การรักษาความปลอดภัยฐานข้อมูลบนข้อมูลที่ถูกเข้ารหัสโดยการเข้ารหัสแบบสาทิสสัณฐาน

วันที่รับบทความ	01/07/2560
วันแก้ไขบทความ	20/10/2560
วันตอบรับบทความ	19/11/2562

ธัญพร ศรีดอกไม้[1]

บทคัดย่อ

แนวคิดในการรักษาความมั่นคงปลอดภัยของข้อมูลได้มีผู้คิดค้นการเข้ารหัสมากมายเพื่อใช้ในการปกป้องข้อมูลทั้งส่วนตัวและขององค์กร เนื่องจากวิธีการรักษาความมั่นคงปลอดภัยที่มีอยู่เดิมอาจไม่เพียงพอ เช่น ข้อมูลถูกเรียกดูโดย DBA ทำให้ความลับของข้อมูลถูกโจมตีจากผู้ไม่หวังดี โดยการถอดรหัสข้อมูลจากฐานข้อมูลแล้วเปลี่ยนแปลงหรือนำความลับไปเผยแพร่อาจทำให้เกิดปัญหาร้ายแรงได้ บทความฉบับนี้ เป็นการนำเสนอหลักการของวิธีการรักษาความปลอดภัยฐานข้อมูลบนข้อมูลที่ถูกเข้ารหัสโดยการเข้ารหัสแบบสาทิสสัณฐานซึ่งเป็นวิธีการหนึ่งซึ่งมีความปลอดภัยที่อยู่ในระดับที่สูงและเป็นที่ยอมรับกันอย่างกว้างขวางในเรื่องของความปลอดภัยเพราะด้วยคุณสมบัติที่สามารถป้องกันผู้ที่ไม่หวังดีจากภายในและภายนอกได้ เนื่องจากมีความซับซ้อนของระบบตัวเลขที่นำมาใช้ในการเข้ารหัสสูงจึงถูกนำมาใช้อย่างแพร่หลายกับข้อมูลที่มีความสำคัญ

คำสำคัญ: การเข้ารหัส การเข้ารหัสแบบโฮโมมอฟิค ความมั่นคงปลอดภัยของระบบสารสนเทศ

[1] อาจารย์ประจำหลักสูตรบริหารธุรกิจบัณฑิต สาขา คอมพิวเตอร์ธุรกิจ มหาวิทยาลัยราชภัฏธนบุรี
อีเมล: tanyaporn.s@dru.ac.th.

_ 13 2 -- 2562.indd 224 23/12/2562 9:51:59

Security Database on Encrypted Data Using Homomorphic Encryption

Received	01/07/2560
Revised	20/10/2560
Accepted	19/11/2562

Tanyaporn Sridokmai[1]

Abstract

Based on the concept of data security, many encryption methods have been invented to protect both personal and corporate information because the available security methods may not be sufficient. For example, the data is retrieved by DBA and that results in confidential information being attacked by malicious users. Decrypting data from the database and changing or distributing confidentiality can cause serious problems.

This article presents the principles of database security methods in data encrypted by amorphous encryption, which has a high level of security and is widely accepted in terms of security. As its features can prevent ill-intentioned users internally and externally due to a high complexity of the coding system used in encryption, it is widely used for sensitive data.

Keywords: cryptography, homomorphic encryption, information security

[1] Lecturer, Business Administration Program, Business Computer Department, Dhonburi Rajabhat University
e-mail: tanyaporn.s@dru.ac.th.

บทนำ

ปัจจุบันเป็นยุคที่ข้อมูลและสารสนเทศมีบทบาทสำคัญของทุกภาคส่วนไม่ว่าจะเป็นองค์กรภาครัฐหรือองค์กรภาคเอกชนทั้งขนาดเล็กหรือขนาดใหญ่ การพัฒนาอย่างรวดเร็วของเทคโนโลยีสื่อสารทำให้ข้อมูลข่าวสารกลายเป็นปัจจัยสำคัญในการพัฒนาเศรษฐกิจและสังคมของประเทศ การแข่งขันทางธุรกิจที่จะประสบความสำเร็จในยุคนี้จำเป็นต้องอาศัยสารสนเทศที่มีความถูกต้องแม่นยำ มีความรวดเร็วในการตัดสินใจและยังจำเป็นต้องมีฐานข้อมูลที่มั่นคงปลอดภัย บทความฉบับนี้ได้นำเสนอวิธีการการรักษาความมั่นคงปลอดภัยให้กับฐานข้อมูลบนข้อมูลที่ถูกเข้ารหัสเพื่อแก้ไขปัญหาการรั่วไหลของข้อมูลอันเกิดจากการทุจริตของผู้บริหารข้อมูลโดยใช้เทคนิคการเข้ารหัสแบบ Homomorphic Encryption ประโยชน์ที่จะได้รับ คือการช่วยลดความเสี่ยงและความเสียหายที่เกิดจากการขโมยและการใช้งานระบบในทางที่ผิดและทำให้ว่าผู้ใช้หรือผู้มีส่วนเกี่ยวข้องมั่นใจในระบบรักษาความปลอดภัย สามารถปกป้องข้อมูลของตนจากภัยทั้งภายในและภายนอกองค์กรส่งผลให้ทำงานได้อย่างมีประสิทธิภาพดีขึ้นกว่าเดิม

แนวความคิดในการรักษาความมั่นคงปลอดภัยของข้อมูล

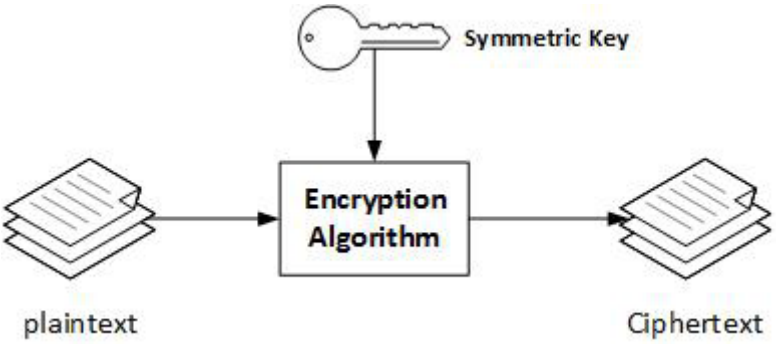
ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) มีจุดเริ่มต้นมาจากความต้องการความปลอดภัยของคอมพิวเตอร์ (Computer Security) เนื่องจากในยุคแรกภัยคุกคามส่วนใหญ่เป็นภัยคุกคามทางกายภาพ เช่น การลักขโมยอุปกรณ์ การก่อวินาศกรรมและการโจรกรรมผลผลิตที่ได้จากระบบ เป็นต้น ต่อมาเมื่อเทคโนโลยีคอมพิวเตอร์และการสื่อสารมีความก้าวหน้ามากขึ้นจึงเกิด ภัยคุกคามหลายรูปแบบ เช่น การโจรกรรมข้อมูลที่เป็นความลับ การลักลอบเข้าสู่ระบบโดยไม่ได้รับอนุญาต ตลอดจนการทำลายระบบด้วยวิธีต่าง ๆ ซึ่งก่อให้เกิดความเสียหายทั้งต่อบุคคลและทรัพย์สินอย่างมาก จึงต้องมีการกำหนดขอบเขตของความมั่นคงปลอดภัยคอมพิวเตอร์จึงมีเพิ่มขึ้น โดยให้ครอบคลุมถึงความปลอดภัยของข้อมูล การจำกัดการเข้าถึงข้อมูล และการจำกัดระดับความเกี่ยวข้องกับข้อมูลของคนในองค์กรด้วย ซึ่งขอบเขตที่เพิ่มเติมเข้ามาเหล่านี้เพื่อเสริม “ความมั่นคงปลอดภัยของสารสนเทศ”(ศิริพร อ่องรุ่งเรือง, 2560)

ในช่วงหลายปีที่ผ่านมาความต้องการการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนตัวและข้อมูลขององค์นั้นมีความสูงมากขึ้นตามความก้าวหน้าของเทคโนโลยีการสื่อสารที่มีเพิ่มมากขึ้นทั้งในส่วนของเครื่องมือและเครือข่ายที่ใช้จึงทำให้มีวิธีหรืออัลกอริทึม (Algorithm) ในการรักษาความมั่นคงปลอดภัยออกมาหลากหลายมากขึ้น(เพ็ญศรี ปักกะสีนัง, 2556, หน้า 101–108)เพื่อจัดการการโจมตีหรือขโมยข้อมูลที่สำคัญในส่วนของข้อมูลส่วนตัวก็มีการตั้งรหัสผ่านเพื่อเข้าใช้งานเพื่อป้องกันข้อมูลในเบื้องต้นหรืออาจจะใช้เป็นการบ่งบอกระดับสิทธิ์การเข้าใช้งานหรือเข้าถึงข้อมูลขององค์กรต่าง ๆโดยมีหัวหน้างาน เป็นผู้กำหนดสิทธิ์และมีผู้บริหารข้อมูล (Database Administer) หรือ DBA เป็นผู้จัดการและดูแลการเข้าถึงข้อมูลบนเครือข่าย เพื่อความมั่นคงปลอดภัยที่มากขึ้นจึงได้มีนำวิธีการต่าง ๆที่ถูกคิดค้นเพื่อใช้รักษาความมั่นคงปลอดภัยของข้อมูลโดยแปลงข้อมูลปกติ (Plaintext) ให้เป็นข้อมูลลับ (Ciphertext) ด้วยการเข้ารหัสข้อมูลจัดเก็บหรือส่งข้อมูล

การสร้างกุญแจ (Key) ซึ่งเป็นตัวเลขผ่านกระบวนการทางคณิตศาสตร์ให้เป็นข้อมูลที่เข้ารหัส (Encryption) เมื่อต้องการอ่านหรือเข้าถึงข้อมูลก็นำข้อมูลที่เข้ารหัสมาผ่านกระบวนการทางคณิตศาสตร์ทำการถอดรหัส (Decryption) การเข้ารหัสข้อมูล (Cryptography) แบ่งออกเป็นสองรูปแบบได้แก่ ระบบเข้ารหัสแบบกุญแจสมมาตร (Symmetric-Key Cryptography) และระบบเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric-Key Cryptography or Public Key Technology) (วรเศรษฐ สุวรรณิก, 2553,หน้า 356–359)

ระบบเข้ารหัสแบบกุญแจสมมาตร (Symmetric-Key Cryptography)

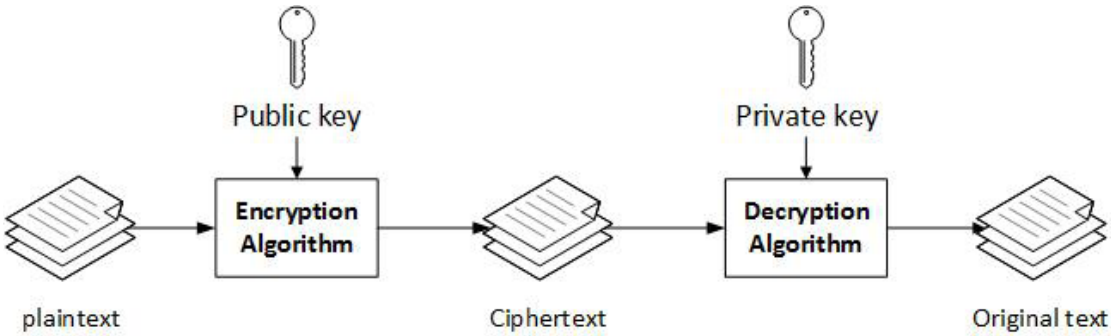
ระบบเข้ารหัสแบบกุญแจสมมาตรคือการเข้ารหัสข้อมูลด้วยกุญแจเดี่ยวมีผู้ส่งและผู้รับตกลงกันในการเข้ารหัสข้อมูลซึ่งเป็นกุญแจลับ (Secret key) ส่วนระบบเข้ารหัสแบบกุญแจอสมมาตรจะใช้หลักกุญแจคู่ในการเข้ารหัสและถอดรหัสประกอบด้วยกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ดังแสดงในภาพที่ 1 โดยหลักการทำงานใดเข้ารหัสจะใช้กุญแจอีกดอกถอดรหัส ข้อดีเข้ารหัสแบบกุญแจสมมาตรคือทำงานได้รวดเร็วกว่าและง่ายต่อการใช้งานกว่าการเข้ารหัสแบบกุญแจสมมาตรแต่ข้อเสียคือ ในการใช้งานอัลกอริทึมนี้ สองกลุ่มที่ต้องการแลกเปลี่ยนข้อมูลกันและความยุ่งยากในการเก็บรักษากุญแจและจำนวนกุญแจจะต้องเพิ่มขึ้นตามขนาดของผู้มีส่วนเกี่ยวข้องทั้งหมดทำให้ยุ่งยากหากมีผู้ใช้งานหลายคนซึ่งปัญหาที่เกิดขึ้นคือการมีกุญแจเยอะเกินไปดังนั้นจึงมีการใช้กุญแจแบบอสมมาตรช่วยแก้ปัญหาที่เกิดขึ้น



ภาพที่ 1 ระบบเข้ารหัสแบบกุญแจสมมาตร (Symmetric-Key Cryptography)

ระบบเข้ารหัสแบบกุญแจสมมาตร (Symmetric-Key Cryptography)

หลักการทำงานนั้นจะใช้หลักกุญแจคู่ในการเข้ารหัสและถอดรหัสประกอบด้วยกุญแจส่วนตัว(Private Key) และกุญแจสาธารณะ(Public Key) ดังแสดงในภาพที่ 2 โดยหลักการทำงานใดเข้ารหัสจะใช้กุญแจอีกดอกถอดรหัส กุญแจแบบอสมมาตรถูกสร้างมาเพื่อแก้ปัญหาของเข้ารหัสแบบกุญแจสมมาตรแต่ก็ยังมีข้อเสียที่สำคัญ คือ ต้องใช้เวลาในการคำนวณการเข้าและถอดรหัสนานมากกว่าหลายเท่าเมื่อเทียบกับระบบกุญแจสมมาตร



ภาพที่ 2 ระบบเข้ารหัสแบบกุญแจสมมาตร (Symmetric-Key Cryptography)

ปัญหาของข้อมูลที่เข้ารหัสรักษาความมั่นคงปลอดภัยที่พบคือเมื่อต้องการใช้ข้อมูลจะต้องนำข้อมูลออกมาทำการถอดรหัสก่อนถึงจะนำไปได้ซึ่งอาจทำให้ใช้เวลานานและยุ่งยากหากปริมาณข้อมูลที่เข้ารหัสนั้นมีหลายชุดข้อมูลและในทุกขั้นตอนการทำงานนอกเหนือจากผู้ใช้ที่ทราบรหัสข้อมูลแล้ว DBA ก็ทราบด้วยโดยจะเป็นผู้ที่เก็บรหัสของข้อมูลไว้ด้วยเพื่อใช้ในการจัดการข้อมูลในฐานข้อมูล ปัญหาที่พบต่อมาหาก DBA เป็นทุจริตเองโดยการถอดรหัสข้อมูลจากฐานข้อมูลแล้วเปลี่ยนแปลงหรือ นำความลับไปเผยแพร่อาจทำให้เกิดปัญหาร้ายแรงได้

วัตถุประสงค์ของการรักษาความปลอดภัย

วัตถุประสงค์ของการรักษาความปลอดภัยของระบบฐานข้อมูลก็เพื่อลดปัจจัยเสี่ยงที่เกี่ยวกับความเสียหายกับฐานข้อมูล เนื่องจากความผิดพลาดในการทำงานของผู้ใช้ระบบฐานข้อมูล แฟ้มข้อมูลเสียหาย ความผิดพลาดในการทำงานของเครื่อง การปฏิบัติงานที่ไม่เหมาะสม การทุจริต และการเปิดเผยข้อมูลที่เป็นความลับ โดยสามารถแยกวัตถุประสงค์โดยรวมของการรักษาความปลอดภัยในระบบฐานข้อมูลได้ 4 ประการ คือ (วรกฤต แสนโภชน์, 2560 ,หน้า 245) เพื่อให้สามารถรักษาข้อมูลเป็นความลับได้ (secrecy) ระบบจะต้องปกป้องข้อมูลไม่ให้ผู้ไม่มีสิทธิในการใช้ข้อมูลเข้าใช้ข้อมูลได้ และจะต้องสามารถกำหนดให้ผู้ใช้งานแต่ละคนสามารถใช้งานได้ตามสิทธิที่กำหนดเท่านั้นด้วย ควรมีการกำหนดสิทธิไว้ชัดเจน อยู่ในห้องเครื่อง มีการรักษาความปลอดภัยโดยใช้บัตรผ่าน มีการควบคุมสิทธิผู้ใช้งานอย่างรอบคอบ มีความปลอดภัยในการใช้งานในระบบเครือข่าย และมีระบบสำรองกู้คืนข้อมูลที่ดี สามารถใช้งานได้สะดวก

1. เพื่อให้ข้อมูลในฐานข้อมูลมีความถูกต้องครบถ้วนสมบูรณ์ (integrity) นั่นคือจะต้องสามารถรักษาข้อมูลให้มีความถูกต้องตามกฎเกณฑ์หรือเงื่อนไขที่ได้กำหนดไว้ตอนสร้างฐานข้อมูล ข้อมูลต้องไม่ผิดเพี้ยน รวมทั้งความถูกต้องของข้อมูลในการประมวลผลข้อมูลพร้อมกันด้วย

_ 13 2 -2562.indd 228 23/12/2562 9:51:59

2. เพื่อให้มีฐานข้อมูลพร้อมใช้งานอยู่เสมอ (availability) สามารถทำงานได้ตามปกติและเต็มประสิทธิภาพตามจุดมุ่งหมายในการใช้ และมีขีดความสามารถปฏิบัติงานได้ตามที่ต้องการเนื่องถ้าการใช้งานระบบฐานข้อมูลมักจะมีข้อขัดข้องอยู่เสมอ เช่นเครื่องเสีย หรือไฟดับ หรือข้อมูลสูญหาย ถ้ามีการรักษาความปลอดภัยที่ดีจะทำให้ผู้ใช้งานมีความเชื่อถือในระบบฐานข้อมูลนั้น

3. เพื่อลดความเสี่ยง (Risk Assessment) การรักษาความปลอดภัยที่ดีจะช่วยลดความเสี่ยงในค่าใช้จ่ายที่จะเกิดขึ้นจากการเสียหายของข้อมูล การวางแผนด้านการรักษาความปลอดภัยได้อย่างเหมาะสมจะช่วยลดความเสี่ยงในการเกิดความเสียหายของข้อมูลค่าใช้จ่าย มีการประเมินความสมดุลระหว่างค่าใช้จ่ายหรือต้นทุนคุ้มค่ากับประโยชน์ที่จะได้รับจากการรักษาความปลอดภัย

แนวคิดในการรักษาความมั่นคงปลอดภัยของข้อมูลได้มีผู้คิดค้นการเข้ารหัสมากมายในปัจจุบันเพื่อใช้ในปกป้องข้อมูลทั้งส่วนตัวและขององค์กรเนื่องจากวิธีการรักษาความมั่นคงปลอดภัยที่มีอยู่เดิมอาจไม่เพียงพอ เช่น ข้อมูลจะถูกเปิดเผยเมื่อต้องการประมวลผล หรือข้อมูลถูกเรียกดูโดย DBA ทำให้ความลับของข้อมูลถูกโจมตีจากผู้ไม่หวังดี การเข้ารหัสแบบสาทิสสัณฐาน (Homomorphic Encryption) เป็นอีกวิธีหนึ่งที่นักวิจัยให้ความสนใจและนำไปประยุกต์ซึ่งเป็นการพัฒนาต่อยอดแนวความคิดของ Rivest, Adleman, Dertouzos (1978 ,pp 169–180) ออกแบบขึ้นตั้งแต่ปี1978 การเข้ารหัส Homomorphic มีข้อดีคือเป็นการเข้ารหัสที่เปิดโอกาสให้สามารถกระทำบางคำสั่งกับข้อมูลที่เข้า รหัสอยู่ โดยไม่ต้องถอดรหัสออกมาก่อน ในปี 2009 Craig (Gentry, 2009,pp 169–178) ได้นำวิธีการเข้ารหัสนี้มาใช้และวิจัยทำให้สามารถจัดเก็บไฟล์ที่เข้ารหัสแล้วไว้บนเซิร์ฟเวอร์ แล้วส่งคำสั่งค้นหาไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์สามารถตอบได้ว่าในไฟล์มีที่ต้องการหรือไม่โดยไม่ต้อง รู้ว่าไฟล์นั้นมีข้อมูลอะไร หรือกระทั่งว่ากำลังหาข้อมูลอะไรอยู่

คณิตศาสตร์พื้นฐานสร้างรหัสและถอดรหัส(The mathematics of cryptology)

พีชคณิตนามธรรม (Abstract Algebra)

พีชคณิตนามธรรม (Abstract Algebra) เป็นสาขาหนึ่งของคณิตศาสตร์โดย เอวาริสต์กาลัวส์ (Évariste Galois) เป็นผู้คิดค้นและวางรากฐาน ในปี 1832 เป็นศึกษาเกี่ยวกับโครงสร้างเชิงพีชคณิตเช่น แนวคิดเกี่ยวกับ ริงและฟีลด์ สาทิสสัณฐาน ปริภูมิเวกเตอร์ พหุนาม ฟีลด์ภาคขยาย การแยกตัวประกอบของพหุนามและไฟไนต์ คำว่า “พีชคณิตนามธรรม” ถูกใช้เพื่อแยกแยะสาขาออกจากพีชคณิตพื้นฐาน พื้นฐานของการเข้ารหัสและถอดรหัสนั้นจะอยู่ในพื้นฐานคณิตศาสตร์กาลัวร์ หรือทฤษฎีกาลัวร์ฟิลด์เป็นหลักโดยเฉพาะคุณสมบัติของอาบีเลียนกรุป (Abelian Group) เนื่องจากมีการดำเนินการที่มีคุณสมบัติสลับที่ (Commutative Property) (ธัญพร ศรีดอกไม้, 2561,หน้า 121-132)

สาทิสสัณฐาน (Homomorphism)

สาทิสสัณฐาน (Homomorphism) (Pierpont, 1899: 113-143) เป็นหนึ่งในฟังก์ชั่นทางคณิตศาสตร์ของพีชคณิตนามธรรมโดยมีคุณสมบัติที่ไม่มีการเปลี่ยนแปลงโครงสร้างการดำเนินการ

นิยาม ให้ $(G,*)$ *และ* $(H,\Diamond)$ *เป็นกรุป แล้วการส่ง* (Map) $\varphi : G \to H$ ที่ซึ่ง $\varphi(x*y)=\varphi(x)\Diamond\varphi(y)$ ที่ซึ่ง $\varphi(x*y)=\varphi(x)\Diamond\varphi(y)$ เรียกว่า สาทิสสัณฐาน (Homorphic) โดยที่ φ เป็นสาทิส φ *เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง*

การเข้ารหัสแบบโฮโมมอฟิค

การเข้ารหัสแบบโฮโมมอฟิค (Homomorphic Encryption Schemes) ถูกนำมาเผยแพร่อย่างกว้างขวางในช่วงและถูกนำไปประยุกต์ ใช้งานไม่กี่ปีที่ผ่านมาจากคุณสมบัติเด่นในการรักษาความปลอดภัยจึงถูกนำไปสร้างเป็นโพรโตคอลในระบบที่ต้องการความปลอดภัยที่ค่อนข้างสูงและข้อมูลมีความสำคัญมาก เช่น การเลือกตั้งอิเล็กทรอนิกส์ (Electronic Voting) การประมูลอิเล็กทรอนิกส์ (Electronic Auctions) หรือแม้กระทั่งการนำไปใช้ในการรักษาข้อมูลส่วนบุคคล เช่น ประวัติผู้ป่วยของโรงพยาบาลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Sridokmai & Prakancharoen, 2015,pp 356-359) รูปแบบการเข้ารหัสแบบ Homomorphic ถูกนำไปวิจัยต่อจากนักวิจัยอีกหลายท่านตั้งแต่อดีตจนถึงปัจจุบันซึ่งในช่วงก่อนปี 2009 จะเป็นการนำเอาหลักการของ Homomorphism ซึ่งเป็นฟังก์ชั่นการทำงานของกรุป(Group)ใน Abstract Algebra ร่วมกับวิธีเข้ารหัสแบบกุญแจสาธารณะโดยรวมของวิธีการเหล่านี้ว่า “Partially Homomorphic Cryptosystems” (Fontaine & Galand, 2007,pp 1-10) ซึ่งมีหลายวิธีที่เป็นที่รู้จักหลายวิธีได้แก่

Unpadded RSA (Rivest, Adleman & Dertouzos, 1978 ,pp 169-180)เป็นตัวอย่างของการเข้ารหัสแบบ Homomorpic ที่ถูกนำเสนอขึ้นใช้การเข้ารหัสในรูปแบบของ RSA มาใช้ในรูปแบบของการคูณความปลอดภัยนั้นขึ้นอยู่กับจำนวนความยาวของบิตในการคำนวณและยังเป็นเทคนิคที่ใช้คุณสมบัติของ Homomorphic น้อย ดังสมการที่ 1 การเข้ารหัสเป็นแบบการคูณ Modulo m และกำหนดให้ $\varepsilon(\mathrm{x}) = \mathrm{x}^e$

$$\varepsilon(\mathrm{x}_1)*\varepsilon(\mathrm{x}_2) = x_1^e x_2^e \bmod m = (\mathrm{x}_1\mathrm{x}_2)^e \bmod m = \varepsilon(\mathrm{x}_1*\mathrm{x}_2) \quad (1)$$

ElGamal Scheme (ElGamal, 1985) เป็นการเข้ารหัส Homomorphic แบบการคูณเหมือนกับ RSA แต่รูปแบบการทำงานจะอยู่บนพื้นฐานของลอการิทึมแบบไม่ต่อเนื่องดังสมการที่ 2กำหนดให้

G เป็นกรุปและให้กุญแจสาธารณะ (pk) $pk=(G,q,g,h)$ โดยที่ $h=g^x$ และให้ x เป็น Secret key และข้อความที่เข้ารหัสแล้วเป็น m และให้ $\varepsilon(m)=(g^r, m*h^r)$ และ r เป็นเลขสุ่ม (Random) โดยที่ $r\in\{0,....,q-1\}$

$$\varepsilon(x_1)*\varepsilon(x_2)=(g^{r1},x_1*h^{r1})(g^{r2},x_2*h^{r2})=(g^{r1+r2},(x_1*x_2)h^{r1+r2})=\varepsilon(x_1*x_2) \quad (2)$$

Goldwasser and Micali Scheme (GM) (Goldwasser & Micali, 1984, pp 270-299) เป็นการเข้ารหัสแบบความน่าจะเป็นมาใช้เพื่อปรับปรุงคุณสมบัติของ RSA ให้ปลอดภัยมากขึ้นต่อมาดังสมการที่ 3กำหนดให้ กุญแจสาธารณะเป็นแบบ Modulo m และ x ให้เป็นสมการกำลังสองแบบNon-Residue และให้การเข้ารหัสบิต b คือ $\varepsilon(b)=x^b r^2$ mod m และ r เป็นเลขสุ่ม $r\in\{0,....,m-1\}$

$$\varepsilon(b_1)*\varepsilon(b_2)=x^{b1}r_1^2x^{b2}r_2^2=x^{b1+b2}(r_1r_2)^2=\varepsilon(b_1\oplus b_2) \quad (3)$$

Benaloh's Scheme (Boneh & Lipton, 1996,pp 79-94) การเข้ารหัส Homomorphic ที่นำเอาคุณสมบัติของวิธีการแบบ GM ปรับเพิ่มความซ้ำซ้อนของการคำนวณรหัสลับให้มากขึ้นและวิธีการนี้มีจุดที่น่าสนใจคือค่าใช้จ่ายในการดำเนินงานน้อยเมื่อเปรียบเทียบกับวิธีอื่น ๆ ที่ผ่านมาดังสมการที่ 4

กำหนดให้ กุญแจสาธารณะเป็นแบบ Modulo m และให้การเข้ารหัส x เป็น $\varepsilon(x)=g^x r^c \bmod m$ และให้เลขสุ่ม $r\in\{0,....,q-1\}$

$$\varepsilon(x_1)*\varepsilon(x_2)=(g^{x1}r_1^c)(g^{x2}r_2^c)=g^{x1+x2}(r_1r_2)^c=\varepsilon(x_1+x_2 \bmod c) \quad (4)$$

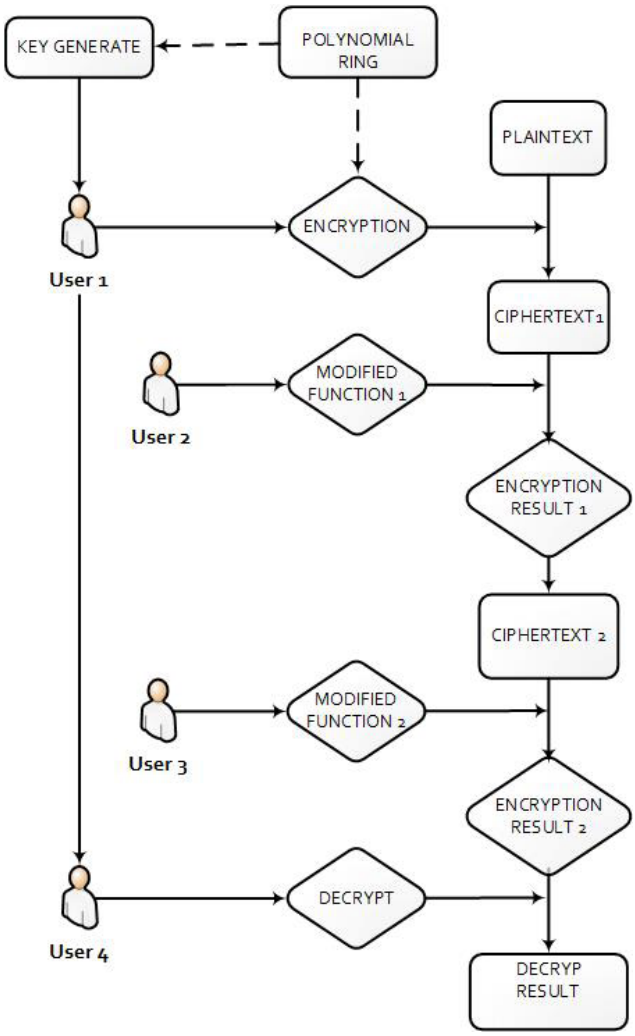
Naccache-Stern Scheme (Naccache & Stern, 1998, pp 59-66) ถูกสร้างเพื่อปรับปรุงวิธีการ Benaloh ให้มีประสิทธิภาพมากขึ้นและมีขนาดที่เล็กลงโดยการปรับค่าพารามิเตอร์ในการคำนวณให้สูงขึ้น ซึ่งถือว่าเป็นวิธีที่มีประสิทธิ์ภาพในการรักษาความปลอดภัยอีกตัวหนึ่งและประสบความสำเร็จเหมือนกับวิธีของ Benaloh

Paillier Cryptosystem ในปี 1999 Pascal Paillier (Paillier, 1999, pp 223-238) ผู้ที่นำเสนอเป็นรูปแบบของการเข้ารหัสแบบ Homomorpic ที่เป็นที่รู้จักมากตัวหนึ่งเนื่องจากเป็นการปรับปรุงการเข้ารหัสแบบเดิมให้มีขนาดที่เล็กลงและค่าใช้จ่ายในการดำเนินงานต่ำกว่าวิธีอื่น ๆ ดังสมการ 5

กำหนดให้ $\varepsilon(x)=g^x r^m \bmod m^2$ และให้ r เป็นเลขสุ่มโดยที่ $r\in\{0,....,q-1\}$

$$\varepsilon(x_1)*\varepsilon(x_2)=(g^{x1}r_1^m)(g^{x2}r_2^m)=g^{x1+x2}(r_1r_2)^m=\varepsilon(x_1+x_2 \bmod m^2) \quad (5)$$

ขั้นตอนการเข้ารหัสข้อมูล Homomorphic Encryption



ภาพที่ 3 แสดงขั้นตอนการเข้ารหัสข้อมูล Homomorphic Encryption

ขั้นตอนการเข้ารหัสข้อมูล Homomorphic Encryption ที่แสดงในภาพที่ 3

1. เริ่มจากการทำ Key Generate ด้วยวิธีการของ Polynomial Ring ซึ่งเป็นฟังก์ชันการทำงานหนึ่งของ พีชคณิตนามธรรม

2. User 1 ตัวเลขจากการ Generateในการเข้ารหัส ข้อมูล (PlanText) ให้อยู่ในรูปแบบของ CipherText 1

3. User 2 นำ CipherText 1แก้ไขข้อมูลโดยไม่ต้องถอดรหัสออกมาและทำการเข้ารหัสซ้ำเป็นครั้งที่สองเพื่อให้อยู่ในรูป CipherText2

_ 13 2 -2562.indd 232 23/12/2562 9:52:10

4. User 3 นำ CipherText 2 ปรับปรุงข้อมูลภายในโดยไม่ต้องถอดรหัสออกมาและทำการเข้ารหัสเป็นครั้งที่สามเพื่อให้อยู่ในรูป CipherText3

5. User 4 (อาจจะเป็นผู้มีสิทธิ์ถอดรหัสเพียงคนเดียว) นำ CipherText 3 ที่ได้รับการแก้ไขและปรับปรุงข้อมูลมาถอดรหัส (Decryption) ข้อมูลที่อยู่ในรูปของข้อความธรรมดาก็จะเป็นข้อมูลที่ได้รับการเปลี่ยนแปลงล่าสุด User 3เป็นผู้ปรับปรุง

การนำวิธีการเข้ารหัสแบบโฮโมมอฟิคไปประยุกต์ใช้งาน

การเข้ารหัสแบบโฮโมมอฟิค นั้นถูกนำไปประยุกต์ใช้ในงานด้านรักษาความปลอดภัยให้กับข้อมูลในรูปแบบที่หลากหลายโดยสามารถนำไปประยุกต์ใช้งานร่วมกับวิธีการรักษาความปลอดภัยรูปแบบอื่นๆ เช่น Peng, K. (2014,pp 64–76) ได้นำไปประยุกต์ใช้ร่วมกับวิธี Secret Sharing เพื่อป้องกันให้กับระบบ E-Auction ซึ่งระบบสามารถตรวจสอบความถูกต้องเสนอราคาเป็นสิ่งที่จำเป็นในการประมูลโครงการและป้องกันการโจมตีโดยไม่สูญเสียความเป็นส่วนตัวในเสนอราคา และ การเข้ารหัสแบบโฮโมมอฟิค ถูกยังนำไปใช้กับองค์กรธุรกิจชั้นนำของโลกหลายบริษัท ได้แก่ IBM เป็นบริษัทแรกที่นำวิธีการนี้ไปใช้โดยได้ซื้อลิขสิทธิ์งานวิจัยของ Craig Gentry ซึ่งเป็นผู้พัฒนาการเข้ารหัสการเข้ารหัสโฮโมมอฟิคแบบสมบูรณ์ และนำไปพัฒนาต่อยอดไปใช้กับระบบ Cloud Computing ในการเก็บข้อมูลต่าง ๆ โดยเพื่อรักษาความรักษาความปลอดภัยแทนระบบเดิมเนื่องจากฐานข้อมูลที่มีขนาดใหญ่และต้องการความปลอดภัยที่มากขึ้น (R. Bocu & C. Costache, 2018) รวมถึง SAP AG ที่เป็นบริษัทซอฟต์แวร์ที่ใหญ่ที่สุดของยุโรปและใหญ่เป็นอันดับ 3 ของโลกซึ่งเป็นผู้พัฒนาซอฟต์แวร์ประเภท ERP ได้นำวิธีการนี้มาพัฒนาและใช้ในการช่วยรักษาความปลอดภัยกับข้อมูลของลูกค้านำไปใช้กับการปกป้องความเป็นส่วนตัวในระบบคลาวด์คอมพิวติ้งที่ใช้บริการซอฟท์แวร์ของบริษัทSAP ทั่วโลก (Mallaiah & Sirandas, 2014) หรือ แม้กระทั้งบริษัท Microsoft ได้พัฒนาซอฟต์แวร์รักษาความปลอดภัยที่มีชื่อว่า Microsoft SEAL โดยนำมาใช้รักษาความปลอดภัยให้กับข้อมูลต่าง ๆที่ถูกเก็บอยู่ระบบคลาวด์ของบริษัท (Chen, Laine, & Player, 2017)

บทสรุป

การรักษาความมั่นคงปลอดภัยให้กับข้อมูลนั้นถือว่าเป็นเรื่องจำเป็นและสำคัญมากสำหรับทุกภาคส่วนไม่ว่าจะเป็นทั้งภาครัฐและภาคเอกชนทั้งขนาดเล็กและขนาดใหญ่ การเลือกวิธีการที่จะนำมาใช้รักษาความมั่นคงปลอดภัยให้กับข้อมูลของตนเองนั้นควรคำถึงวัตถุประสงค์ของการรักษาความปลอดภัยเป็นหลัก วิธีการรักษาความปลอดภัยแบบโฮโมมอฟิค นั้นเป็นวิธีการหนึ่งซึ่งมีความปลอดภัยที่อยู่ในระดับที่สูงและเป็นที่ยอมรับกันอย่างกว้างขวางในเรื่องของความปลอดภัยซึ่งถูกนำไปใช้งานกันอย่างแพร่หลาย เช่นการรักษาความปลอดภัยในระบบธนาคารและการรักษาความปลอดภัยให้กับโรงพยาบาลต่างๆในต่างประเทศได้นำไปใช้กับระบบการเลือกตั้งออนไลน์เพราะด้วยคุณสมบัติของวิธีการแบบโฮโมมอฟิค สามารถป้องกันผู้ที่ไม่หวังดีจากภายในและ

ภายนอกได้โดยในการรักษาความปลอดภัยให้กับข้อมูลและระดับของความปลอดภัยนั้นขึ้นอยู่กับความซับซ้อนของระบบตัวเลขที่นำมาใช้ในการเข้ารหัสซึ่งในวิธีการแบบ Partially Homomorphic Cryptosystems เป็นวิธีการที่อาศัยหลักการมาจากวิธีการรักษาความปลอดภัยที่มีการยอมรับในเรื่องของความปลอดภัยมาสร้างเป็นรูปแบบของการเข้ารหัสในรูปแบบของ Homomorphic Encryption แต่สิ่งหนึ่งซึ่งไม่อาจลืมไปได้เลยในการรักษาความมั่นคงปลอดภัยให้กับข้อมูลคือความเหมาะสมเพราะในบางครั้งข้อมูลนำมาเข้ากระบวนการรักษาความปลอดภัยไม่สำคัญมากพอจึงไม่จำเป็นต้องใช้การรักษาความปลอดภัยที่ยุ่งยากและสลับซับซ้อนเพราะในการสร้างการรักษาความมั่นคงปลอดภัยของข้อมูลให้มีความสลับซับซ้อนมากเท่าไหร่ก็จะมีค่าใช้จ่ายสูงขึ้นและใช้เวลาในการทำงานมากขึ้นตามไปด้วย

_ 13 2 -2562.indd 234 23/12/2562 9:52:10

บรรณานุกรม

ธัญพร ศรีดอกไม้. (2558). **ขั้นตอนวิธีสำหรับการเข้ารหัสบนฐานข้อมูลแบบกระจาย**. ปริญญาเอก (เทคโนโลยีสารสนเทศ). มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ, หอสมุดกลาง.

เพ็ญศรี ปักกะสีนัง. (2556). วิทยาการเข้ารหัสลับเบื้องต้น. **วารสารราชนครินทร์**, 10(24), หน้า 101–108.

วรกฤต แสนโภชน์. 2560. **เอกสารประกอบการสอน รายวิชา ระบบฐานข้อมูล**.พะเยา: คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยพะเยา

วรเศรษฐ สุวรรณิก. (2553). ความปลอดภัยในระบบคอมพิวเตอร์. ใน อรวรรณ วัชนุภาพร(บรรณาธิการ). **วิทยาการรหัสลับ Cryptography** .(หน้า 356–359). กรุงเทพฯ: ดวงกมลสมัย.

ศิริพร อ่องรุ่งเรือง. (2560). **ความมั่นคงปลอดภัยของสารสนเทศ**. ค้นเมื่อ 11 กุมภาพันธ์ 2560 จาก http://www.cpe.ku.ac.th/~srp/603352/Chapter2_InfoSecurity.pptx

Bocu, R., & Costache, C. (2018). A homomorphic encryption-based system for securely managing personal health metrics data. **IBM Journal of Research and development**.62(1), NJ, USA: IBM, pp. 1–10.

Boneh, D., & Lipton, R. J. (1996). Algorithms for black-box fields and their application to cryptography. In Neal Koblitz (editor). **Annual International Cryptology Conference**. (pp. 283–297).Santa Barbara, California, USA: Springer.

Chen, H., Laine, K., & Player, R. (2017). Simple encrypted arithmetic library-SEAL v2. 1. In M. Brenner, K. Rohloff, et al (editor). **Financial Cryptography and Data Security. FC 2017**. Lecture Notes in Computer Science, 10323. (pp. 3-18) Malta: Springer International Publishing.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. **IEEE transactions on information theory**, 31(4), 469–472.

Fontaine, C., & Galand, F. (2007). A survey of homomorphic encryption for non-specialists. **EURASIP Journal on Information Security**, 1(1), pp. 1–10.

Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In **Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing**. (pp.169–178). New York, USA: ACM

Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. **Journal of computer and system sciences**, 28(2), pp. 270–299.

Mallaiah, K., & Sirandas, R. (2014). Applicability of Homomorphic Encryption and CryptDB in Social and Business Applications: Securing Data Stored on the Third Party Servers while Processing through Applications. **International Journal of Computer Applications.** 100(1), pp. 5–19.

Naccache, D., & Stern, J. (1998). A new public key cryptosystem based on higher residues. In **Proceedings of the 5th ACM conference on Computer and communications security**. (pp. 59–66). New York, USA: ACM.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In J. Stern (editor) **International Conference on the Theory and Applications of Cryptographic Techniques**. (pp. 223–238). Berlin, Heidelberg: Springer.

Peng, K. (2014). Efficient homomorphic sealed-bid auction free of bid validity check and equality test. **Security and Communication Networks**. 7(1), pp. 64–76.

Pierpont, J. (1899). Galois' theory of algebraic equations. **Annals of Mathematics**, 1(1/4): pp.113–143.

Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. **Foundations of secure computation.** 4(11),169–180.

Sridokmai, T., & Prakancharoen, S. (2015). The homomorphic other property of Paillier cryptosystem. In **Science and Technology (TICST), 2015 International Conference on**. (pp. 356-359) . Pathum Thani, Thailand : IEEE