บรรณาธิการปริทัศน์/Editorial Corner

# แนวทางการวิจัยการเข้ารหัสลับในยุคหลังควอนตัม

# Research Approach on Cryptography in Post-quantum

วชิรพงศ์ จิรกิจภูวพัฒน์ และ ภูมิ คำเอม*
ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

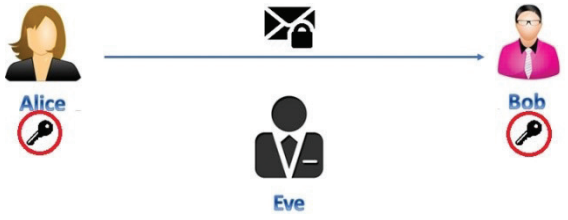
Wachirapong Jirakitpuwapat and Poom Kumam*
Department of Mathematics, Faculty of Science, King Mongkut's University of Technology Thonburi, Bangkok, Thailand

*Corresponding Author, E-mail: poom.kum@kmutt.ac.th DOI: 10.14416/j.kmutnb.2019.08.003


## 1. บทนำ

การเข้ารหัสมีบทบาทสำคัญในการแบ่งปันข้อมูลอย่างปลอดภัยในช่องทางที่ไม่ปลอดภัย ตัวอย่างเช่น Diffie และ Hellman [1], ElGamal [2] และ RSA [3] ฯลฯ ความปลอดภัยของระบบเหล่านี้ตั้งอยู่บนสมมติฐานทางคณิตศาสตร์ เช่น ความยากในการคำนวณค่าผกผันของฟังก์ชันลอการิทึมแบบไม่ต่อเนื่อง ความยากในการแยกตัวประกอบ [4] ฯลฯ อย่างไรก็ตาม ในปี ค.ศ. 1997 Shor [5] แสดงให้เห็นว่าปัญหาเหล่านี้สามารถแก้ไขได้อย่างง่ายโดยใช้ควอนตัมอัลกอริทึม ดังนั้นการใช้โพรโทคอลแบบดั้งเดิมเหล่านี้อาจไม่ปลอดภัย เพราะการพัฒนาคอมพิวเตอร์ควอนตัมในทางปฏิบัติ

การแจกแจงกุญแจแบบควอนตัมช่วยให้สามารถสร้างกุญแจลับระหว่างทั้งสองฝ่ายปลอดภัยต่อการโจมตี การแจกแจงกุญแจแบบควอนตัมขึ้นอยู่บนหลักการฟิสิกส์ควอนตัม ในปี ค.ศ. 1982 Wootters และ Zurek [6] ได้พิสูจน์ว่า เป็นไปไม่ได้ที่จะคัดลอกข้อมูลควอนตัมโดยพลการอย่างสมบูรณ์ ดังนั้นกำลังดักข้อมูลควอนตัมเป็นไปไม่ได้ หากผู้ดักฟังพยายามดักจับการสื่อสารควอนตัม เขาจะทิ้งร่องรอยไว้ ทำให้ตรวจพบและสามารถเปลี่ยนรหัสได้ทันที สิ่งนี้ช่วยให้มีความปลอดภัยที่สูงมากขึ้น




**รูปที่ 1** ระบบรหัสลับ

## 2. ความสำคัญของการแจกแจงกุญแจไขรหัสลับ

เราใช้ระบบรหัสลับเพื่อป้องกันการดักจับข้อมูลการสื่อสาร อย่างไรก็ตาม ระบบรหัสลับตามรูปที่ 1 ต้องการกุญแจในการเข้ารหัสและถอดรหัส ทำให้ต้องมีกระบวนการตกลงกุญแจและป้องกันการดักจับข้อมูล

## 3. BB84

ในปี ค.ศ. 1984 Bennett และ Brassard [7] เสนอขั้นตอนการแจกแจงกุญแจลับบนหลักการฟิสิกส์ควอนตัมเป็นครั้งแรก ซึ่งถูกเรียกว่า BB84 โดยสามารถอธิบายได้ดังต่อไปนี้

### 3.1 การตั้งค่า

1. ตั้งค่าสถานะทั้ง 4 คือ $|\alpha_1\rangle=|0\rangle$, $|\alpha_2\rangle=|1\rangle$, $|\alpha_3\rangle=$

การอ้างอิงบทความ: วชิรพงศ์ จิรกิจภูวพัฒน์ และ ภูมิ คำเอม, "แนวทางการวิจัยการเข้ารหัสลับในยุคหลังควอนตัม," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, ปีที่ 29, ฉบับที่ 4, หน้า 539–541, ต.ค.–ธ.ค. 2562.

$\frac{1}{\sqrt{2}}(|0>+|1>)$ และ $|\alpha_4>=\frac{1}{\sqrt{2}}(|0>-|1>)$

2. ตั้งค่าเวกเตอร์ฐานเชิงตั้งฉากหนึ่งหน่วย 2 แบบ คือ เชิงเส้น (+) จาก $|\alpha_1>$ และ $|\alpha_2>$ เชิงทแยงมุม (x) จาก $|\alpha_3>$ และ $|\alpha_4>$

**3.2 ขั้นตอน**

1. อลิซสุ่มเตรียม $m$ คิวบิต แต่ละคิวบิตในสี่สถานะ จากนั้นเธอส่งคิวบิตทั้งหมดให้บ็อบ

2. สำหรับแต่ละคิวบิตที่บ็อบได้รับ เขาเลือกสุ่มหนึ่งในสองฐานและทำการวัดคิวบิตพร้อมบันทึกผล

3. อลิซประกาศฐานที่เธอใช้ในแต่ละคิวบิตผ่านช่องทางสาธารณะ

4. บ็อบบอกคิวบิตที่เขาวัดได้ถูกต้องให้อลิซผ่านช่องทางสาธารณะ หากไม่มีการดักฟังข้อมูลต่อไปนี้จะเป็นจริง

1) ถ้าเลือกฐานเดียวกับอลิซผลการวัดของเขาเหมือนคิวบิตที่อลิซส่งให้

2) ถ้าเลือกฐานที่แตกต่างจากอลิซแล้วผลการวัดของเขาจะกลายเป็นแบบสุ่ม

5. อลิซและบ็อบปฏิเสธคิวบิตที่พวกเขาไม่ได้ใช้ฐานเดียวกัน

6. อลิซและบ็อบทดสอบความปลอดภัยของกุญแจ โดยใช้การสุ่มเลือกบางส่วนของกุญแจ ผลลัพธ์ที่ได้มี 2 แบบ คือ

1) ตรวจพบข้อผิดพลาด แสดงว่าการส่งไม่ปลอดภัย ดังนั้นพวกเขาปฏิเสธและเริ่มกระบวนการใหม่อีกครั้ง

2) ตรวจสอบไม่พบข้อผิดพลาด พวกเขายอมรับกุญแจและใช้ร่วมกัน ซึ่งไม่ใช่ส่วนที่ใช้ทดสอบ

## 4. ความสำคัญของงานวิจัยการแจกแจงกุญแจไขรหัสลับแบบควอนตัม

ธนาคารและโทรศัพท์มือถือดูเหมือนว่าไม่จำเป็นต้องมีการแจกแจงกุญแจแบบควอนตัม อย่างไรก็ตาม สำหรับการเข้ารหัสในปัจจุบัน หากมีการสร้างคอมพิวเตอร์ควอนตัมสำเร็จ เทคนิคการเข้ารหัสลับในปัจจุบันจะไม่ปลอดภัย เนื่องจากคอมพิวเตอร์ควอนตัมจะแก้ปัญหาทางคณิตศาสตร์บางอย่างด้วยความรวดเร็ว ทำให้ทำลายการเข้ารหัสลับได้ง่าย ปัจจุบันนักออกแบบการเข้ารหัสกำลังพัฒนารูปแบบการเข้ารหัสลับแบบใหม่ที่จะไม่ถูกทำลายได้โดยง่ายจากคอมพิวเตอร์ควอนตัม

## 5. แนวทางการพัฒนางานวิจัยการเข้ารหัสลับ

เราจะพัฒนางานวิจัยการเข้ารหัสลับโดยสมมุติว่ามีการสร้างคอมพิวเตอร์ควอนตัม ซึ่งแน่นอนว่าระบบการเข้ารหัสลับแบบเก่าบางอย่างถูกทำลายได้ง่าย เช่น Diffie และ Hellman [1], ElGamal [2] และ RSA [3] ฯลฯ แต่เราไม่จำเป็นต้องละทิ้งองค์ความรู้เก่าทั้งหมดเพื่อมาทำงานวิจัยการเข้ารหัสลับในยุคหลังมีคอมพิวเตอร์ควอนตัม ตัวอย่างเช่น เราใช้รูปแบบโครงสร้างหลักของการเข้ารหัสลับแบบเดิม แต่เปลี่ยนการเข้ารหัสบนพื้นฐานคอมพิวเตอร์ทั่วไปเป็นแบบการเข้ารหัสบนพื้นฐานคอมพิวเตอร์ควอนตัม จากงานวิจัยของ Woottters และ Zurek [6] ทำให้การทำลายการเข้ารหัสลับแบบควอนตัมได้ยาก และหากทำได้จะถูกตรวจสอบง่าย

**เอกสารอ้างอิง**

[1] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[2] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[3] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[4] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, 1st ed. Boca Raton, CRC Press, Inc., 1996.

[5] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Review*, vol. 41,

no. 2, pp. 303–332, 1999.

[6] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014.

ศาสตราจารย์ ดร.ภูมิ คำเอม
กองบรรณาธิการ