วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏมหาสารคาม
Journal of Science and Technology, Rajabhat Maha Sarakham University

การกระจายและการแชร์กุญแจลับอย่างง่าย บนระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่ไม่อาศัยศูนย์กลาง

A simple Secret Key Splitting and Sharing of Decentralized Multiple Agent Key Recovery System

*กนกวรรณ กันยะมี
*Kanokwan Kanyamee
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏอุตรดิตถ์
Faculty of Science and Technology, Uttaradit Rajabhat University
*ผู้นิพนธ์หลัก: kanokwan@uru.ac.th
*Corresponding author: kanokwan@uru.ac.th

Received	Reviewed	Revised	Accepted
02/03/2023	30/03/2023	17/04/2023	29/04/2023

Abstract

Cryptography technology will help to strengthen security and privacy of various network activities. This technology uses methods to encrypt and decrypt data using a secret key (*Ks*). When the recipient is unable to use the key to decrypt the data or if the decryption key is lost, the secret key recovery process will be required, by using Key Recovery Field (KRF) to be used to decrypt the data.

The objective of this research is to present the development and improvement of a new SSDM-KRS algorithm model for higher stability. The design focuses on the secrecy of the Ks and solves the problem of revealing the key, when an agent collusion occurs in the key recovery group. As a result, information is safe, reliable, and user privacy. Finally, it supports law enforcement needs and is based on the Public Key Infrastructure (PKI). The KRF is slightly larger in size and requires less time to create KRF than previously proposed DM-KRS.

Keyword: Splitting and Sharing, Secret key, Key recovery, Agent, KRF

บทคัดย่อ

วิทยาการเข้ารหัสลับ เป็นเทคโนโลยีที่ช่วยเพิ่มความมั่นคงปลอดภัยและเพิ่มความเป็นส่วนตัวแก่ผู้ที่ใช้งานระบบเครือข่าย ซึ่งเทคโนโลยีนี้จะใช้วิธีการเข้ารหัสและถอดรหัสข้อมูลโดยใช้กุญแจลับ (Secret Key : *Ks*) เมื่อเกิดกรณีที่ผู้รับไม่สามารถใช้กุญแจในการถอดรหัสข้อมูลได้ หรือกุญแจที่ใช้ในการถอดรหัสสูญหาย จะต้องอาศัยกระบวนการเพื่อให้ได้มาซึ่งกุญแจลับ หรือเรียกว่า วิธีการกู้คืนกุญแจลับจากฟิลด์ในการกู้คืนกุญแจ (Key Recovery Field: KRF) เพื่อนำมาใช้ในการถอดรหัสข้อมูล

งานวิจัยนี้มีวัตถุประสงค์เพื่อนำเสนอการพัฒนาปรับปรุงรูปแบบขั้นตอนวิธีการสำหรับการกระจายและการแชร์กุญแจลับอย่างง่าย ในระบบการกู้คืนกุญแจแบบหลายเอเจนต์ ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ (SSDM-KRS) รูปแบบใหม่ เพื่อให้มีความมั่นคงสูงขึ้น การออกแบบได้คำนึงถึงเรื่องความลับของกุญแจเป็นสำคัญ และได้แก้ปัญหากุญแจถูกเปิดเผยเมื่อมีการสมรู้ร่วมคิดกันของเอเจนต์ จากการพัฒนาพบว่า กุญแจลับมีความมั่นคงเพิ่มขึ้น กล่าวคือ เป็นวิธีการที่สามารถรักษาความลับของกุญแจได้ แม้เกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์ ทำให้ข้อมูลมีความปลอดภัย น่าเชื่อถือ ผู้ใช้งานระบบเครือข่ายและสารสนเทศมีความเป็นส่วนตัว รองรับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย และทำงานบนโครงสร้างพื้นฐานกุญแจสาธารณะ โดยที่ฟิลด์ KRF มีขนาดเพิ่มขึ้นเล็กน้อยอย่างไม่มีนัยสำคัญ และใช้เวลาในการสร้างฟิลด์ KRF น้อยกว่ารูปแบบเดิม

คำสำคัญ: กระจายและแชร์, กุญแจลับ, การกู้คืนกุญแจ, เอเจนต์, ฟิลด์ในการกู้คืนกุญแจ

บทนำ

ในยุคปัจจุบันความมั่นคงปลอดภัยของข้อมูล ถือว่าเป็นเรื่องที่มีความสำคัญอย่างมาก โดยเฉพาะการส่งข้อมูลผ่านระบบเครือข่ายจำเป็นต้องมีการรักษาความปลอดภัยและรักษาความลับของข้อมูลเพื่อป้องกันการลักลอบดักจับข้อมูล หรือการเข้าถึงข้อมูลโดยผู้ประสงค์ร้าย เทคโนโลยีการเข้ารหัสลับ (Cryptography Technology) (Stallings, 2011) เป็นเทคโนโลยีที่นำมาใช้เป็นกลไกควบคุม และป้องกันที่ต้องเกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ช่วยเพิ่มความมั่นคงปลอดภัยให้กับข้อมูลสารสนเทศ และเพิ่มความเป็นส่วนตัวแก่ผู้ที่ใช้งานระบบเครือข่าย การเข้ารหัสลับแบบสมมาตรจะใช้กุญแจลับในการเข้ารหัสและถอดรหัสข้อมูล ในกรณีที่ผู้รับไม่สามารถใช้กุญแจในการถอดรหัสข้อมูลได้ หรือกุญแจที่ใช้ในการถอดรหัสสูญหาย หรือภาครัฐต้องการใช้สิทธิ์ในการเข้าถึงข้อมูลที่ต้องสงสัย จะต้องขอใช้บริการกู้คืนกุญแจจากหน่วยงานที่ทำหน้าที่ให้บริการระบบกู้คืนกุญแจ (Al-Salqan, 1997; Sun & Harayama, 2011) ซึ่งเรียกว่า เอเจนต์กู้คืนกุญแจ (Key Recovery Agent: KRA) (Denning & Branstad, 1997) โดยเอเจนต์จะอาศัยข้อมูลที่ถูกจัดเก็บอยู่ในฟิลด์การกู้คืนกุญแจ (Key Recovery Field: KRF) (Kim et al., 2020)

การกู้คืนกุญแจ มีการทำงานสองรูปแบบ (Wang et al., 2019) คือ การกู้คืนกุญแจแบบใช้เอเจนต์เดียว (Single Key Recovery System: S-KRS) และการกู้คืนกุญแจแบบใช้หลายเอเจนต์ (Multiple Key Recovery System: M-KRS) โดยกระบวนการทำงานของ S-KRS (Lee & Laih, 1997) จะใช้เอเจนต์เดียว (Single Key Recovery Agent: S-KRA) ในการจัดเก็บและกู้คืนกุญแจ ส่วน M-KRS

จะใช้หลายเอเจนต์ (Multiple Key Recovery Agent: M-KRA) (Lim et al., 2003; Lim et al., 2001) ในการจัดเก็บส่วนประกอบของกุญแจและร่วมกันกู้คืนกุญแจ การพัฒนาระบบในช่วงเริ่มแรกจะเป็นรูปแบบ S-KRS ซึ่งมีกระบวนการทำงานที่ไม่ซับซ้อน จึงทำให้เกิดภัยคุกคามต่อระบบได้ง่าย ระบบมีความมั่นคงปลอดภัยน้อยเมื่อเทียบกับภัยคุกคามที่มีหลากหลายรูปแบบ และมีความรุนแรงมากขึ้น ต่อมาการพัฒนาระบบในช่วงหลัง จึงได้ออกแบบระบบโดยใช้รูปแบบ M-KRS ทั้งนี้เพื่อลดความเสี่ยงต่อความเสียหายที่เกิดขึ้นกับ S-KRS

ระบบการกู้คืนกุญแจแบบ M-KRS มีการทำงาน 2 รูปแบบคือ (1) M-KRS ที่อาศัยศูนย์กลางในการกู้คืนกุญแจ และ (2) M-KRS ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ (Decentralized Multiple Key Recovery System: DM-KRS) โดยทั้ง 2 ลักษณะมีกระบวนการทำงานที่แตกต่างกัน ทั้งนี้การทำงานในรูปแบบที่ 2 จะมีข้อดีคือ กระบวนการทำงานจะมีความมั่นคงปลอดภัยมากขึ้น เนื่องจากไม่มีบุคคลที่สาม (Third Party) เข้ามาเกี่ยวข้อง อย่างไรก็ตามการกู้คืนกุญแจในรูปแบบ DM-KRS ที่คำนึงถึงความเป็นส่วนของผู้ใช้งาน การรองรับการเข้าถึงข้อมูลอย่างถูกต้อง โดยกุญแจยังคงเป็นความลับเมื่อเกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์ จะต้องอาศัยกระบวนการกระจายและการแชร์กุญแจไปยังเอเจนต์ที่เกี่ยวข้อง ซึ่งจากการศึกษางานวิจัยที่ผ่านมา (Kanyamee & Sathitwiriyawong, 2009; Kanyamee & Sathitwiriyawong, 2014) ยังไม่มีการนำเสนอองค์ความรู้เกี่ยวกับวิธีขั้นตอนของกระบวนการในการกระจายและการแชร์กุญแจลับ ที่คำนึงถึงเรื่องดังกล่าว

ดังนั้นผู้วิจัยจึงจะได้ศึกษาคิดค้นและนำเสนอ ขั้นตอนวิธีของการกระจายและการแชร์กุญแจลับสำหรับ DM-KRS รูปแบบใหม่ ที่กุญแจมีความมั่นคงสูง เป็นความลับแม้เกิดเหตุการณ์สมรู้ร่วมคิดกันระหว่างเอเจนต์ ทำให้ผู้ใช้งานมีความเป็นส่วนตัว การกู้คืนกุญแจมีความน่าเชื่อถือ สามารถพิสูจน์ตัวจริงของเอเจนต์ที่อยู่ในกลุ่มการกู้คืนกุญแจเดียวกัน และทำงานบนโครงสร้างพื้นฐานกุญแจสาธารณะหรือพีเคไอ (Public Key Infrastructure: PKI) (Guo, Okuyama & Finley, 2005; Slagell, 2006)

วิธีการวิจัย

ขั้นตอนและวิธีการที่ใช้ในการวิจัยแบ่งออกเป็น 2 ระยะ คือ

ระยะที่ 1 ศึกษาและเปรียบเทียบ

1.1 ศึกษากระบวนการทำงานของระบบการกู้คืนกุญแจแบบ DM-KRS ซึ่งมี 2 รูปแบบด้วยกัน คือ (1) ระบบการกู้คืนกุญแจหลายเอเจนต์แบบกระจายที่มีความพร้อมใช้งานสูง (High-Availability Decentralized Multiple-Agent Key Recovery System: HADM-KRS) (Kanyamee & Sathitwiriyawong, 2009) และ (2) ระบบการกู้คืนกุญแจหลายเอเจนต์แบบกระจายที่มีความพร้อมใช้งานสูงอย่างง่าย (Simple High-Availability Decentralized Multiple-Agent Key Recovery System: SHADM-KRS) (Kanyamee & Sathitwiriyawong, 2014) โดยทั้งสองรูปแบบมีจุดเด่นคือ (1) ระบบสามารถทำงานโดยไม่ใช้ศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center: KRC) แต่เป็นการออกแบบให้ใช้เฉพาะกลุ่มของเอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent: KRA) โดยแต่ละเอเจนต์ทำการกู้คืนส่วนประกอบของกุญแจโดยอิสระจากกัน และ (2) ระบบมีความพร้อมใช้งานสูง กล่าวคือระบบสามารถทำงานได้แม้ในกรณีที่มีบางเอเจนต์ในกลุ่มการกู้คืนล่ม โดยเมื่อมีบางเอเจนต์

ในกลุ่มการกู้คืนล่ม เอเจนต์อื่นที่อยู่ในกลุ่มการกู้คืนเดียวกันสามารถทำงานแทนกันได้ จุดเด่นทั้งสองประการนี้จะช่วยลดโอกาสการเกิดความล้มเหลวในการกู้คืนกุญแจ ทำให้ระบบมีความพร้อมใช้งานสูง

ความแตกต่างของ HADM-KRS และ SHADM-KRS คือ ความสามารถในการบริหารจัดการจำนวนเอเจนต์ที่ใช้ในการกู้คืนกุญแจ *Ks* กล่าวคือ HADM-KRS สามารถกำหนดจำนวนเอเจนต์ขั้นต่ำที่ใช้ในการกู้คืนกุญแจได้ โดยใช้ทฤษฎีพื้นฐานเรื่องเพาเวอร์เซต (Power Set) (Jech, 2006) มาใช้ในกระบวนการสำรองส่วนประกอบของกุญแจสำหรับการกู้คืนกุญแจ เช่น เมื่อใช้เอเจนต์จำนวน 6 เอเจนต์ในการกู้คืนกุญแจ ระบบ HADM-KRS สามารถกำหนดได้ว่าจะให้มีเอเจนต์ล่มได้อย่างมากที่สุดกี่เอเจนต์ หรืออย่างน้อยต้องเหลือเอเจนต์ที่สามารถให้บริการได้กี่เอเจนต์ จึงจะให้บริการกู้คืนกุญแจ *Ks* ได้สำเร็จ ส่วนระบบ SHADM-KRS ไม่มีฟังก์ชันนี้ แต่สามารถกู้คืนกุญแจได้เมื่อมีบางเอเจนต์ล่ม

อย่างไรก็ตามทั้งสองรูปแบบ ยังมีจุดอ่อนคือ เมื่อเกิดกรณีสมรู้ร่วมคิดกันของ KRA จะทำให้กุญแจลับเปิดเผยได้ ส่งผลให้ความมั่นคงลดลง และความเป็นส่วนตัวของผู้ใช้งานน้อยลงเช่นกัน ในการสมรู้ร่วมคิดกันของ KRA สามารถเกิดขึ้นได้หาก KRA ในกลุ่มการกู้คืนร่วมมือกันกู้คืนกุญแจลับ *Ks* โดยแต่ละ KRA เปิดเผยส่วนประกอบของกุญแจ (S_i) ที่ตนเองครอบครอง เมื่อได้ S_i จาก KRA ครบจำนวนก็จะสามารถคำนวณกุญแจลับ *Ks* ได้ ดังนั้นในงานวิจัยนี้จึงได้ออกแบบให้มีการจัดเก็บส่วนประกอบของกุญแจชิ้นสุดท้าย (S_R) ไว้ที่ KRF และเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ $Ku_R(S_R)$ และกุญแจสาธารณะของหน่วยงานรัฐบาล $Ku_G(S_R)$ เพื่อรองรับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย จากวิธีการออกแบบดังกล่าว หาก KRA สมรู้ร่วมคิดกันเปิดเผยส่วนประกอบของกุญแจครบทุก KRA ก็จะไม่สามารถกู้คืนกุญแจลับ *Ks* ได้ เนื่องจากได้ส่วนประกอบของกุญแจไม่ครบจำนวน

1.2 ศึกษาวิธีการกระจายและการแชร์ความลับ (Secret Sharing) ของ *Ks* จากฟิลด์ KRF ของ HADM-KRS และ SHADM-KRS ดังแสดงใน Table 1 และมีแอตทริบิวต์ที่เกี่ยวข้องดังนี้

S_i คือ ส่วนประกอบของกุญแจ Ks

SGN คือ ค่าสำหรับการยืนยันตัวตนของ KRA ที่อยู่ในกลุ่มการกู้คืน

h(SGN) เป็นค่าสำหรับการพิสูจน์ตัวจริงของ KRA ในกลุ่มการกู้คืน โดยฟังก์ชั่นแฮชที่เหมาะสม คือ MD5 (Zheng & Jin 2012) SHA-1 SHA-2 (Al-Odat, Abbas & Khan, 2019) เป็นต้น

TT_i เป็นค่าสำหรับการกู้คืน Si ในกรณี KRA ที่อยู่ในกลุ่มการกู้คืนล่ม

Other information เก็บค่าอื่น ๆ ที่จำเป็นสำหรับการพิสูจน์ตัวจริงหรือการตรวจสอบเพื่อเพิ่มความมั่นคงปลอดภัยให้กับระบบ เช่น ใบรับรองกุญแจสาธารณะของเอเจนต์ และของผู้ที่มีสิทธิ์ในการร้องขอการกู้คืนกุญแจ เป็นต้น

Ku_{agi} คือ กุญแจสาธารณะของเอเจนต์

Table 1 Comparison of KRF structures of HADM-KRS and SHADM-KRS

HADM-KRS	SHADM-KRS
KRF = {Ku_{agi}[KRF_i's]}	KRF = {Ku_{agi}[KRF_i's || *h*(SGN) || TT_i's]}
KRF_i = Ku_{agi}[S_i || SGN || TT_i's || other information]	KRF_i = Ku_{agi}[S_i || SGN || other information]

ระยะที่ 2 ออกแบบ พัฒนา เปรียบเทียบ และสรุปผล

2.1 ออกแบบ พัฒนารูปแบบขั้นตอนวิธีการกระจายและการแชร์กุญแจลับในการกู้คืนกุญแจแบบ DM-KRS โดยใช้แนวคิดพื้นฐานเรื่องการแชร์ความลับ (Secret Sharing) มาใช้ในการแบ่งกุญแจออกเป็นส่วน ๆ และจัดสรรส่วนประกอบของกุญแจ

2.2 เปรียบเทียบความสามารถในการทำงานของการกู้คืนกุญแจ *Ks* โดยพิจารณาตามฟังก์ชันความสามารถ 7 ประเด็น ดังนี้ (1) การทำงานโดยไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ (KRC) (2) การรักษาความลับของกุญแจลับของ *Ks* (3) ความพร้อมใช้งานสูง (4) ความสามารถในการกำหนดจำนวน KRA ขั้นต่ำ (5) ความสามารถในการพิสูจน์ตัวจริงของ KRA (6) การใช้รูปแบบมาตรฐานของฟิลด์ KRF และ (7) ระบบมีความมั่นคงเมื่อเกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์

2.3 ประเมินขนาดและเวลาของการสร้าง KRF สำหรับการกู้คืนกุญแจ *Ks* วิเคราะห์ผล สรุปผล

ผลการวิจัยและอภิปรายผลการวิจัย

1. การออกแบบวิธีการกระจายและการแชร์กุญแจ *Ks* อย่างง่าย

งานวิจัยนี้มุ่งนำเสนอวิธีการกระจายและการแชร์กุญแจลับอย่างง่ายบนระบบการกู้คืนกุญแจแบบ DM-KRS หรือ SSDM-KRS รูปแบบใหม่ ที่สามารถรักษาความลับของ *Ks* แม้เกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์

1.1 การกระจายส่วนประกอบของกุญแจ *Ks*

ขั้นตอนวิธีการกระจายส่วนประกอบของกุญแจ *Ks* ใช้วิธีการแบ่งและจัดสรรส่วนประกอบของกุญแจ ไว้ในฟิลด์การกู้คืนกุญแจ (KRF) โดยมีวิธีการดังแสดงใน Table 2

Table 2 Distribution of (portion) *Ks*

Distribution of (portion) *Ks*	
❶ Random number S_i for n KRA (S_i's)	$S_1, S_2,..., S_n$
❷ Calculate S_R for receiver $Ku_R(S_R)$ and government $Ku_G(S_R)$	$S_R = S_1 \oplus S_2 \oplus ... \oplus S_n \oplus Ks$
❸ Random number R_i for n KRA (R_i's)	$R_1, R_2,..., R_n$
❹ Calculate a Share Group Number (SGN)	$SGN = R_1 \oplus R_2 \oplus ... \oplus R_n$

❺ Calculate a Unique Number (TT) for n KRA (TT_i's)	$TT_i = S_i \oplus SGN$; when i = 1 to n	
❻ Calculate hash value of SGN for KRA_i authentication	h(SGN) (A suitable hash function are MD5 SHA-1 SHA-2)	
The attributes used to recover *Ks* as follows: { S_R , S_i , SGN }	S_R	: portion of *Ks* that has been encrypted with receiver's public key (Ku_R) and government's public key (Ku_G)
	S_i	: portion of *Ks* { $Ks = S_R \oplus S_1 \oplus S_2 \oplus ... \oplus S_n$ }
	SGN	: a value used to authenticate agents in the recovery group

Note : The value of n is determined based on the appropriateness of the level of reliability in key recovery

1.2 การแชร์กุญแจ *Ks*

จาก Table 2 สามารถออกแบบการแชร์กุญแจ *Ks* โดยการสร้างฟิลด์ KRF ได้ดังต่อไปนี้ ฟิลด์ KRF ประกอบด้วยข้อมูลต่อไปนี้ (1) SR และ Si คือ ส่วนประกอบของกุญแจ *Ks* (2) SGN คือ แอตทริบิวต์สำหรับการยืนยันตัวตนของ KRA ในกลุ่มการกู้คืน (3) TT_i คือ แอตทริบิวต์สำหรับการกู้คืนส่วนประกอบของกุญแจ *Ks* ในกรณี KRA ที่อยู่ในกลุ่มการกู้คืนล่ม และ (4) Other information คือ ข้อมูลที่จำเป็นสำหรับการระบุตัวตนของผู้ที่มีส่วนร่วมในกระบวนการกู้คืนกุญแจการพิสูจน์ตัวจริงหรือการตรวจสอบเพื่อเพิ่มความมั่นคงปลอดภัยให้กับการกู้คืน เช่น ใบรับรองกุญแจสาธารณะของเอเจนต์ และของผู้ที่มีสิทธิ์ในการร้องขอการกู้คืนกุญแจ เป็นต้น

ฟิลด์ KRF_i จะถูกเข้ารหัสด้วยกุญแจสาธารณะของ KRA (Ku_{agi}) ดังนั้น KRA_i เท่านั้นที่สามารถถอดรหัส KRF_i ได้ โดย KRA_i จะถอดรหัสฟิลด์ KRF_i เพื่อส่ง S_i และ SGN ไปยังผู้ร้องขอการกู้คืนส่วนประกอบของกุญแจ เพื่อจะได้ทำการคำนวณกุญแจลับ *Ks* ต่อไป

รูปแบบโครงสร้างฟิลด์ KRF ของ SSDM-KRS สามารถแสดงได้ดังนี้

$$KRF = \{ Ku_{agi}[KRF_i\text{'s}] \,||\, TT_i\text{'s} \,||\, Ku_R(S_R) \,||\, Ku_G(S_R) \,||\, h(SGN) \}$$

$$KRF_i = Ku_{agi}[S_i \,||\, SGN \,||\, \text{Other information}]$$

จากการนำเสนอวิธีการกระจายและการแชร์กุญแจลับอย่างง่ายบนระบบการกู้คืนกุญแจแบบ DM-KRS (SSDM-KRS) รูปแบบใหม่ จะเห็นได้ว่าเป็นวิธีการที่ทำให้การกู้คืนกุญแจ *Ks* มีความมั่นคงสูง ถึงแม้จะเกิดกรณีสมรู้ร่วมคิดกันระหว่างเอเจนต์ ก็จะไม่สามารถล่วงรู้กุญแจ *Ks* ได้ จะมีเพียงผู้รับหรือหน่วยงานของรัฐบาลเท่านั้นที่จะสามารถกู้คืนกุญแจ *Ks* ได้

2. เปรียบเทียบความสามารถในการทำงานของการกู้คืนกุญแจ *Ks*

ผู้วิจัยได้ทำการเปรียบเทียบความสามารถในการทำงานของการกู้คืนกุญแจ *Ks* ในรูปแบบเก่า (HADM-KRS และ SHADM-KRS) กับรูปแบบใหม่ (SSDM-KRS) ที่ผู้วิจัยได้นำเสนอ ดังแสดงใน Table 3

Table 3 Capabilities comparison of various M-KRS's

Capabilities	HADM-KRS	SHADM-KRS	SSDM-KRS
1) Without the need of KRC	✓	✓	✓
2) High Secrecy of *Ks*	✓	✓	✓
3) High availability	✓	✓	✓
4) Flexibility to manage the number of KRAs	✓	-	-
5) Group Authentication of KRAs	✓	✓	✓
6) Use the standard format of KRF	✓	✓	✓
7) Able to keep *Ks* secret even after collusion between Agents	-	-	✓

จาก Table 3 SSDM-KRS มีการออกแบบมาให้มีความสามารถโดดเด่นกว่า DM-KRS รูปแบบเก่า ในแง่ของการรักษาความลับของ *Ks* แม้เกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์ อีกทั้งยังคงรักษามาตรฐานเดิมที่มีความมั่นคงของการกู้คืนกุญแจ *Ks*

3. การประเมินขนาดของฟิลด์ KRF สำหรับการกู้คืนกุญแจ *Ks*

เมื่อทำการเปรียบเทียบขนาดของฟิลด์ KRF สำหรับการกู้คืนกุญแจ *Ks* ทั้ง 3 รูปแบบ สามารถแสดงผลได้ดัง Table 4 และ Figure 1

Table 4 Size comparison of KRF (bits)

Number of KRA	Size of KRF (bits)		
	HADM-KRS	SHADM-KRS	SSDM-KRS
2	2560	3072	3328
4	5376	5888	6144
6	8192	8704	8960
8	11008	11520	11776
10	13824	14336	14592

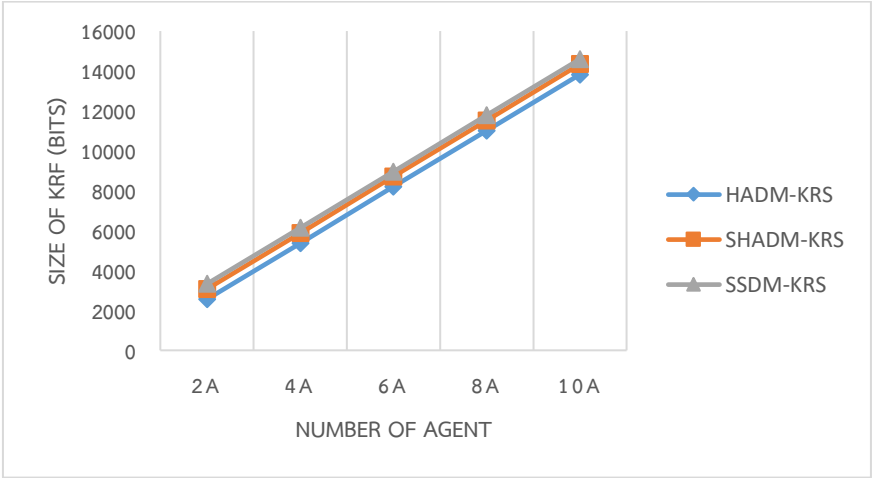

Figure 1 Size of KRF

จาก Table 4 จะสังเกตเห็นว่าเมื่อใช้จำนวน KRA สำหรับการกู้คืนกุญแจ จำนวน 2 เอเจนต์ การกู้คืนกุญแจแบบ DM-KRS จะมีจำนวนบิตที่บรรจุใน KRF ใกล้เคียงกัน เมื่อเพิ่มจำนวน KRA สำหรับการกู้คืนกุญแจ เป็น 4 6 8 และ 10 เอเจนต์ตามลำดับ จะใช้จำนวนบิตที่เพิ่มขึ้น โดยที่ SSDM-KRS มีขนาดของฟิลด์ KRF ที่ใหญ่ที่สุด รองลงมาคือ SHADM-KRS และ HADM-KRS ตามลำดับ

4. การประเมินเวลาที่ใช้ในกระบวนการการสร้างฟิลด์ KRF สำหรับการกู้คืนกุญแจ *Ks*

เมื่อทำการเปรียบเทียบเวลาที่ใช้ในกระบวนการสร้างฟิลด์ KRF สำหรับการกู้คืนกุญแจ *Ks* ทั้ง 3 รูปแบบ สามารถแสดงผลได้ดัง Table 5 และ Figure 2

Table 5 Comparison of Processing time of KRF generation

Number of KRA	Processing time of KRF generation (Second)		
	HADM-KRS	SHADM-KRS	SSDM-KRS
2	0.4615	0.4618	0.5003
4	0.9602	0.9224	0.9625
6	1.4872	1.3828	1.4235
8	2.0059	1.8434	1.8844
10	2.6069	2.3041	2.3452

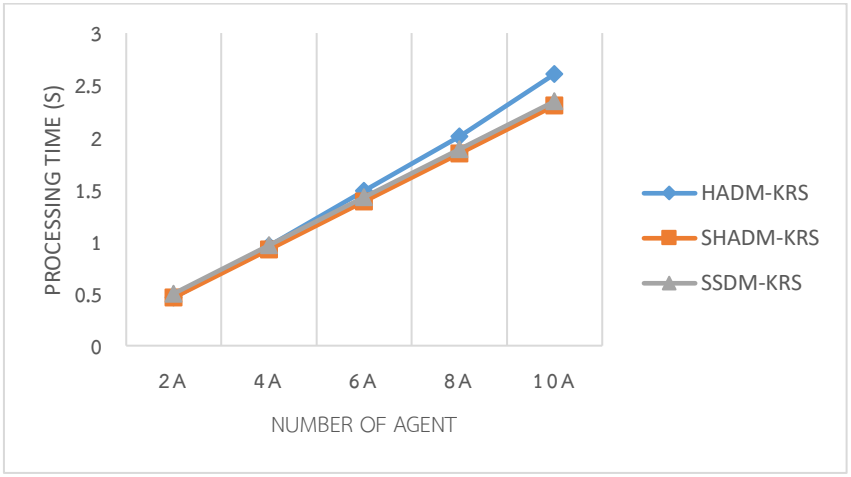

Figure 2 Processing time of KRF generation

จาก Table 5 และ Figure 2 ผลการประเมินเวลาที่ใช้ในการสร้างฟิลด์ KRF พบว่า เมื่อใช้ KRA จำนวน 2 ถึง 4 เอเจนต์ SSDM-KRS ใช้เวลาในกระบวนการสร้างฟิลด์ KRF มากกว่า SHADM-KRS และ HADM-KRS ตามลำดับ และเมื่อใช้จำนวน KRA เพิ่มขึ้นที่ 6 เอเจนต์ SSDM-KRS ใช้เวลาน้อยกว่า HADM-KRS แต่มากกว่า SHADM-KRS เพียงเล็กน้อยอย่างไม่มีนัยสำคัญ ทั้งนี้สาเหตุที่ HADM-KRS ใช้เวลามากที่สุด เนื่องจากต้องใช้เวลาสำหรับการจัดสรรแอตทริบิวต์ TT_i ซึ่งเป็นค่าแอตทริบิวต์ที่ถูกนำมาใช้ในกระบวนการกู้คืนส่วนประกอบของกุญแจ ในกรณีที่มีบาง KRA ในกลุ่มการกู้คืนล่มโดยที่กระบวนการจัดสรรค่า TT_i นั้น ช่วยให้สามารถกำหนดเงื่อนไขของจำนวนการคงอยู่ของ KRA ขั้นต่ำที่พร้อมให้บริการในกลุ่มการกู้คืน SHADM-KRS และ SSDM-KRS สามารถกู้คืนกุญแจได้เมื่อมีบาง KRA ในกลุ่มการกู้คืนล่มเช่นกัน แต่ไม่มีฟังก์ชันการกำหนดเงื่อนไขการคงอยู่ของ KRA จึงไม่ต้องใช้เวลาในการจัดสรรค่า TT_i ใน KRF

ดังนั้นเวลาที่ใช้ในกระบวนการสร้างฟิลด์ KRF จะขึ้นอยู่กับจำนวนของ KRA ที่ใช้ในการกู้คืนกุญแจ กล่าวคือหากใช้ KRA จำนวนมาก ก็จะใช้เวลาในกระบวนการสร้างฟิลด์ KRF_i มากขึ้นตามลำดับ เนื่องจากฟิลด์ KRF_i ได้ถูกสร้างขึ้นเท่ากับจำนวนของ KRA ที่ใช้ในการกู้คืนกุญแจ

อย่างไรก็ตาม SSDM-KRS ถือว่าเป็นกระบวนการกู้คืนกุญแจที่มีความมั่นคงสูงมากกว่า HADM-KRS และ SHADM-KRS เนื่องจากสามารถแก้ไขปัญหาการสมรู้ร่วมคิดกันระหว่างเอเจนต์ได้

5. อภิปรายผลการวิจัย

งานวิจัยนี้ได้ออกแบบและนำเสนอวิธีการกระจายและการแชร์กุญแจลับอย่างง่ายบนระบบการกู้คืนกุญแจแบบ DM-KRS หรือ SSDM-KRS รูปแบบใหม่ โดยมีกระบวนการในการรักษาความลับของ *Ks* แม้เกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์ ผู้ใช้งานมีความเป็นส่วนตัว โดยทำงานอยู่บนโครงสร้างพื้นฐานกุญแจสาธารณะหรือพีเคไอ (Public Key Infrastructure: PKI) ดังนั้นการรับ-ส่ง

ข้อมูลระหว่างคู่สนทนาต้องมีการเข้ารหัสลับข้อมูลด้วยกุญแจสาธารณะของผู้รับ และผู้รับจะถอดรหัสลับข้อมูลด้วยกุญแจส่วนตัวของตนเอง

ผลการวิจัยพบว่าการสำรองค่า SR ซึ่งเป็นส่วนประกอบหนึ่งของ *Ks* ที่เข้ารหัสด้วยกุญแจสาธารณะของผู้รับ (Ku_R) และกุญแจสาธารณะของหน่วยงานรัฐบาล (Ku_G) ไว้ใน KRF จะทำให้กุญแจมีความมั่นคงเพิ่มขึ้น เนื่องจากสามารถรักษาความลับของ *Ks* ได้แม้เกิดกรณีการสมรู้ร่วมคิดกันระหว่างเอเจนต์ เพราะการสำรองค่า SR ทำให้เอเจนต์ไม่สามารถล่วงรู้ส่วนประกอบของ *Ks* ได้ครบ ดังนั้นจึงไม่สามารถกู้คืนกุญแจ *Ks* ได้ จะมีเพียงผู้ที่ร้องขอการกู้คืนกุญแจ (ผู้รับหรือหน่วยงานของรัฐบาล) เท่านั้นที่จะสามารถกู้คืนกุญแจ *Ks* ได้ ด้วยการถอดรหัสชิ้นส่วน *Ks* ชิ้นสุดท้าย คือ SR ด้วยกุญแจส่วนตัวของตนเอง โดยแอตทริบิวต์ในการกู้คืนกุญแจ ถูกจัดเก็บไว้ในฟิลด์ KRF อย่างปลอดภัย

อย่างไรก็ตามงานวิจัย DM-KRS ที่ผ่านมายังไม่มีงานวิจัยใดที่นำเสนอวิธีการกระจายและการแชร์กุญแจลับ *Ks* ที่สามารถรักษาความลับของกุญแจได้ในกรณีที่เกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์

สรุปผลการวิจัย

งานวิจัยนี้เป็นงานวิจัยพื้นฐาน (Pure Research) มีวัตถุประสงค์เพื่อปรับปรุงพัฒนารูปแบบขั้นตอนวิธีการสำหรับการกระจายและการแชร์กุญแจลับอย่างง่าย ในระบบการกู้คืนกุญแจแบบ DM-KRS ให้มีความมั่นคงสูง

รูปแบบวิธีการที่ได้นำเสนอในงานวิจัยนี้คือ กระจายและการแชร์กุญแจลับ แบบ SSDM-KRS ซึ่งเป็นกระบวนการกู้คืนกุญแจ *Ks* แบบ DM-KRS ที่มีจุดเด่นอยู่ที่ฟังก์ชันวิธีการในการรักษาความลับของกุญแจลับ *Ks* แม้เกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์ (High Secrecy DM-KRS) มีกระบวนการทำงานที่ไม่ใช้ศูนย์กลางการกู้คืนกุญแจ (KRC) และมีความพร้อมใช้งานสูง (High Availability DM-KRS) กล่าวคือ สามารถกู้คืนกุญแจได้แม้ในกรณีที่มีบาง KRA ในกลุ่มการกู้คืนล่ม

โดยผู้วิจัยได้ออกแบบกระบวนการแชร์ความลับของกุญแจ *Ks* โดยใช้พื้นฐานของทฤษฎีการแชร์ความลับเพื่อนำมาใช้ในขั้นตอนการกระจายและการแชร์กุญแจลับได้อย่างดีและมีประสิทธิภาพ นอกจากนี้ยังมีคุณสมบัติเด่นอื่น ๆ อีก เช่น มีฟังก์ชั่นการพิสูจน์ตัวจริงของ KRA ที่อยู่ในกลุ่มการกู้คืน มีการทำงานบนโครงสร้างพื้นฐานกุญแจสาธารณะหรือพีเคไอ (Public Key Infrastructure: PKI) เป็นต้น

References

Al-Odat, Z. Abbas, A. & Khan, S. (2019). Randomness Analyses of the Secure Hash Algorithms, SHA-1, SHA-2 and Modified SHA. In *2019 International Conference on Frontiers of Information Technology (FIT)* (pp. 316–3165). Pakistan: Islamabad.

Al-Salqan, Y. (1997). Cryptographic Key Recovery. In *The Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems* (pp. 34-37). Tunisia: Tunis.

Denning, D. & Branstad, D. (1997). A Taxonomy for Key Recovery Encryption Systems. *Internet besieged: countering cyberspace scofflaws*, pp. 357-371. ACM Press/Addison-Wesley Publishing Co.

Guo, Z., Okuyama. T. and Finley, M.R. (2005). A New Trust Model for PKI Interoperability. In *The International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services. Papeete*, Tahiti.

Kanyamee, K. & Sathitwiriyawong, C. (2014). High-Availability Decentralized Cryptographic Multi-Agent Key Recovery. *The International Arab Journal of Information Technology (IAJIT)*, 11(1), 52-58.

Kanyamee, K. & Sathitwiriyawong, C. (2009). High-Availability Decentralized Multi-Agent Key Recovery System. In *The Eighth IEEE/ACIS International Conference Computer and Information Science* (pp. 290-294). China: Shanghai.

Kim, T. Kim, W. Seo, D. & Lee, I. (2020). A Secure Encapsulation Schemes Based on Key Recovery System. *In Silicon Valley Cybersecurity Conference* (pp. 25–37). USA: California.

Lee, Y. & Laih, C. (1997). On the Key Recovery of the Key Escrow System. In *The 13th Annual Computer Security Applications Conference* (pp. 216-220). USA: San Diego, CA.

Lim, S. Kang, S. & Sohn, J. (2003). Modeling of Multiple Agent Based Cryptographic Key Recovery Protocol. In *The 19th Annual Computer Security Applications Conference* (pp. 119-128). USA: Las Vegas, NV.

Lim, S. Hani, H. Kim, M. & Kim, T. (2001). In Design of Key Recovery System Using Multiple Agent Technology for Electronic Commerce. In *The Industrial Electronics* (pp. 1351-1356). Korea (South): Pusan.

Sun, W. & Harayama, M. (2011). A Proposal of Key Recovery Mechanism for Personal Decryptographic Keys. In *The International Conference on Internet Technology and Applications* (p. 1-6). China: Wuhan.

Slagell, A. Bonilla, R. & Yurcik, W. (2006). A survey of PKI components and scalability issues. In *The 25th IEEE International Performance Computing and Communications Conference* (pp. 473-483). USA: Phoenix, Arizona.

Stallings, W. (2011). Cryptography and Network Security. (5th ed). Prentice Hall.

Wang, H. Zhao, Y. Yu, X. Nag, A. Ma, Z. Wang, J. Yan, L. & Zhang, J. (2019). *Resilient Quantum Key Distribution (QKD)-Integrated Optical Networks with Secret-Key Recovery Strategy*. IEEE Access.

Zheng, X., & Jin, J. (2012). Research for the Application and Safety of MD5 Algorithm in Password Authentication. In *The 9th International Conference on Fuzzy Systems and Knowledge Discovery* (pp. 2216–19). Chongqing, China