การประยุกต์ของทฤษฎีเศษเหลือของจีนและโครงสร้างต้นไม้ในการส่งข้อมูลแบบกลุ่มด้วยการเข้ารหัสลับในเทคนิควิธี NTRU

An Application of Chinese Remainder Theorem and Tree on NTRU Based Group Encryption

แวววรรณ จันทร์ชูกลิ่น (Wawwan Chanchuklin)* และ พิพัฒน์ หิรัณย์วณิชชากร (Pipat Hiranvanichakorn)*

บทคัดย่อ

การเข้ารหัสลับแบบกลุ่มได้รับความนิยมอย่างแพร่หลายในการส่งข้อมูลเพียงครั้งเดียวให้กับผู้รับปลายทางพร้อมกัน รูปแบบที่อาศัยเทคนิควิธีการเข้ารหัสแบบกุญแจสมมาตร (Symmetric Key Encryption) จำเป็นต้องอาศัยช่องทางที่ปลอดภัยเพื่อส่งกุญแจระหว่างกัน จึงมีการวิจัยที่ส่งข้อมูลแบบกลุ่ม โดยเทคนิควิธีการเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric Key Encryption) เพื่อแก้ปัญหาการส่งกุญแจ และยังทำให้สามารถให้บุคคลภายนอกกลุ่มสามารถส่งข้อมูลซึ่งเป็นความลับให้แก่สมาชิกในกลุ่มได้ ในงานวิจัยนี้ได้ประยุกต์ทฤษฎีเศษเหลือของจีน (Chinese Remainder Theorem) เข้ามาช่วยในการส่งกุญแจของกลุ่ม เพื่อลดจำนวนข้อความที่จำเป็นต้องส่งออกไป ทั้งยังเสนอแนวคิดการนำโครงสร้างต้นไม้มาช่วยลดเวลาในการประมวลผลของทฤษฎีเศษเหลือของจีนสำหรับการเข้ารหัสลับข้อมูล ได้นำเสนอเทคนิควิธี NTRU ซึ่งเป็นอัลกอลิทึมในการเข้ารหัสข้อมูลแบบกุญแจอสมมาตรที่มีความเร็วในการทำงานสูง

คำสำคัญ: การเข้ารหัสลับแบบกลุ่ม, ทฤษฎีเศษเหลือของจีน, การเข้ารหัสลับข้อมูลด้วยเทคนิควิธี NTRU

Abstract

Group encryption is widely used for one time transmitting data from sender to receivers. Both symmetric-key and asymmetric-key algorithms are proposed in the study of group encryption. Symmetric-key algorithm is fast but it has a problem of key distribution. Asymmetric-key one is considered to be slower but it can deal with key distribution problem. It also provides a way for a user outside the group to send message to the group members. In this paper, NTRU which is known as a fast asymmetric-key algorithm is proposed for group encryption. Chinese remainder theorem is applied for reducing transmitting messages to only one message. An efficient tree is also introduced to intuitively reduce the time to compute the inverses in the Chinese remainder theorem.

Keyword: Group Encryption, Chinese Remainder Theorem, NTRU encryption algorithm.

1. บทนำ

การเข้ารหัสลับแบบกลุ่ม เป็นการส่งข้อมูลจากผู้ส่งไปยังกลุ่มสมาชิกผ่านการเข้ารหัสลับเพื่อให้สามารถถอดรหัสและรับทราบข้อมูลที่ต้องการส่ง ด้วยกุญแจส่วนตัวของแต่ละสมาชิก [1] ซึ่งในการเข้ารหัสลับแบบกลุ่มนี้ บุคคลที่ไม่ใช่สมาชิกในกลุ่มไม่สามารถถอดรหัสเพื่อทราบข้อมูลได้การวิจัยของการเข้ารหัสลับแบบกลุ่มมีการดำเนินการอย่างแพร่หลาย เพราะสามารถนำมาประยุกต์ใช้ในด้านต่างๆ เช่น การโทรศัพท์ผ่านทางเครือข่ายอินเทอร์เน็ต การประชุมทางไกล อีเลิร์นนิง และการสื่อสารกันผ่านเครือข่ายอินเทอร์เน็ตทั้งจากบุคคลทั้งจากภายในและภายนอกกลุ่มไปยังกลุ่มสมาชิก [2], [3]

ในบทความ [2], [3] ได้กล่าวถึงงานวิจัยหลายชิ้นที่ได้นำเสนอการเข้ารหัสลับแบบกลุ่ม ที่อาศัยเทคนิควิธีการเข้ารหัสแบบกุญแจสมมาตร เป็นการเข้าและถอดรหัสโดยใช้กุญแจส่วนตัวที่เหมือนกัน ซึ่งจะต้องเป็นที่รู้กันเพียงผู้ส่งและกลุ่มผู้รับเท่านั้น

* *สาขาวิทยาการคอมพิวเตอร์ คณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์*

ทำให้จำเป็นต้องเพิ่มวิธีการระบุตัวตนเพื่อเข้าร่วมกลุ่มสื่อสาร และมีความจำเป็นต้องเลือกใช้ช่องทางที่ปลอดภัยสำหรับการส่งกุญแจจาก key server ให้กับสมาชิกใหม่ที่ต้องการเข้าร่วมกลุ่มสื่อสาร จึงมีผู้เสนองานวิจัยที่นำการเข้ารหัสแบบกุญแจอสมมาตร เข้ามาประยุกต์ใช้เพื่อลดปัญหาดังกล่าว ซึ่งยังคงพบข้อเสีย คือในการส่งข้อความลับแต่ละครั้งนั้นจำเป็นต้องเข้ารหัสด้วยกุญแจสาธารณะ สำหรับแต่ละสมาชิก ซึ่งทำให้มีข้อความที่ต้องส่งออกไปให้แต่ละสมาชิก แต่ละข้อความแตกต่างกันไป ซึ่งเป็นการภาระหนักในการทำงานของ key server

เพื่อแก้ปัญหาของการส่งข้อความจำนวนมาก จึงมีงานวิจัยที่นำเสนอแนวคิดการส่งข้อมูลแบบกลุ่ม โดยประยุกต์ทฤษฎีเศษเหลือของจีนเข้ามาช่วยในการจัดการกุญแจกลุ่ม (group key) ด้วยเทคนิควิธีเข้ารหัสแบบกุญแจสมมาตร [4] และแบบกุญแจอสมมาตร [5] ซึ่งมีจุดประสงค์เพื่อสามารถส่งข้อความที่เข้ารหัสแค่ข้อความเดียว กระจายให้แก่สมาชิกในกลุ่ม และยังคงรักษาความปลอดภัยให้กับผู้ที่เป็นสมาชิกในภายในกลุ่มเท่านั้นที่ได้รับสิทธิ์ในการเข้าถึงข้อมูลที่ถูกเข้ารหัสดังกล่าว แต่ก็มีปัญหาเนื่องจากในการประมวลผลเพื่อหาค่า inverse เพื่อใช้คำนวณผลเฉลยตามทฤษฎีเศษเหลือของจีนนั้นต้องคำนวณให้แก่ทุกสมาชิกในกลุ่มจึงส่งผลให้ต้องสูญเสียเวลาเป็นอย่างมาก จึงมีการนำเสนอแนวคิดที่นำโครงสร้างต้นไม้มาช่วยลดเวลาในการดำเนินการประมวลผล ค่า inverse เหล่านี้ [6]

Avadhani and Prasad [7] นำเสนอการทดลองเพื่อวิจัยเปรียบเทียบการทำงานของการเข้ารหัสลับข้อมูลด้วยเทคนิควิธี NTRU (Ntru Cryptosystems) ซึ่งเป็นอัลกอลิทึมในการเข้ารหัสข้อมูลแบบกุญแจอสมมาตรที่มีความเร็วในการประมวลผลสูงกว่าการเข้าหัสแบบ RSA และ ECC ทำให้เทคนิควิธีนี้เหมาะสำหรับอุปกรณ์ที่มีหน่วยความจำน้อยๆ เช่นในอุปกรณ์เคลื่อนที่ ดังนั้นการเข้ารหัสลับด้วยเทคนิควิธี NTRU เป็นทางเลือกหนึ่งที่น่าสนใจเป็นอย่างยิ่ง

งานวิจัยนี้ได้นำเอาทฤษฎีเศษเหลือของจีนมาประยุกต์ในการคำนวณของการเข้ารหัสลับแบบกลุ่มที่ใช้เทคนิคของ NTRU โดยมีการใช้ key server ทำหน้าที่ในการเข้ารหัสลับแบบกลุ่มเพื่อส่งกุญแจกลุ่ม (group key) ที่ใช้สำหรับเข้ารหัสลับข้อมูลจริง ให้แก่สมาชิกในกลุ่มโดยส่งกุญแจกลุ่ม ซึ่งถูกเข้ารหัสไปเพียงข้อความเดียว แล้วสมาชิกแต่ละคนจะสามารถใช้หลักการของทฤษฎีเศษเหลือของจีนคำนวณหาข้อมูลที่ส่งมาเฉพาะสำหรับตนเองได้กุญแจกลุ่มซึ่งใช้ในการส่งข้อความที่เป็นความลับให้กับสมาชิกในกลุ่ม นอกจากนี้เพื่อให้ key server มีการประมวลผลอย่างรวดเร็ว จึงมีการใช้โครงสร้างต้นไม้มาช่วยในการประมวลผลด้วยการเก็บค่า inverse สำหรับคำนวณค่าผลเฉลยสำหรับทฤษฎีเศษเหลือของจีนในลักษณะความสัมพันธ์กันแบบต้นไม้สำหรับสมาชิกในกลุ่ม สำหรับต้นไม้ที่นำเสนอ มีโครงสร้างที่ทำให้การประมวลผลทำได้อย่างรวดเร็ว ทั้งในกรณีของสมาชิกออกจากกลุ่มและเข้าสู่กลุ่มจึงนับได้ว่ามีความยืดหยุ่นต่อการเปลี่ยนแปลงสมาชิก

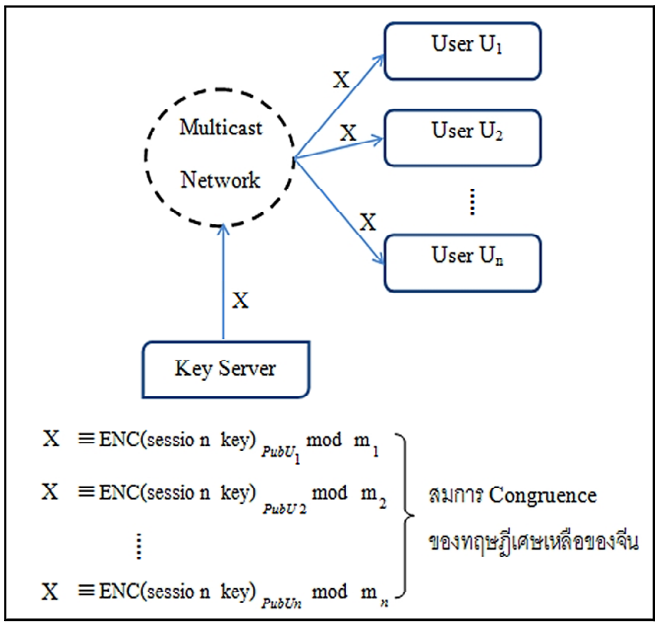
2. งานวิจัยที่เกี่ยวข้อง

มีงานวิจัยหลายชิ้นได้ประยุกต์ทฤษฎีเศษเหลือของจีนในการส่งข้อมูลเป็นความลับในกลุ่ม

Chiou and Chen ได้นำเสนอวิธีการคำนวณค่า Lock session key สำหรับสมาชิกด้วยทฤษฎีเศษเหลือของจีน [5] เป็นแนวคิดพื้นฐานในการประยุกต์เพื่อใช้ส่งข้อมูลลับในกลุ่ม สามารถใช้กับการเข้ารหัสได้ทั้ง 2 รูปแบบทั้งกุญแจสมมาตร และกุญแจอสมมาตร ซึ่งข้อดีคือสามารถลดจำนวน ข้อความที่จำเป็นต้องแพร่ออกไปในเครือข่ายลงได้ แต่ต้องใช้เวลามากในการคำนวณค่า Lock Session key ดังกล่าว จึงเหมาะกับการสื่อสารแบบกลุ่มขนาดเล็ก ดังนั้นเพื่อลดเวลาในการคำนวณของทฤษฎีเศษเหลือของจีนที่ key server และเพื่อเพิ่มประสิทธิภาพ ด้านการเก็บรักษากุญแจ Zheng และคณะ [4] ได้พัฒนาโพรโทคอล CRGK (Chinese Remainder Group Key Protocol) และ FCRCK (Fast Chinese Remainder Group Key Protocol) ในการส่งข้อมูลแบบกลุ่มโดยใช้เทคนิควิธีกุญแจสมมาตร แต่โพรโทคอลนี้มีการกำหนดจำนวนสมาชิกในกลุ่มที่คาดว่าจะมีทั้งหมดไว้ก่อนล่วงหน้า เพื่อคำนวณค่าต่างๆ ที่ต้องใช้เอาไว้ก่อนส่งผลให้ไม่เหมาะกับกลุ่มที่มีการเปลี่ยนแปลงสมาชิกในกลุ่มบ่อยครั้ง จึงถือว่ามีความยืดหยุ่นน้อยสำหรับการสื่อสารแบบกลุ่ม อีกงานวิจัยหนึ่งที่นำเสนอแนวคิดในการลดเวลาการประมวลผลของทฤษฎีเศษเหลือของจีนคือ Zhou and Ou [6] ซึ่งงานวิจัยนี้ได้ใช้ Key Tree มาช่วยในการคำนวณ แต่ในงานนี้มีการกำหนดสมาชิกทั้งหมดไว้ล่วงหน้าแล้วส่งข้อมูลให้กลุ่มย่อยภายในสมาชิกทั้งหมดเหล่านั้นจึงไม่ยืดหยุ่นกรณีที่มีสมาชิกเข้าใหม่และออกจากกลุ่ม

3. การประยุกต์ทฤษฎีเศษเหลือของจีนในการส่งข้อมูลแบบกลุ่มด้วยการเข้ารหัสลับในเทคนิค NTRU

งานวิจัยชิ้นนี้นำเสนอ วิธีการจัดการกุญแจกลุ่มเพื่อเป็นแนวคิดการสื่อสารแบบกลุ่ม ที่มีจุดประสงค์ในการแบ่งปันข้อมูลระหว่างกันอย่างมีประสิทธิภาพ โดยให้ความสำคัญกับความปลอดภัยในการสื่อสารกันระหว่างในกลุ่มสมาชิก จึงต้องมีการเข้ารหัสกุญแจที่กำหนดขึ้นก่อนส่ง โดยผู้ที่ไม่ใช่สมาชิกของกลุ่มไม่สามารถดูข้อมูลที่ถูกส่งระหว่างสมาชิกของกลุ่มได้ เมื่อมีสมาชิกเข้าหรือออกจากกลุ่มจำเป็นต้องมีการเปลี่ยนกุญแจของกลุ่มเพื่อไม่ให้สมาชิกใหม่ที่เข้าร่วมกลุ่มสามารถดูข้อมูล ที่ส่งก่อนหน้านั้นได้ (backward secrecy) และสมาชิกที่ออกจากกลุ่มไปไม่สามารถดูข้อมูลที่ส่งหลังจากนั้นได้อีก (forward secrecy) ทั้งนี้ขอเสนอแนวคิดในการนำทฤษฎีเศษเหลือของจีนและการเข้ารหัสลับด้วยเทคนิควิธี NTRU มาประยุกต์ใช้



ภาพที่ 1 *การเข้ารหัส session key กระจายให้สมาชิก*

จากรูปในการสื่อสารแบบกลุ่มจะมี Key Server ทำหน้าที่กำหนด pairwise relatively prime ให้กับสมาชิกที่เข้าร่วมกลุ่มการสื่อสาร เพื่อใช้ถอดเฉพาะข้อความที่ส่งให้แก่ตนเอง และทำหน้าที่เปลี่ยนกุญแจกลุ่มใหม่เมื่อมีการเปลี่ยนแปลงสมาชิกของกลุ่มแล้วส่งกุญแจในการเข้ารหัสลับข้อมูลของกลุ่มไปให้สมาชิกโดยใช้กุญแจสาธารณะของแต่ละสมาชิกในกลุ่มมาดำเนินการเข้ารหัส และ Key server จะคำนวณข้อความอันหนึ่ง (X) แพร่ให้แก่สมาชิก ซึ่งสมาชิกแต่ละคนจะใช้ค่า prime ของตนเองถอดข้อความสำหรับตนเองออกมาจากค่า X แล้วถอดรหัสด้วยกุญแจส่วนตัว และเก็บกุญแจกลุ่มไว้ใช้สื่อสารในกลุ่มจนกว่าจะได้รับข้อความเปลี่ยนแปลงกุญแจใหม่อีกครั้ง (re-key message)

3.1 Chinese Remainder theorem (CRT)

ให้ $m_1, m_2, \ldots, m_n$ เป็นจำนวนเฉพาะซึ่งเป็นจำนวนเต็มบวกซึ่งหรม.ของ $(m_i, m_j) = 1$ เมื่อ $i \neq j$ (pairwise relatively prime positive integer) และ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็ม กำหนดให้ $m = m_1 m_2 \ldots m_n$ และ $M_i = \frac{m}{m_i}$ สำหรับแต่ละ i ให้ y_i เป็นจำนวนเต็มซึ่งเป็น inverse ของ $M_i \bmod m_i$ กล่าวคือ $M_i y_i \equiv 1 (\bmod m_i)$ และสำหรับ Linear Congruence System และสำหรับ Linear Congruence System

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$\vdots$$
$$x \equiv a_n \bmod m_n$$

จะสามารถหาผลเฉลยร่วมกันเพียงตัวเดียวคือ $x = M_1 a_1 y_1 + M_2 a_2 y_2 + \ldots + M_n a_n y_n (\bmod m)$

จากทฤษฎีเศษเหลือของจีนค่า X ที่คำนวณได้นั้นเป็นผลเฉลยเพียงค่าเดียวที่สอดคล้องกับระบบ Linear Congruence และสามารถคำนวณหาค่า a_i ได้ด้วยการคำนวณค่า $x \bmod m_i$

3.2 การเข้ารหัสข้อความด้วยวิธี NTRU

ในการเข้ารหัสด้วยอัลกอลิทึม NTRU นั้นจะอยู่บนพื้นฐานของวงรอบพหุนาม (Polynomials Ring: $R = Z[x]/(x^N-1)$) ซึ่งเป็นพหุนามที่มีดีกรีสูงสุดไม่เกินค่าคงที่ค่าหนึ่ง (N)

$$a = a_0 + a_1 X + a_2 X^2 + \ldots + a_{N-2} X^{N-2} + a_{N-1} X^{N-1}$$

ตัวอย่างการเข้ารหัสลับแบบกลุ่มโดยกำหนดค่า $p = 3, q = 11,$ $N = 7$ และกำหนด $f = x^6 - x^4 + x^2 + 1$ สำหรับสมาชิกที่ 1 (User 1) เก็บเป็นความลับเนื่องจากใช้เป็น private key ซึ่งสามารถหาค่า Inverse f mod q (คือ f_q) และ $f \bmod p$ (คือ f_p) ได้ดังนี้

$f_q = -8x^6 + 4x^5 - 9x^4 - 3x^3 + 6x^2 - 7x + 1$ และ

$f_p = -x^6 + 2x^5 - 2x^4 + x^2 - 2x + 1$ จากนั้นกำหนด

$g = -x^6 + x^2 - 1$ และ $r = x^5 + x^2 + 1$

คำนวณค่า public key จาก $h = pf_q * g \pmod q$

ดังนั้น $h = 5x^6 + 3x^5 + 4x^3 + 5x^2 + 1x + 8$

กำหนดกุญแจเพื่อทำการเข้ารหัส $me = x^4 - x^3 + 1$

กำหนด $r = x^5 + x^2 + 1$ เพื่อดำเนินการเข้ารหัสข้อมูล

$$e = (r * h + me) \pmod q$$
$$e = -5x^6 + 4x^5 - 4x^3 + 2x^2 - 1x - 5$$

ตารางที่ 1 *กระบวนการเข้ารหัสด้วยวิธี NTRU*

เลือกค่าที่เกี่ยวข้อง	1. กำหนดค่า p ,q ที่ gcd(p,q) = 1 2. เลือก polynomial 2 ค่า แทนด้วย polynomials f ซึ่งสามารถหาค่า inverse ได้ และค่า g ใดๆเก็บไว้เป็นความลับ
กำหนดกุญแจสำหรับเข้าและถอดรหัส (Key Creation)	1. คำนวณ inverse ของ f mod q (คือ f_q) และ inverse ของ f mod p (คือ f_p) ซึ่งจะมีคุณสมบัติคือ f* f_q = 1 mod q และ f* f_p = 1 mod p 2. คำนวณหา public key ดังนั้น h = pf_q * g(modq)
ดังนั้น	public Key Polynomial = h Private Key Polynomial = {f , f_p }
เข้ารหัส (Encryption)	1. เตรียมข้อความที่ต้องการส่ง แทนด้วย me กำหนดให้อยู่ในรูปแบบ Polynomial 2. กำหนด Random Polynomial r ขึ้นเพื่อใช้ซ่อนข้อมูล 3. ทำการเข้ารหัสข้อมูล e = (r * h + me) (mod q)
ถอดรหัส (Decryption)	*1. เมื่อฝ่ายรับได้รับข้อความรหัสลับแทนด้วย e* *นำมาคำนวณ a = f * e(mod q)* *2. คำนวณ b = a * f_p (mod p)* *3. ข้อความต้นฉบับเดิมคือ me = b*

ตารางที่ 2 *ตัวอย่าง Key และการเข้ารหัสสำหรับ 2 สมาชิก*

User 1	
f = x^6-x^4+x^2+1	
f_q = -8x^6+4x^5-9x^4-3x^3+6x^2-	
f_p = -x^6+2x^5-2x^4+ x^2-2x+1	
h = 5x^6+3x^5+4x^3+5x^2+x+8	คือ a1 ในสมการทฤษฎีเศษเหลือของ
e= -5x^6+4x^5-4x^3+2x^2-1x-5	
User 2	
f = x^4+x^2-1	
f_q = -5x^6-4x^5-7x^4-6x^3-1x^2-8x-1	
f_p = -2x^5-x^3-1x^2-2x-2	
h = 8x^6+9x^5+8x^4+4x^3+7x^2+x+4	คือ a2 ในสมการทฤษฎี
e= -5x^6-5x^5+2x^4+2x^3-3x^2+2x-1	

ตารางที่ 2 แสดงการคำนวณกุญแจกลุ่มที่ถูกเข้ารหัสด้วยกุญแจสาธารณะของผู้ใช้คนที่ 1 และผู้ใช้คนที่ 2 แล้วนำค่าที่เข้ารหัสลับทั้งสองมาประยุกต์กับทฤษฎีเศษเหลือของจีน เพื่อหาค่าผลเฉลย (x) สำหรับส่งข้อมูลออกไปเพียงค่าเดียว

ตัวอย่างกำหนดให้ m_1= 13, m_2= 17, M_1= 17, M_2= 13, y_1 = -3, y_2 = 4 และ $m = 13 \times 17 = 221$

$$x = a_1M_1y_1 + a_2M_2y_2 \pmod m$$
$$= (255x^6 - 204x^5 + 204x^3 - 102x^2 + 51x^1 + 255) +$$
$$(-260x^6 - 260x^5 + 104x^4 + 104x^3 - 156x^2 + 104x^1 - 52) \bmod 221$$
$$= 216x^6 + 199x^5 + 104x^4 + 87x^3 + 184x^2 + 155x + 203 \quad (1)$$

สมาชิกในกลุ่มเมื่อได้รับค่าผลเฉลย (x) จะถอดค่าดังกล่าวเพื่อรับกุญแจกลุ่มที่เข้ารหัสแบบกุญแจอสมมาตรด้วยกุญแจสาธารณะของตน

$$a_1 = x \bmod m_1$$
$$= (216x^6 + 199x^5 + 104x^4 + 87x^3 + 184x^2 + 155x + 203) \bmod 13$$
$$= 8x^6 + 4x^5 + 9x^3 + 2x^2 + 12x + 8 \pmod{13} \quad (2)$$
$$= -5x^6 + 4x^5 - 4x^3 + 2x^2 - 1x - 5$$
$$= e_1$$

เมื่อได้รับข้อความซึ่งถูกเข้ารหัสลับไว้ ดำเนินการถอดรหัสลับด้วยการคำนวณด้วยกุญแจส่วนตัว

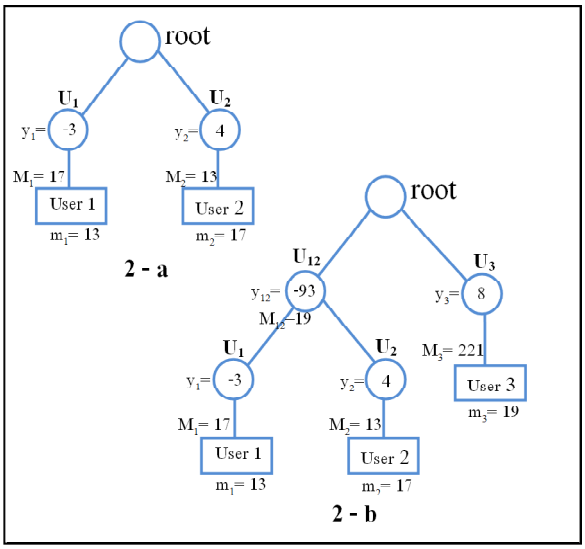
$$a = f * e \pmod q$$
$$= 10x^6 + 7x^5 + 7x + 2$$
$$b = a * f_p \pmod p$$
$$= x^4 - x^3 + 1$$
$$= \text{me} \quad (3)$$

4. การประยุกต์โครงสร้างต้นไม้

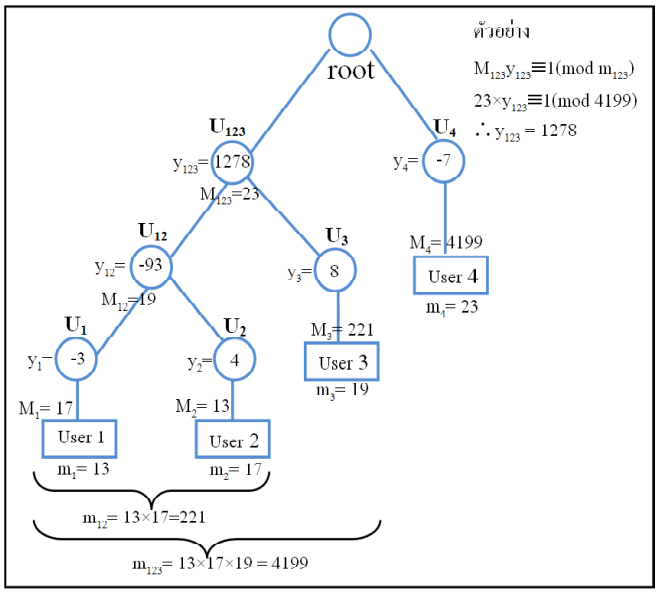
ในการเปลี่ยนแปลงสมาชิกในกลุ่มนั้นต้องคำนึงถึงความปลอดภัยในการสื่อสารเป็นสำคัญทั้ง forward secrecy และ backward secrecy ซึ่งส่งผลให้ต้องคำนวณค่า inverse ในสมการทฤษฎีเศษเหลือของจีนสำหรับทุกๆ สมาชิกในกลุ่มใหม่ทุกๆ ครั้ง ซึ่งทำให้ Key Server ต้องใช้เวลาในการประมวลมาก ในงานวิจัยนี้ได้เสนอการนำโครงสร้างต้นไม้มาช่วยลดเวลาการคำนวณค่า inverse ดังกล่าวลงได้

เมื่อเริ่มต้นในการสร้างข้อมูลลับสำหรับสมาชิกในกลุ่ม Key Server จะประมวลผลค่าผลเฉลย (x) ด้วยทฤษฎีเศษเหลือของจีน ซึ่งต้องมีการคำนวณค่า inverse ให้กับทุกๆ สมาชิก Key Server จะเพิ่มการจัดการค่า inverse ดังกล่าวให้อยู่ในรูปแบบโครงสร้างต้นไม้เพื่อลดการคำนวณที่ต้องเกิดขึ้นอีกเมื่อมีการเปลี่ยนแปลงสมาชิกเข้าหรือออกจากกลุ่ม ดังตัวอย่าง แสดงในภาพที่ 2 และ 3

ในภาพที่ 2 - a เมื่อเริ่มต้นคำนวณค่าเพื่อส่ง session key สำหรับการเข้ารหัสลับแบบกลุ่มในขั้นต้นที่มีสมาชิกเท่ากับ 2 คน ขั้นตอนแรกดำเนินการหาค่า inverse ระหว่างผู้ใช้คนที่ 1 และผู้ใช้คนที่ 2



ภาพที่ 2 *คำนวณค่า inverse สำหรับกลุ่ม*



ภาพที่ 3 *คำนวณค่า inverse เมื่อมีสมาชิกใหม่เข้าสู่กลุ่ม*

จากนั้นจึงคำนวณ inverse สำหรับผู้ใช้คนที่ 3 เมื่อเทียบกับโหนด U_{12} ซึ่งค่า m_{12} คำนวณมาจาก $m_1 \times m_2 = 13 \times 17 = 221$ ดังภาพที่ 2 – *b* และจากการคำนวณเบื้องต้นสามารถหาผลเฉลย $x = (a_1M_1y_1 + a_2M_2y_2)M_{12}y_{12} + a_3M_3y_3 (\text{mod } m)$ ซึ่งเมื่อคำนวณค่า $x \text{ mod } m_1$ จะได้ค่า a_1 เนื่องจาก M_2 มีค่าเท่ากับ m_1 และ M_3 เท่ากับ $m_1 \bullet m_2$

สำหรับตัวอย่างการคำนวณในกรณีที่มีสมาชิก 3 คน ดังแสดงได้ดังต่อไปนี้

$$x = ((255x^6 - 204x^5 + 204x^3 - 102x^2 + 51x + 255) +$$
$$(-260x^6 - 260x^5 + 104x^4 + 104x^3 - 156x^2 + 104x - 52))(-1767) +$$
$$(-8840x^6 - 8840x^5 + 3536x^4 + 3536x^3 - 5304x^2 + 3536x - 1768)$$
$$(\text{mod } 13 \text{ X } 17 \text{ X } 19)$$
$$= 4194x^6 + 1083x^5 + 325x^4 + 971x^3 + 1289x^2 + 2586x + 4181 \quad (4)$$

หมายเหตุ กำหนดให้ $h_3 = 8x^6 + 9x^5 + 8x^4 + 4x^3 + 7x^2 + x + 4$ (h_3 คือ กุญแจสาธารณะของสมาชิกคนที่ 3)

เมื่อผู้ใช้คนที่ 1 รับค่า x แล้วถอดข้อความด้วย m_1 ดังต่อไปนี้

$$a_1 = x \text{ mod } m_1$$
$$= (4194x^6 + 1083x^5 + 325x^4 + 971x^3 + 1289x^2 + 2586x + 4181) \text{ mod } 13$$
$$= 8x^6 + 4x^5 + 9x^3 + 2x^2 + 12x + 8 \quad (5)$$

จากนั้นนำ a_1 มาถอดรหัสด้วยกุญแจส่วนตัวของผู้ใช้คนที่ 1 เองเพื่อรับ key

ในกรณีที่ผู้ใช้คนที่ 4 เข้ามาเป็นสมาชิกใหม่ ดังแสดงในภาพที่ 3 Key Server สามารถคำนวณหา y_4 ได้อย่างรวดเร็ว ดังนั้น Key Server ก็จะกำหนดกุญแจใหม่แล้วเข้ารหัสสำหรับผู้ใช้คนที่ 1, 2, 3 และ 4 ได้ค่าเป็น a_1, a_2, a_3 และ a_4 ตามลำดับแล้วคำนวณผลเฉลยด้วยทฤษฎีเศษเหลือของจีนจึงได้

$$x = ((a_1M_1y_1 + a_2M_2y_2)M_{12}y_{12} + a_3M_3y_3)M_{123}y_{123} + a_4M_4y_4 (\text{mod } m)$$

และกรณีที่สมาชิกใดออกจากกลุ่ม key server จะ set Flag ให้แก่โหนดของสมาชิกนั้นโดย กำหนดให้ค่าหลังการเข้ารหัสของกุญแจ (e) ของสมาชิกผู้นั้นมีค่าเป็น 0 ดังนั้นหากผู้ใช้คนนั้นทำการ Mod ค่า X ที่ได้แพร่มา ก็จะได้ค่าเป็น 0 ทำให้ User คนนั้นไม่สามารถที่จะทราบข้อมูลในกลุ่มได้ นอกจากนั้นเมื่อสมาชิกใหม่เข้ามาสามารถกำหนดให้สมาชิกใหม่ใช้โหนดของต้นไม้ที่ได้เคย set Flag ไว้ทำให้สามารถใช้ค่า M, y และ m ของโหนดเดิมได้

5. วิเคราะห์และเปรียบเทียบประสิทธิภาพ

5.1 กรณีของสมาชิกในกลุ่มสื่อสาร ($User_i$)

5.1.1 ด้านหน่วยความจำ สำหรับพื้นที่เก็บข้อมูลบนหน่วยความจำของแต่ละสมาชิกนั้น จะใช้พื้นที่สำหรับเก็บกุญแจส่วนตัวของตนเองเพียงค่าเดียวเท่านั้น

5.1.2 ด้านการคำนวณ เมื่อสมาชิกแต่ละคนได้รับค่า X มาแล้วเขา mod ค่า X ที่ได้รับด้วย m_i แล้วถอดรหัสด้วยเทคนิควิธี NTRU เพียง 1 ครั้งเท่านั้น

5.2 กรณีของ Key Server

5.2.1 ด้านหน่วยความจำ Key Server จะต้องใช้พื้นที่ในการเก็บโครงสร้างต้นไม้เพื่อเก็บค่า inverse ซึ่งแต่ละโหนดมีค่า M, y และ m

5.2.2 ด้านการคำนวณ เมื่อมีสมาชิกใหม่เข้ามา Key Server จะทำการคำนวณค่า inverse ของโหนดลูกเพียงแค่ 2 โหนดของรากต้นไม้ แล้วคำนวณค่า e (ค่า a_i) ของสมาชิกประมาณ n ครั้ง และค่า $a \times My$ ประมาณ $2n$ ครั้ง และคำนวณผลบวกของค่า aMy ประมาณ n ครั้ง

5.3 กรณีที่ไม่ใช้โครงสร้างต้นไม้ key server ต้องคำนวณค่า inverse ประมาณ n ครั้ง คำนวณ e จำนวน n ครั้ง ค่าประมาณ n ครั้ง คำนวณผลบวกของประมาณ n ครั้ง

6. สรุป

งานวิจัยนี้ได้นำเอาทฤษฎีเศษเหลือของจีนมาประยุกต์เพื่อเข้ารหัสลับแบบกลุ่มซึ่งใช้เทคนิคของ NTRU โดยมีการใช้ key server ทำหน้าที่ในการเข้ารหัสลับแบบกลุ่มเพื่อส่งกุญแจกลุ่มที่ใช้สำหรับเข้ารหัสลับข้อมูลจริง ให้แก่สมาชิกในกลุ่ม โดยส่งกุญแจกลุ่มซึ่งถูกเข้ารหัสไปเพียงข้อความเดียว ซึ่งอาศัยทฤษฎีเศษเหลือของจีน แล้วสมาชิกแต่ละคนจะสามารถถอดข้อความที่ส่งมาเฉพาะสำหรับตนเองได้ จากนั้นใช้กุญแจส่วนตัวของตน เพื่อถอดรหัสลับเพื่อได้กุญแจกลุ่ม

เพื่อให้ key server มีการประมวลผลอย่างรวดเร็วจึงมีการใช้โครงสร้างต้นไม้มาช่วยในการประมวลผล ซึ่งการใช้โครงสร้างต้นไม้ ทำให้การใช้ทฤษฎีเศษเหลือของจีน ซึ่งเคยใช้ได้เฉพาะกลุ่มเล็กๆ เนื่องจากต้องคำนวณค่า inverse ของทุกสมาชิกใหม่ทุกครั้งเมื่อมีสมาชิกเข้าออกนั้น กลับสามารถรองรับการทำงานของกลุ่มที่มีสมาชิกจำนวนมากได้ เพราะมีการคำนวณ inverse เพียง 2 ค่าทุกๆ ครั้งที่มีสมาชิกใหม่เข้าสู่กลุ่มและไม่ต้องคำนวณค่า inverse ในกรณีที่มีสมาชิกออกจากกลุ่ม

7. เอกสารอ้างอิง

[1] A. Fiat and M. Naor, "Broadcast Encryption : Advances in cryptology-CRYPTO '93," *Proceedings of 13th Annual International Cryptology Conference*, Santa Barbara, California, USA, Vol. 773, pp. 480-491, August 22-26, 1993.

[2] Y. Challal and H. Seba, "Group key management protocols: a novel taxonomy," *International Journal of Information Technology*, Vol. 2, No. 1, pp. 105-118, 2005.

[3] K.-C. Chan and S.-H. G. Chan. "Key management approaches to offer data confidentiality for secure multicast," *IEEE network*, Vol. 17, No. 8, pp. 30-39, 2003.

[4] X. Zheng, C.-T. Huang and M. Matthews, "Chinese remainder theorem based group key management," *Proceedings of the 45th annual southeast regional conference (ACM-SE 45)*, New York, USA, March 23-24, 2007.

[5] G.-H. Chiou and W.-T. Chen, "Secure broadcasting using the secure lock," *IEEE Transactions on Engineering*, Vol. 15, No. 8, pp. 929-934, 1989.

[6] J. Zhou and Y.-H. Ou, "Key tree and Chinese remainder theorem based group key distribution scheme," *Journal of the Chinese of Engineerings*, Vol. 32, pp. 967-974, 2009.

[7] P. P. Roja, P. S. Avadhani and E. V. Prasad, "An efficient method of shared key generation based on truncated polynomials," *IJCSNS International Journal of Computer Science and Network Security*, Vol. 6, No.8B, pp. 156-160, 2006.