญแจรหัสลับบิตที่ผิดและแก้ไขบิตที่ผิดนั้นให้กลับมาถูกต้องพร้อมกับตัดกุญแจรหัสลับบิตในตำแหน่งสุดท้ายของบล็อกออก

ขั้นตอนที่ 5 *Alice* และ *Bob* จะนำกุญแจรหัสลับบิตที่ผ่านการแก้ไขความผิดพลาดและกุญแจรหัสลับบิตของบล็อกที่ไม่เกิดความผิดพลาดรวมเข้าด้วยกันอีกครั้ง จากนั้นจะทำการเพิ่มขนาดของบล็อกพร้อมกับสับเปลี่ยนตำแหน่งของกุญแจรหัสลับบิตที่ตนมีอยู่แล้วทำซ้ำตามขั้นตอนที่ 1 จนเหลืออัตราความผิดพลาดในปริมาณที่ยอมรับได้

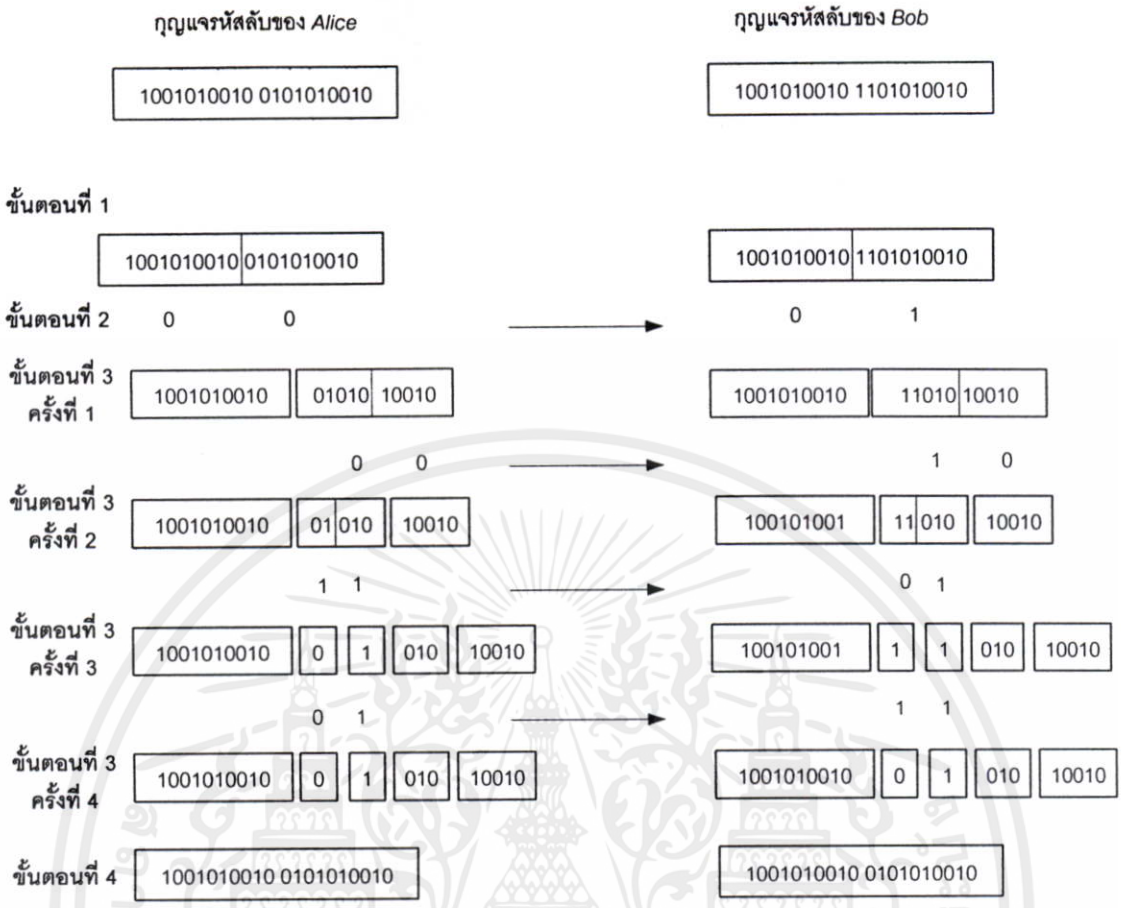
4.4.2 โพรโทคอล CASCADE

โพรโทคอล CASCADE เป็นโพรโทคอลที่ปรับปรุงมาจากโพรโทคอล BBBSS เนื่องจากในระหว่างกระบวนการแก้ไขความผิดพลาดของโพรโทคอล BBBSS นี้จะทำการตัดกุญแจรหัสลับบิตในตำแหน่งสุดท้ายของแต่ละบล็อกออก การตัดกุญแจรหัสลับบิตเหล่านี้ออกส่งผลให้โพรโทคอล BBBSS นี้มีความปลอดภัย สามารถลดข้อมูลเกี่ยวกับกุญแจรหัสลับบิตที่ *Eve* จะได้จากการเข้ามาขโมยระหว่างการแก้ไขความผิดพลาด แต่จะส่งผลต่อประสิทธิภาพในการแก้ไขความผิดพลาดของโพรโทคอลและจำนวนกุญแจรหัสลับบิตที่เหลือภายหลังจากการแก้ไขความผิดพลาด[12] โพรโทคอล CASCADE เป็นโพรโทคอลการแก้ไขความผิดพลาดเช่นเดียวกับโพรโทคอล BBBSS ที่อาศัยพาริตี้บิตในการตรวจสอบและแก้ไขความผิดพลาดที่เกิดขึ้น แต่โพรโทคอลนี้จะไม่ทำการตัดกุญแจรหัสลับบิตในตำแหน่งสุดท้ายของแต่ละบล็อกออก เพื่อเพิ่มประสิทธิภาพการแก้ไขความผิดพลาด โดยรายละเอียดของแต่ละขั้นตอนมีดังต่อไปนี้

ขั้นตอนที่ 1 การคำนวณหาขนาดของบล็อกและจำนวนครั้งในการวนซ้ำ (Pass) เพื่อหาขนาดของบล็อกที่เหมาะสมในการเปรียบเทียบพาริตี้บิตและจำนวนรอบในการทำงานทั้งหมดโดยใช้ค่าของอัตราการผิดพลาดของกุญแจรหัสลับบิตที่ส่งผ่านทางช่องทางการสื่อสารเชิงควอนตัม (e) ข้อดีของโพรโทคอลนี้คือขนาดของบล็อกจะสามารถปรับเปลี่ยนได้ ขึ้นอยู่กับอัตราความผิดพลาดที่เกิดจากการส่งกุญแจรหัสลับ โดยขนาดของบล็อกเริ่มต้น (Initial Block) หรือ N_0 นั้นจะคำนวณจากการประมาณการผิดของบิตภายในบล็อก ซึ่งความน่าจะเป็นที่จะเกิดการผิดของบิตจำนวน k บิตภายในบล็อกขนาด N บิต แสดงดังสมการ[34]

$$P_k(N) = \binom{N}{k} p^k (1-p)^{N-k} \tag{4.19}$$

พิจารณาขนาดของบล็อกและอัตราการผิดของชิฟคีย์ ผลคูณของขนาดของบล็อกและอัตราความผิดพลาดของกุญแจรหัสลับ (e) มีค่าอยู่ระหว่าง 0.7 ถึง 0.75 เช่น อัตราการผิดของกุญแจรหัสลับมีค่าเท่ากับ 0.01 จะใช้ขนาดของบล็อกเท่ากับ 73 บิต อัตราการผิดของกุญแจรหัสลับมีค่าเท่ากับ 0.05 ขนาดของบล็อกเท่ากับ 14 เป็นต้น [12] ซึ่งเมื่อทำการหาความน่าจะเป็นในการเกิดการผิดของบิตภายในบล็อกข้อมูลขนาด N บิต ตามสมการที่ (4.18) แสดงได้ดังตารางที่ 4.2 ซึ่งความน่าจะเป็นที่เกิดขึ้นนี้มีรูปแบบการกระจายโอกาสแบบปัวส์ซอง (Poisson Distribution) ที่ค่าเฉลี่ยเท่ากับ $ln(2)$ [35] จากสมการที่ (4.18) และตารางที่ 4.2 ความน่าจะเป็นของบล็อกข้อมูลขนาด N บิตจะมีจำนวนบิตผิดภายในบล็อกจำนวนคู่ดังสมการ



รูปที่ 4.7 ตัวอย่างการทำงานของโพรโทคอล CASCADE

ตารางที่ 4.2 ความน่าจะเป็นของจำนวนบิตผิดในบล็อกและการกระจายแบบปัวส์ซอง

จำนวนบิตผิดภายในบล็อก	ความน่าจะเป็นเท่ากับ 0.01 ขนาดของบล็อกเท่ากับ73	การกระจายโอกาสแบบปัวส์ซอง ค่าเฉลี่ยเท่ากับ *ln(2)*
0	0.4801	0.5
1	0.3540	0.3466
2	0.1287	0.1201
3	0.0308	0.0278
4	0.0054	0.0048
5	0.0008	0.0007
6 และ จำนวนบิตผิดอื่นๆ	0.0001	0.0001

$$P = \sum \frac{N!}{j!(N-j)!} e^j (1-e)^j \quad \text{โดยที่ } j = 0,2,4,... \tag{4.20}$$

e คืออัตราการผิดของกุญแจรหัสลับบิต P คือความน่าจะเป็นของการเกิดบิตผิดเป็นจำนวนคู่ภายในบล็อกขนาด N บิต

ถ้าผลคูณของขนาดของบล็อกและอัตราการผิดของคิวบิตมีค่าประมาณ $\ln(2)$ หรือ $N \times e \approx \ln(2)$ ดังนั้นความน่าจะเป็นของการเกิดความผิดพลาดเป็นจำนวนคู่ภายในบล็อกขนาด N บิตจะมีค่าประมาณ 0.625 [35] ส่วนขนาดของบล็อกเริ่มต้น N_0 จะหาได้ดังสมการ

$$N_0 = \frac{\ln(2)}{e} \tag{4.21}$$

N_0 คือขนาดของบล็อกเริ่มต้น

ขนาดของบล็อกถัดไปของโพรโทคอลCASCADE จะเพิ่มขนาดบล็อกเป็นสองเท่าของขนาดของบล็อกก่อนหน้าดังสมการ [12]

$$N_{i+1} = 2N_i \quad \text{โดยที่ } i = 0,1,2,.... \tag{4.22}$$

N_{i+1} เป็นขนาดของบล็อกในรอบที่ $i+1$ และขนาดของบล็อกมากที่สุดแสดงดังสมการ

$$N \geq \frac{l}{4} \tag{4.23}$$

l คือขนาดความยาวทั้งหมดของชิฟคีย์และ N_m คือขนาดบล็อกสุดท้ายของรอบปกติและมีขนาดของบล็อกเกินกว่า $1/4$ ของความยาวทั้งหมดของชิฟคีย์

หลังจากได้ขนาดของบล็อกทั้งหมด จำนวนรอบทั้งหมดในการวนซ้ำจะมีค่าเท่ากับจำนวนของขนาดบล็อกทั้งหมดที่หาได้รวมกับจำนวนรอบที่เพิ่มขึ้นมาอีกสองรอบ ซึ่งขนาดของบล็อกของแต่ละรอบในการวนซ้ำที่เพิ่มขึ้นมานี้จะมีขนาดเท่ากับขนาดของบล็อกสูงสุด โดยการเพิ่มจำนวนรอบของการวนซ้ำ เพื่อเพิ่มโอกาสที่ *Alice* และ *Bob* จะแก้ไขความผิดพลาดที่ยังเหลืออยู่ให้ได้มากที่สุดซึ่งจะช่วยเพิ่มประสิทธิภาพการทำงานของโพรโทคอล

ขั้นตอนที่ 2 *Alice* และ *Bob* แบ่งกุญแจรหัสลับของตนออกเป็นบล็อกตามขนาดที่หาได้จากขั้นตอนแรกจากนั้น *Alice* และ *Bob* จะหาพาริตี้บิตในแต่ละบล็อก

ขั้นตอนที่ 3 *Alice* ส่งพาริตี้บิตของตนไปให้ *Bob* และเมื่อ *Bob* ทำการเปรียบเทียบพาริตี้บิตเหล่านี้แล้วหากพบพาริตี้บิตมีความแตกต่างกันทั้ง *Alice* และ *Bob* จะทราบทันทีว่ามีกุญแจรหัสลับบิตแตกต่างกันอยู่ภายในบล็อกนั้นและจะทำการแบ่งบล็อกกุญแจรหัสลับบล็อกนั้นออกเป็นสองบล็อกๆ ละเท่าๆ กันแล้ว *Alice* และ *Bob* จะทำการหาค่าพาริตี้บิตและเปรียบเทียบพาริตี้บิตเหล่านี้อีกครั้ง ซึ่งกระบวนการนี้จะดำเนินซ้ำจนกว่า *Alice* และ *Bob* จะทราบตำแหน่งของบิตที่ผิดและทำการแก้ไขบิตนั้น หากผลการเปรียบเทียบพาริตี้บิตมีความเหมือนกัน *Alice* และ *Bob* จะดำเนินการในรอบการวนซ้ำถัดไปจะกว่าจะดำเนินการเสร็จทั้งหมด

ขั้นตอนที่ 4 หาก *Alice* และ *Bob* เพิ่มขนาดของบล็อกตามขนาดของบล็อกที่ได้หาไว้ก่อนหน้าตามจำนวนรอบการวนซ้ำ โดยอาจจะทำการสลับตำแหน่งของกุญแจรหัสลับบิตด้วยเพื่อเพิ่มประสิทธิภาพการหาความผิดพลาด จากนั้นจะดำเนินการตามขั้นตอนที่ 2 ถึงขั้นตอนที่ 4 ใหม่จนกว่าจะสิ้นสุดจำนวนรอบของการวนซ้ำ (Pass) หรือจนกว่าจะเหลืออัตราการผิดของกุญแจรหัสลับเป็นที่ยอบรับได้โดยการทำงานของโพรโทคอล CASCADE แสดงดังรูปที่ 4.7

หลังจากที่ทำการแก้ไขความผิดพลาดด้วยโพรโทคอล CASCADE เสร็จเรียบร้อยแล้ว กระบวนการตรวจสอบความผิดพลาดที่อาจจะยังเหลืออยู่จะถูกดำเนินต่อเพื่อยืนยันว่ากุญแจรหัสลับบิตที่ได้มีความเหมือนกันหรือมีความผิดพลาดเหลืออยู่น้อยที่สุด ซึ่งการหาโอกาสที่จะมีกุญแจรหัสลับบิตที่ผิดเหลืออยู่จะดำเนินการโดย *Alice* และ *Bob* จะสุ่มกุญแจรหัสลับบิตที่ผ่านการแก้ไขความผิดพลาดแล้วนำมารวมกัน จากนั้นจะทำการแบ่งออกเป็นบล็อกพร้อมกับหาค่าพาริตี้บิตในแต่ละบล็อกแล้วจึงนำพาริตี้บิตเหล่านี้มาเปรียบเทียบ หากพาริตี้บิตที่เปรียบเทียบทั้งหมด (w บิต) มีความเหมือนกัน *Alice* และ *Bob* จะมีค่าความน่าจะเป็นที่จะมีกุญแจรหัสลับที่ต่างกันเท่ากับ 2^{-w} [36] บิตที่สุ่มมาทั้งหมดเหล่านี้จะถูกทิ้งไปเนื่องจากเปิดเผยให้แก่บุคคลที่สามได้รับทราบ นอกจากจะหาจำนวนกุญแจรหัสที่มีโอกาสเกิดการผิดพลาดอยู่แล้วจำนวนบิตที่เปิดเผยทั้งหมดจากการแก้ไขความผิดพลาดก็เป็นอีกหนึ่งสิ่งที่ถูกนำมาพิจารณาด้วยเช่นกัน ซึ่งหากจำนวนบิตที่เปิดเผยมีจำนวนมากโอกาสที่ *Eve* จะนำข้อมูลนี้ไปใช้สร้างหรือทำสำเนากุญแจรหัสลับบิตใหม่ขึ้นมาก็ยิ่งมีโอกาสสูงขึ้นเช่นกัน โดยจำนวนบิตที่เปิดเผยแสดงดังสมการ [37]

$$d = l(1+\xi)H(e) \tag{4.24}$$

d คือจำนวนบิตที่เปิดเผยทั้งหมด l คือจำนวนชิฟคีย์ (Sifted Key) และ ξ คือ Overhead Factor หรือจำนวนบิตที่เปิดเผยนอกเหนือจากพาริตี้บิตที่เปิดเผยจากกระบวนการแก้ไขความผิดพลาด

4.4.3 โพรโทคอล Winnow

โพรโทคอล Winnow เป็นหนึ่งในโพรโทคอลที่ใช้แก้ไขความผิดพลาดในกระบวนการกระจายกุญแจรหัสลับเชิงควอนตัม โดยใช้พาริตี้บิตตรวจสอบความผิดพลาดที่เกิดขึ้นระหว่างการส่งกุญแจรหัสลับ ซึ่งพาริตี้บิตจะตรวจพบความผิดพลาดที่เกิดขึ้นกับกุญแจรหัสลับบิตภายในบล็อกเป็นจำนวนคี่แต่จะไม่พบความผิดพลาดที่เกิดขึ้นหากมีการผิดเป็นจำนวนคู่ หากพบความผิดพลาดเกิดขึ้นโพรโทคอลนี้จะใช้รหัสแฮมมิงช่วยแก้ไขความผิดพลาดที่เกิดขึ้น ซึ่งรหัสแฮมมิงจะสามารถแก้ไขความผิดพลาดที่เกิดขึ้นได้หนึ่งบิตต่อบล็อกกุญแจรหัสลับบิต N บิตและสามารถตรวจจับข้อผิดพลาดที่เกิดขึ้นภายในบล็อกข้อมูลนั้นได้มากกว่าสองบิต การทำงานของโพรโทคอล Winnow และรายละเอียดของแต่ละขั้นตอนมีดังต่อไปนี้ [38]

4.4.3.1 การเปรียบเทียบพาริตี้บิต

การเปรียบเทียบพาริตี้บิตเพื่อตรวจสอบความผิดพลาดที่เกิดขึ้นภายในบล็อกกุญแจรหัสลับบิต หากพาริตี้บิตที่นำมาเปรียบเทียบกันเกิดความแตกต่างกัน แสดงว่าภายในบล็อกกุญแจรหัสลับบิตระหว่าง *Alice* และ *Bob* มีกุญแจรหัสลับบิตแตกต่างกันเป็นจำนวนคี่ ซึ่งอาจจะมีความแตกต่างกันหนึ่งบิต สามบิตหรือห้าบิต เป็นต้น แต่พาริตี้บิตที่นำมาเปรียบเทียบมีความเหมือนกัน *Alice* และ *Bob* จะไม่ทราบว่ากุญแจรหัสลับของตนมีความผิดพลาดเกิดขึ้นหรือไม่ โดยขนาดของบล็อก N ที่ใช้ในการเปรียบเทียบพาริตี้บิตสามารถแสดงได้ดังสมการ

$$N = 2^m \qquad \text{โดยที่} \quad m = 3,4,5,.... \tag{4.25}$$

หลังจากที่ทำการเปรียบเทียบพาริตี้บิตแล้ว *Alice* และ *Bob* จะทำการตัดกุญแจรหัสลับบิตตำแหน่งสุดท้ายของบล็อกทุกบล็อกออกเพื่อเป็นการลดข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* จะได้รับระหว่างกระบวนการเปรียบเทียบพาริตี้บิตดังนั้นขนาดของบล็อกใหม่มีดังสมการ

$$N_h = 2^m - 1 \quad \text{โดยที่ } m = 3,4,5,.... \quad \text{หรือ}$$

$$N_h = N - 1 \tag{4.26}$$

N_h คือขนาดของบล็อก และ m คือขนาดของซินโดรม

ตัวอย่างการหาขนาดของบล็อกหากทำการเปรียบเทียบพาริตี้โดยใช้ m เท่ากับ 3 จะทำการแบ่งบล็อกกุญแจรหัสลับออกเป็นบล็อกโดยขนาดของบล็อกจะเท่ากับแปดบิต เมื่อเปรียบเทียบพาริตี้บิตแล้ว *Alice* และ *Bob* จะตัดกุญแจรหัสลับบิตตำแหน่งสุดท้ายของบล็อกทุกบล็อกออก ซึ่งขนาดของบล็อกจะลดลงเหลือเจ็ดบิต

4.4.3.2 การแก้ไขความผิดพลาดด้วยโพรโทคอล Winnow

การเปรียบเทียบพาริตี้บิตจะเป็นการหาความผิดพลาดที่อาจจะเกิดขึ้นภายในบล็อกกุญแจรหัสลับ หากผลการเปรียบเทียบมีความเหมือนกัน *Alice* และ *Bob* จะเพิ่มขนาดของบล็อกและทำการเปรียบเทียบพาริตี้ใหม่อีกครั้ง แต่ถ้าผลการเปรียบเทียบพาริตี้บิตของบล็อกมีความแตกต่างกัน ทำให้ *Alice* และ *Bob* ทราบทันทีว่าในบล็อกกุญแจรหัสลับนั้นมีกุญแจรหัสลับที่แตกต่างกันอยู่ ดังนั้น *Alice* และ *Bob* จะใช้รหัสแฮมมิงเข้ามาแก้ไขความผิดพลาดที่เกิดขึ้นโดยการแก้ไขความผิดพลาดมีขั้นตอนการทำงานดังต่อไปนี้

- **การสร้างเมทริกซ์ตรวจสอบพาริตี้**

เมทริกซ์ตรวจสอบพาริตี้ (Parity Check Metric: H) เป็นเมทริกซ์ที่ถูกสร้างขึ้นมาเพื่อหาค่าซินโดรม ซึ่งค่าซินโดรมนี้จะบ่งบอกถึงการผิดของบิตที่เกิดขึ้นหรือไม่และจะบอกถึงตำแหน่งของบิตที่ผิดได้อย่างถูกต้องเมื่อมีการผิดเกิดขึ้นหนึ่งบิตต่อบล็อก โดยซินโดรมเกิดจากผลคูณระหว่างเมทริกซ์ตรวจสอบพาริตี้และบล็อกกุญแจรหัสลับที่เกิดความผิดพลาด หลังจากการเปรียบเทียบพาริตี้บิต โดยเมทริกซ์ตรวจสอบพาริตี้สามารถสร้างขึ้นได้ดังสมการ

$$H_{i,j}^{(m)} = \left[\frac{j}{2^{i-1}}\right] (\mathrm{mod}\, 2) \tag{4.27}$$

i และ j คือแถวและหลักของเมทริกซ์ตรวจสอบพาริตี้และ m คือขนาดของซินโดรม ตัวอย่างของเมทริกซ์ตรวจสอบพาริตี้ขนาด 3×7 และ 4×15 มีดังนี้

$$H_{i,j}^{3} = \begin{bmatrix} 1010101 \\ 0110011 \\ 0001111 \end{bmatrix}$$

$$H_{i,j}^{4} = \begin{bmatrix} 101010101010101 \\ 011001100110011 \\ 000111100001111 \\ 000000011111111 \end{bmatrix}$$

- **คำนวณค่าซินโดรม**

การคำนวณหาค่าซินโดรมหาได้จาก การนำเมทริกซ์ตรวจสอบพาริตี้คูณกับค่ากุญแจรหัสลับบิตที่ได้หลังจากการเปรียบเทียบพาริตี้บิต ซึ่งค่าซินโดรมแสดงดังสมการ

$$S_i = \left(\sum_{j=1}^{N_h} X_j h_{i,j}^m \right) \bmod 2 \tag{4.28}$$

$i \in \{A, B\}$ หมายถึง S_A คือค่าซินโดรมของ *Alice* และ S_B คือค่าซินโดรมของ *Bob*

N_h คือขนาดของบล็อกข้อมูลภายหลังจากการเปรียบเทียบพาริตี้บิต

- **ขั้นตอนการเปรียบเทียบซินโดรมและการแก้ไขความผิดพลาด**

ขั้นตอนการเปรียบเทียบซินโดรม เป็นการหาตำแหน่งของกุญแจรหัสลับบิตที่แตกต่างกันระหว่าง *Alice* และ *Bob* โดย *Alice* จะส่งค่าซินโดรมผ่านทางช่องสื่อสารสาธารณะมาให้ *Bob* หลังจากนั้น *Bob* จะนำค่าซินโดรมที่รับได้มาทำการบวกแบบมอดุโล 2 กับค่าซินโดรมของตน ซึ่งผลที่ได้จากการเปรียบเทียบซินโดรมจะบอกถึงความผิดพลาดที่เกิดขึ้นภายในบล็อกกุญแจรหัสลับบิต หากผลการเปรียบเทียบมีค่าเท่ากับศูนย์แสดงว่าบล็อกกุญแจรหัสลับบิตของ *Alice* และ *Bob* มีความเหมือนกันแต่ถ้าผลการเปรียบเทียบซินโดรมมีค่าไม่เท่ากับศูนย์ ค่าที่ได้จากการเปรียบเทียบจะบอกถึงตำแหน่งของกุญแจรหัสลับบิตที่ผิดทำให้ *Bob* สามารถแก้ไขบิตที่ผิดให้กลับมาถูกต้องได้ โดยการเปรียบเทียบซินโดรมแสดงดังสมการ

$$S_d = S_A \oplus S_B \neq \{0\}^m \tag{4.29}$$

S_d คือผลการเปรียบเทียบซินโดรมโดยจะบ่งบอกถึงความเหมือนหรือความแตกต่างของกุญแจรหัสลับบิตดังนี้

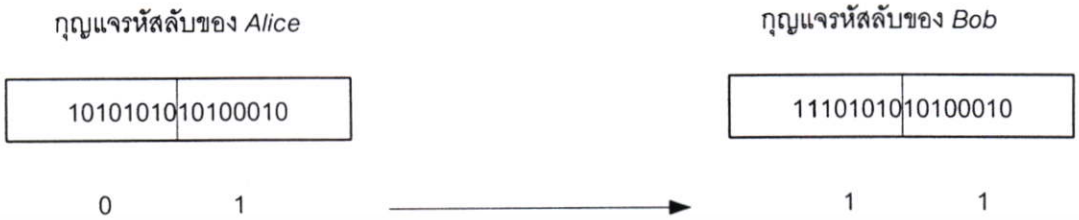
- ในกรณีที่ S_d มีค่าเท่ากับศูนย์แสดงว่ากุญแจรหัสลับบิตของทั้ง *Alice* และ *Bob* มีความเหมือนกัน
- ในกรณีที่ S_d มีค่าเท่ากับแสดงว่ามีความผิดพลาดเกิดขึ้นภายในบล็อกและ *Bob* จะทราบว่าตำแหน่งกุญแจรหัสลับบิตที่ผิดภายในบล็อกนั้น

- **การลดข้อมูลเกี่ยวกับกุญแจรหัสลับ**

หลังจากที่ทำการแก้ไขความผิดพลาด การลดข้อมูลเกี่ยวกับกุญแจรหัสลับเป็นกระบวนการลดโอกาสที่บุคคลที่สามจะนำข้อมูลเกี่ยวกับกุญแจรหัสลับที่ขโมยได้ระหว่างการแก้ไขความผิดพลาดไปสร้างหรือทำสำเนากุญแจรหัสลับขึ้นมาใหม่ ซึ่งโพรโทคอล Winnow นี้จะลดข้อมูลเกี่ยวกับกุญแจรหัสลับ โดยทำการตัดบิตของกุญแจรหัสลับที่ผ่านการแก้ไขความผิดพลาดบางส่วนออกจากบล็อก ซึ่งจะตัดกุญแจรหัสลับบิตในตำแหน่ง $\{2^j\}$ โดยที่ $j = 0,1,2,...,m-1$

- **จำนวนบิตที่ส่งผ่านเครือข่ายสาธารณะ**

หลังจากที่ทำการแก้ไขความผิดพลาดระหว่างกุญแจรหัสลับบิตที่ผิดของ *Alice* และ *Bob* เสร็จเรียบร้อยแล้วนั้น การวัดปริมาณข้อมูลที่ส่งผ่านเครือข่ายสาธารณะเป็นอีกหนึ่งตัวแปรที่ใช้วัด



รูปที่ 4.8 การแบ่งบล็อกกุญแจรหัสลับและการหาพาริตี้บิตของโพรโทคอล Winnow

ประสิทธิภาพของโพรโทคอลแก้ไขความผิดพลาด โดยโพรโทคอล Winnow เป็นหนึ่งในโพรโทคอลที่มีการติดต่อสื่อสารกัน (Interactivity) เช่นเดียวกับโพรโทคอลCASCADE โดยโพรโทคอล Winnow นี้จะทำการเปรียบเทียบพาริตี้บิตเพื่อหาความผิดพลาดที่เกิดขึ้นภายในบล็อก หากพบความผิดพลาดโพรโทคอลWinnow จะแก้ไขความผิดพลาดโดยใช้หลักการของรหัสแฮมมิง เข้ามาช่วยในแก้ไขความผิดพลาด โดยจำนวนบิตที่ส่งจะขึ้นอยู่กับขนาดของซินโดรมของรหัสแฮมมิง โดยจำนวนบิตที่ส่งทั้งหมดจะแสดงดังสมการ

$$d = \sum_{i=1}^{n} \frac{l}{N} + m \times N_{Error} \tag{4.30}$$

n คือจำนวนรอบในการวนซ้ำ (Pass) d คือจำนวนบิตที่ส่งผ่านช่องสื่อสารสาธารณะทั้งหมด l คือจำนวนชิฟคีย์ทั้งหมด N คือขนาดของบล็อก และ N_{Error} คือจำนวนบล็อกที่มีพาริตี้บิตแตกต่างกัน

ตัวอย่างกำหนดให้ *Alice* และ *Bob* มีกุญแจรหัสลับจำนวนทั้งสิ้น 16 บิต โดยมีความผิดพลาดเกิดขึ้นหนึ่งบิต การทำงานของโพรโทคอล Winnow มีดังต่อไปนี้

กำหนดให้กุญแจรหัสลับบิตของ *Alice* มีดังต่อไปนี้ “1010101010100010” และกุญแจรหัสลับของ *Bob* มีดังต่อไปนี้ “1110101010100010” โดยบิตที่ตัวอักษรหนาจะแสดงตำแหน่งของกุญแจรหัสลับบิตที่เกิดความผิดพลาด และให้ *Alice* และ *Bob* ใช้รหัสแฮมมิง (7,4) หรือ m เท่ากับ 3 ขนาดของบล็อกเริ่มแรกก่อนการเปรียบเทียบพาริตี้บิตจะเท่ากับ 8 บิต

ขั้นตอนที่ 1 *Alice* และ *Bob* แบ่งบล็อกกุญแจรหัสลับของตนโดยขนาดของบล็อกเท่ากับ 8 บิต หลังจากนั้น *Alice* และ *Bob* จะทำการเปรียบเทียบพาริตี้บิตของแต่ละบล็อก ซึ่งการแบ่งกุญแจรหัสลับออกเป็นบล็อกขนาด 8 บิตและพาริตี้บิตของแต่ละบล็อกแสดงดังรูปที่ 4.8

ขั้นตอนที่ 2 หลังจากเปรียบเทียบพาริตี้บิต *Alice* และ *Bob* จะทำการตัดบิตตำแหน่งสุดท้ายของบล็อกออกซึ่งกุญแจรหัสลับของ *Alice* ที่เหลืออยู่มีดังนี้ “1010101 1010001” และกุญแจรหัส

ลับของ *Bob* ที่เหลืออยู่มีดังนี้ "1110101 1010001" โดยจากรูปที่ 4.8 พาริตี้บิตของบล็อกแรกมีความแตกต่างกันทำให้ *Alice* และ *Bob* ทราบทันทีว่ามีกุญแจรหัสลับที่ผิดอยู่ภายในบล็อกนั้น ดังนั้น *Alice* และ *Bob* จะนำรหัสแฮมมิง (7,4) มาแก้ไขความผิดพลาดโดยการเปรียบเทียบซินโดรมที่ได้จากรหัสแฮมมิง ซึ่งซินโดรมของ *Alice* และ *Bob* แสดงดังต่อไปนี้

จากสมการที่ (4.28) จะได้

$$S_i = \left(\sum_{j=1}^{N_h} X_j h_{i,j}^m \right) \bmod 2 \quad \text{โดยที่ } i \in \{A, B\}$$

$$S_A = \begin{bmatrix} 1010101 \\ 0110011 \\ 0001111 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = [0\,0\,0]$$

$$S_B = \begin{bmatrix} 1010101 \\ 0110011 \\ 0001111 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = [0\,1\,0]$$

S_A คือซินโดรมของ *Alice* และ S_B คือซินโดรมของ *Bob*

ขั้นตอนที่ 3 *Alice* และ *Bob* ทำการเปรียบเทียบซินโดรมและแก้ไขความผิดพลาดที่เกิดขึ้นภายในบล็อกจากตำแหน่งที่ได้จากผลการเปรียบเทียบซินโดรม ซึ่งผลการเปรียบเทียบซินโดรมแสดงดังนี้

$$\begin{aligned} S_D &= S_A \oplus S_B \\ &= [0\,0\,0] \oplus [0\,1\,0] \\ &= [0\,1\,0] \end{aligned}$$

S_D คือผลการเปรียบเทียบซินโดรม

ซึ่งจากผลการเปรียบเทียบค่าซินโดรมจะทำให้ *Bob* ทราบตำแหน่งกุญแจรหัสลับบิตที่ผิดคือตำแหน่งที่สองในบล็อกกุญแจรหัสลับ

ขั้นตอนที่ 4 เมื่อ *Bob* แก้ไขกุญแจรหัสลับบิตผิดในบล็อกกุญแจรหัสลับของตนเรียบร้อยแล้วนั้น *Alice* และ *Bob* จะทำการตัดกุญแจรหัสลับบิตภายในบล็อกนั้นออกเพื่อลดข้อมูลเกี่ยวกับกุญแจรหัสลับที่ *Eve* อาจจะได้รับจากการเข้ามาขโมยข้อมูลเกี่ยวกับกุญแจรหัสลับภายในช่องสื่อสารสาธารณะแก้ไขความผิดพลาด ซึ่งการตัดกุญแจรหัสลับบิตจะตัดในตำแหน่ง $\{2^j\}$ โดย $j = 0,1,2,...,m-1$ เมื่อ m เท่ากับ 3 จะได้ตำแหน่งที่ *Alice* และ *Bob* ต้องตัดคือ ตำแหน่งที่ "1" ตำแหน่งที่ "2" และตำแหน่งที่ "4" ดังนั้นกุญแจรหัสลับของ *Alice* และ *Bob* เหลืออยู่จะมีดังนี้ "1101 1010001" และ "1101 1010001" ตามลำดับ

4.4.4 การแก้ไขความผิดพลาดด้วยรหัสบล็อกเชิงเส้นตามวิธีของฟุรุคาวา

การแก้ไขความผิดพลาดด้วยรหัสบล็อกเชิงเส้นตามวิธีของฟุรุคาวา [14] เป็นอีกรูปแบบหนึ่งของโพรโทคอลที่มีการติดต่อสื่อสารกัน (Interactivity) โดยโพรโทคอลที่พัฒนาขึ้นนี้เป็นการนำรหัสแฮมมิงมาช่วยในการแก้ไขความผิดพลาดหากพบความผิดพลาดเกิดขึ้นในบล็อกกุญแจรหัสลับภายหลังจากการเปรียบเทียบพาริตี้บิต โดยการแก้ไขความผิดพลาดแสดงการทำงานดังขั้นตอนต่อไปนี้

ขั้นตอนที่ 1 *Alice* และ *Bob* แบ่งกุญแจรหัสลับบิตของตนออกเป็นบล็อก ซึ่งขนาดของบล็อกสามารถหาได้ตามขั้นตอนต่อไปนี้

ความน่าจะเป็นที่บล็อกขนาด N บิตจะเกิดความผิดพลาดขึ้นเป็นจำนวนคู่แสดงดังสมการ

$$P(N,e) = \sum_{k=0}^{(N/2)-1} \binom{N}{2k+1} e^{2k+1}(1-e)^{N-2k-1} = \frac{1}{2}(1-(1-2e)^N) \tag{4.31}$$

N คือขนาดของบล็อกและ e คืออัตราความผิดพลาดระหว่างการส่งกุญแจรหัสลับบิตทางช่องทางการสื่อสารเชิงควอนตัม

ความน่าจะเป็นที่ความผิดพลาดจะถูกแก้ไขภายในบล็อกขนาด N แสดงดังสมการ

$$P_{err}(N,e) = Ne(1-e)^{N-1} + \sum_{k=1}^{(N/2)-1} \binom{N}{2k+1} e^{2k+1}(1-e)^{N-2k-1}\left(\frac{2k+1}{N} - \frac{N-2k-1}{N}\right) \tag{4.32}$$

อัตราการความสามารถในการแก้ไขความผิดพลาดแสดงดังสมการ

$$\eta = \frac{P_{err}(N,e)}{1+P(N,e)\log_2(N)} \tag{4.33}$$

η คืออัตราการความสามารถในการแก้ไขความผิดพลาด

ขนาดของบล็อก (N) ในการแก้ไขความผิดพลาดจะมีค่าเท่ากับขนาดของบล็อกที่มีอัตราการแก้ไขความผิดพลาดมากที่สุด

โดยขนาดของบล็อกจะมีค่าดังสมการ

$$N = 2^m \qquad \text{โดยที่ } m = 3,4,5,.... \tag{4.34}$$

ขั้นตอนที่ 2 *Alice* และ *Bob* ทำการแบ่งกุญแจรหัสลับของตนออกเป็นบล็อกตามขนาดของบล็อกที่ได้จากขั้นตอนที่ 1 แล้วหลังจากนั้นจึงทำการหาพาริตี้บิตของแต่ละบล็อก

ขั้นตอนที่ 3 *Alice* และ *Bob* เปรียบเทียบพาริตี้บิตที่ได้จากขั้นตอนที่ 2 หากไม่พบพาริตี้บิตที่แตกต่างกันเลย *Alice* และ *Bob* จะกระทำตามขั้นตอนที่ 1 ใหม่โดยอาจจะเพิ่มขนาดของบล็อก รวมทั้งเปลี่ยนตำแหน่งของกุญแจรหัสลับ แต่ถ้าผลการเปรียบเทียบพบพาริตี้บิตที่แตกต่างกัน *Alice* และ *Bob* จะทำการแก้ไขความผิดพลาดที่เกิดขึ้นตามขั้นตอนต่อไปนี้

การแก้ไขความผิดพลาดขั้นตอนที่ 1

กำหนดให้ $X = x_1, x_2, ..., x_n$ เป็นกุญแจรหัสลับของ *Alice* ที่มีพาริตี้บิตแตกต่างจากพาริตี้บิตของกุญแจรหัสลับของ *Bob* ในตำแหน่งบล็อกที่ตรงกันโดยให้ n คือขนาดของบล็อกมีค่าเท่ากับความยาวของบล็อกที่นำมาเปรียบเทียบพาริตี้บิตลบหนึ่ง ($N-1$) m คือจำนวนพาริตี้บิตของรหัสแบบบล็อกเชิงเส้นและ k คือจำนวนข้อมูลที่จะนำมาเข้ารหัสแบบบล็อกเชิงเส้น หลังจากนั้น *Alice* ทำการสุ่มจำนวนสุ่ม $U = u_1, u_2, .., u_k$ โดยที่ $k = n - m$ และ U คือข้อมูลที่จะถูกนำมาเข้ารหัสแฮมมิงเมื่อนำจำนวนสุ่ม U ไปผ่านกระบวนการเข้ารหัสจะได้คำรหัส W โดยที่ $W = u_1, u_2, u_3, ..., u_k, c_1, c_2, ..., c_m$ และ $c_1, c_2, ..., c_m$ คือพาริตี้บิตของคำรหัส

ขั้นตอนการแก้ไขความผิดพลาดขั้นตอนที่ 2

Alice นำคำรหัสใหม่ที่สร้างใหม่ W มาทำการรวมกับรหัสลับของตนแบบมอดุโล 2 (Modulo-2) กับกุญแจรหัสลับของตนดังนี้

$$Y = X \oplus W \tag{4.35}$$

ซึ่งหลังจากนั้น *Alice* จะได้คำรหัสลับใหม่ Y และจะทำการส่งคำรหัสใหม่ Y นี้ไปยัง *Bob* ผ่านทางช่องสื่อสารสาธารณะ

ขั้นตอนการแก้ไขความผิดพลาดขั้นตอนที่ 3

Bob นำคำรหัสที่ได้รับ Y มาทำรวมกับกุญแจรหัสลับของตน $Z = z_1, z_2, ..., z_n$ แบบมอดุโล 2 เพื่อสร้างคำรหัสใหม่ดังสมการ

$$\begin{aligned} V &= Y \oplus Z \\ &= X \oplus W \oplus Z \\ &= (X \oplus Z) \oplus W \end{aligned} \tag{4.36}$$

จากสมการที่ (4.36) หากกุญแจรหัสลับของ *Alice* และ *Bob* เหมือนกันจะทำให้ *Bob* ได้รับคำรหัส W เมื่อนำคำรหัส W มาถอดรหัสจะได้ซินโดรมที่มีค่าเท่ากับศูนย์ ถ้ากุญแจรหัสลับของ *Alice* และ *Bob* มีความแตกต่างกันจะทำให้คำรหัส W เกิดความผิดพลาด กำหนดให้ E เป็นเวกเตอร์ความผิดพลาดที่เกิดขึ้นภายในบล็อกกุญแจรหัสลับระหว่าง *Alice* และ *Bob* เมื่อนำคำรหัส W ที่เกิดการผิดพลาดมาผ่านเข้าสู่กระบวนการถอดรหัสแฮมมิง หลังจากนั้น *Bob* จะได้รับจำนวนสุ่ม U' ซึ่งการที่หาตำแหน่งกุญแจรหัสลับบิตที่ผิดของ *Bob* เริ่มจากนำจำนวนสุ่ม U' ผ่านเข้าสู่วงจรเข้ารหัสแฮมมิงโดยจะได้คำรหัส W' และเมื่อนำไปรวมกับ V แบบมอดุโล 2 จะได้

$$\begin{aligned} Q &= V \oplus W' \\ &= (Y \oplus Z) \oplus W' \\ &= (X \oplus W \oplus Z) \oplus W' \\ &= (X \oplus Z) \oplus (W \oplus W') \end{aligned} \tag{4.37}$$

ซึ่งถ้า Q มีค่าเท่ากับ "0" เสดงว่ากุญแจรหัสลับของ *Alice* และ *Bob* ในบล็อกขนาด $N-1$ มีความเหมือนกัน ดังนั้นความผิดพลาดที่เกิดขึ้นจะอยู่ในตำแหน่งที่ N ภายในบล็อกกุญแจรหัสลับ แต่ถ้า Q มีค่าไม่เท่ากับศูนย์ตำแหน่งที่กุญแจรหัสลับภายในบล็อกของ Q เป็นบิต "1" คือตำแหน่งบิตที่ผิด ซึ่งจะทำให้ *Bob* แก้ไขบิตที่ผิดนั้นได้อย่างถูกต้อง

การวัดข้อมูลเกี่ยวกับกุญแจรหัสลับที่ส่งผ่านเครือข่ายสาธารณะของโพรโทคอลฟุรุคาวาสามารถแสดงได้ดังสมการ

$$d = \sum_{i=1}^{n} \left(\frac{l}{N_i} + (N_i - k)\right) \tag{4.38}$$

d คือจำนวนข้อมูลที่เปิดเผยระหว่างกระบวนการแก้ไขความผิดพลาด n คือจำนวนรอบของการวนซ้ำ (Pass) N_i คือขนาดของบล็อกในการแก้ไขความผิดพลาดรอบที่ i และ k คือขนาดของบิตสุ่มที่สุ่มขึ้นเพื่อใช้ในการเข้ารหัสแฮมมิง

4.5 การแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง

การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) เป็นการส่งกุญแจรหัสลับในรูปแบบจำนวนจริงที่กระจายตัวแบบเกาส์ แทนรูปแบบของกุญแจรหัสลับบิตเหมือนระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) ซึ่งกุญแจรหัสลับในรูปแบบจำนวนจริงนี้จะเกิดความผิดพลาดได้ง่ายและยากที่จะแก้ไขความผิดพลาดให้กุญแจรหัสลับกลับมาถูกต้อง ดังนั้นการแก้ไขความผิดพลาดที่เกิดขึ้นนี้จึงต้องทำการเปลี่ยนกุญแจรหัสลับที่อยู่ในรูปจำนวนจริงที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิตดังระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) โดยใช้วิธีการแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) ซึ่งผลการเปลี่ยนกุญแจรหัสลับด้วยวิธีนี้ จะทำให้ผู้ส่งและผู้รับมีกุญแจรหัสลับบิตแต่ยังคงมีความผิดพลาดเกิดขึ้นอยู่ภายในกุญแจรหัสลับบิตเหล่านั้น เพื่อทำการแก้ไขหลังจากนั้น *Alice* และ *Bob* จะเลือกใช้โพรโทคอลแก้ไขความผิดพลาดใดโพรโทคอลหนึ่งมาแก้ไขกุญแจรหัสลับบิตที่ผิดให้กลับมาถูกต้อง โดยวิธีการแก้ไขข้อผิดพลาดแบบสไลซ์มีการทำงานดังนี้

4.5.1 การแก้ไขข้อผิดพลาดแบบสไลซ์

การแก้ไขข้อผิดพลาดแบบสไลซ์เป็นวิธีการจัดการชิฟคีย์ (Sifted Key) ในรูปแบบจำนวนจริงให้อยู่ในรูปแบบไบนารี (Binary) เพื่อให้กุญแจรหัสลับบิตที่ได้มีความผิดพลาดน้อยที่สุดและเพื่อแก้ไขความผิดพลาดที่ยังคงเหลืออยู่ *Alice* และ *Bob* จะใช้โพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมเช่น โพรโทคอล CASCADE โพรโทคอล Winnow เป็นต้นมาช่วยแก้ไขความผิดพลาดให้ความผิดพลาดที่เกิดขึ้นเหลือน้อยที่สุดหรืออยู่ในอัตราที่ยอมรับได้

การทำงานของการแก้ไขข้อผิดพลาดแบบสไลซ์เริ่มจาก *Alice* จะกำหนดฟังก์ชันสไลซ์ (Slices Function) โดยให้สไลซ์ (Slice: $S(x)$) คือฟังก์ชันของกุญแจรหัสลับของ *Alice* ซึ่งเวกเตอร์ของสไลซ์สามารถเขียนได้ดังต่อไปนี้

$$S_{1,2,3,...,m}(x) = (S_1(x), S_2(x), S_3(x), ..., S_m(x)) \tag{4.39}$$

สมการที่ (4.39) นี้เป็นสมการพื้นฐานที่ใช้เปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Alice* จากตัวเลขจำนวนจริงเป็นตัวเลขไบนารี่ การประมาณค่าบิตของ *Bob* จะใช้ตัวประมาณค่าสไลซ์

(Slice Estimator) ที่ประกอบด้วยสไลซ์ (Slice) ก่อนหน้าและกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Bob* ร่วมกัน เพื่อเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิต ซึ่งตัวประมาณค่าสไลซ์แสดงดังต่อไปนี้

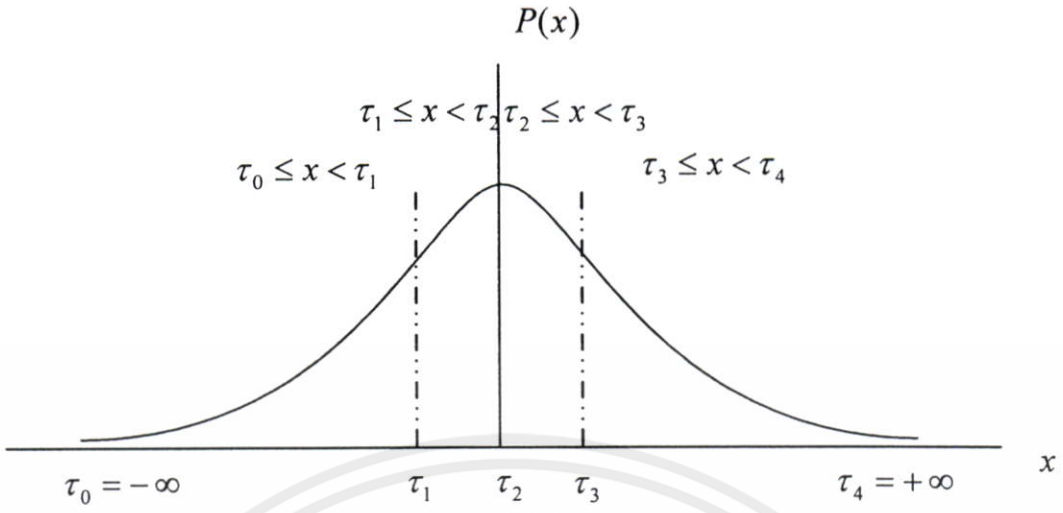
$$\widetilde{S}_1(x'),\widetilde{S}_2(x',S_1(x)),\widetilde{S}_3(x',S_1(x),S_2(x)),...,\widetilde{S}_m(x',S_1(x),...,S_{m-1}(x))$$

หลังจากที่ทำการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตเรียบร้อยแล้ว กุญแจรหัสลับบิตที่ได้ยังคงมีความผิดพลาดอยู่ โดยทั้ง *Alice* และ *Bob* จะใช้โพรโทคอลแก้ไขความผิดพลาด เช่น โพรโทคอล CASCADE หรือโพรโทคอล Winnow เป็นต้น เพื่อแก้ไขความผิดพลาดที่เกิดขึ้นนี้ให้กุญแจรหัสลับบิตที่ *Alice* และ *Bob* มีอยู่มีความเหมือนกัน [33]

4.5.2 การประมาณค่าจากจำนวนจริงเป็นตัวเลขแบบไบนารี

การประมาณค่ากุญแจรหัสลับบิตนั้น *Alice* และ *Bob* จะแบ่งจำนวนจริงจากฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ที่ตนใช้สร้างกุญแจรหัสลับออกเป็นส่วนๆ เพื่อกำหนดค่าไบนารีให้ในแต่ละส่วนที่ได้แบ่งไว้ โดยขอบเขตของแต่ละส่วนบนฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์นี้จะทำให้ปริมาณข่าวสารร่วม (Mutual Information) ระหว่างส่วนที่ทำการแบ่งหรือ $T(X)$ และกุญแจรหัสลับของ *Bob* (X') มีค่ามากที่สุด โดย $T(X)$ จะถูกแบ่งออกทั้งหมด t จุดซึ่งประกอบไปด้วย $\tau_1,\tau_2,\tau_3,....,\tau_{t-1}$ ซึ่งจากรูปที่ 4.9 แสดงการแบ่งฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ที่ *Alice* ออกเป็นส่วนสี่ส่วนด้วยกัน ซึ่ง τ_0 จะเท่ากับ $-\infty$ และ τ_t เท่ากับ ∞ โดยปริมาณข่าวสารร่วมระหว่างส่วนที่ถูกแบ่งและกุญแจรหัสลับของ *Bob* หรือ $I(T(X),X')$ หาได้ดังต่อไปนี้

จากการส่งกุญแจรหัสลับของ *Alice* ที่ได้จากการสุ่มจากฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ที่ค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวนเท่ากับ σ_A แสดงดังสมการ



รูปที่ 4.9 การแบ่งฟังก์ชันการกระจายแบบเกาส์ออกเป็น 4 ส่วนคือ $\tau_0 \le x < \tau_1$, $\tau_1 \le x < \tau_2$, $\tau_2 \le x < \tau_3$ และ $\tau_3 \le x < \tau_4$

$$f(x) = \frac{1}{\sqrt{2\pi\sigma_A^2}} e^{-x^2/2\sigma_A^2} \tag{4.40}$$

เมื่อ *Alice* ส่งกุญแจรหัสลับผ่านช่องสื่อสารแบบ AWGN (Additive White Gaussian Noise) ไปยังภาครับ กุญแจรหัสลับที่ *Bob* ได้รับจะเป็นกุญแจรหัสลับของ *Alice* รวมกับสัญญาณรบกวนดังสมการ

$$X' = X + n \tag{4.41}$$

X' คือตัวแปรสุ่มที่แทนกุญแจรหัสลับของ *Bob* X คือตัวแปรสุ่มที่แทนกุญแจรหัสลับของ *Alice* และ n คือตัวแปรสุ่มที่แทนสัญญาณรบกวนแบบเกาส์

ซึ่งสัญญาณรบกวนที่เกิดขึ้นภายในช่องสัญญาณนั้นมีการกระจายตัวแบบเกาส์ที่มีค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวนเท่ากับ α^2 ดังสมการ

$$n = \frac{1}{\sqrt{2\pi\alpha^2}} e^{-x^2/2\alpha^2} \tag{4.42}$$

ดังนั้นกุญแจรหัสลับที่ *Bob* ได้รับยังคงมีการกระจายตัวแบบเกาส์ ซึ่งฟังก์ชันความหนาแน่นของความน่าจะเป็นร่วม (Joint Probability Density Function) ระหว่างกุญแจรหัสลับของ *Bob* และกุญแจรหัสลับของ *Alice* แสดงดังสมการ

$$\begin{aligned} f(x,x') &= f(x)\times n \\ &= \frac{1}{2\pi\sigma_A\alpha} e^{-x^2/2\sigma_A^2} e^{-(x-x')^2/2\alpha^2} \end{aligned} \tag{4.43}$$

จากทฤษฎีข่าวสารที่กล่าวโดย C. Shannon ในปี ค.ศ. 1948 [15] ค่าของปริมาณข่าวสารร่วมแสดงได้ดังต่อไปนี้

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y) \\ I(X;Y) &= H(X) - H(X\,|\,Y)\,,\, H(Y) - H(Y\,|\,X) \end{aligned} \tag{4.44}$$

ดังนั้นจากสมการที่ (4.44) ค่าของปริมาณข่าวสารร่วม (Mutual Information) $I(T(X),X')$ แสดงดังต่อไปนี้

$$\begin{aligned} &I(X;Y) = H(T(X)) + H(X') - H(T(X),X') \text{ หรือ} \\ &I(X;Y) = H(T(X)) - H(T(X)\,|\,X')\,,\, H(X') - H(X'|\,T(X)) \end{aligned} \tag{4.45}$$

$H(T(X))$ คือค่าปริมาณข่าวสารเฉลี่ยของ $T(X)$

$H(T(X),X')$ คือปริมาณข่าวสารเฉลี่ยร่วม (Joint Entropy) ระหว่าง $T(X)$ และ X' ซึ่ง $H(T(X))$ แสดงดังต่อไปนี้

$$\begin{aligned} H(T(X)) &= -\sum_a P_a \log P_a \\ P_a &= \frac{1}{2}\left(erf(\frac{\tau_a}{\sigma_A\sqrt{2}}) - erf\left(\frac{\tau_{a-1}}{\sigma_A\sqrt{2}}\right)\right) \end{aligned} \tag{4.46}$$

และ $H(X')$ สามารถหาได้จากสมการที่ (4.39) ถึงสมการที่ (4.41) และสมการที่ (4.45) ซึ่งแสดงดังต่อไปนี้

$$P(x') = \frac{1}{\sqrt{2\pi\left(\sigma_A^2+\alpha^2\right)}} e^{\frac{-x^2}{2(\sigma_A^2+\alpha^2)}} \qquad \text{ดังนั้น}$$

$$H(X') = -\int_{-\infty}^{\infty} P(x')\log_2 P(x')dx'$$

$$H(X') = \frac{1}{2}\log 2\pi e(\sigma_A^2 + \alpha^2) \quad (4.47)$$

และ

$$H(T(X), X') = -\sum_a \int_{-\infty}^{\infty} dx'\, f_a(x')\log f_a(x')$$

$$f_a(x') = \int_{\tau_a}^{\tau_a} dx f(x, x') \quad (4.48)$$

ซึ่งจากสมการที่ (4.45) ถึงสมการที่ (4.48) สามารถใช้ในการหาค่าบนฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ $\tau_1, \tau_2, ..., \tau_{l-1}$ หลังจากนั้น *Alice* และ Bob สามารถใช้แต่ละค่านี้ที่แบ่งฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ออกเป็นส่วนๆ เพื่อกำหนดค่าไบนารีบิตให้แต่ละส่วนที่ได้ทำการแบ่งไว้

4.5.2.1 การประมาณค่ากุญแจรหัสลับบิตของ *Alice*

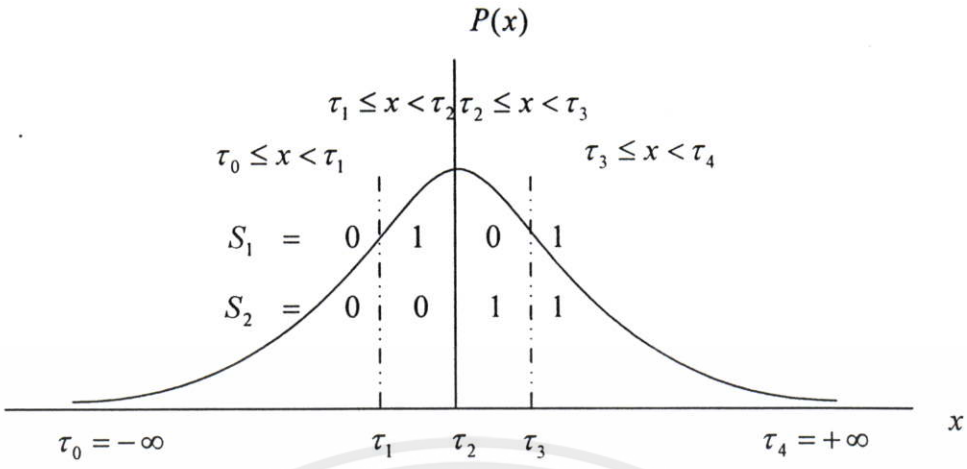
การประมาณค่ากุญแจรหัสลับบิตของ *Alice* เริ่มจากการแบ่งฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ออกเป็นส่วนย่อย เพื่อใช้ในการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิต โดยส่วนที่แบ่งได้จะต้องมีปริมาณข่าวสารร่วม (Mutual Information) ระหว่างส่วนที่แบ่ง $T(X)$ และกุญแจรหัสลับของ *Bob* (X') มีค่ามากที่สุด เมื่อได้ระยะห่างในแต่ละส่วนบนฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์เรียบร้อยแล้ว *Alice* จะกำหนดเลขไบนารี (Binary) เพื่อแทนลงในแต่ละส่วนที่แบ่งไว้โดยเริ่มต้นที่สไลซ์ที่หนึ่งไปถึงสไลซ์ที่ m ดังสมการ

$$S_i(X) = 0 \quad \text{เมื่อ} \quad \tau_{2^{i_n}} \le x < \tau_{2^{i_n}+2^{i-1}} \quad \text{นอกจากนั้น} \quad S_i(X) = 1 \quad (4.49)$$

$i = 1,2,3,...,m$ และ n เป็นลำดับของช่วงบนสไลซ์นั้นๆ

ตัวอย่างการประมาณค่าบิตของ *Alice* เมื่อ *Alice* กำหนดจำนวนสไลซ์เท่ากับหนึ่งดังนั้นค่ากุญแจรหัสลับที่กระจายตัวแบบเกาส์ที่ *Alice* สุ่มจะถูกกำหนดให้เป็นเลขไบนารีดังต่อไปนี้

$$S_1(x) = \begin{cases} 0 & \text{เมื่อ} \quad x \le 0 \\ 1 & \quad\quad x > 0 \end{cases} \quad (4.50)$$



รูปที่ 4.10 ตัวอย่างการกำหนดค่าไบนารีเมื่อจำนวนสไลซ์เท่ากับสอง

ถ้า *Alice* กำหนดจำนวนสไลซ์เท่ากับสองเพื่อแบ่งพังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ออกเป็นสี่ส่วนและใช้ตัวเลขไบนารีจำนวนสองบิตแทนแต่ละส่วนที่ได้แบ่งไว้ดังรูปที่ 4.10 ดังนั้นกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Alice* จะถูกกำหนดเป็นตัวเลขไบนารีดังต่อไปนี้

$$S_1(x)=\begin{cases}0 & \text{เมื่อ } \tau_0 \le x < \tau_1,\ \tau_2 \le x < \tau_3 \\ 1 & \tau_1 \le x < \tau_2,\ \tau_3 \le x < \tau_4\end{cases}$$

และ

$$S_2(x)=\begin{cases}0 & \text{เมื่อ } \tau_0 \le x < \tau_2 \\ 1 & \tau_2 \le x < \tau_4\end{cases} \tag{4.51}$$

4.5.2.2 การประมาณค่ากุญแจรหัสลับบิตของ *Bob*

การประมาณค่ากุญแจรหัสลับบิตของ *Bob* จะอาศัยตัวประมาณค่าสไลซ์ (Slice Estimator) เพื่อเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิต โดยใช้หลักการของความน่าจะเป็นเข้ามาช่วยในการตัดสินใจ เพื่อให้ผลที่ได้จากการประมาณค่ากุญแจรหัสลับบิตมีความผิดพลาดน้อยที่สุด ซึ่งตัวประมาณค่าสไลซ์ประกอบด้วยกุญแจรหัสลับบิตที่ได้จากการประมาณค่าจากสไลซ์ก่อนหน้าและกุญแจรหัสลับที่กระจายตัวแบบเกาส์ดังต่อไปนี้

$$\widetilde{S}_1(x'),\widetilde{S}_2(x',S_1(x)),\widetilde{S}_3(x',S_1(x),S_2(x)),...,\widetilde{S}_m(x',S_1(x),...,S_{m-1}(x))$$

โดยการประมาณค่าของตัวประมาณค่าสไลซ์ที่หนึ่งอาศัยเพียงค่ากุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Bob* ส่วนในตัวประมาณค่าในสไลซ์ถัดไปจะอาศัยค่ากุญแจรหัสลับบิตที่ประมาณค่าได้

ก่อนหน้าและค่ากุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Bob* เป็นค่าเริ่มต้นในการประมาณค่ากุญแจรหัสลับบิตถัดไปดังต่อไปนี้

$$\widetilde{S}_i(x^{'}, S_1(x),...,S_{i-1}(x)) \text{ โดย } i = 2,3,4,...,m$$

ตัวอย่างการประมาณค่ากุญแจรหัสลับบิตโดยกำหนดจำนวนสไลซ์เท่ากับหนึ่ง ($m = 1$) ซึ่ง *Bob* จะใช้เพียงค่ากุญแจรหัสลับที่กระจายตัวแบบเกาส์ของตนเท่านั้น เพื่อประมาณค่ากุญแจรหัสลับบิตตามค่าที่ได้ทำการแบ่งไว้บนฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ ซึ่งค่ากุญแจรหัสลับบิตที่ *Bob* ประมาณได้จะแสดงดังสมการ

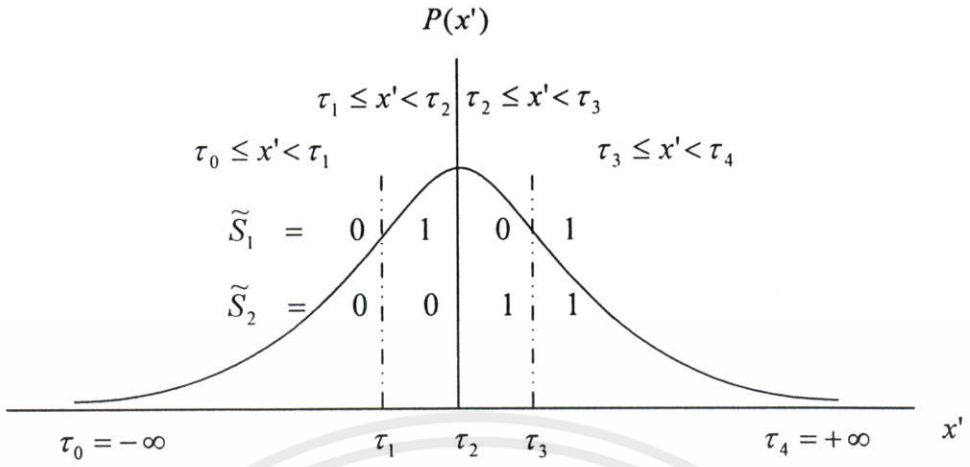
$$S_1(x') = \begin{cases} 0 & \text{เมื่อ } x' \le 0 \\ 1 & x' > 0 \end{cases} \tag{4.52}$$

$P_{S_1\ S_2....S_i}^{\beta_1\ \beta_2....1}$ คือความน่าจะเป็นที่สไลซ์ที่หนึ่งจะเกิดไบนารี β_1 และสไลซ์ที่สองจะเกิดค่าไบนารี β_2 เรื่อยไปจนถึงสไลซ์ที่ i จะเกิดค่าไบนารีบิต "1"
และ $P_{S_1\ S_2....S_i}^{\beta_1\ \beta_2....0}$ สามารถหาได้จาก

$$P_{S_1\ S_2....S_i\widetilde{S}_i}^{\beta_1\ \beta_2....ab} = \sum \int P_{S_1\ S_2....S_i}^{\beta_1\ \beta_2....a}(x')dx'$$
$$P_{S_1\ S_2....S_i}^{\beta_1\ \beta_2....a}(x') = \int_{A_{S_1\ S_2....S_i-1}^{\beta_1\ \beta_2....a}} p(x,x')dx \tag{4.54}$$

โดยที่ $A_{S_1.....S_{i-1}}^{\beta_1.....\beta_{i-1}}$ เป็นค่าจำนวนจริงบนฟังก์ชันความหนแน่นของความน่าจะเป็นที่ทำให้ $S_1(x) = \beta_1 \wedge S_2(x) = \beta_2 \wedge ..... \wedge S_{i-1}(x) = \beta_{i-1}$

ตัวอย่างการประมาณค่าบิตที่ *Bob* โดยกำหนดให้จำนวนสไลซ์เท่ากับสอง ($m = 2$) ซึ่งค่าที่กุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Bob* แสดงได้ดังรูปที่ 4.11 การประมาณค่ากุญแจรหัสลับบิตเริ่มต้นจากการประมาณค่าบิตเมื่อสไลซ์เท่ากับหนึ่งหรือ $\widetilde{S}_1(x')$ ซึ่งสามารถประมาณค่ากุญแจรหัสลับบิตได้ดังต่อไปนี้



รูปที่ 4.11 การประมาณค่าบิตของ *Bob* เมื่อจำนวนสไลซ์เท่ากับสอง

$$\widetilde{S}_1(x') = \begin{cases} 0 & \text{เมื่อ } \tau_0 \le x' < \tau_1,\ \tau_2 \le x' < \tau_3 \\ 1 & \tau_1 \le x' < \tau_2,\ \tau_3 \le x' < \tau_4 \end{cases}$$

หลังจากที่ประมาณค่ากุญแจรหัสลับบิตในสไลซ์ที่หนึ่งเสร็จเรียบร้อย *Alice* และ *Bob* จะแก้ไขความผิดพลาดที่เกิดจากการประมาณค่าบิตโดยใช้โพรโทคอลแก้ไขความผิดพลาด เพื่อทำให้กุญแจรหัสลับบิตที่ได้จากการประมาณค่ามีค่าเหมือนกันหรือใกล้เคียงกันมากที่สุด ต่อจากนั้น *Bob* จะใช้ค่ากุญแจรหัสลับบิตภายหลังจากการแก้ไขความผิดพลาดจากสไลซ์ที่หนึ่งหรือ $\widetilde{S}_1(x')$ และกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของตนเพื่อเป็นค่าเริ่มต้นในการประมาณค่าไบนารีในสไลซ์ที่สอง หรือ $\widetilde{S}_2(x')$ ดังนี้

จากสมการที่ (4.42) และสมการที่ (4.53) ความน่าจะเป็นที่สไลซ์ที่หนึ่งเป็นบิต "0" และสไลซ์ที่สองเป็นบิต "0" $P^{0\ 0}_{S_1 S_2}$ แสดงได้ดังนี้

$$P(X' = x') = \sum \int_{x'}^{x'+\Delta x'} \int_{-\infty}^{\tau_1} f(x, x')\, dx dx'$$

ความน่าจะเป็นที่สไลซ์ที่หนึ่งเป็นบิต "0" และสไลซ์ที่สองเป็นบิต "1" $P^{0\ 1}_{S_1 S_2}$ แสดงได้ดังนี้

$$P(X' = x') = \sum \int_{x'}^{x'+\Delta x'} \int_{\tau_1}^{\tau_2} f(x, x')\, dx dx'$$

ความน่าจะเป็นที่สไลซ์ที่หนึ่งเป็นบิต “1” และสไลซ์ที่สองเป็นบิต “0” $P_{S_1 S_2}^{1\ 0}$ แสดงได้ดังนี้

$$P(X'=x') = \sum \int_{x'}^{x'+\Delta x'} \int_{\tau_2}^{\tau_1} f(x,x')\, dxdx'$$

ความน่าจะเป็นที่สไลซ์ที่หนึ่งเป็นบิต “1” และสไลซ์ที่สองเป็นบิต “1” $P_{S_1 S_2}^{1\ 1}$ แสดงได้ดังนี้

$$P(X'=x') = \sum \int_{x'}^{x'+\Delta x'} \int_{\tau_3}^{\infty} f(x,x')dxdx'$$

ผลการประมาณค่าบิตที่สไลซ์ที่สองมีดังต่อไปนี้ถ้าสไลซ์ที่หนึ่งมีผลการประมาณค่าบิตเท่ากับศูนย์แล้วสไลซ์ที่สองจะมีผลการประมาณค่าดังนี้

$$\widetilde{S}_2(x) = \begin{cases} 0 & \text{เมื่อ} \quad P_{S_1 S_2}^{0\ 0} >= P_{S_1 S_2}^{0\ 1} \\ 1 & \qquad\quad P_{S_1 S_2}^{0\ 1} < P_{S_1 S_2}^{0\ 0} \end{cases}$$

ถ้าสไลซ์ที่หนึ่งมีผลการประมาณค่าบิตเท่ากับหนึ่งแล้วสไลซ์ที่สองจะมีผลการประมาณค่าดังนี้

$$\widetilde{S}_2(x) = \begin{cases} 0 & \text{เมื่อ} \quad P_{S_1 S_2}^{1\ 0} >= P_{S_1 S_2}^{1\ 1} \\ 1 & \qquad\quad P_{S_1 S_2}^{1\ 1} < P_{S_1 S_2}^{1\ 0} \end{cases}$$

หลังจากการประมาณค่าบิตที่สไลซ์ที่สองผลการประมาณค่าที่ได้ยังคงมีความผิดพลาดเกิดขึ้นอยู่ ดังนั้น *Alice* และ *Bob* จะใช้โพรโทคอลแก้ไขความผิดพลาดมาแก้ไขความผิดพลาดให้กุญแจรหัสลับบิตที่ประมาณค่าได้เหมือนกัน

บทที่ 5
วิธีการออกแบบและจำลองการทำงาน

รหัสแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correcting Code: FEC) เป็นหนึ่งในวิธีการที่นำมาใช้เพื่อลดผลกระทบจากสัญญาณรบกวน ที่เป็นสาเหตุให้เกิดความผิดพลาดระหว่างการส่งข้อมูลในระบบสื่อสารดิจิตอล ทำให้ความผิดพลาดที่เกิดขึ้นระหว่างการส่งข้อมูลข่าวสารลดลง โดยภาคส่งไม่จำเป็นต้องส่งข้อมูลนั้นใหม่เมื่อภาครับตรวจพบความผิดพลาดเกิดขึ้น ซึ่งจากข้อดีของรหัสแก้ไขความผิดพลาดล่วงหน้านี้ทำให้มีการนำรหัสแก้ไขความผิดพลาดล่วงหน้ามาใช้พัฒนาโพรโทคอลแก้ไขความผิดพลาดที่ใช้ในระบบวิทยาการรหัสลับเชิงควอนตัมปัจจุบัน เพื่อให้การแก้ไขความผิดพลาดที่เกิดขึ้นระหว่างการส่งกุญแจรหัสลับทำได้อย่างรวดเร็ว สอดคล้องกับระบบการส่งกุญแจรหัสลับเชิงควอนตัมความเร็วสูง ในบทนี้กล่าวถึงการออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสบีซีเอช และรหัสคอนโวลูชัน (Convolutional Code) ซึ่งเป็นหนึ่งในรหัสแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correcting Code: FEC) โดยวิธีที่ได้ทำการพัฒนาขึ้นนี้จะถูกใช้เพื่อแก้ไขความผิดพลาดที่เกิดขึ้นจากการส่งกุญแจรหัสลับบิต ในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) เพื่อนำรหัสแก้ไขความผิดพลาดล่วงหน้า (FEC) มาช่วยพัฒนาโพรโทคอลแก้ไขความผิดพลาด ลดจำนวนรอบการติดต่อระหว่างผู้ส่งและผู้รับ ซึ่งจำนวนรอบการติดต่อสื่อสารจะทำให้การสร้างกุญแจรหัสลับทำได้อย่างล่าช้า นอกจากนี้วิธีการที่ทำการพัฒนาขึ้น สามารถที่จะนำไปใช้ในการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD) โดยจะนำไปใช้ภายหลังจากการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตโดยใช้วิธีการแก้ไขความผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) ซึ่งจากนั้นสามารถที่จะนำวิธีที่ได้พัฒนาขึ้นนี้ มาแก้ไขความผิดพลาดดังเช่นระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) โดยวิธีที่ได้พัฒนาขึ้นมีรายละเอียดดังต่อไปนี้

5.1 การออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาด

วิทยานิพนธ์นี้นำเสนอการพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยรหัสบีซีเอชและรหัสคอนโวลูชัน (Convolution Code) โดยวิธีการที่หนึ่งเสนอการนำรหัสบีซีเอชมาประยุกต์ร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง (Side Information) ในเรื่องของ Distributed Source Coding ที่นำเสนอครั้งแรกโดย [40] วิธีการที่สองนำเสนอการนำรหัสบีซีเอชมาพัฒนาโพรโทคอลฟุรุคาวา (Furukawa) [14] และวิธีที่สามเป็นการนำเสนอการนำรหัสคอนโวลูชัน (Convolution Code) มาพัฒนาการแก้ไขความผิดพลาดร่วมกับการ

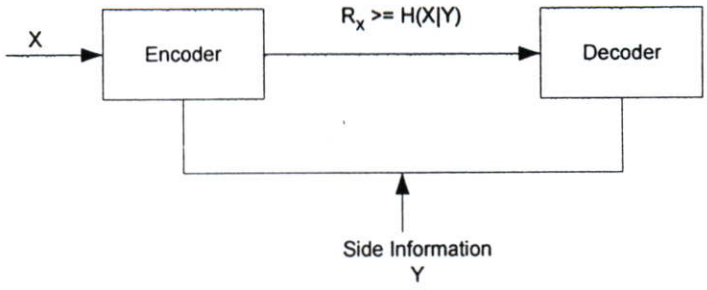
เข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง โดยใช้วิธีการถอดรหัสด้วยวิธีไวเทอร์บี (Viterbi Decoding Algorithm) และการตัดสินใจแบบหยาบ ซึ่งหลักการที่ออกแบบทั้งหมดนี้สามารถใช้แก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) เนื่องจากกุญแจรหัสลับจะอยู่ในรูปแบบไบนารี แต่หากนำวิธีที่นำเสนอนี้ไปใช้ในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) ซึ่งกุญแจรหัสลับจะอยู่ในรูปการกระจายตัวแบบเกาส์ (Gaussian Distribution) ไม่สามารถที่จะนำหลักการที่นำเสนอไปใช้ในการแก้ไขความผิดพลาดได้ การแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD) จึงต้องทำการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิตก่อน โดยใช้การแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) หลังจากนั้นผู้ส่งและผู้รับจะมีกุญแจรหัสลับบิต ซึ่งสามารถที่จะนำโพรโทคอลแก้ไขความผิดพลาดมาใช้ในการแก้ไขความผิดพลาดได้ ดังรายละเอียดการออกแบบมีดังต่อไปนี้

5.1.1 รหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

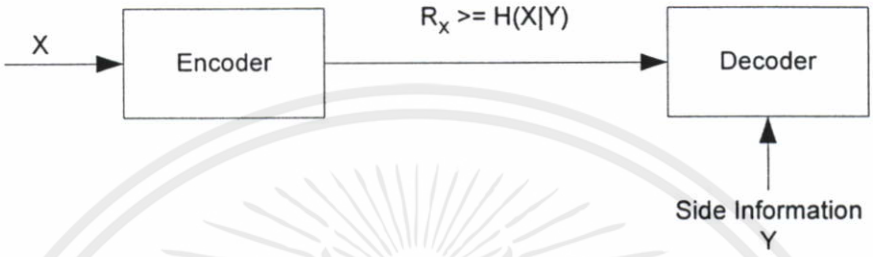
การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง นี้สามารถนำมาใช้ในการประยุกต์พัฒนาโพรโทคอลแก้ไขความผิดพลาดร่วมกับรหัสแก้ไขความผิดพลาดล่วงหน้า เช่น รหัสแบบบล็อกเชิงเส้น รหัสเทอร์โบ รหัสพาริตี้เช็กความหนาแน่นต่ำ (LDPC) รหัสคอนโวลูชัน เป็นต้น โดยหลักการพื้นของการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง และรหัสบีซีเอชที่นำมาพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม ที่นำเสนอในวิทยานิพนธ์เล่มนี้มีดังต่อไปนี้

5.1.1.1 การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

หลักการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง (Side Information) นำเสนอขึ้นเป็นครั้งแรกในปี ค.ศ. 1973 โดย Slepian-Wolf [39] โดยสามารถพัฒนาร่วมกับรหัสแก้ไขความผิดพลาดล่วงหน้าอื่นได้ เช่น รหัสบล็อกเชิงเส้น รหัสเทอร์โบและรหัสพาริตี้เช็กความหนาแน่นต่ำ เป็นต้น การทำงานของการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างร่วมกับรหัสแก้ไขความผิดพลาดมีการทำงานดังต่อไปนี้ กำหนดให้แหล่งกำเนิดสองแหล่งกำเนิดสร้างข้อมูลข่าวสารที่มีความสัมพันธ์กัน โดยแหล่งกำเนิดแรกสร้างข้อมูลที่แทนด้วยตัวแปรสุ่ม X และแหล่งกำเนิดที่สองสร้างข้อมูลที่แทนด้วยตัวแปรสุ่ม Y การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง แสดงได้ดังรูปที่ 5.1 จากรูปตัวแปรสุ่ม X จะผ่านเข้าสู่วงจรเข้ารหัส



(ก)



(ข)

รูปที่ 5.1 การเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง
(ก) ข้อมูลข่าวสารข้างทั้งทางผู้ส่งและผู้รับ (ข) ข้อมูลข่าวสารข้างที่ภาครับ

ซึ่งอัตราในการเข้ารหัสจะขึ้นอยู่กับทางด้านผู้ส่งนั้นจะรับทราบข้อมูลของตัวแปรสุ่ม Y หรือไม่ โดยหากวงจรเข้ารหัสแสดงดังรูปที่ 5.1(ก) ทางด้านผู้ส่งและผู้รับนั้นรับทราบข้อมูลของตัวแปรสุ่ม Y ด้วยนั้นอัตราการเข้ารหัสโดยผู้ส่งจะมีค่าไม่น้อยกว่า $H(X,Y)$ ดังสมการ [40]

$$R_X + R_Y \geq H(X,Y) \tag{5.1}$$

แต่ถ้าทางผู้ส่งนั้นไม่ทราบข้อมูลของตัวแปรสุ่ม Y ดังรูปที่ 5.1(ข) อัตราในการเข้ารหัสนั้นจะมีค่าไม่น้อยกว่า $H(X \mid Y)$ ดังสมการ [40]

$$R_X \geq H(X \mid Y) \tag{5.2}$$

5.1.1.2 พื้นฐานรหัสบีซีเอช

รหัสบีซีเอช (BCH Code) เป็นหนึ่งในรหัสแก้ไขความผิดพลาดล่วงหน้าที่นำมาใช้ในระบบสื่อสารดิจิตอล เพื่อแก้ไขบิตที่ผิดระหว่างการส่งข้อมูลผ่านช่องทางการสื่อสารที่มีสัญญาณรบกวน (Noisy Channel) โดยรหัสบีซีเอชนี้จัดเป็นหนึ่งในรหัสแบบบล็อกเชิงเส้น (Linear Block Code) ซึ่งการเข้ารหัสบีซีเอชมีการทำงานโดยเริ่มจากการนำข้อมูลที่ต้องการเข้ารหัสขนาด k บิต มาผ่านเข้าสู่วงจรเข้ารหัส (Encoder) ซึ่งผลจากการเข้ารหัสจะได้คำรหัส (Codeword) ขนาด n บิต

โดยคำรหัสนี้ประกอบด้วยข้อมูลที่นำมาเข้ารหัสและพาริตี้บิตหรือบิตที่ถูกเพิ่มขึ้นมา (Redundancy Bit) ในคำรหัสเพื่อเป็นส่วนหนึ่งที่จะใช้ในการแก้ไขความผิดพลาดซึ่งรหัสบีซีเอชนี้สามารถที่แก้ไขความผิดพลาดได้ t บิตในบล็อกขนาด n บิต

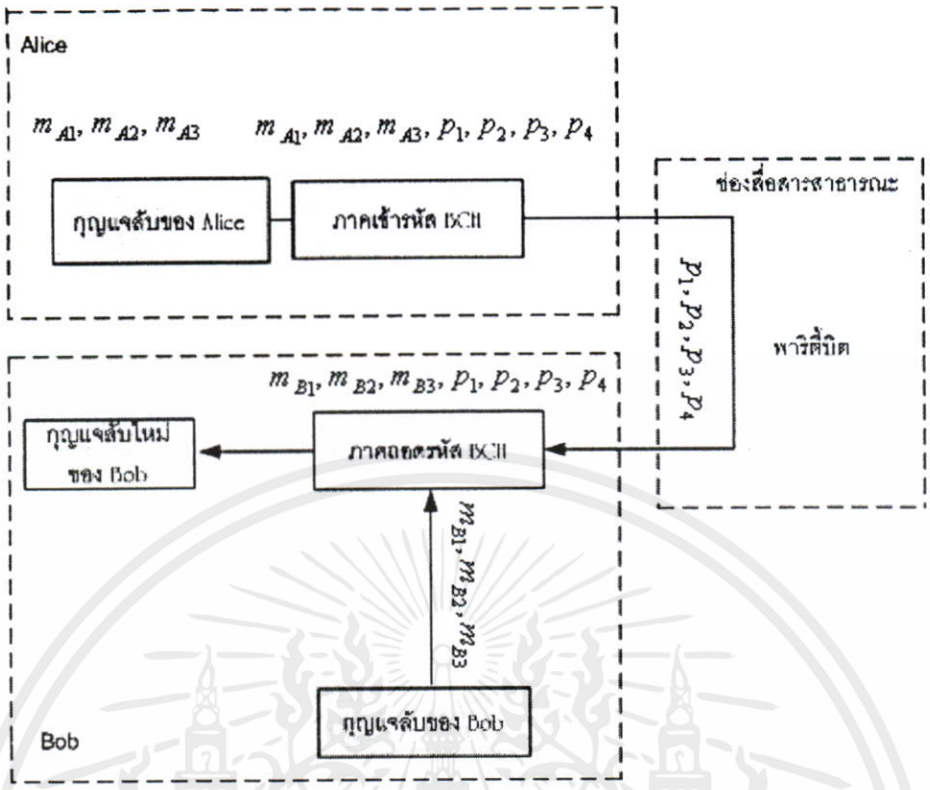
5.1.1.3 การพัฒนาโพรโทคอลด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

การพัฒนาโพรโทคอลด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง ที่ได้ทำการออกแบบนี้มีจุดประสงค์เพื่อทำให้โพรโทคอลที่พัฒนาขึ้นมานี้สามารถแก้ไขกุญแจรหัสลับบิตในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) ที่ผิดได้อย่างรวดเร็ว ลดจำนวนรอบการติดต่อสื่อสารระหว่าง *Alice* และ *Bob* ซึ่งเป็นสาเหตุสำคัญที่ทำให้การสร้างกุญแจรหัสลับทำได้อย่างล้าช้า มีการส่งข้อมูลผ่านระบบเครือข่ายจำนวนมากและใช้เวลาในการประมวลผลนาน หลังจาก *Alice* ทำการส่งกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัมไปยัง *Bob* ซึ่งจะทำให้ *Alice* และ *Bob* มีชิฟคีย์บางส่วนที่แตกต่างกันหรือมีความผิดพลาดเกิดขึ้นในระหว่างการส่ง การแก้ไขความผิดพลาดของโพรโทคอลที่ทำการพัฒนาขึ้นมีการทำงานดังรูปที่ 5.2 โดยแบ่งการทำงานเป็นขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 การหาอัตราความผิดพลาดจากการกระจายกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัม (Quantum Bit Error Rate: QBER) สามารถหาได้โดย *Alice* และ *Bob* จะทำการสุ่มกุญแจลับบิตของตนขึ้นมาในตำแหน่งเดียวกัน หลังจากนั้นจะนำกุญแจลับบิตที่สุ่มขึ้นมาได้เหล่านี้มาเปรียบเทียบกันผ่านทางช่องสื่อสารสาธารณะ ซึ่งผลที่ได้จะทำให้ *Alice* และ *Bob* ทราบการเข้ามาบุกรุกขโมยสถานะควอนตัมของบุคคลที่สาม ถ้าหากความผิดพลาดระหว่างการส่งมีค่าสูง แต่หากอัตราความผิดพลาดอยู่ในระดับที่ยอมรับ *Alice* และ *Bob* จะทำการแก้ไขความผิดพลาด โดยใช้โพรโทคอลแก้ไขความผิดพลาด ซึ่งอัตราความผิดพลาดคือจำนวนบิตแตกต่างกันต่อจำนวนบิตทั้งหมดดังสมการ

$$e = \frac{Bit\_error}{l} \tag{5.3}$$

e คืออัตราความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม Bit_error คือจำนวนบิตที่ผิดพลาดและ l คือจำนวนบิตที่นำมาเปรียบเทียบกันทั้งหมด



รูปที่ 5.2 วิธีการแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

หลังจากที่นำกุญแจรหัสลับบิตบางส่วนมาเปรียบเทียบเพื่อหาอัตราความผิดพลาดระหว่างการส่งกุญแจรหัสลับที่สุ่มขึ้นมาทั้งหมดนี้จะถูกทิ้งทั้งหมดเพื่อความปลอดภัยของกุญแจรหัสลับ ซึ่งอัตราความผิดพลาดจากการกระจายกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัมนี้จะถูกใช้เพื่อ หาขนาดของบล็อกของรหัสบีซีเอชและความสามารถในการแก้ไขความผิดพลาด ซึ่งจะส่งผลต่อจำนวนข้อมูลเกี่ยวกับกุญแจรหัสลับที่ส่งผ่านระบบเครือข่าย โดยจำนวนข้อมูลที่ส่งผ่านระบบเครือข่ายทั้งหมดแสดงดังต่อไปนี้

$$\text{จำนวนข้อมูลที่ส่ง} = (n-k) \times \frac{l}{N} \tag{5.4}$$

l คือจำนวนกุญแจรหัสลับทั้งหมด N คือขนาดของบล็อก

ขั้นตอนที่ 2 *Alice* และ *Bob* เลือกขนาดความยาวของคำรหัส n บิตและความสามารถในการแก้ไขบิตที่ผิดพลาดภายในบล็อกตามคุณสมบัติของรหัสบีซีเอช โดยความยาวของคำรหัสแสดงดังสมการ

$$n = 2^m - 1 \qquad \text{โดยที่ } m = 3,4,5,.... \tag{5.5}$$

จากคุณสมบัติของรหัสบีซีเอช คำรหัสขนาด n บิต เกิดจากข้อมูลขนาด k บิต ร่วมกับพาริตี้บิต (Parity) หรือรีดันแดนซีบิต (Redundancy) ขนาด n-k บิต ซึ่งความสามารถในการแก้ไขความผิดพลาดของรหัสบีซีเอชแสดงดังต่อไปนี้

$$n - k \le mt \tag{5.6}$$

t คือความสามารถในการแก้ไขบิตที่ผิดของรหัสบีซีเอช

ขั้นตอนที่ 3 *Alice* และ *Bob* ทำการแบ่งกุญแจรหัสลับบิตของตนออกเป็นบล็อกขนาด k บิต ก่อนที่จะส่งกุญแจรหัสลับบิตเหล่านี้เข้าสู่วงจรเข้ารหัสบีซีเอช เช่น *Alice* แบ่งกุญแจรหัสลับบิตของตนออกเป็นบล็อกขนาดสี่บิตซึ่งจะทำให้ข้อมูลที่จะถูกนำมาเข้ารหัสบีซีเอชมีดังต่อนี้

$$k_{Ai_1}, k_{Ai_2}, k_{Ai_3}, k_{Ai_4} \text{ โดยที่ } i = 1,2,3,...$$

i คือตำแหน่งของชิฟคีย์ของ *Alice*

ขั้นตอนที่ 4 *Alice* นำกุญแจลับที่แบ่งเป็นบล็อกผ่านเข้าสู่วงจรเข้ารหัสบีซีเอชซึ่งจะได้คำรหัสขนาด n บิต หลังจากนั้น *Alice* จะส่งเพียงเฉพาะพาริตี้บิตหรือรีดันแดนซีบิตไปให้ *Bob* ผ่านทางช่องสื่อสารสาธารณะ

ขั้นตอนที่ 5 เมื่อ *Bob* ได้รับพาริตี้บิตหรือรีดันแดนซีบิตแล้ว *Bob* จะนำมารวมเข้ากับกุญแจลับของตนที่ได้แบ่งออกเป็นบล็อกขนาด k บิตไว้ก่อนหน้าเพื่อสร้างคำรหัสใหม่ก่อน หลังจากนั้น *Bob* จะนำคำรหัสใหม่นี้ผ่านเข้าสู่วงจรถอดรหัสบีซีเอชซึ่งผลลัพธ์ที่ได้จากวงจรถอดรหัสบีซีเอชคือกุญแจรหัสลับใหม่ของ *Bob*

ตัวอย่างการแก้ไขความผิดพลาด เมื่อ *Alice* และ *Bob* มีชิฟคีย์จำนวน 11 บิต โดยชิฟคีย์ของ *Alice* มีดังต่อไปนี้ "11100110100" และชิฟคีย์ของ *Bob* มีดังต่อไปนี้ "11100110101" ซึ่งตำแหน่งของชิฟคีย์ตัวอักษรหนาแสดงตำแหน่งชิฟคีย์ที่ผิดเพื่อลดขั้นตอนการแก้ไขความผิดพลาด กรณีที่หนึ่งจะทำการกำหนดขนาดของบล็อกและความสามารถในการแก้ไขความผิดพลาด (t) โดยความสามารถในการแก้ไขความผิดพลาดเท่ากับหนึ่งบิตต่อบล็อก n เท่ากับ 15 บิต และ k เท่ากับ 11 บิต หรือรหัสบีซีเอช (15,11) ดังนั้นการแก้ไขความผิดพลาดเริ่มจากขั้นตอนที่ 3 ดังนี้

ขั้นตอนที่ 3 *Alice* แบ่งกุญแจรหัสลับของตนออกเป็นบล็อกขนาด 11 บิตดังนี้ "11100110100" ขั้นตอนที่ 4 *Alice* นำกุญแจรหัสลับของตนเข้าสู่วงจรเข้ารหัสบีซีเอช ซึ่งจะได้คำรหัสขนาด 15 บิต ดังต่อไปนี้ "111001101001000" โดยจะแบ่งเป็นชิฟคีย์ขนาด 11 บิตดังนี้

"11100110100" และรีดันแดนซีบิตหรือพาริตี้บิตขนาดสี่บิตดังนี้ "1000" หลังจากนั้น *Alice* จะส่งพาริตี้บิตนี้ไปให้ *Bob* ผ่านทางช่องสื่อสารสาธารณะ

ขั้นตอนที่ 5 *Bob* นำพาริตี้บิตที่รับได้ไปรวมกับชิฟคีย์ของตนที่ได้แบ่งเป็นบล็อกขนาด 11 บิตไว้ก่อนหน้าเพื่อสร้างคำรหัส (Codeword) ขึ้นมาใหม่ ซึ่งคำรหัสที่สร้างขึ้นมาใหม่มีดังนี้ "11100110101**1**000" หลังจากนั้น Bob จะนำคำรหัสที่สร้างขึ้นใหม่นี้ไปผ่านเข้าสู่วงจรถอดรหัสบีซีเอชซึ่งจะได้ชิฟคีย์ใหม่ดังนี้ "11100110100" ซึ่งจะทำให้กุญแจรหัสลับที่ *Bob* และ *Alice* มีอยู่กลับมาเหมือนกัน

ดังนั้นจากสมการที่ (5.4) จำนวนบิตหรือจำนวนข้อมูลเกี่ยวกับกุญแจรหัสลับที่ส่งผ่านช่องสื่อสารสาธารณะมีค่าเท่ากับสี่บิต

กรณีที่สอง หาก *Alice* และ *Bob* กำหนดความสามารถในการแก้ความผิดพลาดของรหัสบีซีเอชเพิ่มขึ้นเป็นห้าบิต โดย n เท่ากับ 31 บิต และ k เท่ากับ 11 บิต หรือรหัสบีซีเอช (31,11) ดังนั้นการแก้ไขความผิดพลาดเริ่มจากขั้นตอนที่ 3 ดังนี้

ขั้นตอนที่ 3 *Alice* แบ่งกุญแจรหัสลับของตนออกเป็นบล็อกขนาด 11 บิตดังนี้ "11100110100" ขั้นตอนที่ 4 *Alice* นำกุญแจรหัสลับของตนเข้าสู่วงจรเข้ารหัสบีซีเอช ซึ่งจะได้คำรหัสขนาด 31 บิต ดังต่อไปนี้ "11100110100100000101011101100011" โดยจะแบ่งเป็นชิฟคีย์ขนาด 11 บิตดังนี้ "11100110100" และรีดันแดนซีบิตหรือพาริตี้บิตขนาด 20 บิตดังนี้ "10000101011101100011" หลังจากนั้น *Alice* จะส่งพาริตี้บิตนี้ไปให้ *Bob* ผ่านทางช่องสื่อสารสาธารณะ

ขั้นตอนที่ 5 *Bob* นำพาริตี้บิตที่รับได้ไปรวมกับชิฟคีย์ของตนที่ได้แบ่งเป็นบล็อกขนาด 11 บิตไว้ก่อนหน้าเพื่อสร้างคำรหัส (Codeword) ขึ้นมาใหม่ ซึ่งคำรหัสที่สร้างขึ้นมาใหม่มีดังนี้ "11100110101**1**00001010111011000**1**1" หลังจากนั้น *Bob* จะนำคำรหัสที่สร้างขึ้นใหม่นี้ไปผ่านเข้าสู่วงจรถอดรหัสบีซีเอชซึ่งจะได้ชิฟคีย์ใหม่ดังนี้ "11100110100" ซึ่งจะทำให้กุญแจรหัสลับที่ *Bob* และ *Alice* มีอยู่กลับมาเหมือนกัน

ดังนั้นจากสมการที่ (5.4) จำนวนบิตหรือจำนวนข้อมูลเกี่ยวกับกุญแจรหัสลับที่ส่งผ่านช่องสื่อสารสาธารณะมีค่าเท่ากับ 20 บิต ซึ่งสามารถที่จะสรุปได้ว่า ชิฟคีย์ที่ *Bob* และ *Alice* มีอยู่ภายหลังจากการแก้ไขความผิดพลาดยังคงเหมือนกัน ไม่ว่าจะใช้ความสามารถแก้ไขความผิดพลาดเท่ากับหนึ่งบิตหรือห้าบิต แต่หากใช้ความสามารถในการแก้ไขความผิดพลาดเท่ากับห้าบิต จะทำให้ *Alice* ส่งรีดันแดนซีบิตมากกว่า ดังนั้นในกรณีนี้จึงอาจกล่าวได้ว่ากรณีที่หนึ่งจะให้ประสิทธิภาพในการแก้ไขความผิดพลาดได้ดีกว่ากรณีที่สองเมื่อเปรียบเทียบผลการแก้ไขความผิดพลาดที่ได้ และจำนวนข้อมูลที่ *Alice* ส่งให้ *Bob* ผ่านเครือข่ายสาธารณะ

5.1.2 การพัฒนาการแก้ไขความผิดพลาดวิธีฟุรุคาวาด้วยรหัสบีซีเอช

รหัสบีซีเอชนอกจากจะนำมาใช้ร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง เพื่อพัฒนาโพรโทคอลแก้ไขความผิดพลาดแล้ววิทยานิพนธ์นี้ยังเสนอการนำรหัสบีซีเอช นำมาพัฒนากระบวนการแก้ไขความผิดพลาดฟุรุคาวา (Furukawa) [14] ซึ่งโพรโตคอลของฟุรุคาวานี้จะใช้พาริตี้บิตเพื่อตรวจสอบความผิดพลาดของกุญแจรหัสลับบิตก่อน หากพบความผิดพลาดเกิดขึ้นภายในบล็อกกุญแจรหัสลับบิต โพรโทคอลนี้จะใช้รหัสแก้ไขความผิดพลาดแบบบล็อกเชิงเส้นเพื่อแก้ไขความผิดพลาดที่เกิดขึ้นแต่หลักการของพาริตี้บิตที่นำมาใช้งานนี้จะทำให้การทำงานของโพรโทคอลมีความล่าช้า เนื่องมาจากพาริตี้บิตจะตรวจพบการผิดของกุญแจรหัสลับบิตก็ต่อเมื่อ จำนวนกุญแจรหัสลับบิตที่ผิดมีจำนวนคี่ถ้าจำนวนกุญแจรหัสลับที่ผิดมีจำนวนคู่ พาริตี้บิตจะไม่สามารถพบความผิดพลาดทำให้โพรโทคอลนี้คาดเดาว่ากุญแจรหัสลับที่มีอยู่นั้นถูกต้อง ถ้า *Alice* และ *Bob* ต้องการแก้ไขความผิดพลาดที่ยังอาจจะเหลืออยู่ *Alice* และ *Bob* จะดำเนินการดังที่กล่าวมาทั้งหมดซ้ำอีกครั้ง โดยเปลี่ยนขนาดของบล็อกให้มีขนาดใหญ่ขึ้นเพื่อให้พาริตี้บิตในบล็อกที่มีพาริตี้บิตเหมือนกันก่อนหน้านี้ เกิดมีบิตผิดเพิ่มมากขึ้นทำให้พาริตี้บิตของบล็อกใหม่มีความแตกต่างกัน ดังนั้นจะเห็นได้ว่าหลักการนี้มีทำงานในลักษณะวนซ้ำ ซึ่งจะส่งผลให้การแก้ไขความผิดพลาดทำได้อย่างล่าช้า วิธีการที่พัฒนาขึ้นมาใหม่นี้ด้วยรหัสบีซีเอชนี้ จะตัดการตรวจสอบบล็อกที่ผิดด้วยพาริตี้บิตและใช้รหัสแก้ไขความผิดพลาดที่มีความสามารถในการแก้ไขความผิดพลาดที่สูงเข้ามาช่วยแก้ไขความผิดพลาดที่เกิดขึ้นทั้งหมดซึ่งมีการทำงานดังต่อไปนี้

ขั้นตอนที่ 1 การหาอัตราความผิดพลาดจากการกระจายกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัม (Quantum Bit Error Rate: QBER) โดยอัตราความผิดพลาดคือจำนวนบิตแตกต่างกันต่อจำนวนบิตทั้งหมดดังสมการ (5.3) ซึ่งอัตราความผิดพลาดจากการกระจายกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัมนี้ จะถูกใช้เพื่อหาขนาดของบล็อกและความสามารถในการแก้ไขความผิดพลาด ซึ่งจะส่งผลต่อจำนวนข้อมูลเกี่ยวกับกุญแจรหัสลับที่ส่งผ่านระบบเครือข่ายโดย ปริมาณข้อมูลเกี่ยวกับกุญแจรหัสลับที่ส่งผ่านระบบเครือข่ายในแต่ละบล็อกแสดงดังต่อไปนี้ [14]

$$\text{จำนวนข้อมูลที่ส่ง} = n - k \tag{5.7}$$

ขั้นตอนที่ 2 *Alice* และ *Bob* แบ่งกุญแจรหัสลับของตนออกเป็นบล็อก ซึ่งกำหนดให้ตัวแปรสุ่ม X แทนกุญแจรหัสลับของ *Alice* และตัวแปรสุ่ม Y แทนกุญแจรหัสลับของ *Bob*

ขั้นตอนที่ 3 *Alice* สร้างบิตสุ่มขนาด k บิตที่แทนด้วยตัวแปรสุ่ม $U = u_1, u_2, .., u_k$ และนำตัวแปรสุ่ม U นี้มาผ่านเข้าสู่วงจรเข้ารหัส BCH ซึ่งจะได้คำรหัสขนาด n บิต ที่แทนด้วยตัวแปรสุ่ม $W = w_1, w_2, ..., w_n$ หลังจากนั้นจึงนำคำรหัส W มารวมกันแบบมอดุโล 2 กับกุญแจรหัสลับของ *Alice* ดังนี้

$$Z = W \oplus X \tag{5.8}$$

หลังจากนั้น *Alice* จะทำการส่งตัวแปรสุ่ม Z นี้ไปยัง *Bob* ผ่านทางช่องสื่อสารสาธารณะ

ขั้นตอนที่ 4 *Bob* นำตัวแปรสุ่ม Z มารวมแบบมอดุโล 2 กับกุญแจรหัสลับบิตของตน Y ดังนี้

$$\begin{aligned} V &= Z \oplus Y \\ &= (W \oplus X) \oplus Y \\ &= W \oplus (X \oplus Y) \end{aligned} \tag{5.9}$$

จากนั้นตัวแปรสุ่ม V ที่ *Bob* สร้างได้จะถูกส่งผ่านกระบวนการถอดรหัส BCH ซึ่งจะได้ตัวเลขสุ่ม U' หรือเป็นบิตสุ่มใกล้เคียงหรือเหมือนกับ *Alice* สร้างขึ้น ตัวแปรสุ่ม U' นี้จะถูกใช้เพื่อแก้ไขความผิดพลาดโดยจะทำการส่งผ่านวงจรเข้ารหัสบีซีเอชอีกครั้งเพื่อสร้างรหัส W' ขึ้นมาใหม่ หากนำW'มารวมกับตัวแปรสุ่ม V แบบมอดุโล 2 ที่ *Bob* ซ้ำอีกครั้งจะทำให้ *Bob* ทราบตำแหน่งบิตที่ผิดและแก้ไขบิตผิดให้กลับมาถูกต้องได้ดังนี้

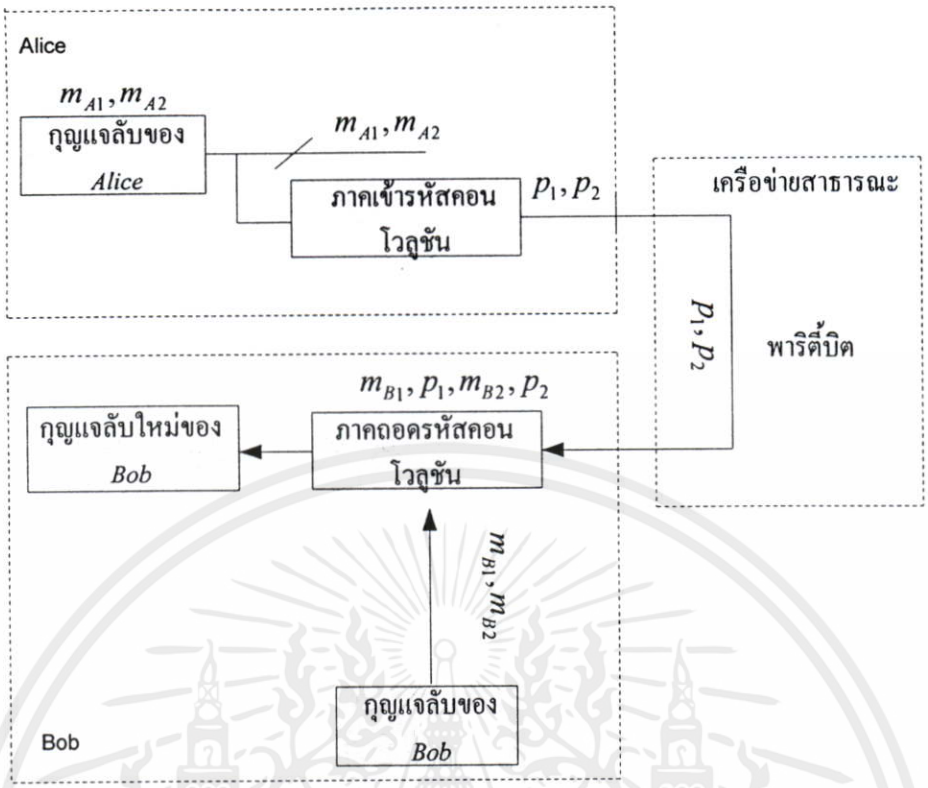
$$\begin{aligned} Q &= V \oplus W' \\ &= (W \oplus X) \oplus Y \oplus W' \\ &= (W \oplus W') \oplus (X \oplus Y) \end{aligned} \tag{5.10}$$

ถ้ากุญแจรหัสลับของ *Alice* และ *Bob* เหมือนกันจะทำให้ Q มีค่าเท่ากับศูนย์แต่ถ้า Q มีค่าไม่เท่ากับศูนย์แสดงว่า *Alice* และ *Bob* มีกุญแจรหัสลับที่ไม่เหมือนกันและตำแหน่งของกุญแจรหัสลับที่แตกต่างกันคือตำแหน่งของบิต "1" ในตัวแปรสุ่ม Q

ตัวอย่างการแก้ไขความผิดพลาด เมื่อ *Alice* และ *Bob* มีชิฟคีย์จำนวน 15 บิต โดยชิฟคีย์ของ *Alice* มีดังต่อไปนี้ "111001101001010" และชิฟคีย์ของ *Bob* มีดังต่อไปนี้ "111001101011010" ซึ่งตำแหน่งของชิฟคีย์ตัวอักษรหนาแสดงตำแหน่งชิฟคีย์ที่ผิด เพื่อลดขั้นตอนการแก้ไขความผิดพลาด กรณีที่หนึ่ง จะกำหนดขนาดของบล็อกและความสามารถในการแก้ไขความผิดพลาดของรหัสบีซีเอชก่อนล่วงหน้า โดยความสามารถในการแก้ไขความผิดพลาดเท่ากับหนึ่งบิตต่อบล็อก n เท่ากับ 15 บิต และ k เท่ากับ 11 บิต หรือรหัสบีซีเอช (15,11) ดังนั้นการแก้ไขความผิดพลาดเริ่มจากขั้นตอนที่ 2 ดังนี้

ขั้นตอนที่ 2 *Alice* ทำการสร้างบิตสุ่ม U ขึ้นมา11 บิตดังนี้ "10000100010"

ขั้นตอนที่ 3 *Alice* นำบิตสุ่มU มาผ่านเข้าสู่วงจรเข้ารหัสบีซีเอช (15,11) ซึ่งจะได้คำรหัส W จำนวน 15 บิตดังนี้ "100001000100101" หลังจากนั้น *Alice* จะนำคำรหัส W



รูปที่ 5.3 การแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

มามอดุโลกับชิฟคีย์ของตนตามสมการที่ (5.8) เพื่อสร้างคำรหัส Z ขึ้นมาโดยผลที่ได้จากการสร้างคือ "011000101101111" จากนั้น Alice จะทำการส่งคำรหัส Z นี้ไปให้ยัง *Bob* ผ่านช่องสื่อสารสาธารณะ

ขั้นตอนที่ 4 *Bob* นำตัวแปรสุ่ม Z มารวมแบบมอดุโล 2 กับกุญแจรหัสลับบิตของตน Y ดังสมการที่ (5.9) ที่ผลลัพธ์ที่ได้จะเป็นคำรหัสใหม่ V ดังนี้ "100001000110101" หลังจากนั้นตัวแปรสุ่ม V ที่ *Bob* สร้างได้จะถูกส่งผ่านกระบวนการถอดรหัสบีซีเอชซึ่งจะได้ตัวแปรสุ่ม U' ดังนี้ "10000100010" จากนั้นตัวแปรสุ่ม U' จะถูกส่งเข้าสู่วงจรเข้ารหัสบีซีเอช อีกครั้งเพื่อสร้างรหัส W' จะได้ "100001000100101" หากนำ W' มารวมกับตัวแปรสุ่ม V แบบมอดุโล 2 ที่ *Bob* ซ้ำอีกครั้งจะทำให้ *Bob* ทราบตำแหน่งบิตที่ผิดและแก้ไขบิตผิดให้กลับมาถูกต้องได้ดังสมการที่ (5.10) ดังนี้

$$\begin{aligned} Q &= V \oplus W' \\ &= (100001000110101) \oplus (100001000100101) \\ &= 000000000010000 \end{aligned}$$

หาก *Bob* นำตัวแปรสุ่ม Q ไปรวมแบบมอดุโล 2 กับกุญแจรหัสลับของตนจะทำให้ *Bob* ได้กุญแจรหัสลับที่ถูกต้องกลับคืนมาดังนี้ "111001101011010" ⊕ "000000000010000" กุญแจรหัสลับใหม่ของ *Bob* คือ "111001101001010"

5.1.3 การพัฒนาโพรโทคอลด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

การพัฒนาโพรโทคอลแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง เป็นการพัฒนาโพรโทคอลแก้ไขความผิดพลาดร่วมกับรหัสที่มีประสิทธิภาพในการแก้ไขความผิดพลาดสูง โดยรหัสคอนโวลูชันที่นำมาใช้ในการพัฒนาโพรโทคอลจะเป็นรหัสแบบสมมาตร (Systematic Convolution Code) และใช้การถอดรหัสคอนโวลูชันแบบไวเทอร์บี (Viterbi Decoding Algorithm) ด้วยรูปแบบการตัดสินใจแบบหยาบ (Hard Decision) ซึ่งวิธีการนี้จะถูกนำมาใช้แก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) เนื่องจากวิธีการนี้เหมาะสำหรับการแก้ไขความผิดพลาดในรูปแบบไบนารี ไม่สามารถที่จะนำมาใช้แก้ไขความผิดพลาดในระบบ (CV-QKD) เนื่องจากกุญแจรหัสลับจะอยู่ในรูปแบบการกระจายตัวแบบเกาส์ หากต้องการนำโพรโทคอลที่พัฒนาขึ้นนี้มาใช้แก้ไขความผิดพลาดในระบบ (CV-QKD) กุญแจรหัสลับที่กระจายตัวแบบเกาส์จะต้องถูกเปลี่ยนรูปให้อยู่ในรูปแบบข้อมูลไบนารีด้วยวิธีการแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) ก่อน ซึ่งการทำงานของวิธีการนี้แสดงดังรูปที่ 5.3 โดยขั้นตอนการทำงานมีดังต่อไปนี้

ขั้นตอนที่ 1 การหาอัตราความผิดพลาดจากการกระจายกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัม (Quantum Bit Error Rate: QBER) ดังสมการที่ (5.3) ซึ่งอัตราความผิดพลาดจากการกระจายกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัมนี้จะใช้เพื่อ กำหนดจำนวนพาริตี้บิตที่จะถูกส่งไปยัง *Bob* หากอัตราความผิดพลาดมีค่าน้อย *Alice* สามารถที่จะลดพาริตี้บิตที่จะส่งไปให้ *Bob* ผ่านเครือข่ายสาธารณะได้โดยการใช้เทคนิค Puncture ซึ่งจำนวนข้อมูลที่ส่งผ่านระบบเครือข่ายแสดงดังต่อไปนี้

$$\text{จำนวนข้อมูลที่ส่ง} = \text{จำนวนรีดันแดนซีบิต} \tag{5.11}$$

ขั้นตอนที่ 2 *Alice* ส่งกุญแจรหัสลับบิตของตนเข้าสู่วงจรเข้ารหัสคอนโวลูชัน ซึ่ง *Alice* จะได้คำรหัสที่ประกอบด้วยกุญแจรหัสลับบิตของตนและพาริตี้บิต โดย *Alice* ส่งเพียงเฉพาะพาริตี้บิตหรือรีดันแดนซีบิตไปให้ *Bob* ผ่านทางเครือข่ายสื่อสารสาธารณะ

ขั้นตอนที่ 3 เมื่อ *Bob* ได้รับพาริตี้บิตหรือรีดันแดนซีบิตแล้ว *Bob* จะนำมารวมเข้ากับกุญแจลับของตนเพื่อสร้างคำรหัสใหม่ หลังจากนั้น *Bob* จะนำคำรหัสใหม่ที่สร้างได้นี้ผ่านเข้าสู่วงจรถอดรหัสคอนโวลูชัน ซึ่งผลลัพธ์ที่ได้จากวงจรถอดรหัสคอนโวลูชันคือกุญแจรหัสลับใหม่ของ *Bob*

ตัวอย่างการแก้ไขความผิดพลาด เมื่อ *Alice* และ *Bob* มีชิฟคีย์จำนวน 11 บิต โดยชิฟคีย์ของ *Alice* มีดังต่อไปนี้ "11100110100" และชิฟคีย์ของ *Bob* มีดังต่อไปนี้ "11100110101" ซึ่งตำแหน่งของชิฟคีย์ตัวอักษรหนาแสดงตำแหน่งชิฟคีย์ที่ผิด โดยการทำงานจะเริ่มจาก

Alice นำกุญแจรหัสลับของตน "11100110100" เข้าสู่วงจรเข้ารหัสคอนโวลูชันแบบสมมาตร (Systematic Convolution Code) ด้วยเมทริกซ์กำเนิด $[4_8,7_8]$ อัตราการเข้ารหัส 1/2 ด้วยค่า Constraint length เท่ากับ 3 ซึ่งจะได้คำรหัสดังต่อไปนี้ "11101100011111000100101"

จากนั้น *Alice* จะส่งพาริตี้บิต "-1-0-1-0-1-1-0-0-0-1-1" ไปให้ *Bob* ผ่านทางช่องสื่อสารสาธารณะ เมื่อ *Bob* ได้รับพาริตี้บิต *Bob* จะนำพาริตี้บิตที่รับได้ไปรวมกับชิฟคีย์ของตนเพื่อสร้างคำรหัส (Codeword) ขึ้นมาใหม่ ซึ่งคำรหัสที่สร้างขึ้นมาใหม่มีดังนี้ "11101100011111000100111" หลังจากนั้น Bob จะนำคำรหัสที่สร้างขึ้นใหม่นี้ไปผ่านเข้าสู่วงจรถอดรหัสคอนโวลูชัน ซึ่งจะทำให้ *Bob* ได้ชิฟคีย์ใหม่ดังนี้ "11100110100" ซึ่งจะทำให้กุญแจรหัสลับที่ *Bob* และ *Alice* มีอยู่กลับมาเหมือนกัน

ดังนั้นจากสมการที่ (5.11) จำนวนบิตหรือจำนวนข้อมูลเกี่ยวกับกุญแจรหัสลับที่ส่งผ่านช่องสื่อสารสาธารณะมีค่าเท่ากับ 11 บิต

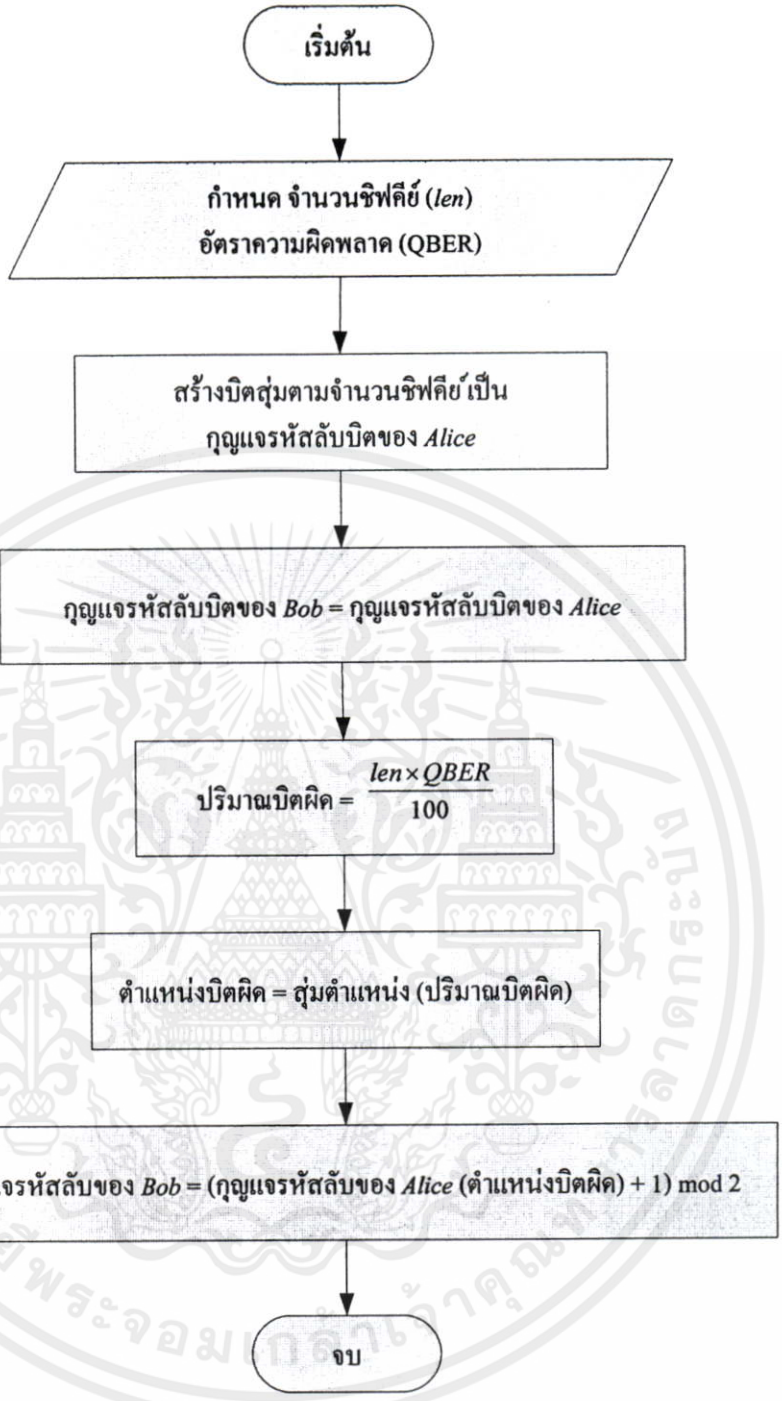
ในกรณีที่ *Alice* และ *Bob* ใช้ Puncture เมทริกซ์ $\begin{bmatrix}1&1\\1&0\end{bmatrix}$ ซึ่งจะทำให้พาริตี้บิตที่ *Alice* ส่งไปให้ *Bob* มีดังต่อไปนี้ "-1---1---1---0---0---1" หลังจากนั้น *Bob* จะสร้างคำรหัสลับใหม่โดยรวมชิฟคีย์ของตนเข้ากับพาริตี้บิตซึ่งคำรหัสลับที่ *Bob* สร้างได้มีดังต่อไปนี้ "11101100011010001000011" ผลลัพธ์ที่ได้จากการถอดรหัสคอนโวลูชันจะได้ "11100110100" ดังนั้นหากทำการใช้ Puncture จำนวนพาริตี้บิตที่ส่งจะลดลง เท่ากับ 6 บิต

5.2 การจำลองการทำงานกระบวนการรับส่งกุญแจรหัสลับเชิงควอนตัม

การจำลองการทำงานกระบวนการรับและส่งกุญแจรหัสลับเชิงควอนตัมที่ทำการออกแบบเป็นการจำลองกระบวนการส่งกุญแจรหัสลับเชิงควอนตัมเพื่อนำโพรโตคอลที่ได้พัฒนาขึ้น มาใช้ทดสอบการแก้ไขความผิดพลาดและเปรียบเทียบผลกับโพรโทคอลต่างๆเช่น โพรโตคอล CASCADE โพรโทคอล Winnow เป็นต้น ในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) และระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) ซึ่งหลักการจำลองการทำงานมีดังต่อไปนี้

5.2.1 การจำลองการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง

ระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) เป็นการส่งกุญแจรหัสลับบิตผ่านทางช่องสื่อสารเชิงควอนตัมจาก *Alice* และ *Bob* ซึ่งการจำลองการสร้างกุญแจรหัสลับเริ่มจากกำหนดความยาวของชิฟคีย์ที่ต้องการสร้างขึ้น โดยกำหนดความยาวของชิฟคีย์ทั้งหมด ซึ่งแทนด้วยตัวแปร"*len*" และกำหนดอัตราการผิดของบิตทางช่องสื่อสารเชิงควอนตัม (QBER) ซึ่งจะเป็นการจำลองการส่งกุญแจรหัสลับที่มีความผิดพลาดอยู่ จากนั้น *Alice* จะทำการสุ่มกุญแจรหัสลับบิตของตนให้มีความยาวเท่ากับความยาวของกุญแจรหัสลับที่กำหนด การสร้างกุญแจรหัสลับบิตของ *Bob* เริ่มจากการหาตำแหน่งกุญแจรหัสลับบิตผิดที่ได้จากการสุ่มตำแหน่งบิตที่ผิดตามค่าของอัตราการผิดของบิตทางช่องสื่อสารเชิงควอนตัม (QBER) ที่ได้กำหนดไว้ จากนั้นกุญแจรหัสลับของ *Bob* จะมีค่าเท่ากับกุญแจรหัสลับของ *Alice* ยกเว้นในตำแหน่งบิตที่ผิดกุญแจรหัสลับบิตของ *Bob* จะแตกต่างจากกุญแจรหัสลับบิตของ *Alice* ตามการทำงานดังรูปที่ 5.4



รูปที่ 5.4 แผนภาพการจำลองการสร้างกุญแจรหัสลับแบบไม่ต่อเนื่อง

5.2.2 การจำลองการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง

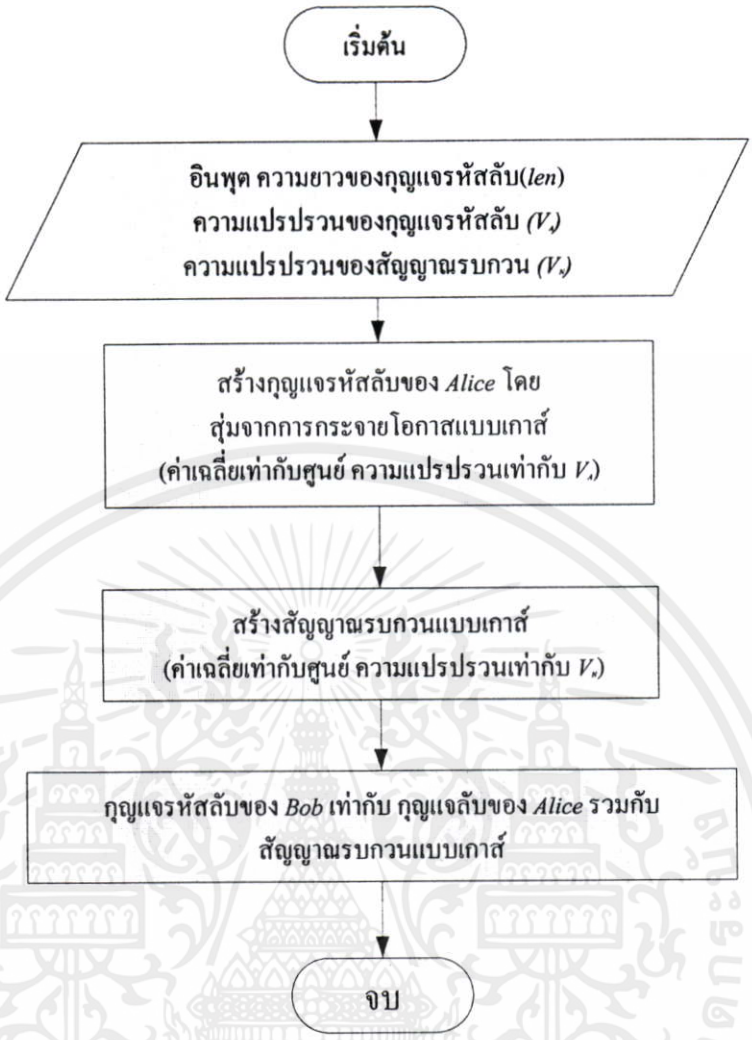
การจำลองการสร้างกุญแจรหัสลับในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD) เป็นการส่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์ผ่านช่องสื่อสารเชิงควอนตัมที่มีสัญญาณรบกวนแบบเกาส์ (Gaussian Noise) โดยการจำลองการสร้างกุญแจรหัสลับที่กระจายตัวแบบเกาส์ เริ่มจากกำหนดความยาวของกุญแจรหัสลับที่ต้องการสร้างในตัวแปร *len* ซึ่งกุญแจรหัสลับที่สร้างจะได้มาจากการสุ่มจากฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ ที่ค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวนเท่ากับ V_A หลังจากนั้น *Alice* จะทำการส่งกุญแจรหัสลับที่สร้างได้ผ่านช่องทางการสื่อสารแบบ Additive White Gaussian Noise (AWGN) โดยค่าเฉลี่ยของสัญญาณรบกวนเท่ากับศูนย์และค่าความแปรปรวนของสัญญาณรบกวนแบบเกาส์เท่ากับ V_N เมื่อกุญแจรหัสลับถูกส่งมาถึงยังภาครับ กุญแจรหัสลับของ *Bob* จะได้จากการนำกุญแจรหัสลับของ *Alice* มารวมกับสัญญาณรบกวนแบบเกาส์ภายในช่องสื่อสารดังสมการ

$$Y = X + n \tag{5.12}$$

X คือ ตัวแปรสุ่มที่แทนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Alice*
Y คือ ตัวแปรสุ่มที่แทนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Bob*
n คือ ตัวแปรสุ่มที่แทนสัญญาณรบกวนแบบเกาส์
ซึ่งกระบวนการสร้างกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Alice* และ *Bob* ทั้งหมดมีการทำงานแสดงดังรูป 5.5

5.3 การจำลองการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม

เมื่อทำการจำลองการสร้างกุญแจรหัสลับระหว่าง *Alice* และ *Bob* เสร็จเรียบร้อยแล้ว ผลที่ได้จากการจำลองระบบกระจายกุญแจรหัสลับจะทำให้กุญแจรหัสลับบางส่วนของ *Alice* และ *Bob* มีความผิดพลาดหรือเกิดความแตกต่างกันขึ้น ดังนั้นกระบวนการแก้ไขความผิดพลาดจึงถูกนำมาใช้เพื่อแก้ไขกุญแจรหัสลับบิตที่ผิดเหล่านี้ให้กลับมาถูกต้อง ซึ่งการจำลองการทำงานของการแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมมีดังต่อไปนี้



รูปที่ 5.5 แผนภาพการสร้างกุญแจรหัสลับที่กระจายตัวแบบเกาส์

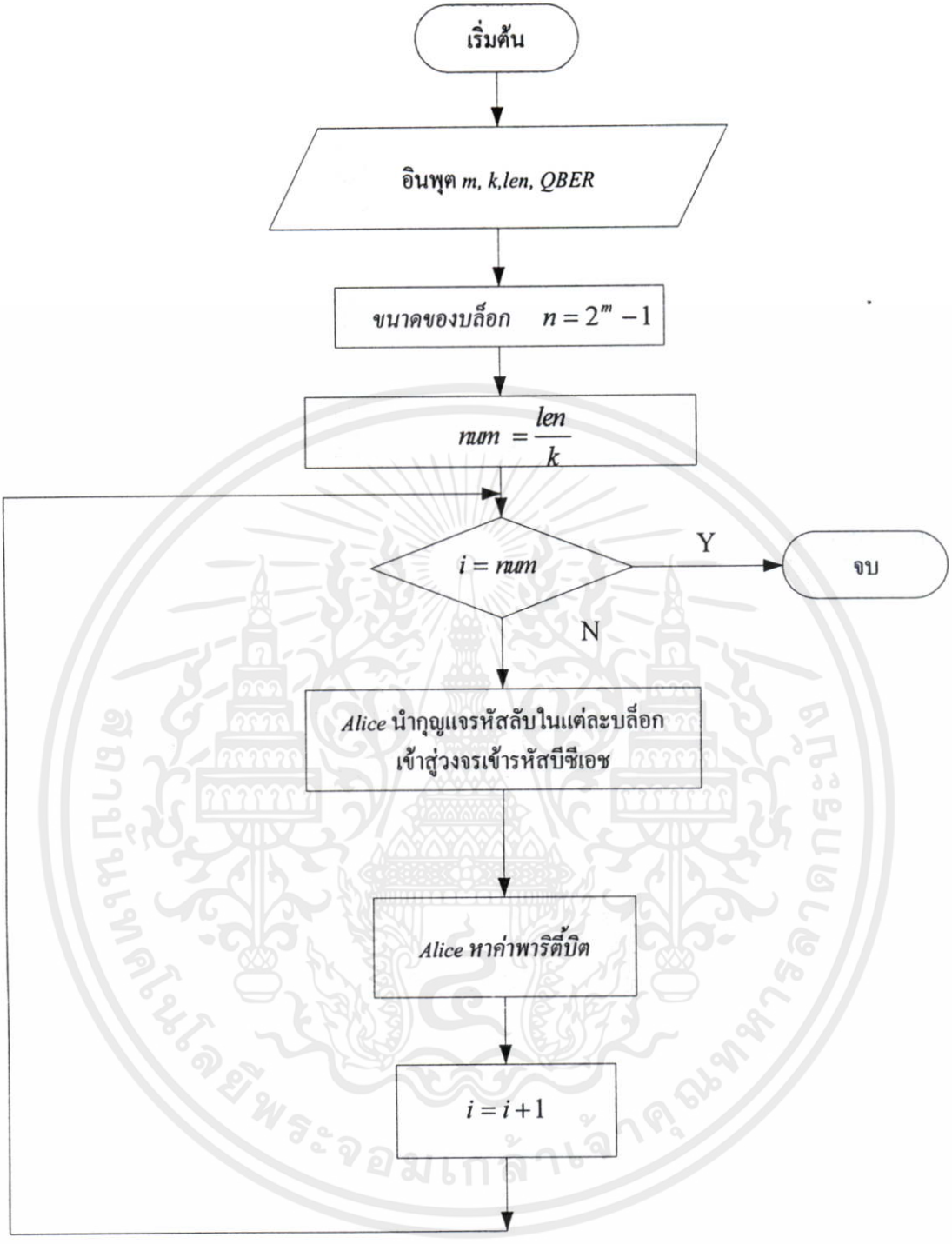
5.3.1 การจำลองการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง

การจำลองการทำงานในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) เป็นการแก้ไขความผิดพลาด ให้กุญแจรหัสลับบิตของ *Alice* และ *Bob* มีความเหมือนกัน โดยวิทยานิพนธ์เล่มนี้เลือกใช้การไกล่เกลี่ยความผิดพลาดทางตรง (Direct Reconciliation) เพื่อจำลองการทำงาน โดย *Alice* จะทำการส่งข้อมูลเกี่ยวกับกุญแจรหัสลับของตนไปให้ *Bob* ผ่านทางเครือข่ายสื่อสารสาธารณะ โดยการทำงานมีดังต่อไปนี้

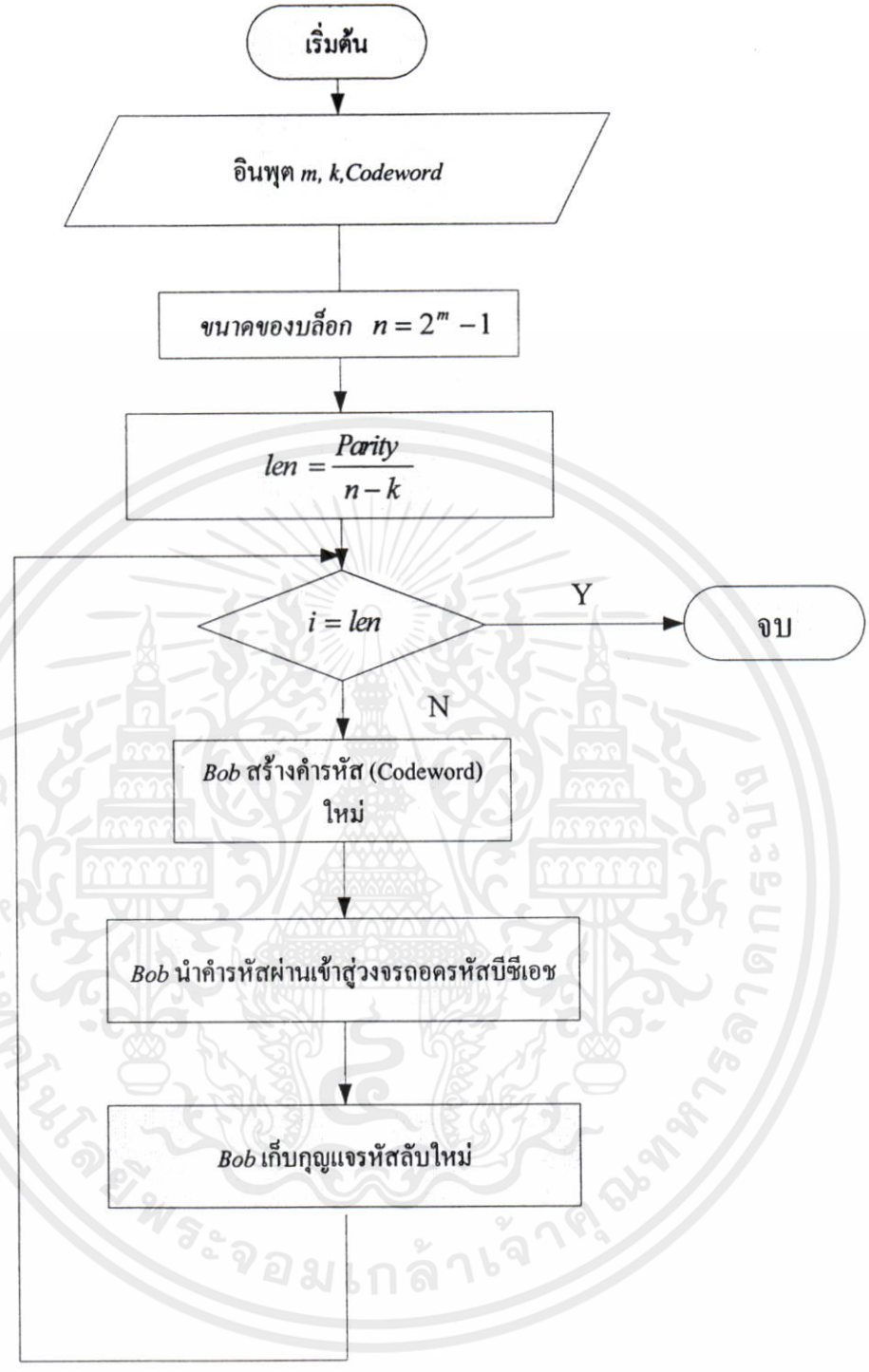
- **การแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง**

วิธีการแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง เป็นรูปแบบการแก้ไขความผิดพลาดที่เกิดจากการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) มีขั้นตอนในการจำลองการทำงานดังรูปที่ 5.6 และ 5.7 โดยในรูปที่ 5.6 แสดง

กระบวนการหาพาริตี้บิตหรือรีดันแดนซีบิตที่เกิดจากการนำกุญแจรหัสลับของ *Alice* ขนาด k บิต ผ่านเข้าสู่วงจรเข้ารหัสบีซีเอช ซึ่งจะได้คำรหัสขนาด n บิตโดยคำรหัสนี้ประกอบด้วยกุญแจรหัสลับของ *Alice* ขนาด k บิตและพาริตี้บิตขนาด $(n-k)$ บิต ซึ่งพาริตี้บิตนี้จะถูกส่งผ่านช่องสื่อสารสาธารณะไปให้ยัง *Bob* เพื่อให้ *Bob* ใช้พาริตี้บิตเหล่านี้ร่วมกับกุญแจรหัสลับบิตของตนแก้ไขความผิดพลาด รูปที่ 5.7 เป็นการแก้ไขความผิดพลาดที่เกิดขึ้นภายในกุญแจรหัสลับบิตของ *Bob* โดย Bob จะนำค่าพาริตี้บิตขนาด $(n-k)$ บิตที่ได้จาก *Alice* มารวมกับกุญแจรหัสลับของตนขนาด k บิต เพื่อสร้างคำรหัสใหม่ขนาด n บิต หลังจากนั้น *Bob* จะนำคำรหัสนี้มาผ่านเข้าสู่วงจรถอดรหัสบีซีเอช ผลลัพธ์ที่ได้จากวงจรถอดรหัสบีซีเอชจะทำให้ *Bob* ได้รับกุญแจรหัสลับบิตใหม่ที่มีเหมือนกับกุญแจรหัสลับของ *Alice* มากที่สุด (ขึ้นอยู่กับความสามารถในการแก้ไขความผิดพลาดของรหัสบีซีเอช)



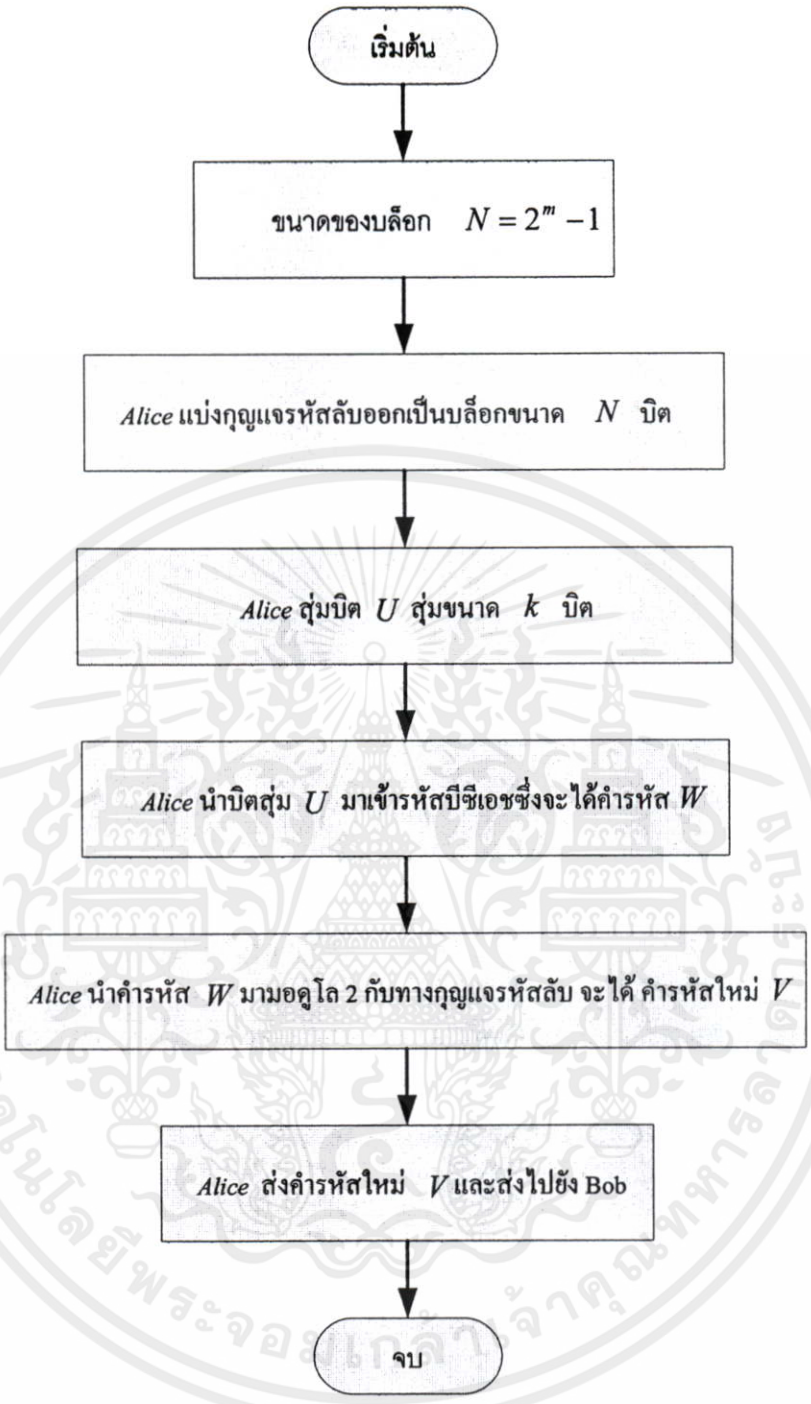
รูปที่ 5.6 กระบวนการหาพาริตี้บิตของรหัสบีซีเอชทางด้าน *Alice*



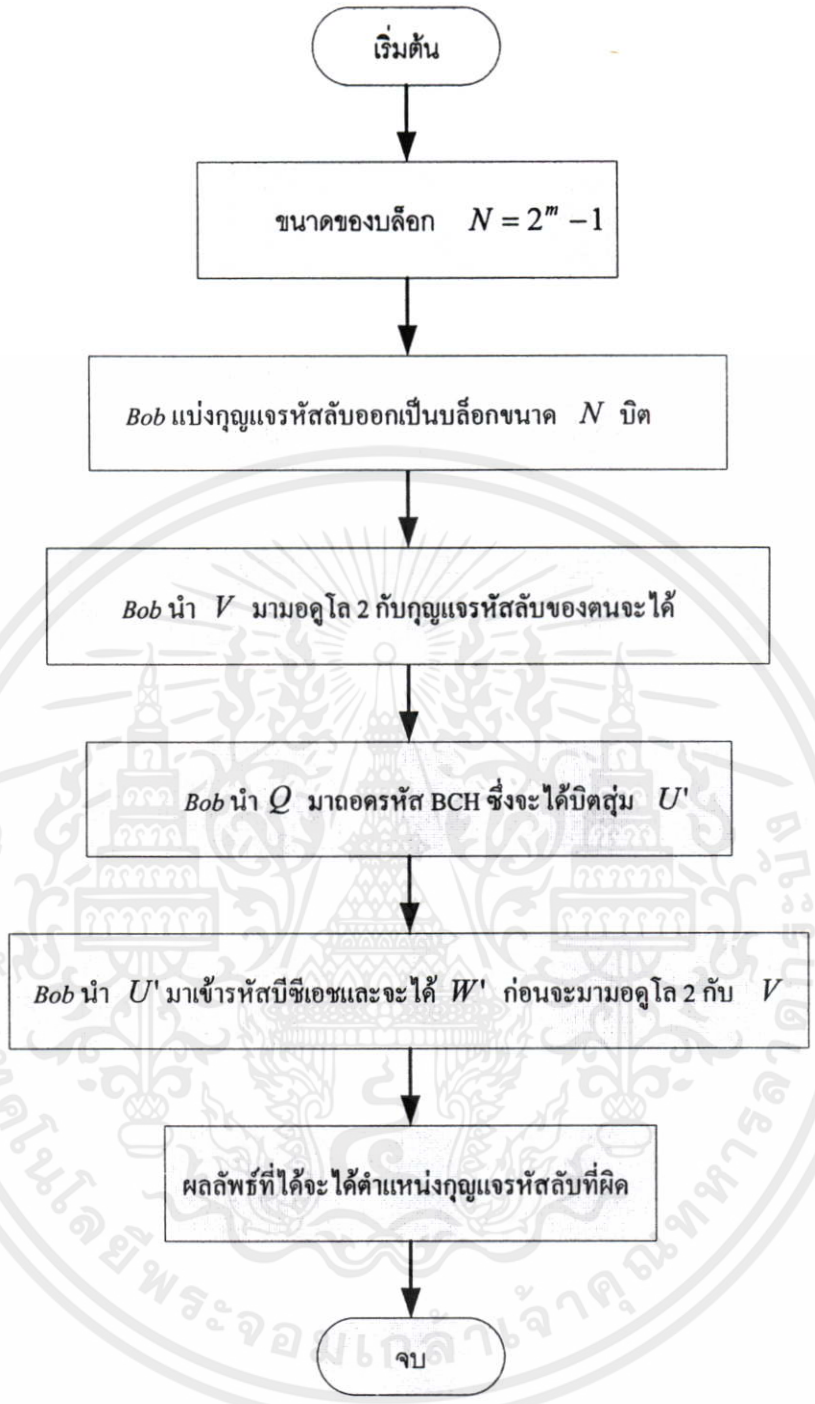
รูปที่ 5.7 กระบวนการสร้างคำรหัสใหม่และแก้ไขความผิดพลาดของ *Bob*

- **การแก้ไขความผิดพลาดจากการพัฒนาโพรโทคอลฟุรุคาวาด้วยรหัสบีซีเอช**

การจำลองการแก้ไขความผิดพลาดจากการพัฒนาโพรโทคอลฟุรุคาวาด้วยรหัสบีซีเอช มีขั้นตอนในการจำลองการทำงานดังรูปที่ 5.8 และรูปที่ 5.9 โดยในรูปที่ 5.8 แสดงกระบวนการแก้ไขความผิดพลาดทาง *Alice* ซึ่งการทำงานเริ่มจาก *Alice* ทำการแบ่งกุญแจรหัสลับของตนออกเป็นบล็อก โดยในแต่ละบล็อกจะมีขนาดเท่ากับความยาวของคำรหัสบีซีเอชหรือเท่ากับ n บิตหลังจากนั้น *Alice* จะทำการสุ่มบิตสุ่ม U ขนาด k บิตก่อนจะนำมาเข้ารหัสบีซีเอชซึ่งจะได้คำรหัส W ที่มีความยาว n บิตจากนั้น *Alice* จะนำคำรหัส W มารวมกับกุญแจรหัสลับของตนแบบมอดุโล 2 เพื่อสร้างคำรหัสใหม่ V และส่งคำรหัส V นี้ไปให้ *Bob* ผ่านทางช่องสื่อสารสาธารณะ รูปที่ 5.9 แสดงการแก้ไขความผิดพลาดหลังจาก *Bob* ได้รับคำรหัส V เรียบร้อยแล้วโดย *Bob* จะนำคำรหัสนี้ไปรวมแบบมอดุโล 2 กับรหัสลับของตนซึ่งจะได้คำรหัสใหม่ Q ก่อนจะผ่าน Q เข้าสู่วงจรถอดรหัสบีซีเอชซึ่ง *Bob* จะได้บิตสุ่ม U' จากนั้น *Bob* จะทำการหาตำแหน่งบิตที่ผิดโดยนำ U' ไปเข้ารหัสบีซีเอชซึ่งจะได้คำรหัส W' จากนั้นจะนำคำรหัสนี้ไปรวมกับ Q แบบมอดุโล 2 ดังนั้นหาก Q นี้มีค่าเท่ากับศูนย์จะสรุปได้ว่ากุญแจรหัสลับของ *Alice* และกุญแจรหัสลับของ *Bob* เหมือนกันแต่หาก Q มีค่าไม่เท่ากับศูนย์ตำแหน่งของบิตหนึ่งภายใน Q จะแสดงตำแหน่งของกุญแจรหัสลับบิตที่ผิดของ *Bob* และจะทำให้ *Bob* สามารถแก้ไขความผิดพลาดที่เกิดขึ้นได้



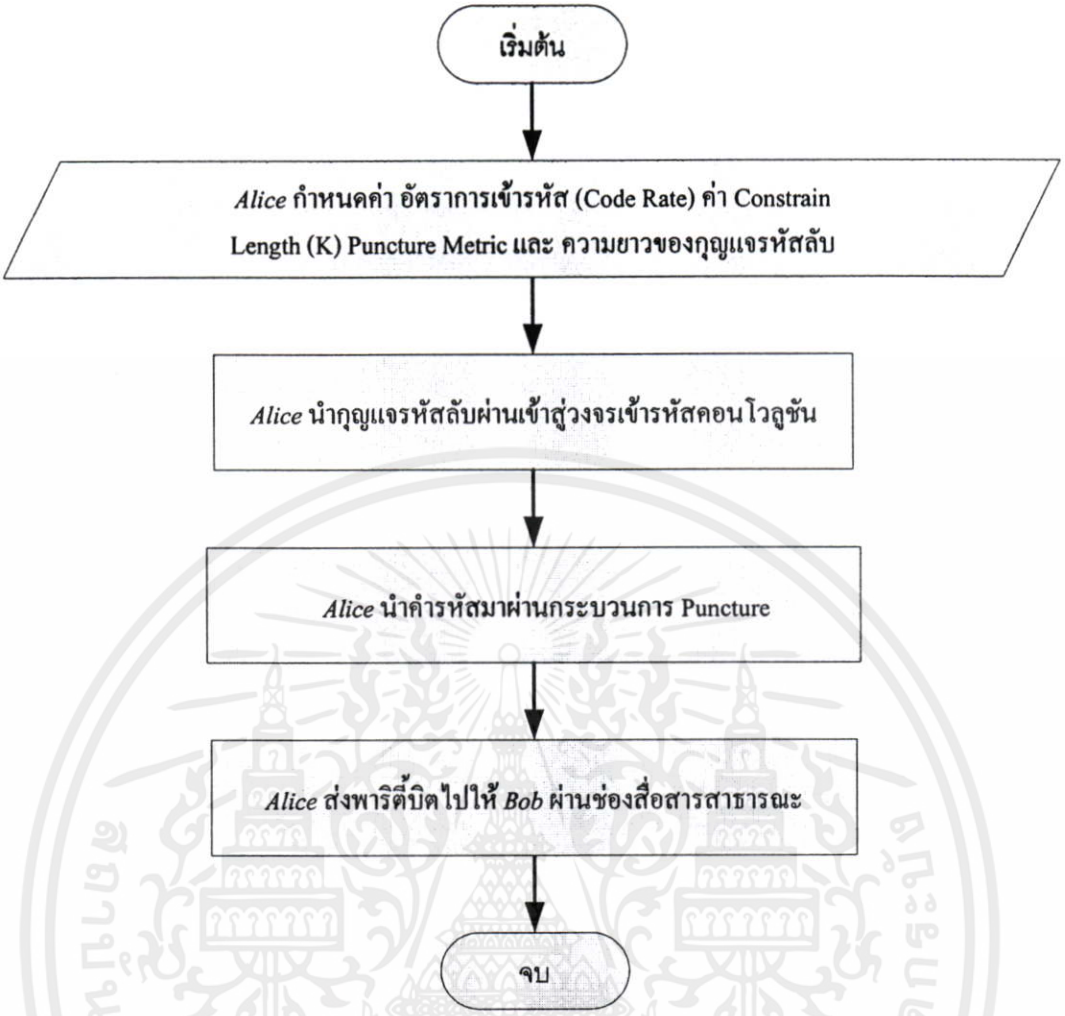
รูปที่ 5.8 การแก้ไขความผิดพลาดด้วยรหัสบีซีเอชทาง *Alice*



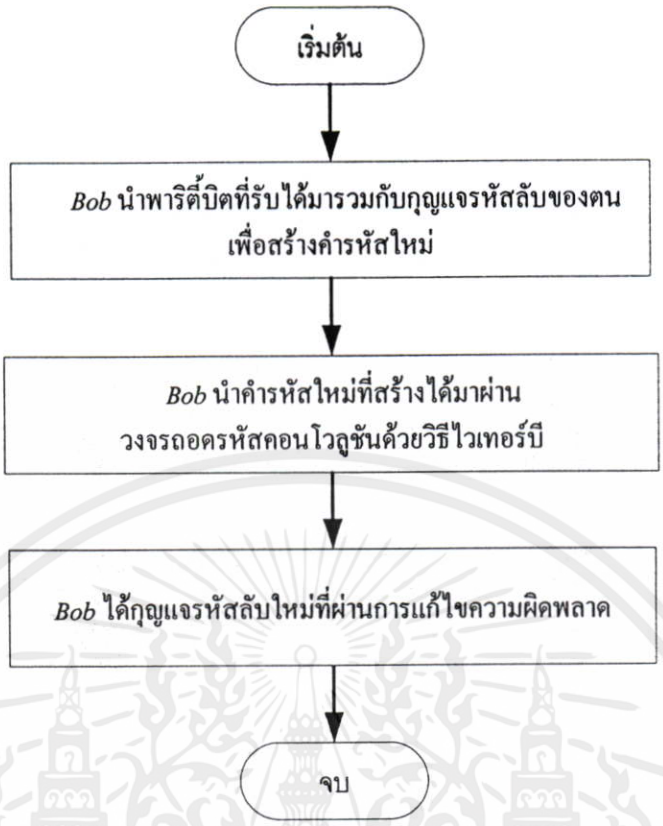
รูปที่ 5.9 การแก้ไขความผิดพลาดด้วยรหัสบีซีเอชทาง *Bob*

- **การแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง**

วิธีการแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง เป็นรูปแบบการแก้ไขความผิดพลาดที่เกิดจากการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) หรือใช้สำหรับการแก้ไขความผิดพลาดของกุญแจรหัสลับที่อยู่ในรูปไบนารี โดยรหัสคอนโวลูชันที่ใช้ในการพัฒนาโพรโทคอลแก้ไขความผิดพลาดเป็นรหัสคอนโวลูชันแบบสมมาตร (Systematic Convolution Code) ร่วมกับการตัดสินใจแบบหยาบ (Hard Decision) โดยวิทยานิพนธ์เล่มนี้จะใช้วิธีไวเทอร์บี ในการถอดรหัสคอนโวลูชัน ซึ่งขั้นตอนในการจำลองการทำงานดังรูปที่ 5.10 และ 5.11 โดยในรูปที่ 5.10 แสดงกระบวนการหาพาริตี้บิตหรือรีดันแดนซีบิตที่เกิดจากการนำกุญแจรหัสลับของ *Alice* ผ่านเข้าสู่วงจรเข้ารหัสคอนโวลูชัน โดยจำนวนพาริตี้บิตจะขึ้นอยู่กับอัตราการเข้ารหัส (Code Rate) ของรหัสคอนโวลูชัน ตัวอย่างเช่น หากใช้อัตราการเข้ารหัสที่ 1/2 คำรหัสที่สร้างขึ้นได้จะมีพาริตี้บิตเท่ากับจำนวนของกุญแจรหัสลับ นอกจากนี้ประสิทธิภาพของรหัสคอนโวลูชันจะขึ้นอยู่กับค่า Constrain Length (K) โดยพาริตี้บิตที่ได้จากวงจรเข้ารหัสคอนโวลูชันนี้จะถูกส่งผ่านช่องสื่อสารสาธารณะไปให้ยัง *Bob* เพื่อให้ *Bob* ใช้พาริตี้บิตเหล่านี้ร่วมกับกุญแจรหัสลับบิตของตนสร้างคำรหัสขึ้นมาใหม่เพื่อส่งเข้าสู่วงจรถอดรหัสคอนโวลูชัน เพื่อใช้แก้ไขความผิดพลาด ซึ่ง *Alice* สามารถลดจำนวนพาริตี้บิตที่ส่งได้โดยใช้หลักการ Puncture รูปที่ 5.11 เป็นการแก้ไขความผิดพลาดที่เกิดขึ้นภายในกุญแจรหัสลับบิตของ *Bob* โดย Bob จะนำค่าพาริตี้บิตที่ได้จาก *Alice* มารวมกับกุญแจรหัสลับของตน เพื่อสร้างคำรหัสใหม่ หลังจากนั้น *Bob* จะคำรหัสนี้มาผ่านเข้าสู่วงจรถอดรหัสคอนโวลูชันโดยวิธีไวเทอร์บี ซึ่งผลลัพธ์ที่ได้จากวงจรถอดรหัสคอนโวลูชัน จะทำให้ *Bob* ได้รับกุญแจรหัสลับบิตใหม่ที่มีเหมือนกับกุญแจรหัสลับของ *Alice* มากที่สุด



รูปที่ 5.10 กระบวนการหาพาริตี้บิตของรหัสคอนโวลูชันทางด้าน *Alice*



รูปที่ 5.11 กระบวนการสร้างคำรหัสคอนโวลูชันใหม่และแก้ไขความผิดพลาดของ *Bob*

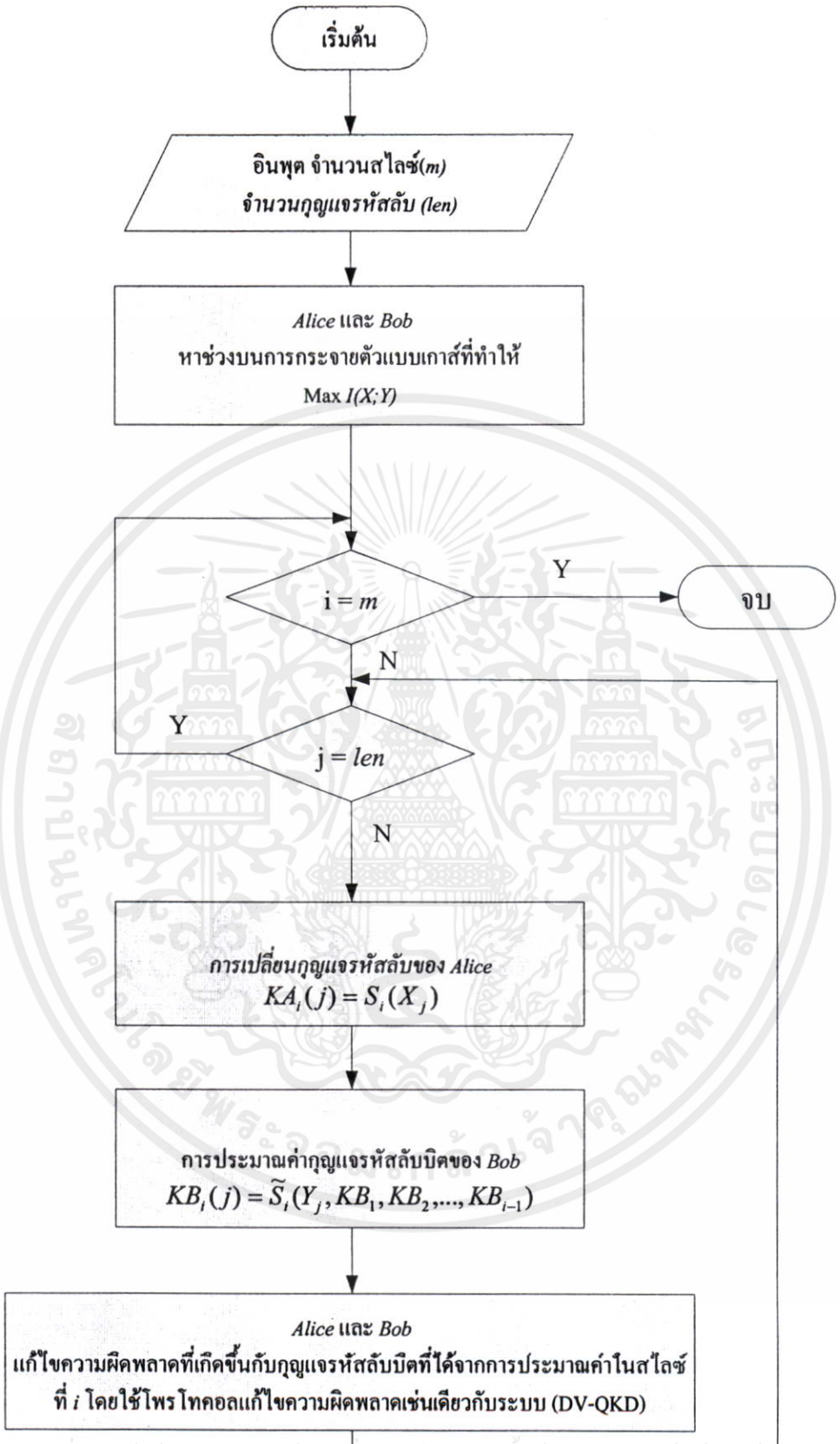
5.3.2 การจำลองการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง

การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) เป็นการส่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์ ซึ่งสัญญาณรบกวนภายในช่องสื่อสารเชิงควอนตัมเป็นสาเหตุหลักที่ทำให้กุญแจรหัสลับที่กระจายตัวแบบเกาส์เกิดความผิดพลาด ทำให้ยากที่จะแก้ไขความผิดพลาดให้กุญแจรหัสลับกลับมาถูกต้อง หากผู้ส่งและผู้รับต้องการที่จะแก้ไขความผิดพลาด ผู้ส่งและผู้รับจะต้องเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตโดยใช้วิธีการแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction) ซึ่งการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส?ให้อยู่ในรูปแบบไบนารีนี้ยังคงเกิดความผิดพลาดอยู่ ผู้ส่งและผู้รับสามารถที่จะใช้โพรโทคอลแก้ไขความผิดพลาดมาแก้ไขความผิดพลาดที่เกิดขึ้นระหว่างการแปลงกุญแจรหัสลับนี้ได้เช่นเดียวกับระบบการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) โดยหลักการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตมีหลักการทำงานดังต่อไปนี้

- **การจำลองการแก้ไขข้อผิดพลาดแบบสไลซ์**

การจำลองการทำงานของกระบวนการแก้ไขข้อผิดพลาดแบบสไลซ์มีการทำงานดังรูปที่ 5.12โดยกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Alice* แทนด้วยตัวแปรสุ่ม X และกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Bob* แทนด้วยตัวแปร Y การแก้ไขข้อผิดพลาดแบบสไลซ์เริ่มจาก *Alice*

และ *Bob* จะทำการแบ่งฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ที่ใช้ในการสุ่มเพื่อสร้างกุญแจรหัสลับออกเป็นส่วนๆ ซึ่งจำนวนช่วงทั้งหมดจะขึ้นอยู่กับจำนวนสไลซ์ที่ได้กำหนดก่อนหน้า หลังจากนั้นกุญแจรหัสลับบิตของ *Alice* จะได้จากสไลซ์ฟังก์ชัน $S(X)$ และกุญแจรหัสลับบิตของ *Bob* จะหาได้จากการประมาณค่าสไลซ์ (Slice Estimator) ดังต่อไปนี้ $KB_i(j) = \widetilde{S}_i(Y_j, KB_1, KB_2, ..., KB_{i-1})$ หลังจากทำการเปลี่ยนกุญแจรหัสลับบิตในสไลซ์ที่หนึ่ง *Alice* และ *Bob* จะแก้ไขความผิดพลาดโดยใช้โพรโทคอลแก้ไขความผิดพลาด เช่น โพรโทคอล CASCADE โพรโทคอล Winnow เป็นต้นเพื่อให้กุญแจรหัสลับบิตที่ได้มีความเหมือนกัน จากนั้น *Alice* และ *Bob* จะเริ่มเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตในสไลซ์ที่สอง หลังจากนั้น *Alice* และ *Bob* จะทำการแก้ไขความผิดพลาดที่เกิดขึ้นจากการเปลี่ยนกุญแจรหัสลับบิตในสไลซ์ที่สอง โดยใช้โพรโทคอลแก้ไขความผิดพลาด ซึ่ง *Alice* และ *Bob* จะทำเช่นนี้จนกว่าจะเท่ากับจำนวนสไลซ์ที่ได้กำหนดไว้



รูปที่ 5.12 แผนภาพการทำงานการแก้ไขความผิดพลาดแบบสไลซ์

บทที่ 6
ผลการจำลองการทำงาน

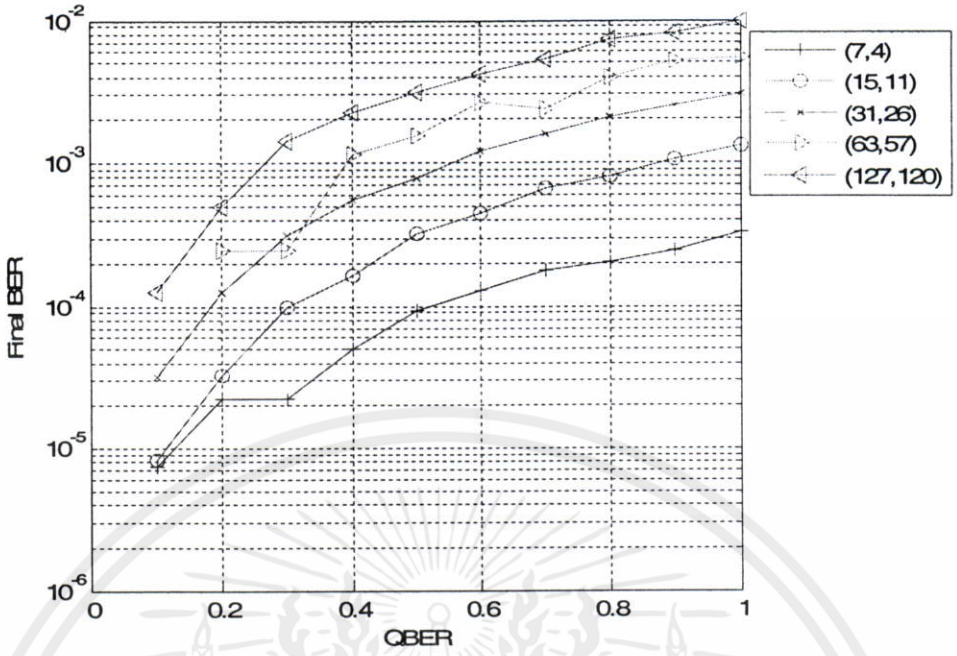
จากการออกแบบโปรแกรมจำลองการทำงานกระบวนการกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) และกระบวนการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) เพื่อนำมาใช้ในการทดสอบการจำลองการทำงานโพรโทคอลแก้ไขความผิดพลาดที่ได้พัฒนาขึ้น ในบทนี้นำเสนอผลการจำลองการทำงานกระบวนการกระจายกุญแจรหัสลับเชิงควอนตัม ผลการจำลองการทำงานการแก้ไขความผิดพลาดด้วยโพรโตคอลที่ได้พัฒนาขึ้นเมื่อเปรียบเทียบกับการทำงานของโพรโทคอลแก้ไขความผิดพลาดอื่น เช่น โพรโทคอลCASCADE โพรโทคอลWinnow เป็นต้น ดังรายละเอียดมีดังต่อไปนี้

6.1 การแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD)

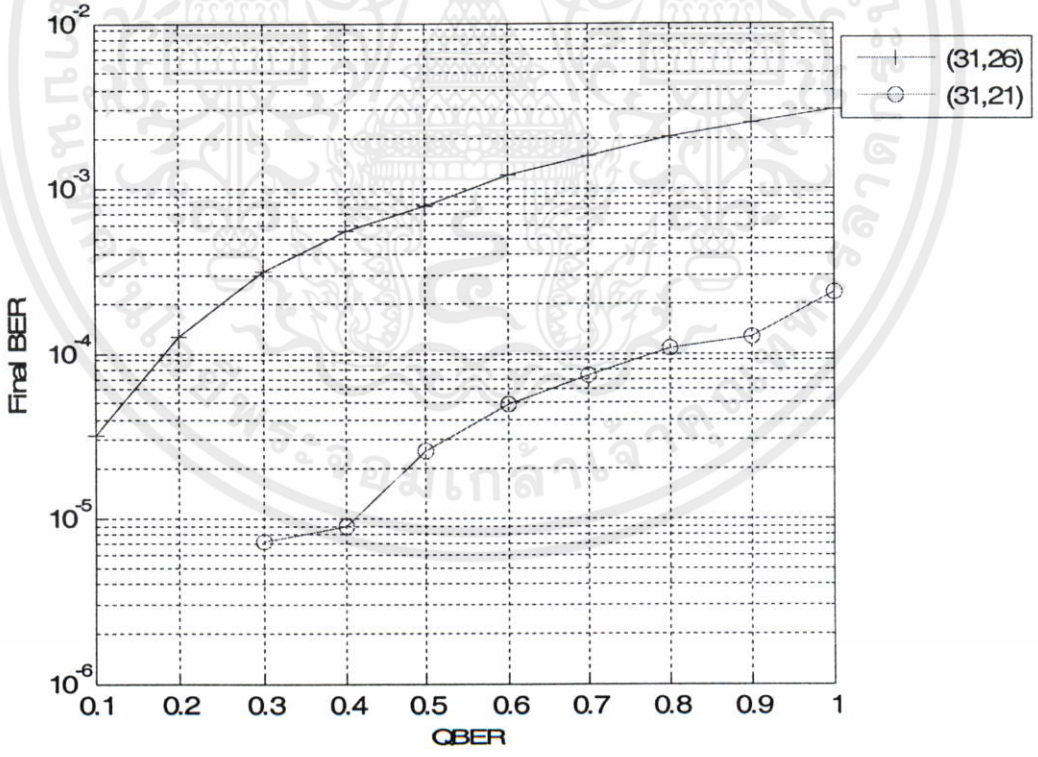
การแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง เป็นการแก้ไขกุญแจรหัสลับบิตที่เกิดความผิดพลาด ให้กลับมาถูกต้องดังเดิม ซึ่งทำให้สามารถนำกุญแจรหัสลับไปใช้ในการเข้ารหัสและถอดรหัสลับข้อมูลที่ต้องการส่ง ลดความผิดพลาดระหว่างการสื่อสาร โดยการจำลองการทำงานของโพรโทคอลที่ได้พัฒนาขึ้นมานี้เลือกใช้รูปแบบการไกล่เกลี่ยทางตรง (Direct Reconciliation) โดยผลการจำลองการทำงานของแต่ละวิธีการแก้ไขความผิดพลาดที่ได้พัฒนาขึ้นมีดังต่อไปนี้

6.1.1 กระบวนการแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

ผลการจำลองการทำงานของการไกล่เกลี่ยความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง (Side Information) โดยเป็นการจำลองการแก้ไขความผิดพลาดที่เกิดขึ้นในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) ซึ่ง *Alice* และ *Bob* ทำการเลือกขนาดของบล็อกและความสามารถในการแก้ไขความผิดพลาดของรหัสบีซีเอช ตามค่าอัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านทางช่องสื่อสารเชิงควอนตัม (QBER) ดังแสดงตามสมการที่ (5.3) ซึ่งผลการจำลองการทำงานจะพิจารณาที่อัตราความผิดพลาดที่เหลือจากการแก้ไขความผิดพลาดน้อยกว่า 10^{-3} โดยรูปที่ 6.1 แสดงผลการจำลองการทำงานเปรียบเทียบระหว่างประสิทธิภาพการแก้ไขความผิดพลาดของรหัสบีซีเอชและค่าอัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านทางช่องสื่อสารเชิงควอนตัมที่ค่าระหว่าง 0.1 ถึง 1

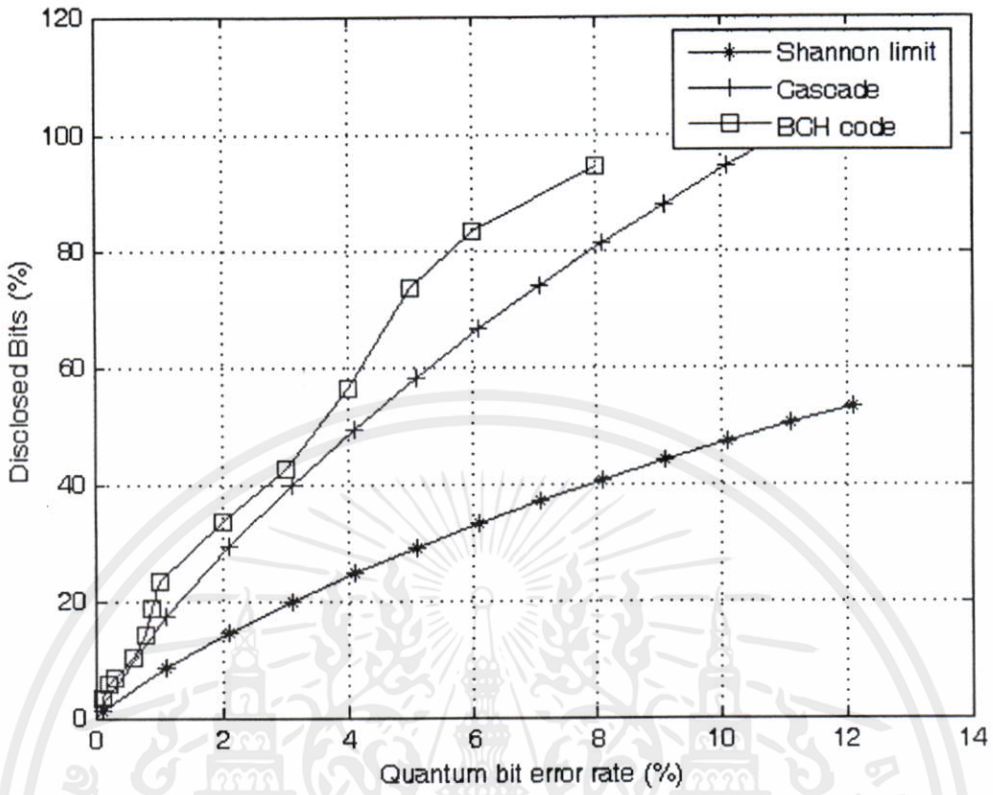


รูปที่ 6.1 การเปรียบเทียบความสามารถในการแก้ไขความผิดพลาดรหัสบีซีเอชที่อัตราความสามารถในการแก้ไขความผิดพลาดเท่ากับหนึ่ง



รูปที่ 6.2 การเปรียบเทียบประสิทธิภาพการแก้ไขความผิดพลาดของรหัสบีซีเอชที่อัตราความสามารถในการแก้ไขความผิดพลาดต่างกัน

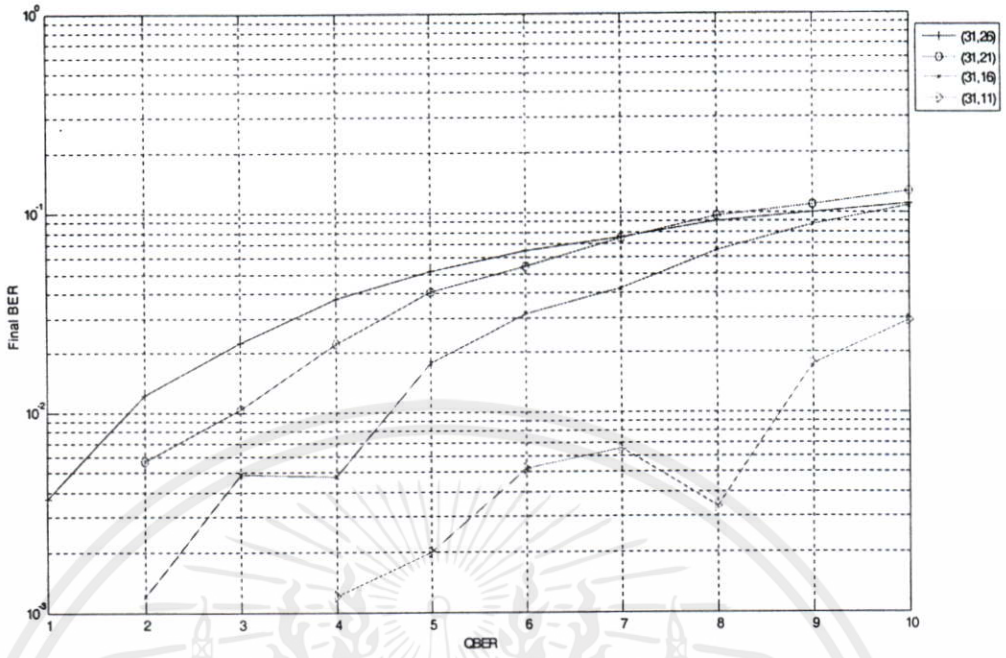
โดย *Alice* เลือกใช้รหัสบีซีเอชที่มีความสามารถในการแก้ไขความผิดพลาดได้หนึ่งบิตต่อบล็อกข้อมูล ซึ่งผลการเปรียบเทียบจะเห็นได้ว่ารหัสบีซีเอช (7,4) จะให้ประสิทธิภาพในการแก้ไขความผิดพลาดได้ดีกว่ารหัสบีซีเอชอื่นๆ โดยที่ QBER เท่ากับหนึ่งรหัสบีซีเอช (7,4) ความผิดพลาดที่ยังเหลืออยู่ยังคงน้อยกว่า 10^{-3} แต่จากสมการที่ (5.4) แสดงให้เห็นว่ารหัสบีซีเอชนี้จะมีจำนวนบิตที่ส่งผ่านช่องสื่อสารสาธารณะเป็นจำนวนทั้งสิ้น 75% ในส่วนของรหัสบีซีเอช (15,11) จะมีความผิดพลาดที่เหลือจากการแก้ไขความผิดพลาดน้อยกว่า 10^{-3} ที่ค่า QBER เท่ากับ 0.8 จากสมการที่ (5.4) รหัสบีซีเอชนี้จะทำการส่งจำนวนบิตทั้งสิ้น 36.67% ซึ่งจะเห็นได้ว่าลดลงจากรหัสบีซีเอช (7,4) ในส่วนของรหัสบีซีเอช (127,120) จากรูปสามารถที่จะนำมาใช้แก้ไขความผิดพลาดได้ที่ QBER น้อยกว่า 0.2 ซึ่งจะให้อัตราความผิดพลาดที่เหลืออยู่น้อยกว่า 10^{-3} ซึ่งจากสมการที่ (5.4) จำนวนบิตที่ส่งจะมีค่าเท่ากับ 5.83% ดังนั้นจากรูปสามารถที่จะสรุปได้ว่า หาก QBER มีค่าน้อยวิธีการที่นำเสนอนี้จะทำการแก้ไขความผิดพลาด โดยเลือกขนาดของบล็อกที่ใหญ่เพื่อลดจำนวนข้อมูลที่จะส่งผ่านเครือข่ายสาธารณะไปให้ *Bob* รูปที่ 6.2 แสดงความสามารถในการแก้ไขความผิดพลาดของโพรโทคอลที่ทำการพัฒนาขึ้นเมื่อใช้รหัสบีซีเอชด้วยความยาวของคำรหัส 31 บิตที่ความสามารถในการแก้ไขความผิดพลาดต่างๆ โดยจากรูปความสามารถในการแก้ไขความผิดพลาดหนึ่งบิตต่อบล็อกรหัสบีซีเอช(31,26) จะให้ประสิทธิภาพในการแก้ไขความผิดพลาดน้อยกว่ารหัสบีซีเอช (31,21) ที่มีความสามารถในการแก้ไขความผิดพลาดสองบิตต่อบล็อก แต่จากสมการที่ (5.4) รหัสบีซีเอช (31,26) จะส่งข้อมูลผ่านช่องสื่อสารสาธารณะคิดเป็น 19.23% เมื่อเปรียบกับรหัสบีซีเอช (31,21) ซึ่งคิดเป็น 47.61% รูปที่ 6.3 แสดงผลการจำลองการทำงานเมื่อเปรียบเทียบระหว่างจำนวนบิตที่ส่งผ่านทางช่องสื่อสารสาธารณะหรือจำนวนบิตเปิดเผยที่แสดงดังสมการที่ (5.4) และค่าอัตราความผิดพลาดของการส่งกุญแจรหัสลับบิตที่ส่งผ่านทางช่องสื่อสารเชิงควอนตัมหรือ QBER ดังสมการที่ (5.3) ระหว่างโพรโทคอลที่ทำการออกแบบโดยใช้รหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างโพรโทคอล CASCADE และข้อจำกัดของแชลนอน (Shannon Limit) โดยจำนวนบิตที่เปิดเผยของโพรโทคอลที่ออกแบบร่วมกับรหัสบีซีเอช คำนวณได้จากการนำความยาวคำรหัสที่ได้จากวงจรเข้ารหัสบีซีเอช ขนาด n บิตลบกับความยาวของบล็อกกุญแจรหัสลับขาด k บิต ดังสมการที่ (5.4) ในส่วนของจำนวนบิตที่ส่งผ่านระบบสื่อสารของโพรโทคอลCASCADE สามารถหาได้จากสมการที่ (4.24) และข้อจำกัดของแชลนอนสามารถหาได้จากสมการที่ (4.15) จากรูปวิธีการที่นำเสนอนี้สามารถแก้ไขความผิดพลาดได้ที่ค่าอัตราการผิดพลาดของการส่งกุญแจรหัสลับผ่านทางช่องสื่อสารเชิงควอนตัม (QBER) มีค่าน้อยกว่า 8% แต่ถ้าค่า QBER มีค่ามากกว่า 8% วิธีการที่นำเสนอนี้จะไม่สามารถนำมาใช้ในการแก้ไขความผิดพลาดได้เนื่องจากวิธีการนี้จะทำการส่งข้อมูลเกี่ยวกับกุญแจรหัสลับมากเกินไปซึ่งอาจจะทำให้ *Eve* สามารถที่จะนำข้อมูลส่วนนี้ไปสร้างหรือทำสำเนากุญแจรหัสลับใหม่ขึ้นมาได้



รูปที่ 6.3 การเปรียบเทียบจำนวนพาริตี้บิตที่ส่ง

6.1.2 การนำรหัสบีซีเอชมาพัฒนาโพรโทคอลของฟุรุคาวา

ผลการจำลองการทำงานกระบวนการแก้ไขความผิดพลาดด้วยการนำรหัสบีซีเอช มาพัฒนาโพรโทคอลของฟุรุคาวา ซึ่งเป็นรูปแบบการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) โดยวิธีการที่ออกแบบจะเลือกความสามารถในการแก้ไขความผิดพลาดและขนาดของบล็อกของรหัสบีซีเอชขึ้นอยู่กับอัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านทางช่องสื่อสารเชิงควอนตัมที่สามารถหาได้จากสมการ (5.3) เพื่อให้อัตราความผิดพลาดหลังจากการแก้ความผิดพลาดเหลือน้อยกว่า 10^{-3} ซึ่งรูปที่ 6.4 แสดงกราฟความสัมพันธ์ระหว่างอัตราความผิดพลาดที่เหลืออยู่ภายหลังจากการแก้ไขความผิดพลาด ที่ค่าอัตราความผิดพลาดการการส่งกุญแจรหัสลับบิตทางช่องสื่อสารเชิงควอนตัม (QBER) ต่างๆ เมื่อใช้รหัสแฮมมิงที่มีความยาวของคำรหัส 31 บิต และความสามารถในการแก้ไขความผิดพลาดต่างๆ ซึ่งจากผลการจำลองการทำงานรหัสบีซีเอช (31,11) จะมีความสามารถในการแก้ไขความผิดพลาดสูงสุดจะมีประสิทธิภาพในการแก้ไขความผิดพลาดสูงสุดเช่นเดียวกัน แต่จากสมการที่ (5.7) รหัสบีซีเอช (31,11) นี้จะทำการส่งข้อมูลผ่านระบบเครือข่ายมากที่สุดเช่นเดียวกัน ในการจำลองการทำงานที่อัตราความผิดพลาด (QBER) เท่ากับ 1% ความยาวของกุญแจรหัสลับบิตทั้งหมดเท่ากับ 10,200 บิต เพื่อเปรียบเทียบการทำงานกับโพรโทคอลแก้ไขความผิดพลาดอื่นๆ



รูปที่ 6.4 การเปรียบเทียบประสิทธิภาพของรหัสบีซีเอชเมื่อนำมาใช้ในการพัฒนาวิธีฟุรุคาวา

ผลการจำลองการทำงานเป็นการเปรียบเทียบระหว่างจำนวนรอบของการติดต่อระหว่าง *Alice* และ *Bob* (Interactivity) จำนวนบิตที่ส่งผ่านช่องสื่อสารสาธารณะและอัตราความผิดพลาดของบิตที่เหลืออยู่เมื่อเปรียบเทียบกับโพรโทคอลWinnow ที่ทำการเปรียบเทียบพาริตี้บิตและแก้ไขความผิดพลาด หากพบพาริตี้บิตที่นำมาเปรียบเทียบมีความแตกต่างกันและวิธีฟุรุคาวา แสดงดังตารางที่ 6.1 ซึ่งวิธีที่นำเสนอจะลดจำนวนรอบการติดต่อระหว่าง *Alice* และ *Bob* เหลือการติดต่อเพียงหนึ่งรอบ เมื่อเปรียบเทียบกับโพรโทคอล Winnow ที่ใช้การติดต่อสองรอบ (ในการจำลองการทำงานนี้เลือกจำนวนรอบเท่ากับสองรอบซึ่งอาจจะมีจำนวนรอบในการติดต่อมากขึ้นหากต้องการลดจำนวนกุญแจรหัสลับบิตผิดลงน้อยที่สุด) และวิธีของฟุรุคาวา ที่มีการติดต่อโดยเฉลี่ยสูงถึง 16.42 รอบ ในส่วนของจำนวนบิตที่ส่งผ่านระบบสื่อสารสาธารณะหรือจำนวนบิตเปิดเผยตามสมการที่ (5.4) วิธีการที่ออกแบบจะมีจำนวนบิตที่ส่งผ่านระบบเครือข่ายสาธารณะทั้งสิ้น 21.96% เมื่อเทียบกับจำนวนกุญแจรหัสลับทั้งหมด จากสมการ (4.30) โพรโทคอล Winnow จะมีจำนวนบิตที่ส่งทั้งสิ้น 15.29% และจากสมการที่ (4.38) โพรโทคอลฟุรุคาวาจะทำการส่งพาริตี้บิตน้อยที่สุดคือเท่ากับ 10.96% ในส่วนของขนาดของบล็อก วิธีที่นำเสนอใช้ขนาดของบล็อกเท่ากับ 255 บิตและความสามารถแก้ไขความผิดพลาดของรหัสบีซีเอช เท่ากับ 7 บิตต่อบล็อก โฟรโทคอล Winnow ที่ใช้ในการจำลองการทำงานจะใช้รหัสแฮมมิง (7,4) ในส่วนของวิธีฟุรุคาวาจะไม่สามารถบอกขนาดบล็อกได้เนื่องจากมีการติดต่อระหว่าง *Alice* และ *Bob* จำนวนมากซึ่งในแต่ละรอบของการติดต่อจะใช้รหัสแฮมมิงที่ขนาดของบล็อกต่างกัน ดังนั้นจึงไม่สามารถระบุขนาดของบล็อกได้

ตารางที่ 6.1 การจำลองการแก้ไขความผิดพลาด ที่ค่าอัตราการผิดของบิต 0.01 (1%) และจำนวนกุญแจรหัสลับ 10,200 บิต

วิธี	รหัสบีซีเอช	Winnow	วิธีฟุรุคาวา
จำนวนรอบ	1	2	16.42
บิตที่ส่ง	21.96%	15.29%	10.69%
BER	0	6.312×10^{-4}	0
(n,k)	(255,199)	(7,4)	-
t	7	1	1
Shannon Limit	8.08%	8.08%	8.08%

ตารางที่ 6.2 การจำลองการแก้ไขความผิดพลาด ที่ค่าอัตราการผิดของบิต 0.1 (10%) และจำนวนกุญแจรหัสลับ 10,200 บิต

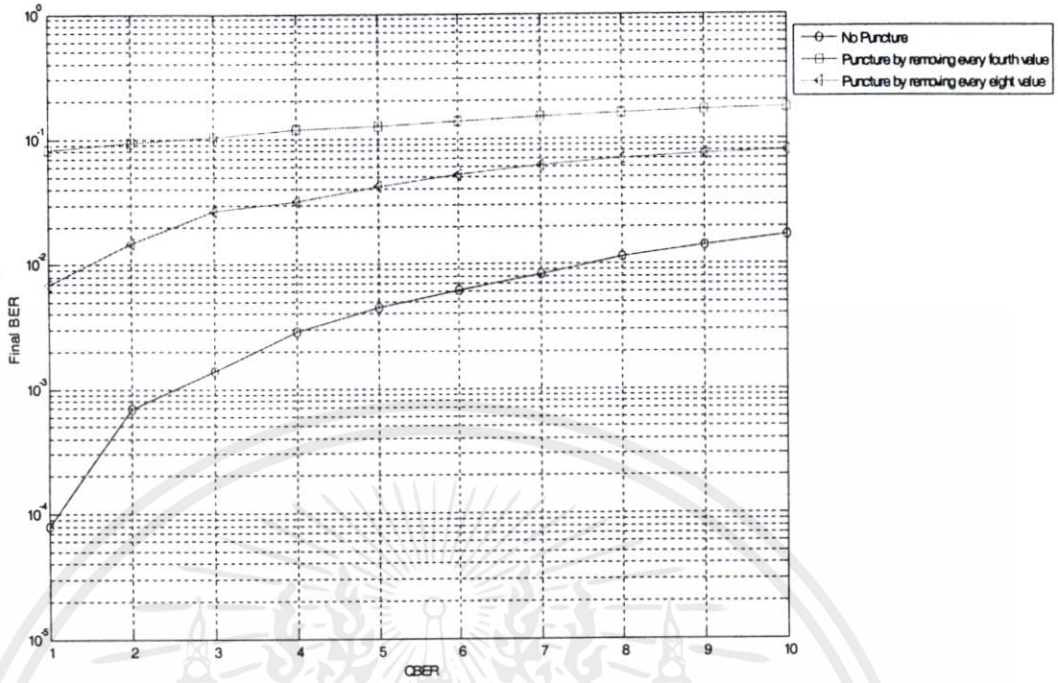
วิธี	รหัสบีซีเอช	Winnow	วิธีฟุรุคาวา
จำนวนรอบ	1	2	18.20
บิตที่ส่ง	81.56%	27.96%	66.9%
BER	0	4.9×10^{-2}	0
(n,k)	(255,47)	(7,4)	-
t	42	1	1
Shannon Limit	46.96%	46.96%	46.96%

การจำลองการทำงานที่อัตราความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมสูงขึ้นเป็น 10% จำนวนกุญแจรหัสลับที่นำมาใช้ในการจำลองการทำงานทั้งสิ้น 10,200 บิต ซึ่งผลการจำลองการทำงานจำนวนรอบของการติดต่อวิธีที่นำเสนอนี้จะมีการติดต่อระหว่าง *Alice* และ *Bob* เพียงหนึ่งรอบเมื่อเปรียบเทียบกับโพรโทคอล Winnow ที่ใช้จำนวนรอบในการติดต่อสองรอบ และวิธีฟุรุคาวาจะมีจำนวนการติดต่อเฉลี่ยเพิ่มขึ้นเป็น 18.2 รอบ ในส่วนของจำนวนพาริตี้บิตที่ส่งผ่านเครือข่ายสาธารณะ วิธีที่นำเสนอจะมีมากที่สุดคือ 81.56% เมื่อเทียบกับความยาวของกุญแจรหัสลับทั้งหมด โพรโทคอล Winnow จะส่งพาริตี้บิตทั้งสิ้นเท่ากับ 27.96% และวิธีฟุรุคาวาจะส่งพาริตี้บิตน้อยที่สุดเท่ากับ 66.9% โดยวิธีที่ออกแบบใช้รหัสบีซีเอชขนาดของบล็อกเท่ากับ 255 บิต ความสามารถในการแก้ไขความผิดพลาดเท่ากับ 42 บิตในส่วนของโพรโทคอล Winnow ใช้รหัสแฮมมิง ขนาดของบล็อกเท่ากับ 7 บิตและความสามารถในการแก้ไขความผิดพลาดเท่ากับหนึ่งบิตต่อบล็อก ในส่วนวิธีฟุรุคาวาจะใช้ขนาดของบล็อกแตกต่างกันในการแก้ไขความผิดพลาดในแต่ระ

รอบของการติดต่อ เพื่อให้มีจำนวนบิตเปิดเผยน้อยที่สุดและให้ขนาดของบล็อกเหมาะสมที่สุดตามอัตราความผิดพลาดที่ยังคงเหลืออยู่ในการแก้ไขความผิดพลาดในแต่ละรอบ

6.1.3 กระบวนการแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

ผลการจำลองการทำงานของการไกล่เกลี่ยความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง โดยเป็นการจำลองการแก้ไขความผิดพลาดที่เกิดขึ้นในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) ซึ่งรหัสคอนโวลูชันที่นำมาใช้ในการจำลองการทำงานเป็นรหัสแบบสมมาตร (Systematic Convolution Code) ด้วยค่า Constraint Length เท่ากับสาม อัตราการเข้ารหัส (Code Rate) เท่ากับ 1/2 และเมทริกซ์กำเนิด (Generator Metric) $[4_8,7_8]$ โดยการจำลองการทำงานของวิธีการนี้จะส่งเพียงพาริตี้บิตผ่านช่องเครือข่ายสาธารณะ ไปยัง *Bob* และ *Bob* จะนำพาริตี้บิตเข้าไปรวมกับกุญแจรหัสลับของตนเพื่อสร้างคำรหัสลับใหม่ ก่อนจะผ่านเข้าสู่วงจรถอดรหัสคอนโวลูชัน ซึ่งจะทำให้ *Bob* ได้กุญแจรหัสลับใหม่ที่ผ่านการแก้ไขความผิดพลาดเรียบร้อย นอกจากนี้หากอัตราความผิดพลาดจากการส่งกุญแจรหัสลับผ่านช่องสื่อสารเชิงควอนตัม (QBER) มีค่าน้อย *Alice* และ *Bob* สามารถใช้เทคนิค Puncture เพื่อลดจำนวนพาริตี้บิตที่ส่งผ่านระบบเครือข่ายสาธารณะ จากรูปที่ 6.5 แสดงผลการจำลองการทำงานเมื่อนำรหัสคอนโวลูชันมาใช้ในการแก้ไขความผิดพลาดที่ค่าอัตราความผิดพลาด (QBER) ที่ค่าต่างๆ โดยจะเป็นผลการเปรียบเทียบระหว่างการนำรหัสคอนโวลูชันมาใช้ในการแก้ไขความผิดพลาดและการใช้เทคนิค Puncture เพื่อหาประสิทธิภาพการแก้ไขความผิดพลาด ซึ่งจากรูป รหัสคอนโวลูชันที่นำมาใช้งานจะแก้ไขความผิดพลาดให้มีอัตราความผิดพลาดเหลืออยู่น้อยกว่า 10^{-3} ที่ QBER น้อยกว่าสอง แต่เมื่อนำหลักการ Puncture มาใช้โดยการตัดตำแหน่งของพาริตี้บิตในทุกๆ ตำแหน่งที่สี่ของพาริตี้บิตออกและตัดตำแหน่งพาริตี้บิตทุกๆ ตำแหน่งที่แปดออก จะให้



รูปที่ 6.5 ประสิทธิภาพการนำรหัสคอนโวลูชันมาใช้ในการแก้ไขความผิดพลาด

ตารางที่ 6.3 การจำลองการแก้ไขความผิดพลาดด้วยรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง

วิธี	รหัสคอนโวลูชัน	Winnow	วิธีฟุรุคาวา
จำนวนรอบ	1	2	16.42
บิตที่ส่ง	96%	15.29%	10.69%
BER	9.8×10^{-4}	6.312×10^{-4}	0

ประสิทธิภาพการแก้ไขความผิดพลาดลดลง แต่จะลดจำนวนบิตที่ส่งผ่านช่องสื่อสารสาธารณะเมื่อเปรียบเทียบกับรหัสคอนโวลูชันที่ไม่ใช้เทคนิค Puncture เมื่อนำรหัสคอนโวลูชันร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง มาใช้ในการแก้ไขความผิดพลาดที่ค่าอัตราความผิดพลาดระหว่างการส่งกุญแจรหัสลับ (QBER) เท่ากับ 1% ความยาวของกุญแจรหัสลับเท่ากับ 10,000 บิต วิธีการนี้จะลดการติดต่อสื่อสารระหว่าง *Alice* และ *Bob* เมื่อเปรียบเทียบกับโพรโทคอล Winnow ที่ใช้รหัสแฮมมิง (7,4) ความสามารถในการแก้ไขความผิดพลาดเท่ากับหนึ่งบิตต่อบล็อก และวิธีฟุรุคาวาที่ใช้รหัสแฮมมิง ซึ่งไม่สามารถระบุขนาดของบล็อกได้เนื่องจากการทำงานของวิธีฟุรุคาวาในแต่ละรอบของการแก้ไขความผิดพลาดจะใช้ขนาดของบล็อกไม่เท่ากัน เพื่อให้การส่งข้อมูลระหว่างผู้ส่งและผู้รับน้อยที่สุด และให้ประสิทธิภาพการแก้ไขความผิดพลาดดีที่สุด จากตารางวิธีการที่นำเสนอนี้จะใช้เทคนิคการ Puncture เพื่อลดจำนวนบิตที่ส่งผ่านระบบสื่อสาร

สาธารณะ โดยจะตัดพาริตี้บิตออกหนึ่งบิตเมื่อส่งพาริตี้บิตครบ 400 บิต จะทำการส่งส่งพาริตี้บิตของวิธีการที่นำเสนอนี้มีค่าเท่ากับ 96% ซึ่งจะมากกว่าโพรโทคอล Winnow ที่จะแบ่งบล็อกกุญแจรหัสลับบิตออกเป็นบล็อกขนาด 8 บิตและทำการเปรียบเทียบพาริตี้บิต หากพบพาริตี้บิตที่แตกต่างโพรโทคอล Winnow จะใช้รหัสแฮมมิงในการแก้ไขความผิดพลาด จากสมการที่ (4.30) โพรโทคอล Winnow จะทำการส่งพาริตี้บิตทั้งสิ้น 15.29 % และจากสมการที่ (4.38) วิธีฟุรุคาวาจะส่งพาริตี้บิตทั้งสิ้น 10.69% เมื่อเทียบกับจำนวนกุญแจรหัสลับทั้งหมด

6.2 การแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD)

การกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD) เป็นระบบในการส่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์ ซึ่งสัญญาณรบกวนภายในช่องสื่อสารเชิงควอนตัมเป็นสาเหตุที่ทำให้กุญแจรหัสลับที่ส่งเกิดความผิดพลาด ทำให้ผู้รับยากที่จะแก้ไขความผิดพลาดให้กลับมาถูกต้องดังเดิมได้ หากผู้ส่งและผู้รับต้องการแก้ไขความผิดพลาด ผู้ส่งและผู้รับจะต้องทำการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิตก่อน ซึ่งกุญแจรหัสลับบิตนี้จะง่ายในการแก้ไขความผิดพลาดที่เกิดขึ้นโดยสามารถใช้โพรโทคอลแก้ไขความผิดพลาด เช่น โพรโทคอลCASCADE หรือโพรโทคอลWinnow เป็นต้น ซึ่งผลการจำลองการทำงานการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่องมีดังต่อไปนี้

- **ผลการจำลองการทำงานการแก้ไขข้อผิดพลาดแบบสไลซ์**

การจำลองการทำงานของการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง ดังที่นำเสนอวิธีการออกแบบและจำลองการทำงานในบทที่ผ่านมา ซึ่งผลการจำลองการทำงานแสดงได้ดังตารางที่ 6.4 โดยกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Alice* ได้จากการสุ่มจากฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ที่ค่าเฉลี่ยเท่ากับศูนย์และค่าความแปรปรวนเท่ากับหนึ่ง ในส่วนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของ *Bob* เกิดจากการนำกุญแจรหัสลับของ *Alice* รวมกับสัญญาณรบกวนแบบเกาส์ที่ค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวนเท่ากับ $1/\sqrt{3}$ การประมาณค่ากุญแจรหัสลับบิตของ *Alice* และ *Bob* จะกำหนดจำนวนสไลซ์ทั้งสิ้นสี่สไลซ์ ซึ่งจะทำให้ได้จุดหรือค่าจำนวนจริงที่ใช้ในการแบ่งกุญแจรหัสลับทั้งสิ้น 16 ค่าดังแสดงในตารางที่ 6.4 [33] โดยผลการจำลองการทำงานและผลการเปรียบเทียบกับผลการจำลองการทำงานที่เสนอในบทความ [33] แสดงดังตารางที่ 6.5

ตารางที่ 6.4 ค่าจำนวนจริงที่แบ่งช่วงบนฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์

ช่วงจากการกระจายตัวแบบเกาส์	ค่าการกระจายตัวแบบเกาส์ (x)
$-\tau_1 = \tau_{15}$	2.347
$-\tau_2 = \tau_{14}$	1.808
$-\tau_3 = \tau_{13}$	1.411
$-\tau_4 = \tau_{12}$	1.081
$-\tau_5 = \tau_{11}$	0.768
$-\tau_6 = \tau_{10}$	0.514
$-\tau_7 = \tau_9$	0.254
τ_8	0

ตารางที่ 6.5 ผลการจำลองการทำงานการแก้ไขข้อผิดพลาดแบบสไลซ์

วิธีการจำลอง / สไลซ์	การจำลองเมื่อใช้บิตเริ่มต้นเป็นของ *Bob*	การจำลองเมื่อใช้บิตเริ่มต้นเป็นของ *Alice*	ความผิดพลาดที่เสนอในบทความ [33]
1	0.495	0.4953	0.496
2	0.49235	0.47537	0.468
3	0.4215	0.33985	0.25
4	0.24495	0.0545	0.02

ถ้ากำหนดจำนวนสไลซ์เท่ากับหนึ่งกุญแจรหัสลับบิตที่ *Alice* และ Bob จะประมาณค่าได้ไบนารีบิตเป็น "1" ก็ต่อเมื่อค่ากุญแจรหัสลับที่กระจายตัวแบบเกาส์น้อยกว่าหรือเท่ากับศูนย์และมีค่าไบนารีบิตเป็น "0" เมื่อค่ากุญแจรหัสลับที่กระจายตัวแบบเกาส์มากกว่าศูนย์ดังต่อไปนี้

$$S(x) = \begin{cases} 0 & x > 0 \\ 1 & x \le 0 \end{cases}$$

ผลที่ได้จากการจำลองการประมาณค่ากุญแจรหัสลับบิตจากกุญแจรหัสลับที่กระจายตัวแบบเกาส์ของทั้ง *Alice* และ *Bob* เมื่อกำหนดจำนวนสไลซ์เท่ากับหนึ่งจะมีอัตราความผิดพลาดเท่ากับ 16.7 % จากผลการจำลองการทำงานของการแก้ไขข้อผิดพลาดแบบสไลซ์ในตารางที่ 6.5 เมื่อนำรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง มาใช้ในการแก้ไขความผิดพลาดจากการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตด้วยวิธีการแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC)

ตารางที่ 6.6 การแก้ไขความผิดพลาดด้วยรหัสบีซีเอชร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างในระบบการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง

สไลซ์	*QBER*	โพรโทคอล	บิตที่ส่ง	ข้อจำกัดของแชลนอน
1	0.496	-	l	0.999
2	0.468	-	l	0.997
3	0.33	-	l	0.9149
4	0.05	BCH	$73.46l$	0.2864

ผลการจำลองการทำงานแสดงดังตารางที่ 6.6 โดยกำหนดจำนวนสไลซ์ทั้งสิ้นสี่สไลซ์ กุญแจรหัสลับที่ *Alice* ใช้ในการส่งจะถูกสุ่มจากฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ที่ค่าเฉลี่ยเท่ากับศูนย์และค่าความแปรปรวนเท่ากับหนึ่ง ช่องสื่อสารที่ใช้ในการจำลองการทำงานแบบ AWGN สร้างจากการสุ่มจากฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบเกาส์ที่ค่าเฉลี่ยเท่ากับศูนย์และค่าความแปรปรวนเท่ากับ $1/\sqrt{3}$ ซึ่งผลการจำลองการทำงานในสไลซ์ที่หนึ่งจะมีความผิดพลาดที่เกิดขึ้นจากการแปลงค่ากุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นค่ากุญแจรหัสลับบิตมีอัตราความผิดพลาด 49.6% ที่อัตราความผิดพลาดนี้จะไม่สามารถใช้วิธีการที่นำเสนอในการแก้ไขความผิดพลาดได้เนื่องจากในรูปที่ 6.3 แสดงให้เห็นว่าวิธีการที่นำเสนอสามารถใช้แก้ไขความผิดพลาดได้เมื่อระบบมีอัตราความผิดพลาดน้อยกว่า 8% ซึ่งหากนำมาใช้ในระบบที่มีความผิดพลาดมากกว่า 8% จะทำให้วิธีการแก้ไขความผิดพลาดที่ได้จะส่งข้อมูลเกี่ยวกับกุญแจรหัสลับมากเกินไปซึ่งอาจจะทำให้ *Eve* สามารถสร้างกุญแจรหัสลับใหม่ขึ้นได้ ดังนั้น *Alice* จึงต้องส่งกุญแจรหัสลับบิตของตนทั้งหมดมาให้ *Bob* เพื่อให้ *Bob* ใช้ในการประมาณบิตในสไลซ์ถัดไปและกุญแจรหัสลับนี้จะถูกทิ้งทั้งหมด ในสไลซ์ที่สองผลการแปลงค่ากุญแจรหัสลับจะมีอัตราความผิดพลาดลดลงเหลือ 46.8% ซึ่งในสไลซ์ที่สองนี้จะยังไม่สามารถใช้วิธีการที่นำเสนอในการแก้ไขความผิดพลาดได้ เนื่องจากอัตราความผิดพลาดยังคงสูงกว่า 8% ดังนั้น *Alice* จึงต้องส่งกุญแจรหัสลับบิตที่สไลซ์ที่สองของตนทั้งหมดมาให้ *Bob* เพื่อให้ *Bob* ใช้ในการประมาณค่ากุญแจรหัสลับของตนในสไลซ์ที่สาม ซึ่งการประมาณค่าในสไลซ์ที่สามจะมีอัตราความผิดพลาดลดลงเหลือ 33% ซึ่งสไลซ์ที่สามนี้ยังคงไม่สามารถนำวิธีการที่ได้พัฒนามาใช้ในการแก้ไขความผิดพลาดได้ดังนั้น *Alice* ยังคงต้องส่งกุญแจรหัสลับบิตของตนไปให้ *Bob* เพื่อให้ *Bob* ใช้กุญแจรหัสลับนี้ในการประมาณค่ากุญแจรหัสลับบิตในสไลซ์ถัดไป ซึ่งอัตราความผิดพลาดในการประมาณค่ากุญแจรหัสลับบิตในสไลซ์ที่สี่มีค่าเท่ากับ 5% ดังนั้นที่อัตราความผิดพลาดนี้สามารถใช้วิธีการที่ได้ออกแบบเพื่อแก้ไขความผิดพลาดได้โดย *Alice* จะทำการส่งพาริตี้บิตไปให้ *Bob* ทั้งหมด $73.46l$ โดยที่ l คือจำนวนกุญแจรหัสลับทั้งหมด

บทที่ 7
สรุปและข้อเสนอแนะ

บทนี้กล่าวถึงบทสรุปที่ได้ทำการออกแบบพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมด้วยการนำรหัสแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correction: FEC) โดยนำมาใช้ในการพัฒนาโพรโทคอลร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง (Side Information) และการนำรหัสแก้ไขความผิดพลาดล่วงหน้ามาใช้ในการพัฒนาโพรโทคอลของฟุรุคาวา โดยวิธีการที่ได้ออกแบบนี้เหมาะสำหรับการนำมาใช้ในการแก้ไขความผิดพลาดกุญแจรหัสลับบิต ในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) รวมถึงการนำไปใช้ในการแก้ไขความผิดพลาดที่เกิดขึ้น จากกระบวนการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตด้วยวิธีการแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction: SEC) ในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD) ดังรายละเอียดดังต่อไปนี้

7.1 สรุปผลการวิจัย

ระบบวิทยาการรหัสลับเชิงควอนตัมเป็นระบบที่ใช้ส่งกุญแจรหัสลับระหว่างผู้ส่งและผู้รับ และใช้กฎกลศาสตร์ควอนตัมมาช่วยยืนยันความปลอดภัยของระบบ หากบุคคลที่สามหรือผู้ไม่พึงประสงค์เข้ามาขโมยกุญแจรหัสลับระหว่างการส่ง ผู้ส่งและผู้รับจะทราบทันทีถึงการเข้ามาขโมยกุญแจรหัสลับและสามารถยกเลิกการส่งกุญแจรหัสลับได้ทันก่อนเกิดความเสียหายตามมา ปัจจุบันวิทยาการรหัสลับแบ่งออกเป็นสองระบบคือ การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง (DV-QKD) เป็นระบบการส่งกุญแจรหัสลับบิตโดยแทนด้วยสถานะควอนตัมของโฟตอนเดี่ยว และการกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) เป็นระบบส่งกุญแจรหัสลับที่กระจายตัวแบบเกาส์โดยแทนด้วยเฟสและแอมพลิจูดของสถานะโคฮีเรนต์ของแสง แต่ในระหว่างการส่งทั้งในระบบ DV-QKD และ CV-QKD สัญญาณรบกวน ความไม่เป็นอุดมคติของอุปกรณ์ภายในภาคส่งและภาครับและการเข้ามาขโมยสถานะควอนตัมของบุคคลที่สาม ภายในช่องสื่อสารเชิงควอนตัม เป็นสาเหตุทำให้สถานะควอนตัมเกิดการเปลี่ยนแปลง ส่งผลให้กุญแจรหัสลับที่ส่งเกิดความผิดพลาดตามไปด้วย ดังนั้นการแก้ไขความผิดพลาดและการลดความสำคัญของข้อมูลเกี่ยวกับกุญแจรหัสลับที่บุคคลที่สามสามารถขโมยได้ จึงมีความสำคัญเพื่อทำให้กุญแจรหัสลับที่ส่งยังคงเป็นความลับ วิทยานิพนธ์เล่มนี้นำเสนอการนำรหัสแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correcting Code: FEC) มาใช้ในการพัฒนาโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม โดยนำรหัสบีซีเอชและรหัสคอนโวลูชันมาใช้ในการพัฒนาโพร

โทคอลแก้ไขความผิดพลาดร่วมกับการเข้ารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้างและการนำรหัสบีซีเอชมาใช้ในการพัฒนาวิธีการแก้ไขความผิดพลาดของฟุรุคาวา โดยการออกแบบพัฒนาโพรโทคอลเพื่อลดจำนวนรอบการติดต่อระหว่างผู้ส่งและผู้รับ เหมาะสำหรับนำมาใช้ในการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) เนื่องจากกุญแจรหัสลับอยู่ในรูปแบบข้อมูลไบนารี ผลการจำลองการทำงานมีรายละเอียดดังต่อไปนี้

การพัฒนาโพรโทคอลด้วยรหัสบีซีเอชร่วมกับการเขารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง โพรโทคอลที่ได้พัฒนานี้สามารถลดจำนวนรอบการติดต่อระหว่าง *Alice* และ *Bob* โดยขนาดของบล็อกรหัสบีซีเอชจะขึ้นอยู่กับอัตราความผิดพลาดจากการส่งกุญแจรหัสลับทางช่องสื่อสารเชิงควอนตัม (QBER) จำนวนข้อมูลที่ส่งระหว่างการแก้ไขความผิดพลาดจะขึ้นอยู่กับขนาดของบล็อกและความสามารถในการแก้ไขความผิดพลาด การแก้ไขความผิดพลาดที่ QBER ต่ำ ขนาดของบล็อกที่ใช้จะเลือกใช้ขนาดของบล็อกใหญ่ เนื่องจากจะลดจำนวนข้อมูลที่ส่งระหว่างการแก้ไขความผิดพลาด หากค่า QBER มีค่าสูงวิธีที่พัฒนาขึ้นมานี้สามารถจะเลือกใช้รหัสบีซีเอชที่มีความสามารถในการแก้ไขความผิดพลาดสูง แต่จะส่งข้อมูลระหว่างการแก้ไขความผิดพลาดสูงเช่นเดียวกัน

การพัฒนาโพรโทคอลแก้ไขความผิดพลาดที่เสนอโดยฟุรุคาวาด้วยรหัสบีซีเอช เพื่อลดจำนวนรอบในการติดต่อสื่อสารระหว่าง *Alice* และ *Bob* โดยทำการลดขั้นตอนการตรวจสอบความผิดพลาดด้วยพาริตี้บิตและใช้รหัสบีซีเอชเข้ามาช่วยในการแก้ไขความผิดพลาด ซึ่งขนาดของบล็อกและความสามารถในการแก้ไขความผิดพลาดของรหัสบีซีเอชจะขึ้นอยู่กับ อัตราความผิดพลาดจากการส่งกุญแจรหัสลับทางช่องสื่อสารเชิงควอนตัม (QBER) โดยหากทำการเพิ่มความสามารถในการแก้ไขความผิดพลาดของรหัสบีซีเอชจะส่งผลให้การแก้ไขความผิดพลาดได้ดียิ่งขึ้นแต่จะทำการส่งข้อมูลเกี่ยวกับกุญแจรหัสลับเพิ่มมากขึ้นเช่นกัน เมื่อทำการเปรียบเทียบผลการจำลองการกับโพรโทคอลฟุรุคาวา โพรโทคอลWinnow และ โพรโทคอลCASCADE วิธีการนี้จะเปิดเผยข้อมูลเกี่ยวกับกุญแจรหัสลับมากกว่าแต่จะลดจำนวนลอบการติดต่อระหว่าง *Alice* และ *Bob*

การพัฒนาโพรโทคอลด้วยรหัสคอนโวลูชันร่วมกับการเขารหัสแหล่งกำเนิดด้วยข้อมูลข่าวสารข้าง โพรโทคอลที่ได้พัฒนานี้สามารถลดจำนวนรอบการติดต่อระหว่าง *Alice* และ *Bob* โดยหากระบบมี QBER วิธีการนี้จะลดจำนวนข้อมูลที่เปิดเผยโดยการใช้เทคนิค Puncture

นอกจากนี้วิธีการที่นำเสนอนี้สามารถนำมาใช้แก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับแบบต่อเนื่อง (CV-QKD) โดยจะต้องเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิตก่อน ด้วยการใช้วิธีการแก้ไขข้อผิดพลาดแบบสไลซ์ (Slice Error Correction) เมื่อทำการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์เป็นกุญแจรหัสลับบิตเรียบร้อยแล้ว กุญแจรหัสลับบิตที่ได้ยังคงมีความผิดพลาดอยู่ ดังนั้นผู้ส่งและผู้รับสามารถที่จะใช้วิธีการที่นำเสนอมาแก้ไขความผิดพลาดได้เช่นเดียวกับระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง

7.2 ปัญหาและอุปสรรคที่พบในงานวิจัย

การจำลองการทำงานโพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัมที่ได้ออกแบบและพัฒนา เป็นการจำลองการทำงานแลกเปลี่ยนข้อมูลระหว่างกระบวนการแก้ไขความผิดพลาด ซึ่งทำให้ยังไม่พบปัญหาหรืออุปสรรคระหว่างการวิจัย

7.3 ข้อเสนอแนะในการพัฒนา

รหัสบีซีเอชเป็นหนึ่งในรหัสแบบบล็อกเชิงเส้นที่ยังมีประสิทธิภาพในการแก้ไขความผิดพลาดได้น้อยเมื่อเปรียบเทียบกับ รหัสเทอร์โบ หรือรหัสพาริตี้เช็กความหนาแน่นต่ำ (LDPC) หากนำรหัสแก้ไขความผิดพลาดนี้มาใช้ในการพัฒนา โพรโทคอลแก้ไขความผิดพลาดจากการกระจายกุญแจรหัสลับเชิงควอนตัม อาจจะสามารถเพิ่มประสิทธิภาพการแก้ไขความผิดพลาดได้ดียิ่งขึ้น แต่รหัสแก้ไขความผิดพลาดเหล่านี้จะมีความซับซ้อนในการทำงานสูงนอกจากนี้อาจจะทำให้เวลาในการประมวลสูงด้วยเช่นกัน

หลักการที่นำเสนอเหมาะสมสำหรับการนำไปใช้แก้ไขความผิดพลาดที่เกิดขึ้นกับกุญแจรหัสลับบิตในระบบกระจายกุญแจรหัสลับแบบไม่ต่อเนื่อง (DV-QKD) หากนำมาใช้ในการแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง (CV-QKD) หลักการที่นำเสนอนี้จะต้องใช้วิธีการแก้ไขข้อผิดพลาดแบบสไลซ์มาใช้ในการเปลี่ยนกุญแจรหัสลับที่กระจายตัวแบบเกาส์ให้เป็นกุญแจรหัสลับบิตก่อน จากนั้นจึงสามารถนำวิธีการที่นำเสนอมาใช้แก้ไขความผิดพลาด ซึ่งจะยังคงให้ประสิทธิภาพในการแก้ไขความผิดพลาดต่ำ หากทำการพัฒนาโพรโทคอลแก้ไขความผิดพลาดในระบบกระจายกุญแจรหัสลับแบบต่อเนื่อง ร่วมกับการใช้รหัสแก้ไขความผิดพลาดที่มีประสิทธิภาพสูง ร่วมกับการตัดสินใจแบบละเอียด (Soft-Decision) อาจจะทำให้ประสิทธิภาพของโพรโทคอลแก้ไขความผิดพลาดที่ได้มีประสิทธิภาพเพิ่มสูงขึ้น

เอกสารอ้างอิง

[1] C.H.Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", *Proceedings of IEEE International Conference on computers, Systems & Signal Processing*, Bangalore, India, pp. 175-179, December 1984.

[2] C.H.Bennett, F.Bessette, G.Brassard, L.Salvail and J. Smolin, "Experimental Quantum Cryptography", *Journal of Cryptography* 5(1), pp.3-28, 1992.

[3] C. Elliot, D. Pearson and G. Troxel, "Quantum Cryptography in Practice", Proc. ACM SIDCOMM 2003, ACM Press, pp.227-238, 2003.

[4] Chip Elliott, "Building the quantum network", New Journal of Physics", Vol. 4, page 46.1-46.12, 2002.

[5] Chip Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer and H. Yeh "Current Status of The DARPA Quantum Network", arxiv:quant-ph/0503058, 2005.

[6] **Europe Research.** [Online] Available: http://www.thestandard.com/article.php?story=20040517152322624. 2006.

[7] C. H. Bennett , "Quantum Cryptography Using any Two Nonorthogonal States", Physical Review Letters, Vol. 68, No.21, pp. 3121-3124. , 1992.

[8] A. K. Ekert, "Quantum cryptography based on Bell's Theorem", Physical Review Letters, Vol. 67, No. 6, pp 661-663, 1991.

[9] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. j. Cerf and P. Grangier, "Quantum Key Distribution Using Gaussian-Modulated Coherence State", Nature, Vol. 421, pp. 238-241, 2003.

[10] F.Grosshans and P.Grabgier, "Continuous Variable Quantum Cryptography Using Coherent State", Physical Review Letters 88, 057902, 2002.

[11] T.C.Ralph, "Continuous Variable Quantum Cryptography", Phys. Rev. A, Vol.61, 010303, 2000.

[12] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion", Advance in Cryptology Proc. EUROCRYPT 93, pp. 410-423, 1994.

[13] D. Pearson, "High-speed QKD Reconciliation Using Forward Error Correction", Proc. 7th International Conference on Quantum Communication, Measurement and Computing (QCMC), pp.299-302, 2004.

[14] E. Furukawa and K. Yamazaki, "Application of Existing Perfect Code to Secret Key Reconciliation", in Conf. Proc. Of Int. Symp. On Commun. and Inform. Thech., pp.397-400, 2001.

[15] C. E. Shannon, "A Mathematical Theory of Communication", *Bell System Technical Journal*, 27, pp. 379–423 & 623–656, July & October, 1948.

[16] B. Sklar, **Digital Communications Fundamentals and Applications,** New Jersey: Prentice Hall, Inc. 1988.

[17] S. Haykin, **Communication Systems**, 3rd ed. New York, NY: Wiley, 1994.

[18] H. Imai. **Essentials of Error-Control Coding Techniques**, Academic Press, Inc. 1990.

[19] H.L Lou. "Implementing the Viterbi Algorithm", IEEE Signal Processing Magazine, Vol. 12, pp. 42-52. 1995.

[20] S. Wiesner, "Conjugate Coding", *Sigact News,* Vol. 15, no. 1, pp. 78-88, 1983.

[21] T.C. Ralph, "Continuous Variable Quantum Cryptography", Phys.Rev. A, Vol. 61, 010303, 1999.

[22] Ch. Silberhorn, N. Korolkova and G. Leuchs, "Quantum Cryptography with bright Entangled Beams", Phys. Rev. Lett. Vol 88, 167902, 2002.

[23] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher and T. Scheidl, "Experimental Demonstration of Free Space Decoy-State Quantum Key Distribution over 144 km", Phys. Rev. Lett. 98, 010504, 2007.

[24] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K.Tamaki and Y. Yamamoto, "Quantum Key Distribution over 40 dB Channel Loss Using Superconducting Single Photon Detectors", arXiv: 0706.0397v1, 2007.

[25] F. Grosshans and P. Grangier, "Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variable", arXiv:quant-ph/0204127v1, 2002.

[26] A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble and E.S. Polzik, "Unconditional Quantum Teleportation", Science, Vol. 282, No. 5389, pp.706-709, 1998.

[27] N.J. Cerf, A. Ipe and X. Rottenberg, "Cloning of Continuous Quantum Variable", Phys. Rev. Lett., Vol. 85, pp.175-1757, 2000.

[28] X. Qing, B. Marcia, D. Jean-Luc, G. Sylvain, B. Patrick, G. Philippe and M. Francisco "Toward Quantum Key Distribution System Using Homodyne Detection with Difference Time-Multiplexed Reference", Research, Innovation and Vision for the Future, pp. 158-165, 2007.

[29] S. Chiangga, P. Zarda, T. Jennewein and H. Weinfurter, "Toward Practical Quantum Cryptography", Appl. Phys. B, Vol 69, pp389-393, 1999.

[30] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography", Rev. of Mod. Phy., Vol.74, pp.145-195, 2002.

[31] A. Muller, T. Herzog, B. Huttner, W. Tittle, H.Zbinden and N. Gisin, "Plug and Play systems for Quantum Cryptography", Appl. Phys. Lett., Vol.70, No. 7, pp.793-795, 1997.

[32] H. Kosaka, A. Tomita, Y. Namba, T. Kimura and K. Nakamura, "Single-Photon Interference Experiment over 100 km for Quantum Cryptography System using a Balanced Gated-Mode Photon Detector", Electronics Letters, pp. 1199-1201, 2003.

[33] G. Van Assche, J. Cardinal and N.J. Cerf, "Reconciliation of a Quantum-Distributed Gaussian Key", IEEE Trans. Inform. Theory, Vol. 50, pp. 394, 2004.

[34] พิทักษ์ พานทอง, "การทำงานของระบบวิทยาการรหัสลับเชิงควอนตัม" วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาฟิสิกส์, มหาวิทยาลัยเกษตรศาสตร์, 2548

[35] A. Nakassis, J. Bienfang and C. Williams, "Expeditious Reconciliation for Practical Quantum Key Distribution", Proceedings of SPIE, Vol.5436, Quantum Information and Computation II, pp. 28-35.2004

[36] **CASCADE** [Online] Available: http://www.cki.au.dk/experiment/qrypto/templates/initiator /RecBB84/output2_1.htm. 2006.

[37] K.C. Nguyen, G. V. Assche and N. J. Cerf, "Side-Information Coding with Turbo Codes and its Application to Quantum Key Distribution", in Proc. International Symposium on Information Theory and Its Applications, 2004.

[38] 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(Atomic, Molecular and Optical Physics), Vol. 67, 052303, 2003.

[39] D. Slepian and J.K. Wolf, "Noiseless coding of Correlated information sources", IEEE Trans.Inform. Theory, Vol. IT-19, pp. 471-480, July 1973.

[40] A. D. Liveris, Z. Xiong and C. N. Georghiades, "Compression of Binary Sources With Side Information at the Decoder Using LDPC Codes", IEEE Communications Letters, Vol. 6, 2002.

[41] Alberto Leon-Garcia, **Probability and Random Processes for Electrical Engineering,** Second Edition, 1994.

[42] Donald G. Childers, **Probability and Random Processes Using MATLAB,** Irwin/McGraw-Hill, 1997.

[43] M. Legre, H. Zbinden and N. Gisin, "Implementation of Continuous Variable Quantum Cryptography in Optical Fibres Using a go & return Configuration", aeXiv:quant-ph/0511113, 2005 .

[44] **Electro Optic Modulator** [Online] Available: http://www.rp-photonics.com/electro_optic_modulators.html. 2007.

ภาคผนวก ก

พื้นฐานทฤษฎีความน่าจะเป็นกับวิทยาการรหัสลับเชิงควอนตัม

ระบบหรือการทดลองบางกรณีอาจจะเกี่ยวข้องกับเหตุการณ์ที่ผลของเหตุการณ์หรือผลของการทดลองไม่สามารถระบุแน่ชัดว่าผลจะออกมาเป็นอย่างไร ซึ่งการทดลองหรือระบบในรูปแบบนี้เรียกว่าเป็นการทดลองแบบสุ่มหรือระบบแบบสุ่ม การทำความเข้าใจระบบแบบสุ่มนี้มีความสำคัญมากเพื่อจะนำผลจากการวิเคราะห์มาช่วยออกแบบ และจำลองการทำงานของระบบแบบสุ่มรวมถึงการสร้างระบบขึ้นมาเพื่อช่วยวิเคราะห์และออกแบบระบบใหม่เช่น การจำลองระบบสื่อสาร การจำลองสัญญาณรบกวนที่เกิดขึ้นภายในช่องสัญญาณของระบบสื่อสาร เพื่อช่วยให้ผู้ออกแบบระบบสามารถประเมินประสิทธิภาพของระบบสื่อสารที่ได้ออกแบบ หรือในเรื่องของการเข้ารหัสช่องสัญญาณ (Channel Coding) การจำลองสัญญาณรบกวนถูกนำมาใช้เพื่อช่วยให้ผู้ออกแบบระบบสื่อสารสามารถวิเคราะห์ประสิทธิภาพของรหัสที่ได้ออกแบบ ช่วยให้ผู้ออกแบบสามารถพัฒนารหัสแก้ไขความผิดพลาดให้เหมาะสมกับช่องสัญญาณ เพื่อเพิ่มประสิทธิภาพของระบบให้มากที่สุด ซึ่งจากตัวอย่างที่กล่าวมาทั้งหมดนี้จะเห็นได้ว่าการทำความเข้าใจเกี่ยวกับการทดลองแบบสุ่มหรือระบบแบบสุ่มมีความสำคัญเป็นอย่างมาก โดยหลักการที่จะนำมาใช้ในการวิเคราะห์และทำความเข้าใจในเรื่องนี้เช่น หลักการของความน่าจะเป็น (Probability Theory) ซึ่งหลักการของความน่าจะเป็น ตัวแปรสุ่มและกระบวนการสุ่มมีดังต่อไปนี้

ก.1 ความน่าจะเป็น

ความน่าจะเป็นของเหตุการณ์หนึ่งสามารถหาได้จากอัตราส่วนระหว่างจำนวนครั้งของการเกิดเหตุการณ์นั้นต่อจำนวนครั้งของเหตุการณ์ที่เกิดขึ้นทั้งหมดเช่น ความน่าจะเป็นของการเกิดเหตุการณ์ A หรือ $P(A)$ คือจำนวนครั้งของการเกิดเหตุการณ์ A ที่เกิดขึ้นทั้งหมด N_A ครั้งต่อจำนวนครั้งของเหตุการณ์ที่เกิดขึ้นทั้งหมดในแซมเปิลสเปซ (N) ดังสมการ

$$P(A) = \frac{N_A}{N} \qquad ; N \to \infty \qquad \text{(ก.1)}$$

จากสมการความน่าจะเป็นของเหตุการณ์ใดเหตุการณ์หนึ่งมีค่าอยู่ระหว่าง [0,1] ถ้าความน่าจะเป็นของเหตุการณ์ A ที่เกิดขึ้นมีค่าเท่ากับหนึ่ง ($P(A)$=1) ผลจากการทดลองนั้นจะมีเหตุการณ์ A เกิดขึ้นเสมอแต่ถ้าความน่าจะเป็นของเหตุการณ์ A มีค่าเท่ากับศูนย์แสดงว่าผลของการทดลองจะไม่มีเหตุการณ์ A เกิดขึ้นอย่างแน่นอน นอกจากนี้เมื่อพิจารณาเหตุการณ์ที่เกิดขึ้นสองเหตุการณ์โดย

ให้ A เป็นเหตุการณ์หนึ่งและ B เป็นอีกเหตุการณ์หนึ่ง จำนวนเหตุการณ์ที่การทดลองครั้งหนึ่งจะเกิดเหตุการณ์ A หรือเหตุการณ์ B คือ N_{A+B} (เรียกเหตุการณ์นี้ว่าเหตุการณ์ที่ยูเนี่ยนกัน) โดยทั้งสองเหตุการณ์เกิดขึ้นอย่างเป็นอิสระต่อกันโดยเหตุการณ์ A และ B จะเรียกว่าเป็นเหตุการณ์ที่อิสระต่อกันก็ต่อเมื่อ $A \cap B = \phi$ ดังนั้นค่าของความน่าจะเป็นในการเกิดเหตุการณ์ A หรือเหตุการณ์ B แสดงดังต่อไปนี้

$$\begin{aligned} P(A \cup B) &= \frac{N_{A+B}}{N} \\ &= \frac{N_A}{N} + \frac{N_B}{N} \\ &= P(A) + P(B) \end{aligned} \qquad \text{(ก.2)}$$

ถ้าเหตุการณ์ A และเหตุการณ์ B เป็นเหตุการณ์ที่ไม่เป็นอิสระต่อกันหรือ $A \cap B \neq \phi$ ความน่าจะเป็นของผลจากการทดลองที่เกิดเหตุการณ์ A หรือเหตุการณ์ B แสดงได้ดังนี้

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \qquad \text{(ก.3)}$$

ดังนั้น

$$\begin{aligned} P(A) &= P(A \cap B') + P(A \cap B) \\ P(B) &= P(B \cap A') + P(A \cap B) \\ P(A \cup B) &= P(A) + P(B) - P(A \cap B) \end{aligned}$$

$P(A \cap B)$ คือความน่าจะเป็นที่เหตุการณ์ A และเหตุการณ์ B เกิดร่วมกันหรือเรียกว่า *ความน่าจะเป็นร่วม*

$$P(A \cap B) = \frac{N_{AB}}{N} \qquad N \to \infty \qquad \text{(ก.4)}$$

N_{AB} คือ จำนวนครั้งในการเกิดเหตุการณ์ A และ B พร้อมกันหรือ $A \cap B$

จากสมการที่ (ก.1) ถึงสมการที่ (ก.4) สามารถสรุปคุณสมบัติของความน่าจะเป็นได้ดังต่อไปนี้

- $P(A) \geq 0$ หมายถึงความน่าจะเป็นคืออัตราส่วนระหว่างจำนวนเหตุการณ์ A ที่เกิดขึ้นต่อจำนวนเหตุการณ์ที่เกิดขึ้นทั้งหมดทำให้ความน่าจะเป็นมีค่าอยู่ระหว่าง [0,1]
- $P(S) = 1$ ความน่าจะเป็นของแซมเปิลสเปซ (Sample Space: S) จะมีค่าเท่ากับหนึ่งเสมอ
- ถ้าหาก $A \cap B = \phi$ แล้ว $P(A \cup B) = P(A) + P(B)$ และถ้า $A \cap B \neq \phi$ แล้ว $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

ก.2 ความน่าจะเป็นแบบมีเงื่อนไขและความเป็นอิสระต่อกันเชิงสถิติ

เหตุการณ์บางเหตุการณ์ที่เมื่อมีเหตุการณ์หนึ่งเกิดขึ้นเหตุการณ์นั้นจะส่งผลทำให้เกิดเหตุการณ์อีกเหตุการณ์ขึ้นตามมาเรียกเหตุการณ์ที่เกิดขึ้นในลักษณะนี้ว่า *เหตุการณ์แบบมีเงื่อนไข* (Conditional Probability) เช่น เมื่อมีเหตุการณ์ A เกิดขึ้นแล้วเหตุการณ์ A ส่งผลให้เกิดเหตุการณ์ B ตามมา สัญลักษณ์ที่ใช้แทนความน่าจะเป็นในการเกิดเหตุการณ์ในลักษณะนี้คือ $P(B \mid A)$ เช่น ถ้าพิจารณาการทอดลูกเต๋าสองลูก กำหนดให้เหตุการณ์ A คือผลรวมของแต้มบนหน้าลูกเต๋าเท่ากับหรือมากกว่าห้าและเหตุการณ์ B คือแต้มบนลูกเต๋าใดลูกหนึ่งในสองลูกมีค่าเท่ากับสาม จากทั้งสองเหตุการณ์สามารถหาความน่าจะเป็นในการเกิดเหตุการณ์ B ขึ้นอยู่กับเหตุการณ์ A หรือ $P(B|A)$ ถ้ามีเหตุการณ์ A เกิดขึ้นแล้วเหตุการณ์ A อาจจะไม่ส่งผลไปยังอีกเหตุการณ์หนึ่งก็ได้หรือไม่ทำให้อีกเหตุการณ์หนึ่งขึ้นมาเรียกเหตุการณ์ที่เกิดขึ้นนี้ว่าเหตุการณ์ที่เป็นอิสระต่อกัน (Statistic Independence)

ก.2.1 ความน่าจะเป็นแบบมีเงื่อนไข

ถ้าให้การทดลองหนึ่งที่มีเหตุการณ์ A และเหตุการณ์ B เกิดขึ้นซึ่งการเกิดของเหตุการณ์ B ขึ้นอยู่กับการเกิดของเหตุการณ์ A โดยเรียกความน่าจะเป็นที่เกิดขึ้นในลักษณะนี้ว่า *ความน่าจะเป็นแบบมีเงื่อนไข* (Conditional Probability) โดยหาได้ดังสมการ

$$P(B/A) = \frac{P(A \cap B)}{P(A)} \qquad \text{(ก.5)}$$

$P(A)$ ไม่เท่ากับศูนย์ และ $P(B/A)$ คือความน่าจะเป็นแบบมีเงื่อนไขเมื่อการเกิดของเหตุการณ์ B ขึ้นอยู่กับเหตุการณ์ A

เมื่อเหตุการณ์ A และเหตุการณ์ B เกิดขึ้นอย่างเป็นอิสระต่อกันดังนั้นเหตุการณ์ B จะไม่ขึ้นอยู่กับการเกิดของเหตุการณ์ A แล้ว $P(A \cap B) = 0$ ดังนั้น $P(B/A) = 0$ และในทำนองเดียวกันความน่าจะเป็นของของเหตุการณ์ A ขึ้นอยู่กับเหตุการณ์ B แล้วความน่าจะเป็นแบบมีเงื่อนไขสามารถหาค่าได้ดังนี้

$$P(A/B) = \frac{P(A \cap B)}{P(B)} \qquad \text{(ก.6)}$$

$P(B)$ ไม่เท่ากับศูนย์

จากสมการที่ (ก.5) และ (ก.6) จะได้

$$P(A \cap B) = P(A \mid B)P(B) \text{ หรือ} \qquad \text{(ก.7)}$$
$$P(A \cap B) = P(B \mid A)P(A)$$

กำหนดให้ $B_1, B_2, B_3, ..., B_n$ เป็นเหตุการณ์ที่มีอิสระต่อกันและผลรวมของเหตุการณ์ที่เกิดขึ้นทั้งหมดเท่ากับแซมเปิลสเปซ (S) เหตุการณ์ A สามารถแสดงความสัมพันธ์กับเหตุการ B ได้ดังต่อไปนี้

$$\begin{aligned} A &= A \cap S \\ &= A \cap (B_1 \cup B_2 \cup .... \cup B_n) \\ &= (A \cap B_1) \cup (A \cap B_2) \cup .... \cup (A \cap B_n) \end{aligned}$$

จากสมการที่ (ก.7) ความน่าจะเป็นของเหตุการณ์ A สามารถหาได้โดย [41]

$$\begin{aligned} P(A) &= P(A \cap B_1) + P(A \cap B_2) + ... + P(A \cap B_n) \\ &= P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + ... + P(A \mid B_n)P(B_n) \end{aligned} \qquad \text{(ก.8)}$$

ก.2.2 หลักการพื้นฐานของกฎของเบย์ (Baye's Theory)

สมมติให้ $B_1, B_2, B_3, ..., B_n$ เป็นหนึ่งในเหตุการณ์ที่อยู่ในแซมเปิลสเปซ (S) และกำหนดให้มีเหตุการณ์ A เกิดขึ้นดังนั้นความน่าจะเป็นที่เกิดเหตุการณ์ B_j จากเหตุการณ์ A จากสมการที่ (ก.7) จะแสดงดังสมการ

$$\begin{aligned} P(B_j \mid A) &= \frac{P(B_j \cap A)}{P(A)} \\ &= \frac{P(A \mid B_j)P(B_j)}{P(A)} \end{aligned} \qquad \text{(ก.9)}$$

และจากสมการที่ (ก.8) สมการที่ (ก.9) จะสามารถเขียนอีกรูปแบบหนึ่งได้ดังนี้

$$P(B_j \mid A) = \frac{P(A \mid B_j)P(B_j)}{\sum_{i=1}^{n} P(A \mid B_i)P(B_i)} \qquad \text{(ก.10)}$$

ก.2.3 ความน่าจะเป็นที่เป็นอิสระต่อกันทางสถิติ

เมื่อการทดลองมีเหตุการณ์ A และเหตุการณ์ B เกิดขึ้นเหตุการณ์ทั้งสองจะถูกเรียกว่าเป็น *เหตุการณ์ที่เป็นอิสระต่อกันทางสถิติ* ก็ต่อเมื่อผลคูณระหว่างความน่าจะเป็นในการเกิดเหตุการณ์ A และความน่าจะเป็นในการเกิดเหตุการณ์ B มีค่าเท่ากับความน่าจะเป็นร่วมระหว่างเหตุการณ์ A และเหตุการณ์ B ดังสมการ

$$P(A \cap B) = P(A) \times P(B) \qquad \text{(ก.11)}$$

จากสมการที่ (ก.7) สามารถที่จะเขียนสมการที่ (ก.11) ได้ใหม่ดังนี้

$$P(A \mid B) = P(A) \text{ เมื่อ } P(B) \neq 0 \text{ หรือ}$$
$$P(A \mid B) = P(A) \text{ เมื่อ } P(A) \neq 0$$

ดังนั้นสามารถที่จะสรุปได้ว่าเหตุการณ์ที่เป็นอิสระต่อกันทางสถิตินั้นต้องเป็นไปตามเงื่อนไขต่อไปนี้

$$P(A \cap B) = P(A) \times P(B)$$
$$P(A \mid B) = P(A)$$
$$P(A \mid B) = P(A)$$

หากเหตุการณ์สองเหตุการณ์เป็นอิสระต่อกัน (Mutually Exclusive) และมีความน่าจะเป็นไม่เท่ากับศูนย์ เหตุการณ์ทั้งสองอาจจะไม่เป็นเหตุการณ์ที่เป็นอิสระต่อกันทางสถิติก็ได้ นอกจากนี้ถ้าหากมีเหตุการณ์เกิดขึ้นมากกว่าสองเหตุการณ์เช่น $A_1, A_2, A_3, ..., A_n$ เหตุการณ์เหล่านี้จะเรียกว่าเป็นเหตุการณ์ที่เป็นอิสระต่อกันทางสถิติก็ต่อเมื่อ

$$P(A_1 \cap A_1 \cap A_3 \cap ... \cap A_n) = P(A_1)P(A_2)P(A_3)...P(A_n)$$

ก.3 ตัวแปรสุ่ม

ตัวแปรสุ่ม (Random Variable) หรือ X(s) คือฟังก์ชันระหว่างเหตุการณ์ที่เกิดขึ้นในแซมเปิลสเปซ (s) และค่าจำนวนจริง x โดยเป็นการเปลี่ยนเหตุการณ์ทั้งหมดที่เกิดขึ้นในแซมเปิลสเปซให้มาอยู่ในแกนของตัวเลขจำนวนจริงเช่น การโยนเหรียญหนึ่งเหรียญโดยความน่าจะเป็นในการเกิดหัวและก้อยมีเท่ากันคือ 1/2 ถ้ากำหนดให้เหตุการณ์ A คือเหตุการณ์ในการเกิดหัวและเหตุการณ์ B เป็นเหตุการณ์ในการเกิดก้อย กำหนดให้ตัวแปรสุ่ม x มีค่าเท่ากับ "-1" แทนเหตุการณ์

A และตัวแปรสุ่ม x มีค่าเท่ากับ "1" แทนเหตุการณ์ B ดังนั้นตัวแปรสุ่ม $X(-1)=P(A)=1/2$ และ $X(1)=P(B)=1/2$ ซึ่งตัวแปรสุ่มแบ่งได้เป็นสามชนิด [41] คือ ตัวแปรสุ่มแบบต่อเนื่อง (Continuous Random Variable) ตัวแปรสุ่มแบบไม่ต่อเนื่อง (Discrete Random Variable) และตัวแปรสุ่มแบบผสมที่รวมระหว่างตัวแปรสุ่มแบบต่อเนื่องและแบบไม่ต่อเนื่อง ซึ่งในวิทยานิพนธ์นี้จะกล่าวเพียงตัวแปรสุ่มแบบต่อเนื่องและตัวแปรสุ่มแบบไม่ต่อเนื่อง โดยความแตกต่างระหว่างตัวแปรสุ่มแบบต่อเนื่องและตัวแปรสุ่มแบบไม่ต่อเนื่องขึ้นอยู่กับค่าตัวเลขที่นำมาใช้แทนเหตุการณ์ที่เกิดขึ้นในแซมเปิลสเปซ ถ้าค่าที่นำมาแทนเป็นตัวเลขจำนวนเต็มหรือตัวเลขที่ไม่ต่อเนื่องตัวแปรสุ่มเหล่านั้นจะถูกเรียกว่าตัวแปรสุ่มแบบไม่ต่อเนื่อง ในทางกลับกันถ้าหากตัวเลขที่นำมาแทนเหตุการณ์ที่เกิดขึ้นในแซมเปิลสเปซเป็นตัวเลขจำนวนจริงที่ต่อเนื่องตัวแปรสุ่มนั้นจะถูกเรียกว่า ตัวแปรสุ่มแบบต่อเนื่อง ตัวอย่างตัวแปรสุ่มแบบต่อเนื่องได้แก่ ระยะเวลาการใช้งานหลอดไฟแต่ละหลอดในแต่ละวันของครอบครัวทั้งหมดในประเทศไทย เมื่อกำหนดให้จำนวนหลอดไฟที่นำมาใช้ในการทดลองมีจำนวนมากเข้าใกล้ค่าอนันต์หรือน้ำหนักของคนที่อยู่บนโลก ซึ่งจะเห็นได้ว่าค่าน้ำหนักหรือระยะเวลาการใช้งานหลอดไฟมีค่าที่เป็นจำนวนจริงอย่างต่อเนื่อง เป็นต้น เมื่อนำหลักการของความน่าจะเป็นมาวิเคราะห์ตัวแปรสุ่มจะได้คุณสมบัติของตัวแปรสุ่มดังต่อไปนี้

ก.3.1 ฟังก์ชันความหนาแน่นของความน่าจะเป็น

ฟังก์ชันความหนาแน่นของความน่าจะเป็น (Probability Density Function: PDF) เป็นฟังก์ชันระหว่างตัวแปรสุ่ม X และค่าความน่าจะเป็นของตัวแปรสุ่มนั้นหรือ $P(x)$ ซึ่งจะบอกถึงโอกาสในการเกิดเหตุการณ์นั้น รูปแบบของฟังก์ชันความหนาแน่นของความน่าจะเป็นจะแบ่งได้ตามรูปแบบของตัวแปรสุ่มดังต่อไปนี้

- **ฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มไม่ต่อเนื่อง**

ถ้าหากว่าตัวแปรสุ่มเป็นแบบตัวแปรสุ่มที่ไม่ต่อเนื่องจะสามารถเขียนฟังก์ชันความหนาแน่นของความน่าจะเป็นได้ดังสมการ

$$f(x)=\sum_{i=1}^{n} P(x_i)\delta(x-x_i) \qquad \text{(ก.12)}$$

n คือจำนวนเหตุการณ์ที่เกิดขึ้นทั้งหมด $P(x_i)$ คือความน่าจะเป็นของเหตุการณ์

- **ฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มต่อเนื่อง**

ในส่วนของตัวแปรสุ่มแบบต่อเนื่อง การที่จะกำหนดตัวค่าความน่าจะเป็นให้ตัวแปรสุ่มแบบต่อเนื่องจะไม่สามารถทำได้หรือจะทำให้ผลของความน่าจะเป็นจะมีค่าเท่ากับศูนย์ [41] ดังนั้นในการหาความน่าจะเป็นของตัวแปรสุ่มแบบต่อเนื่องจึงต้องหาค่าความน่าจะเป็นระหว่างค่าสองค่า

เช่น $P(a \le x < b)$ หรือ $P(a \le x < a + \Delta a)$ โดยคุณสมบัติฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มแบบต่อเนื่องจะมีคุณสมบัติเหมือนกับตัวแปรสุ่มแบบไม่ต่อเนื่องดังนี้คือ

1. $f(x) \ge 0$
2. $\int_{-\infty}^{\infty} f(x)dx = 1$
3. $P(a \le x < b) = \int_{a}^{b} f(x)dx$

ก.3.2 ฟังก์ชันแจกแจงสะสม

ฟังก์ชันแจกแจงสะสม(Cumulative Distribution Function: CDF) เป็นอีกหนึ่งฟังก์ชันที่ได้จากการวิเคราะห์ความน่าจะเป็นของตัวแปรสุ่ม โดยฟังก์ชันแจกแจงสะสมเป็นผลรวมของความน่าจะเป็นหรือเขียนแทนได้โดย $P(X \le x)$ ซึ่งรายละเอียดของฟังก์ชันแจกแจงสะสมมีดังต่อไปนี้

- **ฟังก์ชันแจกแจงสะสมของตัวแปรสุ่มแบบไม่ต่อเนื่อง**

กำหนดให้ X(s) คือตัวแปรสุ่มแบบไม่ต่อเนื่อง (Discrete Random Variable) เมื่อนำหลักการของความน่าจะเป็นมาวิเคราะห์ตัวแปรสุ่มแบบไม่ต่อเนื่อง โดยพิจารณาเฉพาะเพียงเหตุการณ์ที่ $X \le x$ ดังนั้นความน่าจะเป็นของเหตุการณ์ที่เกิดขึ้นนี้คือ $P(X \le x)$ โดยที่ $-\infty \le x \le \infty$ ซึ่งเรียกความน่าจะเป็นของเหตุการณ์ $X \le x$ นี้ว่าฟังก์ชันแจกแจงสะสมของตัวแปรสุ่ม X ดังสมการต่อไปนี้

$$F(x) = P(X \le x) \quad , -\infty \le x \le \infty \qquad \text{(ก.13)}$$

$F(x)$ คือฟังก์ชันแจกแจงสะสม

เนื่องจาก $F(x)$ จะแสดงออกมาในรูปของความน่าจะเป็นดังนั้นฟังก์ชันแจกแจงสะสมจึงมีค่าอยู่ระหว่าง $0 \le F(x) \le 1$ และ $F(-\infty) = 0, F(\infty) = 1$ โดยค่าฟังก์ชันแจกแจงสะสมของตัวแปรสุ่มแบบไม่ต่อเนื่องสามารถหาได้จากผลรวมของฟังก์ชันความหนาแน่นของความน่าจะเป็นดังสมการต่อไปนี้

$$F_X(x) = \sum_{i=1}^{n} P(x_i) \qquad \text{(ก.14)}$$

- **ฟังก์ชันแจกแจงสะสมของตัวแปรสุ่มแบบต่อเนื่อง**

จากฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มแบบต่อเนื่อง (Continuous Random Variable) ค่าความน่าจะเป็น $P(a < x < b)$ คือความน่าจะเป็นระหว่าง a และ b ถ้าทำการหาค่าของความน่าจะเป็นระหว่าง $-\infty$ ถึงค่าใดค่าหนึ่งเช่น a หรือ $P(-\infty < x < a)$ แล้วค่าความน่าจะเป็นที่ได้จะเรียกว่าฟังก์ชันแจกแจงสะสมของ a หรือ $F(a)$ โดยนิยามของฟังก์ชันแจกแจงสะสมเป็นดังสมการ

$$F(a) = P(X \le a)$$
$$= \int_{-\infty}^{a} f(x)dx$$

เมื่อ a อยู่ระหว่าง $(-\infty, \infty)$

ก.4 ตัวอย่างรูปแบบการกระจายโอกาส

จากฟังก์ชันความหนาแน่นของความน่าจะเป็นที่ได้กล่าวมา ในหัวข้อนี้จะแสดงตัวอย่างของฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบไม่ต่อเนื่องและฟังก์ชันความหนาแน่นของความน่าจะเป็นแบบต่อเนื่องดังต่อไปนี้

ก.4.1 การกระจายโอกาสแบบปัวส์ซอง

การกระจายโอกาสแบบปัวส์ซอง (Poisson Distribution) เกิดขึ้นเมื่อเกิดเหตุการณ์หนึ่งซึ่งเป็นเหตุการณ์แบบสุ่มอย่างแท้จริงภายในช่วงเวลาที่กำหนดเช่น การนับจำนวนความต้องการเชื่อมต่อในการใช้งานระบบโทรศัพท์ การนับจำนวนโฟตอนที่เกิดขึ้นภายในพัลส์แสงหรือการนับจำนวนไอซีที่เสียจากกระบวนการผลิต เป็นต้น ซึ่งการกระจายโอกาสแบบปัวส์ซองเป็นรูปแบบหนึ่งของตัวแปรสุ่มแบบไม่ต่อเนื่องโดยฟังก์ชันความหนาแน่นของความน่าจะเป็นของการกระจายโอกาสแบบปัวส์ซองแสดงดังสมการ

$$f(x) = \frac{\lambda^x}{x!} e^{-\lambda} \qquad x = 0,1,2,... \qquad (ก.15)$$

λ คือค่าเฉลี่ยของการกระจายโอกาสแบบปัวส์ซองเช่น ค่าเฉลี่ยในการเกิดอุบัติเหตุในรอบหนึ่งสัปดาห์ ค่าเฉลี่ยของจำนวนโฟตอนในพัลส์แสง x คือจำนวนครั้งในการเกิดเหตุการณ์ เช่นจำนวนครั้งในการเกิดอุบัติเหตุในระยะเวลาหนึ่งสัปดาห์

ก.4.2 การกระจายโอกาสแบบเกาส์

การกระจายโอกาสแบบเกาส์ (Gaussian Distribution) หรือการกระจายโอกาสแบบปกติ (Normal Distribution) เป็นตัวอย่างหนึ่งของเหตุการณ์ที่เกิดขึ้นโดยทั่วไปในธรรมชาติหรือเหตุการณ์ที่มนุษย์สร้างขึ้น ซึ่งการกระจายโอกาสแบบเกาส์จัดเป็นรูปแบบหนึ่งของตัวแปรสุ่มแบบต่อเนื่องซึ่งมีฟังก์ชันความหนาแน่นของความน่าจะเป็นดังนี้

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-m_x)^2/2\varsigma^2} \qquad (ก.16)$$

m_x คือค่าเฉลี่ยและ σ^2 คือค่าความแปรปรวนของการกระจายโอกาสแบบเกาส์
ลักษณะฟังก์ชันความหนาแน่นของความน่าจะเป็นของการกระจายโอกาสแบบเกาส์ จะมีรูปแบบระฆังคว่ำมีจุดศูนย์กลางอยู่ที่ค่าเฉลี่ย (m_x) และการกระจายตัวจะมีการระจายออกจากศูนย์กลางหรือค่าเฉลี่ยตามค่าของความแปรปรวน

ก.5 ค่าเฉลี่ยของตัวแปรสุ่ม

นอกจากฟังก์ชันความหนาแน่นของความน่าจะเป็น (PDF) และ ฟังก์ชันการแจกแจงสะสม (CDF) ที่ใช้อธิบายลักษณะของตัวแปรสุ่ม (Random Variable) ยังมีวิธีการวัดคุณสมบัติของตัวแปรสุ่มอีกหลายวิธีที่ใช้บ่งบอกถึงลักษณะของตัวแปรสุ่มเช่น ค่าเฉลี่ยของตัวแปรสุ่ม (Mean) เป็นต้น โดยค่าเฉลี่ยของตัวแปรสุ่ม X ใช้สัญลักษณ์แทนคือ m_X หรือ $\overline{X}$ และใช้สัญลักษณ์ E[X] แทนกระบวนการหาค่าเฉลี่ยเรียกว่า ค่าคาดคะเนของตัวแปรสุ่ม X (Expectation of X หรือ Statistical Averaging) ซึ่งค่าเฉลี่ยมีความสัมพันธ์กับค่าของฟังก์ชันความหนาแน่นของความน่าจะเป็นโดยเป็นค่าที่บอกถึงศูนย์กลางของการกระจายของผลลัพธ์ที่ได้จากการทดลอง หรือค่ากึ่งกลางของฟังก์ชันความหนาแน่นของความน่าจะเป็น ซึ่งค่าเฉลี่ยของตัวแปรสุ่มแบบไม่ต่อเนื่องสามารถหาได้ดังสมการ

$$\overline{X} = E(X) = m_x = \sum_{i=1}^{k} x_i P(x_i) \qquad (ก.17)$$

ถ้า X_i เป็นตัวแปรสุ่มแบบไม่ต่อเนื่องและ $P(x_i)$ เป็นค่าความน่าจะเป็นของตัวแปรสุ่มแบบไม่ต่อเนื่อง

ในกรณีของตัวแปรสุ่มแบบต่อเนื่องค่าเฉลี่ยสามารถหาค่าได้จากฟังก์ชันความหนาแน่นของความน่าจะเป็นดังต่อไปนี้

$$m_x = E[x] = \int_{-\infty}^{\infty} x p_x(x)\,dx \qquad \text{(ก.18)}$$

ก.6 ค่าเบี่ยงเบนมาตรฐานและความแปรปรวนของตัวแปรสุ่ม

ค่าเฉลี่ยของตัวแปรสุ่มเป็นเพียงค่าหนึ่งที่ใช้บอกคุณสมบัติของตัวแปรสุ่มแต่ค่านี้ยังไม่สามารถให้รายละเอียดได้อย่างชัดเจนเช่น ถ้าค่าเฉลี่ยมีค่าเท่ากับศูนย์สิ่งนี้อาจจะแสดงถึงผลจากการทดลองในเหตุการณ์หนึ่ง ให้ผลออกมามีค่าเท่ากับศูนย์ทั้งหมดหรือผลจากการทดลองมีค่าที่ไม่เท่ากับศูนย์รวมมาอยู่ด้วย ดังนั้นเพื่อเป็นการวัดการกระจายโอกาสของผลการทดลองจึงใช้ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) เขียนแทนด้วย σ_x เพื่อใช้วัดการกระจายของค่าตัวแปรสุ่มออกจากค่าเฉลี่ยหรือจุดกึ่งกลาง โดยค่าเบี่ยงเบนมาตรฐานนั้นสามารถมีได้ทั้งค่าบวกหรือค่าลบ ดังนั้นผลการวัดนี้อาจจะสามารถทำให้อยู่ในรูปแบบของขนาดของการกระจายตัวที่มีค่าเป็นบวกเสมอ โดยนำค่าเบี่ยงเบนมาตรฐานยกกำลังสองจะได้ค่าทางสถิติที่เรียกว่า *ความแปรปรวน* (Variance: σ_x^2) ซึ่งค่าความแปรปรวนของตัวแปรสุ่มแบบไม่ต่อเนื่องสามารถหาค่าได้ดังต่อไปนี้

$$\sigma_x^2 = E[(X - m_x)^2] \qquad \text{(ก.19)}$$

กระจายสมการได้ $E[X^2 - 2m_x X + m_x^2] = E[X^2] - 2m_x E[X] + m_x^2$

$$= \overline{x^2} - 2m_x^2 + m_x^2$$

$$= \overline{x^2} - m_x^2 \qquad \text{(ก.20)}$$

ก.7 ค่าเฉลี่ยของตัวแปรสุ่มหลายตัวแปร

ในการหาค่าเฉลี่ยหรือ Expected Value ของตัวแปรสุ่มสองหรือหลายตัวแปรสุ่มนั้นสามารถหาได้ดังเช่นการหาค่าเฉลี่ยของตัวแปรสุ่มหนึ่งตัวแปรสุ่มเช่น การหาค่าค่าเฉลี่ยของฟังก์ชัน $Z = g(X,Y)$ สามารถหาได้ดังต่อไปนี้ [41]

$$E(Z) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(x,y) f_{X,Y}(x,y)\,dxdy \qquad \text{(ก.21)}$$

กรณีที่ตัวแปรสุ่ม Z เป็นตัวแปรสุ่มแบบต่อเนื่อง $f_{X,Y}(x,y)$ คือฟังก์ชันความหนาแน่นของความน่าจะเป็นร่วมระหว่างตัวแปรสุ่ม X และตัวแปรสุ่ม Y ในกรณีของตัวแปรสุ่มไม่ต่อเนื่องค่าเฉลี่ยแสดงได้ดังต่อไปนี้

$$E(Z) = \sum_i \sum_n g(x_i, y_n) p_{X,Y}(x_i, y_n) \qquad \text{(ก.22)}$$

โดยที่ $p_{X,Y}(x_i, y_n)$ คือความน่าจะเป็นร่วมระหว่างตัวแปรสุ่ม X และตัวแปรสุ่ม Y ในส่วนของค่าเฉลี่ยของผลคูณของตัวแปรสุ่มคือผลคูณของค่าเฉลี่ยของตัวแปรสุ่มแต่ละตัวแปรสุ่ม เมื่อตัวแปรสุ่มในแต่ละตัวแปรสุ่มเป็นอิสระต่อกันดังสมการ

$$E(X_1 X_2 ... X_n) = E(X_1)E(X_2)....E(X_n) \qquad \text{(ก.23)}$$

ก.7.1 ค่าความสัมพันธ์ของตัวแปรสุ่มสองตัวแปรสุ่ม

เมื่อทำการหาค่าเฉลี่ยของฟังก์ชัน $G(X,Y) = X^i Y^j$ หรือเรียกว่าโมเมนต์ร่วม โดยที่ i และ j ของตัวแปรสุ่ม X และตัวแปรสุ่ม Y สามารถแสดงได้ดังต่อไปนี้

ในกรณีของตัวแปรสุ่ม X และตัวแปรสุ่ม Y เป็นตัวแปรสุ่มแบบต่อเนื่อง

$$E(Z) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^i y^j f_{X,Y}(x,y)dxdy$$

ในกรณีของตัวแปรสุ่ม X และตัวแปรสุ่ม Y เป็นตัวแปรสุ่มแบบไม่ต่อเนื่อง

$$E(Z) = \sum_m \sum_n x_m^i y_n^j p_{X,Y}(x_i, y_n)$$

ถ้า i เท่ากับศูนย์จะได้ค่าของเฉลี่ยหรือค่าโมเมนต์ (Moment) ของตัวแปรสุ่ม Y ถ้า j เท่ากับศูนย์จะได้ค่าโมเมนต์หรือค่าเฉลี่ยของตัวแปรสุ่ม X หาก i และ j เท่ากับหนึ่งจะเรียกว่าค่าเฉลี่ยหรือ $E(XY)$ นี้ว่าความสัมพันธ์ของตัวแปรสุ่ม X และ Y (Correlation of X and Y) หาก $E(XY) = 0$ จะได้ว่าตัวแปรสุ่ม X และ ตัวแปรสุ่ม Y ตังฉากกัน (Orthogonal)

ก.7.2 โควาร์เรียนของตัวแปรสุ่ม

จากการหาความสัมพันธ์ระหว่างตัวแปรสุ่ม X และ Y หากทำการหาค่าเฉลี่ยของฟังก์ชันแสดงได้ดังต่อไปนี้

$$E\{(X - E[X])^i (Y - E[Y])^j\} \qquad \text{(ก.24)}$$

จากสมการจะได้ข้อสรุปของการหาโควาร์เรียนดังนี้คือ $E\{(X - E[X])^i (Y - E[Y])^j\}$

ถ้า $i=2$ และ $j=0$ จะได้ค่าของความแปรปรวนของตัวแปรสุ่ม X และในทำนองเดียวกัน หาก $j=2$ และ $i=0$ จะได้ความแปรปรวนของตัวแปรสุ่ม Y หาก $i=1$ และ $j=1$ จะเรียกว่า โควาร์เรียน (Covariance) ของตัวแปรสุ่ม X และตัวแปรสุ่ม Y ดังนี้

$$COV(X,Y) = E\{(X - E[X])(Y - E[Y])\}$$

หรือ

$$COV(X,Y) = E[XY] - E[X]E[Y]$$

หากตัวแปรสุ่มสองตัวแปรสุ่มเกิดขึ้นอย่างอิสระต่อกันค่าของโควาร์เรียนจะมีค่าเท่ากับศูนย์ ซึ่งสัมประสิทธิ์ความสัมพันธ์ระหว่างตัวแปรสุ่ม X และ ตัวแปรสุ่ม Y สามารถหาได้ดังนี้

$$p_{X,Y} = \frac{COV(X,Y)}{\sigma_X \sigma_Y} = \frac{E[(X - E[X])(Y - E[Y])]}{\sigma_X \sigma_Y} \qquad \text{(ก.25)}$$

σ_X คือส่วนเบี่ยงเบนมาตรฐานของตัวแปรสุ่ม X หรือ $\sigma_X = \sqrt{VAR(X)}$ และ σ_Y คือส่วนเบี่ยงเบนมาตรฐานของตัวแปรสุ่ม Y หรือ $\sigma_Y = \sqrt{VAR(Y)}$

ค่าของ $p_{X,Y}$ จะมีค่าอยู่ระหว่าง [-1,1] ซึ่งจะบ่งบอกถึงระดับความสัมพันธ์ (Correlation)ระหว่างตัวแปรสุ่ม หาก $p_{X,Y}$ มีค่าเท่ากับหนึ่งนั้นคือตัวแปรสุ่มสองตัวจะมีความสัมพันธ์กันและ หาก $p_{X,Y}$ เท่ากับศูนย์นั่นคือตัวแปรสุ่มสองตัวแปรสุ่มจะไม่มีความสัมพันธ์กัน หากตัวแปรสุ่มสองตัวมีความเป็นอิสระต่อกันตัวแปรสุ่มทั้งสองอาจจะมีความสัมพันธ์กันหรือไม่มีความสัมพันธ์กันก็ได้ [41] เนื่องจากค่าโควาร์เรียนของตัวแปรสุ่มที่มีอิสระต่อกันเท่ากับศูนย์

ก.8 กระบวนการสุ่ม

เหตุการณ์แบบสุ่มที่เกิดขึ้นในธรรมชาติจะเป็นฟังก์ชันของเวลาเช่น แรงดันไฟฟ้าของสัญญาณรบกวนที่เกิดขึ้นภายในตัวต้านทานของอุปกรณ์อิเล็กทรอนิกส์หรือภายในเครื่องรับวิทยุ เช่นเดียวกับสัญญาณข้อมูลที่ออกมาจากแหล่งกำเนิด สัญญาณที่เกิดขึ้นนี้จะมีลักษณะสัญญาณเป็นแบบสุ่มที่เปลี่ยนแปลงตามเวลา ซึ่งที่กล่าวมาทั้งหมดนี้เป็นตัวอย่างของกระบวนการสุ่ม (Random process) หรือ $X(\varepsilon,t)$ เมื่อพิจารณากระบวนการสุ่มที่เป็นฟังก์ชันระหว่างเวลา (t) และผลของเหตุการณ์จากกรทดลองแบบสุ่ม (ε) ถ้าให้กระบวนการสุ่มมีเวลาเป็นค่าคงที่ค่าของกระบวนการสุ่มหรือค่าของแรงดันไฟฟ้าของสัญญาณรบกวนที่ถูกสร้างโดยตัวต้านทานหรือขนาดของแอมพลิจูดของสัญญาณที่ถูกสร้างโดยแหล่งกำเนิดสัญญาณเสียงจะถูกเรียกว่า "ตัวแปรสุ่ม" ถ้าแรงดันไฟฟ้า

ของสัญญาณรบกวนที่ถูกสร้างโดยตัวต้านทานเพียงตัวเดียวหรือแหล่งกำเนิดเพียงตัวเดียวจะแสดงกระบวนการสุ่มเพียงอันเดียวซึ่งถูกกำหนดโดยเหตุการณ์ที่เกิดขึ้นจะเรียกว่า Sample Function หรือ $X(t)$ ซึ่ง Sample Function จะเป็นฟังก์ชันที่เปลี่ยนแปลงตามเวลาของกระบวนการสุ่มเซ็ตของ Sample Function ที่เป็นไปได้ทั้งหมดเช่น เซ็ตของแรงดันไฟฟ้าของสัญญาณรบกวนที่เกิดจากตัวต้านทานหลายตัวจะมีค่าเท่ากับกระบวนการสุ่มหรือเรียกว่า *เอ็นเซ็มเบิล* (Enseble) ซึ่งโดยทั่วไปเซ็ตของกระบวนการสุ่มที่เกิดขึ้นทั้งหมดมีขนาดใหญ่มากโดยทั่วไปจะเท่ากับอินฟินิตี้(Infinity)[41]

กระบวนการสุ่มสามารถแบ่งออกได้เป็นสองประเภทได้แก่ กระบวนการสุ่มที่ต่อเนื่องตามเวลา (Continuous-Time Random Process) และกระบวนการสุ่มที่ไม่ต่อเนื่องตามเวลา (Discrete-Time Random Process) [41]

- **กระบวนการสุ่มที่ต่อเนื่องตามเวลา**

เมื่อพิจารณาถึงระดับสัญญาณแรงดันไฟฟ้าที่เกิดขึ้นภายในตัวต้านทางหรือ ระดับสัญญาณไฟฟ้าที่ได้จากไมโครโฟน (Microphone) จะเห็นได้ว่าระดับของสัญญาณที่ได้จะต่อเนื่องตามแกนของเวลา ซึ่งสัญญาณดังตัวอย่างนี้เป็นหนึ่งในตัวอย่างของสัญญารแอนะล็อกในระบบสื่อสารและเรียกกระบวนการสุ่มที่ทำให้เกิดสัญญาณเหล่านี้ว่า *กระบวนการสุ่มที่ต่อเนื่องตามเวลา* นอกจากนี้กระบวนการสุ่มที่ต่อเนื่องตามแกนเวลาสามารถแบ่งได้เป็น กระบวนการสุ่มที่ต่อเนื่องตามเวลาและมีขนาดหรือระดับสัญญาณต่อเนื่อง ตัวอย่างของกระบวนการสุ่มเหล่านี้เช่น สัญญาณแอนะล็อกหรือระดับสัญญาณแรงดันไฟฟ้าที่เกิดขึ้นภายในตัวต้านทาน กระบวนการสุ่มที่ต่อเนื่องตามเวลาแต่ระดับสัญญาณไม่ต่อเนื่องเช่น สัญญาณที่เกิดจากการแปลงสัญญาณดิจิตอลเป็นสัญญาณแอนะล็อกโดย D/A (Digital to Analog Converter)

- **กระบวนการสุ่มที่ไม่ต่อเนื่องตามเวลา**

กระบวนการสุ่มที่ไม่ต่อเนื่องตามแกนเวลานั้นสามารถแบ่งออกเป็นสองประเภทเช่นเดียวกับกระบวนการสุ่มที่ต่อเนื่องตามแกนเวลาคือ กระบวนการสุ่มที่ไม่ต่อเนื่องตามแกนเวลาและกระบวนการสุ่มที่ไม่ต่อเนื่องของระดับสัญญาณ

ก.8.1 ค่าเฉลี่ย ออโตคอร์รีเลชัน และ ออโตโควาร์เรียนฟังก์ชัน

ค่าเฉลี่ยของกระบวนการสุ่มสามารถหาได้เช่นเดียวกับค่าเฉลี่ยของตัวแปรสุ่มดังต่อไปนี้

$$m_x(t) = E[X(t)] = \int_{-\infty}^{\infty} x f_{X(t)}(x)dx \qquad \text{(ก.26)}$$

$f_{X(t)}(x)$ คือฟังก์ชันความหนาแน่นของความน่าจะเป็นของกระบวนการสุ่ม $X(t)$

ฟังก์ชันออโตคอร์รีเลชัน (Autocorrelation) ของกระบวนการสุ่ม $X(t)$ แสดงได้ดังต่อไปนี้

$$R_X(t_1,t_2) = E[X(t_1)X(t_2)] = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} xy f_{X(t_1)X(t_2)}(x,y)dxdy \qquad (ก.27)$$

โดยที่ $f_{X(t_1)X(t_2)}(x,y)$ คือฟังก์ชันความหนาแน่นของความน่าจะเป็นร่วมของกระบวนการสุ่ม หรือ Second-order pdf ของกระบวนการสุ่ม

ฟังก์ชันออโตโควาร์เรียน (Autocovariance) ของกระบวนการสุ่ม $X(t)$ แสดงได้ดังต่อไปนี้

$$C_X(t_1,t_2) = E[\{X(t_1) - E[X(t_1)]\}\{X(t_2) - E[X(t_2)]\}] \qquad (ก.28)$$

หรือ

$$C_X(t_1,t_2) = R_X(t_1,t_2) - m_x(t_1)m_x(t_2)$$

โดยที่ค่าความแปรปรวนของกระบวนการสุ่ม $X(t)$ จะมีค่าเท่ากับ $C_X(t,t)$ ดังนี้

$$VAR[X(t)] = E[(X(t) - m_x(t))^2] = C_X(t,t) \qquad (ก.29)$$

สัมประสิทธิ์ของความสัมพันธ์ (Correlation Coefficient) หาได้ดังต่อไปนี้

$$p_x(t_1,t_2) = \frac{C_X(t_1,t_2)}{\sqrt{C_X(t_1,t_1)}\sqrt{C_X(t_2,t_2)}} \qquad (ก.30)$$

ก.8.2 กระบวนการสุ่มคงที่และกระบวนการสุ่มคงที่ในลักษณะกว้าง

ตัวแปรสุ่ม X_{t_i} โดยที่ i = 1,2 ,3, 4,.....n ได้มาจากกระบวนการสุ่ม $X(t,\varepsilon)$ สำหรับทุกๆ ค่าเวลา ซึ่งจะมีลักษณะทางสถิติคือค่าความน่าจะเป็นร่วมเป็น $p(x_{t_1}, x_{t_2}, ...x_{t_n})$ พิจารณาเซตของตัวแปรสุ่มอื่นๆ $X_{t_i+t} \equiv X(t_i + t)$ i = 1,2 ,3, 4,.....n โดย t เป็นเวลาที่เปลี่ยนไปอย่างอิสระตัวแปรสุ่มนี้จะมีลักษณะของความน่าจะเป็นร่วมเป็น $p(x_{t_1+t}, x_{t_2+t}, ..., x_{t_n+t})$ โดยที่ค่าความน่าจะเป็นร่วมของตัวแปรสุ่ม $X(t_i)$ และ $X(t_i + t)$ อาจจะมีค่าเท่าหรือไม่เท่ากันก็ได้ถ้า

$$X(t_i) = X(t_i + t) \text{ หรือ}$$
$$p(x_{t_1}, x_{t_2}, ...x_{t_n}) = p(x_{t_1+t}, x_{t_2+t}, ..., x_{t_n+t}) \quad \text{(ก.31)}$$

สำหรับทุกค่า t และ n ดังนั้นกระบวนการสุ่มแบบนี้จะถูกเรียกว่า *กระบวนการสุ่มคงที่* (Stationary Random Process) และถ้า

$$X(t_i) \neq X(t_i + t) \quad \text{(ก.32)}$$

กระบวนการสุ่มแบบนี้จะถูกเรียกว่า *กระบวนการสุ่มแบบไม่คงที่* (Nonstationary Random Process) [41] ในกรณีของกระบวนการสุ่มที่ถูกเรียกว่ากระบวนการสุ่ม (Wine-Sense Stationary: WSS) ก็ต่อเมื่อกระบวนการสุ่มนั้นจะมีค่าเฉลี่ยที่คงที่หรือ

$$m_{X(t)} = m \qquad \text{เมื่อ } t \text{ มีค่าใดๆ และ } m \text{ คือค่างที่}$$

และค่าของออโตคอร์รีเลชันหรือค่าของออโตโควาร์เรียนของกระบวนการสุ่ม $X(t, \varepsilon)$ นี้ขึ้นอยู่กับฟังก์ชันเวลา คือ $t_2 - t_1$ ดังนี้

$$C_X(t_1, t_2) = C_X(t_2 - t_1) \qquad \text{สำหรับ } t_1\ t_2 \text{ ใดๆ หรือ}$$
$$R_X(t_1, t_2) = R_X(t_2 - t_1) \qquad \text{สำหรับ } t_1\ t_2 \text{ ใดๆ} \quad \text{(ก.33)}$$

ในเรื่องของการประมวลผลสัญญาณ (Signal Processing) ค่าของออโตคอร์รีเลชันของกระบวนการสุ่มแบบคงที่ในลักษณะกว้าง จะมีคุณสมบัติต่างๆมากมายที่ถูกนำมาประยุกต์ใช้เช่น ค่าออโตคอร์รีเลชันที่เวลา $\tau = 0$ จะมีค่าเท่ากับกำลังงานเฉลี่ย [41] นั่นคือ

$$R_X(0) = E[X(t)^2] \quad \text{(ก.34)}$$

ภาคผนวก ข

อุปกรณ์เชิงแสงสำหรับระบบวิทยาการรหัสลับเชิงควอนตัม

แหล่งกำเนิดแสง (Laser Diode: LD)

แหล่งกำเนิดแสงในระบบวิทยาการรหัสลับเชิงควอนตัมส่วนใหญ่ จะใช้แหล่งกำเนิดแสงจากเลเซอร์ไดโอด (Laser Diode: LD) เนื่องจากแสงที่สร้างได้จะมีคุณสมบัติของความเป็นโคฮีเรนต์ (Coherent) และยังช่วงของความยาวคลื่นแสงที่สร้างได้แคบกว่าแหล่งกำเนิดแสง Light Emitting Diode (LED)

กระจกแยกลำแสง (Beam Splitter)

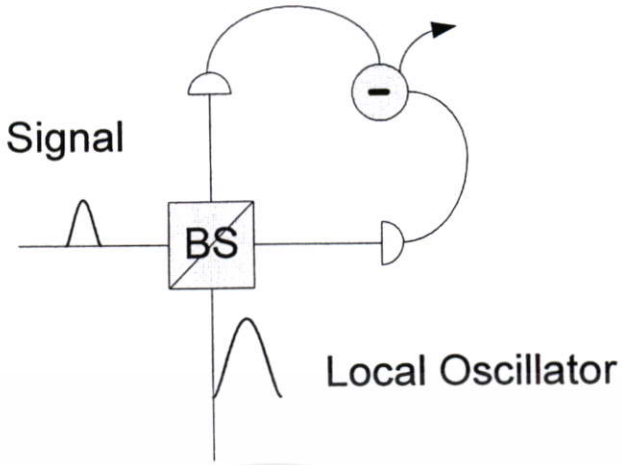
กระจกแยกลำแสงเป็นอุปกรณ์ทางแสงที่ทำหน้าที่ในการแบ่งแสงออกเป็นสองหรือรวมแสงจากเส้นทางอื่นๆเข้ามาในเส้นทางที่กำหนดขึ้นอยู่กับการจัดวางอุปกรณ์ทาง โดยมีอัตราการแบ่งแสงหลายอัตรา เช่น 70:30 60:40 และ 50:50 กระจกแยกลำแสงที่ใช้ในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่องส่วนใหญ่จะใช้อัตราการแบ่งลำแสงที่ 50:50 เนื่องจากจะใช้เพื่อทำการสุ่มเวกเตอร์ฐานจากการนำโปรโตคอล BB84 มาประยุกต์ใช้งาน

กระจกแยกลำแสงโพลาไรเซชัน (Polarization Beam Splitter: PBS)

กระจกแยกลำแสงโพลาไรเซชันเป็นอุปกรณ์ทางแสงที่มีการทำงานคล้ายกับ กระจกแยกลำแสงโดยเป็นอุปกรณ์ที่ใช้ในการแยกลำแสงออกเป็นสองเส้นทาง หรือใช้รวมลำแสงทั้งสองเส้นทางเป็นเส้นทางเดียวขึ้นอยู่กับการจัดวางอุปกรณ์และสถานะโพลาไรเซชันของแสง

อะวัลลันซ์โฟโตไดโอด (Avalanche Photodiode: APD)

ในระบบกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง จะใช้อะวัลลันซ์โฟโตไดโอดที่ทำงานแบบ Passive quenching circuit โดยทำจากสารกึ่งตัวนำซิลิกอน (Silicon) ซึ่งคุณสมบัติในการตรวจจับโฟตอนเดี่ยวได้ดีในช่วงความยาวคลื่น 830 นาโนเมตร แต่ที่ความยาวคลื่น เช่น 1330 และ 1550 นาโนเมตร จะใช้อะวัลลันซ์โฟโตไดโอดที่สร้างจาก InGaAs แทนอะวัลลันซ์โฟโตไดโอดที่สร้างจากสารกึ่งตัวนำซิลิกอนเนื่องจากอะวัลลันซ์โฟโตไดโอดที่สร้างจาก InGaAs จะสามารถตรวจจับโฟตอนเดี่ยวในช่วงความยาวคลื่นแสงนี้ได้ดีกว่าแต่ก็ยังคงตรวจจับโฟตอนเดี่ยวได้ประสิทธิภาพต่ำ



รูปที่ ข.1 การตรวจจับแสงโดยใช้โฮโมไดน์ [43]

ตัวตรวจจับแบบโฮโมไดน์

ตัวตรวจจับแสงแบบโฮโมไดน์ (Homodyne Detector) นั้นมีการทำงานที่แตกต่างจากอะวัลลันซ์โฟโตไดโอด (APD) ตรงที่ตัวตรวจจับแสงแบบโฮโมไดน์นี้จะใช้พัลส์แสงความเข้มสูงเป็นสัญญาณในการอ้างอิงหรือเรียกว่า "Local Oscillator: LO" ซึ่งการทำงานจะแสดงได้ดังรูป ข.1 สัญญาณที่ประกอบด้วยแอมพลิจูด (Amplitude) และเฟส (Phase) ของแสงที่ส่งมาจากภาคส่ง หรือเรียกว่า "Signal" จะมารวมเข้ากับสัญญาณในการอ้างอิง หรือเรียกว่า "Local Oscilator: LO" โดยใช้กระจกแยกลำแสง (Beam Splitter: BS) แบบ 50:50 ทำหน้าที่ในการรวมลำแสงเข้าด้วยกัน ซึ่งสัญญาณ "Signal" และ "LO" จะเข้ามารวมกันที่กระจกแยกลำแสงนี้ หลังจากนั้นจะถูกตรวจจับโดยตัวตรวจจับแบบโฮโมไดน์ ซึ่งจะให้ผลลัพธ์ในรูปแบบของขนาดสัญญาณไฟฟ้า (ระดับแรงดันไฟฟ้า)

Electro-optic modulator

เป็นอุปกรณ์ในการผสมสัญญาณแสงทั้งขนาดของแอมพลิจูดและเฟสของสถานะโพลาไรเซชันของแสงโดยอาศัยการเปลี่ยนระดับแรงดันไฟฟ้า ตัวอย่างของ EOM อย่างง่ายเช่น Pockels Cell ซึ่งจะทำหน้าที่ในการเปลี่ยนมุมของโพลาไรเซชัน ให้มีมุมในทิศทางที่ต่างกันตามที่กำหนดโดยอาศัยสัญญาณไฟฟ้าเข้ามาควบคุมการทำงาน [44] ตัวอย่างการนำ Pockel Cell มาใช้ในระบบวิทยาการรหัสลับเชิงควอนตัมเช่น ระบบที่นำเสนอโดย C.H. Bennett และ G. Brassard [2] ในปี ค.ศ. 1992

บัญชีศัพท์

กฎความไม่แน่นอนของไฮเซนแบร์ก	Uncertainty Principle
กระจกแยกลำแสง	Beam Splitter
กระจกแยกลำแสงโพลาไรเซชัน	Polarized Beam Splitter
กระบวนการกลั่นกุญแจรหัสลับ	Secret Key Distillation
กระบวนการไกล่เกลี่ยความผิดพลาด	Reconciliation
การกระจายกุญแจรหัสลับเชิงควอนตัม	Quantum Key Distribution
การกระจายกุญแจรหัสลับเชิงควอนตัมแบบต่อเนื่อง	Continuous Variable Quantum Key Distribution
การกระจายกุญแจรหัสลับเชิงควอนตัมแบบไม่ต่อเนื่อง	Discrete Variable Quantum Key Distribution
การกระจายโอกาสแบบเกาส์	Gaussian Distribution
การกระจายโอกาสแบบปัวส์ซอง	Poisson Distribution
การแก้ไขข้อผิดพลาดแบบสไลซ์	Slice Error Correction
การไกล่เกลี่ยความผิดพลาดทางตรง	Direct Reconciliation
การไกล่เกลี่ยความผิดพลาดย้อนกลับ	Reverse Reconciliation
การขยายสภาวะส่วนตัว	Privacy Amplification
การเข้ารหัสช่องสัญญาณ	Channel Coding
การเข้ารหัสลับ	Encryption
การเข้ารหัสแหล่งกำเนิด	Source coder
การตัดสินใจแบบละเอียด	Soft Decision
การตัดสินใจแบบหยาบ	Hard Decision
การถอดรหัสช่องสัญญาณ	Channel Decoding
การถอดรหัสด้วยวิธีไวเทอร์บี	Viterbi Decoding
การถอดรหัสลับ	Decryption
การถอดรหัสแหล่งกำเนิด	Source Decoding
การประมาณค่าสไลซ์	Slice Estimator
การผสมสัญญาณทางความถี่	Frequency Shift Keying

บัญชีศัพท์ (ต่อ)

การผสมสัญญาณทางเฟส	Phase Shift Keying
การผสมสัญญาณหรือการกล้ำสัญญาณ	Modulator
การส่งข่าวสารเชิงควอนตัม	Quantum Teleportation
กุญแจรหัสลับ	Secret Key
กุญแจรหัสลับส่วนตัว	Private Key
กุญแจรหัสลับสาธารณะ	Public Key
ข้อมูลข่าวสารข้าง	Side Information
ควอนตัมคอมพิวเตอร์	Quantum Computer
คำรหัส	Codeword
คิวบิต	Qubit
คีย์ดิบ	Raw Key
เครื่องกำเนิดจำนวนสุ่มเชิงควอนตัม	Quantum Random Number Generator
ช่องทางการสื่อสารเชิงควอนตัม	Quantum Channel
ช่องสัญญาณแบบไบนารี	Binary Symmetric Channel
ช่องสื่อสารสาธารณะ	Public Channel
ช็อตนอยส์ (ชื่อเฉพาะ)	Shot Noise
ซินโดรม	Syndrome
ชิฟคีย์ (ชื่อเฉพาะ)	Sifted Key
ไดโอดเปล่งแสงหรือแอลอีดี	Light Emitting Diode
ตัวตรวจจับโฟตอนแบบโฮโมไดน์	Homodyne Detector
ทฤษฎีกลศาสตร์ควอนตัม	Quantum Mechanics
ทฤษฎีข่าวสาร	Information Theory
ทฤษฎีข่าวสารเชิงควอนตัม	Quantum Information Theory
น้ำหนักแฮมมิง	Hamming Weight
บุคคลที่สาม	Eavesdropper วิทยาการรหัสลับเรียกว่า *Eve*
ปริมาณข่าวสารเฉลี่ยหรือเอนโทรปี	Entropy

บัญชีศัพท์ (ต่อ)

ปริมาณข่าวสารร่วม	Mutual Information
ผลคูณร่วมน้อย	Least Common Multiple
ผู้รับ	Receiver วิทยาการรหัสลับเรียกว่า *Bob*
ผู้ส่ง	Sender วิทยาการรหัสลับเรียกว่า *Alice*
พหุนามกำเนิด	Generator Polynomial
พหุนามต่ำสุด	Minimum Polynomial
พาริตี้บิต	Parity Bit
โพลาไรเซชัน	Polarization
ฟังก์ชันความหนาแน่นของความน่าจะเป็น	Probability Density Function
ฟังก์ชันแจกแจงสะสม	Cumulative Distribution Function
ฟังก์ชันทางเดียว	One-way Function
ฟังก์ชันสไลซ์ (ชื่อเฉพาะ)	Slices Function
เฟส	Phase
โฟตอนเดี่ยว	Single Photon
โฟโตไดโอด	Photodiode
เมทริกซ์กำเนิด	Generator Matrix
เมทริกซ์ตรวจสอบพาริตี้	Parity Check Matrix
รหัสแก้ไขความผิดพลาดล่วงหน้า	Forward Error Correcting Code
รหัสคอนโวลูชัน	Convolution Code
รหัสคอนโวลูชันแบบไม่สมมาตร	Nonsystematic Convolution Code
รหัสคอนโวลูชันแบบสมมาตร	Systematic Convolution Code
รหัสเทอร์โบ	Turbo Code
รหัสบล็อกเชิงเส้น	Linear Block Code
รหัสแบบสมมาตร	Systematic Code
รหัสแบบอสมมาตร	Nonsystematic Code
รหัสวน	Cyclic Code
รหัสแฮมมิง	Hamming Code

บัญชีศัพท์ (ต่อ)

ระยะแฮมมิง	Hamming Distance
ระยะแฮมมิงน้อยที่สุด	Minimum Hamming Distance
รีดันแดนซี	Redundancy
เรเดียน	Radian
วิทยาการรหัสลับ	Cryptography
วิทยาการรหัสลับเชิงควอนตัม	Quantum Cryptography
วิทยาการรหัสลับแบบสมมาตร	Systematic Cryptography
วิทยาการรหัสลับแบบอสมมาตร	Asystematic Cryptography
วิธีการส่งซ้ำอัตโนมัติ	Automatic Retransmission Query หรือ Automatic Repeat Request
สถานะโคฮีเรนต์	Coherent State
สัญญาณรบกวน	Noise
สัญญาณรบกวนขาวหรือสัญญาณรบกวนช่วงกว้าง	White Noise
สัญญาณรบกวนเนื่องจากอุณหภูมิ	Thermal Noise
สัญลักษณ์	Symbol
เส้นใยนำแสง	Fiber Optic
แหล่งกำเนิดข่าวสาร	Information Source
อะวัลลันซ์โฟโตไดโอด	Avalanche Photodiode
อัตราส่วนกำลังงานของสัญญาณต่อกำลังงานของสัญญาณรบกวน	Signal to Noise Ratio (dB)

ประวัติผู้เขียน

ชื่อ- นามสกุล นายวุฒิกรณ์ ตรัยศิลานันท์

วัน เดือน ปีเกิด 19 ตุลาคม 2526 ที่นครราชสีมา

ประวัติการศึกษา 2543 มัธยมศึกษาปีที่ 6 โรงเรียนบุญวัฒนา จังหวัดนครราชสีมา

2547 วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

2548 ศึกษาต่อระดับปริญญาโท ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และได้รับทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST)

งานวิจัยที่สนใจ วิทยาการรหัสลับเชิงควอนตัม รหัสแก้ไขความผิดพลาดล่วงหน้า (FEC) และระบบสื่อสารดิจิตอล