แนวทางการใช้จำนวนเต็มเกาส์เซียนกับวิทยาการเข้ารหัสลับอสมมาตรแบบคลาสสิกและแบบหลังควอนตัม

AN OVERVIEW OF GAUSSIAN INTEGER APPROACHES FOR CLASSICAL AND POST-QUANTUM ASYMMETRIC CRYPTOGRAPHY

วนารัตน์ จุฬพันธ์ทอง[1*] และ สุรเดช จิตประไพกุลศาล[2]

Wanarat Juraphanthong[1*] and Suradet Jitprapaikulsarn[2]

[1]สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏพิบูลสงคราม
อ.เมือง จ.พิษณุโลก ประเทศไทย 65000

[2]ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร
อ.เมือง จ.พิษณุโลก ประเทศไทย 65000

[1]Department of Computer Engineering, Faculty of Industrial Technology, Pibulsongkram Rajabhat University, Muang Phitsanulok, Phitsanulok, Thailand 65000

[2]Department of Electrical and Computer Engineering, Faculty of Engineering, Naresuan University, Muang Phitsanulok, Phitsanulok, Thailand 65000

* Corresponding author E-mail: wanaratj15@gr

วันที่เข้าระบบ 17 มิถุนายน 2563
วันที่แก้ไขบทความ 9 กรกฎาคม 2563
วันที่ตอบรับบทความ 9 กรกฎาคม 2563

บทคัดย่อ

วิทยาการเข้ารหัสลับอสมมาตร หรือวิทยาการเข้ารหัสลับกุญแจสาธารณะ เป็นมาตรการที่นิยมนำมาใช้ในการรักษาความมั่นคงของข้อมูล เนื่องจากเชื่อกันว่าการเข้ารหัสลับแบบนี้ยากต่อการถูกโจมตี แต่เมื่อมีการคิดค้นขั้นตอนวิธีการโจมตีที่ทำงานบนการประมวลผลควอนตัม ส่งผลให้การโจมตีการเข้ารหัสลับอสมมาตรแบบคลาสสิกไม่ใช่เรื่องยากอีกต่อไป จึงนำไปสู่การพัฒนาวิทยาการเข้ารหัสลับหลังควอนตัม การเข้ารหัสลับอสมมาตรแบบคลาสสิกและแบบหลังควอนตัมใช้เลขจำนวนเต็มมิติเดียวเป็นพื้นฐาน การนำคุณลักษณะของจำนวนเต็มเกาส์เซียนซึ่งมีสองมิติมาช่วยเพิ่มความซับซ้อนเพื่อให้การเข้ารหัสลับทนทานต่อการโจมตีจึงเป็นหัวข้อหนึ่งที่น่าสนใจ ในบทความนี้จึงได้รวบรวมแนวคิดการนำจำนวนเต็มเกาส์เซียนมาใช้กับวิทยาการเข้ารหัสลับอสมมาตรทั้งแบบคลาสสิกและแบบหลังควอนตัม

คำสำคัญ: วิทยาการเข้ารหัสลับกุญแจสาธารณะ, วิทยาการเข้ารหัสลับอสมมาตร, วิทยาการเข้ารหัสลับหลังควอนตัม, จำนวนเต็มเกาส์เซียน

Abstract

Asymmetric cryptography or public key cryptography is a popular measure employed to keep information secure. For a long time, it was thought to be very difficult to attack; hence, highly secure. However, the advent of quantum-based attacking algorithms drastically reduces the difficulties of attacking. This leads to the development of the post-quantum cryptography. Classical and post-quantum asymmetric cryptography systems are based on one-dimension integer. The utilization of Gaussian integer, a two-dimension number system, to enhance the complexity in order to resist the attacks is therefore an interesting topic. In this paper, we have surveyed and summarized the various approaches in applying Gaussian integer with classical and post-quantum cryptography.

Keywords: Asymmetric cryptography, Public key cryptography, Post-quantum cryptography, Gaussian integer

1. บทนำ

ในอนาคตอันใกล้การประมวลผลควอนตัมอาจไม่เป็นเพียงแนวคิดอีกต่อไป เนื่องจากในหลายปีที่ผ่านมา บริษัทเทคโนโลยีทั่วโลกได้แข่งขันกันพัฒนาควอนตัมคอมพิวเตอร์และให้การสนับสนุนงานวิจัยเกี่ยวกับการประมวลผลควอนตัมมาอย่างต่อเนื่อง การมาถึงของการประมวลผลควอนตัมนี้ทำให้วิทยาการเข้ารหัสลับหลังควอนตัม (Post-quantum cryptography) ได้รับความสนใจจากนักวิจัยมากขึ้นเช่นกัน เนื่องมาจากวิทยาการเข้ารหัสลับอสมมาตร (Asymmetric Cyptography) ที่นิยมใช้ในปัจจุบันเช่น RSA (Rivest *et al*., 1978) และ ElGamal (1985) มีจุดอ่อนที่เราสามารถใช้ขั้นตอนวิธี (Algorithm) ที่ทำงานบนการประมวลผลควอนตัมอย่างเช่น ขั้นตอนวิธีของ Shor (1997) มาโจมตีระบบให้สำเร็จภายในเวลาที่เป็นพหุนาม (Polynomial time) สถาบันแห่งชาติของมาตรฐานและเทคโนโลยี (NIST) ของสหรัฐอเมริกาจึงประกาศให้มีการนำเสนอวิทยาการเข้ารหัสลับหลังควอนตัมเพื่อจะนำมาคัดเลือกเป็นมาตรฐานการเข้ารหัสลับในปี ค.ศ. 2017 (Computer security division, 2017) คาดการณ์ว่าจะมีการประกาศผลระบบที่จะผ่านการคัดเลือกรอบที่ 3 ในราวกลางปี ค.ศ. 2020

วิทยาการเข้ารหัสลับส่วนใหญ่ตั้งอยู่บนฐานของจำนวนเต็มทั่วไปซึ่งมีมิติเดียว การนำจำนวนเต็มเกาส์เซียนที่มีสองมิติมาใช้ในการเข้ารหัสลับจึงเป็นแนวคิดหนึ่งที่มีนักวิจัยนำมาเพิ่มความซับซ้อนของการเข้ารหัสและถอดรหัส เพื่อทำให้การโจมตีวิทยาการเข้ารหัสลับนั้นทำได้ยากยิ่งขึ้น นอกจากนี้

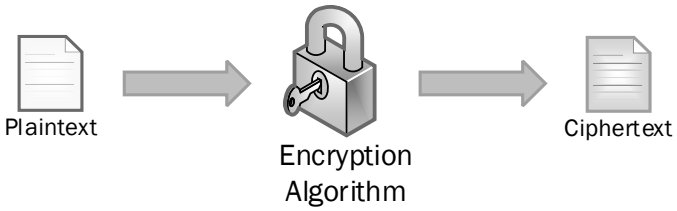
ยังมีงานวิจัยที่นำจำนวนเต็มเกาส์เซียนมาใช้ในการพัฒนาวิทยาการเข้ารหัสลับหลังควอนตัม ทำให้ระบบมีความทนทานต่อการโจมตีด้วยการประมวลผลควอนตัมมากขึ้น

ในบทความนี้ได้รวบรวมแนวคิดการใช้ประโยชน์จากจำนวนเต็มเกาส์เซียนสำหรับวิทยาการเข้ารหัสลับอสมมาตรที่นิยมใช้ในปัจจุบันและวิทยาการเข้ารหัสลับหลังควอนตัมที่กำลังได้รับความสนใจ เพื่อเป็นแนวทางสำหรับนักวิจัยที่สนใจในการพัฒนาวิทยาการเข้ารหัสลับให้มีประสิทธิภาพมากขึ้นและเพิ่มตัวเลือกของระบบที่จะนำไปใช้ป้องกันการโจมตีจากการประมวลผลควอนตัมในอนาคต โดยบทความแสดงวิทยาการเข้ารหัสลับอสมมาตรแบบคลาสสิกและแบบหลังควอนตัมโดยใช้ประโยชน์จากจำนวนเต็มเกาส์เซียน ซึ่งเป็นระบบจำนวนชนิดหนึ่งที่สามารถช่วยเพิ่มความซับซ้อนให้กับการโจมตีไปยังวิทยาการเข้ารหัสลับที่จะกล่าวถึงในหัวข้อต่อไป

2. วิทยาการเข้ารหัสลับ (Cryptography)

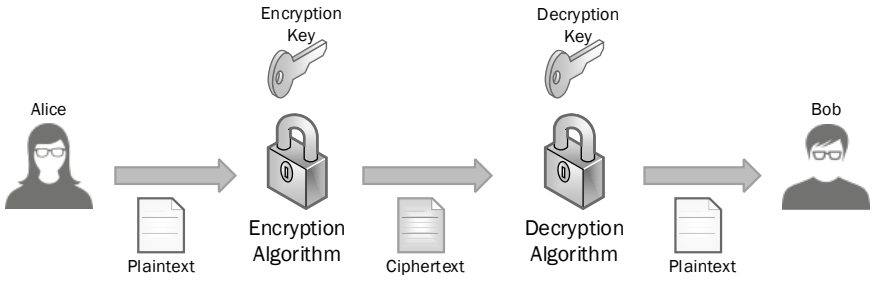
วิทยาการเข้ารหัสลับเป็นมาตรการความมั่นคงทางเทคนิคที่นำมาใช้ในการรักษาความน่าเชื่อถือและความมั่นคงของระบบสารสนเทศดังที่กล่าวถึงในโมเดล RMIAS (Cherdantseva & Hilton, 2013) ซึ่งสามารถบรรลุเป้าหมายหลายข้อ ตัวอย่างเช่น การรักษาความลับ (Confidentiality) การรักษาความสมบูรณ์ (Integrity) การตรวจสอบความน่าเชื่อถือ (Authenticity) และในการป้องกันการปฏิเสธ (Non-repudiation) เป็นต้น โดยการเข้ารหัสลับ แบ่งระบบออกเป็น 3 ประเภท ตามลักษณะของกุญแจที่ใช้ดังนี้

2.1 การเข้ารหัสลับแบบไม่ใช้กุญแจ (Unkeyed cryptography) คือระบบการเข้ารหัสที่ไม่ได้ใช้กุญแจ (Key) ดังภาพที่ 1 ซึ่งเป็นการเข้ารหัสข้อความให้เป็นข้อความลับด้วยวิธีการที่ยากหรือไม่สามารถถอดรหัสข้อความกลับได้ เช่น การเข้ารหัสแบบทางเดียว (One-way function) ฟังก์ชันแบบแฮช (Hashing function) ตัวอย่างมาตรฐานที่ใช้ระบบแบบไม่ใช้กุญแจ ได้แก่ MD5, SHA-1 และ CRC32 เป็นต้น



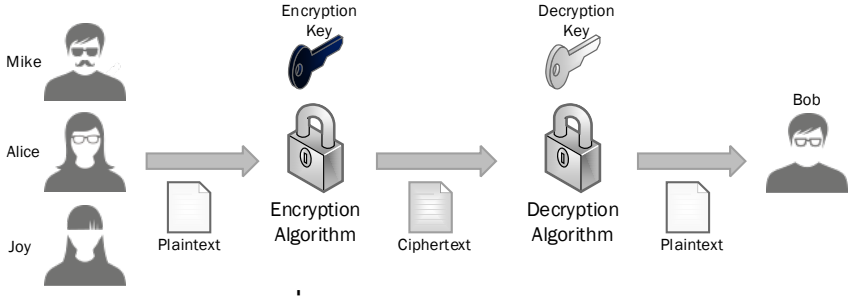
ภาพที่ 1 การเข้ารหัสแบบไม่ใช้กุญแจ

2.2 การเข้ารหัสลับสมมาตร (Symmetric cryptography) คือระบบการเข้ารหัสที่ใช้กุญแจลับ (Secret key) ในการเข้ารหัสข้อมูล ซึ่งจะใช้กุญแจดอกเดียวกันทั้งในการเข้ารหัสข้อความปกติให้เป็นข้อความลับ และถอดรหัสข้อความลับให้กลับเป็นข้อความปกติ ทำให้ผู้ที่ไม่มีกุญแจไม่สามารถเข้าใจข้อความลับได้ ดังภาพที่ 2 โดยตัวอย่างมาตรฐานที่ใช้ระบบแบบสมมาตร ได้แก่ DES, 3DES และ AES เป็นต้น



ภาพที่ 2 การเข้ารหัสลับสมมาตร

2.3 การเข้ารหัสลับอสมมาตร (Asymmetric cryptography) คือวิทยาการเข้ารหัสลับที่กุญแจในการเข้ารหัส และกุญแจในการถอดรหัสเป็นคนละดอกกัน โดยปกติแล้วผู้ใช้จะเผยแพร่กุญแจที่ใช้ในการเข้ารหัสลับสู่สาธารณะ นั่นคือเป็นกุญแจสาธารณะ (Public key) และจะใช้กุญแจอีกดอกหนึ่งซึ่งเก็บเป็นความลับ นั่นคือเป็นกุญแจลับ (Private key) ในการถอดรหัสข้อความลับกลับเป็นข้อความเดิม ดังภาพที่ 3 ทำให้เรียกการเข้ารหัสลับแบบนี้อีกอย่างหนึ่งว่าการเข้ารหัสลับกุญแจสาธารณะ (Public key cryptography) ตัวอย่างมาตรฐานที่ใช้ระบบแบบอสมมาตร ได้แก่ DSS และ RSA เป็นต้น



ภาพที่ 3 การเข้ารหัสลับอสมมาตร

จากคุณลักษณะที่แตกต่างกันของวิทยาการเข้ารหัสลับทั้งสามประเภทข้างต้น ทำให้วิทยาการเข้ารหัสลับแบบไม่ใช้กุญแจมักจะนำไปใช้สำหรับการเข้ารหัสที่ไม่ต้องการการถอดรหัสกลับ เช่น การเข้ารหัส MD5 บนรหัสผ่านสำหรับตรวจสอบการลงชื่อเข้าใช้ระบบ เป็นต้น ส่วนระบบแบบสมมาตร

และอสมมาตรมักจะนำไปใช้ในการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ตที่ต้องมีการเข้ารหัสและถอดรหัสข้อความกลับ เช่น การประยุกต์ใช้ในระบบลายเซ็นดิจิทัลเพื่อตรวจสอบตัวตนที่แท้จริงของผู้ส่งข้อความ เป็นต้น

นอกจากนี้ยังทำให้ระบบแต่ละประเภทมีข้อดีและข้อจำกัดแตกต่างกันไป ดังเช่น ระบบแบบไม่ใช้กุญแจและแบบสมมาตรมีข้อดีคือ ใช้เวลาในการเข้ารหัสหรือถอดรหัสข้อความน้อยกว่าระบบแบบอสมมาตร เนื่องจากใช้ขั้นตอนวิธีที่มีความซับซ้อนน้อยกว่า อย่างไรก็ตามข้อจำกัดของระบบแบบสมมาตรคือความยุ่งยากในการแลกเปลี่ยนกุญแจระหว่างกัน เนื่องจากต้องใช้กุญแจหลายคู่เมื่อจำเป็นต้องแลกเปลี่ยนข้อมูลกับผู้ใช้หลายกลุ่ม รวมถึงปัญหาในการรักษาความปลอดภัยของกุญแจ เนื่องจากคู่กุญแจลับไม่อาจเปิดเผยให้ผู้อื่นรู้ได้ ส่วนระบบแบบอสมมาตรออกแบบมาเพื่อให้เผยแพร่กุญแจเข้ารหัสไปยังสาธารณะได้ ทำให้มีข้อดีคือขจัดปัญหาด้านความปลอดภัยระหว่างการแลกเปลี่ยนคู่กุญแจลับ และใช้กุญแจเพียงคู่เดียวเมื่อต้องการแลกเปลี่ยนข้อมูลกับผู้ใช้หลายกลุ่ม ดังสรุปในตารางที่ 1

ตารางที่ 1 ข้อดีของการเข้ารหัสลับแบบต่าง ๆ

ข้อดี	การเข้ารหัสลับ		
	ไม่ใช้กุญแจ	สมมาตร	อสมมาตร
1. ถอดรหัสข้อความลับกลับเป็นข้อความได้	✗	✓	✓
2. การเข้ารหัส/ถอดรหัสข้อมูลใช้เวลาน้อย	✓	✓	✗
3. ไม่มีการแลกเปลี่ยนกุญแจระหว่างผู้ใช้	✓	✗	✓

3. ระบบเข้ารหัสลับอสมมาตรแบบคลาสสิก

การเข้ารหัสลับอสมมาตรเป็นระบบการเข้ารหัสที่ใช้กุญแจแบบอสมมาตร กล่าวคือใช้คู่กุญแจในการเข้ารหัสและถอดรหัสคนละดอกกัน โดยสามารถเผยแพร่กุญแจเข้ารหัสไปยังสาธารณะได้ ดังที่กล่าวไปข้างต้น ซึ่งระบบออกแบบมาเพื่อขจัดปัญหาด้านความปลอดภัยระหว่างการแลกเปลี่ยนคู่กุญแจลับบนระบบแบบสมมาตรที่ไม่อาจเปิดเผยให้ผู้อื่นรู้ได้ อย่างไรก็ตามข้อจำกัดของระบบแบบอสมมาตรคือความซับซ้อนของขั้นตอนวิธีการเข้ารหัสและถอดรหัส ทำให้ที่ผ่านมาระบบมักจะนำไปใช้กับการเข้ารหัสเฉพาะข้อความสำคัญหรือเข้ารหัสกุญแจลับที่ต้องการแลกเปลี่ยนกันระหว่างผู้ใช้ โดยการเข้ารหัสลับอสมมาตรนั้น สามารถแบ่งประเภทโดยอาศัยพื้นฐานของปัญหา หรือสมมติฐานความยาก ที่กำหนดความซับซ้อนของระบบเพื่อป้องกันการถอดรหัสของผู้โจมตี ซึ่งการเข้ารหัสลับที่นิยมใช้ในปัจจุบัน ได้มีการใช้เลขจำนวนเต็มเกาส์เซียนมาปรับปรุงประสิทธิภาพของระบบดังนี้

3.1 ปัญหาการแยกตัวประกอบจำนวนเต็ม (Integer factorization problem: IFP) ตัวอย่างวิทยาการเข้ารหัสลับอสมมาตรที่อยู่บนพื้นฐานปัญหานี้คือ ระบบการเข้ารหัส RSA นำเสนอโดย Revist Shamar และ Adleman ที่อาศัยความยากในการแยกตัวประกอบของจำนวนเฉพาะสร้างความซับซ้อนในการถอดรหัสข้อความ ต่อมามีการปรับปรุงประสิทธิภาพของระบบให้ดียิ่งขึ้นโดยการประยุกต์ใช้จำนวนเต็มเกาส์เซียน ดังเช่น Pradhan (2013) นำเสนอขั้นตอนวิธีโดยใช้จำนวนเต็มเกาส์เซียนแทนที่การใช้จำนวนเต็มบนระบบเข้ารหัสแบบ RSA ซึ่งผลจากการปรับเปลี่ยนตัวแปรนี้พบว่าช่วยให้ระบบมีความปลอดภัยมากขึ้นเมื่อเปรียบเทียบกับระบบเดิม เนื่องจากมีขอบเขตที่มากขึ้นในการสร้างข้อความเพื่อเข้ารหัส อีกทั้งยังเพิ่มจำนวนกุญแจให้เลือกใช้ได้มากขึ้น ทำให้ผู้โจมตีต้องใช้ความพยายามมากขึ้นในการถอดรหัสข้อความ และค้นหากุญแจ

3.2 ปัญหาลอการิทึมไม่ต่อเนื่อง (Discrete logarithm problem: DLP) ตัวอย่างวิทยาการเข้ารหัสลับอสมมาตรที่อยู่บนพื้นฐานปัญหานี้คือ ระบบ ElGamal ที่อาศัยความยากในการแก้ปัญหาลอการิทึมไม่ต่อเนื่องสร้างความซับซ้อนในการถอดรหัสข้อความ ซึ่งระบบนี้มีผู้วิจัยนำจำนวนเต็มเกาส์เซียนมาปรับปรุงประสิทธิภาพเช่นกัน ดังเช่น Elkamchouchi *et al*. (2003) ได้นำเสนอเทคนิคใหม่ในการเข้ารหัสแบบอสมมาตรโดยใช้การผสมผสานระหว่างระบบแบบ IFP และ DLP บนโดเมนของจำนวนเต็มเกาส์เซียน ซึ่งเทคนิคนี้ช่วยให้มีความปลอดภัยมากขึ้นและช่วยลดความซับซ้อนในการคำนวณเมื่อเปรียบเทียบกับการเข้ารหัสแบบ RSA และ ElGamal นอกจากนี้ Koval (2016) ได้นำเสนอขั้นตอนวิธีการยกกำลังจำนวนเต็มเกาส์เซียนสำหรับนำไปใช้ในระบบการเข้ารหัสแบบ DLP โดยใช้ความสัมพันธ์ระหว่างจำนวนเต็มเกาส์เซียนและ Lucas sequences ซึ่งช่วยเพิ่มประสิทธิภาพการประมวลผลเมื่อเปรียบเทียบกับขั้นตอนวิธีเดิมที่เป็นการยกกำลังจำนวนเต็ม

3.3 ปัญหาลอการิทึมไม่ต่อเนื่องเส้นโค้งเชิงวงรี (Elliptic curve discrete logarithm problem: ECDLP) ตัวอย่างวิทยาการเข้ารหัสลับอสมมาตรที่อยู่บนพื้นฐานปัญหานี้คือ ระบบ ECC (Miller, 1985) ซึ่งมีความซับซ้อนในการถอดรหัสข้อความของระบบอยู่บนพื้นฐานความยากในการแก้ปัญหาลอการิทึมไม่ต่อเนื่องเส้นโค้งเชิงวงรี ต่อมา Mohamed & Elkamchouchi (2009) ได้นำเสนอวิธีการเพื่อปรับปรุงระบบ ECC โดยใช้จำนวนเต็มเกาส์เซียนแทนที่จำนวนเต็มแบบเดิมจำนวนของจุดที่สามารถใช้ได้มากขึ้นบนเส้นโค้งเชิงวงรี ทำให้ระบบมีความปลอดภัยมากขึ้น อย่างไรก็ตามพบว่าการใช้กุญแจที่เป็นจำนวนเต็มเกาส์เซียนต้องใช้พื้นที่มากขึ้นในการจัดเก็บเช่นกัน

4. วิทยาการเข้ารหัสลับหลังควอนตัม

การเข้ารหัสลับที่ทนทานต่อการประมวลผลควอนตัมหรือที่นิยมเรียกว่าวิทยาการเข้ารหัสลับหลังควอนตัม (Post-quantum cryptography) ได้รับความสนใจจากนักวิจัยในไม่กี่ปีที่ผ่านมา เนื่องจากการพัฒนาอย่างต่อเนื่องของควอนตัมคอมพิวเตอร์ และขั้นตอนวิธีบนการประมวลผล

ควอนตัมที่สามารถโจมตีวิทยาการเข้ารหัสลับที่นิยมใช้ในปัจจุบัน ซึ่งเป็นระบบบนพื้นฐานปัญหา IFP DLP และ ECDLP ที่กล่าวไปแล้วข้างต้นได้อย่างมีประสิทธิภาพ โดยการเข้ารหัสแบบอสมมาตรที่ทนทานต่อการประมวลผลควอนตัมนั้น สามารถแบ่งประเภทโดยอาศัยพื้นฐานของปัญหาหรือสมมติฐานความยาก ซึ่งในบทความนี้จะนำเสนอเฉพาะประเภทที่ได้รับความสนใจและเป็นระบบที่เข้าร่วมในการสร้างมาตรฐานสำหรับวิทยาการเข้ารหัสลับหลังควอนตัมของ NIST โดยพบว่าแต่ละระบบมีผู้วิจัยนำเสนอการปรับปรุงประสิทธิภาพด้วยวิธีการต่าง ๆ รวมถึงการใช้เลขจำนวนเต็มเกาส์เซียน ดังนี้

4.1 ปัญหาสมการพหุนามหลายตัวแปรบนเซตจำกัด (Multivariate quadratic polynomial problem: MQP) เป็นวิทยาการเข้ารหัสลับประเภท Multivariate-based อยู่บนพื้นฐานความยากในการแก้ปัญหาสมการพหุนามหลายตัวแปรบนเซตจำกัด จัดอยู่ในกลุ่มความซับซ้อนของปัญหา NP-hard ตัวอย่างของระบบคือ ระบบการเข้ารหัส Hidden field equation (HFE) นำเสนอโดย Patarin (1996) ซึ่งเป็นการสร้างกุญแจสาธารณะจากสมการพหุนามที่ยากต่อการอินเวิร์สหากไม่ทราบสมการพหุนามที่เป็นกุญแจลับ และ Rainbow (Ding & Schmidt, 2005) ซึ่งเป้นระบบลายเซ็นต์ดิจิทัลที่ใช้คุณลักษณะของสมการพหุนามหลายตัวแปรเช่นกัน แต่เนื่องด้วยระบบมีข้อจำกัดคือความซับซ้อนในการคำนวณสมการพหุนามหลายตัวแปร การปรับปรุงระบบจึงเน้นไปที่ลดความซับซ้อนเพื่อให้การเข้ารหัสและถอดรหัสมีความรวดเร็ว เช่น การใช้ Groebner Basis เป็นต้น

4.2 ปัญหาเวกเตอร์ที่สั้นที่สุดบนแลตทิซ (Shortest vector problem: SVP) เป็นวิทยาการเข้ารหัสลับประเภท Lattice-based อยู่บนพื้นฐานความยากในการหาเวกเตอร์ที่สั้นที่สุดบนแลตทิซของกุญแจลับของระบบ ซึ่งอยู่ในกลุ่มความซับซ้อนของปัญหา NP-hard ตัวอย่างของระบบคือ ระบบการเข้ารหัส NTRU นำเสนอโดย Hoffstein *et al*. (1998) ซึ่งระบบ NTRU อยู่บนพื้นฐานของแลทติซ โดยสมการพหุนามดีกรี N-1 ที่มีสัมประสิทธิ์เป็นจำนวนเต็มบนริง ดังสมการที่ 1

$$R=Z[x]/(X^N -1) \quad (1)$$

การเพิ่มระดับความปลอดภัยของระบบสามารถทำได้หลายรูปแบบ ดังเช่น วิธีแรกคือการเปลี่ยนไปใช้สมการพหุนามสองตัวแปร (Caboara *et al*., 2008) ซึ่งทำให้ยากขึ้นในการคาดเดากุญแจลับ วิธีที่สองคือการเพิ่มดีกรีของสมการพหุนาม อย่างไรก็ตามวิธีการนี้ทำให้ระบบต้องใช้เวลามากขึ้นในการคำนวณ นักวิจัยจึงพยายามแก้ปัญหาดังกล่าวโดยการปรับปรุงขั้นตอนวิธีในการหาอินเวิร์สของสมการพหุนาม(Zhao & Su, 2011; Nyokabi *et al*., 2017) และการใช้เมทริกซ์แทนสมการพหุนาม (Nayak *et al*., 2012) เป็นต้น วิธีที่สามคือ การใช้สัมประสิทธิ์ของสมการพหุนามเป็นจำนวนประเภทอื่นแทนที่จำนวนเต็ม ซึ่งมีการนำจำนวนเต็มเกาส์เซียนมาใช้ปรับปรุงระบบด้วย เช่น Nanda *et al*. (2015) ใช้จำนวนเต็มเกาส์เซียนและใช้การคำนวณบนเมทริกซ์แทนสมการพหุนามบน NTRU วิธีการนี้เพิ่มฟิล์ดในการสร้างกุญแจ ทำให้ผู้โจมตีต้องใช้ความพยายามมากขึ้นในการคาดเดากุญแจ

แม้จำนวนเต็มเกาส์เซียนทำให้ต้องคำนวณอย่างซับซ้อนมากขึ้น แต่การใช้เมทริกซ์ก็สามารถช่วยลดความซับซ้อนบนระบบลงได้ นอกจากจำนวนเต็มเกาส์เซียนแล้ว ยังมีการนำเสนอจำนวนประเภทอื่นเพื่อปรับปรุงระบบ NTRU เช่น การใช้จำนวน Kleinian (Thakur *et al*., 2017) จำนวน Eisenstein (Jarvis & Nevins, 2015) จำนวน Quaternion (Bagheri *et al*., 2017) และจำนวนOctonion (Malekian & Zakerolhosseini, 2010; Bagheri & Sadeghi, 2015) เป็นต้น

4.3 ปัญหาชุดข้อมูลความผิดพลาดบนรหัสบล็อกเชิงเส้น (Syndrome decoding problem: SDP) เป็นระบบการเข้ารหัสประเภท Code-based ที่อยู่บนพื้นฐานความยากในการหาชุดข้อมูลความผิดพลาดบนรหัสบล็อกเชิงเส้น สมมติฐานความยากของระบบนี้อยู่ในกลุ่มความซับซ้อนของปัญหา NP-complete ข้อดีของระบบนี้คือการเข้ารหัสและถอดรหัสมีความรวดเร็ว ตัวอย่างของระบบคือ ระบบการเข้ารหัส McEliece (1978) โดยใช้รหัส Goppa เป็นรหัสเชิงเส้นแก้ไขข้อผิดพลาดสำหรับการเข้ารหัสและถอดรหัสบนระบบ สร้างจากสมการพหุนาม g(x) ดีกรี t บนเซตจำกัด GF(p) เนื่องจากระบบ McEliece มีข้อเสียเรื่องของขนาดของกุญแจที่มากกว่าระบบอื่น ดังนั้นการปรับปรุงระบบจึงให้ความสำคัญกับการเลือกใช้รหัสแบบอื่น ๆ เพื่อต้องการลดขนาดของกุญแจของระบบลง ซึ่งหมายถึงการทำให้ระบบมีระดับความปลอดภัยที่มากขึ้นเมื่อเทียบกับขนาดของกุญที่เท่ากัน โดยรหัสที่นำเสนอเป็นรหัสที่อยู่บนฐานของจำนวนเต็ม ยกตัวอย่างเช่น การใช้รหัส Reed-Muller (Sidelnikov, 1994) รหัส Generalized Reed-Solomon (Niederreiter, 1986) รหัส LDPC (Monico *et al*., 2000) QC-LDPC (Baldi *et al*., 2008) รหัส MDPC และ QC-MDPC (Misoczki et al., 2013) และสุดท้ายรหัส Polar (Shrestha & Kim, 2014; Hooshmand *et al*., 2017) เป็นต้น

5. การใช้ประโยชน์จากจำนวนเต็มเกาส์เซียน

จากการรวบรวมแนวคิดของวิทยาการเข้ารหัสลับอสมมาตรสามารถสรุปได้ดังตารางที่ 2 โดยพบว่ามีการใช้ประโยชน์จากจำนวนเต็มเกาส์เซียนบนวิทยาการเข้ารหัสลับแบบคลาสสิกทั้ง 3 ประเภท คือ IFP DLP และ ECDLP ซึ่งการใช้จำนวนเต็มเกาส์เซียนนี้ ได้เพิ่มประสิทธิภาพในด้านความปลอดภัยและด้านการประมวลผลของระบบ อย่างไรก็ตามด้วยข้อจำกัดของระบบแบบเดิมซึ่งสามารถถูกโจมตีด้วยขั้นตอนวิธีบนการประมวลควอนตัม ระบบที่ทนทานต่อการประมวลผลควอนตัมจึงเป็นอีกทางเลือกหนึ่ง ซึ่งนักวิจัยได้ให้ความสนใจ และพยายามปรับปรุงระบบ โดยพบว่าระบบประเภท MQP ยังไม่มีการนำเลขจำนวนเต็มเกาส์เซียนมาใช้ ส่วนระบบประเภท SVP นอกจากการนำจำนวนเต็มเกาส์เซียนมาใช้แล้ว ยังมีการนำเลขแบบอื่น ๆ มาใช้เพื่อเพิ่มประสิทธิภาพอีกด้วย สุดท้ายระบบประเภท SDP ผู้วิจัยส่วนมากเน้นไปที่การนำรหัสชนิดต่าง ๆ ซึ่งยังคงเป็นรหัสที่อยู่บนฐานของจำนวนเต็มแบบมิติเดียว ยังไม่มีการนำรหัสที่ใช้จำนวนเต็มเกาส์เซียนมาใช้เช่นกัน

ตารางที่ 2 การใช้ประโยชน์จากเลขจำนวนเต็มเกาส์เซียนบนวิทยาการเข้ารหัสลับอสมมาตร

ประเภทของวิทยาการเข้ารหัสลับ	ตัวอย่างระบบ	ทนทานต่อควอนตัม	ใช้ประโยชน์จากเกาส์เซียน
IFP	RSA	✗	✓
DLP	Elgamal	✗	✓
ECDLP	ECC	✗	✓
MQP	HFE, Rainbow	✓	✗
SVP	NTRU	✓	✓
SDP	McEliece	✓	✗

6. สรุป

บทความนี้ชี้ให้เห็นว่า มีนักวิจัยได้ใช้ประโยชน์จากเลขจำนวนเต็มเกาส์เซียนเพื่อเพิ่มประสิทธิภาพทั้งด้านความปลอดภัย และด้านการประมวลผลของวิทยาการเข้ารหัสลับอสมมาตรในหลายวิธีการ โดยนำไปใช้กับระบบแบบคลาสสิกที่นิยมใช้งานอยู่ในปัจจุบันอย่างเช่นระบบ RSA Elgamal และ ECC ซึ่งเป็นระบบประเภท IFP DLP และ ECDLP ตามลำดับ และนำไปใช้กับบางระบบ บนระบบแบบทนทานต่อการประมวลผลควอนตัม ซึ่งเป็นระบบที่กำลังได้รับความสนใจ เช่น บนระบบ NTRU ซึ่งเป็นระบบประเภท SVP อย่างไรก็ตามพบว่ายังไม่มีงานวิจัยที่นำเสนอการใช้ประโยชน์จากจำนวนเต็มเกาส์เซียน บนระบบประเภท MQP และ SDP มากนัก ซึ่งเป็นแนวทางสำหรับการวิจัยและพัฒนาวิธีการเพื่อนำมาใช้ปรับปรุงประสิทธิภาพของระบบสำหรับป้องกันการโจมตีที่เกิดขึ้นบนควอนตัมคอมพิวเตอร์ในอนาคต

7. เอกสารอ้างอิง

Bagheri, K. , & Sadeghi, M.-R. (2015). A new non-associative cryptosystem based on NTOW public key cryptosystem and octonions algebra. **ACM Communications in Computer Algebra**, 49(1), 13.

Bagheri, K., Sadeghi, M.-R., & Panario, D. (2017). A non-commutative cryptosystem based on quaternion algebras. **Designs, Codes and Cryptography**, 86(10), 2345–2377.

Baldi, M., Bodrato, M., & Chiaraluce, F. (2008). A new analysis of the McEliece cryptosystem based on QC-LDPC codes. **Security and Cryptography for Networks**, 246–262.

Caboara, M., Caruso, F., & Traverso, C. (2008). GröBner bases for public key cryptography. **Proceedings of the Twenty-First International Symposium on Symbolic and Algebraic Computation,** 315–324.

Cherdantseva, Y., & Hilton, J. (2013). A reference model of Information assurance security. **2013 International Conference on Availability, Reliability and Security**, 546–555.

Computer Security Division. (2017). **Post-quantum cyptography | CSRC. CSRC | NIST**. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

Ding, J., & Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In J. Ioannidis, A. Keromytis, & M. Yung (Eds.), **Applied Cryptography and Network Security**, 164–175.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. **IEEE Transactions on Information Theory**, 31(4), 469–472.

Elkamchouchi, H., Elshenawy, K., & Shaban, H. A. (2003). Two new public key techniques in the domain of Gaussian integers. **Radio Science Conference, 2003. NRSC 2003. Proceedings of the Twentieth National**, C17-1–8.

Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. **Proceedings of the Third International Symposium on Algorithmic Number Theory**, 267–288.

Hooshmand, R., Shooshtari, M. K., & Aref, M. R. (2017). PKC-PC: A variant of the McEliece public key cryptosystem based on polar codes. **Computing Research Repository (CoRR)**, 1712.07672, 1-11.

Jarvis, K., & Nevins, M. (2015). ETRU: NTRU over the Eisenstein integers. **Designs, Codes and Cryptography**, 74(1), 219–242.

Koval, A. (2016). Algorithm for gaussian integer exponentiation. **Information Technology: New Generations** (pp. 1075–1085). Springer.

Malekian, E., & Zakerolhosseini, A. (2010). OTRU: A non-associative and high speed public key cryptosystem. **15th CSI International Symposium on Computer Architecture and Digital Systems**, 83–90.

Mceliece, R. (1978). A public-key cryptosystem based on algebraic coding theory. **JPL DSN Progress Report**, 44.

Miller, V. S. (1985). Use of elliptic curves in cryptography. **Advances in Cryptology - CRYPTO '85 Proceedings**, 417–426.

Misoczki, R., Tillich, J. P., Sendrier, N., & Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. **IEEE International Symposium on Information Theory**, 2069–2073.

Mohamed, E., & Elkamchouchi, H. (2009). Elliptic curve cryptography over gaussian integers. **IJCSNS International Journal of Computer Science and Network Security**, 9, 413–416.

Monico, C., Rosenthal, J., & Shokrollahi, A. (2000). Using low density parity check codes in the McEliece cryptosystem. **IEEE International Symposium on Information Theory**, 215.

Nanda, A. K., Nayak, R., & Awasthi, L. K. (2015). NTRU with gaussian integer matrix. **International Journal of Advanced Research in Computer Science and Software Engineering**, 5(2), 359–365.

Nayak, R., Pradha, J., & Sastry, C. V. (2012). Evaluation of performance characteristics of polynomial based and Lattice based NRTU cryptosystem. **ACEEE International Journal on Network Security**, 3, 1–4.

Niederreiter, H. (1986). Knapsack type cryptosystems and algebraic Coding theory. **Problems of Control and Information Theory**, 15(2), 157–166.

Nyokabi, G. J., Salleh, M., & Mohamad, I. (2017). NTRU inverse polynomial algorithm based on circulant matrices using gauss-jordan elimination. **2017 6th ICT International Student Project Conference**, 1–5.

Patarin, J. (1996). Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. **Advances in Cryptology - EUROCRYPT,** 96, 33–48.

Pradhan, S. (2013). A modified variant of RSA algorithm for gaussian integers. **International Journal of Information and Network Security**, 2.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, 21(2), 120–126.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM Journal on Computing**, 26(5), 1484–1509.

Shrestha, S. R., & Kim, Y. S. (2014). New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. **2014 14th International Symposium on Communications and Information Technologies**, 368–372.

Sidelnikov, V. M. (1994). A public-key cryptosystem based on binary Reed-Muller codes. **Discrete Mathematics and Applications**, 4(3), 191–208.

Thakur, K., Tripathi, B. P., & Yadav, M. R. (2017). KTRU: NTRU over the Kleinian integers. **Journal of International Academy of Physical Sciences**, 20(3), 177–183.

Zhao, N., & Su, S. (2011). An improvement and a new design of algorithms for seeking the inverse of an NTRU polynomial. **Seventh International Conference on Computational Intelligence and Security**, 891–895.