การจัดการกุญแจกลุ่มโดยใช้หลักการของทฤษฎีเศษเหลือของจีน และโครงสร้างต้นไม้และการประยุกต์กับการสนทนา เป็นความลับบนคลาวด์

Chinese Remainder Theorem and Tree Structure Based Group Key Management and Its Application for Secure Chat on the Cloud

พิพัฒน์ หิรัณย์วณิชชากร์ (Pipat Hiranvanichakorn)* และ พูนศักดิ์ พรเพิ่มพูน (Poonsuk Ponpurmpoon)**

บทคัดย่อ

งานวิจัยนี้นำเสนอการจัดการกุญแจกลุ่มเพื่อส่งข้อมูลความลับเฉพาะกลุ่มโดยอาศัยหลักการของทฤษฎีเศษเหลือของจีนและโครงสร้างต้นไม้ และนำแนวคิดนี้ไปประยุกต์กับการสนทนาเป็นกลุ่มผ่านเครือข่ายอินเทอร์เน็ตโดยใช้ทรัพยากรของคลาวด์เป็นแม่ข่ายในการจัดการกุญแจกลุ่มและทำหน้าที่กระจายข้อความที่เป็นความลับให้แก่สมาชิกในกลุ่ม ในงานวิจัยนี้แนวคิดของทฤษฎีเศษเหลือของจีนถูกใช้เพื่อกระจายกุญแจกลุ่มให้เป็นข้อความที่เป็นความลับเพียงข้อความเดียวให้แก่สมาชิกของกลุ่ม และยังมีการใช้โครงสร้างต้นไม้แบบไบนารีทางเดียว เพื่อช่วยลดการคำนวณที่ต้องทำทุกครั้งที่มีการเปลี่ยนแปลงสมาชิก ข้อดีอีกอย่างหนึ่งของแนวคิดที่ใช้ในงานวิจัยนี้คือ เครื่องลูกข่ายเพียงคำนวณการมอดุโล (modulo) หนึ่งครั้ง และทำการ XOR หนึ่งครั้งก็จะคำนวณได้กุญแจกลุ่มมาใช้ในการเข้ารหัสลับ ในการพัฒนาโปรแกรมสนทนาเป็นความลับเฉพาะกลุ่ม งานวิจัยนี้ใช้ทรัพยากรคลาวด์ของ Windows Azure ทำหน้าที่เป็นแม่ข่ายของระบบ และใช้แพลตฟอร์มวินโดวส์และแอนดรอยด์ (Android) ในการพัฒนาโปรแกรมในฝั่งเครื่องลูกข่ายของผู้ใช้

คำสำคัญ: คลาวด์คอมพิวติ้ง ทฤษฎีเศษเหลือของจีน ตัวผกผันการคูณ

Abstract

This paper reports a group key management protocol based on Chinese Remainder Theorem (CRT) and a tree structure. The proposed protocol is applied in the development of a secure group chatting system which uses resources in the cloud for managing the group key and broadcasting encrypted messages to the group members. In this paper, Chinese Remainder Theorem is utilized to combine messages into one for broadcasting to all members. Furthermore, anunidirectional binary tree structure is utilized to lessen the calculation of the multiplicative inverses which have been done each time when a member joins or leaves the group. The other advantage of the proposed method is that each client needs to compute only 1 modulo arithmetic and 1 XOR operation in order to obtain the group key. In developing the chatting system, Windows Azure is used to implement services in the cloud. As for client side, Windows and Android platforms are adopted.

Keyword: Cloud Computing, Chinese Remainder Theorem, Multiplicative Inverses.

* *รองศาสตราจารย์ คณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์*

** *ห้างหุ้นส่วนจำกัดเทียนฮกเฮง*

1. ความเป็นมาของปัญหา

การส่งข้อมูลเป็นความลับเฉพาะกลุ่ม (secure multicast communication) เป็นการส่งข้อมูล ซึ่งมีเฉพาะสมาชิกของกลุ่มขณะนั้นเท่านั้นที่สามารถอ่านข้อความที่ส่งถึงกันได้ งานวิจัยเกี่ยวกับการส่งข้อมูลเป็นความลับแบบกลุ่มได้มีการดำเนินการอย่างแพร่หลาย [1-10] เนื่องจากสามารถนำไปประยุกต์ใช้ในด้านต่างๆ เช่น วีดีทัศน์ตามคำขอ (video on demand) การประชุมทางไกล อีเลิร์นนิง เป็นต้น ในการส่งข้อมูลเป็นความลับแบบกลุ่มนี้ สมาชิกทุกคนที่อยู่ในกลุ่มจะต้องมีกุญแจกลุ่ม (group key) ร่วมกัน เพื่อใช้ในการเข้ารหัสลับและถอดรหัสลับข้อความที่ส่งถึงกัน สำหรับการจัดการกุญแจกลุ่มสามารถแบ่งได้ 3 เทคนิควิธีคือ แบบที่สมาชิกในกลุ่มร่วมกันสร้างและปรับปรุงกุญแจกลุ่ม (contributory key agreement approach) แบบนี้เหมาะสำหรับกลุ่มสมาชิกขนาดเล็ก แบบที่สองเป็นแบบที่แบ่งกลุ่มใหญ่เป็นกลุ่มย่อยและในแต่ละกลุ่มย่อยมีเอเยนต์ที่ทำหน้าที่ส่งต่อกุญแจกลุ่มที่ได้รับจากแม่ข่าย เพื่อกระจายให้สมาชิกในกลุ่มย่อย (distributed group key management) ดังนั้น แบบนี้จึงไม่เหมาะสำหรับงานประยุกต์ที่ต้องการผลแบบทันที (real timeapplication) สำหรับแบบที่สามเป็นแบบที่มีแม่ข่ายกลางทำหน้าที่สร้างและปรับปรุงกุญแจกลุ่ม และกระจายกุญแจกลุ่มให้แก่สมาชิก (centralized group key management) และเพื่อลดภาระในการกระจายข้อมูลของแม่ข่าย จึงมีประเด็นของการวิจัยเพื่อให้สามารถส่งข้อความเป็นความลับเพียงข้อความเดียวให้ทุกคนในกลุ่มได้โดยไม่ต้องส่งให้ทีละคน แนวคิดหลักของแบบใช้แม่ข่ายกลางนี้มีการใช้โครงสร้างต้นไม้เพื่อช่วยจัดการกุญแจกลุ่มให้มีประสิทธิภาพ จึงเป็นวิธีที่สามารถขยายจำนวนสมาชิกกลุ่มได้เป็นจำนวนมากๆ

ในการส่งข้อมูลเป็นความลับแบบกลุ่มนี้ มีผู้เสนองานวิจัย [6] [7] [9] ที่ใช้ทฤษฎีเศษเหลือของจีนในการรวมข้อความที่ต้องการส่งให้แก่แต่ละผู้ใช้ ให้เป็นข้อความเพียงข้อความเดียวแล้วกระจายให้แก่สมาชิกของกลุ่ม แต่ปัญหาของแนวคิดนี้คือ ต้องมีการคำนวณหาค่าตัวผกผันการคูณ (multiplicative inverses) ที่ต้องใช้ในทฤษฎีเศษเหลือของจีนของทุกผู้ใช้ทุกครั้งที่มีการเปลี่ยนแปลงจำนวนสมาชิก ซึ่งเมื่อจำนวนสมาชิกเดิมมีมากขึ้น จำนวนการคำนวณตัวผกผันการคูณก็จะมากตามในลักษณะของเส้นตรง ดังนั้นการคำนวณของตัวผกผันการคูณจึงอยู่ในอันดับของ $O(n)$

ในงานวิจัยนี้จึงได้นำเสนอวิธีการจัดการกุญแจกลุ่มโดยใช้แม่ข่ายกลางในการจัดการกุญแจกลุ่มและใช้โครงสร้างต้นไม้ไบนารีทางเดียวในการลดการคำนวณหาค่าตัวผกผันการคูณให้อยู่ในอันดับของ $O(1)$ เมื่อมีการเปลี่ยนแปลงจำนวนสมาชิก กล่าวคือการคำนวณค่าตัวผกผันการคูณจะเป็นจำนวนคงที่ นอกจากนั้น เทคนิคที่ใช้ในงานวิจัยนี้ยังมีข้อดีคือ ใช้ความสามารถในการประมวลผลของเครื่องลูกข่ายไม่มาก เพียงแต่คำนวณการมอดุโลหนึ่งครั้งและทำการ XOR หนึ่งครั้งเท่านั้น จึงอาจกล่าวได้ว่าเหมาะสำหรับอุปกรณ์เคลื่อนที่ที่มีความสามารถในการประมวลผลไม่มากและมีประเด็นปัญหาของแหล่งพลังงาน และเพื่อนำแนวคิดในงานวิจัยนี้ไปประยุกต์ใช้จริง จึงพัฒนาโปรแกรมสนทนาเป็นความลับเฉพาะกลุ่มบนคลาวด์ โดยมีการใช้ทรัพยากรของคลาวด์คือ Windows Azure ทำหน้าที่เป็นแม่ข่ายของระบบการจัดการกุญแจกลุ่ม และ การจัดการการสนทนากลุ่ม โดยเครื่องลูกข่ายสามารถใช้ได้ทั้งในแพลตฟอร์มวินโดวส์และแอนดรอยด์

2. งานวิจัยที่เกี่ยวข้อง

ในการส่งข้อมูลเป็นการลับในกลุ่ม สมาชิกทุกคนในกลุ่มในขณะนั้นต้องมีกุญแจเดียวกันเพื่อใช้สำหรับเข้ารหัสลับ (encryption) ข้อความและถอดรหัสลับ (decryption) และกุญแจกลุ่ม (group key) นี้ ต้องมีการเปลี่ยนแปลงเสมอเมื่อมีสมาชิกเพิ่ม (join) หรือออก (leave) จากกลุ่ม เพื่อไม่ให้สมาชิกที่เข้ามาใหม่ทราบข้อมูลที่ส่งกันในกลุ่มก่อนหน้าที่เขาจะเข้ามาเป็นสมาชิก (backward secrecy) หรือไม่ให้สมาชิกที่ออกจากกลุ่มไปทราบข้อมูลที่ส่งกันระหว่างสมาชิกที่เหลือในกลุ่ม (forward secrecy) สำหรับการเปลี่ยนกุญแจกลุ่มนั้น มีวิธีการจัดการโดยทั่วไปอยู่ 3 วิธี [1] แบบแรกนั้นสมาชิกทุกคนที่อยู่ในกลุ่มขณะนั้นช่วยกันสร้างกุญแจกลุ่มทุกครั้งที่มีการเปลี่ยนแปลงสมาชิก (contributory key Agreement approach) แบบนี้ภาระในการประมวลผลสร้างกุญแจจะเป็นของสมาชิกทุกคน และในการประมวลผลมีการส่งข้อมูลระหว่างกันเพื่อสร้างกุญแจกลุ่ม สำหรับข้อดีของแบบนี้คือ ไม่ต้องอาศัยแม่ข่ายหลักในการสร้างกุญแจกลุ่มและส่งกุญแจกลุ่มให้กับสมาชิกของกลุ่ม ดังนั้น แบบนี้จึงเหมาะสำหรับสร้างกุญแจกลุ่มสำหรับกลุ่มที่ไม่โตมาก และนิยมใช้ในการส่งข้อมูลของเครือข่ายไร้สายที่มีสมาชิก

เข้าออกอยู่เสมอ (Mobile Adhoc Network) ซึ่งแม่ข่ายหลักอาจไม่สามารถอยู่ในเครือข่ายได้ตลอดเวลา

แบบที่สอง มีการใช้ความสามารถในการประมวลของเครื่องแม่ข่ายในการสร้างกุญแจกลุ่มและกระจายกุญแจกลุ่มให้แก่สมาชิกของกลุ่ม (centralized group key management) แบบนี้จะสามารถจัดการกุญแจกลุ่มสำหรับกลุ่มสมาชิกที่มีขนาดโตได้ และเพื่อให้ระบบทำงานได้รวดเร็วขึ้น จึงมักมีการใช้โครงสร้างต้นไม้มาช่วยในการจัดการกุญแจกลุ่ม ดังนั้น จึงมีประเด็นปัญหาของการปรับโครงสร้างต้นไม้ให้สมดุลย์ทุกครั้งที่มีการเพิ่มหรือลดสมาชิกของกลุ่ม รูปแบบที่สามเป็นแบบกระจาย (distributed group key management) แบบนี้กลุ่มจะถูกแบ่งเป็นกลุ่มย่อยๆ และจะมีตัวควบคุมการทำงานของแต่ละกลุ่มย่อย (control agents) ในการส่งกุญแจกลุ่มแม่ข่ายกลางจะส่งกุญแจกลุ่มซึ่งถูกเข้ารหัสลับให้แก่ตัวควบคุมของแต่ละกลุ่มย่อย ซึ่งตัวควบคุมจะถอดรหัสลับ แล้วส่งกุญแจกลุ่มที่ถูกเข้ารหัสลับด้วยกุญแจเฉพาะของกลุ่มย่อยให้แก่สมาชิกของกลุ่มย่อยนั้น แบบนี้มีข้อดีคือ เมื่อมีการเปลี่ยนแปลงสมาชิกในกลุ่มย่อยใด จะมีการเปลี่ยนกุญแจเฉพาะที่ใช้สำหรับกลุ่มย่อยนั้นๆ เท่านั้น เพื่อไม่ให้สมาชิกใหม่หรือสมาชิกที่ออกไปจากกลุ่มย่อยได้รู้ถึงกุญแจกลุ่มที่ใช้ในการส่งข้อมูลเป็นความลับแก่กัน สำหรับข้อเสียของแบบนี้ ต้องมีตัวควบคุมซึ่งทำหน้าที่เป็นตัวส่งผ่าน (relay) กุญแจกลุ่มให้แก่สมาชิกของแต่ละกลุ่มย่อย ทำให้ระบบต้องมีค่าใช้จ่ายเพิ่มขึ้นและทำให้การส่งกุญแจล่าช้าลงไป จึงไม่เหมาะสำหรับงานประยุกต์ส่งข้อมูลตามเวลาจริง เช่น วิดีโอหรือเสียง เป็นต้น

ในงานวิจัยที่นำเสนอนี้ เป็นการจัดการกุญแจกลุ่มแบบรวมศูนย์โดยใช้แม่ข่ายที่อยู่ในคลาวด์ของผู้ให้บริการคลาวด์ทำการปรับปรุงกุญแจกลุ่มเมื่อมีการเปลี่ยนแปลงสมาชิกในกลุ่ม และกระจายกุญแจกลุ่มให้แก่สมาชิกของกลุ่ม

ในงานวิจัย [7] ได้มีการเสนอเทคนิค Chinese Remaindering Group Key (CRGK) ซึ่งเป็นวิธีจัดการกุญแจกลุ่ม โดยอาศัยความสามารถในการประมวลผลของเครื่องแม่ข่ายเป็นหลักในการสร้างและส่งกุญแจกลุ่ม ในงานวิจัยนี้ แม่ข่ายของระบบจะแจกกุญแจส่วนตัว (private key) ให้แก่ผู้ใช้แต่ละคนในขั้นตอนของการยืนยันตัวเองของผู้ใช้กับแม่ข่าย และในการส่งกุญแจกลุ่มให้แก่สมาชิกของกลุ่มนั้น แม่ข่ายจะกำหนดกุญแจกลุ่มขึ้นและนำกุญแจกลุ่มนี้ไปทำการ XOR กับกุญแจส่วนตัวของสมาชิกแต่ละคน แล้วใช้หลักการของทฤษฎีเศษเหลือของจีน (Chinese Remainder Theorem) ในการรวมผลของการทำ XOR ดังกล่าว แล้วส่งผลรวมที่ได้เป็นข้อความเพียงข้อความเดียวให้แก่สมาชิกของกลุ่ม ซึ่งข้อดีของงานวิจัยนี้คือ แม่ข่ายจะกระจายข้อความที่เป็นความลับเพียงข้อความเดียวให้แก่เหล่าสมาชิก และในส่วนของสมาชิกแต่ละคนจะมีการประมวลผลข้อมูลเพียงเล็กน้อย กล่าวคือ เพียงแค่ทำการมอดุโลข้อความที่รับมา แล้วทำการ XOR ผลจากการมอดุโลด้วยกุญแจส่วนตัวของตน ก็จะคำนวณได้กุญแจกลุ่ม ดังนั้น วิธีการนี้จึงเหมาะสำหรับอุปกรณ์มือถือที่มีความสามารถในการประมวลผลไม่สูงนักและมีข้อจำกัดของแหล่งพลังงาน แต่อย่างไรก็ตาม ในส่วนของแม่ข่ายต้องมีคำนวณหาค่าตัวผกผันการคูณถึง n ค่าสำหรับสมาชิกของกลุ่ม n คน กล่าวคือ การประมวลผลของแม่ข่ายอยู่ในอันดับของ $O(n)$ ดังนั้นเพื่อลดภาระในการประมวลผลของแม่ข่าย งานวิจัย [8] ได้นำเสนอการใช้โครงสร้างต้นไม้ (key tree) เพื่อลดจำนวนการหาค่าตัวผกผันการคูณลง ทำให้การคำนวณของทฤษฎีเศษเหลือของจีนรวดเร็วขึ้น และสามารถรองรับสมาชิกจำนวนมากๆ ได้ แต่อย่างไรก็ตาม แนวคิดของโครงสร้างต้นไม้ที่เสนอในงานวิจัย [8] ใช้ได้สำหรับกรณีที่มีการกำหนดจำนวนสมาชิกของกลุ่มไว้แน่นอนล่วงหน้าแล้วในขณะใดขณะหนึ่งมีการส่งข้อมูลเป็นลับแก่กันในกลุ่มย่อยกลุ่มใดกลุ่มหนึ่งของสมาชิกทั้งหมด กล่าวคือ งานวิจัย [8] นี้ไม่เหมาะสำหรับการส่งข้อมูลเป็นความลับในกลุ่มที่มีสมาชิกเข้าและออกอยู่เสมอ

ในงานวิจัย [9] ได้ใช้หลักการของ Generalized Chinese Remainder Theorem (GCRT) เพื่อให้แม่ข่ายกุญแจส่งกุญแจกลุ่มให้แก่สมาชิกของกลุ่ม โดยมีการยืนยันตัวตนด้วยว่ากุญแจกลุ่มถูกส่งมาจากแม่ข่ายกุญแจจริง ซึ่งในการคำนวณค่ากุญแจกลุ่มนั้น ทั้งแม่ข่ายและแต่ละสมาชิกของกลุ่มจะต้องมีการประมวลผลอยู่ในอันดับของ $O(n)$ จึงไม่เหมาะสำหรับกลุ่มของสมาชิกที่ใช้อุปกรณ์มือถือที่มีความสามารถในการประมวลผลไม่มาก โดยเฉพาะเมื่อสมาชิกกลุ่มมีจำนวนมาก ในงานวิจัย [10] ใช้แนวคิดทำนองเดียวกับเทคนิค Fast CRGK วิธีที่เสนอในงานวิจัย [7] คือการกำหนดจำนวนสมาชิกของกลุ่มที่อาจเป็นไปได้ทั้งหมดไว้ล่วงหน้า และมีการคำนวณค่าตัวผกผันการคูณที่ต้องใช้ไว้ทั้งหมด ดังนั้นเมื่อมีสมาชิกเพิ่มขึ้นหรือลดลงในกลุ่มซึ่งยังไม่ถึงจำนวนที่ตั้งไว้

จึงไม่ต้องมีการคำนวณค่าตัวผกผันการคูณใหม่ กล่าวคือ การคำนวณค่าตัวผกผันการคูณอยู่ในอันดับของ $O(1)$ แต่อย่างไรก็ตาม เมื่อจำนวนสมาชิกของกลุ่มเพิ่มขึ้นถึงจำนวนที่กำหนดไว้แล้ว ระบบต้องมีการคำนวณค่าตัวผกผันการคูณใหม่ทั้งหมดเท่าจำนวนสมาชิกที่คาดว่าจะมีได้ ซึ่งการคำนวณจะอยู่ในอันดับของ $O(n)$ ดังนั้นจึงอาจกล่าวได้ว่าระบบนี้ไม่เหมาะสำหรับงานประยุกต์ที่มีการเปลี่ยนแปลงจำนวนสมาชิกอย่างรวดเร็ว

ในงานวิจัย [5] ได้ใช้เทคนิควิธี NTRU ซึ่งเป็นการเข้ารหัสลับแบบกุญแจอสมมาตรเพื่อเข้ารหัสลับกุญแจกลุ่มสำหรับแต่ละสมาชิกของกลุ่ม แล้วใช้หลักการของทฤษฎีเศษเหลือของจีนและโครงสร้างต้นไม้แบบไบนารีทางเดียวในการรวมข้อมูลที่ต้องการส่งให้แก่แต่ละสมาชิกกลุ่มให้เป็นข้อความเดียวเพื่อส่งให้แก่สมาชิกกลุ่ม ซึ่งสมาชิกแต่ละคนจะทำการคำนวณมอดุโลเพื่อถอดเอาเฉพาะข้อความที่ส่งให้กับตนเองออกมา แล้วถอดรหัสลับของเทคนิควิธี NTRU เพื่อได้กุญแจกลุ่มออกมาใช้ ข้อดีของงานวิจัยนี้คือ การเพิ่มหรือลดสมาชิกของกลุ่มทำได้โดยง่าย แต่การที่จะส่งข้อมูลให้สมาชิก n คนนั้น แม่ข่ายหรือผู้ส่งต้องเข้ารหัสลับแบบกุญแจอสมมาตร n ครั้ง

เพื่อเพิ่มประสิทธิภาพของการส่งข้อมูลเป็นความลับสำหรับกลุ่ม งานวิจัยนี้จึงนำแนวคิดของงานวิจัย [5] มาประยุกต์กับงานวิจัย [7] ซึ่งทำให้การประมวลข้อมูลของทั้งฝั่งแม่ข่ายและผู้ใช้ลดลง โดยการคำนวณหาค่าตัวผกผันการคูณลดลงจาก $O(n)$ เป็น $O(1)$ เมื่อมีการเปลี่ยนแปลงของสมาชิก และในฝั่งรับจะคำนวณเพียงการมอดุโลหนึ่งครั้ง และการ XOR หนึ่งครั้งเท่านั้น ก็จะได้กุญแจกลุ่มมาใช้ นอกจากนั้นยังได้ใช้แนวคิดของงานวิจัยนี้ไปประยุกต์สำหรับการประมวลผลในคลาวด์ ซึ่งประเด็นของการใช้ทรัพยากรเป็นสิ่งสำคัญของระบบ

เพื่อให้เข้าใจแนวคิดของงานวิจัยที่นำเสนอนี้ จะเริ่มด้วยการแนะนำคณิตศาสตร์เศษเหลือดังต่อไปนี้

3. คณิตศาสตร์เศษเหลือ

3.1 ตัวผกผันการคูณ (multiplicative inverse)

กำหนดให้ a และ m เป็นตัวเลขเต็มบวกที่มีค่า หรม. (a, m) เท่ากับ 1 แล้ว โดยหลักการของ extended Euclidean algorithm จะได้ว่า เราสามารถหาตัวเลขจำนวนเต็ม s และ t ที่ทำให้สมการที่ (1) เป็นจริง

$$s \cdot a + t \cdot m = 1 \tag{1}$$

จากสมการที่ (1) จะได้ว่า

$$s \cdot a \equiv 1 \bmod m$$

และ $$t \cdot m \equiv 1 \bmod a$$

กล่าวคือ s เป็นตัวผกผันการคูณของ a modulo m และเช่นเดียวกัน t เป็นตัวผกผันการคูณของ m modulo a

นอกจากนั้น หากให้ $m = m_1 \cdot m_2$ เมื่อ m_1 และ m_2 เป็นตัวเลขเต็มบวกแล้ว เรายังได้ว่าจากสมการที่ (1) $s \cdot a \equiv 1 \bmod m_1$ และ $s \cdot a \equiv 1 \bmod m_2$ ด้วย

3.2 ทฤษฎีเศษเหลือของจีน

ให้ $m_1, m_2, ..., m_n$ เป็นเลขจำนวนเต็มบวกโดยมีคุณสมบัติว่า ค่า หรม. ของ $(m_i, m_j) = 1$ ทุกค่าที่ $i \neq j$ กล่าวคือ m_i, m_j มีคุณสมบัติเป็น pairwise relatively prime positive integers และให้ $a_1, a_2, ..., a_n$ เป็นเลขจำนวนเต็ม ดังนั้นสำหรับ Linear Congruence Systems ข้างล่างนี้

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_n \bmod m_n \end{aligned}$$

จะสามารถหาค่า X ได้จาก

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n (\bmod m) \tag{2}$$

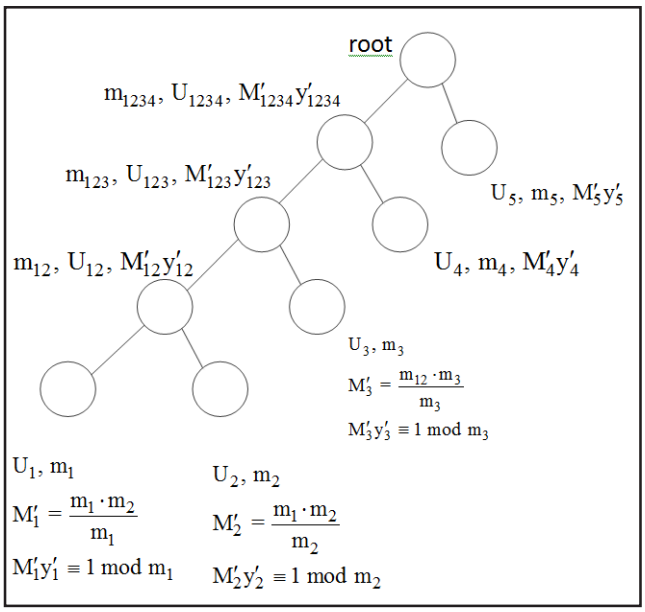
โดยที่ $m = m_1 \cdot m_2 \cdot m_3 \ldots m_n$ และ $M_i = \frac{m}{m_i}$ ส่วน y_i เป็นตัวผกผันการคูณของ M_i modulo m_i กล่าวคือ $M_i y_i \equiv 1 \bmod m_i$

4. โครงสร้างต้นไม้แบบไบนารีทางเดียว

ภาพที่ 1 แสดงโครงสร้างต้นไม้ที่ใช้ในงานวิจัยนี้

สำหรับโครงสร้างต้นไม้นี้โหนดใบไม้ (leaf nodes) ของต้นไม้จะแทนสมาชิก (U_i) ของกลุ่มสนทนาแต่ละโหนด (node) จะเก็บค่ากุญแจส่วนตัว (private key, m_i) และค่าผลคูณของตัวผกผันการคูณ ($M_i' y_i' \equiv 1 \bmod m_i$, โดยที่โหนดใบไม้ด้านขวามีค่า $M_r' = \frac{m_\ell \cdot m_r}{m_r}$ เมื่อ m_ℓ และ m_r เป็นค่ากุญแจส่วนตัวของโหนดด้านซ้ายและด้านขวาตามลำดับ ทำนองเดียวกัน $M_\ell' = \frac{m_\ell \cdot m_r}{m_\ell}$) ของแต่ละสมาชิก สำหรับโหนดภายในของ

ต้นไม้แต่ละโหนดจะเป็นเสมือนตัวแทนของโหนดลูกทั้งสองของมัน เช่น U_{12} จะเป็นตัวแทนของ U_1 และ U_2 ซึ่งโหนด U_{12} จะเก็บค่า m_{12} ซึ่งเท่ากับ $m_1 \cdot m_2$ และเก็บค่า $M'_{12}y'_{12} \equiv 1 \bmod m_{12}$ โดยที่ $M'_{12} = \frac{m_{12} \cdot m_3}{m_{12}}$ และทำนองเดียวกัน $M'_3 = \frac{m_{12} \cdot m_3}{m_3}$ และ $M'_3 y'_3 = 1 \bmod m_3$ สำหรับตัวอย่างของการคำนวณค่าในแต่ละโหนดจะแสดงรายละเอียดในหัวข้อต่อไป



ภาพที่ 1 *โครงสร้างต้นไม้ไบนารีทางเดียว*

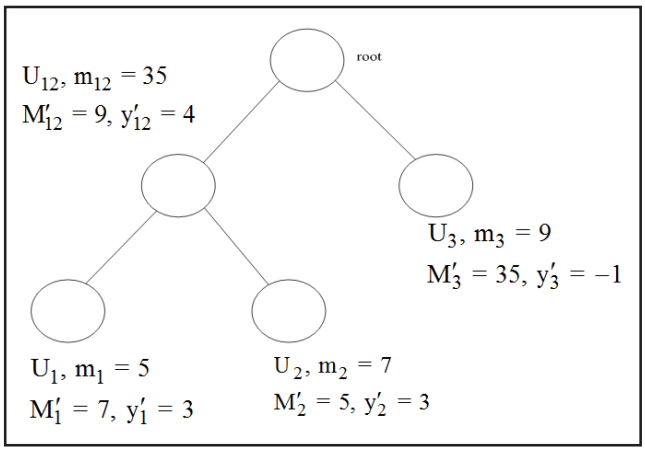
5. การกระจายกุญแจกลุ่มโดยใช้ทฤษฎีเศษเหลือของจีนและโครงสร้างต้นไม้ไบนารีทางเดียว

เพื่อให้เข้าใจถึงการทำงานของระบบที่นำเสนอได้ชัดเจนขึ้น จะขอแบ่งกระบวนการกระจายกุญแจกลุ่มเป็น 3 ขั้นตอน ขั้นตอนแรกเป็นการสร้างกลุ่มเริ่มต้น ในขั้นตอนนี้สมมุติว่ามีสมาชิกต้องการเข้ากลุ่ม 3 คน คือ U_1 U_2 และ U_3 โดยให้กุญแจส่วนตัวของแต่ละคนเป็นค่า m_1 m_2 และ m_3 ซึ่งค่าเหล่านี้แม่ข่ายจะให้แก่ผู้ใช้ในขั้นตอนลงทะเบียนซึ่งมีการยืนยันตัวเองของผู้ใช้ สำหรับการยืนยันตัวเองอาจจะใช้หลักการของกุญแจอสมมาตร ซึ่งหลักการยืนยันตัวเองนี้สามารถศึกษาได้จากหนังสือ [12] และงานวิจัยทั่วๆ ไป [1]

ในขั้นตอนสร้างกลุ่มเริ่มต้นนี้ แม่ข่ายจะกำหนดค่ากุญแจกลุ่ม (K) แบบสุ่มที่มีค่าน้อยกว่าทุก m_i ขึ้นมา แล้วนำมาคำนวณดังต่อไปนี้

$a_1 = K \oplus m_1, a_2 = K \oplus m_2$ และ $a_3 = K \oplus m_3$

และจะสร้างต้นไม้ไบนารีทางเดียวขึ้นมาดังภาพที่ 2 และมีการคำนวณค่า $M'_\ell y'_\ell$ และ $M'_r y'_r$ ของแต่ละคู่ของโหนดที่อยู่ในระดับเดียวกันตั้งแต่โหนดใบไม้ (leaf nodes) ล่างสุดขึ้นไป โดยที่ $M'_\ell = \frac{m_\ell \cdot m_r}{m_\ell}$ และ $M'_r = \frac{m_\ell \cdot m_r}{m_r}$ นอกจากนั้น $M'_\ell \cdot y'_\ell \equiv 1 \bmod m_\ell$ และ $M'_r \cdot y'_r \equiv 1 \bmod m_r$ ซึ่งจากรูปนี้จะเห็นว่า หากโหนด U_1 มีค่า $m_1 = 5$ โหนด U_2 มีค่า $m_2 = 7$ และโหนด U_3 มีค่า $m_3 = 9$ จะได้ค่า $M'_1 = \frac{m_1 \cdot m_2}{m_1} = 7$ และค่า y'_1 คำนวณจาก $M'_1y'_1 \equiv 1 \bmod m_1$ ได้ค่าเท่ากับ 3 ส่วน ค่า $M'_2 = \frac{m_1 \cdot m_2}{m_2} = 5$ และค่า y'_2 คำนวณจาก $M'_2y'_2 \equiv 1 \bmod m_2$ ได้ค่าเท่ากับ 3 นั่นเอง สำหรับโหนดพ่อของโหนด U_1 และ U_2 คือ U_{12} จะเป็นตัวแทนของ U_1 และ U_2 จะมีค่า $m_{12} = m_1 \cdot m_2$ ดังนั้น จะสามารถคำนวณค่า $M'_{12} = \frac{m_{12} \cdot m_3}{m_{12}} = 9$ และค่า $y'_{12} = 4$ ส่วนค่า $M'_3 = \frac{m_{12} \cdot m_3}{m_3} = 35$ และค่า $y'_3 = 1$



ภาพที่ 2 *โครงสร้างต้นไม้ในขั้นตอนการสร้างกลุ่มเริ่มต้น*

ถึงตอนนี้ แม่ข่ายสามารถคำนวณค่า X ของสมการ Congruence Systems ได้โดย

$$X = \left((a_1 M'_1 y'_1 + a_2 M'_2 y'_2) M'_{12} y'_{12} + a_3 M'_3 y'_3\right) \bmod (m_1 \cdot m_2 \cdot m_3) \quad (3)$$

จากสมการของ X นี้จะเห็นว่าค่า $a_1 M'_1 y'_1 + a_2 M'_2 y'_2$ เทียบได้กับค่า X_{12} (ค่า X ที่เกิดจากโหนด U_1 และ U_2) นั่นเอง

จากค่า X ข้างต้น หากทำการคำนวณ $X \bmod m_1$ จะได้ว่า เนื่องจาก $M'_3 = m_1 \cdot m_2$ ดังนั้น ค่า $a_3 M'_3 y' \bmod m_1$ เท่ากับศูนย์ และเนื่องจาก $M'_{12}y'_{12} \equiv 1 \bmod m_{12}$ และ $m_{12} = m_1 \cdot m_2$ ซึ่งจากหัวข้อ 3.1 จะได้ว่า $M'_{12}y'_{12} \equiv 1 \bmod m_1$ เช่นเดียวกัน นอกจากนั้น เนื่องจาก $M'_2 = m_1$ และ $M'_1y'_1 \equiv 1 \bmod m_1$ ดังนั้น ค่า $X \bmod m_1$ จะได้ค่าเป็น a_1

นั่นเอง ทำนองเดียวกันการคำนวณของ $X \bmod m_2$ จะได้ค่า a_2 และ $X \bmod m_3$ ก็จะได้ค่าของ a_3

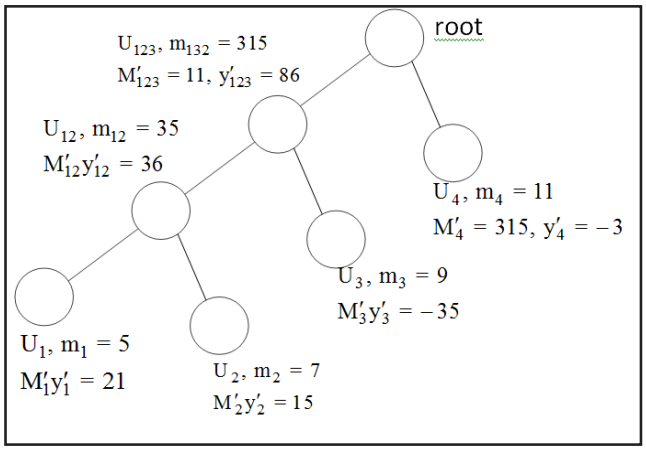
เมื่อแม่ข่ายกระจายค่า X ให้แก่สมาชิกกลุ่ม U_1 U_2 และ U_3 แล้ว สมาชิกแต่ละคนเมื่อคำนวณค่า $X \bmod m_i$ จะได้ค่า a_i ที่ถูกส่งมาให้ตัวเอง และเมื่อคำนวณค่า $a_i \oplus m_i$ ก็จะได้ค่าของกุญแจกลุ่ม (K) ที่ใช้ในการเข้ารหัสลับของกลุ่ม สำหรับผู้ใช้ที่ไม่ได้เป็นสมาชิกของกลุ่ม เนื่องจากไม่ทราบค่าที่ใช้ในการคำนวณค่า X ในทฤษฎีเศษเหลือของจีน จึงไม่สามารถคำนวณหาค่า a_i และ K ได้

เมื่อมีผู้ใช้รายใหม่เข้าร่วมเป็นสมาชิกของการสนทนานี้ แม่ข่ายจะทำการปรับปรุงโครงสร้างต้นไม้ โดยเพิ่มโหนดใบไม้เข้าไปในต้นไม้ต้นเดิม ดังแสดงในภาพที่ 3 ซึ่งแสดงโครงสร้างต้นไม้ที่ถูกปรับปรุงเมื่อผู้ใช้ U_4 ที่มีค่าของกุญแจส่วนตัวเป็น m_4 ถูกเพิ่มเข้าไปเป็นสมาชิกของการสนทนาเมื่อปรับปรุงโครงสร้างต้นไม้แล้ว แม่ข่ายจะสุ่มกุญแจกลุ่มตัวใหม่ (K') แล้วทำการ XOR กับค่ากุญแจส่วนตัวของสมาชิกกลุ่มแต่ละคน จึงได้ค่า $a_1 = K' \oplus m_1$ ค่า $a_2 = K' \oplus m_2$ ค่า $a_3 = K' \oplus m_3$ และค่า $a_4 = K' \oplus m_4$ แล้วคำนวณค่า X ใหม่ได้เป็น

$$X = \left(\left((a_1 M'_1 y'_1 + a_2 M'_2 y'_2) M'_{12} y'_{12} + a_3 M'_3 y'_3\right) M'_{123} y'_{123} + a_4 M'_4 y'_4\right) \bmod (m_1 \cdot m_2 \cdot m_3 \cdot m_4) \quad (4)$$

ซึ่งเมื่อกระจายค่า X ออกไปให้สมาชิกของกลุ่ม แต่ละคนก็จะสามารถคำนวณหาค่าของกุญแจกลุ่มได้ โดยทำการคำนวณมอดุโลหนึ่งครั้ง และ XOR อีกหนึ่งครั้ง

ในการปรับปรุงโครงสร้างต้นไม้ดังกล่าวข้างต้นจะเห็นว่า แม่ข่ายไม่จำเป็นต้องคำนวณค่าตัวผกผันการคูณของทุกสมาชิก จะคำนวณค่าตัวผกผันการคูณสำหรับ 2 โหนดบนสุดของต้นไม้เท่านั้น ดังนั้นจึงกล่าวได้ว่า การคำนวนค่าตัวผกผันการคูณอยู่ในลำดับของ $O(1)$ นอกจากนี้ในสมการที่ (4) จะเห็นว่า เมื่อสมาชิกเพิ่มขึ้นจาก 3 คนเป็น 4 คนนั้น มีการบวก 3 ครั้ง และจะเพิ่มขึ้นเมื่อจำนวนสมาชิกเพิ่มขึ้น ดังนั้นการบวกจะอยู่ในลำดับของ $O(n)$ ส่วนการคูณในสมการที่ (4) นั้นมีการคูณ 6 ครั้ง คือจำนวน $2n$ จึงกล่าวได้ว่าการคูณอยู่ในอันดับของ $O(n)$ ในแง่มุมของความมั่นคงนั้น เนื่องจากแม่ข่ายมีการเปลี่ยนค่ากุญแจกลุ่มใหม่ ดังนั้นสมาชิกใหม่ที่เข้าสู่ระบบจึงไม่สามารถทราบข้อมูลของการสนทนาก่อนหน้านี้ กล่าวคือ เกิด backward secrecy



ภาพที่ 3 *โครงสร้างต้นไม้เมื่อมีสมาชิก U_4 เพิ่มเข้าไป*

ในกรณีที่สมาชิกออกจากกลุ่มนั้น แม่ข่ายเพียงแต่สุ่มค่ากุญแจกลุ่ม (K') ขึ้นใหม่แล้วทำการ XOR กุญแจกลุ่มกับกุญแจส่วนตัวของสมาชิกที่เหลือ แล้วคำนวณค่า X ใหม่ ดังตัวอย่างเช่น จากภาพที่ 3 หาก U_2 ออกจากการเป็นสมาชิก แม่ข่ายจะคำนวณ $a_1 = K' \oplus m_1$ ค่า $a_3 = K' \oplus m_3$ ค่า $a_4 = K' \oplus m_4$ และกำหนดให้ $a_2 = r$ โดยที่ r เป็นค่าสุ่ม (random) ค่าหนึ่งที่ไม่เท่ากับ K' แล้วจะคำนวณค่า X ได้เป็น

$$X = \left(\left((a_1 M'_1 y'_1 + r M'_2 y'_2) M'_{12} y'_{12} + a_3 M'_3 y'_3\right) M'_{123} y'_{123} + a_4 M'_4 y'_4\right) \bmod (m_1 \cdot m_2 \cdot m_3 \cdot m_4) \quad (5)$$

เมื่อสมาชิกของกลุ่มได้รับค่า X ที่ถูกแพร่มาก็จะสามารถคำนวณหาค่ากุญแจกลุ่มได้ แต่สำหรับสมาชิก U_2 ที่ออกจากกลุ่มไป หากคำนวณ $X \bmod m_2$ ก็จะได้ค่าตัวเลขสุ่ม r จึงไม่สามารถคำนวณหากุญแจกลุ่มได้ และไม่ทราบข้อความสนทนาของกลุ่ม หลังจากที่เขาออกจากกลุ่มไปนั่นคือ จะเกิด forward secrecy และจากการคำนวณข้างต้น จะเห็นได้ว่าในกรณีที่สมาชิกออกจากกลุ่มนี้ ไม่จำเป็นต้องคำนวณหาค่าตัวผกผันการคูณใหม่เลย แต่อย่างไรก็ตามเนื่องจากโหนด U_2 ยังอยู่ในโครงสร้างต้นไม้ ดังนั้น ค่ากุญแจส่วนตัว m_2 จึงไม่สามารถนำไปใช้สำหรับผู้ใช้รายใหม่ได้

6. การวิเคราะห์ความมั่นคงของระบบ

ในงานวิจัย [7] ได้วิเคราะห์ความมั่นคงของแนวคิดการใช้ค่า pairwise relatively prime เป็นกุญแจส่วนตัวของผู้ใช้ โดยเนื่องจากค่า pairwise relatively prime นี้ มีจำนวนไม่จำกัด ดังนั้นเมื่อไม่ทราบค่ากุญแจส่วนตัวของสมาชิกในกลุ่ม จึงยากที่ผู้โจมตีจะคำนวณหาค่ากุญแจกลุ่มที่ส่งมาได้ อีกทั้งในการคำนวณค่า X นั้นมีทั้งการบวกและการคูณของตัวเลข

ที่ไม่ทราบค่า จึงยากที่จะใช้หลักการของการแยกตัวประกอบมาโจมตีระบบ นอกจากนั้น ในการอธิบายในหัวข้อ 5 จะเห็นได้ว่าในกรณีที่สมาชิกเพิ่มขึ้น ระบบจะมี backward secrecy และในกรณีที่สมาชิกออกจากกลุ่ม ระบบก็มี forward secrecy

7. การวิเคราะห์ประสิทธิภาพการคำนวณของระบบ

ตารางที่ 1 แสดงประสิทธิภาพการคำนวณของแม่ข่ายที่เสนอในงานวิจัยนี้เปรียบเทียบกับงานวิจัย [7] ส่วนงานวิจัย [8] ซึ่งมีการใช้โครงสร้างต้นไม้เช่นเดียวกัน แต่เนื่องจากไม่สามารถรองรับการเพิ่มและลดของสมาชิกได้ จึงไม่นำมาเปรียบเทียบกับงานวิจัยนี้ นอกจากนี้ เนื่องจากการคำนวนที่ใช้ในงานวิจัย [9] อยู่ในลำดับของ $O(n)$ ทั้งฝั่งของแม่ข่ายกุญแจและฝั่งของสมาชิก แต่ระบบที่เสนอสามารถยืนยันตัวบุคคลของแม่ข่ายกุญแจได้ ซึ่งแตกต่างกับงานวิจัยที่เสนอในบทความนี้ ในที่นี้จึงไม่ได้นำมาเปรียบเทียบเช่นเดียวกัน

จากตารางเห็นว่า ถึงแม้งานวิจัยนี้จะสามารถลดการคำนวณหาค่าตัวคูณผกผันได้ แต่การคูณและการบวกยังอยู่ใน $O(n)$ และจากภาพที่ 4 ซึ่งแสดงการคำนวณค่า X เมื่อมีสมาชิกเข้าร่วมเพิ่มขึ้น 1 คน จากสมาชิกเดิม n คน โดยใช้เครื่อง CPU i3-2530M Ram 8 GB และใช้ภาษา Java ในการพัฒนา จากภาพจะเห็นได้ว่าเมื่อจำนวนสมาชิกมีค่าเพิ่มมากขึ้น เวลาในการคำนวนค่า X จะเพิ่มมากขึ้น เนื่องจากมีการคูณและบวกของตัวเลขที่มีค่าโตเพิ่มมากขึ้น

แต่อย่างไรก็ตาม จากสมการที่ (4) หากให้ค่า a_i เท่ากันทุกๆ ตัว กล่าวคือ ให้ a_i ทุกตัวมีค่าเท่ากับ K ซึ่งเป็นกุญแจกลุ่ม โดยไม่ต้องทำการ XOR กับ m_i แล้วเราจะได้การคำนวนค่า X เป็น

$$X = K\left(\left(\left(M'_1y'_1 + M'_2y'_2\right)M'_{12}y'_{12} + M'_3y'_3\right)M'_{123}y'_{123} + M'_4y'_4\right) \bmod\left(m_1 \cdot m_2 \cdot m_3 \cdot m_4\right) \quad (6)$$

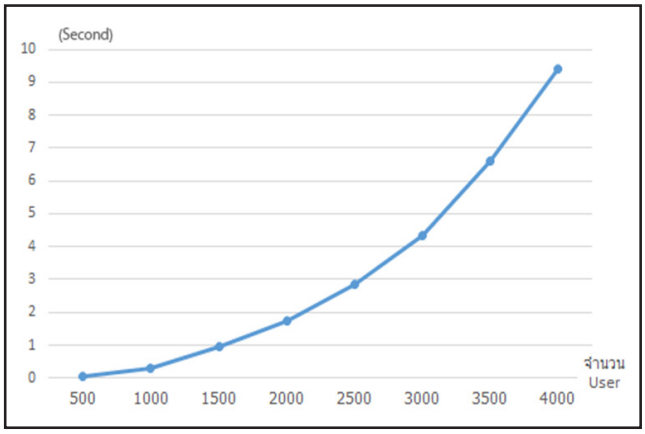
ซึ่งเทอม $\left(\left(M'_1y'_1 + M'_2y'_2\right)M'_{12}y'_{12} + M'_3y'_3\right)$ เป็นส่วนที่ได้จากการคำนวณค่า X ก่อนหน้านี้แล้ว ดังนั้นการคูณ การบวกของสมการที่ (6) จึงอยู่ในอันดับของ $O(1)$ วิธีนี้เป็นตัวอย่างหนึ่งที่อาจจะปรับปรุงระบบให้มีประสิทธิภาพเพิ่มมากขึ้น

8. การประยุกต์การส่งข้อมูลความลับ เฉพาะกลุ่มบนคลาวด์

หัวข้อต่อไปนี้เป็นการนำเอาแนวคิดที่ได้เสนอข้างต้นไปประยุกต์กับการส่งความลับเฉพาะกลุ่มบนคลาวด์ ซึ่งประเด็น

ตารางที่ 1 *การเปรียบเทียบประสิทธิภาพการคำนวณ*

		การสร้างกลุ่มเริ่มต้น	การเพิ่มสมาชิก 1 ราย	การลดสมาชิก 1 ราย
การคำนวณค่าตัวผกผันการคูณ	งานวิจัยที่นำเสนอ	$O(n)$ * ประมาณ $2n$	$O(1)$	$O(1)$
	งานวิจัยของ Zheng	$O(n)$	$O(n)$	$O(n)$
การคูณในการคำนวณค่า X	งานวิจัยที่นำเสนอ	$O(n)$	$O(n)$	$O(n)$
	งานวิจัยของ Zheng	$O(n)$	$O(n)$	$O(n)$
การบวกในการคำนวณค่า X	งานวิจัยที่นำเสนอ	$O(n)$	$O(n)$	$O(n)$
	งานวิจัยของ Zheng	$O(n)$	$O(n)$	$O(n)$



ภาพที่ 4 *เวลาในการคำนวณของแม่ข่ายกุญแจ*

ของการใช้ทรัพยากรของทั้งฝั่งแม่ข่ายให้บริการ และเครื่องลูกข่ายซึ่งอาจเป็นอุปกรณ์มือถือที่มีความสามารถการประมวลผลจำกัดเป็นประเด็นสำคัญอย่างหนึ่ง

จากการสำรวจของ International Data Group (IDG) ปี 2013 [11] พบว่า โปรแกรมประยุกต์บนคลาวด์ส่วนใหญ่เป็นโปรแกรมด้านเครือข่ายสังคม (social network) เพื่อการทำงานร่วมกัน การประชุมร่วมกันเพื่อแก้ปัญหา สำหรับโปรแกรมด้านเครือข่ายสังคม Line เป็นโปรแกรมประยุกต์ที่ทำให้มีการติดต่อสื่อสารระหว่างผู้ใช้ที่มีความนิยมมากอันหนึ่ง แต่มีหลายครั้งที่ผู้ใช้ต้องการให้ข้อมูลที่ส่งเป็นความลับระหว่างกลุ่มที่ส่งข้อมูลถึงกันภายในเครือข่ายอินเทอร์เน็ต

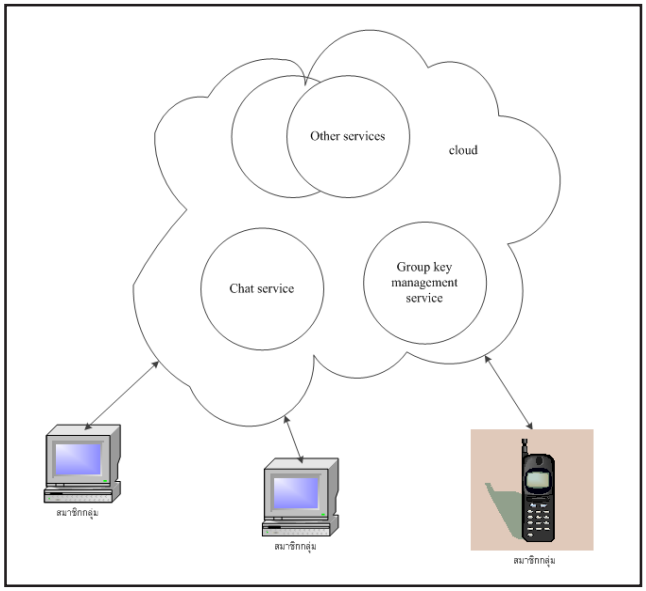
ซึ่งโปรแกรม Line ยังไม่รองรับในขณะนี้ งานวิจัยนี้จึงนำเสนอโปรแกรมที่สามารถสนทนาโดยข้อมูลที่ส่งจะถูกเข้ารหัสลับ และสามารถถอดอ่านได้เฉพาะสมาชิกที่อยู่ในกลุ่มขณะนั้นเท่านั้น

8.1 โปรแกรมสนทนาเป็นความลับเฉพาะกลุ่มบนคลาวด์

โปรแกรมประยุกต์บนคลาวด์ถูกพัฒนาในรูปแบบของ web services ซึ่งเป็นชนิดหนึ่งของการพัฒนาโปรแกรมด้วยเทคโนโลยีสถาปัตยกรรมเชิงให้บริการ (Service–Oriented Architecture, SOA) ซึ่งรูปแบบของ SOA เป็นแบบที่เป็นการพัฒนาโปรแกรมวัตถุที่ให้บริการ (service objects) ต่างๆ ที่มีหน้าที่ชัดเจน เช่นวัตถุ (object) ที่ทำหน้าที่คูณแมททริกซ์ หรือวัตถุ ที่ทำหน้าที่เปลี่ยนอุณหภูมิจากฟาเรนไฮต์เป็นเซลเซียส เป็นต้น ในการทำงาน โปรแกรมลูกข่ายจะส่งคำขอใช้บริการไปยังวัตถุที่ให้บริการในรูปแบบของตัวอักษร (text) เมื่อวัตถุที่ให้บริการทำงานตามคำขอเสร็จ จะส่งผลลัพธ์กลับมาในรูปแบบของตัวอักษรเช่นเดียวกัน การพัฒนารูปแบบ SOA นี้มีข้อดีสำคัญประการแรกคือ วัตถุที่ให้บริการถูกเรียกใช้งานได้หลายๆ ครั้ง (reuse) โดยโปรแกรมที่เรียกใช้ต่างๆ กัน ทำให้เป็นการใช้ทรัพยากรอย่างมีประสิทธิภาพ ข้อดีอีกประการหนึ่งคือ ภาษาที่ใช้ในการพัฒนาโปรแกรมเรียกขอและวัตถุที่ให้บริการไม่จำเป็นต้องเป็นภาษาโปรแกรมเดียวกัน เพราะไม่ว่าคำส่งร้องขอบริการหรือผลลัพธ์ของการให้บริการจะถูกส่งในรูปแบบข้อความตัวอักษรทั่วไป ด้วยสถาปัตยกรรมแบบนี้ จึงทำให้เครื่องคอมพิวเตอร์ต่างชนิดกัน ใช้ระบบปฏิบัติการแตกต่างกันก็สามารถที่จะทำงานส่งข้อมูลติดต่อกันได้

สำหรับโปรแกรมสนทนาเป็นความลับเฉพาะกลุ่มที่เสนอในงานวิจัยนี้ใช้ทรัพยากรของคลาวด์ทำหน้าที่เป็นแม่ข่ายให้บริการ โดยมีโปรแกรมวัตถุที่ให้บริการหลักสองชิ้น เพื่อให้บริการการจัดการกุญแจกลุ่ม ดังอธิบายในหัวข้อข้างต้น และให้บริการกระจายข้อมูลสนทนาของกลุ่ม ดังแสดงในภาพที่ 5 สำหรับภาษาที่ใช้ในการพัฒนางานวิจัยนี้แม่ข่ายใช้ภาษา VB ใน ASP.NET โดยอาศัยแพลตฟอร์ม Windows Azure ของ Microsoft cloud ส่วนเครื่องลูกข่ายใช้ภาษา VB บนแพลตฟอร์มวินโดวส์ และภาษา JAVA บนแพลตฟอร์มแอนดรอยด์ โดยใช้เครื่องคอมพิวเตอร์ CPU i3-2530M Ram 8 GB และโทรศัพท์เคลื่อนที่ Qualcomm MSM8660Dual-core 1.2 GHz 1GB Ram

ในการ implement โปรแกรมแม่ข่าย มีการใช้ Visual studio 2012 เป็นเครื่องมือในการพัฒนาวัตถุที่ให้บริการต่างๆ บนเครื่องคอมพิวเตอร์พีซี เมื่อพัฒนาวัตถุเสร็จแล้ว จึงส่ง (publish) วัตถุขึ้นไปติดตั้งบนคลาวด์สำหรับการส่งข้อมูลโต้ตอบระหว่างเครื่องลูกข่ายและแม่ข่ายนั้นใช้โพรโทคอล Simple Object Access Protocol (SOAP) ซึ่งสำหรับ .NET นั้นมีเครื่องมือในการสร้าง SOAP message ขึ้นมา ส่วน JAVA ในแพลตฟอร์ม Android นั้นผู้พัฒนาโปรแกรมจะต้องสร้าง SOAP message ขึ้นเอง



ภาพที่ 5 *การส่งข้อมูลติดต่อระหว่างผู้ใช้และ services บนคลาวด์*

สำหรับรูปแบบของการสนทนาแบบกลุ่มในงานวิจัยนี้ ในขั้นตอนแรกผู้ใช้ต้องลงทะเบียนกับระบบ secure chat ซึ่งทำงานอยู่บนคลาวด์ แล้วจะได้กุญแจส่วนตัว (m_i) ของผู้ใช้มา หลังจากนั้น ผู้ที่ต้องการสร้างกลุ่มสนทนา จะเลือกสมาชิกจากรายการข้อมูลของผู้ใช้ระบบ ซึ่งแม่ข่ายจะแจ้งไปบอกสมาชิกของกลุ่มให้ทราบว่าตนเองอยู่ในกลุ่มใด อนึ่งในการทำงานจริงนั้น เนื่องจาก web service ทำงานในรูปแบบเครื่องลูกข่ายและแม่ข่าย ดังนั้น เมื่อผู้ใช้เปิดระบบ secure chat โปรแกรมบนเครื่องผู้ใช้จะคอยไปตรวจสอบว่า ตัวเองอยู่ในกลุ่มสนทนากลุ่มใด และจะได้ค่า X ในหัวข้อ 5 ซึ่งแม่ข่ายได้คำนวณไว้แล้วมาคำนวณหากุญแจกลุ่ม แล้วจึงส่งคำร้องขอไปอ่านข้อความที่ถูกเข้ารหัสลับจาก buffer ของแม่ข่ายนำมา

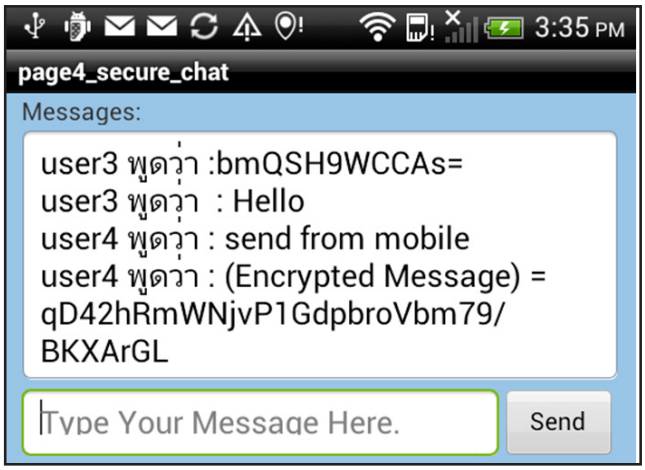
ถอดอ่านข้อความที่คุยกัน หรืออาจจะส่งข้อความที่เข้ารหัสลับไปยังแม่ข่าย เพื่อส่งให้สมาชิกในกลุ่มเมื่อมีสมาชิกเพิ่มหรือออกจากกลุ่ม แม่ข่ายก็กำหนดค่ากุญแจกลุ่มขึ้นใหม่ แล้วคำนวณค่า X ของกลุ่มขึ้นใหม่ แล้วกระจายให้กับสมาชิกปัจจุบัน (ซึ่งในทางปฏิบัติแล้วสมาชิกจะอ่านค่า X จากแม่ข่ายเอง) ดังนั้นระบบที่เสนอนี้จึงมี backward secrecy และ forward secrecy

ภาพที่ 6, 7 และ 8 แสดงผลลัพธ์ของการทำงานของโปรแกรมสนทนากลุ่ม การสนทนานี้มีผู้ที่ร่วมสนทนา 3 ราย คือ ผู้ใช้ ‘user3’ ‘user4’ ‘user5’ ผู้ใช้ ‘user3’ และ ‘user5’ ใช้แพลตฟอร์มวินโดวส์ส่วน ‘user4’ ใช้แอนดรอยด์ ภาพที่ 6 แสดงข้อความที่ส่งจาก ‘user4’ ให้แก่สมาชิกของกลุ่มภาพที่ 7 แสดงผลการสนทนาบนจอภาพของ ‘user3’ และ ‘user5’ สำหรับภาพที่ 8 แสดงผลของการโจมตีเมื่อ ‘user5’ ที่ออกจากกลุ่มแล้ว แต่พยายามเข้าไปอ่านข้อความที่สนทนากันก็จะไม่ได้ข้อมูลการสนทนากันอีก

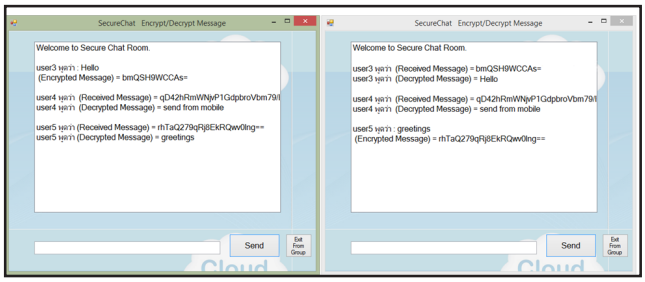
9. ประเด็นที่ควรพิจารณาในการนำไปใช้งานจริง

9.1 ประเด็นด้านความมั่นคงของระบบ

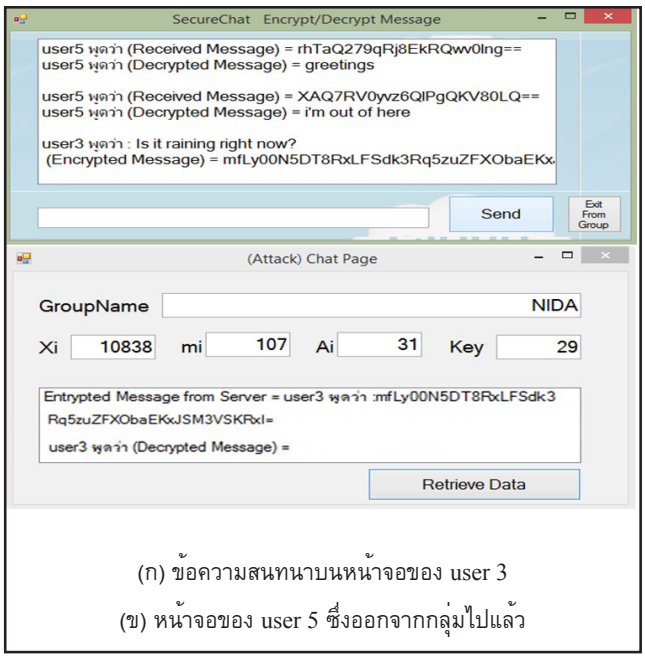
ประเด็นที่สำคัญที่ต้องพิจารณาเพื่อนำไปใช้ในงานจริงอย่างแรกคือ ตัวที่ทำหน้าที่จัดการกุญแจกลุ่ม ในงานวิจัยนี้ใช้แม่ข่ายบนคลาวด์ทำหน้าที่จัดการกุญแจกลุ่ม ดังนั้นแม่ข่ายจะทราบข้อความที่ส่งถึงกัน ประเด็นนี้เป็นประเด็นปัญหาอย่างหนึ่งของการใช้คลาวด์ที่ผู้ใช้คลาวด์อาจต้องเชื่อใจผู้ให้บริการคลาวด์ แต่สำหรับกลุ่มที่ต้องการความเชื่อมั่นของการสนทนาสูง อาจต้องใช้เครื่องลูกข่ายของสมาชิกกลุ่มคนใดคนหนึ่งทำหน้าที่จัดการกุญแจกลุ่ม โดยนำเอาการบริการในการจัดการกุญแจกลุ่มไปทำงานที่เครื่องนั้น ดังนั้น เครื่องลูกข่ายที่ทำหน้าที่นี้จะมีภาระในการประมวลผลสูง ซึ่งการลดเวลาในการคำนวณจึงเป็นประเด็นที่ต้องพิจารณา หรืออีกรูปแบบหนึ่งเป็นการใช้เครื่องลูกข่ายตัวหนึ่งทำหน้าที่สร้างกุญแจกลุ่ม (key generator) และมีการซ่อนค่ากุญแจกลุ่มนี้จากแม่ข่ายบนคลาวด์ แล้วจึงส่งไปให้แม่ข่ายบนคลาวด์ทำการกระจายกุญแจกลุ่มให้แก่สมาชิกของกลุ่ม ซึ่งแนวคิดนี้ได้แสดงในภาพที่ 9 แต่อย่างไรก็ตาม การออกแบบที่ใช้แม่ข่ายของคลาวด์ทำหน้าที่จัดการกุญแจที่เสนอในงานวิจัยนี้ก็สามารถใช้ได้ในกรณีของ private cloud หรือในกรณีที่ผู้ใช้เชื่อใจในผู้ให้บริการ



ภาพที่ 6 *user 4 ส่งข้อความจากโทรศัพท์มือถือ*



ภาพที่ 7 *ข้อความสนทนาบนหน้าจอของ user 3 (รูปทางซ้าย) และ user 5 (รูปทางขวา)*



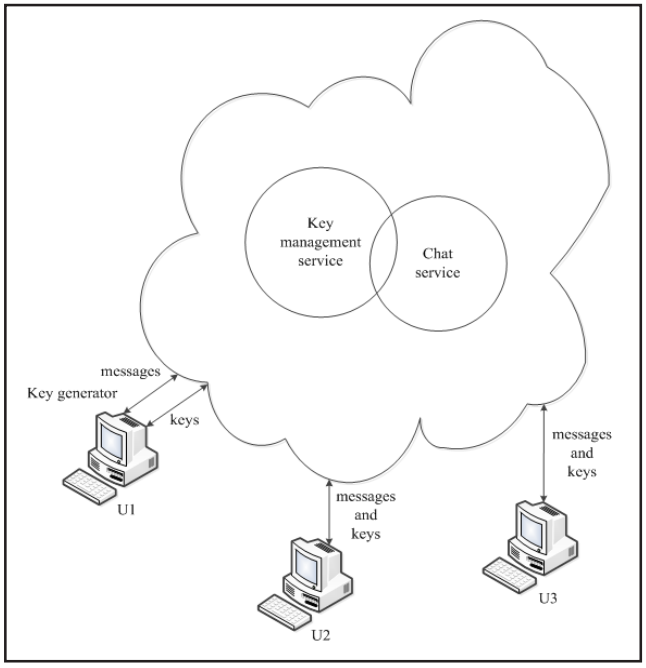
(ก) ข้อความสนทนาบนหน้าจอของ user 3

(ข) หน้าจอของ user 5 ซึ่งออกจากกลุ่มไปแล้ว

ภาพที่ 8 *แสดงผลของการโจมตีของผู้ใช้ที่ออกจากกลุ่มไปแล้ว*

นอกจากนั้น เนื่องจากระบบที่พัฒนาในงานวิจัยนี้เป็นระบบต้นแบบ ดังนั้น ในการยืนยันตัวเองจึงใช้วิธีการง่ายๆ โดยการให้ผู้ใช้ป้อนชื่อและรหัสผ่านของตัวเองเท่านั้น แล้ว

แม่ข่ายก็จะส่งกุญแจส่วนตัวมาให้ผู้ใช้ ซึ่งเป็นระบบที่ไม่มีความปลอดภัยมากนัก ดังนั้นหากนำไปใช้งานจริง ควรจะใช้วิธีการยืนยันตัวเองของผู้ใช้ที่ปลอดภัยกว่านี้ เช่น การยืนยันตัวเองด้วยระบบกุญแจสาธารณะ เพื่อให้แม่ข่ายส่งกุญแจส่วนตัวมาให้ โดยการเข้ารหัสลับที่ปลอดภัย



ภาพที่ 9 แนวคิดของการจัดการกุญแจกลุ่มเพื่อไม่ให้แม่ข่ายบนคลาวด์ทราบค่ากุญแจกลุ่ม

9.2 ประเด็นด้านประสิทธิภาพของระบบ

งานวิจัยนี้จะสามารถลดเวลาของการคำนวณค่าตัวคูณผกผันลงได้ แต่เมื่อจำนวนสมาชิกเพิ่มมากขึ้นจะมีการคูณของค่าตัวเลขที่โตขึ้นในการคำนวณหาค่า X ซึ่งใช้เวลาในการประมวลผลของแม่ข่ายมากขึ้นซึ่งในการวิจัยนี้จะทำการโมดูโลค่าที่ได้หลังจากการคำนวณในแต่ละวงเล็บของสมการ (3-5) เพื่อไม่ให้ค่าตัวเลขโต นอกจากนั้น ค่า X ที่ได้จากงานวิจัยนี้จะโตขึ้นตามจำนวนสมาชิกของกลุ่ม ซึ่งจะสิ้นเปลืองความสามารถการส่งข้อมูล (bandwidth) ของเครือข่าย จึงอาจต้องแก้ไขโดยการใช้โครงสร้างต้นไม้หลายระดับชั้นเพื่อสามารถใช้ค่า pairwise relatively prime เพียงหนึ่งค่าเป็นค่ากุญแจส่วนตัวของกลุ่มย่อยของสมาชิก ซึ่งจะทำให้ค่า X มีขนาดเล็กลงได้ และทำให้เวลาในการคำนวณค่า X ลดลงได้ ซึ่งประเด็นดังกล่าวข้างต้นนี้เป็นปัญหาที่ต้องทำการวิจัยต่อไป

10. สรุปงานวิจัย

งานวิจัยนี้ได้เสนอแนวคิดของการใช้ทฤษฎีเศษเหลือของจีนและโครงสร้างต้นไม้ไบนารีทางเดียว เพื่อส่งกุญแจกลุ่มให้แก่สมาชิกได้อย่างมีประสิทธิภาพ เนื่องจากจำนวนตัวเลขที่มีคุณสมบัติเป็น pairwise relatively prime มีจำนวนไม่จำกัด ดังนั้น ระบบที่นำเสนอจึงมีความมั่นคง กล่าวคือ เป็นการยากที่ผู้โจมตีจะทราบค่ากุญแจส่วนตัวของสมาชิก จึงไม่สามารถคำนวณหากุญแจกลุ่ม นอกจากนั้นระบบที่นำเสนอนี้จะใช้ความสามารถในการประมวลผลของอุปกรณ์ผู้ใช้น้อยมาก เพียงคำนวณมอดุโลหนึ่งครั้ง และทำการ XOR 1 ครั้งเท่านั้นก็สามารถหาค่ากุญแจกลุ่มได้ ในส่วนของแม่ข่ายนั้นก็สามารถลดเวลาของการคำนวณหาค่าของตัวผกผันการคูณลงได้ ไม่ว่าในกรณีของสมาชิกของกลุ่มเพิ่มขึ้นหรือลดลง

ในการประยุกต์งานวิจัยนี้กับการสนทนาเป็นความลับบนคลาวด์นั้น ยังมีประเด็นปัญหาความมั่นคงระบบที่ไม่ต้องการให้คลาวด์ทราบถึงข้อความที่สนทนากัน ตลอดจนประเด็นประสิทธิภาพของระบบ เมื่อกลุ่มสมาชิกมีขนาดโตมากๆ ซึ่งเป็นประเด็นที่ต้องทำการวิจัยต่อไป

11. เอกสารอ้างอิง

[1] K.C. Chan and S.H. Chan. “Key Management Approaches to offer Data Confidentiality Secure Multicast.” *IEEE Network,* pp. 30-39, September-October, 2003.

[2] T. Aneksrup and P. Hiranvanichakorn. “Efficient Group Key Agreement on Tree-based Braid Groups.” *Computer and Information Science,* Vol. 4, pp. 14-27, January 2011.

[3] N. Saguansakdiyotin and P. Hiranvanichakorn. “Broadcast Encryption Based on Braid Groups.” *International Journal of Computer Science and Network Security,* Vol. 12, pp. 12-19, February 2012.

[4] S. Lertvorratham and P. Hiranvanichakorn. “Intergrating Secure Multipath Mobile Ad Hoc Network with Self-Authentication Strategy.” *International Journal of Computers and Applications,* Vol. 34, No. 3, 2012.

[5] แวววรรณ จันทร์ชูกลิ่น และ พิพัฒน์ หิรัณย์วณิชชากร

"การประยุกต์ของทฤษฎีเศษเหลือของจีนและโครงสร้างต้นไม้ในการส่งข้อมูลแบบกลุ่มด้วยการเข้ารหัสลับในเทคนิควิธี NTRU." *วารสารเทคโนโลยีสารสนเทศ,* ปีที่ 8, ฉบับที่ 2, หน้า 14-19, กรกฎาคม-ธันวาคม 2555.

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

[7] X. Zheng, C.T. Huang and M. Mathews. "Chinese Remainder Theorem Based Group Key Management." *In Proceedings of the 45th Association for Computing Machinery annual southeast regional conference (ACMSE 2007),* pp. 266-271, March 2007.

[8] J. Zhou and Y.H. Ou. "Key Tree and Chinese Remainder Theorem Based Group Key Distribution Scheme." *Journal of the Chinese Institute of Engineers,* Vol. 32, No. 7, pp. 967-974, 2009.

[9] C. Guo and C.C. Chang. "An authenticated group key distribution protocol based on the generalized Chinese remainder Theorem." *International Journal of Communication System,* Vol. 27, Issue 1, pp. 126-134, January 2014.

[10] P. Vijayakumar, S. Bose and A. Kannan. "Chinese remainder theorem based centralized group key management for recure multicast communication." *IET Information Security,* Vol. 81, Issue 3, pp. 179-187, 2014.

[11] IDG Cloud Computing Survey: Security, Integration Challenge Growth. Available online at http://www.forbes.com/sites/louiscolumbus/2013/08

[12] B.A. Forouzan. Data Communication and networking. 5E, McGraw-Hill, 2013.