การวิเคราะห์ระบบควอนตัมคริปโตกราฟฟี

AN ANALYSIS OF QUANTUM CRYPTOGRAPHY SYSTEM

วรินดา นาทะสิริ
WARINDA NATASIRI

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมสารสนเทศ
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2547

ISBN 974-15-1189-2

AN ANALYSIS OF QUANTUM CRYPTOGRAPHY SYSTEM

WARINDA NATASIRI

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF ENGINEERING IN INFORMATION ENGINEERING
SCHOOL OF GRADUATE STUDIES
KING MOMGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2004

ISBN 974-15-1189-2

หัวข้อวิทยานิพนธ์	การวิเคราะห์ระบบควอนตัมคริปโตกราฟฟี
นักศึกษา	นางสาว วรินดา นาทะสิริ
รหัสนักศึกษา	44612902
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
พ.ศ.	2547
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ.ดร. ปิติเขต สู้รักษา

บทคัดย่อ

การรักษาความปลอดภัยของข้อมูล ถือเป็นส่วนประกอบที่สำคัญของขั้นตอนการสื่อสารข้อมูลในปัจจุบัน ระบบควอนตัมคริปโตกราฟฟีเป็นระบบที่ทำการส่งคีย์ที่ใช้ในการเข้ารหัสข้อมูล โดยแทนค่าคีย์แต่ละบิตด้วยทิศการโพลาไรซ์ของโฟตอน และได้รับการยอมรับว่าสามารถรักษาความปลอดภัยของข้อมูลได้อย่างมีประสิทธิภาพ โดยมีพื้นฐานจากหลักความไม่แน่นอนในทฤษฎีของควอนตัมฟิสิกส์ วิทยานิพนธ์นี้ทำการศึกษาและวิเคราะห์โปรโตคอล BB84 ซึ่งเป็นโปรโตคอลหนึ่งในระบบควอนตัมคริปโตกราฟฟี โดยวิเคราะห์ในส่วนของค่าความน่าจะเป็นของการสุ่มค่าคีย์ในขั้นตอนเริ่มต้น และวิธีการประมาณค่าความผิดพลาดของคิวบิต (QBER) ผลการทดลองที่ได้แสดงถึงประสิทธิภาพการส่งค่าคีย์ที่ดีขึ้น โดยทดลองในโปรแกรมจำลองที่สร้างขึ้นเพื่อจำลองการทำงานของโปรโตคอล

Thesis Title	An Analysis of Quantum Cryptography System
Student	Miss Warinda Natasiri
Student ID.	44612902
Degree	Master of Engineering
Programme	Information Engineering
Year	2004
Thesis Advisor	Assoc.Prof.Dr. Pitikhate Sooraksa

ABSTRACT

One of the important parts of communication system is the information security, which uses the method of cryptography to keep the information secure from any attackers. Quantum cryptography makes use of the polarized photon bases to encode the secret key bit. The system has proved to be secured by the uncertainty principle in quantum physics. This thesis studies and analyses BB84 protocol, which is one of the quantum cryptography protocols. The analysis concerns the method of key random probability adjustment in the first step of BB84 protocol and the qu-bit error rate (QBER) estimation. The simulation shows satisfactory results compared to the conventional protocol. The BB84 simulation program is built to test effectiveness of the overall designed system.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี ด้วยคำแนะนำและคำปรึกษาเกี่ยวกับแนวคิด หลักการ การวิเคราะห์ และการประยุกต์ใช้งานของระบบควอนตัมคริปโตกราฟฟี ข้อคิดเห็น คำเสนอแนะอันมีค่า และคำปรึกษาต่าง ๆ ที่เป็นประโยชน์แก่ข้าพเจ้า ตลอดจนช่วยตรวจทานแก้ไขวิทยานิพนธ์ฉบับนี้จนเสร็จสมบูรณ์จาก รศ.ดร.ปิติเขต สู้รักษา ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ข้าพเจ้าขอกราบขอบพระคุณเป็นอย่างสูง

ขอกราบขอบพระคุณคณาจารย์ทุกท่านที่ได้ประสาทความรู้ให้แก่ข้าพเจ้าตลอดระยะเวลาของการเรียนจนกระทั่งข้าพเจ้ามีโอกาสประสบความสำเร็จ

ขอกราบขอบพระคุณบิดา มารดาของข้าพเจ้า ที่ให้การสนับสนุน และให้กำลังใจในการเรียน และการทำวิจัยเป็นอย่างดีตลอดมา

สุดท้ายขอขอบคุณเพื่อน ๆ พี่ ๆ นักศึกษาปริญญาโทที่ให้คำแนะนำเป็นอย่างดีตลอดมา

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

วรินดา นาทะสิริ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การเข้ารหัสข้อมูลโดยใช้หลักการของระบบคริปโตกราฟฟี เป็นวิธีหนึ่งที่ใช้ในการรักษาความปลอดภัยของข้อมูลในระบบการสื่อสารข้อมูลในปัจจุบัน [1] เนื่องจากในการเข้ารหัสข้อมูลนั้นจะต้องอาศัยส่วนประกอบที่สำคัญ 2 ส่วนทำงานร่วมกันคือ อัลกอริทึมที่ใช้ในการเข้ารหัส และค่าคีย์ ในปัจจุบันอัลกอริทึมที่แต่ละหน่วยงานนำไปใช้ในการเข้ารหัสข้อมูลนั้น โดยส่วนมากแล้วมีหลักการทำงานที่คล้ายกัน ดังนั้นอัลกอริทึมจึงเป็นสิ่งที่สามารถเปิดเผยได้ สิ่งที่ต้องเก็บรักษาเป็นความลับคือ ค่าคีย์ที่ผู้ส่งข้อมูลนำมาใช้ร่วมกับอัลกอริทึมในการเข้ารหัส ซึ่งในระบบคริปโตกราฟฟีแบบสมมาตร (symmetric) ค่าคีย์ที่ใช้เข้ารหัสจะเป็นคีย์ตัวเดียวกันที่ใช้ในการถอดรหัสสำหรับผู้รับข้อมูล [2] ปัญหาที่เกิดขึ้นคือ ทำอย่างไรจึงจะสามารถส่งค่าคีย์ระหว่างผู้ส่งไปยังผู้รับได้อย่างปลอดภัย โดยปราศจากการเข้ามาขโมยหรือคัดลอกข้อมูลระหว่างที่ส่งค่าคีย์ไปในช่องสัญญาณในการส่งค่าคีย์แบบเดิมนั้น ค่าของคีย์จะถูกแทนด้วยระดับสัญญาณดิจิตอล ซึ่งหากมีผู้บุกรุกแอบเข้ามาวัดค่าคีย์ในระหว่างที่ส่งไปในช่องสัญญาณ ผู้รับจะไม่สามารถรู้ได้เลยว่ามีการแอบวัดข้อมูลเกิดขึ้นเนื่องจากระดับสัญญาณดิจิตอลจะไม่เปลี่ยนแปลงไป

เนื่องจากปัญหาในการส่งคีย์ ทำให้มีการเสนอวิธีการเข้ารหัสแบบอสมมาตร (asymmetric) ขึ้น หรือเรียกว่าวิธีการเข้ารหัสแบบคีย์สาธารณะ (Public Key encryption) [3] ซึ่งสามารถแก้ปัญหาการส่งคีย์แบบสมมาตร โดยวิธีการเข้ารหัสแบบคีย์สาธารณะนี้จะใช้คีย์คนละตัวในการเข้าและถอดรหัส และอาศัยความซับซ้อนและเวลาในการคำนวณทางคณิตศาสตร์ของการแยกตัวประกอบของตัวเลขจำนวนมากเป็นหลักการในการรักษาความปลอดภัย ซึ่งในปัจจุบันวิธีการเข้ารหัสแบบคีย์สาธารณะเป็นที่นิยมนำไปใช้ในหน่วยงานองค์กรต่างๆ เนื่องจากยังไม่มีเครื่องคำนวณใด ในปัจจุบันที่สามารถคำนวณหาตัวประกอบของตัวเลขจำนวนมากได้ในเวลารวดเร็ว [4] แต่ในอนาคตหากมีการสร้างเครื่องคำนวณที่คำนวณได้อย่างรวดเร็วกว่าปัจจุบันระบบการเข้ารหัสแบบคีย์สาธารณะอาจไม่ปลอดภัยอีกต่อไป

ระบบควอนตัมคริปโตกราฟฟี เป็นระบบที่สามารถแก้ไขปัญหาความปลอดภัยในการส่งค่าคีย์ได้ [5] โดยใช้การแทนค่าคีย์แต่ละบิตด้วยทิศการโพลาไรซ์ของโฟตอน ซึ่งหากมีการแอบเข้ามาวัดค่าโฟตอนระหว่างที่ส่งโดยที่ไม่รู้สถานะของการโพลาไรซ์ของโฟตอนมาก่อน และใช้ค่าตัววัดที่ผิด จะมีผลทำให้สถานะของการโพลาไรซ์เปลี่ยนไป [6] โดยการเปลี่ยนไปของสถานะมีผลมาจากหลักความไม่แน่นอนในทฤษฎีของควอนตัมฟิสิกส์ จึงทำให้ผู้รับและผู้ส่งสามารถรู้ได้ว่า มีผู้บุกรุก

เข้ามาในระบบ จากการคำนวณค่าความผิดพลาดของโฟตอนที่เปลี่ยนแปลงไป

ในปัจจุบันได้มีการวิจัย วิเคราะห์ และออกแบบโปรโตคอลเพื่อนำมาปรับปรุงวิธีการเข้ารหัสแบบควอนตัมคริปโตกราฟฟีให้มีประสิทธิภาพที่ดีขึ้น นอกจากนั้นยังได้มีการทดลองสร้างระบบฮาร์ดแวร์ของควอนตัมคริปโตกราฟฟี [7-9] รวมถึงมีผลิตภัณฑ์ทางการค้าออกมาจำหน่าย โดยบริษัท ไอดี ควอนติก โดยสามารถสื่อสารข้อมูลโดยใช้สายไฟเบอร์ออพติกได้ในระยะทาง 100 กิโลเมตร [10] และบริษัท เมจิก เทคโนโลยี [11] ที่ทำการวิจัยและออกแบบผลิตภัณฑ์ทางการค้าของระบบควอนตัมคริปโตกราฟฟี ออกมาจำหน่าย

งานวิจัยนี้เป็นการเสนอวิธีการวิเคราะห์ประสิทธิภาพของโปรโตคอล BB84 ซึ่งเป็นโปรโตคอลแรกของระบบควอนตัมคริปโตกราฟฟี โดยการทดลองปรับค่าความน่าจะเป็นในการสุ่มคีย์ ทำให้เพิ่มจำนวนคีย์ที่สามารถเก็บได้มากขึ้นในระบบ และใช้วิธีการคำนวณค่าความผิดพลาดของคิวบิท (QBER : Qubit Error Rate) แบบแบ่งแยก (Seperated QBER estimation) เพื่อให้สามารถตรวจจับผู้บุกรุกในระบบได้ โดยใช้โปรแกรม Matlab เป็นเครื่องมือในการทดสอบ

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

1. เพื่อปรับปรุงประสิทธิภาพของโปรโตคอล BB84 ให้สามารถเก็บคีย์ได้มากขึ้น
2. ปรับปรุงวิธีการคำนวณค่า QBER ให้เหมาะสมกับวิธีใหม่ที่ออกแบบ
3. เปรียบเทียบโปรโตคอลที่ออกแบบใหม่กับโปรโตคอลดั้งเดิมและศึกษาข้อดีข้อเสีย
4. เพื่อประยุกต์ใช้กับโปรโตคอลอื่นของระบบควอนตัมคริปโตกราฟฟีต่อไป
5. ศึกษาระบบฮาร์ดแวร์และการทำงานจริงของควอนตัมคริปโตกราฟฟี

1.3 สมมติฐานของการศึกษา

1. การปรับค่าความน่าจะเป็นในการสุ่มคีย์ ทำให้ได้จำนวนคีย์ที่สามารถเก็บได้มากขึ้นในระบบ

2. การคำนวณ QBER แบบแบ่งแยกมีความเหมาะสมกับวิธีการปรับความน่าจะเป็นและยังสามารถตรวจจับผู้บุกรุกในระบบได้

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

1. ทฤษฎีควอนตัมคริปโตกราฟฟีโปรโตคอล BB84
2. เทคนิคและวิธีของการปรับปรุงประสิทธิภาพในการเก็บคีย์โดยใช้วิธีปรับความน่าจะเป็นในการสุ่ม

3. เทคนิคและวิธีของการคำนวณ QBER แบบแบ่งแยก

1.5 ขอบเขตการวิจัย

1. ออกแบบโปรแกรมจำลอง จากระบบฮาร์ดแวร์ของควอนตัมคริปโตกราฟฟี
2. นำโปรแกรมที่ได้ออกแบบมาทดลองกับโปรโตคอล BB84 โดยใช้โปรแกรม Matlab เป็นเครื่องมือในการเขียนโปรแกรม
3. หาค่าความน่าจะเป็นที่เหมาะสมในการสุ่ม
4. เปลี่ยนวิธีการคำนวณ QBER เป็นแบบแบ่งแยก

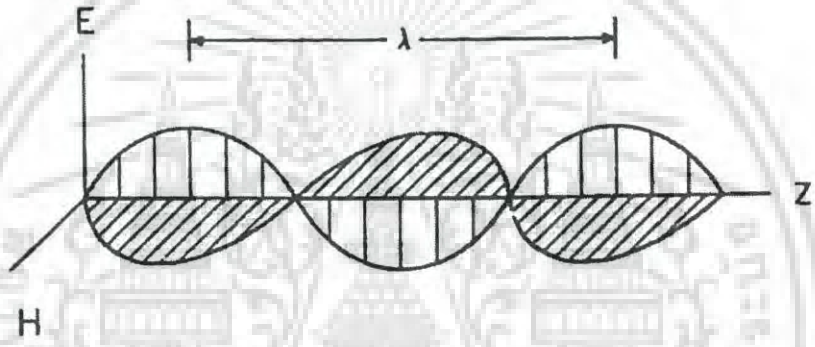
1.6 ขั้นตอนการศึกษา

1. ค้นคว้า รวบรวม ศึกษาเอกสาร และข้อมูลที่เกี่ยวข้อง
2. ออกแบบและทดสอบโปรแกรมจำลองของระบบควอนตัมคริปโตกราฟฟี
3. ทดสอบโปรโตคอล BB84 แบบดั้งเดิม
4. ทดลองเปลี่ยนค่าความน่าจะเป็นในการสุ่ม แล้วเปรียบเทียบผลการทดลอง
5. ทดลองการคำนวณ QBER แบบแบ่งแยก
6. ทำการแก้ไขความผิดพลาด (Error Correction)
7. สรุปผลวิจารณ์ผลการทดลอง และเรียบเรียงวิทยานิพนธ์

บทที่ 2
ทฤษฎีแสงที่เกี่ยวข้อง

2.1 คุณสมบัติของแสงในทางแม่เหล็กไฟฟ้า

แสงเป็นคลื่นแม่เหล็กไฟฟ้า (electromagnetic wave) ซึ่งเกิดจากสนามไฟฟ้าและสนามแม่เหล็กที่มีความถี่เดียวกันตั้งฉากกันและเหนี่ยวนำซึ่งกันและกัน [12] ตามแบบจำลองของ Maxwell ดังรูปที่ 2.1 แสงมีคุณสมบัติเป็นได้ทั้งคลื่นและอนุภาค และมีคุณสมบัติการโพลาไรซ์



รูปที่ 2.1 ภาพของคลื่นแสงซึ่งประกอบด้วยสนามแม่เหล็กและสนามไฟฟ้าตั้งฉากกัน

รูปที่ 2.1 แสดงภาพของคลื่นแม่เหล็กไฟฟ้าที่เป็นคลื่นระนาบ (plane wave) ซึ่งเป็นคลื่นที่ประกอบด้วยสนามไฟฟ้าและสนามแม่เหล็กที่แผ่กระจายในทิศที่แน่นอน และถูกจำกัดไว้ ในที่นี้กำหนดให้ E คือเวกเตอร์ของสนามไฟฟ้าซึ่งมีทิศอยู่ในแนวแกน y และ H คือเวกเตอร์ของสนามแม่เหล็กซึ่งมีทิศอยู่ในแนวแกน x ทิศการเคลื่อนที่ของคลื่นแม่เหล็กไฟฟ้ามีทิศตามแนวแกน z สนามไฟฟ้าเป็นฟังก์ชันของ z และเวลา t มีความสัมพันธ์ดังสมการ

$$E(z,t) = E_x^0 \sin\left[2\pi f\, t - 2\pi z/\lambda + \varphi_0\right] \tag{2.1}$$

โดยที่

f คือ ความถี่ของคลื่นแสง

λ คือ ความยาวคลื่น

E_x^0 คือ แอมปลิจูดของสนามไฟฟ้า

ϕ_0 คือ ค่าเฟส

โดยทั่วไป ความถี่ของแสงมักแสดงด้วยค่า ความถี่เชิงมุม (ω) โดยที่

$$\omega = 2\pi f \tag{2.2}$$

และความยาวคลื่นมักแสดงด้วยค่าคงที่ (k) โดยที่

$$k = 2\pi / \lambda \tag{2.3}$$

ดังนั้น เมื่อแทนค่า ω และ k ลงในสมการที่ 2.1 จะได้

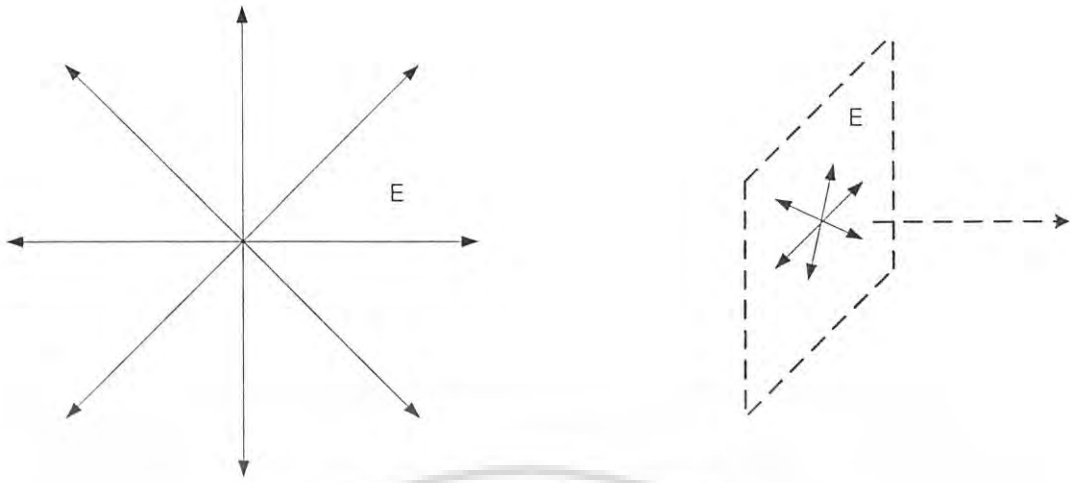
$$E(z,t) = E_x^0 \sin\left[\omega t - k z + \varphi_0\right] \tag{2.4}$$

สนามแม่เหล็ก (H) ของแสงมีเฟสเดียวกันกับสนามไฟฟ้า แต่เวกเตอร์ของสนามแม่เหล็กมีทิศทางตั้งฉากกับสนามไฟฟ้า โดยมีความสัมพันธ์ดังสมการ

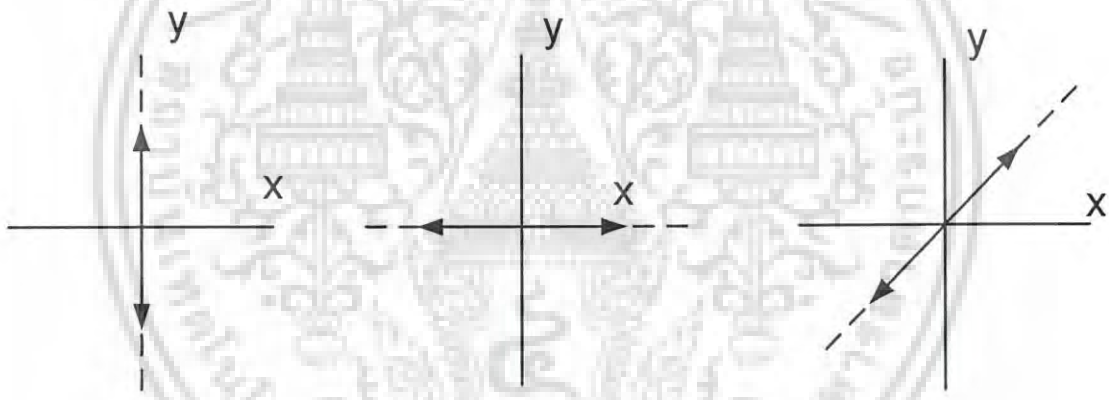
$$H(z,t) = H_y^0 \sin\left[\omega t - k z + \varphi_0\right] \tag{2.5}$$

2.2 การโพลาไรซ์แบบเชิงเส้นของแสง

หัวข้อที่ผ่านมาเป็นการอธิบายถึงแสงซึ่งเกิดจากการเหนี่ยวนำของสนามแม่เหล็กไฟฟ้าตั้งฉากกันในระนาบที่ตั้งฉากกับทิศการแผ่ของคลื่น ในหัวข้อนี้เป็นการอธิบายคุณสมบัติการโพลาไรซ์ของแสง โดยทิศการแผ่กระจายของสนามไฟฟ้า E กำหนดให้เป็นทิศของโพลาไรเซชัน โดยปกติแล้วแสงธรรมดาที่ไม่โพลาไรซ์ (unpolarized light) ประกอบด้วยเวกเตอร์ของสนามไฟฟ้าที่แผ่กระจายในทุกทิศทาง และอยู่บนระนาบที่ตั้งฉากกับทิศการแผ่ของคลื่นดังรูปที่ 2.2 [12] โดยปกติแล้ว ตาของมนุษย์ไม่สามารถบอกความแตกต่างระหว่างแสงโพลาไรซ์กับแสงไม่โพลาไรซ์ได้ แสงโพลาไรซ์ (polarized light) ประกอบด้วยสนามไฟฟ้าซึ่งแผ่กระจายในแนวใดแนวหนึ่งเท่านั้น เช่น ในแนวตั้ง (vertical) หรือแนวนอน (horizontal) ดังแสดงในรูปที่ 2.3



รูปที่ 2.2 ทิศการแผ่กระจายของสนามไฟฟ้าของแสงที่ไม่โพลาไรซ์



รูปที่ 2.3 ทิศการแผ่กระจายของสนามไฟฟ้าของแสงโพลาไรซ์เชิงเส้น

แสงโพลาไรซ์เชิงเส้นตามแนวราบหรือแนวแกน X มีความสัมพันธ์ดังนี้

$$E_x = E_x^0 \sin\left[\omega t - k z + \phi_0\right]\mathbf{i} \qquad (2.6)$$

โดยที่ ค่า E_x^0 คือค่าขนาด (magnitude) ของสนามไฟฟ้า และ i คือเวกเตอร์หนึ่งหน่วย ที่มีทิศทางตามแนวแกน x

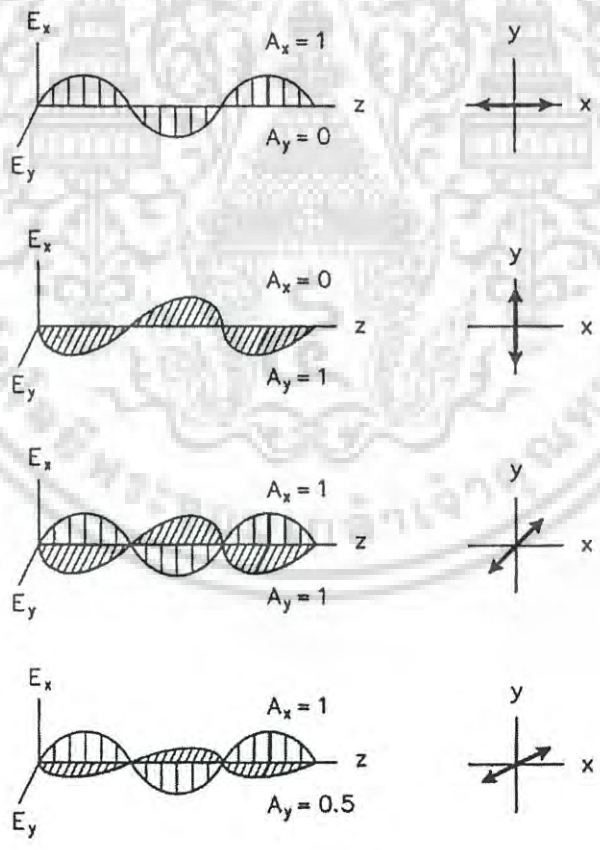
ในทำนองเดียวกัน โพลาไรซ์ของแสงแบบเชิงเส้นตามแนวแกน y มีความสัมพันธ์ดังนี้

$$E_y = E_y^0 \sin\left[\omega t - k z + \phi_0\right] \mathbf{j} \tag{2.7}$$

โดยที่ ค่า E_y^0 คือขนาดของสนามไฟฟ้า และ j คือเวกเตอร์หนึ่งหน่วย ที่มีทิศทางตามแนวแกน y

สนามไฟฟ้าสามารถมีทิศทางการโพลาไรซ์ได้ทุกทิศ โดยทิศการโพลาไรซ์จะตั้งฉากกับทิศของการแผ่ของสนามไฟฟ้าเสมอ ทิศการโพลาไรซ์ใด ๆ ของแสงสามารถแสดงอยู่ในรูปของผลรวมของเวกเตอร์ E_x และ E_y ได้ ดังรูปที่ 2.4 ซึ่งการรวมเวกเตอร์สามารถแสดงในรูปของสมการ ดังนี้

$$E = E_x + E_y = \left\{E_x^0 \mathbf{i} + E_y^0 \mathbf{j}\right\} \sin\left[\omega t - kz + \phi_0\right] \tag{2.8}$$



รูปที่ 2.4 ทิศการโพลาไรซ์ของแสงในรูปของเวกเตอร์ โดยที่ (a) มีการโพลาไรซ์ตามแนวแกน x (b) มีการโพลาไรซ์ตามแนวแกน y (c) มีการโพลาไรซ์ในทิศทำมุม 45 องศา กับแกน x และ (d) มีการโพลาไรซ์ในทิศทำมุม 26.55 องศากับแกน x

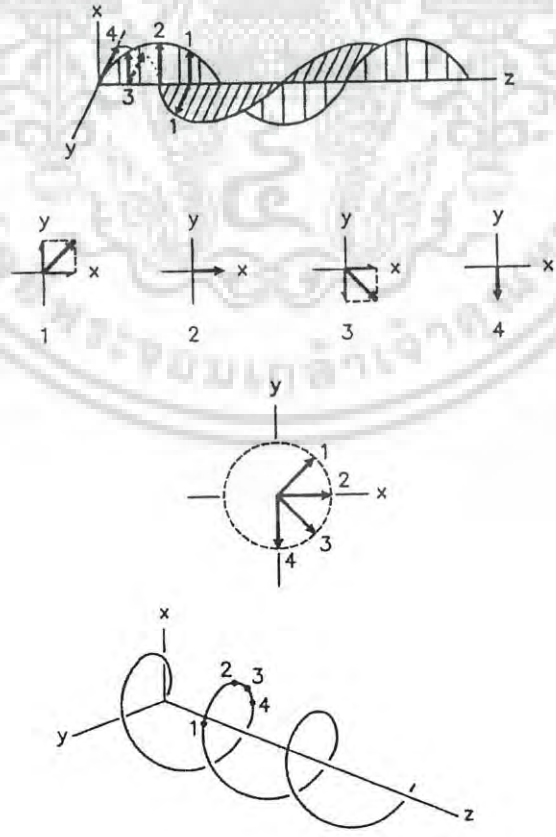
จากรูปที่ 2.4 จะเห็นว่า มุมของทิศการโพลาไรซ์ของแสงเทียบกับแกน x จะขึ้นอยู่กับค่าแอมปลิจูดของเวกเตอร์ที่นำมารวมกัน อย่างไรก็ตาม ทิศการโพลาไรซ์ของแสงที่เกิดจากการรวมเวกเตอร์นี้ กำหนดให้เวกเตอร์ที่นำมารวมนั้นมีค่าความถี่เชิงมุม (ω) และค่าเฟส ϕ_0 เท่ากัน ในหัวข้อต่อไปเป็นการกล่าวถึง การโพลาไรซ์ของแสง ในกรณีที่เวกเตอร์ที่นำมารวมมีเฟสต่างกัน

2.3 การโพลาไรซ์แบบวงกลมของแสง

จากหัวข้อที่ 2.2 หากกำหนดให้ค่าแอมปลิจูดของคลื่นแสงมีค่าเท่ากัน แต่ให้เฟสมีค่าต่างกัน 90 องศา จะได้ความสัมพันธ์ ดังสมการ

$$E_r = E^{\circ}\left\{\sin\left[\omega t - kz + \varphi_0\right]i + \sin\left[\omega t - kz + \varphi_0 + \pi/2\right]j\right\} \qquad (2.9)$$

สมการที่ 2.9 แสดงความสัมพันธ์ของการรวมเวกเตอร์ของแสงโดยกำหนดให้มีเฟสต่างกันเท่ากับ +□/2 แต่มีความสูงของแอมปลิจูดเท่ากัน ซึ่งจะได้ผลลัพธ์เป็นการโพลาไรซ์แบบวงกลมของแสงที่มีทิศการหมุนไปทางขวา (right circular) หรือทิศตามเข็มนาฬิกา (cw) ดังรูปที่ 2.5

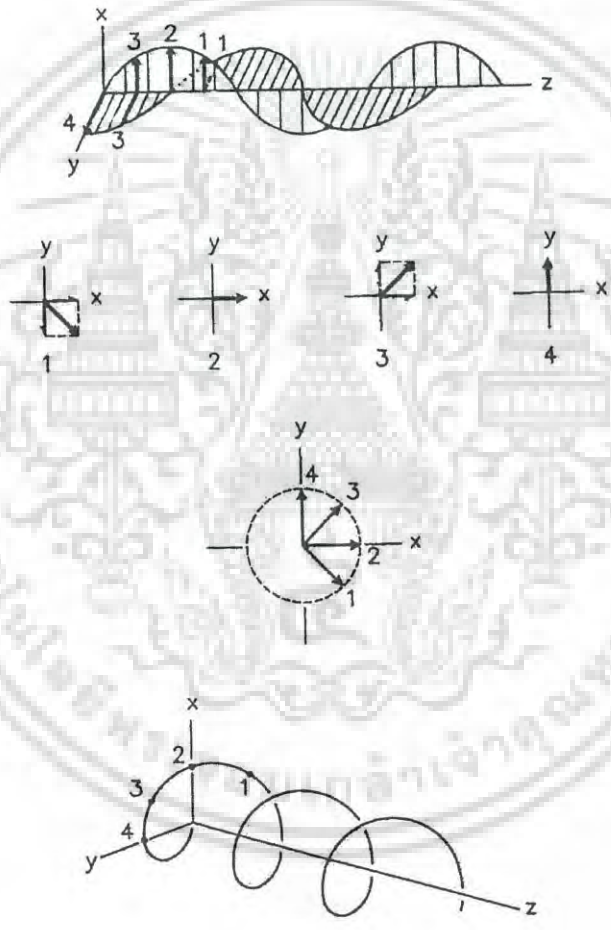


รูปที่ 2.5 การโพลาไรซ์ของแสงแบบหมุนขวา

หากกำหนดให้การรวมเวกเตอร์ของแสงมีเฟสต่างกันเท่ากับ -□/2 แต่มีความสูงของแอมปลิจูดเท่ากัน จะได้ความสัมพันธ์ดังสมการที่ 2.10

$$E_L = E^{\circ} \{\sin[\omega t - kz + \varphi_0]\, \mathbf{i} + \sin[\omega t - kz + \varphi_0 - \pi/2]\, \mathbf{j}\} \qquad (2.10)$$

ซึ่งจะได้ผลลัพธ์เป็นการโพลาไรซ์แบบวงกลมของแสงที่มีทิศการหมุนไปทางซ้าย (left circular) หรือทิศทวนเข็มนาฬิกา (cw) ดังรูปที่ 2.6



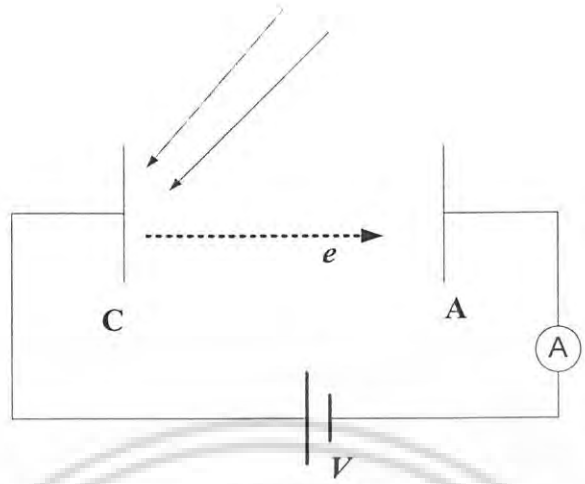
รูปที่ 2.6 การโพลาไรซ์ของแสงแบบหมุนซ้าย

2.4 คุณสมบัติทางควอนตัมของแสง

ในช่วงปลายศตวรรษที่ 19 ถึงช่วงต้นศตวรรษที่ 20 ได้มีผู้ทำการทดลองและศึกษาปรากฏการณ์ต่าง ๆ เช่น การแผ่รังสีของวัตถุดำ ปรากฏการณ์โฟโตอิเล็กตริก การเกิดสเปกตรัมเชิงเส้น การเกิดรังสีเอกซ์ และปรากฏการณ์คอมพ์ตัน แต่ผลสรุปของปรากฏการณ์เหล่านี้ ไม่สามารถใช้ทฤษฎีคลื่นแม่เหล็กไฟฟ้าของแมกซ์เวลอธิบายได้ทุกประการ เช่น ในการแผ่รังสีของวัตถุดำ ไม่สามารถใช้ความรู้ที่กล่าวว่าแสงเป็นคลื่นอธิบายได้ เนื่องจากในปรากฏการณ์นี้ ดูเหมือนว่าแสงประพฤติตัวคล้ายลำอนุภาค ต่อมา Planck [14] สามารถนำแนวคิดอนุภาคแบบควอนตัมมาอธิบายสเปกตรัมของการแผ่รังสีจากวัตถุดำได้ ซึ่งการศึกษาถึงปรากฏการณ์การแผ่รังสีของวัตถุดำและปรากฏการณ์อื่น ๆ ดังที่กล่าวมานั้น จัดว่าเป็นแนวคิดพื้นฐานที่นำไปสู่ทฤษฎีควอนตัม (Quantum Theory) ในวิทยานิพนธ์นี้จะกล่าวถึงเพียงปรากฏการณ์โฟโตอิเลกตริกเนื่องจากเป็นปรากฏการณ์ที่ค้นพบกลุ่มพลังงานในแสงที่เรียกว่าโฟตอน ซึ่งเกี่ยวข้องกับระบบควอนตัมคริปโตกราฟฟีที่ใช้อนุภาคโฟตอนเป็นตัวกำหนดค่าของคีย์

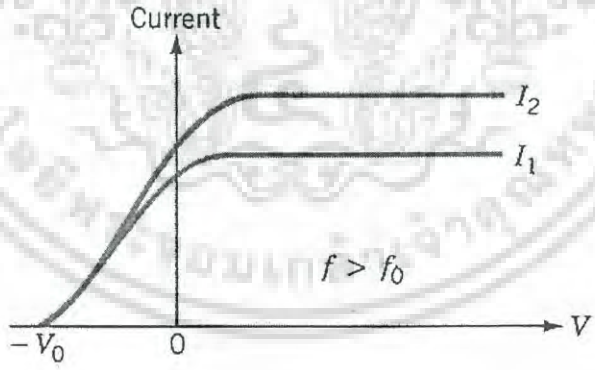
2.4.1 ปรากฏการณ์โฟโตอิเลกตริก

ในช่วงปลายศตวรรษที่ 19 ได้มีการค้นพบว่า เมื่อฉายแสงที่มีความถี่สูงไปบนผิวโลหะจะมีอิเล็กตรอนหลุดออกมาจากผิวโลหะนั้น ปรากฏการณ์ที่แสงทำให้อิเล็กตรอนหลุดมาจากผิวโลหะได้นี้ เรียกว่า ปรากฏการณ์โฟโตอิเลกตริก (photoelectric effect) และเรียกอิเล็กตรอนที่หลุดออกมาจากโลหะว่า โฟโตอิเล็กตรอน (photoelectrons) ผู้ที่ค้นพบปรากฏการณ์นี้เป็นคนแรกคือ นักวิทยาศาสตร์ชาวเยอรมันชื่อ Hertz [15] ปรากฏการณ์โฟโตอิเลกตริกแสดงได้โดยใช้อุปกรณ์ดังรูปที่ 2.7 แผ่นโลหะ C และ A อยู่ในหลอดสุญญากาศ โดยที่ C ต่อกับขั้วไฟฟ้าลบ A ต่อกับขั้วไฟฟ้าบวก เมื่อฉายแสงความถี่เดียวที่มีความถี่สูงพอเหมาะไปบนแผ่นโลหะ C จะสังเกตเห็นว่ามีกระแสในวงจร โดยดูจากการเบนของเข็มแอมป์มิเตอร์ แสดงว่ามีอิเล็กตรอนหลุดออกจากแผ่น C ไปยังแผ่น A



รูปที่ 2.7 วงจรสำหรับศึกษาปรากฏการณ์โฟโตอิเลกตริก

เมื่อทดลองปรับค่าความต่างศักย์ระหว่างขั้ว C และ A แล้วอ่านค่ากระแส พบว่าที่ความต่างศักย์ต่ำ กระแสในวงจรจะน้อย เนื่องจากโฟโตอิเล็กตรอนบางตัวมีพลังงานจลน์ไม่มากพอที่จะไปถึงแผ่น A ได้ แต่เมื่อเพิ่มความต่างศักย์ กระแสจะมากขึ้นและคงตัวในที่สุด ดังแสดงในรูปที่ 2.8



รูปที่ 2.8 กระแสโฟโตอิเล็กตรอนที่ความต่างศักย์ค่าต่างๆ

เมื่อทดลองกลับขั้วไฟฟ้าให้ A เป็นลบเทียบกับ C กระแสในวงจรจะค่อย ๆ ลดลง ทั้งนี้เนื่องจากสนามไฟฟ้ามีทิศการแผ่ต้านกับการเคลื่อนที่ของอิเล็กตรอน โดยอิเล็กตรอนที่มีพลังงานจลน์มากพอเท่านั้นจึงจะมาถึงขั้ว A ได้ เมื่อปรับค่าศักย์ไฟฟ้าที่ A จนเป็นลบที่ค่า ๆ หนึ่งเทียบกับ C คือ $-V_s$ พบว่าไม่มีกระแสในวงจรเลย ค่าความต่างศักย์นี้เรียกว่า ความต่างศักย์หยุดยั้ง (stopping potential) ค่าพลังงานจลน์สูงสุดของโฟโตอิเล็กตรอนสามารถหาได้จากสมการที่ 2.11

$$(E_k)_{max} = \frac{1}{2}mv^2{}_{max} = eV_s \qquad (2.11)$$

โดยที่

E_k คือ พลังงานจลน์ของอิเล็กตรอน

m คือ มวลของโฟโตอิเล็กตรอน

e คือ ประจุของโฟโตอิเล็กตรอน

V_{max} คือ ความเร็วของโฟโตอิเล็กตรอนที่มีพลังงานจลน์สูงสุด

จากรูปที่ 2.8 พบว่าถึงแม้จะใช้แสงที่มีความเข้มต่างกัน (I_1 และ I_2) ก็ยังคงใช้ความต่างศักย์หยุดยั้งเท่าเดิม แสดงว่าความเข้มของแสงไม่มีส่วนให้โฟโตอิเล็กตรอนมีพลังงานจลน์เพิ่มขึ้น แต่มีส่วนทำให้จำนวนอิเล็กตรอนที่หลุดออกมาในหนึ่งหน่วยเวลาเพิ่มขึ้น นั่นคือทำให้กระแสในวงจรเพิ่มขึ้นนั่นเอง

เมื่อทำการทดลองเปลี่ยนค่าความถี่ของแสงแล้วสังเกตค่าของกระแสไฟฟ้าในวงจรผลที่สังเกตได้ไม่สามารถใช้ความรู้ทางฟิสิกส์ดั้งเดิมที่ว่าแสงเป็นคลื่นมาอธิบายได้ [15] ซึ่งข้อสรุปต่าง ๆ ที่กล่าวมามีดังนี้

1. ถ้าความถี่ของแสงมีค่าต่ำกว่าค่าคงตัวค่าหนึ่ง ที่เรียกว่าความถี่เริ่มเปลี่ยน (Threshold Frequency) f_0 ไม่ว่าจะเพิ่มความเข้มแสงเป็นเท่าใด ก็ไม่ทำให้เกิดโฟโตอิเล็กตรอน

2. ถ้าความถี่ของแสงสูงกว่าความถี่เริ่มเปลี่ยน จำนวนโฟโตอิเล็กตรอนที่หลุดออกมาจะขึ้นกับความเข้มแสง แสงที่มีความเข้มสูงกว่าจะให้จำนวนโฟโตอิเล็กตรอนมากกว่า

3. ปรากฏการณ์นี้เกิดขึ้นในช่วงเวลาที่สั้นมาก (น้อยกว่า 10^{-9} วินาที) เมื่อแสงกระทบผิวโลหะก็จะเกิดโฟโตอิเล็กตรอนขึ้นทันที ซึ่งขัดแย้งกับความคิดเดิมที่กล่าวว่าแสงเป็นคลื่น เนื่องจากหากแสงเป็นคลื่นโลหะจะต้องใช้เวลาพอควรในการดูดกลืนพลังงานจากคลื่นแสงที่ตกกระทบจนมีพลังงานสูงพอให้อิเล็กตรอนหลุดออกมาได้

ในปี ค.ศ. 1905 Einstein [15] ได้เสนอแนวคิดเกี่ยวกับทฤษฎีโฟตอนของแสง ซึ่งนำมาอธิบายปรากฏการณ์โฟโตอิเลกตริกได้เป็นผลสำเร็จ และได้รับรางวัลโนเบลในปี ค.ศ. 1921 โดยใช้แนวคิดเกี่ยวกับการแผ่รังสีของวัตถุดำ (Black body) เป็นควอนตัมของพลังงาน Einstein ได้เสนอว่า แสงหรือคลื่นแม่เหล็กไฟฟ้าประกอบด้วยกลุ่มก้อนพลังงานที่เรียกว่า โฟตอน (photons) แสงที่มีความถี่ f ประกอบไปด้วยโฟตอนซึ่งมีพลังงาน E เท่ากับ hf โดยที่ h คือค่าคงตัวของพลังค์ Einstein ได้เสนอว่าแสงที่กระทบแผ่นโลหะมีลักษณะคล้ายลำอนุภาค ซึ่งประกอบด้วยกลุ่มก้อนพลังงานเล็ก ๆ หรือเรียกว่าโฟตอนเป็นจำนวนมาก แต่ละก้อนมีค่าพลังงานเท่ากับ hf โฟตอนแต่ละตัวจะกระทบอิเล็กตรอนในลักษณะการกระทบกันระหว่างอนุภาค โฟตอนจึงมีการถ่ายเท

พลังงานเท่ากับ hf ให้กับอิเล็กตรอน ซึ่งการที่อิเล็กตรอนจะหลุดจากอะตอมของแผ่นโลหะได้จะต้องได้รับพลังงานจากโฟตอนอย่างน้อยเท่ากับค่าฟังก์ชันงาน (work function) W_0 ซึ่งเป็นพลังงานที่อะตอมยึดอิเล็กตรอนไว้ ถ้าพลังงานที่ได้รับมากกว่าค่าฟังก์ชันงาน พลังงานส่วนที่เหลือก็จะเป็นพลังงานจลน์ของอิเล็กตรอน ทำให้อิเล็กตรอนที่หลุดออกมาสามารถเคลื่อนที่ไปยังขั้วไฟฟ้าบวกได้ โดยค่าพลังงานของโฟตอนและค่าพลังงานจลน์ของอิเล็กตรอนมีความสัมพันธ์ดังนี้

$$E_k = hf - W_0 \tag{2.12}$$

E_k คือ พลังงานจลน์ของอิเล็กตรอน

h คือ ค่าคงที่ของพลังค์

W_0 คือ ค่าฟังก์ชันงานคือพลังงานที่อะตอมยึดอิเล็กตรอนไว้

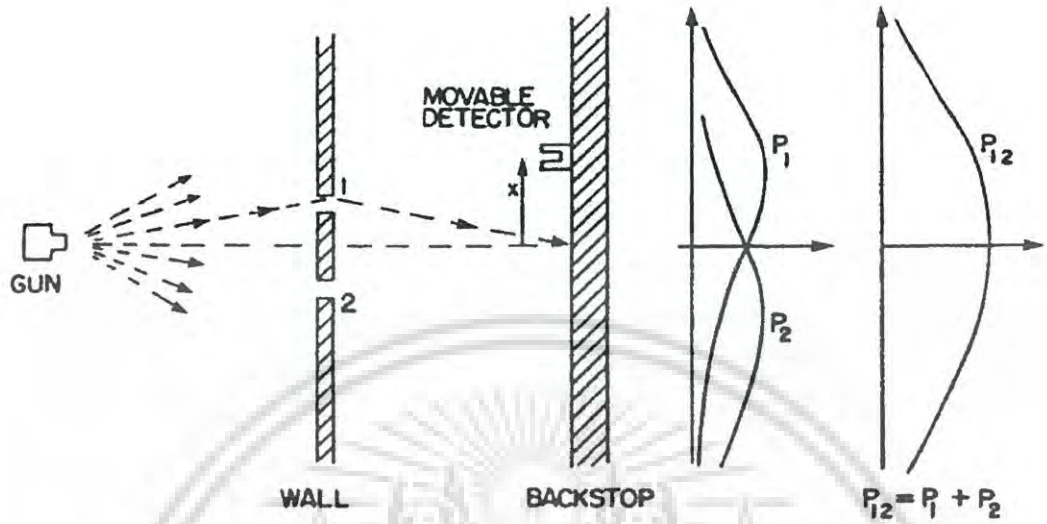
จากแนวคิดเกี่ยวกับทฤษฎีโฟตอนของแสง สรุปได้ว่าแสงประกอบด้วยกลุ่มพลังงานเล็ก ๆ แบบไม่ต่อเนื่องประพฤติตัวคล้ายเป็นลำอนุภาค ซึ่งขัดแย้งกับแบบจำลองของแสงของแมกซ์เวลที่กล่าวว่าแสงประพฤติตัวเป็นคลื่น ในหัวข้อต่อไปเป็นการอธิบายการทดลองเปรียบเทียบคุณสมบัติของอนุภาคซึ่งเป็นแบบไม่ต่อเนื่อง และคลื่นซึ่งเป็นแบบต่อเนื่องโดยการส่งวัตถุที่แทนคุณสมบัติอนุภาคคือการยิงลูกปืนผ่านช่องแคบคู่ โดยเปรียบเทียบผลที่ได้กับการส่งคลื่นน้ำผ่านช่องแคบคู่ และการทดลองสุดท้ายเป็นการยิงอนุภาคอิเลคตรอนผ่านช่องแคบคู่ เพื่อสังเกตผลการทดลองว่าอนุภาคอิเลคตรอนมีคุณสมบัติเป็นคลื่นหรืออนุภาค

2.4.2 คุณสมบัติอนุภาค

ในหัวข้อนี้เป็นการอธิบายการทดลองยิงลูกปืนผ่านกำแพงที่มีช่องแคบคู่ [16] เพื่อหาค่าความน่าจะเป็นของจำนวนลูกปืนที่จะผ่านช่องแคบคู่นั้น การจัดอุปกรณ์การทดลองแสดงดังรูปที่ 2.5 ซึ่งประกอบด้วยปืนซึ่งยิงลูกปืนออกมาในลักษณะแผ่กระจายแบบสุ่ม ถัดจากปืนคือกำแพงที่มีช่องแคบ 2 ช่องที่มีขนาดใหญ่พอจะให้ลูกปืนผ่านไปได้ ถัดมาเป็นกำแพงซึ่งมีตัวตรวจจับอยู่บนกำแพงนั้นโดยตัวตรวจจับสามารถเคลื่อนที่ได้ในระยะทาง x ตัวตรวจจับทำหน้าที่นับจำนวนของลูกปืนที่ผ่านเข้าไปในตัวตรวจจับ เมื่อทำการทดลองยิงลูกปืนและเคลื่อนตัวตรวจจับที่ระยะห่างจากจุดศูนย์กลางเท่ากับระยะ x เราสามารถหาความน่าจะเป็นที่ลูกปืนจะผ่านช่องแคบและหยุดที่ตัวตรวจจับในแต่ละค่า x ที่ต่างกัน โดยมี 3 กรณีคือ

- เปิดช่อง 1 และปิดช่อง 2 จะได้ค่าความน่าจะเป็นแบบ P_1
- เปิดช่อง 2 และปิดช่อง 1 จะได้ค่าความน่าจะเป็นแบบ P_2
- เปิดทั้ง 2 ช่อง จะได้ค่าความน่าจะเป็นแบบ P_{12}

ซึ่งแสดงในรูปที่ 2.9



รูปที่ 2.9 การยิงลูกปืนผ่านกำแพงที่มีช่องแคบคู่ เพื่อหาค่าความน่าจะเป็นของจำนวนลูกปืนที่จะผ่านช่องแคบคู่นั้น

จากผลการทดลองที่ได้จะเห็นว่า ค่าความน่าจะเป็นที่เกิดจากการเปิดช่องแคบทั้ง 2 ช่อง เท่ากับผลรวมของค่าความน่าจะเป็นในการเปิดช่อง 1 หรือช่อง 2 เพียงช่องเดียว ซึ่งมีความสัมพันธ์คือ

$$P_{12} = P_1 + P_2 \tag{2.13}$$

2.4.3 **คุณสมบัติคลื่น**

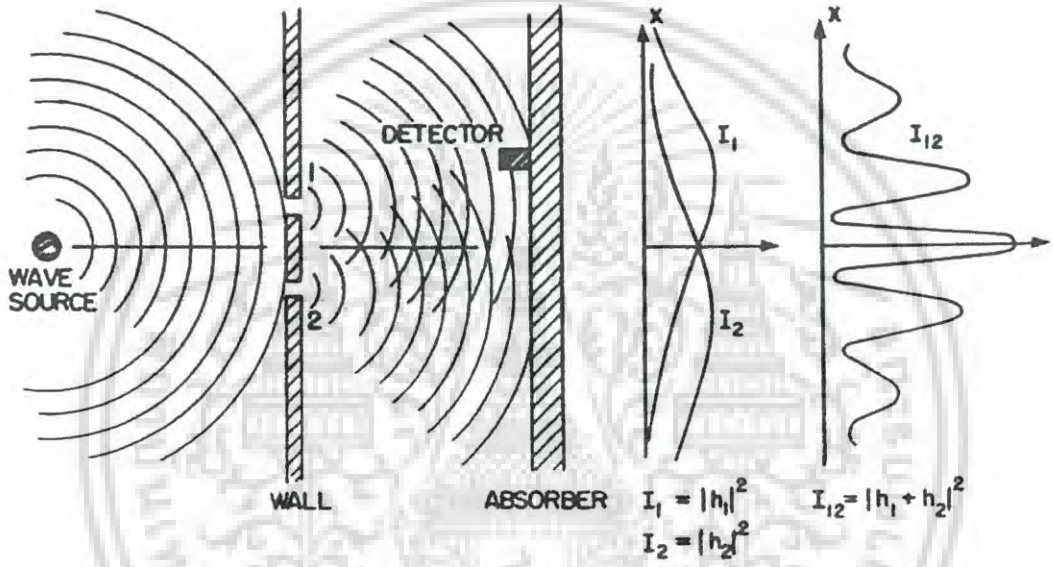
ในหัวข้อนี้ เป็นการแสดงการทดลองส่งคลื่นน้ำผ่านช่องแคบคู่ โดยมีอุปกรณ์แสดงดังรูปที่ 2.10 มีรางน้ำตื้นและมีแหล่งกำเนิดคลื่นซึ่งเคลื่อนไหวขึ้นลงโดยมอเตอร์ทำให้เกิดคลื่นวงกลมทางด้านขวาของแหล่งกำเนิดคลื่น มีกำแพงที่มีช่อง 2 ช่อง ถัดมาเป็นกำแพงที่ทำหน้าที่ดูดกลืนไม่ให้มีการสะท้อนของคลื่นเมื่อตกกระทบ ซึ่งมีตัวตรวจจับวางอยู่บนกำแพงสามารถเคลื่อนที่ได้ในทิศทาง x ตัวตรวจจับนี้เป็นอุปกรณ์ที่ทำหน้าที่วัดความหนาแน่นของคลื่น

ในการทดลองกับคลื่นน้ำนี้ สิ่งที่สังเกตได้คือ ความหนาแน่นของคลื่นที่วัดได้ที่ตัวตรวจจับจะเป็นลักษณะค่าต่อเนื่อง ต่างจากการทดลองในหัวข้อ 2.4.2 ซึ่งเป็นการนับจำนวนลูกปืนที่เป็นค่าไม่ต่อเนื่อง

เมื่อทำการวัดค่าความหนาแน่นของคลื่นที่ตำแหน่ง x ที่ต่างกัน ในขณะที่

- เปิดช่อง 1 และปิดช่อง 2 จะได้ค่าความเข้มของคลื่นที่มีลักษณะการกระจายแบบ I_1
- เปิดช่อง 2 และปิดช่อง 1 จะได้ค่าความเข้มของคลื่นที่มีลักษณะการกระจายแบบ I_2
- เปิดช่อง 1 และช่อง 2 พร้อมกัน จะได้ค่าความเข้มของคลื่นที่มีลักษณะการกระจายแบบ I_{12}

ซึ่งแสดงในรูปที่ 2.10



รูปที่ 2.10 การส่งคลื่นน้ำผ่านช่องแคบคู่ เพื่อหาค่าความหนาแน่นของคลื่นที่ผ่านช่องแคบคู่นั้น

ค่าความหนาแน่น I_{12} ไม่ใช่ค่าที่เกิดจากการรวมของค่า I_1 และ I_2 เหมือนการทดลองยิงลูกปืนผ่านช่องแคบคู่ที่แสดงในหัวข้อ 2.4.2 แต่ลักษณะของ I_{12} เรียกว่าเป็นการแทรกสอดกันของคลื่นที่ส่งมาจากแหล่งกำเนิด 2 แหล่ง บริเวณที่มีแอมปลิจูดสูงสุด คือบริเวณที่จุดสูงสุดของคลื่นจาก 2 แหล่งมาเสริมกัน และบริเวณที่แอมปลิจูดต่ำสุด คือบริเวณที่จุดต่ำสุดของคลื่นจาก 2 แหล่งมาเสริมกัน

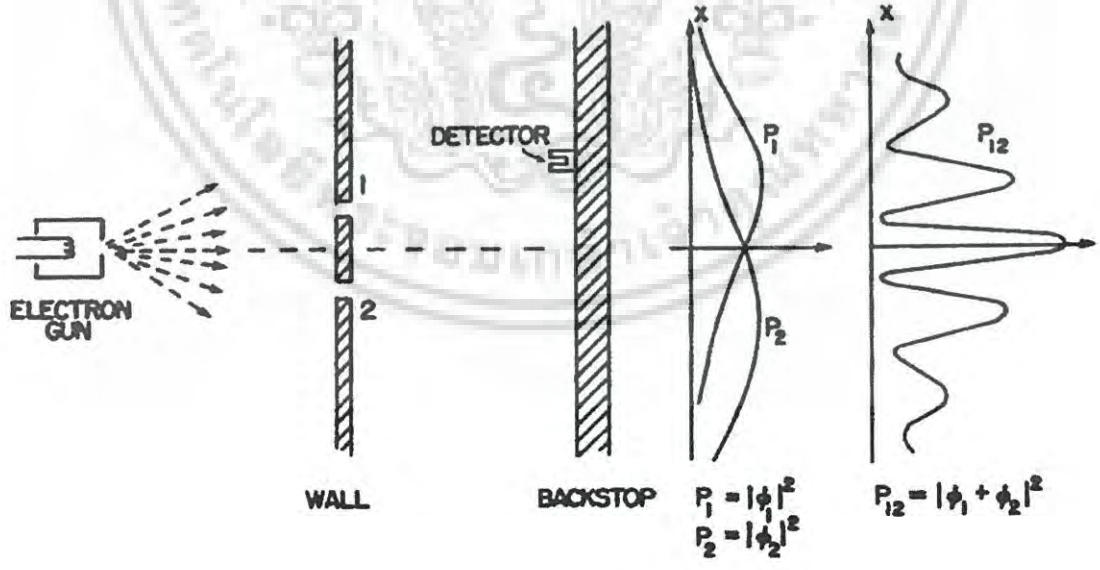
ความสูงของคลื่นที่ผ่านช่องแคบที่ 1 สามารถเขียนในรูปของ $h_1 e^{i\omega t}$ โดยที่แอมปลิจูด คือค่า h_1 ซึ่งเป็นจำนวนเชิงซ้อน และความหนาแน่นของคลื่นคือ I_1 มีค่าเท่ากับกำลังสองของแอมปลิจูด คือ $|h_1|^2$ สำหรับคลื่นที่ผ่านช่องแคบที่ 2 มีความสัมพันธ์เหมือนกับคลื่นที่ผ่านช่องแคบที่ 1 โดยมีความสูงเท่ากับ $h_2 e^{i\omega t}$ โดยแอมปลิจูด คือค่า h_2 และความหนาแน่นของคลื่นคือ I_2 มีค่าเท่ากับกำลังสองของ แอมปลิจูด คือ $|h_2|^2$ และเมื่อเปิดช่องแคบทั้งสองช่องพร้อมกัน ค่าความสูงของคลื่นจะเท่ากับ $(h_1 + h_2)e^{i\omega t}$ และความเข้มจะเท่ากับ $|h_1 + h_2|^2$

2.4.4 คุณสมบัติของอนุภาคอิเลคตรอน

ในหัวข้อนี้เป็นการทดลองซึ่งมีลักษณะคล้ายกับการทดลองในหัวข้อ 2.4.2 และ 2.4.3 แต่เปลี่ยนจากปืนและแหล่งกำเนิดคลื่นน้ำ เป็นปืนที่สามารถยิงอิเลคตรอนออกมา ซึ่งปืนนั้นทำจากลวดทังสเตนถูกทำให้ร้อนด้วยกระแสไฟฟ้าอยู่ในกล่องโลหะมีรู ถ้าเส้นลวดมีแรงดันไฟฟ้าเป็นลบเมื่อเทียบกับกล่องโลหะอิเลคตรอนจะถูกปลดปล่อยจากเส้นลวดไปยังกำแพง และจะมีบางส่วนผ่านช่องแคบ 2 ช่องที่อยู่บนกำแพง อิเลคตรอนทั้งหมดมีพลังงานเท่ากันหรือใกล้เคียงกันมาก ถัดจากปืนอิเลคตรอนเป็นกำแพงที่ทำจากแผ่นโลหะบางมีช่องแคบ 2 ช่อง ถัดมาเป็นกำแพงซึ่งมีตัวตรวจจับซึ่งอาจเป็น Geiger counter หรือ Electron multiplier และตัวตรวจจับนี้ต่อกับลำโพงเพื่อให้มีเสียงออกมาขณะที่มีการตรวจจับอิเลคตรอน ดังรูปที่ 2.11

สิ่งที่สังเกตได้เมื่อทำการทดลองนี้คือ ในขณะที่มีการยิงอิเลคตรอน เราจะได้ยินเสียงจากลำโพงดัง คลิก และเป็นเสียงที่มีลักษณะและความดังเท่ากันทุกครั้ง แต่จะเกิดเสียงขึ้นในระยะเวลาที่ไม่แน่นอน ซึ่งหากทำการนับจำนวนเสียงใน 2 ช่วงเวลา โดยกำหนดให้มีช่วงเวลาที่เท่ากัน จะพบว่าจำนวนเสียงที่เกิดขึ้นมีจำนวนใกล้เคียงกัน ทำให้สามารถหาอัตราเฉลี่ยได้

เมื่อทำการเปลี่ยนตำแหน่งของตัวตรวจจับไปในระยะ x ต่าง ๆ กัน อัตราการเกิดเสียงจะเกิดขึ้นช้าหรือเร็วต่างกัน แต่ความดังของเสียงยังเท่าเดิมเสมอ หากทำการลดอุณหภูมิของเส้นลวด อัตราการเกิดเสียงจะช้าลงแต่ความดังเสียงยังเท่าเดิม



รูปที่ 2.11 การยิงอนุภาคอิเล็กตรอนผ่านช่องแคบคู่ เพื่อหาค่าความน่าจะเป็นของจำนวนอิเล็กตรอนที่จะ ผ่านช่องแคบคู่นั้น

ดังนั้น จากความดังของเสียงที่เท่าเดิมเสมอ สรุปได้ว่า อิเลคตรอนมีลักษณะเป็นอนุภาคซึ่งมีค่าไม่ต่อเนื่อง มีลักษณะเหมือนลูกปืนในการทดลองในหัวข้อ 2.4.2 ต่างจากคลื่นน้ำซึ่งวัดค่าความหนาแน่นที่ตัวตรวจจับได้เป็นค่าต่อเนื่อง

เมื่อทำการวัดจำนวนของอิเลคตรอนที่ผ่านตัวตรวจจับที่ตำแหน่ง x ที่ต่างกัน ในขณะที่

- เปิดช่อง 1 และปิดช่อง 2 จะได้จำนวนอิเลคตรอนที่มีลักษณะการกระจายแบบ P_1
- เปิดช่อง 2 และปิดช่อง 1 จะได้จำนวนอิเลคตรอนที่มีลักษณะการกระจายแบบ P_2
- เปิดช่อง 1 และช่อง 2 พร้อมกัน จะได้จำนวนอิเลคตรอนที่มีลักษณะการกระจายแบบ P_{12}

จากผลที่ได้จะเห็นว่า

$$P_{12} \neq P_1 + P_2$$

ความสัมพันธ์ทางคณิตศาสตร์ของ P_1 P_2 และ P_{12} มีลักษณะเหมือนการทดลองคลื่นน้ำ หากกำหนดให้ ϕ เป็นจำนวนเชิงซ้อนค่าหนึ่ง ค่ากำลังสองของ ϕ คือค่าความน่าจะเป็นที่จะตรวจจับอิเลคตรอนได้เมื่อปิดช่อง 1 กล่าวคือ

$$P_1 = |\phi_1|^2$$

และ

$$P_1 = |\phi_1|^2$$

และเมื่อเปิดทั้ง 2 ช่อง จะได้ P_{12} โดยที่

$$P_{12} = |\phi_1 + \phi_2|^2$$

จากการทดลองนี้สรุปได้ว่า อิเลคตรอนจะประพฤติตัวเป็นอนุภาคเมื่อทำการตรวจจับ ซึ่งสรุปจากระดับความดังของเสียงที่ออกมาจากลำโพงขณะที่มีการตรวจจับอิเลคตรอน โดยที่เสียงเหล่านั้นมีความดังเท่าเดิมเสมอและมีลักษณะไม่ต่อเนื่องเหมือนการนับลูกปืนในหัวข้อ 2.4.2 แต่เมื่อพิจารณาการกระจายของความน่าจะเป็นที่จะพบจำนวนอิเล็กตรอนหลังจากเคลื่อนที่ผ่านช่องแคบคู่ ความน่าจะเป็นที่จะพบอิเล็กตรอนมีการกระจายเป็นแบบคลื่นโดยมีลักษณะเหมือน

การกระจายของคลื่นน้ำในหัวข้อที่ 2.4.3 ดังนั้นสรุปได้ว่า อิเลคตรอนมีคุณสมบัติเป็นทั้งคลื่นและอนุภาคแล้วแต่ว่าเราจะพิจารณาคุณสมบัติของมันในแง่ใด

2.5 สรุป

ในบทนี้เป็นการอธิบายถึงทฤษฎีพื้นฐานของแสงที่เกี่ยวข้องในวิทยานิพนธ์นี้ คือแสงในเชิงคลื่นซึ่งมีคุณสมบัติการโพลาไรซ์แบบเชิงเส้นและแบบวงกลม เนื่องจากในวิทยานิพนธ์นี้ได้ใช้ทิศการโพลาไรซ์ของโฟตอนทั้งแบบเชิงเส้นและแบบวงกลมในการแทนค่าบิตข้อมูลที่ส่ง นอกจากนี้ยังได้อธิบายถึงปรากฏการณ์โฟโตอิเลกตริกและคุณสมบัติในเชิงอนุภาคของแสง ในบทต่อไปเป็นการอธิบายถึงหลักการเข้ารหัสข้อมูลแบบคริปโตกราฟฟี

บทที่ 3
การเข้ารหัสข้อมูลแบบคริปโตกราฟฟี

การเข้ารหัสข้อมูลแบบคริปโตกราฟฟี เป็นหลักการนำข้อมูลในระบบสื่อสารมาเข้ารหัส โดยมีวัตถุประสงค์เพื่อรักษาความปลอดภัยของข้อมูล การสื่อสารข้อมูลในปัจจุบันมีข้อมูลจำนวนมากที่จำเป็นต้องรักษาไว้เป็นความลับ เช่น รหัสลับ (password) ซึ่งใช้ในการเข้าสู่ระบบ หรือ ลายเซ็นดิจิตอล (Digital Signature) ซึ่งใช้เป็นตัวบ่งบอกว่าเป็นบุคคลนั้นจริง ซึ่งหากข้อมูลเหล่านี้ไม่ถูกเก็บไว้เป็นความลับแล้ว อาจก่อให้เกิดความเสียหายแก่หน่วยงานและบุคคลจำนวนมากได้ [17]

การเข้ารหัสข้อมูลแบบคริปโตกราฟฟีได้มีการพัฒนาวิธีการออกแบบอัลกอริทึมที่ใช้ในการเข้ารหัสอย่างต่อเนื่อง โดยมุ่งเน้นที่การเพิ่มความซับซ้อนและเวลาที่ใช้ในการเข้าและถอดรหัส [18] เพื่อให้บุคคลที่สามไม่สามารถลักลอบเข้ามาถอดรหัสข้อมูลได้โดยง่าย ในบทนี้เป็นการอธิบายถึงหลักการทำงานของการเข้ารหัสคริปโตกราฟฟีแบบดั้งเดิมในหัวข้อ 3.1 และระบบการเข้ารหัสแบบควอนตัมคริปโตกราฟฟีในหัวข้อ 3.2 3.3 และ 3.4

3.1 คริปโตกราฟฟีแบบดั้งเดิม (Conventional Cryptography)

โดยทั่วไปแล้ว การเข้ารหัสข้อมูลแบบคริปโตกราฟฟีแบ่งได้เป็น 2 ประเภท คือ สมมาตร (Symmetric) และ อสมมาตร (Asymmetric)

3.1.1 การเข้ารหัสแบบสมมาตร

การเข้ารหัสข้อมูลแบบสมมาตร คือการเข้ารหัสที่ทั้งผู้ส่งและผู้รับข้อมูลใช้ค่าคีย์ตัวเดียวกันในการเข้ารหัสและถอดรหัสตามลำดับ ตัวอย่างของการเข้ารหัสข้อมูลแบบสมมาตร เช่น Caesar Cipher ซึ่งใช้หลักการการแทนที่ของข้อมูล และ Rail Fence Cipher [19] ซึ่งใช้หลักการการสลับตำแหน่งของข้อมูล ภาพแสดงการเข้ารหัสแบบสมมาตร แสดงได้ดังรูปที่ 3.1

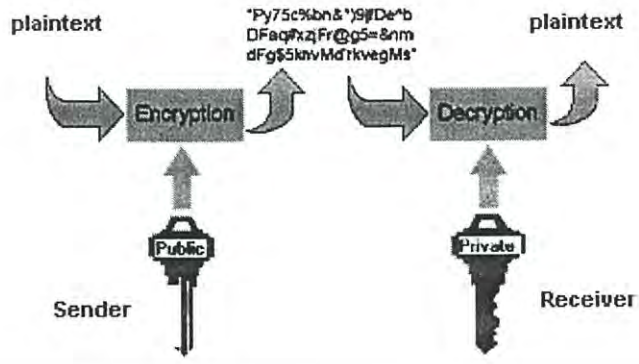
รูปที่ 3.1 แผนภาพการเข้ารหัสแบบสมมาตร

จากรูป 3.1 cleartext หรือ plaintext คือข้อมูลที่ผู้ส่งต้องการส่งให้ผู้รับและไม่ต้องการให้ผู้อื่นสามารถเห็นข้อความนี้ได้ จึงนำข้อมูลนั้นมาเข้ารหัสด้วยคีย์ เมื่อผ่านการเข้ารหัสแล้วจะได้ข้อมูลที่เรียกว่า ciphertext ซึ่งเป็นข้อมูลที่ไม่มีความหมายและไม่สามารถเข้าใจได้ จากนั้นจึงส่ง ciphertext ไปยังช่องสัญญาณสาธารณะ ซึ่งเป็นช่องสัญญาณที่อนุญาตให้ผู้อื่นเข้ามาดูข้อมูลที่ส่งไปได้ แต่เนื่องจากข้อมูลนั้นเป็น ciphertext ซึ่งเป็นข้อมูลที่ไม่มีความหมาย ดังนั้นผู้ที่เข้ามาดูจึงไม่สามารถรู้และเข้าใจข้อมูลนั้นได้ เมื่อผู้รับได้รับ ciphertext แล้ว ต้องทำการถอดรหัสด้วยค่าคีย์เดียวกับที่ผู้ส่งใช้ในการเข้ารหัส แต่อัลกอริทึมที่ใช้ในการถอดรหัสจะต่างกับอัลกอริทึมที่ใช้เข้ารหัส เมื่อผู้รับทำการถอดรหัสแล้วจะได้ผลลัพธ์เป็น cleartext เหมือนเดิม

ความปลอดภัยของการเข้ารหัสแบบสมมาตรขึ้นอยู่กับปัจจัย 2 ประการคือ อัลกอริทึมที่ใช้ในการเข้ารหัส และค่าคีย์ที่ใช้ เนื่องจากการเข้ารหัสแบบสมมาตรนั้น ทั้งผู้ส่งและผู้รับต้องใช้คีย์ตัวเดียวกันในการเข้ารหัสและถอดรหัส ดังนั้นจึงจำเป็นต้องมีการส่งค่าคีย์จากผู้ส่งไปยังผู้รับเพื่อให้ได้คีย์ที่ตรงกัน ซึ่งกระบวนการนี้เรียกว่า การกระจายคีย์ (key distribution) การกระจายคีย์อาจหมายถึง การส่งคีย์จากผู้ส่งไปยังผู้รับ หรือการส่งคีย์จากบุคคลที่สามไปยังผู้ส่งและผู้รับ ซึ่งความซับซ้อนของการกระจายคีย์จะแปรผันตามจำนวนผู้ส่งและผู้รับในระบบ

3.1.2 การเข้ารหัสแบบอสมมาตร

การเข้ารหัสแบบอสมมาตร หรือการเข้ารหัสคีย์สาธารณะ (Public-key Encryption) มีความแตกต่างจากการเข้ารหัสแบบสมมาตร เนื่องจากทั้งผู้ส่งและผู้รับไม่ได้ใช้ค่าคีย์เดียวกัน แต่ใช้หลักการคำนวณทางคณิตศาสตร์ เช่นการแยกตัวประกอบ (factoring) ในการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูล [20] การเข้ารหัสแบบอสมมาตรสามารถอธิบายได้ดังรูปที่ 3.2 เมื่อมีการส่งข้อมูลระหว่างผู้ส่งและผู้รับ ผู้รับจะแจกจ่ายคีย์ให้กับทุกคน ซึ่งคีย์นี้เรียกว่า คีย์สาธารณะ (public-key) โดยที่คีย์สาธารณะนี้ไม่ใช่ข้อมูลที่เป็นความลับ เมื่อผู้ส่งได้รับคีย์สาธารณะแล้วจะทำการเข้ารหัสข้อมูลและส่ง ciphertext ไปยังผู้รับ เมื่อผู้รับได้รับ ciphertext แล้วจะทำการถอดรหัสโดยใช้คีย์ส่วนตัว (private key) ซึ่งคีย์ส่วนตัวนี้ผู้รับจะต้องเก็บเป็นความลับ เนื่องจากหากมีผู้อื่นรู้คีย์ส่วนตัวนี้ ก็จะสามารถนำคีย์ไปถอดรหัสข้อมูลได้



รูปที่ 3.2 ภาพการเข้ารหัสแบบคีย์สาธารณะ

การเข้ารหัสข้อมูลแบบคีย์สาธารณะหรือแบบอสมมาตรได้ถูกคิดค้นขึ้นมาภายหลังการเข้ารหัสข้อมูลแบบสมมาตร โดยมีวัตถุประสงค์หลักคือ เพื่อแก้ปัญหาความไม่ปลอดภัยของการกระจายคีย์ในระบบการเข้ารหัสข้อมูลแบบสมมาตร โดยสามารถแบ่งเป็น 3 ประเภทหลักคือ

- การเข้ารหัสและถอดรหัสข้อมูล
- ลายเซ็นดิจิตอล (Digital Signature)
- การแลกเปลี่ยนคีย์ (Key Exchange)

ตัวอย่างของการเข้ารหัสแบบอสมมาตร เช่น อัลกอริทึม RSA [21] ซึ่งใช้ความยากในการแยกตัวประกอบตัวเลขจำนวนมากเป็นจุดสำคัญในการรักษาความปลอดภัยของข้อมูล การหาค่าคีย์ส่วนตัวสามารถหาได้จากคีย์สาธารณะโดยกระบวนการแยกตัวประกอบ และเนื่องจากการหาค่าตัวประกอบของเลขจำนวนมากนั้น ต้องใช้เวลานานมากสำหรับคอมพิวเตอร์หรือเครื่องคำนวณที่มีใช้อยู่ในปัจจุบัน ดังนั้นระบบการเข้ารหัสแบบอสมมาตรจึงสามารถรักษาความปลอดภัยของข้อมูลได้ อย่างไรก็ตามหากในอนาคตมีเครื่องคำนวณที่สามารถคำนวณได้ในเวลาที่เร็วขึ้นกว่าในปัจจุบันมาก เช่น ควอนตัมคอมพิวเตอร์ (Quantum computer) วิธีการเข้ารหัสข้อมูลแบบอสมมาตรอาจไม่ใช่วิธีที่ปลอดภัยเพียงพออีกต่อไป

3.2 ควอนตัมคริปโตกราฟฟี

ควอนตัมคริปโตกราฟฟี (Quantum Cryptography) หรือการส่งค่าคีย์แบบควอนตัม (Quantum key distribution) [22] เป็นการส่งค่าคีย์จากผู้ส่งไปยังผู้รับโดยมีวัตถุประสงค์คือ เพื่อนำคีย์ที่ส่งได้นั้นไปใช้ในการเข้ารหัสแบบสมมาตรได้อย่างปลอดภัย และสามารถแน่ใจได้ว่าคีย์นั้นจะไม่ถูกบุคคลที่สามแอบดักจับระหว่างที่ส่งข้อมูลไปในช่องสัญญาณ ระบบควอนตัมคริปโตกราฟฟีอาศัยหลักความไม่แน่นอน (Uncertainty property) ในทฤษฎีควอนตัมฟิสิกส์ในการรักษา

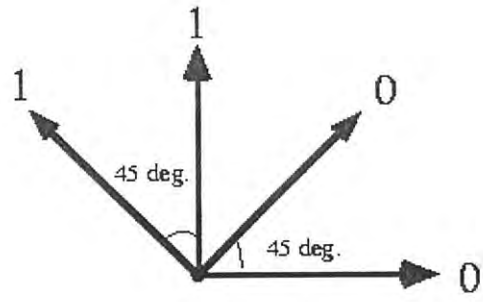
ความปลอดภัยของคีย์ที่ส่ง โดยแนวคิดของระบบควอนตัมคริปโตกราฟฟีถูกเสนอครั้งแรกโดย Stephen Weisner ในต้นปี ค.ศ. 1970 โดยใช้ชื่อว่า Conjugate Coding [23] ต่อมา Charles Bennett และ Gille Brassard ได้เสนอโปรโตคอลแรกของระบบควอนตัมคริปโตกราฟฟีในปี 1984 โดยใช้ชื่อว่า BB84 [24] และในปี 1989 ได้มีการออกแบบและทำการทดลองครั้งแรกในประเทศสหรัฐอเมริกาเพื่อสร้างระบบจริงของควอนตัมคริปโตกราฟฟี โดยการออกแบบระบบนั้นมีพื้นฐานการทำงานบนโปรโตคอล BB84 [25] ในปัจจุบันได้มีการทดลองสร้างระบบจริงของควอนตัม คริปโตกราฟฟี ซึ่งมีหลายรูปแบบ เช่น การส่งข้อมูลทางสายไฟเบอร์ออพติก [26,27] การส่งข้อมูลแบบไร้สาย [28,29] และการนำคุณสมบัติ Entanglement ของอนุภาคโฟตอนมาใช้ในการรักษาความปลอดภัยของข้อมูล [30,31]

ในปัจจุบันโปรโตคอลของระบบควอนตัมคริปโตกราฟฟีที่สามารถนำมาสร้างได้จริง ได้แก่ โปรโตคอล BB84 และโปรโตคอล B92 วิทยานิพนธ์นี้เป็นการปรับปรุงประสิทธิภาพของโปรโตคอล BB84 โดยหลักการและขั้นตอนของโปรโตคอล BB84 จะอธิบายในหัวข้อต่อไป

3.3 โปรโตคอล BB84

โปรโตคอล BB84 เป็นโปรโตคอลหนึ่งของการเข้ารหัสแบบควอนตัมคริปโตกราฟฟี ซึ่งเสนอโดย C.H. Bennett and G. Brassard ในปี คศ. 1984 [24] เป็นโปรโตคอลที่ใช้หลักการความไม่แน่นอนของกลศาสตร์ควอนตัมเพื่อช่วยในการรักษาความปลอดภัยของข้อมูล โดยใช้ทิศการโพลาไรซ์ของอนุภาคโฟตอนแทนความหมายของบิตข้อมูลศูนย์หรือหนึ่ง เนื่องจากคุณสมบัติความไม่แน่นอนของกลศาสตร์ควอนตัม เมื่ออนุภาคโฟตอนถูกรบกวนโดยผู้บุกรุกโดยการเข้ามาวัดค่าทิศการโพลาไรซ์ในขณะส่ง ทิศการโพลาไรซ์จะเปลี่ยนไปแบบย้อนกลับไม่ได้ (irreversible) ทำให้เกิดค่าความผิดพลาด (error) ขึ้น และจากการคำนวณค่าความผิดพลาด (QBER) นั้น ทำให้สามารถตรวจจับผู้ที่บุกรุกเข้ามาขโมยข้อมูลในระบบได้ โดยเปรียบเทียบว่าค่าความผิดพลาดที่คำนวณได้มีค่ามากกว่าค่า Threshold ที่กำหนดหรือไม่

ในการแทนค่าบิตข้อมูลด้วยทิศการโพลาไรซ์ของโฟตอนของโปรโตคอล BB84 แสดงได้ดังรูปที่ 3.3



รูปที่ 3.3 ทิศการโพลาไรซ์ของโฟตอนที่นำมาใช้ในโปรโตคอล BB84

โดยที่

ทิศการโพลาไรซ์ที่ 0 และ 90 องศา เรียกว่า Rectilinear basis

ทิศการโพลาไรซ์ที่ 45 และ 135 องศา เรียกว่า Diagonal basis

จากรูปจะเห็นว่า บิตข้อมูล 0 ถูกแทนด้วยโฟตอนที่มีทิศการโพลาไรซ์ 0 และ 45 องศา และบิตข้อมูล 1 ถูกแทนด้วยโฟตอนที่มีทิศการโพลาไรซ์ 90 และ 135 องศา

ระบบควอนตัมคริปโตกราฟฟีได้รับการยอมรับว่าปลอดภัยจากการแอบเข้ามาดักจับข้อมูลของบุคคลที่สามได้ ดังอาศัยคำอธิบายโดยใช้หลักความไม่แน่นอนทางควอนตัมฟิสิกส์ ดังนี้คือ การวัดทิศการโพลาไรซ์ของโฟตอนด้วยตัววัดที่ไม่ถูกต้อง จะทำให้ทิศการโพลาไรซ์ของโฟตอนเปลี่ยนไปแบบไม่สามารถคืนกลับได้ โดยคุณสมบัตินี้แสดงได้ดังรูปที่ 3.4 และ 3.5

รูปที่ 3.4 การวัดค่าโฟตอนโดยใช้ตัววัดที่ถูกต้อง ค่าที่ได้จะถูกต้อง100 %

รูปที่ 3.5 การวัดค่าโฟตอนโดยใช้ตัววัดที่ไม่ถูกต้อง ค่าที่ได้จะเป็นค่าสุ่มโดยมีโอกาสถูกและผิดเท่ากัน

กระบวนการของโปรโตคอล BB84 มีขั้นตอนดังนี้

1. ผู้ส่งทำการสุ่มเลือกทิศการโพลาไรซ์ของโฟตอนให้แต่ละบิตข้อมูล โดยเลือกจาก 1 ใน 4 ของทิศการโพลาไรซ์ (0, 45, 90, 135) แล้วส่งไปให้ผู้รับ

2. ผู้รับทำการสุ่มค่าเบสิส (Basis) ที่ใช้วัด โดยเลือกว่าจะวัดโฟตอนแต่ละตัวด้วย Rectilinear หรือ Diagonal

3. ผู้รับทำการวัดค่าโฟตอนที่ส่งมา แล้วบันทึกผลการวัดที่ได้

4. ผู้รับบอกเบสิสที่ใช้ในการวัดโฟตอนแต่ละตัว (ไม่ได้บอกค่าที่วัดได้) แก่ผู้ส่งทางช่องสัญญาณสาธารณะ

5. ผู้ส่งบอกผู้รับว่า เบสิสใดบ้างที่ถูกต้องตรงกับที่ผู้รับสุ่มในขั้นตอนแรก

6. ทั้งผู้ส่งและผู้รับทำการทิ้งค่าคีย์ที่ใช้เบสิสในการวัดไม่ตรงกัน และเก็บเฉพาะบิตที่ใช้เบสิสตรงกัน เนื่องจากโฟตอนที่ใช้เบสิสในการวัดถูกต้อง จะได้ผลการวัดที่ถูกต้อง 100% (หากไม่คำนึงถึงสัญญาณรบกวนในระบบจริง)

7. ทั้งผู้ส่งและผู้รับทำการสุ่มข้อมูลบิตโฟตอนขึ้นมาจำนวนหนึ่ง และเปรียบเทียบกันเพื่อหาค่าความผิดพลาดคิวบิท (QBER : Q-Bit Error Rate) ซึ่งค่าความผิดพลาดในที่นี้ อาจเกิดจากสัญญาณรบกวน หรือ การแอบมีบุคคลที่สามเข้ามาวัดข้อมูล (Eavesdropper)

8. หากค่าความผิดพลาดคิวบิทเกินกว่าเกณฑ์ที่ยอมรับได้ (Error Threshold) ซึ่งหมายถึงมีคนแอบเข้ามาวัดข้อมูล ทั้งผู้ส่งและผู้รับจะทำการเริ่มต้นส่งค่าคีย์ใหม่อีกครั้ง

9. หากค่าความผิดพลาดคิวบิทอยู่ในเกณฑ์ที่ยอมรับได้ (ไม่เกิน 25%) ซึ่งหมายถึงแน่ใจได้ว่าไม่มีคนแอบเข้ามาวัดข้อมูลระหว่างส่ง ทั้งผู้ส่งและผู้รับจะเริ่มกระบวนการแก้ไขความผิดพลาดของข้อมูล (Error Correction) เพื่อให้คีย์ที่อยู่ที่ทั้งผู้ส่งและผู้รับมีค่าเดียวกัน เนื่องจากบิตข้อมูลที่ได้อาจมียังมีความผิดพลาดที่เกิดจากความไม่สมบูรณ์ของอุปกรณ์ฮาร์ดแวร์ หรือสัญญาณรบกวนในระบบ

10. นำคีย์ที่ได้ไปเข้ารหัสข้อมูลแบบ Vernam Cipher

ขั้นตอนการทำงานของโปรโตคอล BB84 ในรูปแบบของโฟลวชาร์ทแสดงดังรูปที่ 3.6

รูปที่ 3.6 ขั้นตอนการทำงานของโปรโตคอล BB84

3.3.1 การสุ่มค่าเบสิสโฟตอนในภาคส่ง

จากหัวข้อที่ 3.3 ขั้นตอนที่ 1 ของโปรโตคอล BB84 มีการสุ่มค่าโฟตอนในภาคส่ง และส่งออกไป การสุ่มค่าจะต้องเลือกทิศการโพลาไรซ์จาก 1 ใน 4 คือ 0, 45, 90 และ 135 องศา โดยที่ทิศการโพลาไรซ์ 0 องศาและ 90 องศา เรียกว่า Rectilinear basis และ ทิศการโพลาไรซ์ 45 องศา และ 135 องศา เรียกว่า Diagonal basis โดยความน่าจะเป็นในการเลือกทิศการโพลาไรซ์

1 ใน 4 ทิศนี้จะต้องเท่ากัน คือ1/4 หรือ 25% หรืออาจกล่าวได้ว่า ความน่าจะเป็นในการเลือกทิศการโพลาไรซ์ของโฟตอนระหว่าง Rectilinear basis และ Diagonal basis เท่ากับ 1/2 หรือ 50%

3.3.2 การสุ่มค่าเบสิสโฟตอนในภาครับ

ในขั้นตอนที่ 2 หัวข้อที่ 3.3 ในภาครับผู้รับจะทำการสุ่มค่าเบสิสที่ใช้วัด โดยเลือกว่าจะวัดโฟตอนแต่ละตัวด้วยแบบ Rectilinear หรือ Diagonal โดยค่าความน่าจะเป็นในการเลือกตัววัดเท่ากับ 1/2 หรือ 50% เหมือนกับในภาคส่ง

3.3.3 การเก็บค่าคีย์ที่ใช้ได้

ในขั้นตอนที่ 6 หัวข้อที่ 3.3 ทั้งผู้ส่งและผู้รับทำการทิ้งค่าคีย์ที่ใช้เบสิสในการวัดไม่ตรงกัน และเก็บเฉพาะบิตที่ใช้เบสิสตรงกัน เนื่องจากโฟตอนที่ใช้เบสิสในการวัดถูกต้อง จะได้ผลการวัดที่ถูกต้อง 100% ดังนั้นหากทั้งผู้ส่งและผู้รับเลือกใช้ค่าความน่าจะเป็นในการเลือกเบสิสของโฟตอนแบบ Rectilinear เท่ากับแบบ Diagonal คือ 0.5 แล้ว โอกาสที่คีย์และตัววัดคีย์จะตรงกัน คือ 50% หรือครึ่งหนึ่งของคีย์ที่ส่งไปทั้งหมด

3.3.4 การคำนวณค่า Q-Bit Error Rate

ค่า Q-Bit Error Rate (QBER) เป็นค่าที่บอกถึงอัตราความผิดพลาดของบิทข้อมูลที่ส่งในระบบควอนตัมคริปโตกราฟฟี และค่านี้สามารถนำมาใช้พิจารณาว่าระบบมีผู้บุกรุกเข้ามาวัดข้อมูลหรือไม่ โดยสามารถคำนวณได้จาก

$$\frac{\text{Error bit}}{\text{All bit}} \times 100 \qquad (3.1)$$

ค่าที่ได้อยู่ในรูปของเปอร์เซ็นต์ของบิทที่ผิดพลาด ในโปรโตคอล BB84 หากในระบบมีความผิดพลาดทางฮาร์ดแวร์ หรือมีสัญญาณรบกวนจากภายนอกหรือแม้แต่สัญญาณรบกวนที่เกิดขึ้นจากอุปกรณ์ในระบบเองก็จะมีผลทำให้เกิดความผิดพลาดในการส่งคีย์และมีผลให้ QBER สูงขึ้น โดยทั่วไปแล้วในงานวิจัยที่มีการทดลองสร้างระบบฮาร์ดแวร์จริงของระบบควอนตัมคริปโตกราฟฟีในปัจจุบันจะมีค่าความผิดพลาดประมาณ 1% ถึง 5% [32] แต่หากมีคนแอบเข้ามาวัดค่าของโฟตอนในขณะที่ส่ง โดยสุ่มค่าเบสิสที่ใช้ในการวัดโฟตอน Rectilinear เท่ากับ Diagonal คือ 0.5 ค่าความผิดพลาดจะมีค่าประมาณ 25% ซึ่งสูงกว่าค่าความผิดพลาดของระบบขณะที่ไม่มีคนแอบเข้ามาวัดโฟตอนมาก ดังนั้นจึงสามารถรู้ได้ว่าระบบมีผู้บุกรุกเข้ามาวัดโฟตอนหรือไม่โดยเทียบค่า QBER ที่ได้จากการคำนวณว่ามากกว่าค่าความผิดพลาดจากสัญญาณรบกวนในระบบหรือไม่ หากค่าความผิดพลาดมากกว่าที่ยอมรับ ระบบจะเริ่มต้นการส่งค่าคีย์ใหม่ตั้งแต่ขั้นตอนแรก

หากค่าความผิดพลาดเป็นที่ยอมรับได้ ก็จะทำกระบวนการต่อไปคือการแก้ไขความผิดพลาดของข้อมูล

3.3.5 กระบวนการ Error Correction

เนื่องจากในบิทข้อมูลหลังจากที่ทำการเช็คค่า QBER แล้ว จะยังมีค่าที่ผิดพลาดอยู่ และในการเข้ารหัสข้อมูลแบบสมมาตร ผู้ส่งและผู้รับจะต้องใช้ค่าคีย์ตัวเดียวกันในการเข้ารหัสและถอดรหัสข้อมูล ดังนั้นจึงต้องมีกระบวนการแก้ไขความผิดพลาดเพื่อให้ทั้งผู้ส่งและผู้รับมีข้อมูลคีย์ที่ตรงกัน เช่น กระบวนการเรียงสับเปลี่ยนแบบสุ่ม (Random permutation) [33] มีหลักการคือแบ่งข้อมูลเป็นบล็อก แล้วหาพาริตีบิต หากบล็อกไหนไม่ตรงกัน ให้นำบล็อกนั้นมาแบ่งครึ่ง แล้วหา พาริตีของแต่ละส่วน และเมื่อเช็กพาริตีเสร็จแล้วต้องลบข้อมูลไป 1 ตัว แบ่งบล็อกไปเรื่อย ๆ จนเจอตัวที่ผิด แล้วสลับข้อมูลและเริ่มกระบวนการเช็คพาริตี้อีกจนแน่ใจว่าไม่มีตัวผิดแล้ว

3.3.6 Vernam Cipher

การเข้ารหัสข้อมูลแบบ Vernam Cipher หรือ One-Time Pad เป็นการเข้ารหัสที่สามารถพิสูจน์ได้ทางคณิตศาสตร์ว่ามีความปลอดภัยอย่างสมบูรณ์ [34] การเข้ารหัสข้อมูลแบบ Vernam Cipher พัฒนาโดย Gilbert Vernam ในปี 1918 และจัดว่าอยู่ในประเภทการเข้ารหัสแบบสมมาตรเนื่องจากทั้งการเข้ารหัสและถอดรหัสใช้ค่าคีย์ตัวเดียวกัน โดยข้อมูลที่นำมาเข้ารหัสจะถูกแปลงให้อยู่ในรูปของเลขฐานสอง หากเป็นตัวอักษรจะถูกแปลงให้เป็นรหัส ASCII ก่อน ค่าคีย์ที่ใช้จะต้องเป็นข้อมูลที่ได้จากการสุ่มอย่างแท้จริง (truly random data) และอยู่ในรูปของเลขฐานสองเช่นเดียวกับข้อมูล อัลกอริทึมที่ใช้ในการเข้ารหัสคือการ Exclusive Or (XOR) ระหว่างข้อมูลและค่าคีย์ ผลลัพธ์ที่ได้จากการ XOR คือ Ciphertext ที่ส่งไปในช่องสัญญาณ และเมื่อผู้รับได้รับ Ciphertext นี้แล้วก็จะใช้ค่าคีย์ตัวเดิมทำการถอดรหัสด้วยวิธี XOR เช่นกันและจะได้ผลลัพธ์กลับเป็น Plaintext เหมือนเดิม

Input bits		Output bit
Message	Key	
0	0	0
0	1	1
1	0	1
1	1	0

รูปที่ 3.7 อัลกอริทึมการเข้ารหัสแบบ Vernam Cipher

การเข้ารหัสแบบ Vernam Cipher มีเงื่อนไขในการรักษาความปลอดภัยของข้อมูล คือ

1. ค่าคีย์ที่ใช้ต้องเป็นค่าที่ได้จากการสุ่มอย่างแท้จริง

2. ค่าคีย์จะสามารถนำมาใช้ได้เพียงครั้งเดียว เมื่อต้องการเข้ารหัสข้อมูลใหม่ จะต้องทำการสุ่มค่าคีย์ขึ้นมาใหม่อีก

3. ความยาวของคีย์ต้องเท่ากับความยาวของข้อมูล plaintext ที่จะนำมาทำการเข้ารหัส

จากเงื่อนไขข้อแรกที่กล่าวว่าค่าคีย์ที่นำมาใช้ในการเข้ารหัสข้อมูลต้องเป็นค่าที่ได้จากการสุ่มอย่างแท้จริง การเข้ารหัสแบบ Vernam Cipher จึงเหมาะที่จะนำมาใช้กับระบบการส่งค่าคีย์แบบควอนตัม เนื่องจากค่าคีย์ที่ได้จากการส่งในระบบควอนตัมนั้น เป็นคีย์ที่ได้จากการสุ่มอย่างแท้จริงโดยไม่สามารถคาดเดารูปแบบ (pattern) ของข้อมูลล่วงหน้าได้ [35] และสามารถสร้างคีย์จำนวนมากได้ในเวลารวดเร็วซึ่งตรงกับเงื่อนไขข้อ (2) และข้อ (3) ของ Vernam Cipher

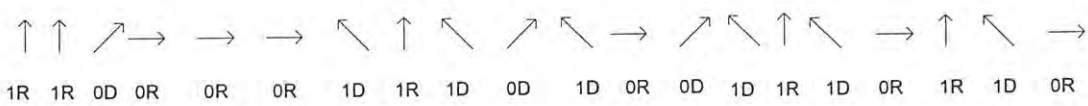
3.4 ตัวอย่างระบบควอนตัมคริปโตกราฟฟีโดยใช้โปรโตคอล BB84

หัวข้อนี้เป็นการแสดงตัวอย่างการเข้ารหัสแบบควอนตัมคริปโตกราฟฟีโดยใช้โปรโตคอล BB84 โดยระบบแบ่งเป็น 2 กรณีคือ กรณีที่ไม่มีผู้แอบดักจับข้อมูล และกรณีที่มีผู้แอบดักจับข้อมูล

3.4.1 กรณีที่ไม่มีผู้แอบดักจับข้อมูล

1. กรณีระบบไม่มีความผิดพลาดจากสัญญาณรบกวน

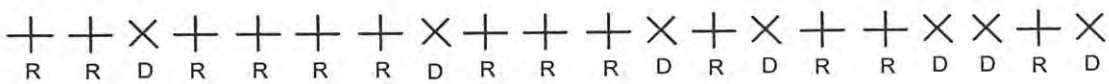
ขั้นตอนแรกของโปรโตคอล BB84 คือผู้ส่งทำการสุ่มเลือกทิศการโพลาไรซ์ของ โฟตอนให้แต่ละบิตข้อมูลแล้วส่งไปให้ผู้รับ โดยเลือกจาก 1 ใน 4 ของทิศการโพลาไรซ์ (0, 45, 90, 135 องศา) ความน่าจะเป็นในการสุ่มโฟตอนทั้ง 4 ทิศมีค่าเท่ากัน รูปที่ 3.8 แสดงทิศการโพลาไรซ์ของโฟตอนที่สุ่มขึ้นมาจำนวน 20 บิต โดยใช้สัญลักษณ์ทิศของลูกศรแทนทิศการโพลาไรซ์ตามที่กำหนดไว้ในรูปที่ 3.3 ภายใต้สัญลักษณ์มีค่าบิตข้อมูลกำกับว่าเป็น 0 หรือ 1



รูปที่ 3.8 ทิศการโพลาไรซ์ของโฟตอนที่ถูกสุ่มขึ้นมาจำนวน 20 บิต

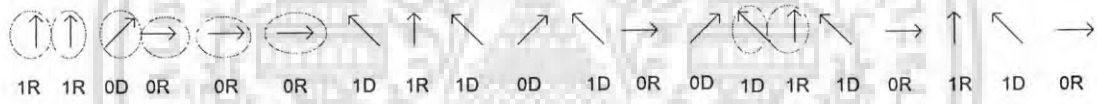
ขั้นตอนถัดมาคือ ผู้รับทำการสุ่มค่าเบสิสที่ใช้วัด โดยเลือกว่าจะวัดโฟตอนแต่ละตัวด้วย Rectilinear หรือ Diagonal ซึ่งความน่าจะเป็นในการสุ่มเบสิสทั้ง 2 มีค่าเท่ากัน รูปที่ 3.9 แสดง

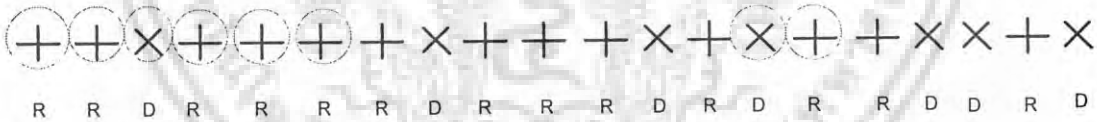
เบสิสที่ใช้วัดโฟตอนที่ผู้รับสุ่มขึ้นมาจำนวน 20 เบสิส โดยใช้สัญลักษณ์ + และ x แทนชนิดของเบสิส Rectilinear และ Diagonal ตามลำดับ ภายใต้สัญลักษณ์มีอักษร R แทนเบสิส Rectilinear และอักษร D แทนเบสิส Diagonal ดังที่กำหนดไว้ในรูปที่ 3.4 และ 3.5



รูปที่ 3.9 ทิศของเบสิสที่ถูกผู้รับสุ่มขึ้นมาวัดโฟตอนจำนวน 20 บิต

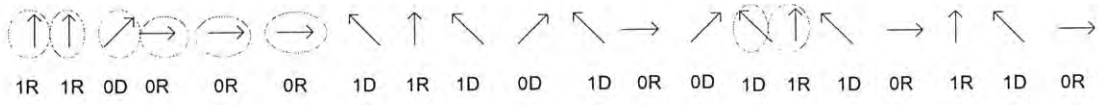
ขั้นตอนถัดมา ผู้รับจะทำการวัดค่าโฟตอนที่ส่งมา แล้วบันทึกผลการวัดที่ได้ โดยหลักการวัดโฟตอนเป็นไปตามรูปที่ 3.4 และ 3.5 กล่าวคือ การวัดค่าโฟตอนโดยใช้เบสิสที่ตรงกัน ค่าที่ได้จะถูกต้อง100 % และการวัดค่าโฟตอนโดยใช้เบสิสที่ไม่ตรงกัน ค่าที่ได้จะเป็นค่าสุ่มโดยมีโอกาสถูกและผิดเท่ากัน รูปที่ 3.10 แสดงการวัดโฟตอน โดยส่วนที่มีวงกลมล้อมรอบแสดงถึงโฟตอนและ เบสิสที่ตรงกัน





รูปที่ 3.10 การวัดโฟตอน

ผลที่วัดได้แสดงดังรูปที่ 3.11 ส่วนที่มีวงกลมล้อมรอบแสดงถึงโฟตอนที่วัดได้ถูกต้อง



รูปที่ 3.11 ผลของโฟตอนที่วัดได้

ในขั้นตอนถัดมา ผู้รับข้อมูลบอกเบสิสที่สุ่มขึ้นมาใช้ในการวัดโฟตอนแต่ละตัวให้แก่ผู้ส่งทางช่องสัญญาณสาธารณะ และผู้ส่งจะส่งข้อความตอบผู้รับว่าเบสิสใดบ้างที่ถูกต้องตรงกับโฟตอนที่ส่งไป เมื่อถึงขั้นตอนนี้ ทั้งผู้รับและผู้ส่งสามารถรู้ได้ว่าโฟตอนที่ตำแหน่งใดที่มีผลการวัดที่ถูกต้อง เนื่องจากรู้ตำแหน่งที่มีการใช้เบสิสที่ตรงกัน ทั้งผู้ส่งและผู้รับทำการทิ้งค่าคีย์ที่ใช้เบสิสในการวัดไม่ตรงกันและเก็บเฉพาะคีย์ที่ใช้เบสิสที่ตรงกัน เนื่องจากการยกตัวอย่างในหัวข้อนี้เป็นกรณีที่ระบบไม่มีผู้บุกรุกและไม่มีความผิดพลาดจากฮาร์ดแวร์หรือสัญญาณรบกวน ดังนั้นทั้งผู้ส่งและผู้รับสามารถนำคีย์นั้นไปใช้เข้ารหัสข้อมูลได้เลย ค่าคีย์สุดท้ายที่ได้คือ 1 1 0 0 0 0 1 1 โดยคีย์ที่ได้มีจำนวนประมาณครึ่งหนึ่งของคีย์ที่สุ่มขึ้นมาทั้งหมด

2. กรณีระบบมีความผิดพลาดจากสัญญาณรบกวน

ในหัวข้อนี้เป็นการยกตัวอย่างระบบการเข้ารหัสแบบควอนตัมคริปโตกราฟฟี โดยใช้โปรโตคอล BB84 และเป็นกรณีที่ระบบที่มี Error หรือบิตที่ผิดพลาดที่เกิดขึ้นจากสัญญาณรบกวน โดยปกติแล้วหากการวัดค่าโฟตอนใช้เบสิสที่ตรงกันผลการวัดที่ได้จะถูกต้อง 100% แต่หากมีสัญญาณรบกวนในระบบอาจทำให้การวัดโฟตอนมีค่าผิดพลาดไปไม่ถูกต้อง 100% ในระบบที่มีการสร้างฮาร์ดแวร์จริงในปัจจุบันค่าบิตที่ผิดพลาดมีค่าประมาณ 3-5 % [32] ในหัวข้อนี้กำหนดให้จำนวนบิตทั้งหมดที่ส่งมี 100 บิต และความผิดพลาดที่เกิดมีค่าประมาณ 5%

ขั้นตอนแรกผู้ส่งทำการสุ่มเลือกทิศการโพลาไรซ์ของโฟตอนให้แต่ละบิตข้อมูลจำนวน 100 บิตแล้วส่งไปให้ผู้รับ รูปที่ 3.12 แสดงข้อมูลจำนวน 100 บิตที่ผู้ส่งสุ่มขึ้นมาโดยมีค่าของบิตข้อมูล (0 หรือ 1) และมีชนิดของเบสิสโฟตอนแทนด้วยอักษร R หรือ D กำกับไว้ในวงเล็บหมายถึง Rectilinear และ Diagonal

1(R)	1(R)	1(R)	1(R)	1(R)	0(R)	1(D)	1(D)	1(R)	0(D)
0(D)	1(R)	1(D)	0(D)	1(D)	0(R)	0(D)	0(R)	0(D)	1(D)
1(D)	0(D)	1(R)	0(D)	0(R)	0(R)	1(R)	1(D)	1(D)	1(D)
1(R)	0(D)	1(R)	0(D)	1(R)	1(R)	1(R)	1(R)	0(D)	1(D)
1(R)	1(D)	0(R)	0(R)	0(D)	0(R)	1(R)	1(D)	0(R)	0(R)
1(R)	1(D)	1(R)	0(D)	0(D)	0(D)	0(D)	1(R)	0(R)	0(R)
1(D)	0(D)	0(R)	0(R)	1(D)	0(R)	0(D)	1(R)	0(R)	1(R)
0(R)	0(R)	1(R)	1(R)	0(R)	0(D)	1(R)	1(R)	0(R)	0(R)
0(R)	0(R)	0(D)	1(R)	1(D)	0(R)	0(D)	0(D)	0(R)	1(R)
1(D)	0(R)	1(R)	1(D)	0(R)	0(D)	0(R)	0(D)	0(D)	1(D)

รูปที่ 3.12 ข้อมูลจำนวน 100 บิตที่ผู้ส่งสุ่มขึ้นมา

ต่อมาผู้รับทำการสุ่มค่าเบสิสที่ใช้วัดโฟตอน โดยใช้สัญลักษณ์ + และ x แทนชนิดของเบสิส Rectilinear และ Diagonal ตามลำดับ รูปที่ 3.13 แสดงเบสิสที่ใช้วัดโฟตอนที่ผู้รับสุ่มขึ้นมา จำนวน 100 เบสิส

+	+	x	x	+	+	+	+	+	x
x	+	+	x	x	x	+	x	+	x
x	+	+	x	x	x	+	+	+	+
+	+	x	x	x	x	+	x	x	x
+	x	x	x	x	+	+	+	x	+
+	x	x	+	+	x	+	x	x	x
+	+	+	x	x	+	+	x	+	+
+	+	x	+	x	+	x	+	x	+
x	x	+	x	+	+	+	x	+	+
x	+	+	+	x	x	x	x	+	+

รูปที่ 3.13 เบสิสจำนวน 100 เบสิสที่ผู้รับสุ่มขึ้นมา

ขั้นตอนถัดมาผู้รับจะทำการวัดค่าโฟตอนที่ส่งมา แล้วบันทึกผลการวัดที่ได้ รูปที่ 3.14 แสดงผลการวัดโฟตอน โดยบิตที่ขีดเส้นใต้แสดงถึงโฟตอนที่วัดโดยเบสิสที่ตรงกันและบิตที่มีวงกลมล้อมรอบคือบิตที่มีการวัดข้อมูลผิดพลาด

1(R)	1(R)	1(D)	0(D)	1(R)	0(R)	0(R)	1(R)	1(R)	0(D)
0(D)	1(R)	1(R)	0(D)	1(D)	1(D)	1(D)	1(D)	0(R)	1(D)
1(D)	1(R)	1(R)	0(D)	0(D)	1(D)	1(R)	0(R)	1(R)	0(R)
1(R)	0(R)	0(D)	0(D)	1(D)	0(D)	1(R)	1(D)	0(D)	1(D)
1(R)	1(D)	1(D)	0(D)	0(D)	0(R)	1(R)	0(R)	0(D)	0(R)
1(R)	1(D)	0(D)	0(R)	1(R)	1(R)	0(R)	0(D)	0(D)	1(D)
0(R)	0(R)	0(R)	1(D)	1(D)	0(R)	0(R)	0(D)	0(R)	1(R)
0(R)	0(R)	1(D)	1(R)	0(D)	0(R)	1(D)	0(D)	0(D)	0(R)
0(D)	0(D)	0(R)	1(D)	1(R)	0(R)	0(R)	0(D)	0(R)	1(R)
1(D)	0(R)	1(R)	1(R)	0(D)	0(D)	0(D)	0(D)	0(R)	1(R)

รูปที่ 3.14 ผลการวัดโฟตอนในกรณีที่มีสัญญาณรบกวน

ในขั้นตอนถัดมา ทั้งผู้ส่งและผู้รับทำการทิ้งค่าคีย์ที่ใช้เบสิสในการวัดไม่ตรงกันและเก็บเฉพาะคีย์ที่ใช้เบสิสที่ตรงกัน ซึ่งจะได้ค่าคีย์จำนวน 48 บิตดังนี้

1(R)	1(R)	1(R)	0(R)	1(R)	0(D)	0(D)	1(R)
0(D)	1(D)	1(D)	1(D)	1(R)	0(D)	1(R)	1(R)
0(D)	1(R)	0(D)	1(D)	1(R)	1(D)	0(D)	0(R)
1(R)	0(R)	1(R)	1(D)	1(R)	0(R)	1(D)	0(R)
0(R)	1(R)	0(R)	0(R)	1(R)	0(D)	0(R)	0(R)
0(D)	0(R)	1(R)	1(D)	0(R)	1(R)	0(D)	0(D)

รูปที่ 3.15 คีย์ที่ได้จากผลการวัดโฟตอน

ขั้นตอนถัดมาเป็นขั้นตอนการคำนวณค่า QBER ซึ่งใช้วิธีคำนวณตามสมการ 3.1

$$QBER = \frac{\text{Error Bit}}{\text{All Bit}} \times 100$$

$$QBER = \frac{2}{48} \times 100$$

$$QBER = 4.17 \quad \text{(เปอร์เซนต์)}$$

จากค่า QBER ที่คำนวณได้เท่ากับ 4.17% พบว่าค่า QBER มีค่าไม่เกินค่าความผิดพลาดที่ยอมรับได้ (5%) ดังนั้นผู้ส่งและผู้รับจึงแน่ใจได้ว่าไม่มีผู้บุกรุกในระบบ ขั้นตอนต่อมาคือการนำบิตผลลัพธ์ที่ได้มาทำการแก้ไขความผิดพลาด หลังจากแก้ไขความผิดพลาดแล้วคีย์ผลลัพธ์สุดท้ายจะเป็นคีย์ที่ถูกต้องทุกบิต สามารถนำไปทำการเข้ารหัสข้อมูลแบบ Vernam cipher ได้

จากรูปที่ 3.15 บิตผลลัพธ์ที่ได้คือ

11101001 01111011 01011100 10111010 01001000 00110100

จะเห็นว่ายังมีข้อมูล 2 บิตที่ผิดพลาดอยู่ เมื่อทำการแก้ไขความผิดพลาดด้วยกระบวนการเรียงสับเปลี่ยนแบบสุ่มแล้ว คีย์ผลลัพธ์ที่ได้คือ

1110100 0111101 0101110 1011010 0100100 0011010

จะเห็นว่าจำนวนคีย์ที่ได้จะลดลงจาก 48 บิต เหลือเพียง 42 บิต เนื่องจากกระบวนการเรียงสับเปลี่ยนแบบสุ่ม เมื่อเช็กค่าพาริตีบิตในแต่ละบล็อกของข้อมูลเสร็จแล้วต้องลบข้อมูลไป 1 ตัว เมื่อถึงขั้นตอนนี้คีย์ผลลัพธ์ที่ได้สามารถนำไปเข้ารหัสข้อมูลได้ ดังตัวอย่าง

ตัวอย่าง ขั้นตอนการเข้ารหัสแบบ Vernam cipher

Alice ต้องการส่งข้อมูลเป็นคำว่า HELLO ไปให้ Bob ดังรูปที่ 3.16

รูปที่ 3.16 Alice ต้องการส่งข้อมูลเป็นคำว่า HELLO ไปให้ Bob

1. นำคำว่า HELLO มาแปลงเป็นรหัส ASCII จะได้

H = 72 E = 69 L = 76 L = 76 O = 79

2. นำรหัส ASCII ที่ได้มาแปลงเป็นเลขฐานสอง

H = 0100 1000 E = 0100 0101 L = 0100 1100 L = 0100 1100 O = 0100 1111

จำนวนบิตทั้งหมดที่แทนคำว่า HELLO มีทั้งหมด 40 บิต ดังนั้นคีย์ที่ใช้ในการเข้ารหัสต้องมีทั้งหมด 40 บิตเช่นกัน เนื่องจากคีย์ผลลัพธ์ที่ได้มีทั้งหมด 42 บิต จึงต้องทำการตัด 2 บิตสุดท้ายออกเพื่อให้ได้จำนวนคีย์ 40 บิตเท่ากับจำนวนบิตข้อมูล

3. ทำการเข้ารหัสโดยกระบวนการ Exclusive Or ได้ดังรูปที่ 3.17

0100 1000 0100 0101 0100 1100 0100 1100 0100 1111	$\oplus$	บิตข้อมูล
1110 1000 1111 0101 0111 0101 1010 0100 1000 0110		คีย์
1010 0000 1011 0000 0011 1001 1110 1000 1100 1001		Cipher text

รูปที่ 3.17 การเข้ารหัสโดยกระบวนการ Exclusive Or

ข้อมูล 1010 0000 1011 0000 0011 1001 1110 1000 1100 1001 ที่ได้จากการเข้ารหัสเรียกว่า Cipher text

4. เมื่อได้ Cipher text แล้ว Alice จะส่ง Cipher text นี้ไปให้ Bob และ Bob จะทำการถอดรหัสโดยใช้คีย์ตัวเดียวกัน ดังนี้

1010 0000	1011 0000	0011 1001	1110 1000	1100 1001		Cipher text
1110 1000	1111 0101	0111 0101	1010 0100	1000 0110	$\oplus$	คีย์
0100 1000	0100 0101	0100 1100	0100 1100	0100 1111		บิตข้อมูล

รูปที่ 3.18 การถอดรหัสโดยกระบวนการ Exclusive Or

จะเห็นว่าบิตผลลัพธ์ที่ได้จากการถอดรหัสโดยใช้คีย์ตัวเดียวกัน จะมีค่าตรงกับบิตข้อมูลที่ Alice ต้องการส่ง

3.4.2 กรณีที่มีผู้แอบดักจับข้อมูล

ในหัวข้อนี้เป็นการยกตัวอย่างระบบการเข้ารหัสแบบควอนตัมคริปโตกราฟฟีกรณีที่มีผู้แอบดักจับข้อมูลระหว่างการส่งจากผู้ส่งไปยังผู้รับ ในการสุ่มข้อมูลของผู้ส่งขั้นตอนแรกจะใช้ข้อมูลชุดเดียวกับในหัวข้อ 3.4.1 ดังรูปที่ 3.16

1(R)	1(R)	1(R)	1(R)	1(R)	0(R)	1(D)	1(D)	1(R)	0(D)
0(D)	1(R)	1(D)	0(D)	1(D)	0(R)	0(D)	0(R)	0(D)	1(D)
1(D)	0(D)	1(R)	0(D)	0(R)	0(R)	1(R)	1(D)	1(D)	1(D)
1(R)	0(D)	1(R)	0(D)	1(R)	1(R)	1(R)	1(R)	0(D)	1(D)
1(R)	1(D)	0(R)	0(R)	0(D)	0(R)	1(R)	1(D)	0(R)	0(R)
1(R)	1(D)	1(R)	0(D)	0(D)	0(D)	0(D)	1(R)	0(R)	0(R)
1(D)	0(D)	0(R)	0(R)	1(D)	0(R)	0(D)	1(R)	0(R)	1(R)
0(R)	0(R)	1(R)	1(R)	0(R)	0(D)	1(R)	1(R)	0(R)	0(R)
0(R)	0(R)	0(D)	1(R)	1(D)	0(R)	0(D)	0(D)	0(R)	1(R)
1(D)	0(R)	1(R)	1(D)	0(R)	0(D)	0(R)	0(D)	0(D)	1(D)

รูปที่ 3.19 ข้อมูลจำนวน 100 บิตที่ผู้ส่งสุ่มขึ้นมา

หากมีบุคคลที่สามแอบเข้ามาวัดข้อมูลโดยใช้เบสิสดังรูปที่ 3.17

+	+	x	x	+	+	+	+	+	x
x	+	+	x	x	x	+	x	+	x
x	+	+	x	x	x	+	+	+	+
+	+	x	x	x	x	+	x	x	x
+	x	x	x	x	+	+	+	x	+
+	x	x	+	+	x	+	x	x	x
+	+	+	x	x	+	+	x	+	+
+	+	x	+	x	+	x	+	x	+
x	x	+	x	+	+	+	x	+	+
x	+	+	+	x	x	x	x	+	+

รูปที่ 3.20 เบสิสจำนวน 100 เบสิสที่ผู้บุกรุกสุ่มขึ้นมาเพื่อแอบวัดข้อมูล

ข้อมูลที่ถูกผู้บุกรุกวัดจะเปลี่ยนไปก่อนที่จะถึงผู้รับ ดังรูปที่ 3.18

1(R)	1(R)	1(D)	0(D)	1(R)	0(R)	0(R)	1(R)	1(R)	0(D)
0(D)	1(R)	1(R)	0(D)	1(D)	1(D)	1(R)	1(D)	0(R)	1(D)
1(D)	1(R)	1(R)	0(D)	0(D)	1(D)	1(R)	0(R)	1(R)	0(R)
1(R)	0(R)	0(D)	0(D)	1(D)	0(D)	1(R)	1(D)	0(D)	1(D)
1(R)	1(D)	1(D)	0(D)	0(D)	0(R)	1(R)	0(R)	0(D)	0(R)
1(R)	1(D)	0(D)	0(R)	1(R)	0(D)	0(R)	0(D)	0(D)	1(D)
0(R)	0(R)	0(R)	1(D)	1(D)	0(R)	0(R)	0(D)	0(R)	1(R)
0(R)	0(R)	1(D)	1(R)	0(D)	0(R)	1(D)	1(R)	0(D)	0(R)
0(D)	0(D)	0(R)	1(D)	1(R)	0(R)	0(R)	0(D)	0(R)	1(R)
1(D)	0(R)	1(R)	1(R)	0(D)	0(D)	0(D)	0(D)	0(R)	1(R)

รูปที่ 3.21 ผลการวัดโฟตอนของผู้บุกรุก

เมื่อผู้บุกรุกทำการวัดโฟตอน ข้อมูลที่เปลี่ยนไปจะไม่สามารถกลับไปเป็นข้อมูลเดิมได้ เนื่องจากการเปลี่ยนไปของการวัดโฟตอนเป็นแบบย้อนกลับไม่ได้ (Irreversible) และข้อมูลที่เปลี่ยนไปนี้จะถูกส่งไปยังผู้รับ รูปที่ 3.19 แสดงเบสิสที่ผู้ส่งสุ่มขึ้นมาเพื่อวัดข้อมูล

x	+	x	+	x	x	+	+	x	+
x	x	x	x	+	+	x	x	+	x
+	+	x	+	+	+	+	x	+	+
+	x	+	x	+	+	x	x	+	x
x	+	x	+	x	x	x	+	+	+
+	x	+	x	+	x	+	x	x	x
+	x	x	x	x	x	+	+	+	x
x	+	x	x	+	x	x	+	x	x
x	x	x	x	+	x	+	+	x	x
+	+	x	+	+	x	+	+	+	x

รูปที่ 3.22 เบสิสจำนวน 100 เบสิสที่ผู้รับสุ่มขึ้นมา

ผลการวัดโฟตอนแสดงดังรูปที่ 3.20

0(D)	1(R)	1(D)	0(R)	0(D)	1(D)	0(R)	1(R)	0(D)	0(R)
0(D)	0(D)	1(D)	0(D)	0(R)	1(R)	0(D)	1(D)	0(R)	1(D)
1(R)	1(R)	0(D)	0(R)	1(R)	1(R)	1(R)	1(D)	1(R)	0(R)
1(R)	0(D)	1(R)	0(D)	1(R)	1(R)	1(D)	1(D)	1(R)	1(D)
1(D)	0(R)	1(D)	0(R)	0(D)	1(D)	1(D)	0(R)	1(R)	0(R)
1(R)	1(D)	0(R)	1(D)	1(R)	0(D)	0(R)	0(D)	0(D)	1(D)
0(R)	0(D)	1(D)	1(D)	1(D)	0(D)	0(R)	1(R)	0(R)	1(D)
1(D)	0(R)	1(D)	1(D)	1(R)	0(D)	1(D)	1(R)	0(D)	1(D)
0(D)	0(D)	0(D)	1(D)	1(R)	1(D)	0(R)	0(R)	1(D)	1(D)
0(R)	0(R)	1(D)	1(R)	1(R)	0(D)	0(R)	1(R)	0(R)	1(D)

รูปที่ 3.23 ผลการวัดโฟตอนที่ผู้รับวัดได้

แต่ผลการวัดโฟตอนที่ถูกต้องหากไม่มีผู้บุกรุก จะได้ดังรูปที่ 3.21

1(R)	1(R)	1(R)	1(R)	1(R)	0(R)	1(D)	1(D)	1(R)	0(D)
0(D)	1(R)	1(D)	0(D)	1(D)	0(R)	0(D)	0(R)	0(D)	1(D)
1(D)	0(D)	1(R)	0(D)	0(R)	0(R)	1(R)	1(D)	1(D)	1(D)
1(R)	0(D)	1(R)	0(D)	1(R)	1(R)	1(R)	1(R)	0(D)	1(D)
1(R)	1(D)	0(R)	0(R)	0(D)	0(R)	1(R)	1(D)	0(R)	0(R)
1(R)	1(D)	1(R)	0(D)	0(D)	0(D)	0(D)	1(R)	0(R)	0(R)
1(D)	0(D)	0(R)	0(R)	1(D)	0(R)	0(D)	1(R)	0(R)	1(R)
0(R)	0(R)	1(R)	1(R)	0(R)	0(D)	1(R)	1(R)	0(R)	0(R)
0(R)	0(R)	0(D)	1(R)	1(D)	0(R)	0(D)	0(D)	0(R)	1(R)
1(D)	0(R)	1(R)	1(D)	0(R)	0(D)	0(R)	0(D)	0(D)	1(D)

รูปที่ 3.24 ผลการวัดโฟตอนหากไม่มีผู้บุกรุกในระบบ

หากนำรูปที่ 3.20 และ 3.21 มาเปรียบเทียบกัน จะเห็นว่าผลการวัดโฟตอนในกรณีที่มีผู้บุกรุกจะมีบิตผิดพลาดเกิดขึ้น ซึ่งบิตผิดพลาดแสดงดังรูปที่ 3.22

0(D)	1(R)	1(D)	0(R)	0(D)	1(D)	0(R)	1(R)	0(D)	0(R)
0(D)	0(D)	1(D)	0(D)	0(R)	1(R)	0(D)	1(D)	0(R)	1(D)
1(R)	1(R)	0(D)	0(R)	1(R)	1(R)	1(R)	1(D)	1(R)	0(R)
1(R)	0(D)	1(R)	0(D)	1(R)	1(R)	1(D)	1(D)	1(R)	1(D)
1(D)	0(R)	1(D)	0(R)	0(D)	1(D)	1(D)	0(R)	1(R)	0(R)
1(R)	1(D)	0(R)	1(D)	1(R)	0(D)	0(R)	0(D)	0(D)	1(D)
0(R)	0(D)	1(D)	1(D)	1(D)	0(D)	0(R)	1(R)	0(R)	1(D)
1(D)	0(R)	1(D)	1(D)	1(R)	0(D)	1(D)	1(R)	0(D)	1(D)
0(D)	0(D)	0(D)	1(D)	1(R)	1(D)	0(R)	0(R)	1(D)	1(D)
0(R)	0(R)	1(D)	1(R)	1(R)	0(D)	0(R)	1(R)	0(R)	1(D)

รูปที่ 3.25 ผลการวัดโฟตอนกรณีที่มีผู้บุกรุกโดยบิตที่ผิดพลาดคือบิตที่ขีดเส้นใต้

หากนำจำนวนบิตที่ผิดพลาดมาคำนวณค่า QBER จะได้

$$QBER = \frac{9}{42} \times 100$$

$$QBER = 21.43 \quad \text{(เปอร์เซนต์)}$$

จากผลที่คำนวณได้พบว่าค่า QBER มีค่าเกินค่าความผิดพลาดที่ยอมรับได้ (5%) จากกระบวนการของโปรโตคอล BB84 หากค่า QBER มากกว่าค่า Error Threshold ผู้ส่งและผู้รับสามารถรู้ว่าในระบบมีผู้บุกรุกเข้ามาแอบวัดข้อมูล ระบบจะเริ่มทำการสุ่มข้อมูลตั้งแต่ขั้นตอนแรกทั้งหมด

3.5 สรุป

ในบทนี้ได้กล่าวถึงการเข้ารหัสแบบคริปโตกราฟฟีแบบดั้งเดิมซึ่งแบ่งได้เป็น 2 ประเภท คือ แบบสมมาตร ซึ่งใช้คีย์ค่าเดียวกันในการเข้ารหัสและถอดรหัส และแบบอสมมาตร หรือการเข้ารหัสคีย์สาธารณะ ซึ่งใช้คีย์ที่ต่างกันในการเข้ารหัสและถอดรหัส เรียกว่าคีย์สาธารณะและคีย์ส่วนตัวตามลำดับ โดยมีหลักการคือใช้ความยากในการคำนวณทางคณิตศาสตร์ของการแยกตัวประกอบเลขจำนวนเฉพาะที่มีขนาดใหญ่เพื่อรักษาความปลอดภัยของข้อมูล และในบทนี้ยังได้กล่าวถึงระบบการส่งค่าคีย์แบบควอนตัมคริปโตกราฟฟี ซึ่งเป็นการส่งค่าคีย์ที่อาศัยหลักความไม่แน่นอนทางควอนตัมฟิสิกส์มาช่วยในการรักษาความปลอดภัยของข้อมูล โดยได้กล่าวถึงหลักการพื้นฐานและขั้นตอนการทำงานของโปรโตคอล BB84 ซึ่งเป็นโปรโตคอลแรกของระบบควอนตัมคริปโตกราฟฟีและเป็นโปรโตคอลที่นำมาวิเคราะห์เพื่อปรับปรุงประสิทธิภาพในวิทยานิพนธ์นี้ และได้ยกตัวอย่างการทำงานของโปรโตคอล BB84 และวิธีการคำนวณ QBER ในกรณีที่ไม่มีผู้บุกรุกและกรณีที่มีผู้บุกรุกในระบบ

ในบทต่อไปเป็นการกล่าวถึง การออกแบบโปรแกรมจำลองการทำงานและวิธีการวิเคราะห์และปรับปรุงประสิทธิภาพโปรโตคอล BB84 สำหรับระบบควอนตัมคริปโตกราฟฟี

บทที่ 4
การออกแบบโปรแกรมจำลองและโปรโตคอลสำหรับระบบควอนตัมคริปโตกราฟฟี

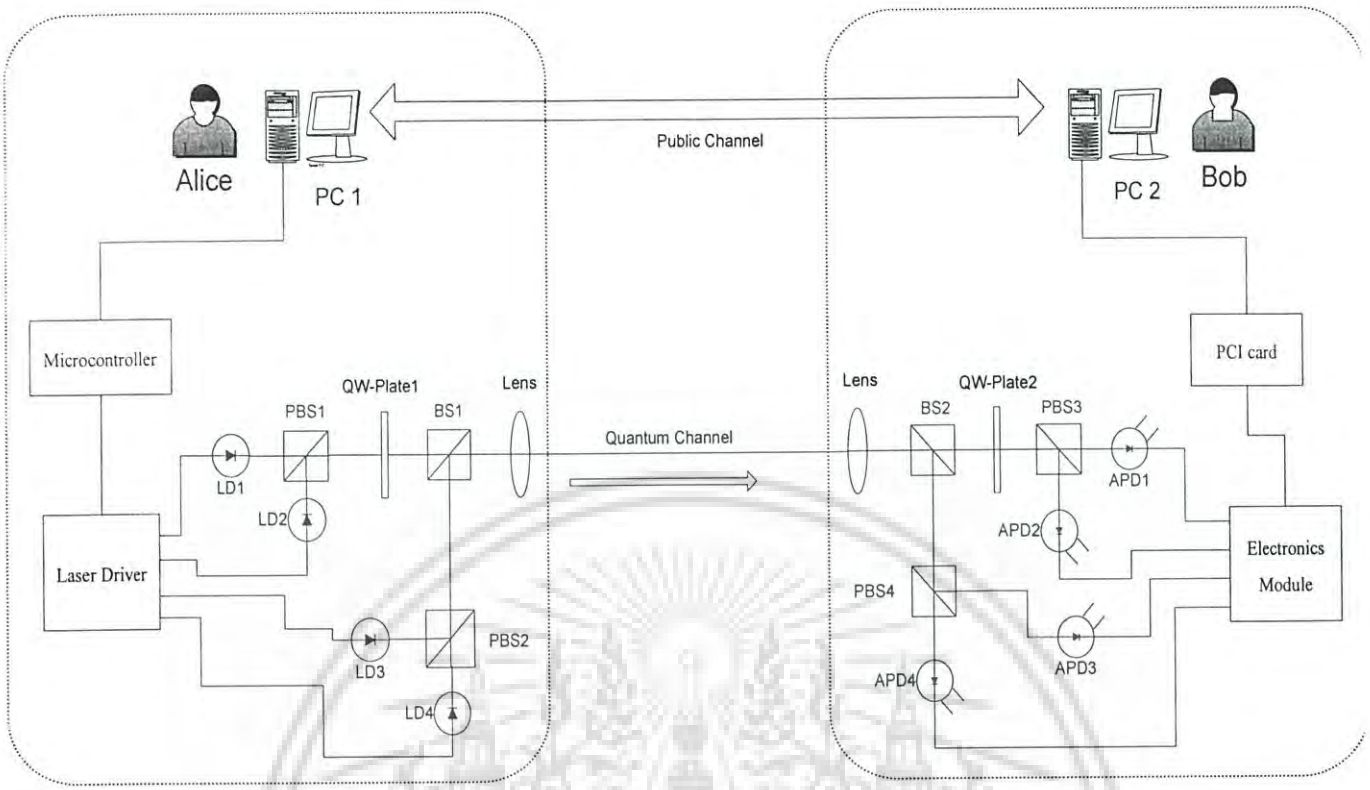
ในบทนี้เป็นการกล่าวถึงการออกแบบโปรแกรมคอมพิวเตอร์เพื่อจำลองระบบควอนตัมคริปโตกราฟฟีและโปรโตคอล BB84 เพื่อนำมาทดสอบวิธีที่นำเสนอในวิทยานิพนธ์ ในปัจจุบันมีการทดลองสร้างระบบฮาร์ดแวร์ของระบบควอนตัมคริปโตกราฟฟีในงานวิจัยหลายฉบับ [26-31] ระบบฮาร์ดแวร์ที่สามารถสร้างได้สำเร็จจริงในปัจจุบันแบ่งเป็น 2 ประเภท คือระบบที่ใช้สายสื่อสารชนิดเส้นใยแก้วนำแสง (Optical Fiber) [26, 27] และระบบแบบไร้สาย (Free Space) [28, 29] สำหรับการสร้างโปรแกรมจำลองในวิทยานิพนธ์นี้ จะอ้างอิงถึงระบบฮาร์ดแวร์ของควอนตัมคริปโตกราฟฟีที่ออกแบบและทดลองการส่งและรับโฟตอนจริงแบบไร้สาย โดยภาควิชาฟิสิกส์มหาวิทยาลัยเกษตรศาสตร์ [35] เนื่องจากสามารถหาข้อมูลเกี่ยวกับค่าพารามิเตอร์ต่าง ๆ ได้สะดวกมากกว่าการจำลองจากระบบของงานวิจัยอื่น

4.1 แนวคิดในการออกแบบโปรแกรมจำลองสำหรับระบบควอนตัมคริปโตกราฟฟี

ในการออกแบบโปรแกรมจำลองบนเครื่องคอมพิวเตอร์เพื่อให้ได้ผลการจำลองที่ใกล้เคียงกับผลที่ได้จากฮาร์ดแวร์ จำเป็นต้องทำความเข้าใจในส่วนประกอบของระบบฮาร์ดแวร์จริง ในหัวข้อนี้เป็นการอธิบายส่วนประกอบและการทำงานของระบบฮาร์ดแวร์ รวมถึงค่าพารามิเตอร์ต่าง ๆ ที่จำเป็นในการจำลองระบบ

4.1.1 ระบบฮาร์ดแวร์

รูปที่ 4.1 แสดงแผนภาพส่วนประกอบและการจัดวางอุปกรณ์ ของระบบฮาร์ดแวร์ควอนตัมคริปโตกราฟฟี ที่ออกแบบและทดลองโดยภาควิชาฟิสิกส์มหาวิทยาลัยเกษตรศาสตร์



รูปที่ 4.1 แผนภาพส่วนประกอบและการจัดวางอุปกรณ์ ของระบบฮาร์ดแวร์ควอนตัมคริปโตกราฟฟี

การทำงานของอุปกรณ์สามารถอธิบายในหัวข้อย่อยต่อไปนี้

4.1.1.1 **อุปกรณ์ในภาคส่ง**

1. PC 1 คือคอมพิวเตอร์ทางด้านส่ง ทำหน้าที่รับคำสั่งจากผู้ส่งและส่งไปยังไมโครคอนโทรลเลอร์เพื่อสั่งให้ตัวขับเลเซอร์ไดโอดขับไดโอดแต่ละตัวให้ทำงาน

2. LD คือเลเซอร์ไดโอด มี 4 ตัว

2.1. หากระบบสั่งให้ LD1 ทำงาน โฟตอนที่ออกจากภาคส่งจะอยู่ในสถานะโพลาไรซ์หมุนขวา (R) (เนื่องจากผ่านอุปกรณ์ PBS และ QW-Plate)

2.2. หากระบบสั่งให้ LD2 ทำงาน โฟตอนที่ออกจากภาคส่งจะอยู่ในสถานะโพลาไรซ์หมุนซ้าย (L)

2.3. หากระบบสั่งให้ LD3 ทำงาน+ โฟตอนที่ออกจากภาคส่งจะอยู่ในสถานะโพลาไรซ์แนวตั้ง (V)

2.4. หากระบบสั่งให้ LD4 ทำงานโฟตอนที่ออกจากภาคส่งจะอยู่ในสถานะโพลาไรซ์แนวนอน (H) โดยในขณะเวลาหนึ่งจะมีเลเซอร์ทำงานเพียงหนึ่งตัว เลเซอร์ทั้งสี่ตัวจะไม่ทำงานพร้อมกัน

3. PBS คือ Polarizing Beam Splitter มี 2 ตัว โดยอุปกรณ์ PBS ในภาคส่งนี้จะถูกจัดให้แสงที่เดินทางผ่านมีสถานะ H และแสงที่สะท้อน 90 องศา จะมีสถานะ V

4. QW-plate คือ Quarter Wave Plate เป็นอุปกรณ์ที่เปลี่ยนสถานะการโพลาไรซ์ของโฟตอน ในภาคส่งจะจัดให้อุปกรณ์เปลี่ยนแสงจากสถานะ H เป็น R และจากสถานะ V เป็น L

5. BS1 คือ Beam Splitter ทำหน้าที่แยกแสง โดยความเข้มแสงที่ผ่านจะสะท้อน 50% และพุ่งผ่าน 50% พัลส์โฟตอนเดี่ยวจะเลือกว่าจะสะท้อนหรือผ่านทางใดทางหนึ่ง โดยมีความน่าจะเป็นในการผ่าน 50% เท่ากัน

6. Lens คือ เลนส์ทำหน้าที่รวมแสง และส่งผ่านแสงจากภาคส่งออกไปยังช่องสัญญาณ

4.1.1.2 **อุปกรณ์ในภาครับ**

7. BS2 คือ Beam Splitter ทำหน้าที่เหมือนในภาคส่งคือแยกแสง โดยความเข้มแสงที่ผ่านจะสะท้อน 50% และพุ่งผ่าน 50% โฟตอนเดี่ยวจะเลือกว่าจะสะท้อนหรือผ่านทางใดทางหนึ่ง

8. QW-plate เปลี่ยนสถานะการโพลาไรซ์ของโฟตอน ในภาครับจะจัดให้อุปกรณ์เปลี่ยนแสงจากสถานะ R เป็น V และจากสถานะ L เป็น H

9. PBS ทำหน้าที่เหมือนในภาคส่ง

10. APD คือ อะวาลานซ์ โฟโตไดโอด (Avalanche Photodiode) มี 4 ตัว

10.1. APD1 ทำหน้าที่ตรวจจับโฟตอนที่อยู่ในสถานะ Left

10.2. APD2 ทำหน้าที่ตรวจจับโฟตอนที่อยู่ในสถานะ Right

10.3. APD3 ทำหน้าที่ตรวจจับโฟตอนที่อยู่ในสถานะ Vertical

10.4. APD4 ทำหน้าที่ตรวจจับโฟตอนที่อยู่ในสถานะ Horizontal

11. วงจรอิเลคทรอนิกส์ (Electronics module) ทำหน้าที่รับค่าการตรวจจับโฟตอนจาก APD แต่ละตัว นอกจากนั้นยังเป็นวงจรคูณความถี่ของสัญญาณ เพื่อสร้างสัญญาณนาฬิกาในการเทียบฐานเวลาระหว่างภาคส่งและภาครับ

12. PCI Card เป็นตัวรับข้อมูลเพื่อนำไปเก็บไว้ในเครื่องคอมพิวเตอร์

4.1.2 **ขั้นตอนการทำงานของระบบ**

จากรูปที่ 4.1

1. ผู้ส่งทำการเลือกค่าสถานะของโฟตอนผ่านทางคอมพิวเตอร์
2. ไมโครคอนโทรลเลอร์รับค่าจากคอมพิวเตอร์ เพื่อสั่งให้เลเซอร์ไดโอดแต่ละตัวทำงาน โดยที่

- หากต้องการให้สถานะของโฟตอนเป็น R (หมุนขวา) : ไมโครคอนโทรลเลอร์จะสั่งให้เลเซอร์ไดโอดตัวที่ 1 ทำงาน โดยปล่อยแสงผ่าน PBS ซึ่งแสงจะแยกออกเป็น 2 แนวคือ พุ่งผ่านและสะท้อน โดยหลักการแล้วแสงที่เดินทางผ่าน PBS จะมีสถานะเป็น H ส่วนแสงที่สะท้อนจะมีสถานะเป็น V ในกรณีนี้เราจะพิจารณาเฉพาะแสงที่พุ่งผ่าน PBS ดังนั้นเมื่อแสงผ่าน PBS แล้วจะมีสถานะโพลาไรซ์เป็น H และเมื่อผ่าน QW-plate จะได้แสงที่มีสถานะเป็นโพลาไรซ์หมุนขวา ต่อมาแสงเดินทางผ่าน BS เพื่อแยกแสงออกเป็น 2 แนว คือ เดินทางผ่านและสะท้อน ซึ่งในกรณีนี้เราจะพิจารณาเฉพาะแสงที่เดินทางผ่านโดยจะเดินทางต่อไปยังเลนส์เพื่อรวมแสงให้เป็นแนวเดียวกันและส่งผ่านทางช่องสัญญาณควอนตัม (Quantum channel)

เมื่อแสงถูกส่งไปถึงภาครับ จะมีเลนส์ทำหน้าที่รวมแสง เข้ามาสู่ beam splitter เพื่อแยกแสงออกเป็น 2 แนว คือ พุ่งผ่านและสะท้อน แต่โฟตอนเดี่ยวซึ่งเป็นอนุภาคนั้น จะเลือกเดินทางผ่านทางใดทางหนึ่ง โดยมีความน่าจะเป็นที่จะพุ่งผ่านเท่ากับ 50% และความน่าจะเป็นที่จะสะท้อนเท่ากับ 50% ซึ่งโฟตอนเดี่ยวที่พุ่งผ่าน BS นั้นขณะนี้อยู่ในสถานะโพลาไรซ์หมุนขวา เมื่อเดินทางผ่านไปยัง QW จะเปลี่ยนจากหมุนขวาเป็น V เมื่อโฟตอนที่มีสถานะเป็น V เดินทางผ่าน PBS ตัวที่ 3 แล้วจะสะท้อนไปยัง อะวาลานซ์โฟโตไดโอด APD/R

ในกรณีที่โฟตอนเดี่ยวสะท้อนจาก BS ตัวที่ 2จะลงไปยัง PBS ตัวที่ 4 โฟตอนอาจจะพุ่งผ่านไปยัง APD/H หรือสะท้อนไปยัง APD/V ซึ่งไม่มีหลักการตายตัวที่จะคาดเดาได้ว่าโฟตอนเดี่ยวจะพุ่งผ่านหรือสะท้อน แต่จากผลการทดลอง จำนวนโฟตอนที่สะท้อนไปยัง APD/V จะมากกว่าจำนวนโฟตอนที่พุ่งผ่านไปยัง APD/H

- หากต้องการให้สถานะของโฟตอนเป็น L (หมุนซ้าย) : ไมโครคอนโทรลเลอร์จะสั่งให้เลเซอร์ไดโอดตัวที่ 2 ทำงาน โดยปล่อยแสงผ่าน PBS แสงที่สะท้อนจาก PBS จะมีสถานะโพลาไรซ์เป็น V และเมื่อผ่าน QW จะได้แสงที่มีสถานะเป็นโพลาไรซ์หมุนซ้าย ต่อมาแสงเดินทางผ่าน BS เพื่อแยกแสงออกเป็น 2 แนว คือ เดินทางผ่านและสะท้อน โดยแสงที่เดินทางผ่านนั้น จะเดินทางต่อไปยังเลนส์เพื่อรวมแสงให้เป็นแนวเดียวกันและส่งผ่านทางช่องสัญญาณควอนตัม

เมื่อแสงถูกส่งไปถึงภาครับ จะมีเลนส์ทำหน้าที่รวมแสง เข้ามาสู่ BS เพื่อแยกแสงออกเป็น 2 แนว แสงซึ่งขณะนี้อยู่ในสถานะโพลาไรซ์หมุนซ้าย เมื่อเดินทางผ่านไปยัง QW จะเปลี่ยนจากหมุนซ้ายเป็น H ซึ่งเมื่อโฟตอนที่มีสถานะเป็น H เดินทางผ่าน PBS ตัวที่3 แล้วจะพุ่งผ่านไปยังอะวาลานซ์โฟโตไดโอด APD/L

ในกรณีที่โฟตอนเดี่ยวสะท้อนจาก BS ตัวที่ 2 จะลงไปยัง PBS ตัวที่ 4 โฟตอนอาจจะพุ่งผ่านไปยัง APD/H หรือสะท้อนไปยัง APD/V ซึ่งไม่มีหลักการตายตัวที่จะคาดเดาได้ว่าโฟตอนเดี่ยวจะพุ่งผ่านหรือสะท้อน แต่จากผลการทดลอง จำนวนโฟตอนที่สะท้อนไปยัง APD/V จะมากกว่าจำนวนโฟตอนที่พุ่งผ่านไปยัง APD/H

- หากต้องการให้สถานะของโฟตอนเป็น V (แนวตั้ง) : Microprocessor จะสั่งให้เลเซอร์ไดโอดตัวที่ 3 ทำงาน โดยปล่อยแสงผ่าน PBS แสงที่สะท้อนจาก PBS จะมีสถานะโพลาไรซ์เป็น V เสมอ ต่อมาแสงเดินทางผ่าน BS เพื่อแยกแสงออกเป็น 2 แนว คือ เดินทางผ่านและสะท้อน โดยแสงที่สะท้อนนั้น จะเดินทางต่อไปยังเลนส์เพื่อรวมแสงให้เป็นแนวเดียวกันและส่งผ่านทาง Quantum channel

เมื่อแสงถูกส่งไปถึงภาครับ จะมีเลนส์ทำหน้าที่รวมแสง เข้ามาสู่ BS เพื่อแยกแสงออกเป็น 2 แนว คือ พุ่งผ่านและสะท้อน แต่โฟตอนเดี่ยวซึ่งเป็นอนุภาคนั้น จะเลือกเดินทางผ่านทางใดทางหนึ่ง โดยมีความน่าจะเป็นที่จะพุ่งผ่านเท่ากับ 50% และความน่าจะเป็นที่จะสะท้อนเท่ากับ 50% ซึ่งหากแสงสะท้อน โฟตอนซึ่งขณะนี้อยู่ในสถานะโพลาไรซ์ V เดินทางผ่าน PBS ตัวที่ 4 แล้วจะสะท้อนไปยังอะวาลานซ์โฟโตไดโอด APD/V

ในกรณีที่โฟตอนเดี่ยวพุ่งผ่าน BS โฟตอนซึ่งในขณะนี้เป็นสถานะ V เมื่อผ่าน QW จะเปลี่ยนเป็นสถานะ L และเดินทางผ่าน PBS ซึ่งไม่มีหลักการตายตัวที่จะคาดเดาได้ว่าโฟตอนเดี่ยวจะพุ่งผ่านหรือสะท้อน แต่จากผลการทดลอง จำนวนโฟตอนที่สะท้อนไปยัง APD/R จะมากกว่าจำนวนโฟตอนที่พุ่งผ่านไปยัง APD/L

- หากต้องการให้สถานะของโฟตอนเป็น H (แนวนอน) : ไมโครคอนโทรลเลอร์จะสั่งให้เลเซอร์ไดโอดตัวที่ 4 ทำงาน โดยปล่อยแสงผ่าน PBS แสงที่พุ่งผ่าน PBS จะมีสถานะโพลาไรซ์เป็น H เสมอ ต่อมาแสงเดินทางผ่าน BS เพื่อแยกแสงออกเป็น 2 แนว คือ เดินทางผ่านและสะท้อน โดยแสงที่สะท้อนนั้น จะเดินทางต่อไปยังเลนส์เพื่อรวมแสงให้เป็นแนวเดียวกันและส่งผ่านทางช่องสัญญาณควอนตัม

เมื่อแสงถูกส่งไปถึงภาครับ จะมีเลนส์ทำหน้าที่รวมแสง เข้ามาสู่ BS เพื่อแยกแสงออกเป็น 2 แนว คือ พุ่งผ่านและสะท้อน หากสะท้อนแสงซึ่งขณะนี้อยู่ในสถานะโพลาไรซ์ H จะเดินทางผ่าน PBS ตัวที่ 4 แล้วพุ่งผ่านไปยังอะวาลานซ์โฟโตไดโอด APD/H

ในกรณีที่โฟตอนเดี่ยวพุ่งผ่าน BS โฟตอนซึ่งในขณะนี้เป็นสถานะ H เมื่อผ่าน QW จะเปลี่ยนเป็นสถานะ R และเดินทางผ่าน PBS ซึ่งไม่มีหลักการตายตัวที่จะคาดเดาได้ว่าโฟตอนเดี่ยวจะพุ่งผ่านหรือสะท้อน แต่จากผลการทดลอง จำนวนโฟตอนที่สะท้อนไปยัง APD/L จะมากกว่าจำนวนโฟตอนที่พุ่งผ่านไปยัง APD/R

3. ผู้รับ รับสัญญาณจาก ยังอะวาลานซ์โฟโตไดโอด แต่ละตัว และนำมาบันทึกในคอมพิวเตอร์

4. ผู้รับและผู้ส่ง ทำการเทียบบิตข้อมูล และแก้ไขความผิดพลาดในข้อมูลนั้น

4.1.3 **ระบบสัญญาณ**

เนื่องจากการส่งโฟตอนในระบบ Free-space เป็นแบบไม่ใช้สายสัญญาณ ดังนั้นจึงต้องมีการกำหนดฐานเวลา เพื่อให้ผู้รับสามารถรู้ได้ว่า ผู้ส่งจะส่งโฟตอนมาในเวลาใด สัญญาณที่เกี่ยวข้องในระบบมีดังนี้

1. สัญญาณนาฬิกา ความถี่ 1 เมกกะเฮิรตซ์ : สัญญาณนาฬิกาเป็นตัวกำหนดการส่งข้อมูล โดยที่ผู้รับจะเก็บเฉพาะข้อมูลที่ส่งมาในเวลาที่ตรงกับสัญญาณนาฬิกาเท่านั้น อย่างไรก็ตาม อุปกรณ์ที่ใช้ตรวจจับโฟตอน อาจมีสัญญาณผิดพลาด (Error) เกิดขึ้น โดยอาจเกิดจากสัญญาณกระแสไฟฟ้ารบกวนขณะมืด (dark current) ซึ่งสัญญาณผิดพลาดนี้จะเกิดแบบสุ่ม ดังนั้นสัญญาณผิดพลาดอาจเกิดตรงกับสัญญาณนาฬิกาหรือไม่ก็ได้ หากสัญญาณผิดพลาดนั้นเกิดขึ้นในเวลาเดียวกับฐานเวลาของสัญญาณนาฬิกาที่ผู้ส่งส่งไปอาจทำให้เกิดการตรวจจับโฟตอนขึ้นแม้ว่าในขณะนั้นไม่มีโฟตอนส่งมาจากผู้ส่ง ซึ่งเป็นสาเหตุของความผิดพลาดในการส่งค่าโฟตอนในระบบ (QBER)

2. สัญญาณฐานเวลา (Time-Base) : ผู้ส่งจะต้องส่งฐานเวลาเพื่อให้ผู้รับรู้ช่วงของเวลาที่จะส่งโฟตอน ฐานเวลาทำได้โดยการส่งสัญญาณแสงความเข้มสูงความกว้างพัลส์ 1 ไมโครวินาที และเว้นไป 25 ไมโครวินาทีจึงส่งสัญญาณแสงความเข้มสูงที่มีความกว้างพัลส์ 1 ไมโครวินาทีอีกครั้ง เมื่อผู้รับได้รับสัญญาณฐานเวลาแล้ว จะต้องนำฐานเวลานั้นมาทำการสร้างสัญญาณนาฬิกาโดยการนำสัญญาณจากอะวาลันซ์โฟโตไดโอด 3 ตัวคือ V, R และ L มาซ้อนทับกัน ได้เป็นความถี่ 40 กิโลเฮิร์ตซ์ และนำไปเข้าวงจรคูณความถี่ จะได้สัญญาณที่มีความถี่ 1 เมกกะเฮิร์ตซ์ เมื่อผู้ส่งและผู้รับมีสัญญาณนาฬิกาที่ตรงกันแล้ว จึงสามารถตรวจจับโฟตอนที่ผู้ส่งส่งมาได้อย่างแม่นยำ

3. สัญญาณข้อมูล : จากที่กล่าวมา ในการสร้างฐานเวลา ผู้ส่งจะต้องทำการส่งแสงที่มีความเข้มสูง 1 ไมโครวินาที ทุก ๆ 25 ไมโครวินาที ช่วง 25 ไมโครวินาทีที่เว้นไปนั้นผู้ส่งจะส่งสัญญาณแสงที่มีความเข้ม 0.08 โฟตอนต่อพัลส์ในระยะเวลาสั้น ๆ (2 นาโนวินาที) [36] ห่างกันทุก ๆ 1 ไมโครวินาที ซึ่งในการส่งโฟตอนในแต่ละช่วง 25 ไมโครวินาทีนี้ โฟตอนจะมีสถานะการโพลาไรซ์เดียวกัน เช่น โฟตอนเป็นสถานะ V ทุก ๆ พัลส์ที่ส่งไปในช่วง 25 ไมโครวินาทีนั้น และในช่วง 25 ไมโครวินาทีนั้น โอกาสที่จะเกิดโฟตอนเดี่ยว มีได้ตั้งแต่ไม่มีโฟตอนเกิดขึ้นเลยจนถึงเกิดขึ้นมากที่สุด 3 ตัว (จากการทดลองส่งจริง) ทั้งนี้เนื่องจากความเข้มแสงเท่ากับ 0.08 หมายถึง หากส่งสัญญาณแสงไป 100พัลส์ โอกาสที่จะตรวจพบโฟตอนจะเท่ากับประมาณ 8 ตัว

4. สัญญาณรบกวน สัญญาณรบกวนที่ทำให้เกิดบิตที่ผิดพลาดในระบบ มีดังนี้

4.1 สัญญาณกระแสไฟฟ้ารบกวนขณะมืด (Dark Current) สัญญาณรบกวนชนิดนี้เกิดขึ้นที่ตัวอะวาลานซ์โฟโตไดโอด เนื่องจากการเคลื่อนที่ของประจุไฟฟ้าผ่านรอยต่อพีเอ็น (PN) ในขณะที่ยังไม่มีการส่งโฟตอน ซึ่งสามารถแก้ปัญหานี้ได้โดยการ

4.1.1 เลือกค่าแรงดันไบแอสให้เหมาะสม เนื่องจากความไวในการตรวจจับโฟตอนขึ้นอยู่กับแรงดันไบแอสกลับทาง (Reverse Bias) ที่สูงกว่าแรงดันพังทลาย (Breakdown voltage) ของอะวาลานซ์โฟโตไดโอด แต่หากเลือกค่าแรงดันกลับทางที่ใช้สูงเกินไป จะทำให้เกิดความร้อนสูงในอะวาลันซ์โฟโตไดโอด ซึ่งทำให้เกิดสัญญาณรบกวนเพิ่มขึ้น

4.1.2 ทำการควบคุมและลดอุณหภูมิของอะวาลานซ์โฟโตไดโอดให้เหมาะสม ซึ่งในการทดลองนี้ ใช้อะวาลันซ์โฟโตไดโอด C30902S กำหนดอุณหภูมิไว้ที่ 14- องศาเซลเซียส หากอุณหภูมิของอะวาลันซ์โฟโตไดโอดมีค่าสูง จะมีผลทำให้สามารถตรวจจับโฟตอนเดี่ยวได้ดีมากขึ้น แต่ในขณะเดียวกันก็ทำให้เกิดสัญญาณรบกวนขณะมืดเพิ่มขึ้น

4.2 สัญญาณรบกวนจากภายนอก สามารถแก้ปัญหาโดยการ จำกัดแสงจากสิ่งแวดล้อมให้รบกวนระบบน้อยที่สุด (ทดลองในห้องมืด หรือออกแบบการวางอุปกรณ์อะวาลานซ์โฟโตไดโอดให้อยู่ในกล่องมืด)

4.1.4 ส่วนประกอบและไดอะแกรมแสดงโปรแกรมจำลอง

ในการออกแบบโปรแกรมคอมพิวเตอร์เพื่อจำลองระบบควอนตัมคริปโตกราฟฟีในวิทยานิพนธ์นี้ ได้มีการพิจารณาผลกระทบของสัญญาณรบกวนและค่าพารามิเตอร์ต่าง ๆ ดังนี้

4.1.4.1 ผลกระทบของสัญญาณรบกวนแบบปัวซอง (Poisson Noise)

สัญญาณรบกวนแบบปัวซองเป็นสัญญาณรบกวนที่มีอยู่ในแสงตามธรรมชาติ เมื่อมีการส่งแสงออกไป การกระจายของโฟตอนที่เกิดขึ้นจะมีลักษณะการกระจายแบบปัวซอง ซึ่งสามารถกำหนดการแจกแจงของจำนวนโฟตอนที่เกิดขึ้นได้จาก ค่าเฉลี่ย μ ในสมการที่ 4.1

$$P(\mu) = \frac{e^{-\mu}\mu^{x}}{x!} \tag{4.1}$$

โดยที่

P(n) คือ การแจกแจงปัวซอง

μ คือ ค่าเฉลี่ยของจำนวนครั้งของโฟตอนที่เกิดขึ้นในช่วงเวลาที่กำหนดช่วงหนึ่ง

x คือ 0,1,2, ...

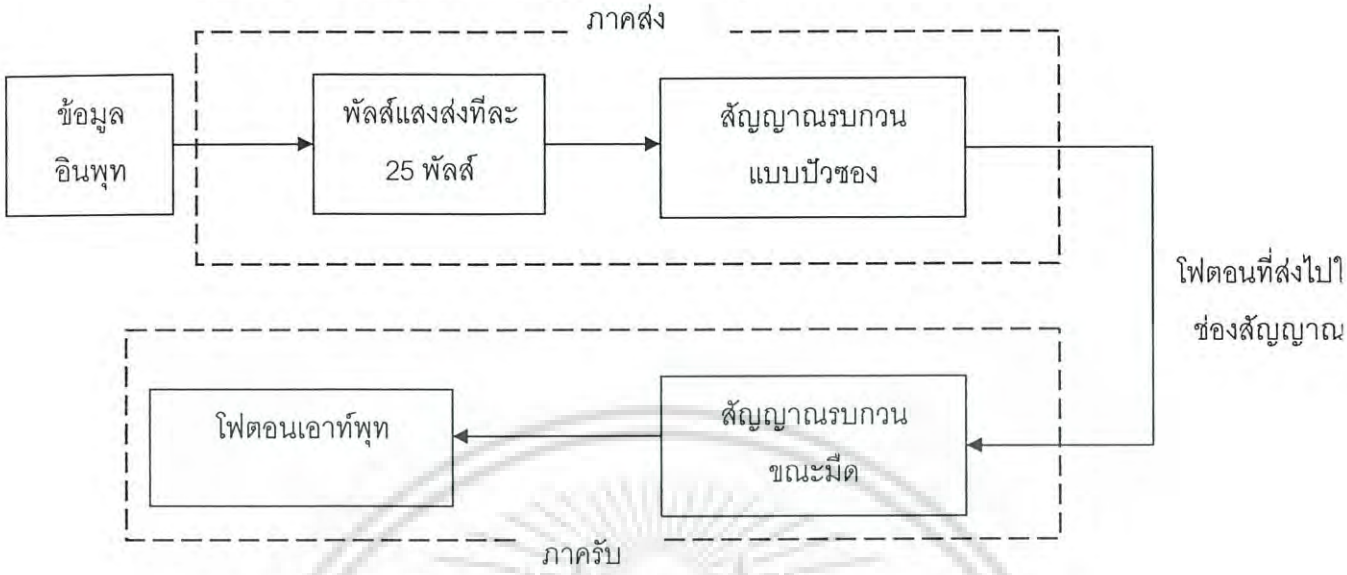
e คือ 2.71828

ในวิทยานิพนธ์นี้ได้ใช้ค่าเฉลี่ยในการเกิดโฟตอน μ ตามแบบของระบบฮาร์ดแวร์ที่นำมาจำลอง คือ 0.08 ซึ่งหมายถึงโอกาสที่จะเกิดโฟตอนมีประมาณ 8 ตัวหากส่งพัลส์แสงออกไป 100 พัลส์ ในการออกแบบโปรแกรมจำลองในโปรแกรม Matlab ได้ใช้ฟังก์ชันการกระจายแบบปัวซองในการสร้างจำนวนโฟตอนในภาคส่งโดยกำหนดตัวแปร μ เท่ากับ 0.08

4.1.4.2 ผลกระทบของสัญญาณรบกวนขณะมืด (Dark Count)

สัญญาณรบกวนขณะมืด เป็นสัญญาณรบกวนที่เกิดขึ้นที่ส่วนของของอะวาลานซ์โฟโตไดโอด เกิดขึ้นจากการเคลื่อนที่ของประจุไฟฟ้าผ่านรอยต่อ PN ขณะที่ยังไม่มีการตรวจจับโฟตอนมีสาเหตุมาจากการถูกกระตุ้นด้วยความร้อนและการปล่อยพาหะไฟฟ้าที่ถูกจับไว้ในหลุมดักพาหะซึ่งเป็นสาเหตุให้เกิดพัลส์ค้าง วิธีลดสัญญาณรบกวนขณะมืดทำได้โดยการเลือกค่าความต่างศักย์ไบแอสให้เหมาะสม และลดอุณหภูมิของอะวาลานซ์โฟโตไดโอด หากอุณหภูมิของอะวาลันซ์โฟโตไดโอดมีค่าสูงจะมีผลทำให้สามารถตรวจจับโฟตอนเดี่ยวได้ดีมากขึ้น แต่ในขณะเดียวกันก็ทำให้เกิดสัญญาณรบกวนขณะมืดเพิ่มขึ้น

ไดอะแกรมของโปรแกรมจำลองแสดงได้ดังรูปที่ 4.2



รูปที่ 4.2 แผนภาพขั้นตอนการทำงานของโปรแกรมจำลอง

4.2 วิธีการปรับปรุงประสิทธิภาพของโปรโตคอล BB84

การปรับปรุงประสิทธิภาพของโปรโตคอล BB84 ในวิทยานิพนธ์นี้ แบ่งออกเป็น 2 ขั้นตอนคือ

4.2.1 การปรับค่าความน่าจะเป็นในการเลือกเบสิส

จากขั้นตอนการทำงานของโปรโตคอล BB84 ในบทที่ 3 การสุ่มค่าโฟตอนในภาคส่งจะใช้ความน่าจะเป็นในการเลือกทิศการโพลาไรซ์ของโฟตอนระหว่าง Rectilinear Basis และ Diagonal Basis เท่ากับ 0.5 หรือ 50% ในขณะเดียวกันทางภาครับก็ต้องใช้ค่าความน่าจะเป็นในการเลือกเบสิส Rectilinear Basis และ Diagonal Basis เท่ากับ 0.5 หรือ 50% เช่นเดียวกัน การปรับปรุงประสิทธิภาพของโปรโตคอลในวิทยานิพนธ์นี้ คือการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนของผู้ส่ง และปรับค่าการสุ่มเบสิสที่ใช้วัดโฟตอนทางผู้รับ โดยการปรับค่านี้จะต้องใช้ค่าความน่าจะเป็นที่เท่ากันทั้งภาคส่งและภาครับ หากพิจารณาค่าความน่าจะเป็นในการสุ่มของโปรโตคอล BB84 แบบเดิมคือ Diagonal/Rectiliner เท่ากับ 50/50 แล้ว ค่าที่ปรับใหม่คือ ตั้งแต่ 60/40, 70/30, 80/20 และ 90/10 เพื่อเปรียบเทียบจำนวนคีย์ที่เก็บได้ในการปรับค่าแต่ละครั้ง สมมติฐานในการทดลองหลังจากปรับค่าความน่าจะเป็นคือ โอกาสของโฟตอนที่ส่งจากภาคส่งและตัววัดที่สุ่มจากภาครับจะมีเบสิสตรงกันมากขึ้น และจะมีผลดีคือระบบจะสามารถเก็บค่าคีย์ที่ใช้ได้มากขึ้น

4.2.2 การคำนวณความผิดพลาดแบบแบ่งแยก (Separated Error estimation)

เนื่องจากแนวคิดในการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนในภาคส่งและความน่าจะเป็นในการสุ่มเบสิสในภาครับดังที่ได้อธิบายในหัวข้อที่ 4.2.1 มีผลเสียคือหากมีผู้บุกรุกเข้ามาแอบวัดข้อมูลโดยใช้ค่าความน่าจะเป็นเดียวกันกับที่ผู้ส่งและผู้รับในระบบใช้ จะมีผลให้โอกาสในการคาดเดาเบสิสของโฟตอนในการวัดของผู้บุกรุกมีโอกาสถูกมากขึ้น และทำให้ระบบมีความปลอดภัยน้อยลง เนื่องจากหากใช้วิธีการคำนวณ QBER แบบเก่าจะทำให้ค่า QBER ลดลงจนใกล้ค่า Error Threshold มีผลให้ตรวจจับผู้บุกรุกได้ยากหรือไม่สามารถตรวจจับได้ ดังนั้นจึงได้มีการใช้วิธีการคำนวณความผิดพลาดแบบแบ่งแยก โดยมีวัตถุประสงค์คือ เพื่อให้ผู้ส่งและผู้รับสามารถตรวจจับผู้ที่เข้ามาแอบวัดค่าโฟตอนระหว่างทางของการส่งข้อมูลได้เหมือนเดิม วิธีการคำนวณทำได้โดยการแบ่งการคำนวณออกเป็น 2 ครั้ง คือ

1. QBER ของ Rectilinear Basis คำนวณได้จาก

$$\frac{\text{Error bit of Rectilinear}}{\text{All Rectilinear bit}} \times 100 \tag{4.2}$$

2. QBER ของ Diagonal Basis คำนวณได้จาก

$$\frac{\text{Error Bit of Diagonal}}{\text{All Diagonal Bit}} \times 100 \tag{4.3}$$

ค่า QBER ที่ได้จากการคำนวณทั้งสองครั้งจะถูกนำมาเปรียบเทียบกับค่า Error Threshold ของระบบ หากมีค่าใดค่าหนึ่งมากกว่าค่า Error Threshold เกินกว่าที่ยอมรับได้ จะตัดสินว่าระบบนั้นมีผู้บุกรุกเข้ามาแอบวัดข้อมูล

4.2.3 การปรับปรุงประสิทธิภาพของโปรโตคอล BB84ในระบบฮาร์ดแวร์จริง

การปรับปรุงประสิทธิภาพของระบบควอนตัมคริปโตกราฟฟีดังที่อธิบายในหัวข้อ 4.2.1 และ 4.2.2 นั้น หากนำมาปรับใช้กับระบบฮาร์ดแวร์จริง ต้องมีการเปลี่ยนในส่วนของฮาร์ดแวร์และในส่วนของโปรแกรมซอฟท์แวร์ที่ใช้ควบคุมทั้งในภาคส่งและภาครับ ดังนี้

4.2.3.1 การปรับค่าความน่าจะเป็นที่ภาคส่ง

ทำได้โดยการแก้ไขโปรแกรมซอฟท์แวร์ที่สั่งให้ผู้ส่งสุ่มเลือกค่าเบสิสจาก 50/50 เป็น 60/40, 70/30, 80/20 และ 90/10 และสั่งให้เลเซอร์ไดโอดแต่ละตัวทำงานตามค่าความน่าจะเป็นในการสุ่มที่ปรับไว้

4.2.3.2 การปรับค่าความน่าจะเป็นที่ภาครับ

ทำได้โดยการเปลี่ยนมุมของอุปกรณ์แยกแสง (Beams-plitter) ที่ภาครับ โดยค่าของโฟตอนที่ผ่านอุปกรณ์แยกแสง สามารถคำนวณได้จาก สมการ

$$I = I_0 \cos^2 \theta \tag{4.4}$$

โดยที่

I_0 คือ ความเข้มแสงก่อนผ่าน Beam-splitter

I คือ ความเข้มแสงหลังจากผ่าน Beam-splitter

θ คือ มุมระหว่างแนวทางเดินของแสงกับการจัดอุปกรณ์แยกแสง (Beam-splitter)

ในระบบฮาร์ดแวร์ที่ใช้โปรโตคอล BB84 แบบเดิมนั้น การจัดวางอุปกรณ์ได้กำหนดให้วางเอียงทำมุม 45 องศา ซึ่งหากแทนค่า θ เท่ากับ 45 องศา ในสมการที่ (4.4) จะได้ผลลัพธ์คือ

$$I = \frac{I_0}{2} \tag{4.5}$$

จะเห็นว่า ความเข้มแสงที่ผ่านอุปกรณ์แยกแสง จะมีค่าเป็นครึ่งหนึ่งของความเข้มแสงก่อนผ่านอุปกรณ์แยกแสง ซึ่งตรงกับโปรโตคอล BB84 แบบเดิมที่กำหนดให้มีการวัดโฟตอนด้วยความน่าจะเป็นแบบ 50/50 เท่ากัน

ดังนั้นในการปรับเปลี่ยนค่าความน่าจะเป็นในการวัดโฟตอนที่ภาครับให้เป็น 60/40, 70/30, 80/20 และ 90/10 สามารถทำได้โดยการคำนวณการเปลี่ยนค่ามุมของอุปกรณ์แยกแสง โดยใช้สมการที่ (4.4)

4.2.3.3 การคำนวณความผิดพลาดแบบแบ่งแยก

ทำได้โดยการแก้ไขโปรแกรมแบบเดิมให้ทำงานตามแบบหัวข้อ 4.2.2 ในส่วนของซอฟท์แวร์ที่ควบคุมการทำงานของภาครับ

4.3 สรุป

บทนี้กล่าวถึงแนวคิดการออกแบบโปรแกรมจำลองและโปรโตคอลสำหรับระบบควอนตัมคริปโตกราฟฟี และอธิบายส่วนประกอบการทำงานของระบบฮาร์ดแวร์ ระบบ รวมถึงแนวคิดในการปรับปรุงประสิทธิภาพของโปรโตคอล BB84 ทั้งในส่วนของทฤษฎี และการนำไปใช้กับระบบฮาร์ดแวร์จริง

บทที่ 5
ผลการจำลองและการวิเคราะห์ผลการจำลอง

เนื้อหาในบทนี้จะเป็นผลการทดลองของแนวคิดการปรับปรุงประสิทธิภาพของโปรโตคอล BB84 ที่ได้ออกแบบไว้ในบทที่ 4 โดยแบ่งออกเป็น 2 ส่วน คือ ผลการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนของเบสิส Rectilinear และ Diagonal ทั้งในภาคส่งและภาครับ และส่วนที่สองจะเป็นผลการเปลี่ยนวิธีการคำนวณอัตราความผิดพลาด QBER แบบแบ่งแยก (Separated Q-bit Error Rate Estimation)

5.1 ลำดับขั้นการทดลอง

หัวข้อนี้เป็นการอธิบายลำดับขั้นการทดลองการปรับปรุงประสิทธิภาพของระบบควอนตัมคริปโตกราฟฟี หากพิจารณาจากขั้นตอนการทำงานของโปรโตคอล BB84 แบบเดิม ในส่วนของการสุ่มค่าเบสิสของโฟตอนจะเป็น 50/50 ซึ่งในการทดลองได้มีการเปลี่ยนค่าความน่าจะเป็นในการสุ่ม Diagonal/Rectilinear เป็น 60/40, 70/30, 80/20 และ 90/10 เพื่อเปรียบเทียบผลในส่วนของจำนวนของคีย์ที่เก็บได้

นอกจากการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนแล้ว การปรับปรุงประสิทธิภาพของโปรโตคอล BB84 ได้รวมถึงการเปลี่ยนวิธีการคำนวณหาค่า QBER โดยใช้วิธีการคำนวณแบบแบ่งแยก (Separated QBER) และเปรียบเทียบผลที่ได้กับวิธีการคำนวณแบบเดิม

5.2 ผลการปรับค่าความน่าจะเป็นของเบสิสของโฟตอน

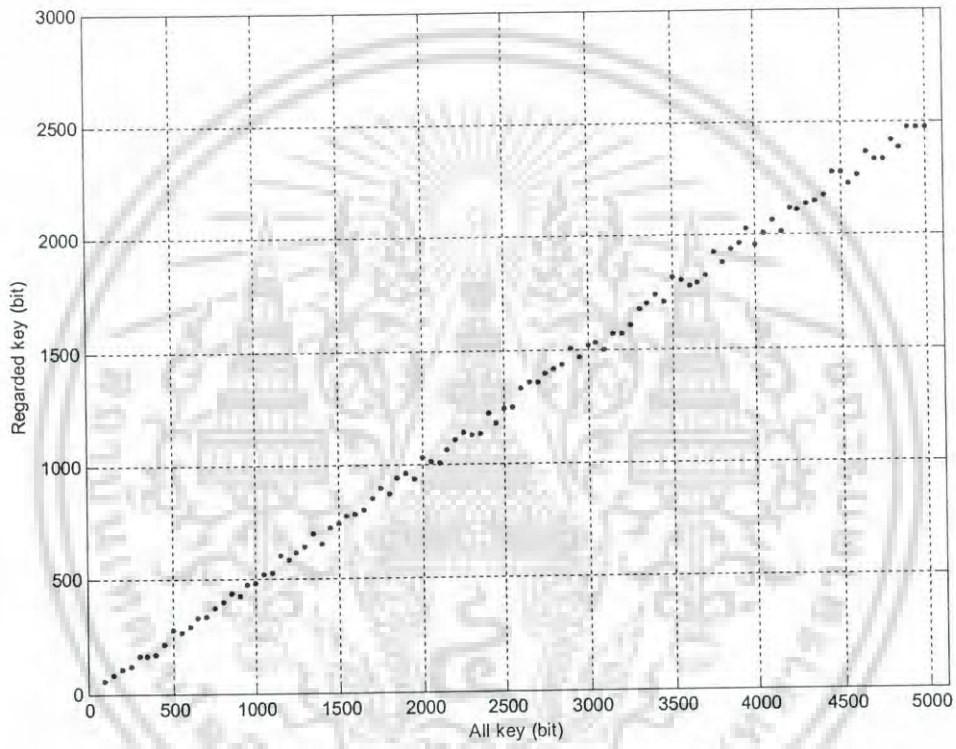
ในการปรับค่าความน่าจะเป็นในการสุ่ม จะทำการทดลอง 2 ส่วน โดยส่งค่าคีย์ทั้งหมดเป็น 2 ช่วง ได้แก่

- ช่วง 100 บิท จนถึง 5000 บิท โดยเพิ่มค่าคีย์ทีละ 50 บิท
- ช่วง 5000 บิท จนถึง 10000 บิท โดยเพิ่มค่าคีย์ทีละ 100 บิท

แล้วเปรียบเทียบผลการทดลองจากกราฟที่ได้ โดยเปรียบเทียบระหว่างค่าความน่าจะเป็นในการสุ่ม Diagonal/Rectilinear ที่ 60/40, 70/30, 80/20 และ 90/10

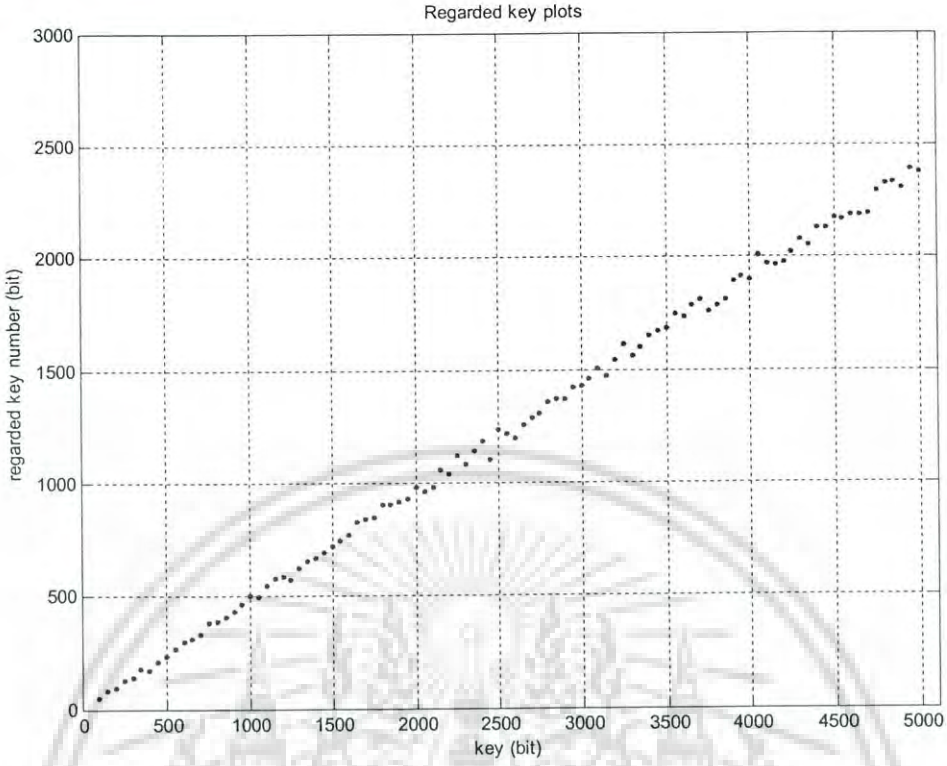
5.2.1 ผลการทดลองในแง่ของจำนวนคีย์ที่ต้องทิ้งไปเมื่อส่งข้อมูลในช่วง 100 บิท ถึง 5000 บิท

ในหัวข้อนี้ เป็นการจำลองการส่งคีย์จากภาคส่งไปยังภาครับและดูผลการทดลองในส่วนของจำนวนคีย์ที่ต้องทิ้งไป ในกรณีที่มีการปรับค่าความน่าจะเป็นจาก 50/50, 60/40, 70/30, 80/20 และ 90/10 และส่งข้อมูลในช่วง 100 บิท ถึง 5000 บิท และไม่มีผู้บุกรุกเข้ามาในระบบ ผลการทดลองการจำลองที่ความน่าจะเป็นเท่ากับ 50/50 แสดงดังรูปที่ 5.1



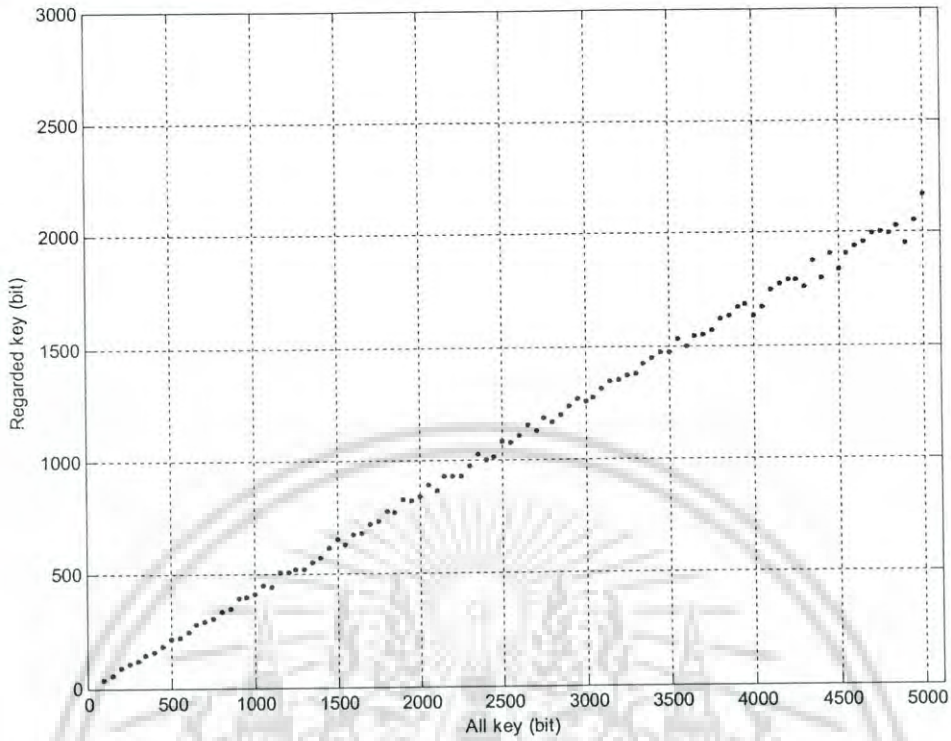
รูปที่ 5.1 ผลการจำลองเมื่อค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 50/50 ในช่วงการส่งค่าคีย์จำนวน 100 บิท ถึง 5000 บิท

รูปที่ 5.1 เป็นผลการจำลองระบบควอนตัมคริปโตกราฟฟีเมื่อไม่มีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear กล่าวคือเป็นโปรโตคอล BB84 แบบเดิม จากผลการจำลองจะเห็นว่า จำนวนคีย์ที่ต้องทิ้งไปมีค่าประมาณครึ่งหนึ่งของจำนวนคีย์ทั้งหมดที่ส่งไป เช่น หากส่งข้อมูลจำนวน 5000 บิทจะต้องทิ้งข้อมูลที่มีเบสิสไม่ตรงกันไปเป็นจำนวนประมาณ 2500 บิท ซึ่งหากทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 60/40 จะได้ผลดังรูปที่ 5.2



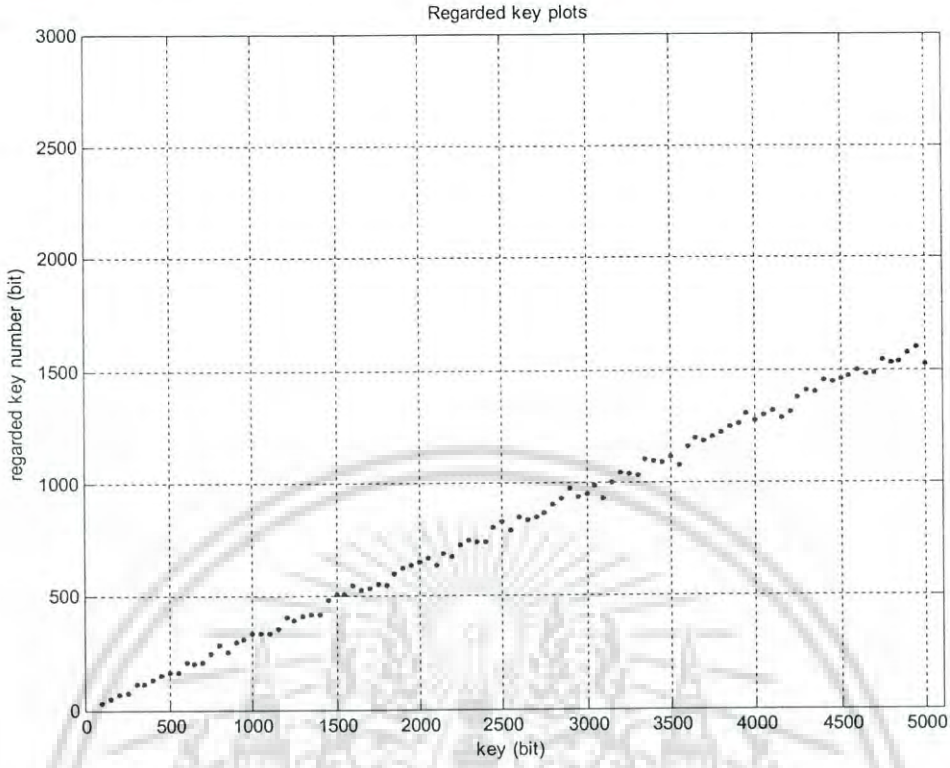
รูปที่ 5.2 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 60/40 ในช่วงการส่งค่าคีย์จำนวน 100 บิท ถึง 5000 บิท

รูปที่ 5.2 เป็นผลการจำลองระบบควอนตัมคริปโตกราฟฟีเมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 60/40 จากผลการจำลองจะเห็นว่าจำนวนคีย์ที่ต้องทิ้งไปมีค่าลดลงเมื่อเปรียบเทียบกับรูปที่ 5.1 ซึ่งเป็นโปรโตคอล BB84 แบบเดิม แต่ไม่ลดลงมากนัก โดยผลการทดลองจะเห็นชัดขึ้นหากการจำลองมีการเพิ่มบิทข้อมูลที่ส่งไปเป็นจำนวนมากขึ้น เช่นที่ 5000 บิท ข้อมูลที่ต้องทิ้งไปจะมีจำนวนประมาณ 2400 บิท ซึ่งถือว่าน้อยกว่าหากเทียบกับ รูปที่ 5.1 ซึ่งใช้ความน่าจะเป็น 50/50 ข้อมูลที่ต้องทิ้งไปจะมีจำนวนประมาณ 2500 บิท หากทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 70/30 จะได้ผลดังรูปที่ 5.3



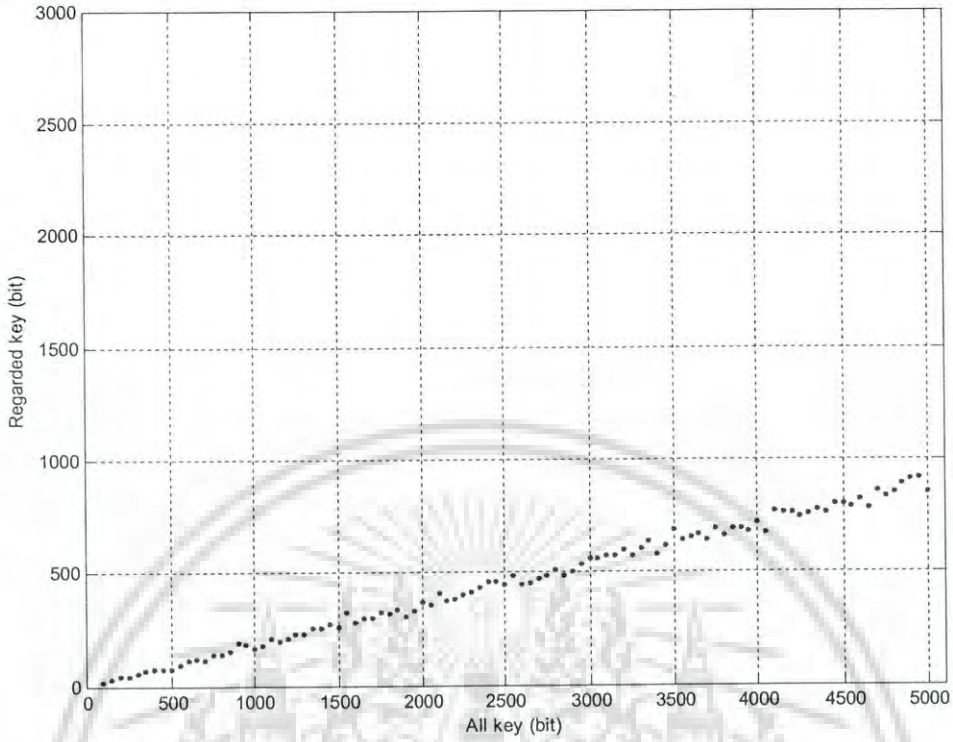
รูปที่ 5.3 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 70/30 ในช่วงการส่งค่าคีย์จำนวน 100 บิท ถึง 5000 บิท

รูปที่ 5.3 เป็นผลการจำลองระบบควอนตัมคริปโตกราฟฟีเมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 70/30 จากผลการจำลองจะเห็นว่าจำนวนคีย์ที่ต้องทิ้งไปมีค่าลดลงเมื่อเปรียบเทียบกับรูปที่ 5.1 ซึ่งเป็นโปรโตคอล BB84 แบบเดิม เช่น ในการส่งบิทจำนวน 5000 บิท ค่าคีย์ที่ต้องทิ้งไปมีประมาณ 2000 บิท หากทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 80/20 จะได้ผลดังรูปที่ 5.4



รูปที่ 5.4 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 80/20 ในช่วงการส่งค่าคีย์จำนวน 100 บิท ถึง 5000 บิท

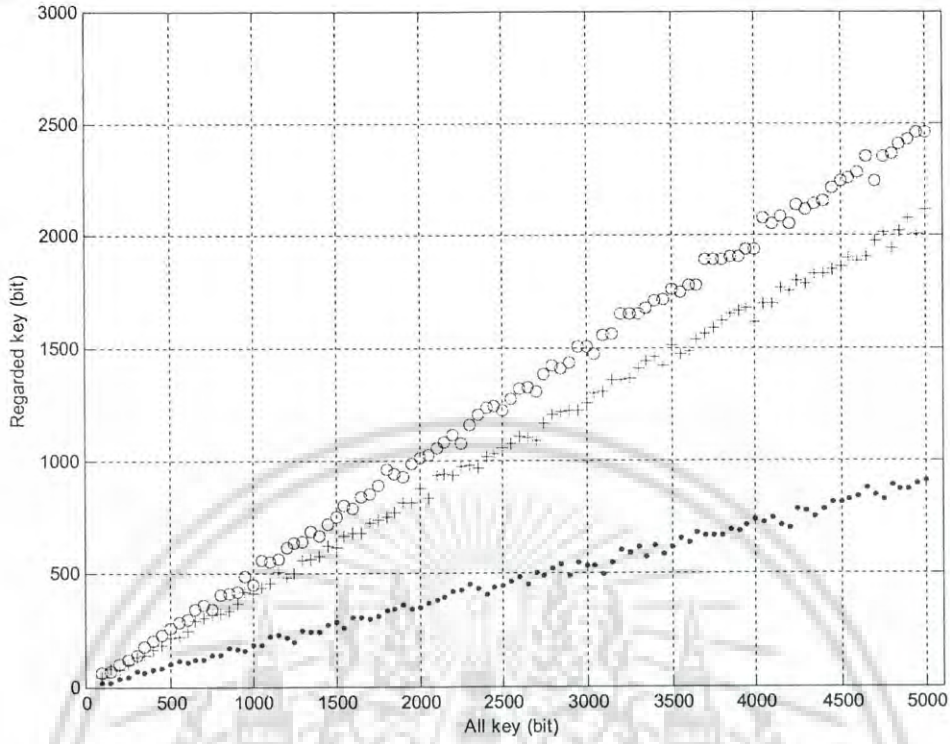
รูปที่ 5.4 เป็นผลการจำลองระบบควอนตัมคริปโตกราฟฟีเมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 80/20 จากผลการจำลองจะเห็นว่าจำนวนคีย์ที่ต้องทิ้งไปมีค่าลดลงเมื่อเปรียบเทียบกับรูปที่ 5.1 ซึ่งเป็นโปรโตคอล BB84 แบบเดิม และน้อยกว่ารูปที่ 5.2 และ 5.3 โดยในขณะที่ส่งข้อมูลไปจำนวน 5000 บิท จำนวนบิทที่ต้องทิ้งไปจะลดลงเหลือเพียงประมาณ 1500 บิท หากทำการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนและเบสิสในการวัดระหว่าง Diagonal/Rectilinear เป็น 90/10 จะได้ผลดังรูปที่ 5.5



รูปที่ 5.5 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 90/10 ในช่วงการส่งค่าคีย์จำนวน 100 บิท ถึง 5000 บิท

รูปที่ 5.3 เป็นผลการจำลองระบบควอนตัมคริปโตกราฟฟีเมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 90/10 จากผลการจำลองจะเห็นว่าจำนวนคีย์ที่ต้องทิ้งไปมีค่าลดลงเมื่อเปรียบเทียบกับรูปที่ 5.1 ซึ่งเป็นโปรโตคอล BB84 แบบเดิม และจำนวนคีย์ที่ต้องทิ้งไปมีค่าน้อยกว่าผลการทดลองในรูปที่ 5.2, 5.3 และ 5.4 โดยในกรณีที่ส่งคีย์ไป 5000 บิท จำนวนบิทที่ต้องทิ้งจะลดลงเหลือเพียงประมาณ 1000 บิท

หากนำกราฟผลการจำลองที่ได้จากการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนและเบสิส ในการวัด ระหว่าง Diagonal/Rectilinear เป็น 50/50, 70/30 และ 90/10 มาเปรียบเทียบในกราฟรูปเดียวกันจะได้ดังรูปที่ 5.6



รูปที่ 5.6 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 50/50, 70/30 และ 90/10 เปรียบเทียบกัน ในช่วงการส่งค่าคีย์จำนวน 100 บิท ถึง 5000 บิท

ooo แทนผลการจำลองของความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 50/50

+++ แทนผลการจำลองของความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 70/30

..... แทนผลการจำลองของความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 90/10

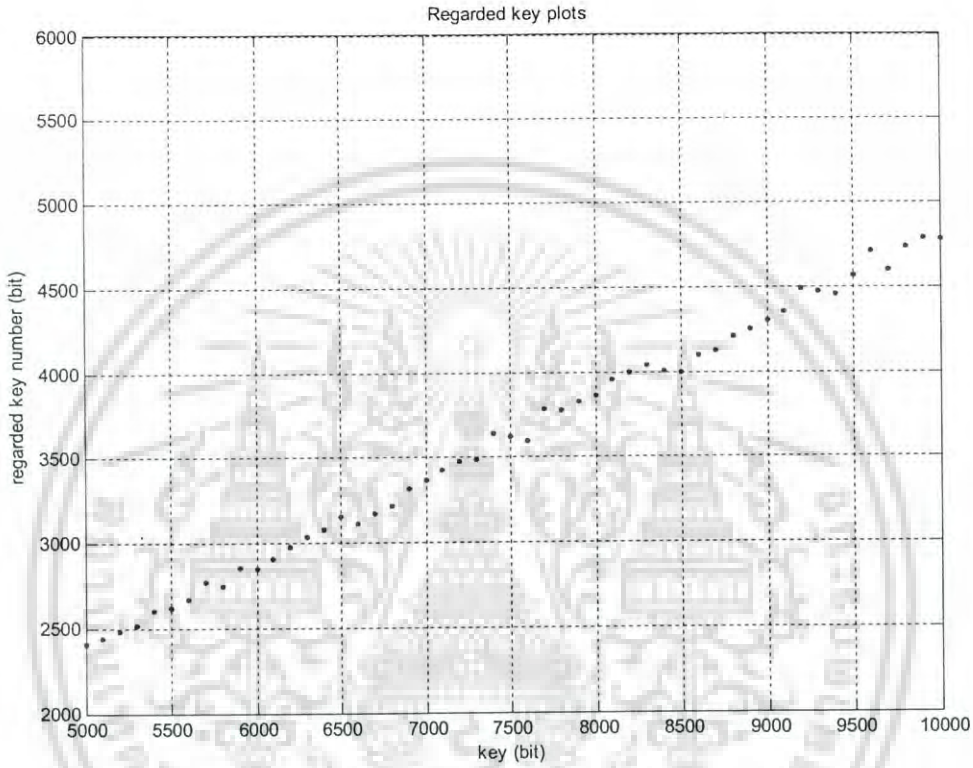
จากผลการทดลองการปรับค่าความน่าจะเป็นในการสุ่มเบสิสของโฟตอน จะเห็นว่า เมื่อทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 ไปยัง 60/40, 70/30, 80/20 และ 90/10 มีผลทำให้ระบบสามารถลดจำนวนคีย์ที่ต้องทิ้งไปได้ ซึ่งหมายความว่าระบบมีจำนวนคีย์ที่ใช้ได้เพิ่มมากขึ้น

5.2.2 ผลการทดลองในแง่ของจำนวนคีย์ที่ต้องทิ้งไปเมื่อส่งข้อมูลช่วง 5000 บิท จนถึง 10000 บิท

จากผลการทดลองในหัวข้อ 5.2.1 สรุปได้ว่าการปรับค่าความน่าจะเป็นในการส่งค่าคีย์จาก 50/50, 60/40, 70/30, 80/20 และ 90/10 และส่งข้อมูลในช่วง 100 บิท ถึง 5000 บิท มีผลทำให้ระบบสามารถลดค่าคีย์ที่ต้องทิ้งไปได้ ในหัวข้อนี้เป็นการจำลองการส่งค่าคีย์ในช่วงข้อมูลที่ต่าง

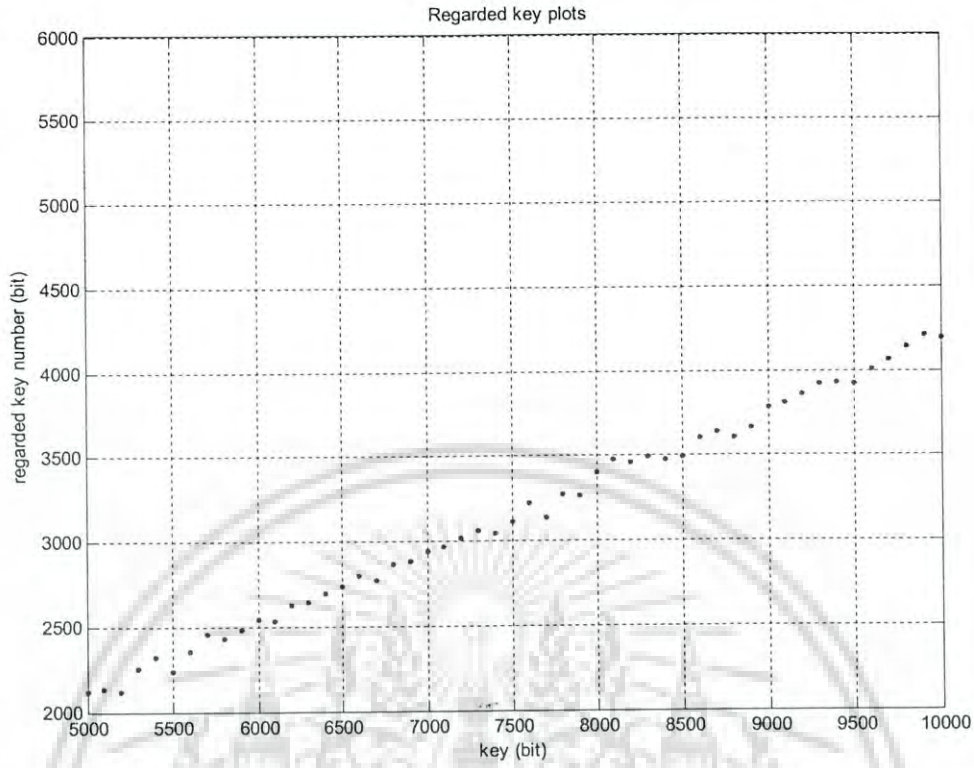
กับหัวข้อ 5.2.1 โดยเพิ่มช่วงข้อมูลจาก 100 บิท ถึง 5000 บิท เป็น 5000 บิท ถึง 10000 บิทและดูผลการจำลองว่ายังสามารถลดจำนวนคีย์ที่ต้องทิ้งไปได้หรือไม่

ผลการทดลองการจำลองที่ความน่าจะเป็น Diagonal/Rectilinear เท่ากับ 60/40 แสดงดังรูปที่ 5.7



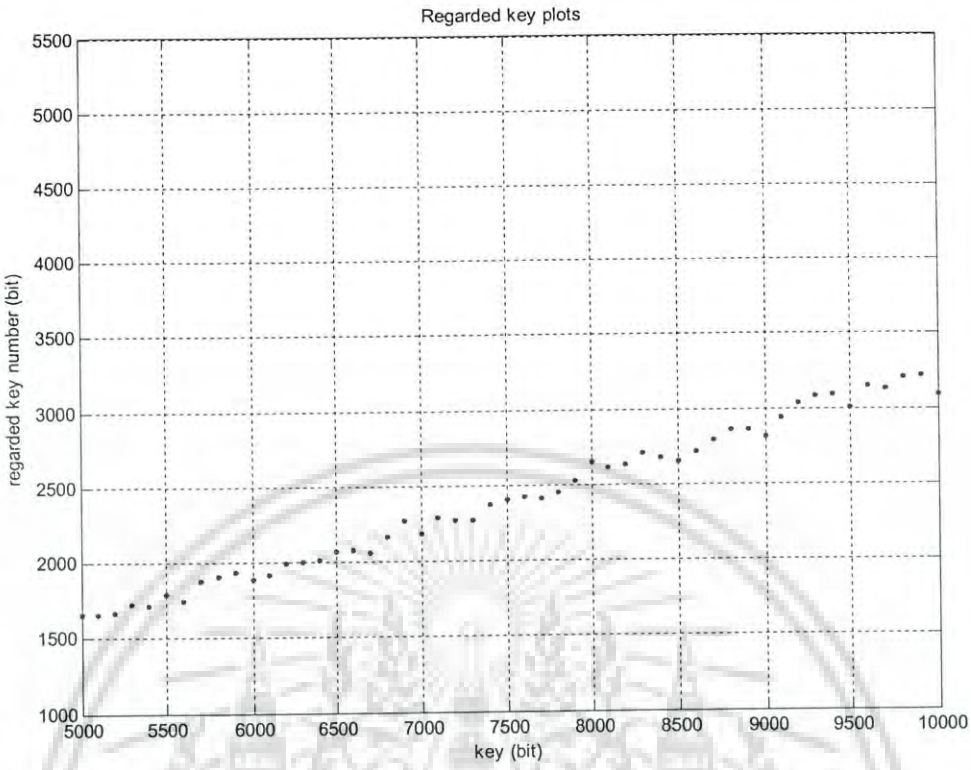
รูปที่ 5.7 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 60/40 ในช่วงการส่งค่าคีย์จำนวน 5000 บิท ถึง 10000 บิท

จากรูปที่ 5.7 การส่งข้อมูลจำนวน 10000 บิทจะมีจำนวนบิทที่ต้องทิ้งไปทั้งหมดประมาณ 4700 บิท ซึ่งน้อยกว่าครึ่งหนึ่งของบิทที่ส่งไปทั้งหมด หากทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 70/30 จะได้ผลดังรูปที่ 5.8



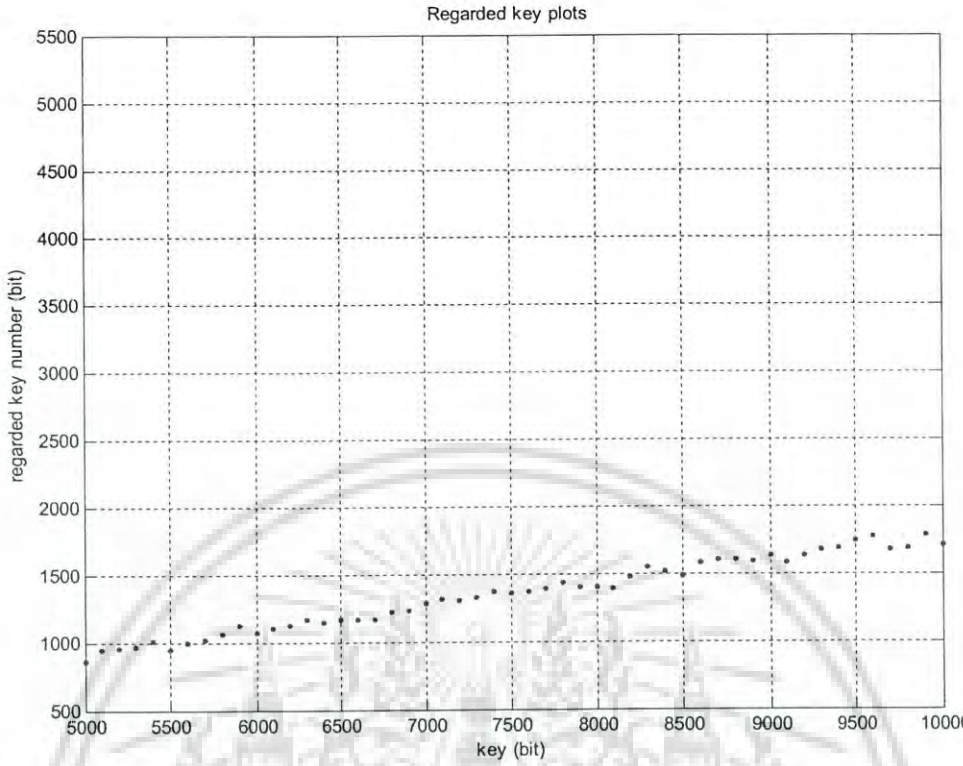
รูปที่ 5.8 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 70/30 ในช่วงการส่งค่าคีย์จำนวน 5000 บิท ถึง 10000 บิท

จากรูปที่ 5.8 การส่งข้อมูลจำนวน 10000 บิทจะมีจำนวนบิทที่ต้องทิ้งไปทั้งหมดประมาณ 4200 บิท ซึ่งน้อยกว่าในกรณีที่ค่าความน่าจะเป็นในการสุ่มเท่ากับ 60/40 หากทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 80/20 จะได้ผลดังรูปที่ 5.9



รูปที่ 5.9 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 80/20 ในช่วงการส่งค่าคีย์จำนวน 5000 บิท ถึง 10000 บิท

จากรูปที่ 5.9 การส่งข้อมูลจำนวน 10000 บิทจะมีจำนวนบิทที่ต้องทิ้งไปทั้งหมดประมาณ 3200 บิท ซึ่งน้อยกว่าในกรณีที่ค่าความน่าจะเป็นในการสุ่มเท่ากับ 60/40 และ 70/30 หากทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear เป็น 90/10 จะได้ผลดังรูปที่ 5.10



รูปที่ 5.10 ผลการจำลองเมื่อปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear ที่ 90/10 ในช่วงการส่งค่าคีย์จำนวน 5000 บิท ถึง 10000 บิท

จากรูปที่ 5.10 การส่งข้อมูลคีย์จำนวน 10000 บิทจะมีจำนวนบิทที่ต้องทิ้งไปทั้งหมดประมาณ 1700 บิท ซึ่งน้อยกว่าในกรณีที่ค่าความน่าจะเป็นในการสุ่มเท่ากับ 60/40, 70/30 และ 80/20

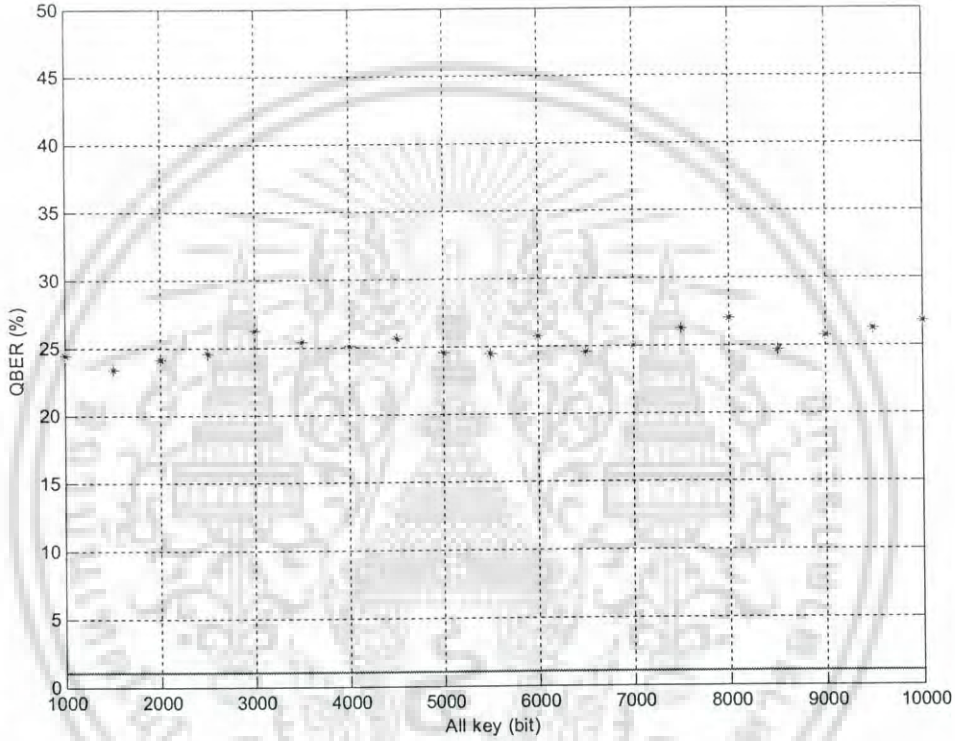
ผลการทดลองในหัวข้อ 5.2.2 สรุปได้ว่า หากเพิ่มจำนวนบิทข้อมูลที่ส่งไปในระบบทั้งหมดให้อยู่ในช่วง 5000 บิท ถึง 10000 บิท และใช้วิธีการปรับค่าความน่าจะเป็นในการสุ่มระหว่างDiagonal/Rectilinear เป็น 60/40, 70/30, 80/20 และ 90/10 ตามลำดับ ระบบยังสามารถลดค่าคีย์ที่ต้องทิ้งไปได้เหมือนเดิม ดังนั้นการวิธีการปรับค่าความน่าจะเป็นในการสุ่มสามารถใช้ได้กับระบบที่มีการส่งข้อมูลในทุกช่วงจำนวน

5.2.3 ผลการทดลองในแง่ของ QBER

จากผลการทดลองในหัวข้อ 5.2.1 จะเห็นว่าการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear มีผลทำให้ระบบสามารถลดจำนวนคีย์ที่ต้องทิ้งไปได้ อย่างไรก็ตามวิธีการปรับค่านี้ มีข้อเสียคือ เนื่องจากทั้งผู้ส่งและผู้รับในระบบต้องใช้ค่าความน่าจะเป็นเดียวกันในการสุ่ม ดังนั้นจึงต้องมีการส่งค่าความน่าจะเป็นนั้นจากผู้ส่งไปยังผู้รับ ซึ่งหากมีคนเข้ามาขโมยค่านี้

แล้วนำไปวัดโฟตอนระหว่างที่ส่ง จะมีผลทำให้การคำนวณค่า QBER ที่ได้มีค่าต่ำ ทำให้การตรวจจับผู้บุกรุกทำได้ยากหรือไม่สามารถตรวจจับผู้บุกรุกในระบบได้

ในการทดลองนี้ได้ทำการจำลองการส่งข้อมูลในกรณีที่มีผู้บุกรุกเข้ามาในระบบและใช้ค่าความน่าจะเป็นในการสุ่มเท่ากับ 50/50, 70/30, 80/20 และ 90/10 โดยรูปที่ 5.11 แสดงผลการจำลองการหาค่า QBER ในกรณีที่มีผู้บุกรุกเข้ามาวัดโฟตอนโดยใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เท่ากับ 50/50



รูปที่ 5.11 ผลการจำลองเพื่อหาค่า QBER ในกรณีที่มีผู้บุกรุกเข้ามาวัดโฟตอนโดยใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 50/50

จากรูปที่ 5.11 จะเห็นว่า หากใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 50/50 ระบบจะสามารถตรวจจับผู้เข้ามาบุกรุกได้ง่ายจากค่า QBER ที่สูงถึง 25% โดยที่ ค่า QBER สามารถคำนวณได้จาก

$$\mathrm{QBER}\,(\%) = \frac{\text{Error bit}}{\text{All bit}} \times 100 \qquad (5.1)$$

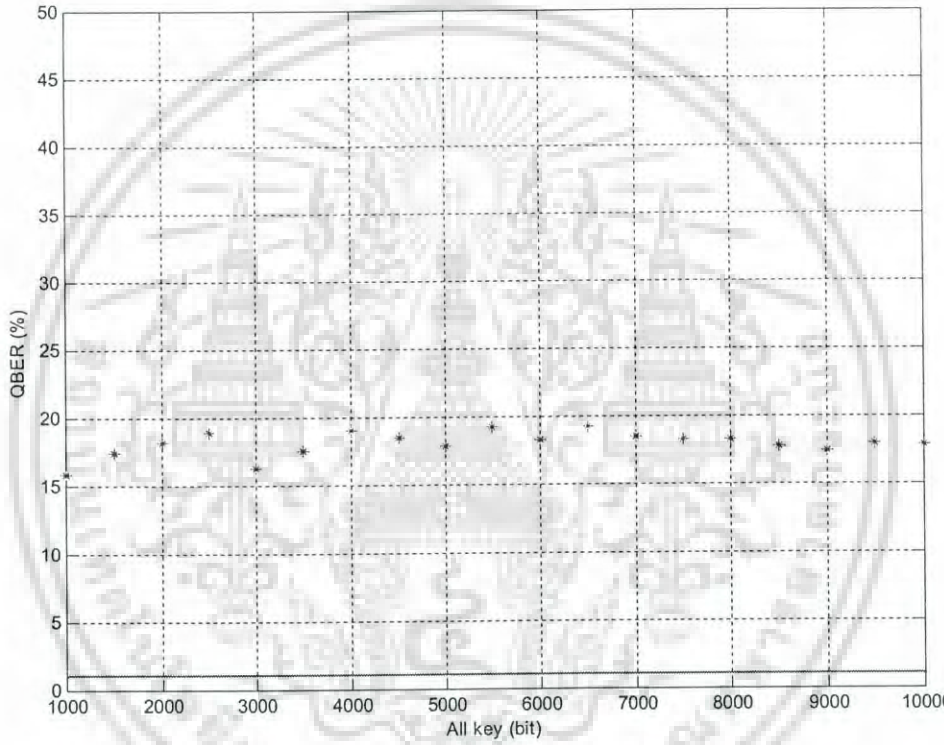
โดยที่

QBER คือ ค่าความผิดพลาดคิวบิทมีหน่วยเป็นเปอร์เซนต์

Error bit คือ จำนวนบิทที่ผิดพลาด

All bit คือ จำนวนบิททั้งหมดที่ใช้เบสิสตรงกัน

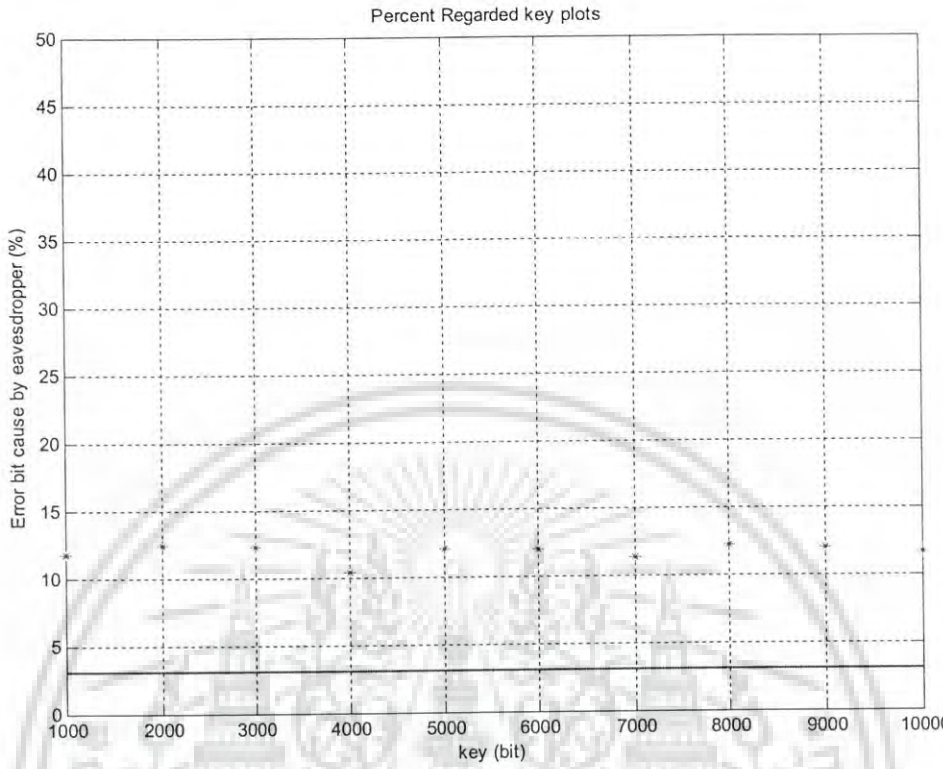
หากระบบทำการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 30/70 ตามที่ได้ออกแบบไว้จะได้ผลการจำลองดังรูปที่ 5.12



รูปที่ 5.12 ผลการจำลองเพื่อหาค่า QBER ในกรณีที่มีผู้บุกรุกเข้ามาวัดโฟตอนโดยใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 30/70

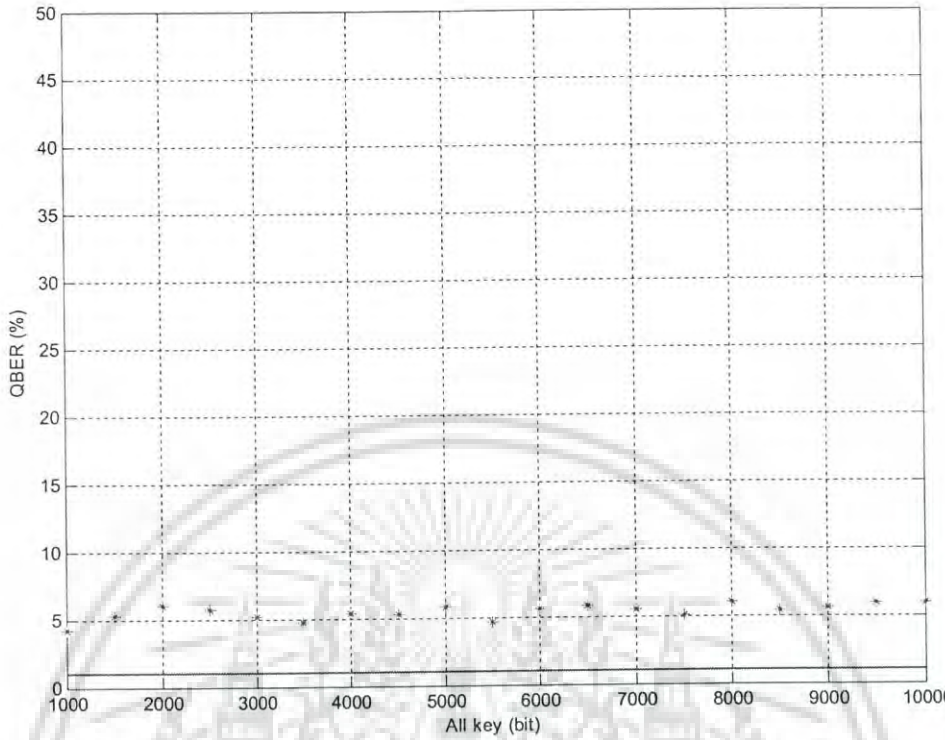
จากรูปที่ 5.12 จะเห็นว่า หากใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 30/70 ค่า QBER จะลดลงเหลืออยู่ที่ประมาณ 15% ซึ่งเมื่อค่า QBER ลดลงจะมีผลเสียทำให้ระบบทำการตรวจจับผู้บุกรุกได้ยากขึ้น

และหากทำการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 20/80 ดังที่ได้ออกแบบไว้ จะได้ผลดังรูปที่ 5.13



รูปที่ 5.13 ผลการจำลองเพื่อหาค่า QBER ในกรณีที่มีผู้บุกรุกเข้ามาวัดโฟตอนโดยใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 20/80

จากรูปที่ 5.13 จะเห็นว่า หากใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 20/80 ค่า QBER จะลดลงเหลืออยู่ที่ประมาณ 12% ซึ่งเมื่อค่า QBER ลดลงจะมีผลเสียทำให้ระบบทำการตรวจจับผู้บุกรุกได้ยากขึ้น และหากทำการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 10/90 ดังที่ได้ออกแบบไว้ จะได้ผลดังรูปที่ 5.14



รูปที่ 5.14 ผลการจำลองเพื่อหาค่า QBER ในกรณีที่มีผู้บุกรุกเข้ามาวัดโฟตอนโดยใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 10/90

จากรูปที่ 5.14 จะเห็นว่า หากใช้ค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 10/90 ค่า QBER จะลดลงเหลืออยู่ที่ประมาณ 5% ซึ่งเป็นค่าที่ต่ำมาก และใกล้เคียงกับค่า QBER threshold (3%) มีผลเสียทำให้ระบบทำการตรวจจับผู้บุกรุกได้ยากขึ้นเนื่องจากไม่สามารถรู้ได้ว่า QBER จำนวนดังกล่าวมาจากความผิดพลาดจากสัญญาณรบกวนในระบบ หรือมาจากการรบกวนของผู้บุกรุก

ในวิทยานิพนธ์นี้ได้ทดลองเปลี่ยนวิธีการคำนวณ QBER จากวิธีเดิมในสมการที่ 5.1 ให้เป็นวิธีการคำนวณแบบแบ่งแยก โดยมีวัตถุประสงค์เพื่อแก้ปัญหาการตรวจจับผู้บุกรุกในระบบเนื่องจากค่า QBER ที่ลดลง ซึ่งจะกล่าวในหัวข้อต่อไป

5.3 ผลการเปลี่ยนวิธีการคำนวณอัตราการผิดพลาด

จากหัวข้อที่ 5.2.1 จะเห็นว่า หากทำการพิจารณาในแง่ของค่าบิทที่ต้องทิ้งไป เมื่อทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 ไปยัง 60/40, 70/30, 80/20 และ 90/10 จะมีผลทำให้ระบบสามารถลดจำนวนคีย์ที่ต้องทิ้งไปได้ แต่จากหัวข้อ

5.2.2 เมื่อพิจารณาในแง่ของ QBER จะเห็นว่าวิธีนี้มีผลเสียคือ ระบบจะตรวจจับผู้บุกรุกได้ยากขึ้น เนื่องจากค่า QBER ลดลงจนใกล้ค่า QBER Threshold

5.3.1 ผลการทดลองเมื่อใช้วิธีการคำนวณอัตราการผิดพลาดแบบแบ่งแยก

ในหัวข้อนี้เป็นการแก้ไขปัญหาดังกล่าว คือการเปลี่ยนวิธีการคำนวณ QBER ให้เป็นการคำนวณแบบแบ่งแยก (Separated QBER) ดังสมการที่ 5.2 และ 5.3

$$\text{QBER in Rectilinear}\,(\%) = \frac{\text{Error Bit in Rectilinear}}{\text{All Bit in Rectilinear}} \times 100 \qquad (5.2)$$

สมการที่ 5.2 เป็นสมการที่ใช้คำนวณหาค่า QBER โดยคำนวณเฉพาะบิทที่อยู่ใน Rectilinear Basis

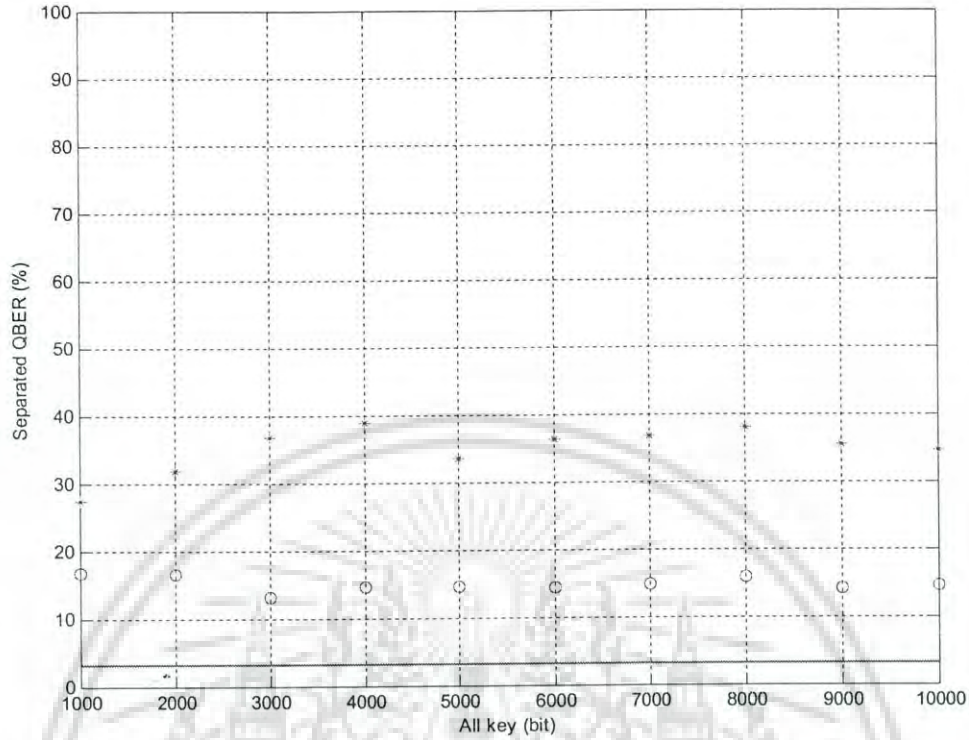
$$\text{QBER in Diagonal}\,(\%) = \frac{\text{Error Bit in Diagonal}}{\text{All Bit in Diagonal}} \times 100 \qquad (5.3)$$

สมการที่ 5.3 เป็นสมการที่ใช้คำนวณหาค่า QBER โดยคำนวณเฉพาะบิทที่อยู่ใน Diagonal Basis

ในการพิจารณาผลการคำนวณ QBER แบบแบ่งแยก ระบบจะพิจารณาจากผลการคำนวณ QBER ของ Rectilinear Basis หรือ Diagonal Basis ตัวใดตัวหนึ่ง โดยพิจารณาแยกกัน

การจำลองด้วยโปรแกรมคอมพิวเตอร์กำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 30/70, 20/80 และ 10/90 ตามลำดับ

รูปที่ 5.15 เป็นการแสดงผลการจำลองเมื่อทำการคำนวณหาค่า QBER แบบแบ่งแยก โดยกำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 30/70



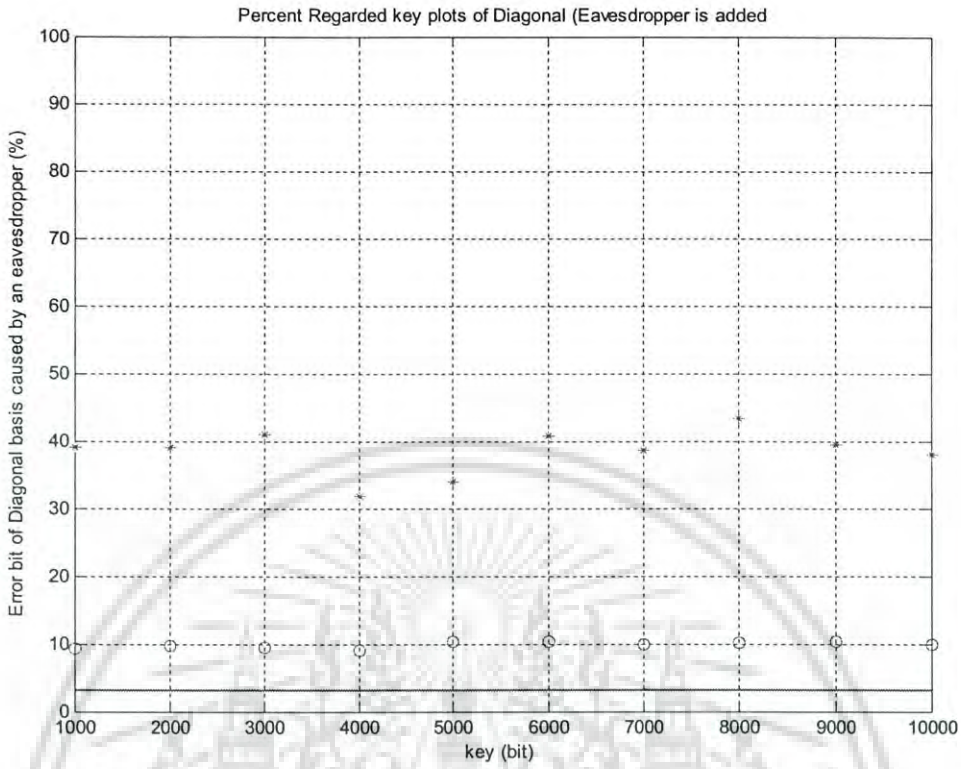
รูปที่ 5.15 ผลการจำลองเมื่อทำการคำนวณหาค่า QBER แบบแบ่งแยก โดยกำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 30/70

โดยที่ *** แทนค่าที่ได้จากการคำนวณ QBER ของ Rectilinear Basis

โดยที่ ooo แทนค่าที่ได้จากการคำนวณ QBER ของ Diagonal Basis

จากรูปที่ 5.15 จะเห็นว่า ค่า QBER ที่ได้จากการคำนวณเฉพาะ Rectilinear Basis นั้นมีค่าที่สูงกว่าค่า QBER Threshold มาก ดังนั้น ระบบจึงสามารถรู้ได้ว่ามีผู้บุกรุกเข้ามาในระบบ

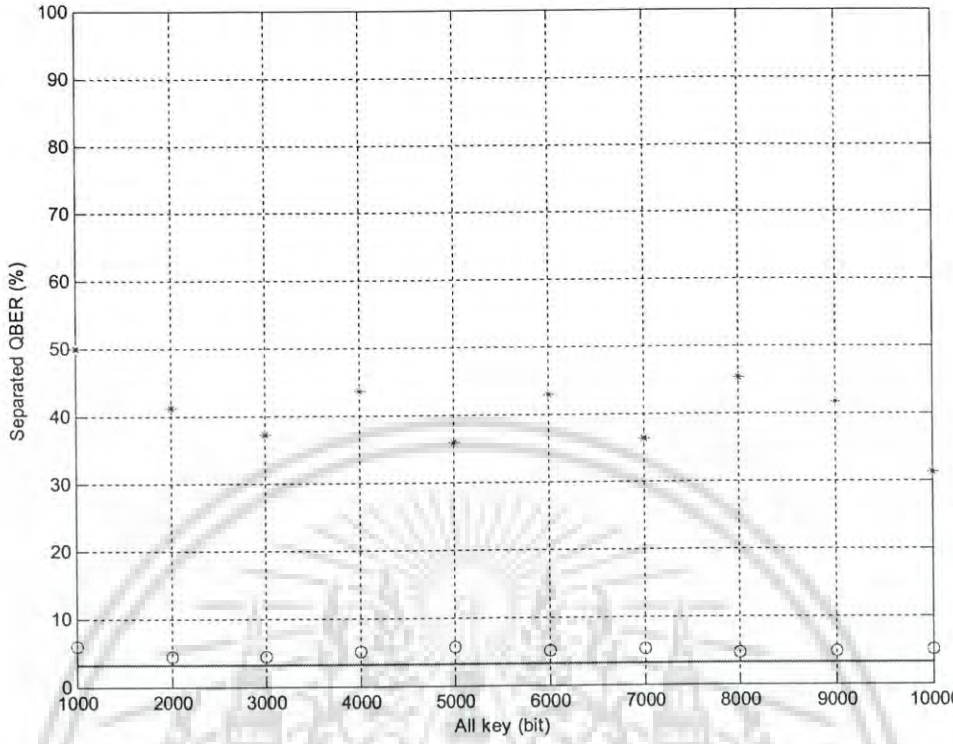
และเมื่อทำการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 20/80 ตามที่ได้ออกแบบไว้ จะได้ดังรูปที่ 5.16



รูปที่ 5.16 ผลการจำลองเมื่อทำการคำนวณหาค่า QBER แบบแบ่งแยก โดยกำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 20/80

จากรูปที่ 5.16 จะเห็นว่า ค่า QBER ที่ได้จากการคำนวณเฉพาะ Rectilinear Basis นั้นมีค่าที่สูงกว่าค่า QBER Threshold มาก ดังนั้น ระบบจึงสามารถรู้ได้ว่ามีผู้บุกรุกเข้ามาในระบบ

และเมื่อทำการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 10/90 ตามที่ได้ออกแบบไว้ จะได้ดังรูปที่ 5.17



รูปที่ 5.17 ผลการจำลองเมื่อทำการคำนวณหาค่า QBER แบบแบ่งแยก โดยกำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 10/90

จากรูปที่ 5.17 จะเห็นว่า ถึงแม้ว่าค่า QBER ที่ได้จากการคำนวณเฉพาะ Diagonal Basis จะต่ำมากจนเกือบถึงค่า Error Threshold แต่ค่า QBER ที่ได้จากการคำนวณเฉพาะ Rectilinear Basis นั้นมีค่าที่สูงกว่า ค่า QBER Threshold มาก ดังนั้น ระบบจึงสามารถรู้ได้ว่ามีผู้บุกรุกเข้ามาในระบบ ซึ่งหากเปรียบเทียบกับผลการคำนวณ QBER แบบเดิม ในรูปที่ 5.13 จะเห็นว่าระบบสามารถตรวจจับผู้บุกรุกได้ง่ายกว่าวิธีการคำนวณ QBER แบบเดิม

5.4 สรุป

ในบทนี้ เป็นการแสดงผลการจำลองโปรแกรมคอมพิวเตอร์ที่ทำการออกแบบเพื่อวิเคราะห์และปรับปรุงประสิทธิภาพของโปรโตคอล BB84 ในระบบควอนตัมคริปโตกราฟฟีโดยในส่วนแรกเป็นการทดลองการปรับค่าความน่าจะเป็นของเบสิสของโฟตอน โดยแสดงผลในแง่ของจำนวนคีย์ที่ต้องทิ้งไปและในแง่ของค่า QBER ผลการทดลองที่ได้สรุปได้ว่าหากทำการปรับค่าในการสุ่ม Diagonal/Rectilinear จาก 50/50 ไปยัง 60/40, 70/30, 80/20 และ 90/10 มีผลทำให้ระบบสามารถลดจำนวนคีย์ที่ต้องทิ้งไปได้ ซึ่งหมายความว่าระบบมีจำนวนคีย์ที่ใช้ได้เพิ่มมากขึ้น แต่

หากพิจารณาในแง่ของค่า QBER จะมีผลเสียคือการปรับค่าความน่าจะเป็นตามที่ออกแบบไว้จะทำให้ตรวจจับผู้บุกรุกในระบบได้ยากขึ้นหรือไม่สามารถตรวจจับผู้บุกรุกในระบบได้

ดังนั้นเพื่อแก้ปัญหานี้ ในส่วนที่สองของการทดลองเป็นการเปลี่ยนวิธีการคำนวณค่า QBER โดยใช้วิธีการคำนวณแบบแบ่งแยก ซึ่งทำการคำนวณค่า QBER ของ Diagonal และ Rectilinear แยกกัน และเปรียบเทียบกับค่า Error Threshold ผลการทดลองที่ได้แสดงให้เห็นว่าการคำนวณค่า QBER โดยใช้วิธีการคำนวณแบบแบ่งแยกสามารถใช้คู่กับวิธีการปรับค่าความน่าจะเป็นในการสุ่มค่าคีย์โดยที่ระบบยังสามารถตรวจจับผู้บุกรุกได้

บทที่ 6
สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยการปรับปรุงประสิทธิภาพของระบบควอนตัมคริปโตกราฟฟีในวิทยานิพนธ์นี้เป็นการปรับค่าความน่าจะเป็นที่ใช้ในการสุ่มค่าเบสิสของโฟตอนในขั้นตอนแรกของโปรโตคอล BB84 ซึ่งเป็นโปรโตคอลแรกของระบบควอนตัมคริปโตกราฟฟี โดยปรับจากค่าเดิมของโปรโตคอล BB84 คือ Diagonal/Rectilinear เท่ากับ 50/50 เป็น 60/40, 70/30, 80/20 และ 90/10 โดยมีสมมติฐานว่า หากทำการปรับค่าความน่าจะเป็นที่ใช้ในการสุ่มค่าเบสิสของโฟตอนแล้ว ระบบจะสามารถลดจำนวนข้อมูลคีย์ที่ต้องทิ้งไปได้ ซึ่งจะใช้โปรแกรม Matlab ในการทดสอบ และในวิทยานิพนธ์นี้ยังได้ทำการทดสอบวิธีการคำนวณหาค่า QBER แบบแบ่งแยก เพื่อแก้ปัญหาการตรวจจับผู้บุกรุกในระบบเมื่อมีการปรับค่าความน่าจะเป็นที่ใช้ในการสุ่มค่าเบสิสของโฟตอน โดยจำลองการทำงานของระบบในกรณีที่มีผู้บุกรุกเข้ามาวัดค่าของโฟตอนในระหว่างส่ง

6.1 สรุปผลการทดลอง

จากการทดลองปรับค่าความน่าจะเป็นที่ใช้ในการสุ่มค่าเบสิสของโฟตอน โดยทดสอบกับโปรแกรมจำลองระบบควอนตัมคริปโตกราฟฟีในกรณีที่ไม่มีผู้บุกรุก ในแง่ของจำนวนคีย์ที่ต้องทิ้งเมื่อทำการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 ไปยัง 60/40, 70/30, 80/20 และ 90/10 โดยเมื่อพิจารณาเปรียบเทียบที่จำนวนบิตข้อมูลที่ส่งเท่ากับ 5000 บิต จะได้ผลการทดลองดังนี้

- เมื่อไม่มีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear กล่าวคือเป็นโปรโตคอล BB84 แบบดั้งเดิม ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 2500 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 60/40 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 2600 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 70/30 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 3000 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 80/20 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 3500 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 90/10 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 4000 บิท

และเมื่อทำการเพิ่มจำนวนบิตข้อมูลเป็น 10000 บิต จะได้ผลการทดลองดังนี้

- เมื่อไม่มีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear กล่าวคือเป็นโปรโตคอล BB84 แบบดั้งเดิม ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 5000 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 60/40 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 5300 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 70/30 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 5800 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 80/20 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 6800 บิท
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 90/10 ระบบจะมีจำนวนคีย์ที่นำไปเข้ารหัสได้ประมาณ 8300 บิท

จากผลการทดลองพบว่าการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนดังกล่าว มีผลทำให้ระบบสามารถลดจำนวนคีย์ที่ต้องทิ้งไปได้ ซึ่งหมายความว่าระบบมีจำนวนคีย์ที่นำไปใช้เข้ารหัสข้อมูลเพิ่มมากขึ้น ดังนั้น ผลการทดลองที่ได้ตรงกับสมมติฐานที่ได้ตั้งไว้ก่อนการทดลอง

หากพิจารณาในแง่ของค่า QBER พบว่าการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนดังกล่าวมานั้น มีผลเสียคือระบบจะตรวจจับผู้บุกรุกในระบบได้ยากขึ้นหรือไม่สามารถตรวจจับผู้บุกรุกในระบบได้ เนื่องจากการปรับค่าความน่าจะเป็นมีผลทำให้ค่า QBER ลดลงจนใกล้ค่า Error Threshold ซึ่งโดยปกติแล้วค่า QBER จะเป็นค่าที่นำมาพิจารณาว่ามีผู้บุกรุกในระบบหรือไม่โดยการเปรียบเทียบกับค่า Error Threshold หากค่า QBER สูงกว่าค่า Error Threshold มาก ๆ ผู้ส่งและผู้รับจะสามารถแน่ใจได้ว่าไม่มีผู้บุกรุกในระบบ ในโปรโตคอล BB84 แบบดั้งเดิม ค่า QBER จะอยู่ที่ประมาณ 25% ซึ่งสูงกว่าค่า Error Threshold ที่โดยทั่วไปแล้วมีค่าประมาณ 1%-5% จากผลการทดลองปรับค่าความน่าจะเป็นในการสุ่มโฟตอนระหว่าง Diagonal/Rectilinear จาก 50/50 ไปยัง 60/40, 70/30, 80/20 และ 90/10 เมื่อพิจารณาในแง่ของค่า QBER จะได้ผลการทดลองดังนี้

- เมื่อไม่มีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear กล่าวคือเป็นโปรโตคอล BB84 แบบดั้งเดิม ค่า QBER อยู่ที่ประมาณ 25%
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 70/30 ค่า QBER จะลดลงอยู่ที่ประมาณ 15%
- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 80/20 ค่า QBER จะลดลงอยู่ที่ประมาณ 12%

- เมื่อมีการปรับค่าความน่าจะเป็นในการสุ่มระหว่าง Diagonal/Rectilinear จาก 50/50 เป็น 90/10 ค่า QBER จะลดลงอยู่ที่ประมาณ 5%

จากผลการทดลอง พบว่าการปรับค่าความน่าจะเป็นในการสุ่มโฟตอนมีผลทำให้ค่า QBER ลดลงจนใกล้ค่า Error Threshold ซึ่งมีผลเสียคือผู้ส่งและผู้รับจะตรวจจับผู้บุกรุกในระบบได้ยากขึ้นหรือไม่สามารถตรวจจับผู้บุกรุกในระบบได้ ดังนั้น เพื่อแก้ปัญหานี้ในส่วนที่สองของการทดลองเป็นการเปลี่ยนวิธีการคำนวณค่า QBER โดยใช้วิธีการคำนวณแบบแบ่งแยก ซึ่งทำการคำนวณค่า QBER ของ Diagonal และ Rectilinear แยกกัน และนำค่าที่คำนวณได้แต่ละค่ามาเปรียบเทียบกับค่า Error Threshold หากมีค่าใดค่าหนึ่งมากกว่าค่า Error Threshold มาก ๆ ผู้ส่งและผู้รับในระบบจะสามารถตรวจจับผู้บุกรุกได้ จากการจำลองวิธีการคำนวณค่า QBER โดยใช้วิธีการคำนวณแบบแบ่งแยก ได้ผลการทดลองดังนี้

- เมื่อทำการคำนวณหาค่า QBER แบบแบ่งแยก โดยกำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 30/70 ค่า QBER ที่ได้จากการคำนวณเฉพาะ Rectilinear Basis อยู่ที่ประมาณ 29% - 40% ซึ่งเป็นค่าที่สูงกว่าค่า QBER Threshold มาก ดังนั้นจึงสามารถรู้ได้ว่ามีผู้บุกรุกเข้ามาในระบบ

- เมื่อทำการคำนวณหาค่า QBER แบบแบ่งแยก โดยกำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 20/80 ค่า QBER ที่ได้จากการคำนวณเฉพาะ Rectilinear Basis อยู่ที่ประมาณ 31% - 43% ซึ่งเป็นค่าที่สูงกว่าค่า QBER Threshold มาก ดังนั้นจึงสามารถรู้ได้ว่ามีผู้บุกรุกเข้ามาในระบบ

- เมื่อทำการคำนวณหาค่า QBER แบบแบ่งแยก โดยกำหนดให้มีการปรับค่าความน่าจะเป็นในการสุ่ม Rectilinear/Diagonal เป็น 10/90 ค่า QBER ที่ได้จากการคำนวณเฉพาะ Rectilinear Basis อยู่ที่ประมาณ 33% - 50% ซึ่งเป็นค่าที่สูงกว่าค่า QBER Threshold มาก ดังนั้นจึงสามารถรู้ได้ว่ามีผู้บุกรุกเข้ามาในระบบ

จากผลการทดลองที่ได้แสดงให้เห็นว่า การคำนวณค่า QBER โดยใช้วิธีการคำนวณแบบแบ่งแยกสามารถนำไปใช้ในการแก้ปัญหาในแง่ของการคำนวณค่า QBER ในกรณีที่มีการปรับค่าความน่าจะเป็นในการสุ่มค่าคีย์ โดยช่วยให้ผู้ส่งและผู้รับสามารถตรวจจับผู้บุกรุกได้

6.2 ปัญหาที่พบในงานวิจัย

เนื่องจากการจำลองโปรแกรมระบบควอนตัมคริปโตกราฟฟีจากระบบฮาร์ดแวร์จริงต้องมีการเก็บข้อมูลในส่วนของค่าพารามิเตอร์ต่าง ๆ จำนวนมากเพื่อใช้ในการออกแบบโปรแกรม แต่เนื่องจากผู้วิจัยไม่ได้เป็นผู้สร้างระบบฮาร์ดแวร์นั้นเอง จึงไม่สามารถนำแนวคิดที่ใช้ในการปรับปรุงระบบไปทดสอบกับระบบฮาร์ดแวร์จริง มีเพียงผลการทดลองจากโปรแกรมจำลอง

6.3 แนวทางการพัฒนาในอนาคต

นอกจากวิธีการปรับค่าความน่าจะเป็นที่ใช้ในการสุ่มค่าเบสิสของโฟตอนและวิธีการคำนวณค่า QBER แบบแบ่งแยกในวิทยานิพนธ์นี้แล้ว ระบบควอนตัมคริปโตกราฟฟียังสามารถพัฒนาต่อไปได้อีกในอนาคต โดยพัฒนาในแง่ของการลดอัตราความผิดพลาดของข้อมูล ซึ่งมีแนวทางการพัฒนา 2 แนวทาง คือ

6.3.1 พัฒนาในส่วนของฮาร์ดแวร์ เนื่องจากในระบบจริงนั้นในขณะทำงานมักมีสัญญาณรบกวนหรือการทำงานผิดพลาดของอุปกรณ์ซึ่งทำให้เกิดบิตข้อมูลที่ผิดพลาดขึ้น การแก้ไขนี้อาจทำได้โดยการเลือกปรับค่าที่ใช้ในอุปกรณ์ต่างๆ เช่น ค่าอุณหภูมิ ค่าแรงดันไฟฟ้าที่ใช้ใน APD เพื่อทำให้สัญญาณรบกวนขณะมืดมีน้อยลง

6.3.2 พัฒนาในส่วนของซอฟท์แวร์ โดยออกแบบอัลกอริทึมที่ใช้ในกระบวนการลดความผิดพลาดของข้อมูล (Error Correction) เพื่อให้สามารถลดความผิดพลาดของข้อมูลโดยใช้เวลาน้อยที่สุดและมีความปลอดภัยมากที่สุด

เอกสารอ้างอิง

[1] W. Stallings. 1999. **Cryptography and Network Security : Principles and Practice.** 3rd ed. New York : Prentice Hall. 1995.

[2] Kasetsart University. **"Encryption."** [Online]. Available : www.ku.ac.th/emagazine/august44/it/encryp.html. 2544.

[3] kitty.in.th **"Public Key Cryptography."** [Online]. Available : www.kitty.in.th/index.php?Room=article&id =76. 2546.

[4] TOT Cooperation limited. **"Certificate Knowledge Authority."** [Online]. Available : http://www.ca.tot.co.th/tha/knowledge.html. 2546.

[5] Lo H-K, Popescu S and Spiller T. **Introduction to Quantum Computation and Information World Scientific.** Singapore. 1998.

[6] Idquantique company. **"Quantum leap for cryptography."** [Online]. Available : http://www.idquantique.com/. 2547.

[7] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, **"Quantum Cryptography Using Entangled Photons in Energy-Time Bell States."**, Phys.Rev. Lett, 84 4737. 2000.

[8] Kyo Inoue. **"Quantum Cryptography Experiment Using a Single-Photon Source"** [Online]. Available : http://www.brl.ntt.co.jp/E/activities/file/report02/E/report17.html. 2004.

[9] patrick zarda. **"Quantum Communication in Higher Dimensional Hilbert Spaces."** [Online]. Available : http://scotty.quantum.physik.uni-muenchen.de/exp/qc/press.html. 2003.

[10] Id-quantique company. **"Quantum Key Distribution over 67 km."** [Online]. Available :http://www.idquantique.com/qkd.html. 2004.

[11] MagiQ Technologies. **"Quantum Information Solutions for the Real World."** [Online]. Available : www.magiqtech.com. 2004.

[12] B. Harris. **University Physics.** Revised Edition. New York : John Wiley & Sons, Inc. 1995.

[13] Wittayapat Library. **"Dara Class room Online : Physics room."** [Online]. Available : http://web1.dara.ac.th/dara/roomonline/Physic/physic.html. 2003.

[14] Frank J. Blatt. **Modern Physics.** New York : McGraw-Hill. 2001.

[15] Michael Fowler. **"The Photoelectric Effect."** [Online]. Available : http://www.phys.virginia.edu/classes/252/photoelectric_effect.html. 1997.

[16] R. P. Feynman. 1964. **Feynman Lectures On Physics : Volume III.** 3rd ed. New York. Addison Wesley Publish Company. 1997.

[17] Electronics Commerce Resource Center. **"Network Security."** [Online]. Available : http://www.ecommerce.or.th/faqs/faq3-1.html. 2546.

[18] W. Stallings. 1999. **Cryptography and Network Security : Principles and practice.** 3rd ed. New York : Prentice Hall. 1997.

[19] ปิยนันท์ ธนบดีภัทร์. **"การเข้ารหัส (Encryption) และ Digital Certificate"** [Online]. Available : http://www.bus.tu.ac.th/usr/wanchai/ba313/reports/encryption/Encryption.htm. 2545.

[20] 2004 RSA Security. **"The New RSA Factoring Challenge : RSA-155 is factored."** [Online]. Available : http://www.rsasecurity.com/rsalabs/node.asp?id=2098. 2004.

[21] RSA Security. **"RSA Security Solutions : Enterprise access."** [Online]. Available : http://www.rsasecurity.com. 2004.

[22] Gilles Brassard. **"A Bibliography of Quantum Cryptography."** [Online]. Available : http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html. 2003.

[23] S. Wiesner. **"Conjugate coding."** Sigact News, 15(1), 1983.

[24] Quantum informatics. **"The BB84 Quantum Coding Scheme."** [Online]. Available : http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html. 1998.

[25] Charles H. Bennett and J. A. Smolin. 2004. **"The early days of experimental quantum cryptography."** IBM Journal Research and Development. 48 : 4. 2004.

[26] Artem Vakhitov. **"Evaluation of security against unauthorized access for practical fiber-based quantum cryptosystems."** Ph.D. Thesis of Norwegian University of Science and Technology. 2004.

[27] Prem Kumar, Marco Fiorentino, Paul Voss and Jay Sharping. **"Radical Improvement for Security of Fiber-Optic Networks - Quantum Cryptography Sources and Detectors."** [Online]. Available : http://ttp.northwestern.edu/abstracts/viewabs.php?id=94&cat=4. 2003.

[28] Los Alamos national laboratory. **"free-space quantum cryptography."** [Online]. Available : http://www.lanl.gov/orgs/pa/science21/QuantumCrypto.html. 2003.

[29] Physicsweb. **"Wireless quantum encryption : 9 October 1998."** [Online]. Available : http://physicsweb.org/article/news/2/10/9/1. 2003.

[30] Th. Jennewein, Ch. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. **"Quantum Cryptography with Entangled Photons."** Phys. Rev. Lett 84 4729. 2000.

[31] James Ford, Neal E. Young. **"Quantum Cryptography Tutorial."** [Online]. Available : http://www.cs.dartmouth.edu/~jford/crypto.html. 2539.

[32] P.A. Hiskett, G. Bonfrate, G.S. Buller and P.D. Townsend. **"80km transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55μm."** Journal of Modern Optics. 48. 2001.

[33] Wolfram Research, Inc. **"Random Permutation"** [Online]. Available : http://mathworld.wolfram.com/RandomPermutation.html. 2003.

[34] Protechnix. **"Cryptology and Data Secrecy : The Vernam Cipher."** [Online]. Available : http://www.pro-technix.com/information/crypto/pages/vernam_base.html. 2003.

[35] สุรศักดิ์ เชียงกา. **"Experimental Quantum Cryptography Based on the BB84 Protocol."** [Online]. Available : http://www.ku.ac.th/kaset60/Theme04/theme-04-38/index-04-38.html. 2003.

ภาคผนวก

ภาคผนวก

บทความวิจัยที่ได้รับการตีพิมพ์ลงในวารสาร ในวิทยานิพนธ์ คือ

[1] W. Natasiri and P. Sooraksa, "The Appropriate Probability for Quantum Key Distribution System", ISCIT2003, The Third International Symposium on Communications and Information Technologies, Bangkok, Thailand. pp. 248-251 2003

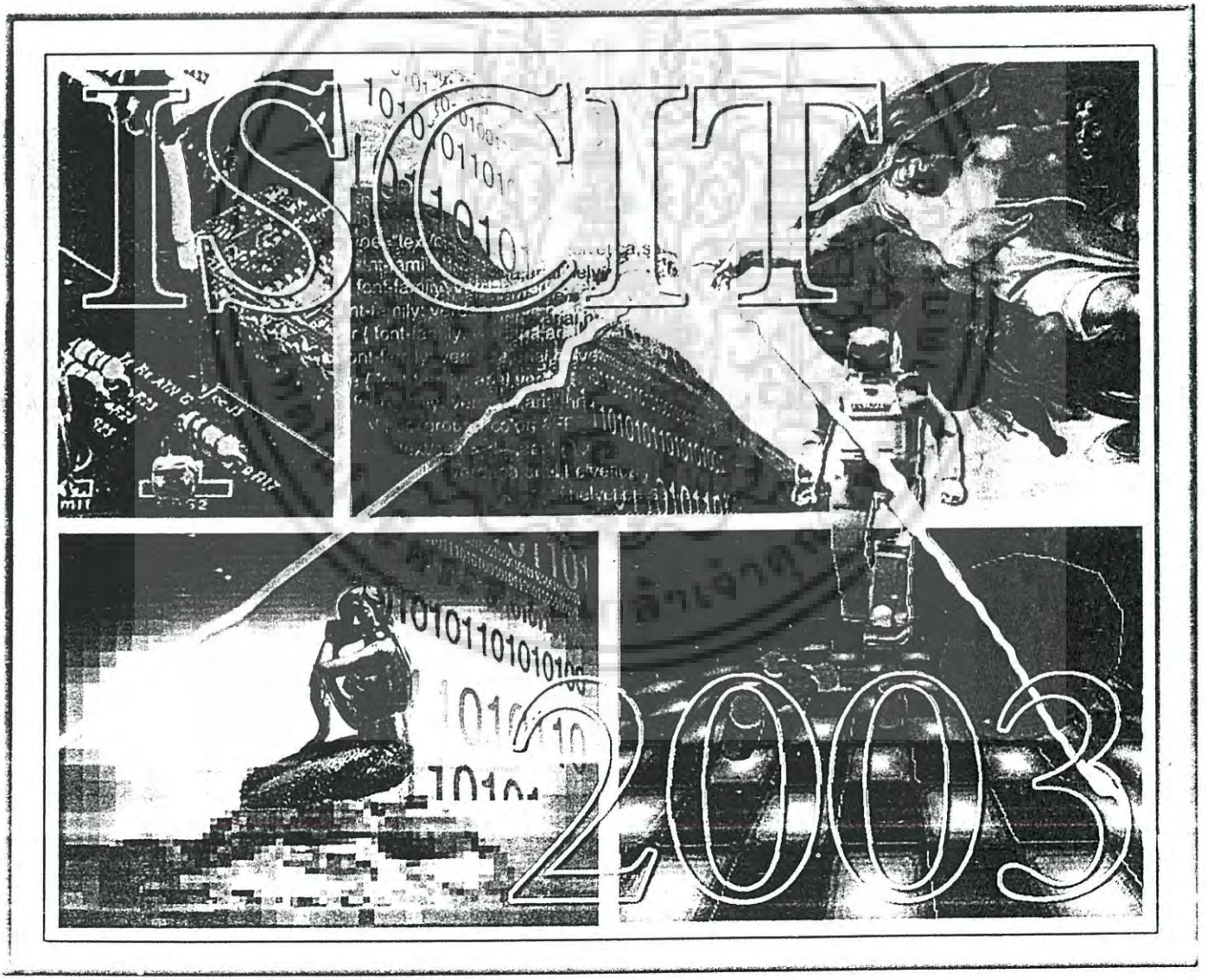
Volume I

Proceedings

The Third International Symposium on Communications and Information Technologie

September 3-5, 2003

BP Samila Beach Hotel and Resort, Songkhla, Thailand



The Appropriate Probability for Quantum Key Distribution System

W. Natasiri and P. Sooraksa

Department of Information Engineering,Faculty of Engineering,
King Mongkut's Institute of Technology Ladkrabang
Chalongkrung Rd.,Ladkrabang,Bangkok, 10520
Email: s4612902@kmitl.ac.th , maewnum@hotmail.com

Abstract

Quantum Cryptography uses the polarized single photon to encode secret key bits. The system has proved to be secure by the uncertainty property. This paper searches for the appropriate probability of polarized photon basis in the first step of BB84 protocol. Assigning the appropriate probability can reduce the discarded data in Quantum Cryptography scheme. The probability will be announced in the public channel so the eavesdropper may try to copy and measure photons illegitimately. In order to solve this problem, the method of separated error rate estimation is considered in this paper. The BB84 simulation results show that using appropriate probability can reduce the discarded data and still can detect the eavesdropper attacks by separated error estimation method.

1. Introduction

The security of almost symmetric cryptography system bases on the secret key that is shared between sender and receiver. Quantum cryptography, also known as quantum key distribution (QKD), makes use of quantum mechanics law to keep the security of the secret key. As the result, the observation of eavesdropper in quantum system affects the information, once communication content is tapped, without knowing any basis of polarization photons in the channel, the content changes irreversibly. So the eavesdropped content is meaningless and the recipients are able to detect eavesdroppers from the calculation of QBER (Q-bit Error Rate) of key bits. Quantum cryptography theory has been widely discussed in the literature [1], and the first experiment was reported in U.S. in 1989[2]. Until now, there are many experiments of quantum key distribution even over distance of several kilometers [3-5].

The standard protocol of quantum key distribution is BB84 protocol proposed by Bennett and Brassard [6]. In the first step of BB84, Alice (the sender) chooses one of two polarization states, which are Rectilinear and Diagonal, of single photon randomly. So each basis of photons generate with 50% probability. Bob (the recipient) do the same as Alice, and they compare their photons and keep only photons that are in the same polarization. So, on average they have to discard 50% of all photons. In order to reduce the discarded data, there is a proposed method in [8]. The idea is to assign the different probability on Rectilinear basis (Pr). As Pr goes to zero, but not exactly reach zero, the discarded key is reduced. The probability Pr must be announced in the public channel so the eavesdropper may try to copy and measure polarized photons with the same probability, which makes it difficult to detect eavesdropper's attack. The paper [8] also proposed the method of separated error estimation, by dividing the data of each basis into two subsets and calculates the QBER separately. This method can be used to detect eavesdropper. However, there are some constraints on choosing the probability. If the probability of Rectilinear is very low, then there are not enough photons to calculate QBER. This paper searches for the appropriate probability of Rectilinear basis using BB84 simulation. The results show that assigning appropriate probability in the system can reduce discarded data and the eavesdropper can still be detected by separated error rate estimation method.

This paper is organized as follow, Section 2 will describe conventional BB84 protocol. Section 3 will be the BB84 with the different probability of polarized photon basis and the problem of eavesdropping detection is in subsection 3.2. Section 4 describes the idea of separated error rate estimation and shows the simulation result.

2. The conventional BB84 Protocol

The BB84 protocol was proposed by C.H. Bennett and G. Brassard in 1984. It was the first quantum encoding of classical information that make use of quantum mechanics uncertainty theory so the receiver, either legitimate or eavesdropper, can not recover information with 100% reliability. It is the basic tool most of the quantum protocols are based upon, for more information, see [6]. The BB84 coding scheme makes a correspondence between classical bits and quantum states. Each classical bit corresponds to a mixture of two non-orthogonal quantum states, which are called 'Rectilinear' and

'Diagonal' basis. The representation looks like:

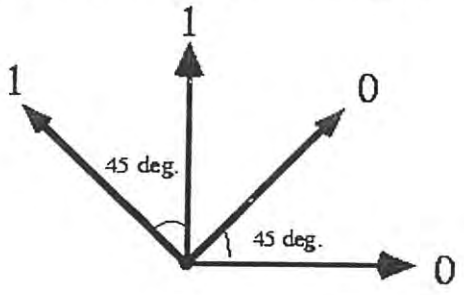


Figure 1. The representation of polarization photon basis

The basis with 0 deg. or 90 deg. is 'Rectilinear basis'
The basis with 45 deg. or 135 deg. is 'Diagonal basis'

In the BB84 coding scheme, the classical bit '0' is encoded either by a photon with horizontal polarization or by a photon with polarization at 45 degrees. The classical bit '1' is encoded by either a photon with polarization along the vertical direction or by a photon polarized at an angle of 135 degrees.

In particular, quantum cryptography makes use of the Heisenberg uncertainty principle. According to the principle, the measurement of any quantum system without knowledge about its states will alter it in such a way that the measurement can not be completely accurate.

BB84 Protocol follows these steps:

1. Alice randomly chooses photon in one of four polarization (horizontal, vertical, 45 degrees and 135 degrees) and send to Bob.
2. Bob randomly choose basis (Rectilinear or Diagonal) to measure Alice's photon.
3. Bob records his measurement basis and the result of measurement.
4. Bob tells Alice his basis (not the bit value) on the public unjammable channel.
5. Alice tells Bob which of his measurement basis is correct.
6. Alice and Bob discard the bits that measure in the wrong basis because the result is random, and keep the bits with the correct basis which is called 'Sifted key'.
7. Alice and Bob randomly choose a subset of photons from the sifted key and publicly compare their polarization data to calculate QBER (Q-bit error rate). Since the polarization data of photons in this subset have been announced in public channel, Alice and Bob must discard those data to avoid information leakage to Eve. From the calculated QBER, Alice and Bob will know that eavesdropper has been measured their photons if the QBER is higher than the threshold error rate (Eth). The threshold error rate comes from channel noise or other disturbances in the system. Alice and Bob may restart the whole procedure again. On the other hand, if the error rate turns out to be reasonably small (QBER < Eth), they go to the next step.
8. Error correction and privacy amplification: Although the QBER in this step is not greater than Eth, but there are still some errors on data and they need to be corrected because Alice and Bob must use the exact identical key in the cryptographic scheme. Error correction solves this problem. As Alice and Bob have to compare data on public channel, Eve may have partial information on the shared data. A realistic scheme must include privacy amplification to make the data more secure see [7] for more details of privacy amplification method.

3. BB84 with different probability

3.1. No Eavesdropper

From section 2, in the first step of BB84 protocol, Alice randomly chooses polarization photon state between Rectilinear and Diagonal with equal probability (0.5). On average, half of the time Bob will guess basis wrong so the discarded bit is 50% of all bits. To reduce the amount of discarded key, the idea of different probability in [8] is assigned. Let Pr be the Rectilinear random probability, so probability for Diagonal is 1-Pr. The simulation is based on the assumption that the regarded bit will decrease when Pr is decreased to zero. To find the amount of regarded bit, this paper tests the result of different probability by the BB84 protocol simulation build in MATLAB. The simulation result is as follow,

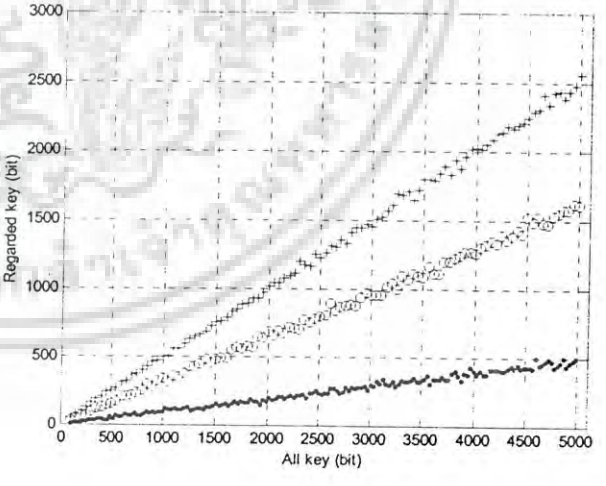


Figure 2. Simulation of regarded bit in BB84 protocol.

*** stands for the system with Pr = 0.5
ooo stands for the system with Pr = 0.2
..... stands for the system with Pr = 0.05
key range is from 100 to 5000 bits

From the result, at the same amount of key, the regarded bit of the system with 0.5 probabilities (Conventional BB84) is the maximum value. The regarded key will decrease as the probability set to be lower, from 0.5 to 0.2 and finally 0.05. So this simulation result shows that setting probability of Rectilinear basis to be lower to zero can reduce the regarded bit and keep more usable key in the system.

3.2 With Eavesdropper

The last section showed satisfied result of assigning different probability on BB84 protocol without eavesdropper. Actually, the main advantage of quantum cryptography is the ability to detect eavesdropper in the system by calculating the QBER and compare with the threshold value. In the conventional BB84 protocol, the QBER can be calculated as follow,

1. Probability that Alice and Bob use the different basis is ½
2. If Alice and Bob use the different basis, the result bit will randomly be '0' or '1' (It could be right or wrong) so the probability of the wrong result is ½

Finally, the probability of error causes by eavesdropper is ½ * ½ = ¼ = 25%

If the different probability is assigned to the system, Alice has to tell Bob the value of 'Pr' on the public channel which can be heard but can not be modified by Eave. Eave then copy and use the same probability for her random basis and has more chance to guess the correct polarization photons. This makes the QBER decreases so Alice and Bob can not detect eave's measurement. As Pr is decreased to zero, the regarded bits will be reduced and the chance to detect Eave is reduced also.

To obviously get to the point, the simulation of BB84 protocol with eavesdropper is demonstrated to compare the QBER of the system with the different probability. The simulation program has the following conditions,

1. Eavesdropper tries to measure Alice's entire bit by choosing the random basis with the same probability as Alice's.
2. The Error rate threshold is set to be 1%, if the QBER is more than 1% then eavesdropper is detected.
3. The amount of key is from 1,000 to 10,000 bits and the probabilities are 0.5 and 0.1 respectively.

The simulation result is as follow,

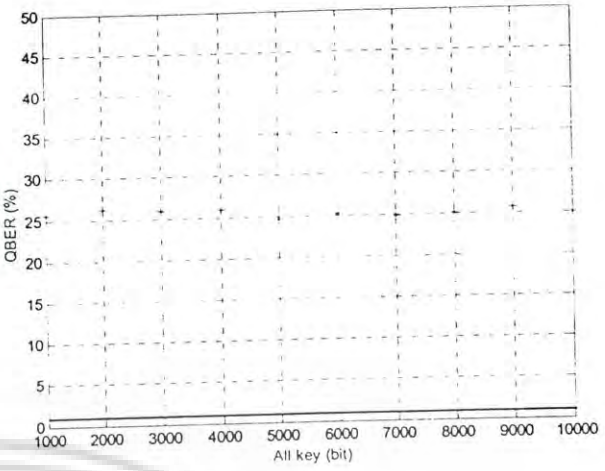


Figure 3. Percent of QBER in BB84 protocol simulation with the 0.5 probability of rectilinear basis

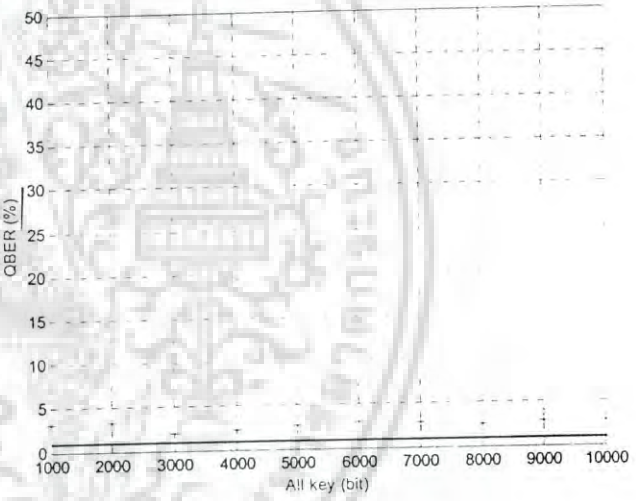


Figure 4. Percent of QBER in BB84 protocol simulation with the probability 0.1 of rectilinear basis.

From the result in figure 3, the QBER of conventional BB84 with 0.5 probabilities is about 25% which is much higher than Eth, so the eavesdropper can easily be detected. But in Figure 4, when the probability is set to be 0.1, the result QBER is only about 3-5 % which is difficult to tell that the error comes from the disturbance or eavesdropper because the error rate is not much different from Eth. To solve this problem, the method of separated error rate estimation is considered and will be described in the next section.

4. Separated QBER

From the last section, the simulation result shows that even though there is an eavesdropper tries to measure our photons, it can not be concluded that the QBER comes from eavesdropper or other disturbances, as the value is near 1%. This section will use separated error estimation, by the calculation of QBER of each basis separately. The condition is, both of Rectilinear and Diagonal QBER must be more than Eth. Percent of each QBER can be calculated as follow,

QBER of Rectilinear = (bit error in rectilinear / all rectilinear bit) * 100

QBER of Diagonal = (bit error in Diagonal / all Diagonal bit) * 100

The simulation result is as follow,

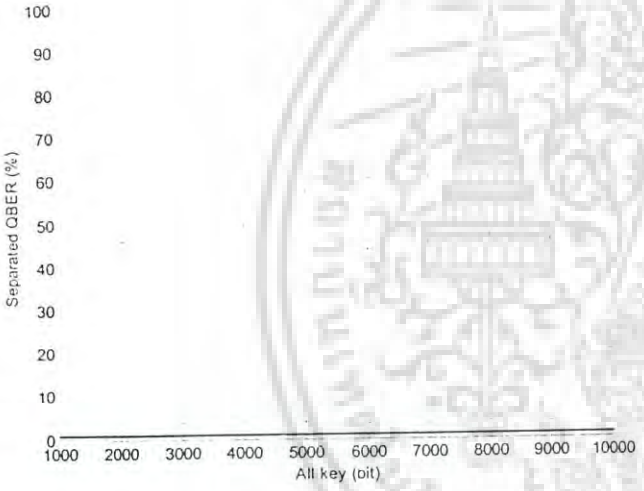


Figure 5. Separated error rate estimation with the probability 0.1 of rectilinear basis

*** stands for error rate from rectilinear basis.
ooo stands for error rate from diagonal basis.

In the simulation, the probability of Rectilinear is set to be 0.1. The result shows that the Rectilinear error rate is much more than 1%. So it is easier to detect eavesdropper compared to the result in Figure 4.

5. Conclusion

This paper searches for the appropriate probability to reduce the discarded data in the first step of BB84 protocol and also assigns the separated error rate estimation method to detect eavesdropper in the system. The simulation shows satisfy result that the discarded key is reduced and the eavesdropper can still be detected in the system.

6. References

[1] Lo H-K, Popescu S and Spiller T, "Introduction to Quantum Computation and Information", World Scientific, Singapore, 1998

[2] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", Journal of Cryptology, vol.5, No.1, 1992, pp.3-28

[3] Toshio Hasegawa, Tsuyoshi Nishioka, Hirokazu Ishizuka, "An Experimental Realization of Quantum Cryptosystem", IEICE Trans. Fundamentals, Vol.E85-A, NO.1 January 2002, pp.149-157.

[4] Hughes R J, Luther G G, Morgan G L, Peterson C G and Simon C, "Quantum cryptography over underground optical fibers" Advances in Cryptology-Proc. Crypto'96, 1996

[5] A. Muller, J. Breguet and N. Gisin, "Experimental demonstration of Quantum Cryptography using polarized photon in optical fiber over more than 1 km", Europhysics Letters, Vol. 23, No.6, 20 August 1993, pp. 3838-388.

[6] C. H. Bennett and G. Brassard, Quantum cryptography: "Public key distribution and coin tossing", in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, IEEE, 1984, pp. 175-179.

[7] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer, "Generalized Privacy Amplification", IEEE Transactions on Information Theory, 1915-1923.

[8] Mohammad Ardehali, Gilles Brassard, H. F. Chau, Hoi-Kwong Lo, "Effcient Quantum Key Distribution", quant-ph/9803007 v3, 23 May 1998

ประวัติผู้เขียน

นางสาววรินดา นาทะสิริ เกิดเมื่อวันที่ 6 กรกฎาคม 2521 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ จากมหาวิทยาลัยเทคโนโลยีสุรนารี ปีการศึกษา 2543 และได้เข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2544

ปัจจุบันมีตำแหน่งเป็นอาจารย์ประจำคณะวิศวกรรมศาสตร์ สาขาวิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยอีสเทิร์นเอเชีย