การสื่อสารอย่างปลอดภัยในเครือข่าย GSM โดยใช้การเข้ารหัสลับแบบ RC4 ที่ถูกปรับปรุง

SECURED GSM NETWORKS USING MODIFIED RC4

กัมพล พรหมจิระประวัติ

KAMPHOL PROMJIRAPRAWAT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2546

ISBN 974-324-483-2

การสื่อสารอย่างปลอดภัยในเครือข่าย GSM โดยใช้การเข้ารหัสลับแบบ RC4 ที่ถูกปรับปรุง

SECURED GSM NETWORKS USING MODIFIED RC4

กัมพล พรหมจิระประวัติ

KAMPHOL PROMJIRAPRAWAT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2546

ISBN 974-324-483-2

SECURED GSM NETWORKS USING MODIFIED RC4

KAMPHOL PROMJIRAPRAWAT

A THESIS SUBMITTED IN PERTIAL FULFILLMENT

OF THE REQUIRMENTS FOR THE DEGREE OF

MASTER OF ENGINEERING IN COMPUTER ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT ' S INSTITUTE OF TECHNOLOGY LARDKRABANG

2003

ISBN 974-324-483-2

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การสื่อสารอย่างปลอดภัยในเครือข่าย GSM โดยใช้การเข้ารหัสลับแบบ RC 4 ที่ถูกปรับปรุง

SECURED GSM NETWORKS USING MODIFIED RC 4

ชื่อนักศึกษา นายกัมพล พรหมจิระประวัติ

รหัสประจำตัว 44061626

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมคอมพิวเตอร์

อาจารย์ผู้ควบคุมวิทยานิพนธ์ รศ.บรรจง ปิยธำรง

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ดร.วรวัฒน์	ลิ้มโภคา	
ดร.อรณัตร	จิตต์โสภักตร์	
ดร.ศักดิ์ชัย	ทิพย์จักษุรัตน์	
รศ.ประทีป	บัญญัตินพรัตน์	
รศ.บรรจง	ปิยธำรง	

วัน/เดือน/ปี ที่สอบ 25 เมษายน 2546 เวลา 10.30-12.30 น.

สถานที่สอบ ณ อาคาร 12 ชั้น ชั้น 4 (ห้อง E12-402)

บัณฑิตวิทยาลัยรับรองแล้ว

(รศ.ดร.บุญวัฒน์ อัตชู)

คณบดีบัณฑิตวิทยาลัย

วันที่.....26.....**เดือน**.....พฤษภาคม.....**พ.ศ**.....2546.....

หัวข้อวิทยานิพนธ์	การสื่อสารอย่างปลอดภัยในเครือข่าย GSM โดยใช้การเข้ารหัสลับแบบ RC4 ที่ถูกปรับปรุง
นักศึกษา	นาย กัมพล พรหมจิระประวัติ
รหัสนักศึกษา	44061626
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
พ.ศ.	2546
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ. บรรจง ปิยธำรง

บทคัดย่อ

ในเวลาไม่กี่ปีที่ผ่านมานี้ความต้องการสำหรับบริการไร้สายกำลังเพิ่มขึ้นอย่างรวดเร็ว GSM เป็นหนึ่งในอุตสาหกรรมการสื่อสารโทรคมนาคมที่มีการเจริญเติบโตรวดเร็วที่สุด อย่างไรก็ตาม ระบบการสื่อสารเคลื่อนที่ไร้สายมีความไม่มั่นคงมากกว่าในการถูกลักลอบดักฟังและเข้าถึงระบบอย่างไม่ถูกต้อง งานวิจัยนี้เสนอวิธีการรักษาความปลอดภัยแบบใหม่บนพื้นฐานของการเข้ารหัสลับแบบ Secret Key สำหรับเครือข่าย GSM ด้วยการรักษาความลับ Identity ของผู้ใช้ที่เข้มแข็ง ในระดับที่ลดการจราจรของเครือข่ายและเวลาในการทำ Call Setup ที่ดีกว่า การเข้ารหัสลับที่นำเสนอนั้นถูกพัฒนาจากอัลกอริทึม RC4 ซึ่งสามารถที่จะผลิตลำดับของบิตที่มีการกระจายของบิตศูนย์และบิตหนึ่งอย่างเท่าเทียมกัน ยิ่งไปกว่านั้นข้อมูลที่ถูกเข้ารหัสอย่างต่อเนื่องโดยใช้การเข้ารหัสลับที่นำเสนอยังมีจำนวนบิตที่เปลี่ยนไปจากข้อมูลก่อนที่จะเข้ารหัสลับมากกว่าการเข้ารหัสลับของเครือข่าย GSM แต่ใช้เวลาในการคำนวณน้อยกว่าอีกด้วย วิธีการที่ถูกนำเสนอไม่ยุ่งยากและเป็นประโยชน์มากสำหรับการสื่อสารไร้สายในปัจจุบันและอนาคต

Thesis Topic	SECURED GSM NETWORKS USING MODIFIED RC4
Student	Mr. Kamphol Promjiraprawat
Student ID	44061626
Degree	Master of Engineering
Programme	Computer Engineering
Year	2003
Thesis Advisor	Assoc. Prof. Bunjong Piyatamrong

ABSTRACT

In the recent years, the demands for wireless services are increasing rapidly. The Global System for Mobile Communication (GSM) is one of the fastest growing of telecommunication industry. However, wireless mobile systems are more vulnerable to fraudulent access and eavesdropping. This research proposes new security method based on secret key encryption for GSM networks with strongly subscriber identity confidentiality. In order to reduce network traffic and better call setup time. The proposed encryption is developed from RC4 algorithm always produces bit sequence of evenly distributed 0's and 1's. Furthermore, The proposed stream cipher has more the number of bits that differ in the plaintext than the GSM stream cipher, but also has less computational time. The proposed approach is simple and it can be very useful for present and future wireless communications.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี ด้วยคำแนะนำและคำปรึกษาเกี่ยวกับวิธีการศึกษาและความรู้ต่างๆเกี่ยวกับระบบการรักษาความปลอดภัยจากรองศาสตราจารย์ บรรจง ปิยธำรง ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์จากท่านและขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ นายวันชัย พรหมจิระประวัติ (บิดา) และ นางทัศนีย์ โมณานนท์ (มารดา) ตลอดจนครอบครัว พรหมจิระประวัติ ทุกคนที่ได้ให้ความรักและอบรมสั่งสอนผู้วิจัยมาโดยตลอด

ขอขอบพระคุณ นางสุรางค์รัตน์ ศรีสมบุญ (คุณป้า) และ นางผ่องศรี แซ่ตั้ง (คุณยาย) ที่ได้ให้ความเมตตาช่วยเหลือผู้วิจัยเสมอมา

ขอขอบคุณ นายสุพจน์ และ นายสุเชาว์ ภารดีไฉไล เพื่อนผู้ช่วยฝึกซ้อมการนำเสนอวิทยานิพนธ์ให้กับผู้วิจัย

และสุดท้ายขอขอบพระคุณ นาง สุรัตน์ ฮอนดา (คุณย่า) ผู้เป็นแรงบันดาลใจให้ผู้วิจัยศึกษาต่อในระดับบัณฑิตศึกษา

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยข้อมอบแด่ผู้มีพระคุณทุกท่าน

กัมพล พรหมจิระประวัติ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูป

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

รายการคำย่อและสัญลักษณ์

A: Transmission Rate between MS and MSC

AB: Access Burst

Ack: Acknowledgement

ACM: Address Complete Message

ANS: Answer Message

AGCH: Access Grant Channel

AuC: Authentication Centre

B: Transmission Rate between MSC and HLR

BCC: Base transceiver Station Color Code

BCCH: Broadcast Control Channel

BCH: Broadcast Channel

Bm: Mobile B Channel

BSC: Base Station Controller

BSIC: Base Transceiver Station Identity Code

BSS: Base Station Subsystem

BTS: Base Transceiver Station

C_{wos} : Costs without Security

$C_{Proposed}$: Costs with Proposed encryption

C_{A5} : Costs with A5 encryption

C_{Auth}^{GSM} : Authentication Cost for GSM Scheme

$C_{Auth}^{Proposed}$: Authentication Cost for Proposed Scheme

C1: Majority Bit of Register R1

C2: Majority Bit of Register R2

C3: Majority Bit of Register R3

CCCH: Common Control Channel

CI: Cell Identity

COUNTM: Mobile Counter

D: Data Size

DB: Dummy Burst

DCCH: Dedicated Control Channel

EIR: Equipment Identity Register

FAC: Final Assembly Code

FACCH: Fast Associated Control Channel

FB: Frequency Burst

FCCH: Frequency Correction Channel

FDMA: Frequency Division Multiple Access

FN: Frame Number

GMSC: Gateway Mobile Switching Centre

GSM: Global Systems for Mobile communication

H: Header

HLR: Home Location Register

IMEI: International Mobile Equipment Identity

IMSI: International Mobile Subscriber Identity

ISC: International Switching Centre

ISDN: Integrated Services Digital Network

Kbps: Kilo-bits per second

Kc: Cipher Key

Kc [DATA]: DATA encrypted with Kc

Kc [n]: n-element Kc vector

Kc [N]: Kc with selected 8-bits Key Number

Kc [M]: Message M encrypted with Kc

Kc [TMSI]: TMSI encrypted with Kc

Kc [TMSIn] : new TMSI encrypted with Kc

Ki: Authentication Key

Kp: Proposed Key

Kp [IMSI, N]: IMSI and N encrypted with Kp

Kp [RANDM [N], N]: RANDM [N] and N encrypted with Kp

Kp [TMSIo, LAIo, N]: old TMSI, old LAI and N encrypted with Kp

Kp [SRES [N]]: SRES [N] encrypted with Kp

Kp [TMSI, N]: TMSI and N encrypted with Kp

Kp [TMSI]: TMSI encrypted with Kp

LA: Location Area

LAC: Location Area Code

LAI: Location Area Identity

LAIn, LAInew: new Location Area Identity

LAIo, LAIold: old Location Area Identity

LFSR: Linear Feedback Shift Register

Lm: Mobile Low-Rate Channel

M: Message

ME: Mobile Equipment

MCC: Mobile Country Code

MHz : Mega-Hertz

MNC: Mobile Network Code

MS: Mobile Station

MSC: Mobile Switching Centre

MSIN: Mobile Subscriber Identity Number

MSISDN: Mobile Station ISDN Number

MSRN: Mobile Station Roaming Number

N: 8-bits Key Number

NB: Normal Burst

NCH: Notification Channel

NCC: Network Color Code

NSS: Network and Switching Subsystem

OMC: Operations and Management Centre

PCH: Paging Channel

PDN: Public Data Network

PLMN: Public Land Mobile Network

PSTN: Public Switched Telephone network

R1: 19-bits Register of Threshold

R2: 22-bits Register of Threshold

R3: 23-bits Register of Threshold

RACH: Random Access Channel

RAND: 128-bits Random Number for GSM network

RAND [n]: n-element RAND vector

RAND [N]: RAND with selected 8-bits Key Number

RANDM: 64-bits Random Number for Proposed Scheme

RANDM [n]: n-element RANDM vector

RANDM [N]: RANDM with selected 8-bits Key Number

SACCH: Slow Associated Control Channel

SB: Synchronization Burst

SCH: Synchronization Channel

SDCCH: Stand-alone Dedicated Control Channel

SIM: Subscriber Identity Module

SNR: Serial Number

SP: Spare Bit

SRES: 32-bits Signature Response

SRES [n]: n-element SRES vector

SRES [N]: SRES with selected 8-bits key number

$T_{Proposed}$: Encryption/Decryption time with proposed algorithm for 64 bits of data

T_{A5} : Encryption/Decryption time with A5 algorithm for 114 bits of data

T_{crypt} : Proposed Encryption/Decryption time

T_{rand} : 128-bits Random Number Generating time

T_{randm} : 64-bits Random Number Generating time

TCH: Traffic Channel

TCH/F: Full Rate Traffic Channel

TCH/H: Half Rate Traffic Channel

TAC: Type Approval Code

TDMA: Time Division Multiple Access

Ti [X]: X-entry of i -level Table

TMSI: Temporary Mobile Subscriber Identity

TMSIn: TMSInew: new Temporary Mobile Subscriber Identity

TMSIo: TMSIold: old Temporary Mobile Subscriber Identity

VLR: Visitor Location Register

VLRn: new Visitor Location Register

VLRo: old Visitor Location Register

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในสภาพการณ์ปัจจุบันบริการต่างๆ เกี่ยวกับการสื่อสารเคลื่อนที่เป็นองค์ประกอบที่สำคัญอย่างยิ่งต่อสภาพเศรษฐกิจ ความสามารถที่จะติดต่อสื่อสารข้อมูลโดยปราศจากข้อจำกัดในเรื่องของเวลา, สถานที่, หรือเครือข่ายที่ให้บริการ ทำให้การติดต่อสื่อสารมีความสะดวกรวดเร็ว ทันต่อเหตุการณ์ นำมาสู่การเจริญเติบโตที่รวดเร็วของอุตสาหกรรมการสื่อสารเคลื่อนที่

Global System for Mobile communications (GSM) เป็นมาตรฐานการสื่อสารเคลื่อนที่ดิจิตอลที่ถูกพัฒนาขึ้นโดยสถาบัน ETSI (European Telecommunication Standards Institute) ระหว่างศตวรรษที่ 80 โดยเริ่มต้นเผยแพร่แก่สาธารณะครั้งแรกในทวีปยุโรป ปัจจุบันนี้เครือข่าย GSM รองรับการใช้งานจากผู้ใช้กว่า 50 ล้านคนในกว่า 100 ประเทศทั่วโลกและมีอัตราการเจริญเติบโตของจำนวนผู้ใช้เพิ่มขึ้นเรื่อยๆ ในแต่ละปี อย่างไรก็ตามปัญหาสำคัญอันหนึ่งของการสื่อสารเคลื่อนที่คือ ความจำเป็นที่จะต้องสื่อสารข้อมูลระหว่างผู้ใช้กับเครือข่ายโดยผ่านทางช่องสัญญาณวิทยุซึ่งเป็นสื่อกลางที่ในการสื่อสารข้อมูลที่ง่ายแก่การถูกโจรกรรมข้อมูลของผู้ใช้และการเข้าถึงบริการของเครือข่ายอย่างไม่ถูกต้อง

การรักษาความปลอดภัยของเครือข่ายจึงเป็นดัชนีตัวหนึ่งที่จะบ่งชี้ถึงประสิทธิภาพของเครือข่ายที่จะให้บริการกับผู้ใช้ แต่การรักษาความปลอดภัยของเครือข่ายย่อมจะต้องมีค่าใช้จ่ายในการสร้างความปลอดภัยให้กับผู้ใช้และเครือข่าย สำหรับเครือข่ายการสื่อสารเคลื่อนที่นั้น ผู้ออกแบบระบบการรักษาความปลอดภัยจะต้องคำนึงประสิทธิภาพในการรักษาความปลอดภัยควบคู่ไปกับค่าใช้จ่ายที่จะเกิดขึ้นด้วย เนื่องการสื่อสารเคลื่อนที่มีบริการต่างๆที่มีข้อจำกัดในเรื่องของเวลาอยู่พอสมควร การรักษาความปลอดภัยที่มีค่าใช้จ่ายสูงจนเกินไปอาจจะมีผลกระทบกับบริการอื่นๆ ของเครือข่าย

วิทยานิพนธ์ฉบับนี้ทำการออกแบบระบบการรักษาความปลอดภัยสำหรับเครือข่าย GSM โดยทำการปรับปรุงโพรโตคอลการตรวจสอบผู้ใช้ (Authentication Protocol) ให้มีความปลอดภัยและมีค่าใช้จ่ายในการักษาความปลอดภัยไม่สูงจนเกินไป และออกแบบอัลกอริทึมในการเข้าและถอดรหัสลับข้อมูลใหม่ เพื่อที่จะสามารถทำให้ผู้ใช้บริการเครือข่ายสามารถที่จะมั่นใจได้ว่าข้อมูลของจะถูกเก็บเป็นความลับและเครือข่ายจะถูกสงวนไว้แด่ผู้ใช้ที่ถูกต้องเท่านั้น

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

ศึกษาถึงข้อดีและข้อเสียของระบบการรักษาความปลอดภัยในเครือข่าย GSM เพื่อนำมาปรับปรุงระบบการรักษาความปลอดภัยของเครือข่าย GSM ให้มีประสิทธิภาพมากยิ่งขึ้น สำหรับการออกแบบระบบการรักษาความปลอดภัยนั้นจะพิจารณาถึงค่าใช้จ่ายที่จะเกิดขึ้นจากการรักษาความปลอดภัยด้วยเพื่อที่จะสามารถออกแบบระบบการรักษาความปลอดภัยให้มีความปลอดภัยสูงขึ้นแต่ประหยัดค่าใช้จ่ายมากกว่าเดิม

คิดค้นอัลกอริทึมในการเข้าและถอดรหัสลับข้อมูลแบบ Secret Key เพื่อที่จะใช้เข้ารหัสลับข้อมูลแทนอัลกอริทึมการเข้ารหัสลับข้อมูลของเครือข่าย GSM เดิม เพื่อที่จะสามารถลดค่าใช้จ่ายและเพิ่มความปลอดภัยให้ข้อมูลผู้ใช้ในเครือข่าย GSM

1.3 สมมติฐานของการศึกษา

การตรวจสอบผู้ใช้ (Authentication) ในเครือข่าย GSM ใช้วิธีการแบบ Challenge-Response ทำให้เครือข่ายจะต้องส่ง Challenge ให้กับผู้ใช้ การลดขนาดของ Challenge ของเครือข่ายลงอาจนำมาซึ่งการประหยัดค่าใช้จ่ายในการรักษาความปลอดภัยของเครือข่ายด้วย และเนื่องจากความจำเป็นที่จะต้องสื่อสารผ่านช่องสัญญาณวิทยุ การเข้ารหัสลับข้อมูลเพิ่มขึ้นในส่วนที่จะส่งข้อมูลผ่านช่องสัญญาณวิทยุจะเพิ่มความปลอดภัยให้กับข้อมูลของผู้ใช้ได้

อัลกอริทึม A5 ที่เครือข่าย GSM ใช้ในการเข้ารหัสลับข้อมูลก่อนที่จะส่งข้อมูลผ่านช่องสัญญาณวิทยุนั้นอาจยังไม่ใช่อัลกอริทึมที่มีประสิทธิภาพที่สุดเท่าที่มีอยู่ในปัจจุบัน การพัฒนาอัลกอริทึมในการเข้ารหัสลับข้อมูลที่ได้รับความนิยมอยู่ในปัจจุบันอาจจะนำมาซึ่งอัลกอริทึมที่มีประสิทธิภาพสูงกว่าอัลกอริทึม A5 ของเครือข่าย GSM

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

สำหรับการลดค่าใช้จ่ายในการรักษาความปลอดภัยของเครือข่าย GSM นั้นในงานวิจัยนี้ทำการลดขนาดของ Challenge ของเครือข่ายลงครึ่งหนึ่งและส่วนข้อมูลนั้นสามารถหาได้จากจำนวนครั้งที่ผู้ใช้ทำการตรวจสอบผู้ใช้ กับเครือข่าย ดังนั้นทั้งทางฝั่งผู้ใช้และเครือข่ายจะต้องทำการสร้างตัวนับ (Counter) จำนวนครั้งการตรวจสอบผู้ใช้กับเครือข่ายขึ้นมา เมื่อจะทำการตรวจสอบผู้ใช้ Challenge จะต้องถูกนำไปรวมกับข้อมูลของตัวนับก่อน เพื่อทำให้ขนาดของอินพุตของการตรวจสอบผู้ใช้มีขนาดเท่าเดิม

สำหรับการออกแบบอัลกอริทึมในการเข้าและถอดรหัสลับข้อมูลนั้น งานวิจัยนี้ทำการปรับปรุงอัลกอริทึม RC4 ซึ่งเป็นอัลกอริทึมการเข้าและถอดรหัสลับแบบ Secret Key โดยมีลักษณะการ

เข้ารหัสลับแบบ Stream Cipher ซึ่งในการปรับปรุงนั้นจะทำเปลี่ยนแปลง S-Box ให้มีคุณสมบัติในการสุ่ม (Randomness) ดีขึ้นกว่าเดิมโดยไม่เพิ่มค่าใช้จ่ายในการเข้ารหัสลับข้อมูล

1.5 ขอบเขตการวิจัย

ในงานวิจัยนี้ทำออกแบบการรักษาความปลอดภัยของเครือข่ายโดยทำการปรับปรุงการตรวจสอบผู้ใช้เมื่อผู้ใช้ทำการติดต่อกับเครือข่าย การตรวจสอบผู้ใช้แบ่งเป็น 3 กรณีคือ กรณีที่ผู้ใช้ทำ Location Registration กับเครือข่าย, กรณีที่ผู้ใช้ทำ Location Updating กับเครือข่าย, และกรณีที่ทำการ Call Setup ระหว่างผู้ใช้กับเครือข่าย

ในส่วนการออกแบบอัลกอริทึมในการเข้าและถอดรหัสลับข้อมูลขึ้นใหม่นั้นจะถูกนำไปใช้แทนที่การเข้ารหัสลับของอัลกอริทึม A5 โดยการเข้าและถอดรหัสลับข้อมูลจะถูกทำที่โทรศัพท์เคลื่อนที่ของผู้ใช้และชุมสายโทรศัพท์เคลื่อนที่ (Mobile Switching Centre, MSC)

1.6 ขั้นตอนของการศึกษา

ในวิทยานิพนธ์ฉบับนี้แบ่งขั้นตอนของการศึกษาออกเป็น 6 บทดังนี้

บทที่ 1 บทนำ กล่าวถึงความเป็นมาและความสำคัญของหัวข้อปัญหาในวิทยานิพนธ์, วัตถุประสงค์ของวิทยานิพนธ์, สมมุติฐานของการศึกษา, ทฤษฎีและแนวคิดตลอดจนขอบเขตในงานวิจัย

บทที่ 2 ความรู้พื้นฐานเกี่ยวกับเครือข่าย GSM เป็นรายละเอียดของสถาปัตยกรรมของเครือข่าย GSM, ฐานข้อมูลของเครือข่าย, การสื่อสารข้อมูลต่างๆของเครือข่าย และลักษณะข้อมูลของผู้ใช้ของเครือข่าย GSM เพื่อที่จะสามารถทำความเข้าใจลักษณะของการสื่อสารเคลื่อนที่ของเครือข่าย GSM

บทที่ 3 การรักษาความปลอดภัยของเครือข่าย GSM อธิบายถึงพื้นฐานในการรักษาความปลอดภัยเบื้องต้น, วิธีการและบริการต่างๆ การรักษาความปลอดภัยที่เครือข่าย GSM จัดเตรียมไว้ให้กับผู้ใช้, รายละเอียดของอัลกอริทึมในการรักษาความปลอดภัยของเครือข่าย GSM

บทที่ 4 การออกแบบระบบรักษาความปลอดภัย กล่าวถึง การปรับปรุงวิธีการตรวจสอบผู้ใช้ (Authentication), โพรโตคอลต่างๆในการรักษาความปลอดภัย, การออกแบบอัลกอริทึมที่ใช้ในการเข้ารหัสลับข้อมูล และแบบจำลองในการคำนวณค่าใช้จ่ายและประสิทธิภาพของวิธีการรักษาความปลอดภัยที่นำเสนอ

บทที่ 5 ผลการทดลอง เป็นการแสดงผลการทดลองเปรียบเทียบของค่าใช้จ่ายระหว่างวิธีการรักษาความปลอดภัยที่นำเสนอกับวิธีการรักษาความปลอดภัยที่เครือข่าย GSM ใช้อยู่เดิมและ

การแสดงผลการทดลองการเปรียบเทียบคุณสมบัติในการรักษาความปลอดภัยต่างๆ ของอัลกอริทึมที่นำเสนอกับอัลกอริทึม A5 ของเครือข่าย GSM

บทที่ 6 บทสรุป เป็นการสรุปผลการทดลองและข้อเสนอแนะเพื่อประโยชน์สำหรับการนำวิทยานิพนธ์ฉบับนี้ไปทำการวิจัยต่อไป

บทที่ 2

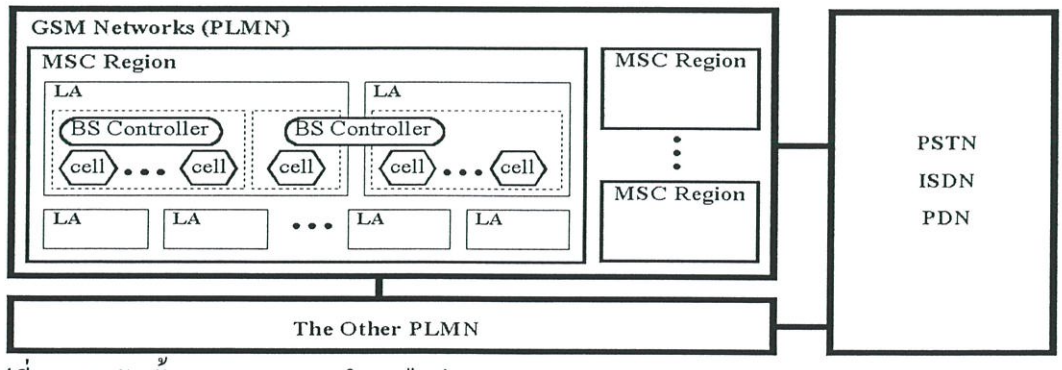
ความรู้พื้นฐานเกี่ยวกับเครือข่าย GSM

ในบทนี้จะกล่าวถึงรายละเอียดต่างๆของสถาปัตยกรรมของเครือข่าย GSM โดยจะอธิบายว่าเครือข่าย GSM มีลำดับชั้นของระบบเป็นอย่างไร ส่วนประกอบต่างๆของเครือข่ายที่สำคัญมีอะไรบ้างและทำหน้าที่อย่างไร ฐานข้อมูลที่จะใช้จัดเก็บข้อมูลของผู้ใช้มีอะไรบ้างและเก็บข้อมูลอย่างไร

2.1 ลำดับชั้นของเครือข่าย GSM

เครือข่าย GSM แบ่งลำดับชั้นของโครงสร้าง(GSM Structure Hierarchy) ดังแสดงในรูปที่ 2.1 ภายในเครือข่ายจะประกอบด้วยพื้นที่การจัดการ (Administrative Region) ของชุมสายโทรศัพท์เคลื่อนที่ (Mobile Switching Center, MSC) หลายๆตัว โดยในแต่ละพื้นที่การจัดการของชุมสายโทรศัพท์เคลื่อนที่จะประกอบด้วยกลุ่มของเซลล์ต่างๆเรียกว่า "Location Area (LA)" หน่วยควบคุมสถานีฐาน (Base Station Controller, BSC) ทำหน้าที่ในการควบคุมกลุ่มของเซลล์ต่างๆ ดังนั้นแต่ละ LA จะมีหน่วยควบคุมสถานีฐานอย่างน้อยหนึ่งตัว แต่หน่วยควบคุมสถานีฐานอาจควบคุมกลุ่มของเซลล์ใน LA ที่ต่างกันได้ ขนาดของแต่ละเซลล์จะถูกกำหนดตามพื้นที่ที่สามารถรับส่งสัญญาณได้ของสถานีฐานรับส่งสัญญาณ (Base Transceiver Station, BTS) สำหรับเซลล์นั้นๆ

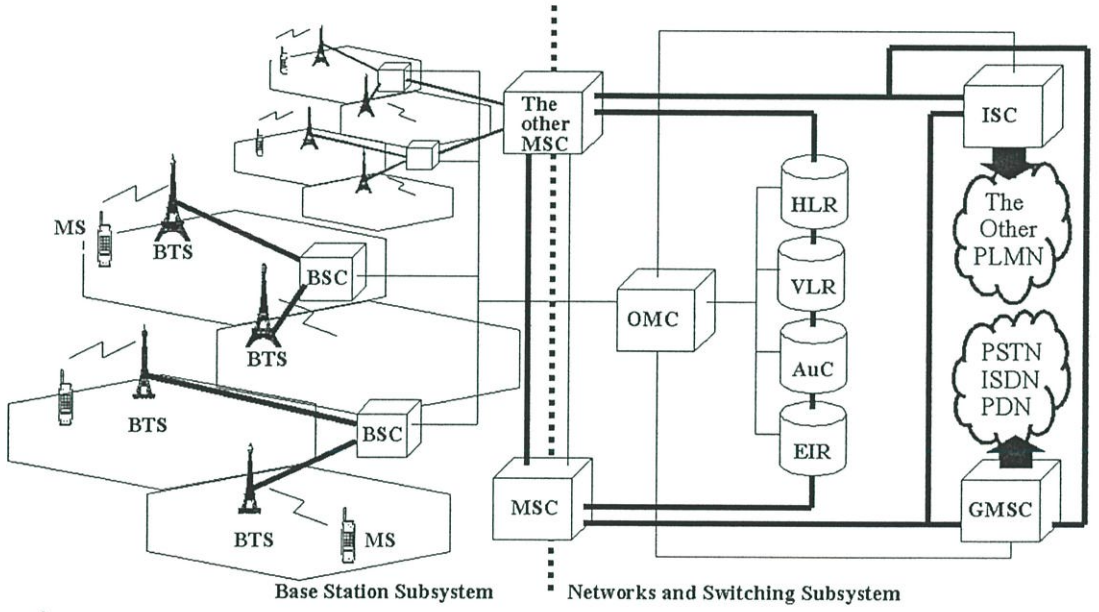
เครือข่ายโทรศัพท์เคลื่อนที่ (Public Land Mobile Networks, PLMN) สามารถที่จะติดต่อกับเครือข่ายประเภทอื่นๆ เช่น เครือข่ายโทรศัพท์ (Public Switched Telephone Networks, PSTN) , เครือข่ายดิจิตอลแบบร่วมบริการ (Integrated Services Digital Network, ISDN),เครือข่ายสื่อสารข้อมูล (Public Data Networks, PDN) และเครือข่ายโทรศัพท์เคลื่อนที่อื่นๆ (The other PLMN) ได้ ปัจจัยต่างๆในการแบ่งลำดับชั้นของระบบไม่ได้มีเพียงเท่านี้ ขึ้นกับผู้ปฏิบัติการเครือข่าย (Network Operators) แต่ละรายซึ่งต้องการให้เกิดประโยชน์สูงสุดเท่าที่จะเป็นไปได้ [1]



รูปที่ 2.1 ลำดับชั้นของระบบภายในเครือข่าย GSM

2.2 สถาปัตยกรรมของระบบ

โครงสร้างของระบบโทรศัพท์เคลื่อนที่ GSM ประกอบด้วย 5 ส่วนหลักคือ ระบบย่อยสถานีฐาน (Base Station Subsystem, BSS), ระบบย่อยเครือข่ายและสวิตช์ชิง (Networks and Switching Subsystem, NSS), ศูนย์กลางการปฏิบัติการและบำรุงรักษา (Operation & Maintenance Centre, OMC), เครื่องโทรศัพท์เคลื่อนที่ (Mobile Stations, MS) และฐานข้อมูลของเครือข่าย แต่ละส่วนมีการเชื่อมต่อกันดังแสดงในรูปที่ 2.2 [2]



รูปที่ 2.2 ส่วนประกอบต่างๆของเครือข่าย GSM

รายละเอียดของส่วนต่างๆของเครือข่ายที่สำคัญมีดังต่อไปนี้

2.2.1 ระบบย่อยสถานีฐาน (Base Station Subsystem, BSS)

BSS ประกอบด้วย 2 ส่วนหลักๆ คือ สถานีฐานรับส่งสัญญาณ (Base Transceiver Stations, BTS) และ หน่วยควบคุมสถานีฐาน (Base Station Controller, BSC)

ในส่วนของ BTS จะทำหน้าที่ในการติดต่อกับโทรศัพท์เคลื่อนที่ (Mobile Station, MS) ของผู้ใช้โดยผ่านทางช่องสัญญาณวิทยุ (Radio Channel) มีหน้าที่ในการจัดเตรียมช่องสัญญาณวิทยุสำหรับการติดต่อสื่อสารระหว่างผู้ใช้กับเครือข่าย นอกจากนั้นยังมีหน้าที่วัดความแรงและคุณภาพของสัญญาณแล้วส่งข้อมูลให้ BSC เพื่อตัดสินใจในการเปลี่ยนสถานีฐานที่จะรับส่งสัญญาณของผู้ใช้ (Handoff) BTS จะทำหน้าที่ในการรับส่งสัญญาณเป็นหลัก ในส่วนของการควบคุมต่างๆจะทำเพียงบางส่วน เช่น Error Protection Coding เป็นต้น ฟังก์ชันส่วนใหญ่ในการควบคุม BTS จะเป็นหน้าที่ของ BSC ซึ่งจะทำให้ BTS มีขนาดไม่ใหญ่จนเกินไป

ในส่วนของ BSC จะทำหน้าที่ในส่วนการควบคุมต่างๆ ของ BTS เช่น การทำแฮนด์ออฟ, ควบคุมการเริ่มและสิ้นสุดการโทรศัพท์ของผู้ใช้ BSC จะเป็นหน่วยงานที่ติดต่อกับชุมสายโทรศัพท์เคลื่อนที่ (Mobile Switching Centre, MSC) ในส่วนของระบบย่อยเครือข่ายและสวิตช์ชิง

2.2.2 ระบบย่อยเครือข่ายและสวิตช์ชิง (Networks and Switching Subsystem, NSS)

NSS ประกอบด้วย 4 ส่วนหลักๆ คือ ชุมสายโทรศัพท์เคลื่อนที่ (Mobile Switching Centre, MSC), ชุมสายโทรศัพท์ทางเข้าออก (Gateway Mobile Switching Centre, GMSC), และชุมสายโทรศัพท์ต่างประเทศ (International Switching Centre, ISC) รายละเอียดของส่วนต่างๆของใน NSS มีดังต่อไปนี้

2.2.2.1 ชุมสายโทรศัพท์เคลื่อนที่ (Mobile Switching Centre, MSC)

MSC ทำหน้าที่ในการจัดเตรียมเส้นทางในการส่งข้อมูลไปยัง MSC ปลายทางที่เหมาะสม MSC จะจัดเตรียมฟังก์ชันต่างๆที่ใช้ในการลงทะเบียน (Registration), ตรวจสอบผู้ใช้ (Authentication), ปรับปรุงตำแหน่งที่อยู่ของผู้ใช้ให้ถูกต้อง (Location Updating), และการเปลี่ยนสถานีฐานในการรับส่งสัญญาณ (Handoff) ในกรณีที่ข้าม BSC หรือข้าม MSC ที่ต่างกันของผู้ใช้ นอกจากนี้ MSC ยังจัดเตรียมการติดต่อกับฐานข้อมูลต่างๆที่จำเป็นของผู้ใช้เพื่อปรับปรุงข้อมูล (Update) ให้ถูกต้องอยู่เสมอ

2.2.2.2 ชุมสายโทรศัพท์เคลื่อนที่ทางเข้าออก (Gateway Mobile Switching Centre, GMSC)

GMSC ทำหน้าที่ในการจัดเตรียมเส้นทางไปยังเครือข่ายที่ไม่เคลื่อนที่ (Fixed Networks) อื่นๆ เช่น เครือข่ายดิจิตอลแบบร่วมบริการ (Integrated Services Digital Networks, ISDN), เครือข่ายโทรศัพท์ (Public Switched Telephone Networks, PSTN), และเครือข่ายสื่อสารข้อมูล (Public Data Networks, PDN) เช่น X.25 โดยการส่งข้อมูลข้ามเครือข่ายนี้จำเป็นต้องใช้ฟังก์ชันการทำงานระหว่างเครือข่าย (Interworking Functions) ในการทำให้โพรโตคอลของ PLMN เข้ากันได้ (Mapping) กับโพรโตคอลของเครือข่ายการสื่อสารอื่นๆ

2.2.2.3 ชุมสายต่างประเทศ (International Switching Centre, ISC)

ISC ทำหน้าที่ในการจัดเตรียมเส้นทางไปยังเครือข่ายโทรศัพท์เคลื่อนที่อื่นๆ (The other PLMN) หรือเครือข่ายโทรศัพท์เคลื่อนที่ในต่างประเทศ

2.2.3 ศูนย์กลางการปฏิบัติการและบำรุงรักษา (Operation & Maintenance Centre, OMC)

OMC เป็นหน่วยงานที่ทำหน้าที่ในการตรวจสอบ, แสดงผล, และควบคุมการทำงานของเครือข่ายทั้งหมดโดยจัดเตรียมฟังก์ชันต่างๆที่จะใช้ในการตรวจจับส่วนประกอบต่างๆในเครือข่ายที่

ได้รับความเสียหายหรือไม่พร้อมในการให้บริการ การปรับตั้งค่าพารามิเตอร์ต่างๆภายในระบบให้ถูกต้องเหมาะสม การคิดค่าบริการและการออกใบเรียกเก็บค่าบริการแก่ผู้ใช้ ซึ่ง OMC จะต้องทำการติดต่อกับฐานข้อมูลของเครือข่าย นอกจากนี้ OMC ยังมีฟังก์ชันในการรวบรวมข้อมูลเพื่อเก็บค่าสถิติต่างๆ เช่น สถิติความผิดพลาดของระบบ สถิติของการจราจรข้อมูล (Traffic) ในเครือข่าย เพื่อใช้ในการปรับปรุงให้เครือข่ายมีประสิทธิภาพต่อไป

2.2.4 ฐานข้อมูลของเครือข่าย

ฐานข้อมูลของเครือข่าย GSM มีทั้งหมด 4 ส่วนคือ Home Location Register (HLR), Visitor Location Register (HLR), Equipment Identity Register (EIR), และ Authentication Centre (AuC) รายละเอียดของฐานข้อมูลต่างๆ มีดังต่อไปนี้

2.2.4.1 Home Location Register (HLR)

HLR เป็นฐานข้อมูลที่เก็บข้อมูลของผู้ใช้ที่มีลักษณะที่ถาวรไม่มีการเปลี่ยนแปลงบ่อยๆ (Permanent Data) เช่น หมายเลขประจำผู้ใช้ (Subscriber Identity), ประวัติของผู้ใช้, หมายเลขโทรศัพท์ของผู้ใช้ นอกจากนี้ HLR ยังเก็บข้อมูลชั่วคราว (Temporary Data) ของผู้ใช้บางส่วนที่จำเป็น เช่น ตำแหน่งที่อยู่ปัจจุบันของผู้ใช้ และทำการปรับปรุงฐานข้อมูลให้ถูกต้อง (Update) อยู่เสมอ โดยปกติแล้วหนึ่งเครือข่ายโทรศัพท์เคลื่อนที่ (PLMN) จะมี HLR หนึ่งตัว แต่อาจมีมากกว่าหนึ่งตัวได้ขึ้นกับจำนวนผู้ใช้ในเครือข่าย

2.2.4.2 Visitor Location Register (VLR)

VLR เป็นฐานข้อมูลที่เก็บข้อมูลชั่วคราว (Temporary Data) ของผู้ใช้ขณะที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC โดยปกติแล้วหนึ่ง MSCจะมี VLR หนึ่งตัวแต่ VLR อาจรองรับการใช้งานมากกว่าหนึ่ง MSC ขึ้นกับจำนวนผู้ใช้ใน MSC เครื่องโทรศัพท์เคลื่อนที่ (Mobile Station, MS) จะติดต่อกับ VLR อย่างสม่ำเสมอเพื่อปรับปรุงข้อมูลอยู่เสมอโดยเฉพาะอย่างยิ่งข้อมูลเกี่ยวกับที่อยู่ปัจจุบันของผู้ใช้ VLR จะทำการแลกเปลี่ยนข้อมูลกับ HLR ที่จำเป็นต้องใช้ในการจัดการต่างๆ

2.2.4.3 Equipment Identity Register (EIR)

EIR เป็นฐานข้อมูลที่เก็บข้อมูลของอุปกรณ์โทรศัพท์เคลื่อนที่ โดยจะเก็บหมายเลขประจำตัวของอุปกรณ์โทรศัพท์เคลื่อนที่ (Mobile Equipment Identity) เพื่อจัดเตรียมบริการระงับใช้งานอุปกรณ์โทรศัพท์เคลื่อนที่ชั่วคราวในกรณีที่อุปกรณ์โทรศัพท์เคลื่อนที่สูญหายหรือถูกโจรกรรม นอกจากนี้เครือข่ายยังสามารถแจ้งให้ผู้ใช้ทราบถึงลักษณะของอุปกรณ์โทรศัพท์เคลื่อนที่ที่ใช้ซอฟท์แวร์ที่ล้าสมัย

2.2.4.4 Authentication Center (AuC)

AuC เป็นฐานข้อมูลที่สร้างและเก็บข้อมูลที่จำเป็นต้องใช้ในการรักษาความปลอดภัยของเครือข่ายและผู้ใช้ ข้อมูลที่ใช้ในการเข้าและถอดรหัสลับ คีย์ต่างๆ ที่ใช้ในการรักษาความปลอดภัยของผู้ใช้แต่ละคน ข้อมูลที่ใช้ตรวจสอบผู้ใช้บริการกับเครือข่าย (Authentication) ในส่วนของการสร้างข้อมูลในการรักษาความปลอดภัย อัลกอริทึมที่ใช้และข้อมูลต่างๆที่เป็นอินพุตและเอาท์พุตจะต้องตรงกันระหว่างผู้ใช้แต่ละคนกับทางฝั่งเครือข่าย โดยปกติแล้วฐานข้อมูล AuC จะถูกนิยามเป็นฟังก์ชันหนึ่งในฐานข้อมูล HLR

2.2.5 เครื่องโทรศัพท์เคลื่อนที่ (Mobile Station, MS)

ภายใน MS จะแบ่งเป็น 2 ส่วนคือ อุปกรณ์โทรศัพท์ (Mobile Equipment, ME) และสมาร์ตการ์ดที่เรียกว่า "Subscriber Identity Module (SIM)" ในส่วนของ ME จะทำหน้าที่ในการรับส่งคลื่นวิทยุระหว่างโทรศัพท์เคลื่อนที่กับสถานีฐาน รวมถึงอุปกรณ์ที่ใช้ติดต่อกับผู้ใช้ เช่น ลำโพง, ปุ่มกด, ไมโครโฟน ส่วน SIM ของผู้ใช้จะเก็บหมายเลขประจำตัวของผู้ใช้ (Subscriber Identity), ประเภทของบริการที่ลงทะเบียนใช้งาน, ตำแหน่งที่ตั้งปัจจุบันของผู้ใช้, หมายเลขโทรศัพท์ของผู้ใช้ , และข้อมูลและอัลกอริทึมที่ใช้ในการรักษาความปลอดภัย

2.3 ลักษณะของข้อมูลในเครือข่าย GSM

ข้อมูลของผู้ใช้บริการเครือข่าย GSM ที่มีความสำคัญในการจัดการและควบคุมการใช้บริการของผู้ใช้ในเครือข่ายมีดังต่อไปนี้ [3]

2.3.1 International Mobile Subscriber Identity (IMSI)

เมื่อผู้ใช้ลงทะเบียนใช้บริการกับเครือข่าย GSM ผู้ปฏิบัติการเครือข่าย (Network Provider) จะกำหนดหมายเลขประจำตัวให้กับผู้ใช้เรียกว่า "International Mobile Subscriber Identity (IMSI)" ซึ่ง IMSI ขนาด 64 บิตจะถูกเก็บไว้ใน SIM ของผู้ใช้และฐานข้อมูล HLR, VLR, และ AuC ทางฝั่งเครือข่ายจะทราบข้อมูลต่างๆของผู้ใช้ได้จากการนำ IMSI ไปค้นหาข้อมูลของผู้ใช้จากฐานข้อมูล

IMSI เป็นข้อมูลขนาด 64 บิตจะประกอบด้วยข้อมูล 3 ส่วนดังนี้

1) Mobile Country Code (MCC) เป็นรหัสที่ระบุประเทศภูมิลำเนาของผู้ใช้ มีขนาด 12 บิต
2) Mobile Network Code (MNC) เป็นรหัสที่ระบุเครือข่ายโมบาย (PLMN) ที่ผู้ใช้ลงทะเบียนด้วย มีขนาด 12 บิต
3) Mobile Subscriber Identity Number (MSIN) เป็นหมายเลขประจำตัวของผู้ใช้แต่ละคนในเครือข่าย GSM มีขนาด 40 บิต

2.3.2 International Mobile Equipment Identity (IMEI)

IMEI เป็นหมายเลขประจำตัวของแต่ละอุปกรณ์โทรศัพท์เคลื่อนที่มีลักษณะเป็นหมายเลขที่เรียงลำดับไปเรื่อยๆ (Serial Number) โดย IMEI จะถูกกำหนดโดยผู้ผลิตอุปกรณ์โทรศัพท์เคลื่อนที่และจะใช้งานได้ก็ต่อเมื่อลงทะเบียนผู้ปฏิบัติการเครือข่าย (Network Operator) IMEI จะถูกแบ่งเป็น 3 กลุ่มภายในฐานข้อมูล EIR คือ

1) White list คือ อุปกรณ์โทรศัพท์เคลื่อนที่ที่ได้รับการลงทะเบียนถูกต้องพร้อมที่จะใช้งาน
2) Black list คือ อุปกรณ์โทรศัพท์เคลื่อนที่ที่ถูกระงับใช้งาน โดย list นี้จะถูกแลกเปลี่ยนกันระหว่างผู้ปฏิบัติการเครือข่ายด้วยกัน
3) Gray list คือ อุปกรณ์โทรศัพท์เคลื่อนที่ที่มีฟังก์ชันในการทำงานไม่ดี หรือใช้ซอฟต์แวร์ที่ล้าสมัย

IMEI เป็นข้อมูลขนาด 64 บิตจะประกอบด้วยข้อมูล 4 ส่วนดังนี้

1) Type Approval Code (TAC) เป็นรหัสที่ระบุประเทศภูมิลำเนาของผู้ใช้ มีขนาด 24 บิต
2) Final Assembly Code (FAC) เป็นรหัสที่ระบุเครือข่ายโมบาย (PLMN) ของผู้ใช้ มีขนาด 8 บิต
3) Serial Number (SNR) เป็นหมายเลขประจำตัวของผู้ใช้แต่ละคนในเครือข่าย GSM มีขนาด 24 บิต
4) Spare (SP) ขนาด 8 บิต

เพื่อตอบสนองแนวความคิดของเครือข่าย GSM ที่ต้องการแบ่งแยกผู้ใช้และอุปกรณ์โทรศัพท์เคลื่อนที่ออกจากกัน หมายเลขประจำตัวของโทรศัพท์เคลื่อนที่และผู้ใช้จะเป็นอิสระจากกัน ทำให้ผู้ใช้จะสามารถติดต่อสื่อสารโดยปราศจากข้อจำกัดของอุปกรณ์ที่ใช้สื่อสาร

2.3.3 Temporary Mobile Subscriber Identity (TMSI)

เมื่อผู้ใช้ได้เคลื่อนที่เข้ามาอยู่ในพื้นที่การจัดการของชุมสายโทรศัพท์เคลื่อนที่ ผู้ใช้จะได้รับ TMSI ขนาด 32 บิตเพื่อใช้เป็นหมายเลขประจำตัวชั่วคราวของตนขณะที่กำลังใช้บริการอยู่ในพื้นที่การจัดการของชุมสายโทรศัพท์เคลื่อนที่นั้นๆ TMSI จะถูกเก็บไว้ใน SIM ของผู้ใช้และฐานข้อมูล VLR

2.3.4 Mobile Station ISDN Number (MSISDN)

MSISDN เป็นหมายเลขโทรศัพท์ของอุปกรณ์โทรศัพท์เคลื่อนที่ โดยอุปกรณ์โทรศัพท์เคลื่อนที่แต่ละเครื่องจะอ่าน MSISDN จาก SIM ของผู้ใช้ ดังนั้นหมายเลขโทรศัพท์ของอุปกรณ์โทรศัพท์เคลื่อนที่สามารถเปลี่ยนไปตาม SIM ที่บรรจุอยู่ในอุปกรณ์โทรศัพท์เคลื่อนที่ MSISDN ขนาด 64 บิตจะถูกเก็บไว้ใน SIM, HLR, และ VLR โดยจะประกอบด้วยข้อมูล 3 ส่วนดังนี้

1) Country Code (CC) เป็นรหัสที่ระบุประเทศที่ MS ลงทะเบียนไว้ขนาด 12 บิตเหมือน IMSI

2) National Destination Code (NDC) เป็นรหัสที่ระบุเครือข่ายโมบาย (PLMN) ภายในประเทศที่ผู้ใช้ลงทะเบียนด้วย มีขนาด 12 บิตเหมือน IMSI

3) Subscriber Number (SN) เป็นหมายเลขโทรศัพท์ผู้ใช้ มีขนาด 40 บิต

2.3.5 Mobile Station Roaming Number (MSRN)

VLR จะทำการกำหนด MSRN จะประกอบด้วยข้อมูล 3 ส่วนเหมือน MSISDN คือ CC, NDC, และ SN เป็นหมายเลขโทรศัพท์ชั่วคราวขณะที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC เมื่อมีการเรียก (Call) เข้ามา MSRN จะถูกใช้ในการหาเส้นทางไปยังอุปกรณ์โทรศัพท์เคลื่อนที่ของผู้ใช้ MSRN จะถูกเก็บไว้ใน SIM, HLR, และ VLR

2.3.6 Location Area Identity (LAI)

ในแต่ละ LA ของ MSC จะมี LAI เป็นหมายเลขประจำตัวของตนเอง LAI เป็นข้อมูลขนาด 40 บิตจะประกอบด้วยข้อมูล 3 ส่วนดังนี้

1) Mobile Country Code (MCC) เป็นรหัสที่ระบุประเทศที่ตั้งของ Location Area มีขนาด 12 บิตเหมือน IMSI

2) Mobile Network Code (MNC) เป็นรหัสที่ระบุเครือข่ายโมบาย (PLMN) ของ LA มีขนาด 12 บิตเหมือน IMSI

3) Location Area Code (LAC) เป็นรหัสหมายเลขประจำตัวของแต่ละ LA ในเครือข่าย GSM มีขนาด 16 บิต

2.3.7 Cell Identity (CI)

ภายใน LA ต่างๆ จะประกอบด้วยเซลล์ต่างๆ โดยแต่ละเซลล์นั้นจะมีเลขประจำตัวของแต่ละเซลล์ที่ไม่ซ้ำกัน, CI มีขนาด 16 บิต

2.3.8 Base transceiver Station Identity Code (BSIC)

เพื่อที่จะสามารถแยกขอบเขตระหว่าง BTS ได้ในแต่ละ BTS จะมีเลขประจำตัวของมันเองคือ BSIC ขนาด 6 บิต ซึ่งประกอบด้วยข้อมูล 2 ส่วนคือ

1) Network Color Code (NCC) เป็นรหัสสีภายใน PLMN ขนาด 3 บิต

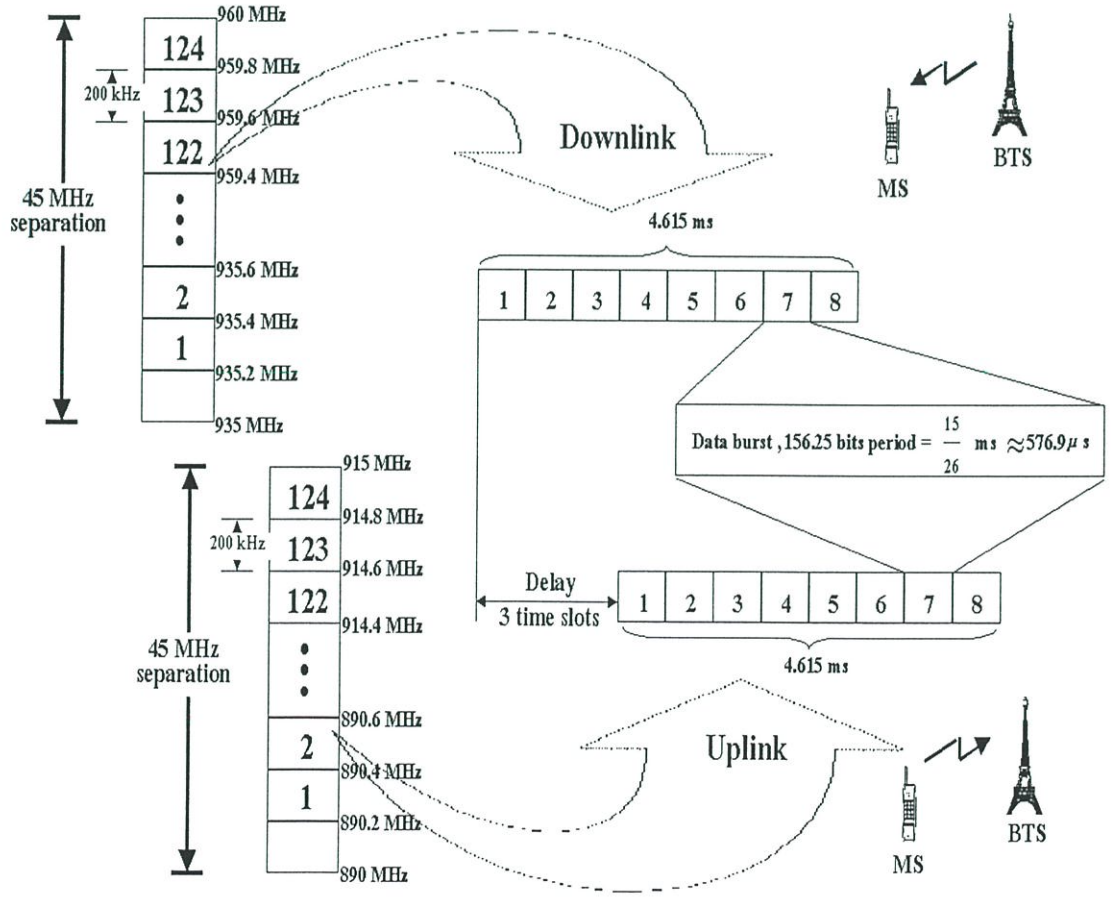
2) Base transceiver station Color Code (BCC) เป็นรหัสสีของ BTS ขนาด 3 บิตโดย BTS ที่อยู่ติดกันจะต้องมีรหัสสีที่แตกต่างกัน

2.4 โครงสร้างของช่องสัญญาณวิทยุ

เครือข่าย GSMใช้เทคโนโลยีการสื่อสารแบบ Time Division Multiple Access, TDMA กับ Frequency Division Multiple Access, FDMA ร่วมกันทำให้จำเป็นที่จะต้องมีฟังก์ชันที่มีความซับซ้อนในการจัดแบ่งช่องสัญญาณวิทยุเพื่อที่จะใช้ติดต่อสื่อสารระหว่างผู้ใช้กับเครือข่าย [4]

2.4.1 การจองช่องสัญญาณ (Channel Reservation)

เครือข่าย GSM จะทำการจอง (Reservation) 2 แถบความถี่คลื่นวิทยุ (Radio Frequency Band) ขนาด 45 MHz ดังแสดงในรูปที่ 2.3 แถบความถี่ 890-915 MHz สำหรับการสื่อสารจากโทรศัพท์เคลื่อนที่ถึงสถานีฐานเรียกว่า "สัญญาณขาขึ้น (Uplink)" และแถบความถี่ 935-960 MHz สำหรับการสื่อสารจากสถานีฐานถึงโทรศัพท์เคลื่อนที่เรียกว่า "สัญญาณขาลง (Downlink)" แต่ละแถบความถี่ขนาด 25 MHz ถูกแบ่งเป็น 124 ช่องสัญญาณแต่ละช่องสัญญาณมีขนาด 200 kHz ในแต่ละช่องสัญญาณขนาด 200 kHz นี้จะถูกแบ่งเป็น 8 ช่วงเวลา (Time Slot) หรือเรียกว่า "เฟรม TDMA" และในแต่ละช่วงเวลาจะสามารถส่ง Burst ข้อมูลขนาด 156.25 บิตหรือช่วงเวลาละ 15/26 ms (576.9 μs)



รูปที่ 2.3 การจองช่องสัญญาณวิทยุของเครือข่าย GSM

2.4.2 ช่องสัญญาณเสมือน (Logical Channels)

GSM นิยามกลุ่มของช่องสัญญาณเสมือน (Logical Channels) ไว้ 2 กลุ่มคือ ช่องสัญญาณการจราจรข้อมูล (Traffic Channels, TCH) และช่องสัญญาณการควบคุม (Signaling or Control Channels) ดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 ตารางช่องสัญญาณเสมือน

Group		Channel	Function	Direction
Traffic Channel	Traffic Channel (TCH)	TCH/F, Bm	Full rate TCH	MS←→BSS
		TCH/H, Lm	Half rate TCH	MS←→BSS
Signaling and Control Channel (Dm)	Broadcast Channel (BCH)	BCCH	Broadcast Control	MS←—BSS
		FCCH	Frequency Correction	MS←—BSS
		SCH	Synchronization	MS←—BSS
	Dedicated Control Channel (DCCH)	SDCCH	Stand-alone Dedicated Control	MS←→BSS
		SACCH	Slow Associated Control	MS←→BSS
		FACCH	Fast Associated Control	MS←→BSS
	Common Control Channel (CCCH)	RACH	Random Access	MS—→BSS
		AGCH	Access Grant	MS←—BSS
		PCH	Paging	MS←—BSS
		NCH	Notification	MS←—BSS

2.4.2.1 ช่องสัญญาณการจราจรข้อมูล (Traffic Channels, TCH)

TCH ถูกใช้สำหรับการสื่อสารข้อมูลของผู้ใช้ เช่น เสียง, ข้อมูล, Fax ช่องสัญญาณนี้จะไม่ใช้สื่อสารข้อมูลเกี่ยวกับการควบคุม การสื่อสารบน TCH สามารถทำงานได้ทั้งแบบ เซอร์กิตสวิทซ์ชิงและแพ็กเกตสวิทซ์ชิง TCH อาจถูกใช้แบบเต็มที่ (Full rate TCH, TCH/F) เรียกว่า "ช่องสัญญาณ Bm (Mobile B Channels)" หรืออาจแบ่งใช้ครึ่งหนึ่ง (Half rate TCH, TCH/H) เรียกว่า "ช่องสัญญาณ Lm (Mobile Low-rate Channels)" คล้ายกันกับการออกแบบช่องสัญญาณของ ISDN [1]

2.4.2.2 ช่องสัญญาณควบคุม (Signaling and Control Channels, Dm)

การจัดการและควบคุมเครือข่ายการสื่อสารเคลื่อนที่นั้นมีความจำเป็นที่จะต้องมีการสื่อสารข้อมูลเกี่ยวกับการควบคุมและการจัดการต่างๆ (Signaling Information) ค่อนข้างมาก เครือข่ายจัดเตรียมช่องสัญญาณวิทยุที่จะใช้สื่อสารข้อมูลการควบคุมต่างๆเรียกว่า "ช่องสัญญาณ Dm (Mobile D Channels)" ดังแสดงในตารางที่ 2.1 โดยแบ่งได้ เป็น 3 แบบคือ

1) Broadcast Channels (BCH) ถูกใช้โดย BTS ในการส่งสัญญาณขาลงให้กับ MS ที่อยู่ในเซลล์การจัดการของ BTS โดยข้อมูลที่ได้รับนั้นจะเหมือนกันหมด สามารถแบ่งย่อยได้ 3 ช่องสัญญาณคือ Broadcast Control Channels (BCCH), Frequency Correction Channels (FCCH), และ Synchronization Channels (SCH)

BCCH ใช้ส่งสัญญาณเพื่อให้ MS ทราบถึงข้อมูลเกี่ยวกับหน่วยงานใน BSS เช่น หมายเลขประจำตัวของหน่วยงานต่างๆ (LAI, CI, BSIC) ส่วน SCH และ FCCH ใช้ส่งข้อมูลเกี่ยวกับการทำ Synchronization ระหว่าง MS กับ BTS โดย SCH ใช้ในการทำให้เฟรมข้อมูลที่ MS ได้รับเข้ากันกับเฟรมข้อมูลที่ BTS ส่ง (Frame Synchronization) และ FCCH ใช้ในการทำให้ความถี่ของช่องสัญญาณที่ MS เข้ากันกับความถี่ของช่องสัญญาณที่ BTS กำหนดให้ (Frequency Synchronization)

2) Dedicated Control Channels (DCCH) ถูกใช้ส่งสัญญาณทั้งขาขึ้นและขาลงซึ่งถูกกำหนดให้ MS แบ่งย่อยได้ 3 ช่องสัญญาณคือ Stand-alone Dedicated Control Channels (SDCCH), Slow Associated Control Channels (SACCH), และ Fast Associated Control Channels (FACCH)

SDCCH ใช้ส่งข้อมูลเกี่ยวกับการจัดการต่างๆ ระหว่าง MS กับ BSS, SACCH ถูกใช้ส่งข้อมูลเกี่ยวกับการวัดประสิทธิภาพของ TCH และ SDCCH ข้อมูลที่ส่งจะเป็นรายงานเกี่ยวกับกำลังของสัญญาณและอัตราส่วนของบิตที่ผิดพลาด (Bit Error Ratio), และสุดท้าย FACCH ใช้ส่งข้อมูลเกี่ยวกับการสร้างการติดต่อ (Connection) ผ่านช่องสัญญาณ TCH

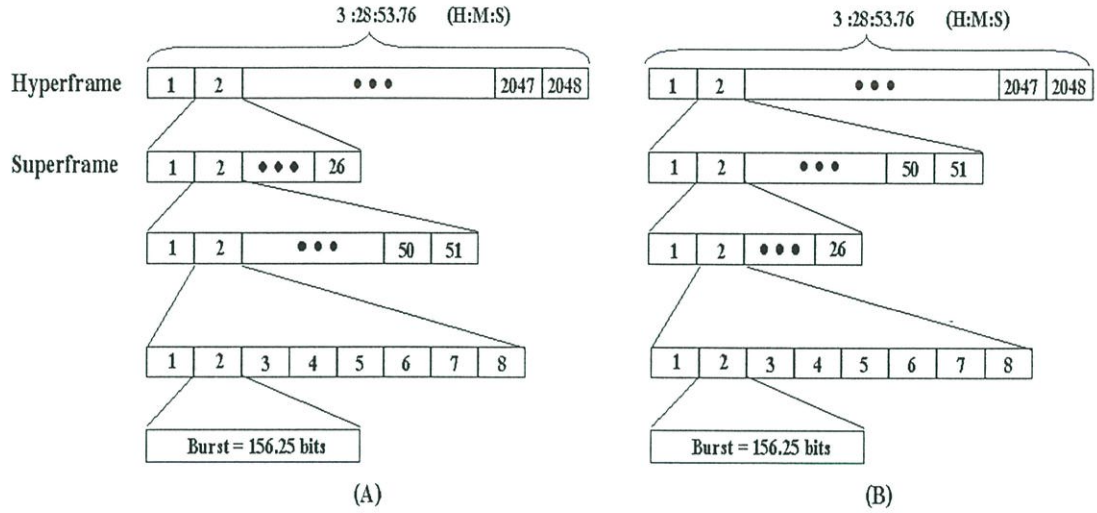
3) Common Control Channels (CCCH) ถูกใช้ในการตกลงเกี่ยวกับการเข้าถึง (Access) เครือข่าย ต่างๆ แบ่งย่อยได้ 4 ช่องสัญญาณคือ Random Access Channels (RACH), Access Grant Channels (AGCH), Paging Channels (PCH), และ Notification Channels (NCH)

RACH ถูกใช้ส่งสัญญาณขาขึ้นเมื่อ MS ต้องการจะขอใช้บริการต่างๆกับเครือข่าย เช่น การขอใช้ช่องสัญญาณ SDCCH, AGCH ถูกใช้ส่งสัญญาณขาลงโดย BTSจะทำการจองช่องสัญญาณวิทยุให้กับผู้ใช้แล้วส่งข้อมูลแจ้งให้ผู้ใช้ทราบถึงช่องสัญญาณที่กำหนดให้โดยผ่าน AGCH, PCH ถูกใช้ส่งสัญญาณขาลงโดย BTS เมื่อมีการเรียกเข้ามาหา MS (Call Termination) ในเซลล์ของ BTS, และสุดท้าย NCH ถูกใช้ส่งสัญญาณขาลงเมื่อการเรียกเป็นกลุ่มเข้ามาหา (Broadcast Call) MS

2.4.3 ช่องสัญญาณกายภาพ (Physical Channels)

ช่องสัญญาณกายภาพของเครือข่าย GSM แบ่งเป็น 2048 ไฮเปอร์เฟรมซึ่งมีรอบของช่วงเวลา (Period) เท่ากับ 3 ชั่วโมง 28 นาที 53.76 วินาที ในแต่ละไฮเปอร์เฟรมจะประกอบด้วยซุปเปอร์ซึ่งประกอบด้วยเฟรม TDMA 1326 เฟรมมีช่วงเวลาเท่ากับ 6.12 วินาที ภาย ในซุปเปอร์เฟรมประกอบด้วยมัลติเฟรม 2 แบบ คือ 51 มัลติเฟรม และ 26 มัลติเฟรม ในหนึ่งซุปเปอร์เฟรมจะประกอบด้วย 51 มัลติเฟรมของ 26 มัลติเฟรม หรือ 26 มัลติเฟรมของ 51 มัลติเฟรม ดังแสดงในรูปที่

2.4.A และ 2.4.B ตามลำดับ โดย 26 มัลติเฟรมของ 51 มัลติเฟรมจะใช้ในการส่งข้อมูลที่เป็นสัญญาณเสียงหรือข้อมูลของผู้ใช้ที่ไม่เกี่ยวข้องกับการควบคุม และโดย 51 มัลติเฟรมของ 26 มัลติเฟรมจะใช้ส่งข้อมูลเกี่ยวกับการควบคุม

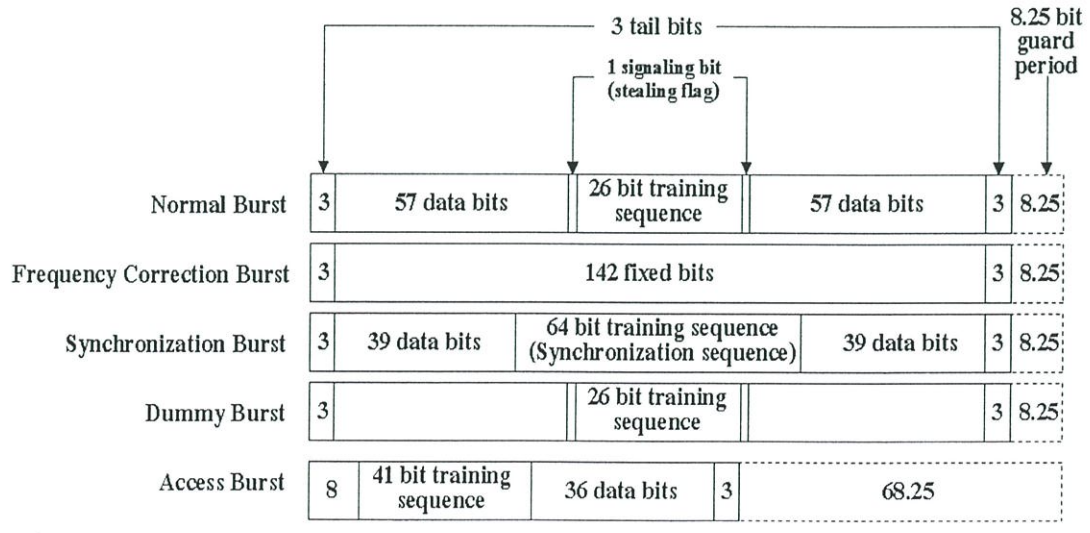


รูปที่ 2.4 โครงสร้างเฟรมข้อมูลของเครือข่าย GSM

ภายในมัลติเฟรมทั้ง 2 แบบ จะประกอบด้วยเฟรม TDMA ที่มี 8 ช่วงเวลา สำหรับ 51 มัลติเฟรมมีช่วงเวลาเท่ากับ 235.4 ms และ 26 มัลติเฟรมมีช่วงเวลาเท่ากับ 120 ms

2.4.4 Burst

Burst ข้อมูลของเครือข่าย GSM แบ่งเป็น 5 ชนิด โดยแบ่งตามลักษณะการส่งไปในช่องสัญญาณต่างๆ Burst ทุกชนิดจะมีขนาดเท่ากันคือ 156.25 บิต ดังแสดงในรูปที่ 2.5



รูปที่ 2.5 ประเภทของ Burst ข้อมูลในเครือข่าย GSM

Normal Burst (NB) ถูกใช้ในการส่งข้อมูลของ TCH และข้อมูลในการควบคุมต่างๆ ยกเว้นข้อมูลของ RACH ในแต่ละ Burst นั้นจะมี Guard Period เป็นส่วนที่จะไม่มีการส่งข้อมูลของ Burst นั้นๆ Tail bits 3 บิตที่อยู่ตรงหัวและท้ายของ Burst ถูกเซ็ตให้เป็น 0 ทั้ง 3 บิต Stealing Flag (SF) ใช้ระบุเป็นข้อมูลในการควบคุม (Control Data) Training Sequence (TS) ขนาด 26 บิตใช้บอกลำดับของข้อมูลที่ส่งและบอกความแรงของสัญญาณที่ได้รับเพื่อเลือกสัญญาณที่แรงที่สุดในกรณีสัญญาณเดินทางแบบหลายเส้นทาง (Multipath Propagation) ในส่วนของข้อมูลที่ส่งจริงๆของ NB จะแบ่งเป็น 2 ส่วนๆละ 57 บิต โดย NB จะถูกส่งผ่าน TCH, FACCH, และ SDCCH

Frequency Correction Burst (FB) ถูกส่งโดย BTS เพื่อบอกให้ MS ทราบถึงความถี่ที่ใช้ MS จะได้รับส่งสัญญาณโดยใช้ความถี่ที่ตรงกัน เนื่องจากมีการใช้หลายความถี่ในการส่งสัญญาณ ซึ่ง FB จะถูกส่งโดย BTS ผ่าน FCCH ให้กับ MS

Synchronization Burst (SB) จะถูกใช้ส่งเพื่อการทำให้การรับสัญญาณของ MS สามารถเข้ากันได้กับการส่งสัญญาณของ BTS (Synchronization) ซึ่ง SB จะถูกส่งผ่าน SCH

Dummy Burst (DB) จะถูกใช้ส่งผ่าน BCCH เมื่อ BTS ไม่มี Burst อื่นๆจะส่ง ดังนั้น BCCH จะต้องส่ง Burst อย่างน้อย 1 Burst เสมอ ทำให้ MS สามารถวัดกำลังสัญญาณของ BCCH ได้ วิธีการนี้เรียกว่า "Quality Monitoring"

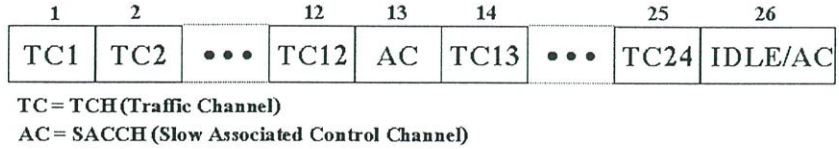
Access Burst (AB) จะถูกส่งผ่าน RACH เมื่อ MS จะทำการติดต่อกับเครือข่ายโดย AB จะมี Guard Period มากกว่า Burst อื่นๆ

2.4.5 การแม็พช่องสัญญาณเสมือนลงในช่องสัญญาณกายภาพ

การแม็พช่องสัญญาณเสมือนลงในช่องสัญญาณการภาพในเครือข่าย GSM มี 2 แบบตามขนาดของมัลติเฟรม คือ การแม็พ 26 มัลติเฟรมและการแม็พ 51 มัลติเฟรม

2.4.5.1 การแม็พ 26 มัลติเฟรม

แต่ละเฟรม TDMA 26 เฟรมจะถูกมัลติเพล็กซ์จากสัญญาณเสมือน 2 ช่องสัญญาณคือ TCH และ SACCH ลงบนช่องสัญญาณกายภาพดังแสดงในรูปที่ 2.6

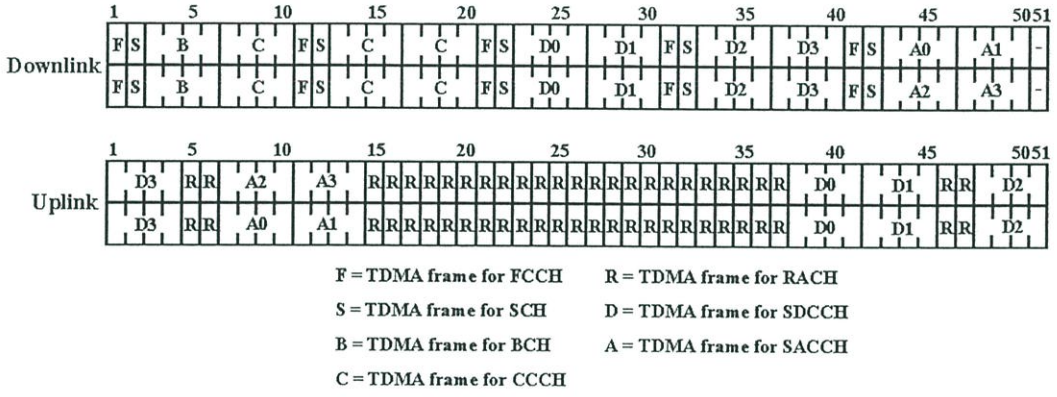


รูปที่ 2.6 การสร้างช่องสัญญาณใน 26 มัลติเฟรม

26 มัลติเฟรมจะประกอบด้วย 24 TCH สำหรับข้อมูลของผู้ใช้และมัลติเฟรมนี้ประกอบด้วยข้อมูลการควบคุม (Signaling Data) ของ SACCH ส่วนเฟรมที่ 26 นั้นจะไม่ถูกใช้ในกรณี Full rate TCH/F แต่จะถูกใช้ในกรณีที่เป็น Half rate TCH/H เนื่องจากข้อมูลที่ส่งผ่าน TCH และ SACCH จะใช้ Burst แบบ NB ซึ่งแต่ละ NB จะมี Stolen Flag 2 บิต สำหรับข้อมูลของ FACCH จะหาได้จากการนำ Stolen Flag ของแต่ละ 8 Time Slot มารวมกัน

2.4.5.2 การแม็พ 51 มัลติเฟรม

51 มัลติเฟรมใช้ในการสื่อสารข้อมูลของช่องสัญญาณควบคุม ยกเว้น FACCH ในแต่ละมัลติเฟรมจะประกอบด้วย 51 เฟรม TDMA โดยการรวมกันของช่องสัญญาณเสมือนจะมีลักษณะดังแสดงในรูปที่ 2.7



รูปที่ 2.7 การสร้างช่องสัญญาณใน 51 มัลติเฟรม

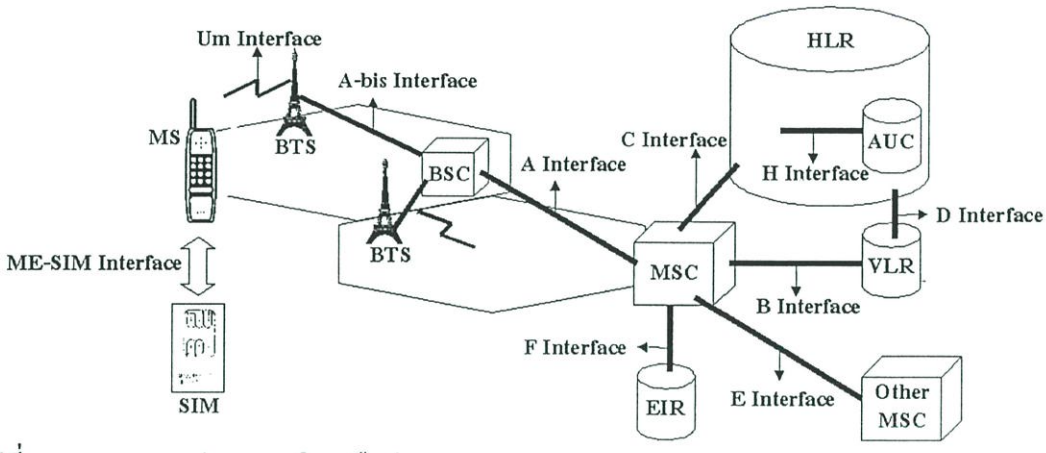
รูปแบบการรวมของช่องสัญญาณเสมือนนั้นในแต่ละช่วงเวลา (Time Slot) จะไม่ซ้ำกันขึ้นอยู่กับการกำหนดของ BSS ที่จะเป็นผู้กำหนดขึ้น

2.5 การติดต่อระหว่างหน่วยงานต่างๆ ของระบบ

เครือข่าย GSM แบ่งการติดต่อสื่อสารข้อมูลของหน่วยงานต่างๆ ในเครือข่ายเป็นช่วงๆดังแสดงในรูปที่ 2.8 [5]

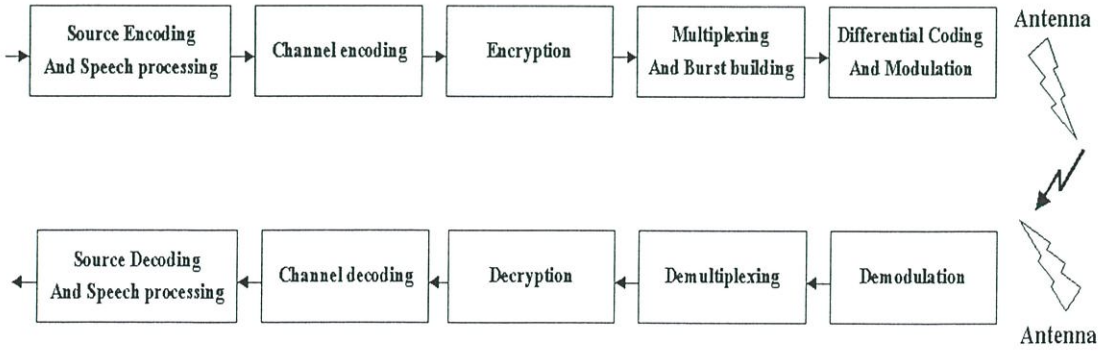
ถ้าแบ่งการติดต่อสื่อสารตามลักษณะของสื่อกลางที่ใช้สื่อสารจะแบ่งได้เป็น 2 ส่วนคือ ส่วนที่สื่อสารผ่านช่องสัญญาณวิทยุและส่วนที่ใช้สายส่งเป็นสื่อกลางในการสื่อสารข้อมูล ส่วนที่สื่อสารผ่านช่องสัญญาณวิทยุจะเรียกว่า Um Interface จะเป็นการติดต่อระหว่าง BTS กับ MS และส่วนที่สื่อสารโดยใช้สายส่งจะแบ่งปันช่วงๆตามการติดต่อของหน่วยงาน การติดต่อระหว่าง BTS กับ BSC ใช้การติดต่อแบบ A-bis Interface, การติดต่อระหว่าง BSC กับ MSC ใช้การติดต่อแบบ A Interface, การติดต่อระหว่าง MSC กับ VLR ใช้การติดต่อแบบ B Interface, การติดต่อระหว่าง

MSC กับ HLR ใช้การติดต่อแบบ C Interface, การติดต่อระหว่าง VLR กับ HLR ใช้การติดต่อแบบ D Interface, การติดต่อระหว่าง MSC ด้วยกันเองใช้การติดต่อแบบ E Interface, ส่วนการติดต่อระหว่าง HLR กับ AuC ที่อยู่ภายใน HLR ใช้การติดต่อแบบ H Interface และการติดต่อระหว่างอุปกรณ์โทรศัพท์เคลื่อนที่ (Mobile Equipment) กับ SIM ใช้การติดต่อแบบ ME-SIM Interface



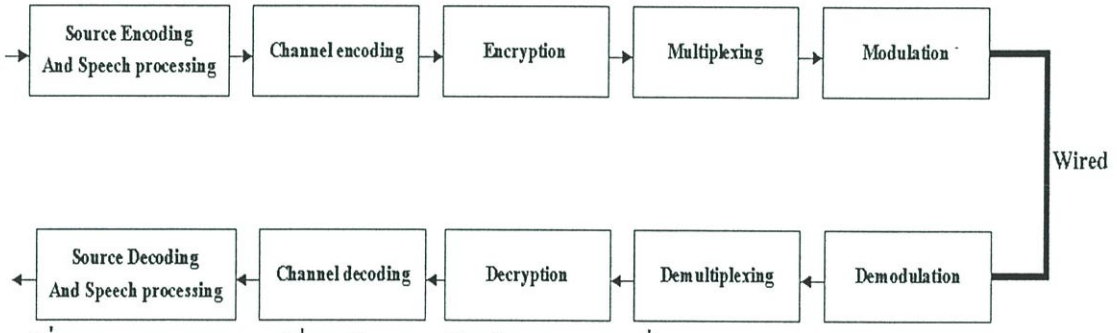
รูปที่ 2.8 Interfaces ต่างๆภายในเครือข่าย GSM

การติดต่อแบบ Um Interface จะมีขั้นตอนการทำงานดังแสดงในรูปที่ 2.9 สัญญาณเสียงของการสนทนา (Speech Signal) ถูกผ่านกระบวนการเข้ารหัสสัญญาณเสียง (Speech Processing) แล้วทำการทำการเข้ารหัสช่องสัญญาณ (Channel Coding) ต่อจากนั้นทำการเข้ารหัสลับข้อมูล (Encryption) ทำการมัลติเพล็กซ์ข้อมูลเป็น Burst ต่างๆ แล้วทำการกล้ำสัญญาณ (Modulation) เพื่อส่งข้อมูลผ่านช่องสัญญาณวิทยุในความถี่ต่างๆ ตามต้องการ ทางฝั่งผู้รับก็จะทำการแยกสัญญาณ (Demodulation) และทำการดีมัลติเพล็กซ์ Burst ที่ได้รับแล้วถอดรหัสลับข้อมูล (Decryption) หลังจากนั้นทำการถอดรหัสช่องสัญญาณ (Channel Decoding) แล้วนำไปผ่านกระบวนการถอดรหัสสัญญาณเสียง (Speech Processing) เพื่อที่จะได้รับฟังเสียงสนทนาตามต้องการ



รูปที่ 2.9 กระบวนการเปลี่ยนสัญญาณเสียงให้เป็นคลื่นวิทยุ

การติดต่อแบบอื่นๆ จะมีขั้นตอนการทำงานดังแสดงในรูปที่ 2.10 สัญญาณเสียงของการสนทนา (Speech Signal) ถูกผ่านกระบวนการเข้ารหัสสัญญาณเสียง (Speech Processing) แล้วทำการทำการเข้ารหัสช่องสัญญาณ (Channel Coding) ต่อจากนั้นทำการเข้ารหัสลับข้อมูล (Encryption) ทำการมัลติเพล็กซ์ข้อมูล แล้วทำการกล้ำสัญญาณ (Modulation) เพื่อส่งข้อมูลผ่านสายส่ง ทางฝั่งผู้รับก็จะทำการแยกสัญญาณ (Demodulation) และทำการดีมัลติเพล็กซ์ข้อมูล ที่ได้รับแล้วถอดรหัสลับข้อมูล (Decryption) หลังจากนั้นทำการถอดรหัสช่องสัญญาณ (Channel Decoding) แล้วนำไปผ่านกระบวนการถอดรหัสสัญญาณเสียง (Speech Processing) เพื่อที่จะได้รับฟังเสียงสนทนาตามต้องการ



รูปที่ 2.10 กระบวนการเปลี่ยนสัญญาณเสียงใน Interface อื่นๆ

บทที่ 3

การรักษาความปลอดภัยของเครือข่าย GSM

ในบทนี้กล่าวถึงรายละเอียดเกี่ยวกับกระบวนการในการรักษาความปลอดภัยของเครือข่าย GSM โดยในส่วนแรกของบทนี้จะเป็นการอธิบายถึงทฤษฎีพื้นฐานของระบบการรักษาความปลอดภัยที่จำเป็นในการศึกษาระบบการรักษาความปลอดภัยของเครือข่าย GSM และในส่วนที่เหลือจะเป็นวิธีการรักษาความปลอดภัยในเครือข่าย GSM

3.1 ทฤษฎีพื้นฐานของระบบการรักษาความปลอดภัย

ในการรักษาความปลอดภัยเครือข่าย ผู้ออกแบบระบบรักษาความปลอดภัยของเครือข่ายจำเป็นต้องที่จะสามารถเลือกใช้อัลกอริทึมที่ใช้รักษาความปลอดภัยอย่างถูกต้องและเหมาะสม

ศาสตร์ของการเข้าและถอดรหัสลับข้อมูล (Cryptography) คือ กรรมวิธีในการป้องกันความลับของข้อมูลทำให้ผู้ส่งและผู้รับที่ถูกต้องเท่านั้นที่จะสามารถเข้าใจเนื้อหาสาระของข้อมูลได้ ข้อมูลก่อนที่จะทำการเข้ารหัสลับเรียกว่า "Plaintext" เมื่อนำไปคำนวณกับอัลกอริทึมการเข้าและถอดรหัสลับที่จะต้องมีความซับซ้อนซึ่งมีผลลัพธ์ทำให้ข้อมูลเปลี่ยนแปลงไปจากเดิมจนไม่สามารถเข้าใจเนื้อหาของข้อมูลได้ ยกเว้นผู้ที่ทราบคีย์ที่ใช้ในการถอดรหัสลับเท่านั้นจึงจะสามารถถอดรหัสลับข้อมูลกลับไปอยู่ในรูปแบบเดิมได้ โดยผลลัพธ์ของอัลกอริทึมที่จะใช้ในการเข้าและถอดรหัสลับเรียกว่า "Cipher หรือ Ciphertext" [6]

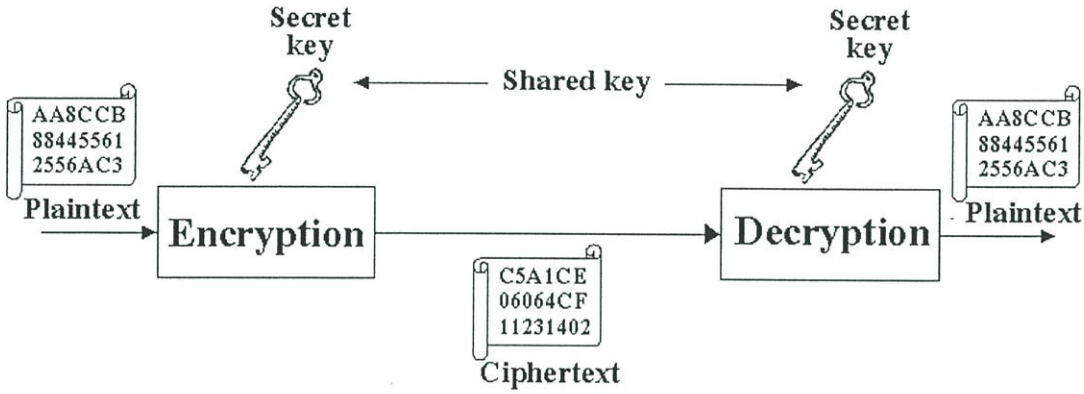
โดยทั่วไปแล้วการเข้าและถอดรหัสลับแบ่งเป็น 2 ชนิดด้วยกัน คือ การเข้ารหัสลับแบบ Secret Key และการเข้ารหัสลับแบบ Public Key

3.1.1 การเข้ารหัสลับแบบ Secret Key

การเข้ารหัสลับแบบ Secret Key หรือ Symmetric หรือ Private Key คือ การเข้ารหัสลับข้อมูลที่ผู้ส่งและผู้รับจะใช้คีย์ในการเข้าถอดรหัสลับร่วมกัน โดยผู้ส่งจะนำข้อมูลมาเข้ารหัสลับโดยใช้คีย์ที่ได้ตกลงไว้กับผู้รับ ทางฝั่งผู้รับจะใช้คีย์อันเดิมในการถอดรหัสลับดังแสดงในรูปที่ 3.1

การเข้ารหัสลับแบบ Secret Key ยังแบ่งเป็นย่อยได้เป็น 2 ประเภทคือ การเข้ารหัสลับข้อมูลครั้งละบล๊อก (หลายๆ ไบต์) เรียกว่า "Block Cipher" และ การเข้ารหัสลับข้อมูลครั้งละบิตหรือครั้งละไบต์เรียกว่า "Stream Cipher" โดยปกติแล้ว Stream Cipher ใช้เวลาในการเข้าและถอดลับน้อยกว่าBlock Cipher แต่ Block Cipher มีกระบวนการเข้าและถอดรหัสลับที่ซับซ้อนกว่า Stream Cipher

ความปลอดภัยของอัลกอริทึมที่ใช้ในการเข้ารหัสลับแบบ Secret Key ขึ้นกับองค์ประกอบหลายส่วน นอกจากอัลกอริทึมต้องมีประสิทธิภาพเพียงพอที่จะทำให้ผู้ถอดรหัสลับถึงแม้จะทราบกระบวนการเข้าและถอดรหัสลับและข้อมูล Ciphertext ก็ยังไม่สามารถถอดรหัสลับ ถ้าปราศจากคีย์ที่ใช้ในการเข้าและถอดรหัสลับ ดังนั้นการเก็บความลับของคีย์ที่ใช้ในการเข้าและถอดรหัสลับก็เป็นอีกองค์ประกอบที่สำคัญเช่นกัน

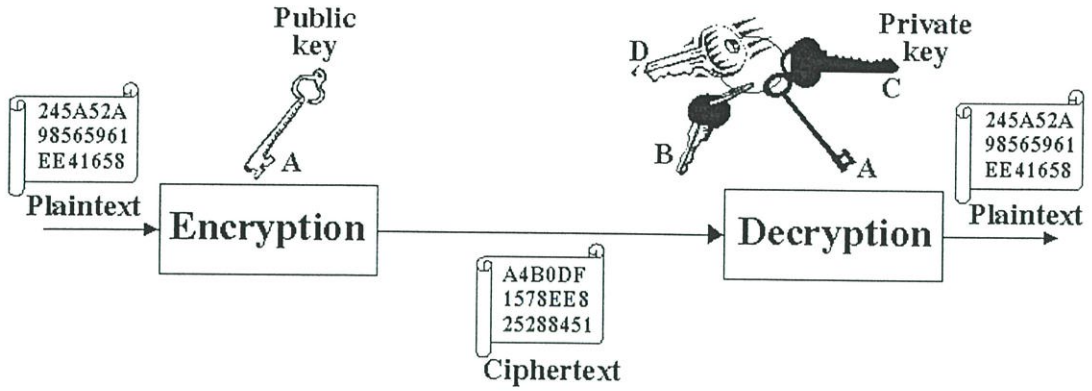


รูปที่ 3.1 การเข้ารหัสลับแบบ Secret Key

3.1.2 การเข้ารหัสลับแบบ Public Key

การเข้ารหัสลับแบบ Public Key คือ การเข้ารหัสลับที่ผู้ส่งและผู้รับจะใช้คีย์ที่แตกต่างกันในการเข้าถอดรหัสลับ โดยคีย์ที่ผู้ส่งใช้เข้ารหัสข้อมูลเรียกว่า "Public Key" ส่วนคีย์ที่ผู้รับใช้ถอดรหัสข้อมูลเรียกว่า "Private Key" ผู้ส่งทุกคนในระบบจะใช้ Public Key ในการเข้ารหัสข้อมูลส่วนทางฝั่งผู้รับจะใช้ Private Key ของผู้ส่งแต่ละคนถอดรหัสข้อมูลดังแสดงในรูปที่ 3.2

โดยปกติแล้วการเข้ารหัสลับแบบ Public Key จะมีความเร็วในการเข้าและถอดรหัสลับต่ำกว่าการเข้ารหัสลับแบบ Secret Key แต่การเข้ารหัสลับแบบ Public Key สามารถเปิดเผย Public Key ที่ผู้ส่งจะใช้เข้ารหัสลับข้อมูลซึ่งจะต่างกับการเข้ารหัสลับแบบ Secret Key ที่ต้องเก็บรักษาคีย์ที่ใช้เข้าและถอดรหัสลับให้เป็นความลับอยู่เสมอ



รูปที่ 3.2 การเข้ารหัสลับแบบ Public Key

ในการรักษาความปลอดภัยนอกจากการเข้ารหัสลับแบบต่างๆแล้วยังมีอัลกอริทึมแบบอื่นๆ ที่ใช้ในการรักษาความปลอดภัยอีก เช่น ฟังก์ชัน Hash

3.1.3 ฟังก์ชัน Hash แบบทางเดียว (One-way Hash Functins)

ฟังก์ชัน Hash แบบทางเดียว คืออัลกอริทึมในการลดขนาดข้อมูลเป็นข้อมูลขนาดที่เล็กลง โดยหลักการทั่วไปแล้วฟังก์ชัน Hash แบบทางเดียวจะเหมือนกับการเข้าและถอดรหัสลับต่างกันที่ว่าขนาดเอาท์พุตจะเล็กลงและไม่สามารถทำกระบวนการย้อนกลับไปหาอินพุตที่ถูกต้องแน่นอนได้ (One-way)

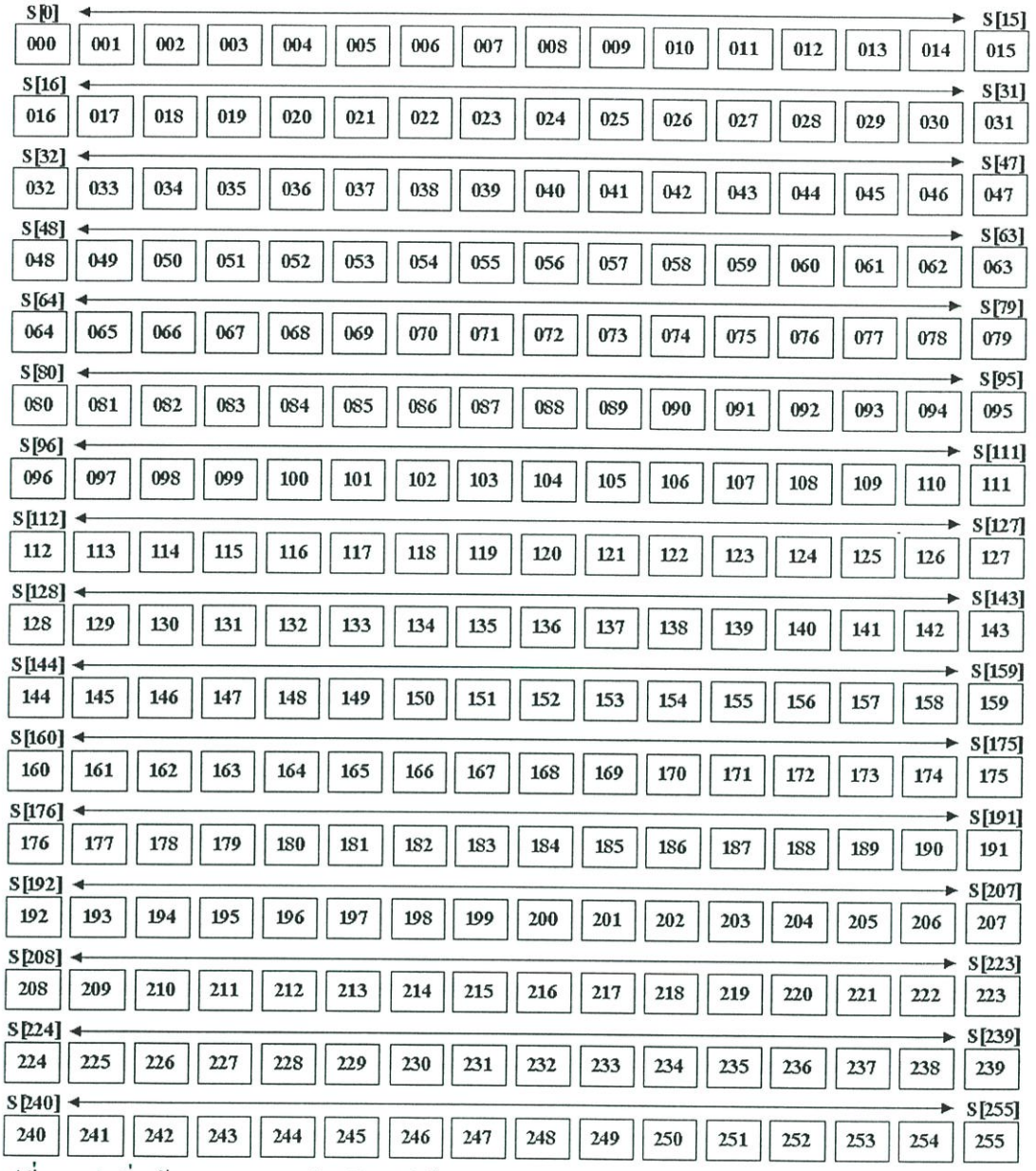
3.1.4 อัลกอริทึม RC 4

อัลกอริทึม RC4 ในการเข้าและถอดรหัสลับข้อมูลแบบ Secret Key โดยมีลักษณะเป็น Stream Cipher ถูกออกแบบโดย Ron L. Rivest ในปี 1992 [7] ในการเข้าและถอดรหัสลับจะทำการผลิตคีย์ต่อเนื่อง (Key Stream) แล้วนำไป XOR กับ Plaintext เพื่อทำการผลิต Ciphertext โดยการผลิตคีย์ต่อเนื่องนั้นจะผลิตคีย์เป็นรอบๆละ 8 บิต

RC 4 เป็นอัลกอริทึมในการเข้าและถอดรหัสลับที่ความยืดหยุ่นสูงในการเข้าและถอดรหัสลับ สามารถเลือกใช้ขนาดของคีย์ที่จะใช้ในการเข้าและถอดรหัสลับได้ตามต้องการ โดยอัลกอริทึม RC4 ประกอบ 2 ส่วนหลักคือ การจัดตารางคีย์ (Key Scheduling) และ การผลิตคีย์ต่อเนื่อง (Key Stream Generator)

3.1.4.1 การจัดตารางคีย์ (Key Scheduling)

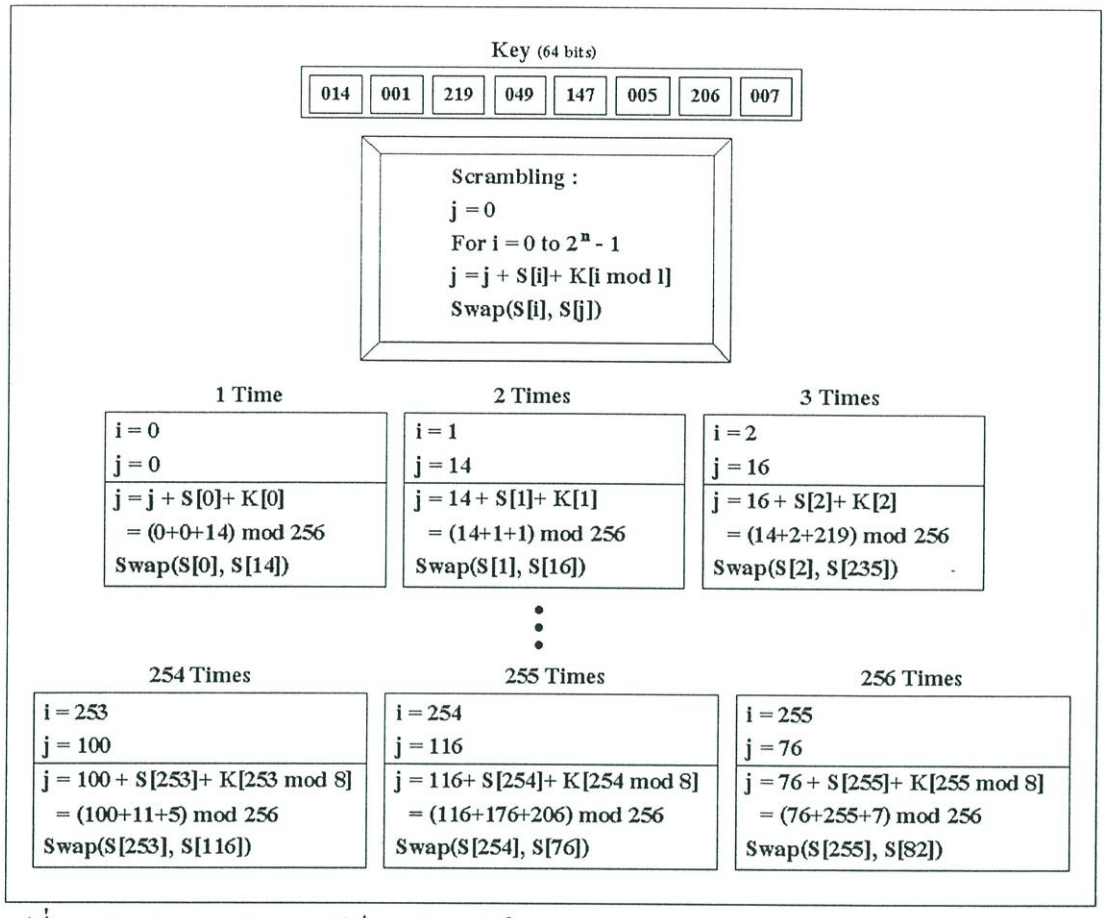
อัลกอริทึม RC4 จะประกอบด้วยตาราง S ที่มีสมาชิกในตาราง S ทั้งหมด 256 ตัว โดยแต่ละตัวมีขนาด 1 ไบต์ เรียกตาราง S ว่า "S-Box" ในตอนเริ่มต้นของการเข้าและถอดรหัสลับข้อมูลของอัลกอริทึม RC4 นั้นสมาชิกแต่ละตัวใน S-Box จะมีค่าตั้งแต่ 0 ถึง 255 เรียงตามลำดับของเลขดัชนี (Index) ของสมาชิกใน S-Box ดังแสดงในรูปที่ 3.3



รูปที่ 3.3 ค่าเริ่มต้นของ S-Box ในอัลกอริทึม RC4

เมื่อเริ่มทำการจัดตารางคีย์ จะนำคีย์ที่ใช้เข้าและถอดรหัสลับข้อมูลมาใส่ลงไปในอาร์เรย์ K โดยอาร์เรย์ K มีจำนวนสมาชิกทั้งหมดตามขนาดของคีย์ที่เลือกใช้และสมาชิกแต่ละตัวจะมีขนาด 1 ไบต์ เช่น ถ้าใช้คีย์ในการเข้ารหัสลับขนาด 64 บิต อาร์เรย์ K จะมีสมาชิก 8 ตัว

ทำการกวนตารางคีย์ (Key Scrambling) เพื่อสลับเปลี่ยนค่าของสมาชิกใน S-Box โดยใช้คีย์ในการเข้าและถอดรหัสลับเป็นตัวควบคุมตำแหน่งการสลับสับเปลี่ยน ขั้นตอนการกวนตารางคีย์นี้จะทำการสลับเปลี่ยนค่าของสมาชิกใน S-Box ทั้งหมด 256 ครั้ง ในการสลับเปลี่ยนค่าของสมาชิกใน S-Box จะทำการสลับเปลี่ยนโดยมีขั้นตอนการคำนวณดังแสดงใน รูปที่ 3.4



รูปที่ 3.4 ตัวอย่างการจัดตารางคีย์ของอัลกอริทึม RC4

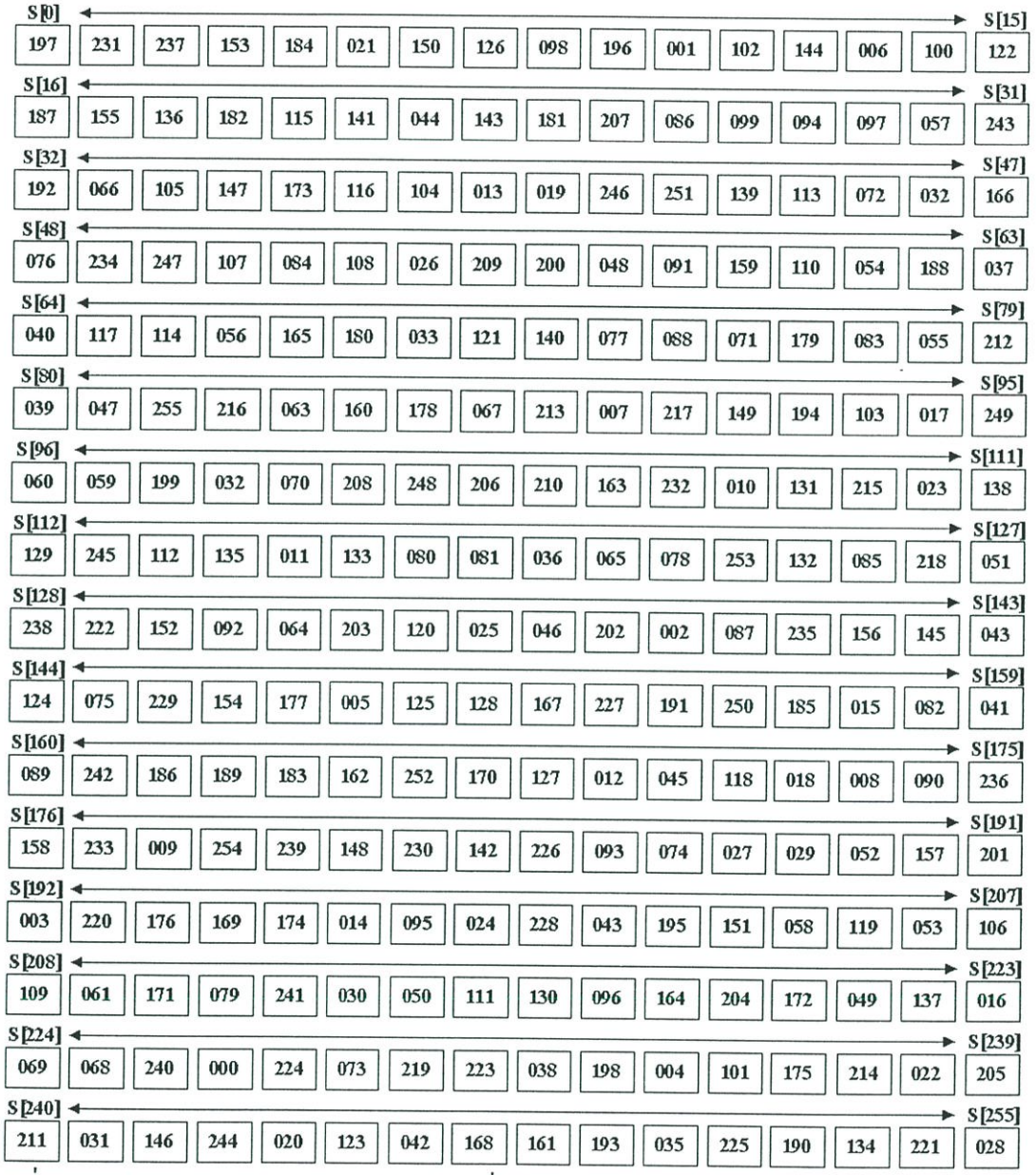
ขั้นตอนการจัดตารางคีย์จะประกอบด้วยตัวแปร 2 ตัวคือ ตัวแปร i และตัวแปร j ค่าของตัวแปร i จะถูกเพิ่มขึ้นทีละ 1 ทุกรอบของการสลับเปลี่ยนโดยค่าตัวแปร i มีค่าเริ่มต้นเป็น 0 ค่าของตัวแปร j ซึ่งมีค่าเริ่มต้นเป็น 0 เช่นเดียวกับค่าตัวแปร i จะถูกนำไปบวกกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i และค่าของสมาชิกในอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วยจำนวนสมาชิกในอาร์เรย์ K หลังจากการนั้นนำค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i สลับเปลี่ยนกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร j

ในการจัดตารางคีย์ที่มีสลับเปลี่ยนค่าของสมาชิกต่างๆใน S-Box ทั้งหมด 256 รอบนี้เพื่อทำให้ค่าของสมาชิกใน S-Box ไม่สามารถคาดเดาได้โดยง่ายเมื่อผู้ถอดรหัสลับไม่ทราบจากคีย์ที่จะใช้ในการเข้าและถอดรหัสลับ

3.1.4.2 การผลิตคีย์ต่อเนื่อง (Key Stream Generator)

ในการผลิตคีย์ต่อเนื่องนั้นจะนำเอา S-Box ที่ได้ผ่านการจัดตารางคีย์มาแล้ว ดังแสดงในรูปที่ 3.5 มาคำนวณหาคีย์ต่อเนื่อง (Key Stream) โดยคีย์ต่อเนื่องจะถูกผลิตเป็นรอบๆ ละ 8 บิต โดยแต่

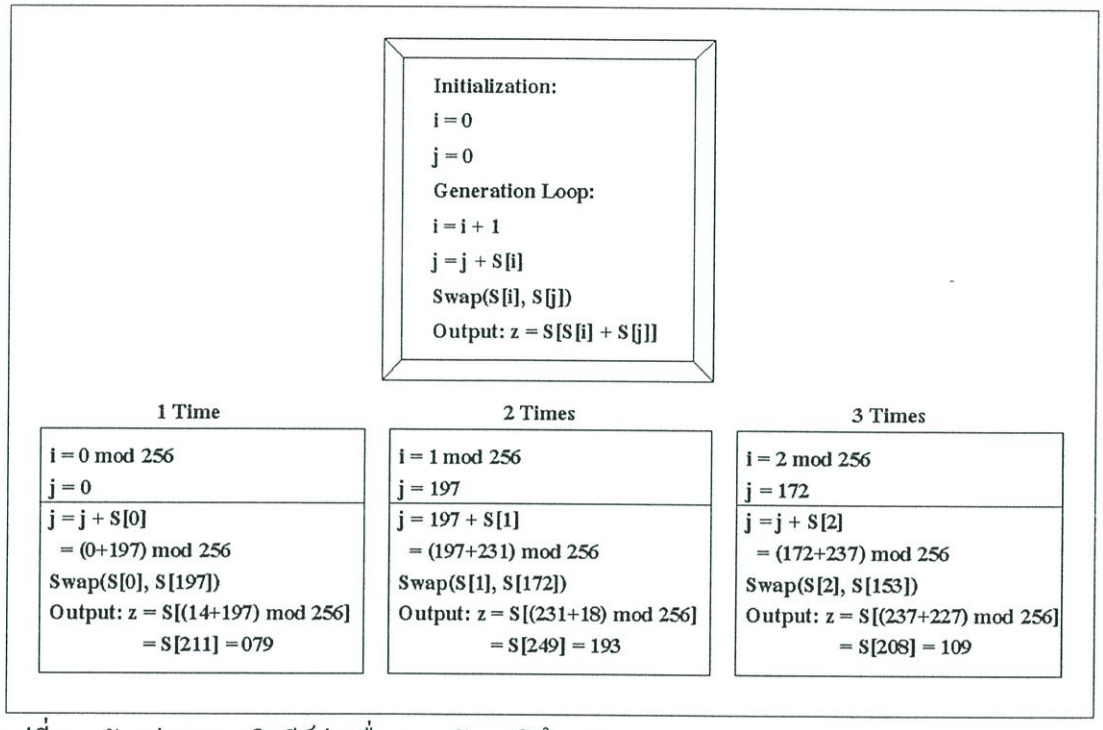
ละรอบของการผลิตจะทำการสลับเปลี่ยนค่าของสมาชิกใน S-Box ทำให้เมื่อต้องผลิตคีย์ต่อเนื่องจำนวนมากๆ ค่าของสมาชิกใน S-Box ยังคงความยุ่งยากในการคาดเดาค่าของสมาชิกใน S-Box



รูปที่ 3.5 ค่าของ S-Box สำหรับการผลิตคีย์ต่อเนื่องในอัลกอริทึม RC4

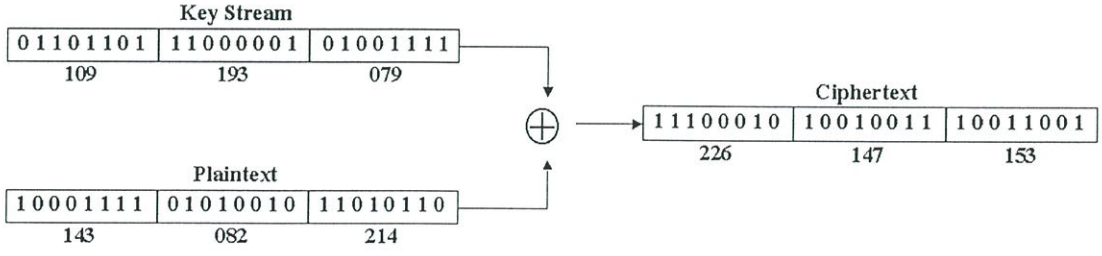
ขั้นตอนการผลิตคีย์ต่อเนื่องจะประกอบด้วยตัวแปร 2 ตัวคือ ตัวแปร i และตัวแปร j เหมือนกับการจัดตารางคีย์ ค่าของตัวแปร i จะถูกเพิ่มขึ้นทีละ 1 แล้วหารเอาเศษด้วย 256 ทุกรอบของการผลิตคีย์ต่อเนื่องโดยค่าตัวแปร i มีค่าเริ่มต้นเป็น 0 สำหรับการหารเอาเศษนั้นเพื่อทำให้ค่าของตัวแปร i ไม่เกินไปกว่าค่าของดัชนีของ S-Box ที่เป็นไปได้ ค่าของตัวแปร j ซึ่งมีค่าเริ่มต้นเป็น 0 เช่นเดียวกับค่าตัวแปร i จะถูกนำไปบวกกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i

หลังจากการนั้นนำค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i สลับเปลี่ยนกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร j เอาท์พุตของการผลิตคีย์ต่อเนื่องในแต่ละรอบคือสมาชิกใน S-Box ที่มีดัชนีเท่ากับค่าของสมาชิกใน S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i บวกกับค่าของสมาชิกใน S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร j ดังแสดงในรูปที่ 3.6



รูปที่ 3.6 ตัวอย่างการผลิตคีย์ต่อเนื่องของอัลกอริทึม RC4

เอาท์พุตของการผลิตคีย์ต่อเนื่องในแต่ละรอบจะถูกนำไป XOR กับ Plaintext เพื่อทำการสร้าง Ciphertext ดังแสดงในรูปที่ 3.7 ลำดับของบิต (Bit Sequence) ใน Plaintext กับลำดับของบิต (Bit Sequence) ใน Ciphertext จะแตกต่างกันทำให้เป็นการยากที่จะเปลี่ยน Ciphertext กลับไปเป็น Plaintext โดยไม่ทราบคีย์ในการเข้าและถอดรหัสลับ



รูปที่ 3.7 การเข้ารหัสลับข้อมูลของอัลกอริทึม RC4

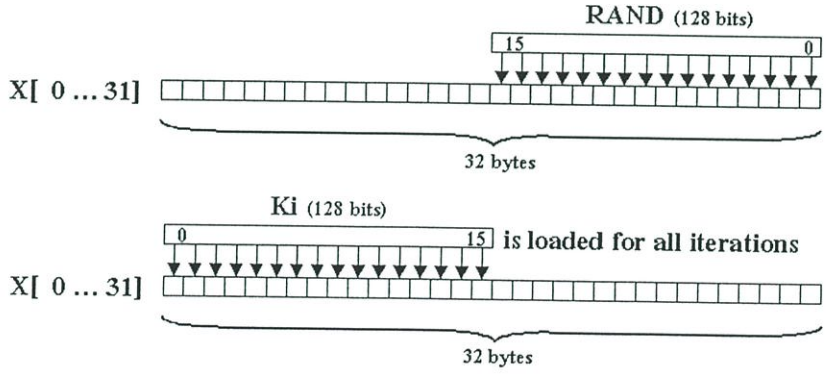
3.2 อัลกอริทึมในการรักษาความปลอดภัยของเครือข่าย GSM

เครือข่าย GSM เลือกใช้อัลกอริทึมในการรักษาความปลอดภัย 3 อัลกอริทึม คือ A3, A8, และ A5 ในส่วนของ A3 และ A8 นั้นในทางปฏิบัติทั้ง 2 อัลกอริทึมจะรวมกันอยู่ในอัลกอริทึม A38 เป็นอัลกอริทึมที่เครือข่าย GSM ใช้ตรวจสอบผู้ใช้และสร้างคีย์ที่ใช้ในการเข้าและถอดรหัสลับ ส่วนอัลกอริทึม A5 ใช้เป็นอัลกอริทึมในการเข้าและถอดรหัสลับข้อมูลระหว่างผู้ใช้กับเครือข่าย [15]

3.2.1 อัลกอริทึม A38 (A3&A8)

อัลกอริทึม A38 เป็นฟังก์ชัน Hash แบบทางเดียวอย่างหนึ่ง โดยจะรับอินพุตขนาด 256 บิต คือ Ki ขนาด 128 บิตและ RAND ขนาด 128 บิตแล้วนำไปคำนวณหาเอาท์พุตขนาด 96 บิตโดย 32 บิตแรกจะใช้เป็น SRES และ 64 บิตที่เหลือจะใช้เป็น Kc

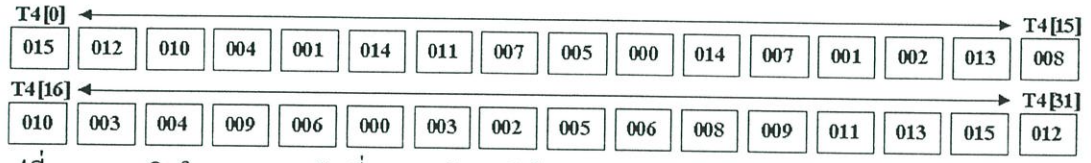
ในการขั้นตอนการบีบอัด (Compression) ข้อมูลจาก 32 ไบต์เหลือ 12 ไบต์นั้น ขั้นตอนแรกจะนำอินพุตไปใส่ไว้ในอาร์เรย์ X ที่มีสมาชิก 32 ตัวโดยสมาชิกแต่ละตัวมีขนาด 1 ไบต์ ข้อมูล 16 ไบต์ของ RAND จะถูกใส่ในอาร์เรย์ X ไบต์ที่ 16 ถึงไบต์สุดท้าย โดยไบต์แรกของ RAND ถูกใส่ลงไปที่ไบต์สุดท้ายของอาร์เรย์ X และไบต์สุดท้ายของ RAND ถูกใส่ลงไปที่ไบต์ที่ 16 ของอาร์เรย์ X ส่วนข้อมูล 16 ไบต์ของ Ki จะถูกใส่ในอาร์เรย์ X ไบต์ที่แรกถึงไบต์ที่ 15 โดยไบต์แรกของ Ki ถูกใส่ลงไปที่ไบต์แรกของอาร์เรย์ X และไบต์สุดท้ายของ Ki ถูกใส่ลงไปที่ไบต์ที่ 15 ของอาร์เรย์ X ดังแสดงในรูปที่ 3.8



รูปที่ 3.8 การโหลด Ki และ RAND ลงในอาร์เรย์ X ของอัลกอริทึม A38

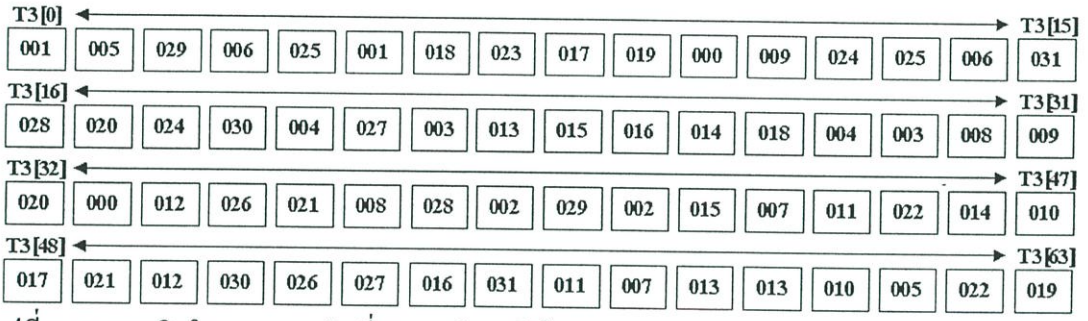
อัลกอริทึม A38 มีโครงสร้างในการบีบอัดข้อมูลแบบ Butterfly Compression ประกอบด้วยตาราง 5 ระดับคือ ตารางระดับ 4 ถึงตารางระดับ 0 โดยตารางแต่ละระดับจะมีสมาชิกทั้งหมด $2^{9-\text{Level}}$ ตัว โดยสมาชิกแต่ละตัวมีขนาด 1 ไบต์ ดังแสดงในรูปที่ 3.9, 3.10, 3.11, 3.12, และ 3.13 ตามลำดับ

ตารางระดับ 4



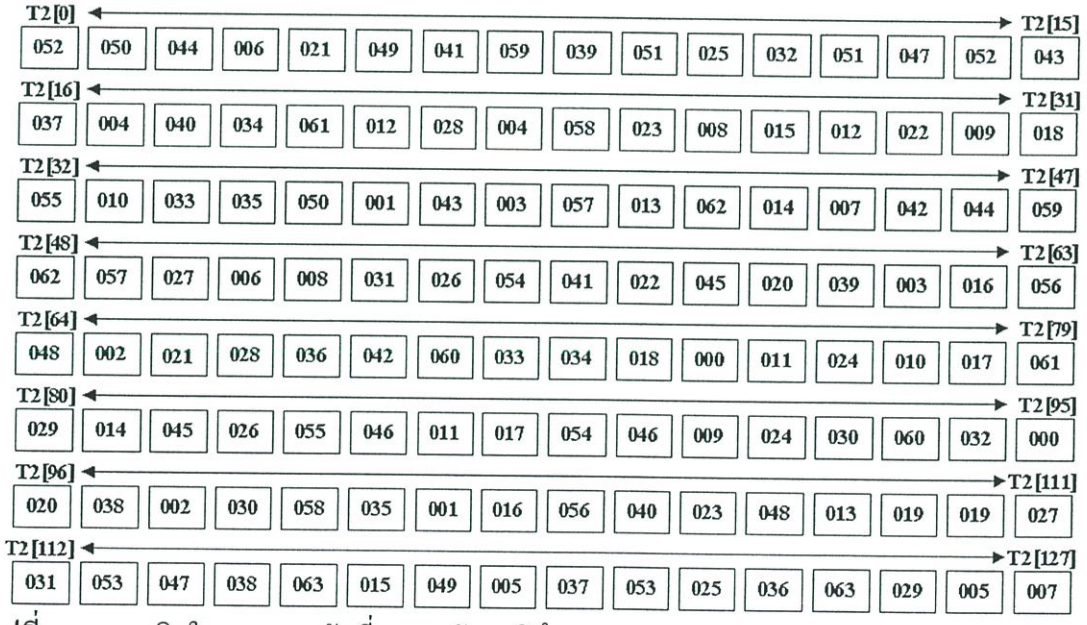
รูปที่ 3.9 สมาชิกในตารางระดับที่ 4 ของอัลกอริทึม A38

ตารางระดับ 3



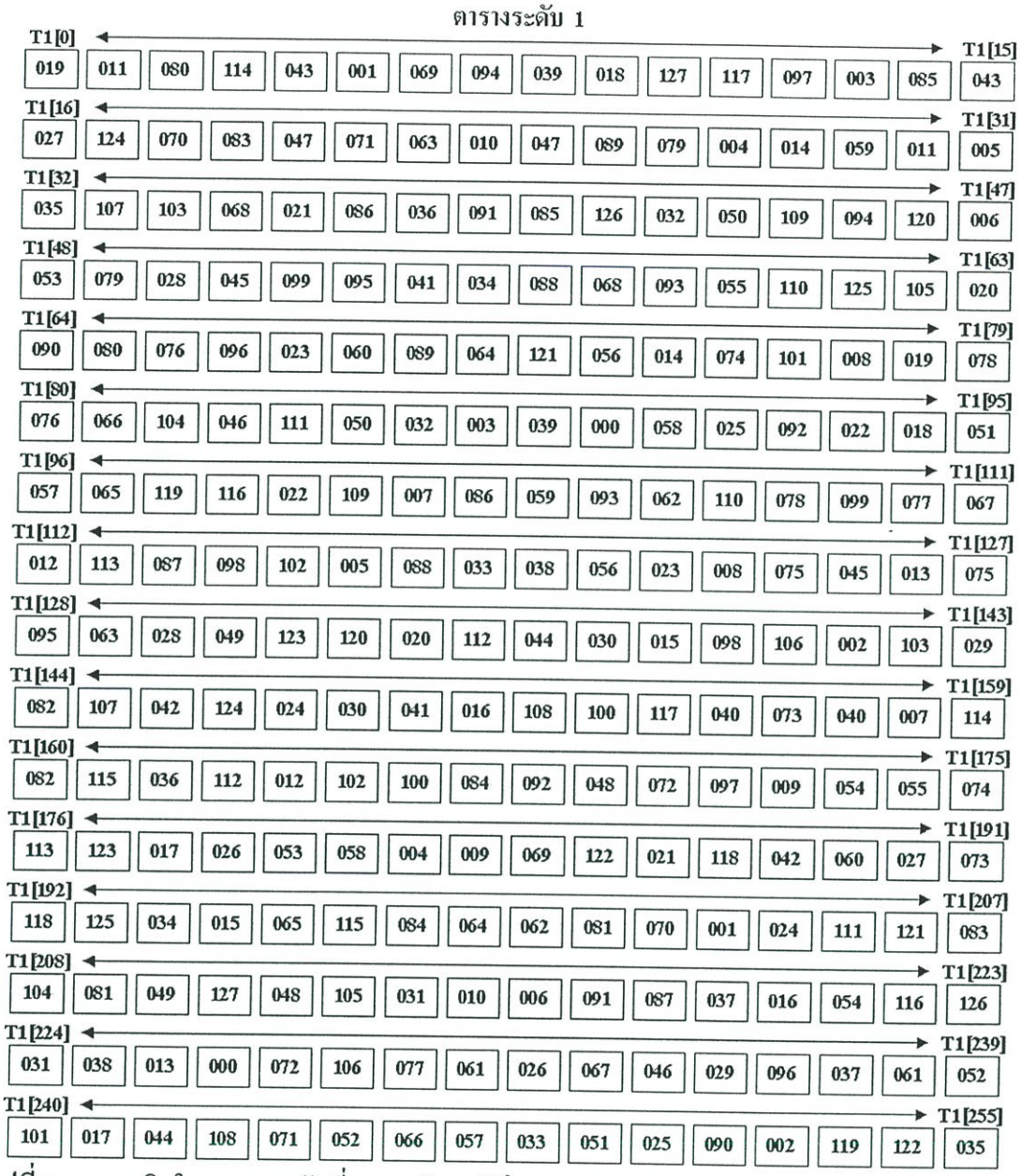
รูปที่ 3.10 สมาชิกในตารางระดับที่ 3 ของอัลกอริทึม A38

ตารางระดับ 2



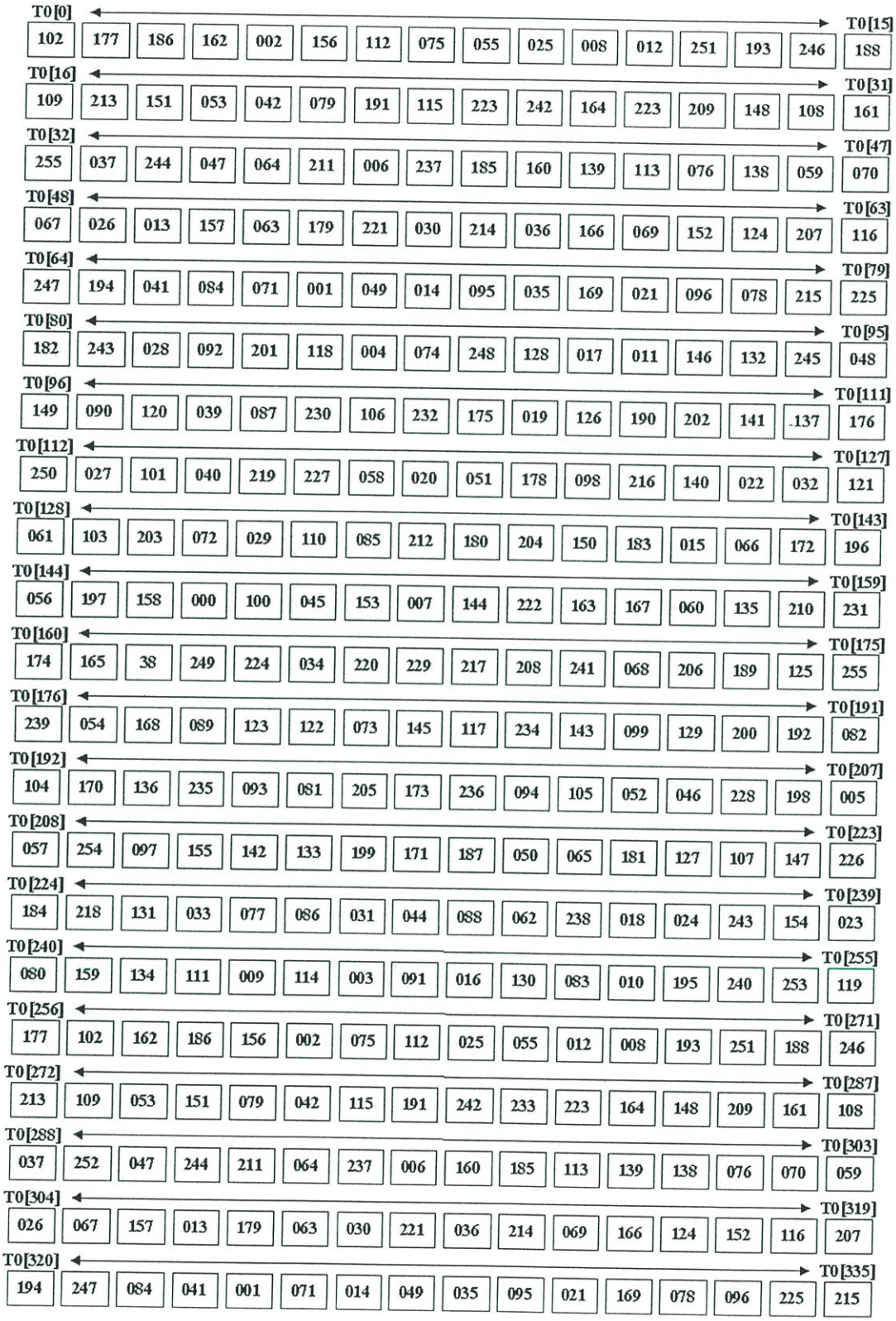
รูปที่ 3.11 สมาชิกในตารางระดับที่ 2 ของอัลกอริทึม A38

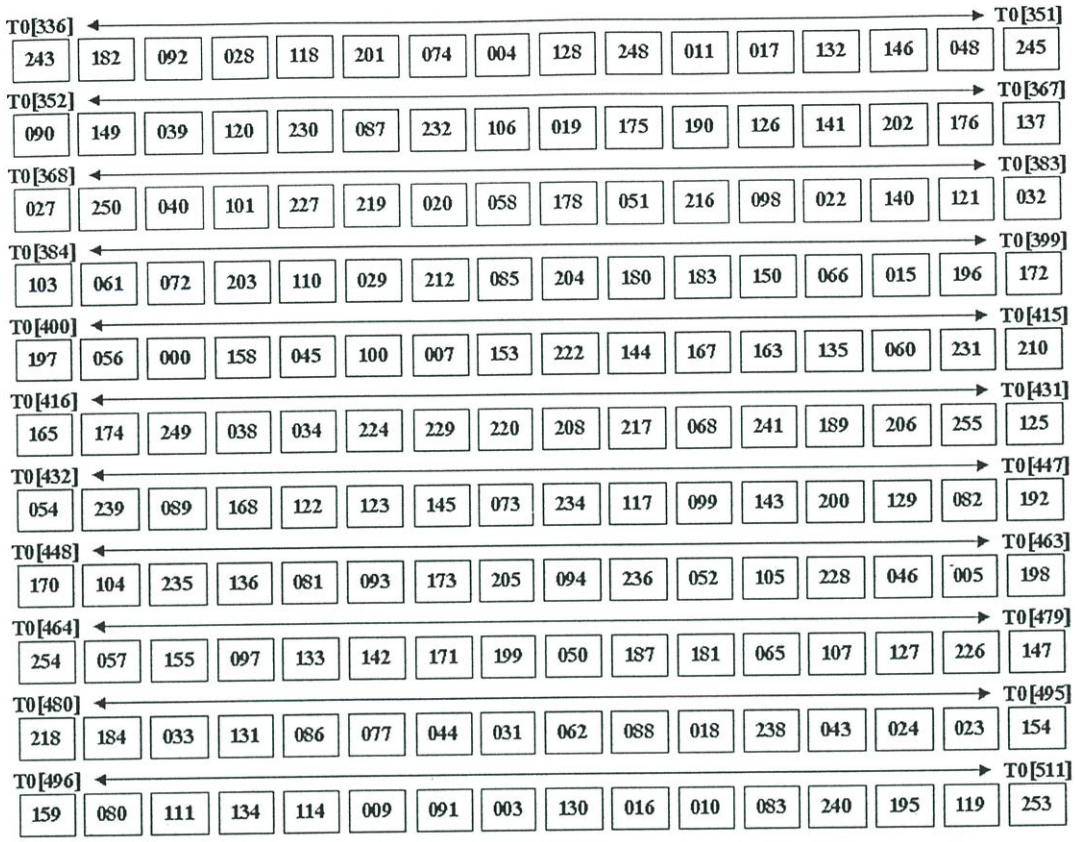
ตารางระดับ 1



รูปที่ 3.12 สมาชิกในตารางระดับที่ 1 ของอัลกอริทึม A38

ตารางระดับ 0


T0[0]
102 177 186 162 002 156 112 075 055 025 008 012 251 193 246 188
T0[15]
T0[16]
109 213 151 053 042 079 191 115 223 242 164 223 209 148 108 161
T0[31]
T0[32]
255 037 244 047 064 211 006 237 185 160 139 113 076 138 059 070
T0[47]
T0[48]
067 026 013 157 063 179 221 030 214 036 166 069 152 124 207 116
T0[63]
T0[64]
247 194 041 084 071 001 049 014 095 035 169 021 096 078 215 225
T0[79]
T0[80]
182 243 028 092 201 118 004 074 248 128 017 011 146 132 245 048
T0[95]
T0[96]
149 090 120 039 087 230 106 232 175 019 126 190 202 141 137 176
T0[111]
T0[112]
250 027 101 040 219 227 058 020 051 178 098 216 140 022 032 121
T0[127]
T0[128]
061 103 203 072 029 110 085 212 180 204 150 183 015 066 172 196
T0[143]
T0[144]
056 197 158 000 100 045 153 007 144 222 163 167 060 135 210 231
T0[159]
T0[160]
174 165 38 249 224 034 220 229 217 208 241 068 206 189 125 255
T0[175]
T0[176]
239 054 168 089 123 122 073 145 117 234 143 099 129 200 192 082
T0[191]
T0[192]
104 170 136 235 093 081 205 173 236 094 105 052 046 228 198 005
T0[207]
T0[208]
057 254 097 155 142 133 199 171 187 050 065 181 127 107 147 226
T0[223]
T0[224]
184 218 131 033 077 086 031 044 088 062 238 018 024 243 154 023
T0[239]
T0[240]
080 159 134 111 009 114 003 091 016 130 083 010 195 240 253 119
T0[255]
T0[256]
177 102 162 186 156 002 075 112 025 055 012 008 193 251 188 246
T0[271]
T0[272]
213 109 053 151 079 042 115 191 242 233 223 164 148 209 161 108
T0[287]
T0[288]
037 252 047 244 211 064 237 006 160 185 113 139 138 076 070 059
T0[303]
T0[304]
026 067 157 013 179 063 030 221 036 214 069 166 124 152 116 207
T0[319]
T0[320]
194 247 084 041 001 071 014 049 035 095 021 169 078 096 225 215
T0[335]

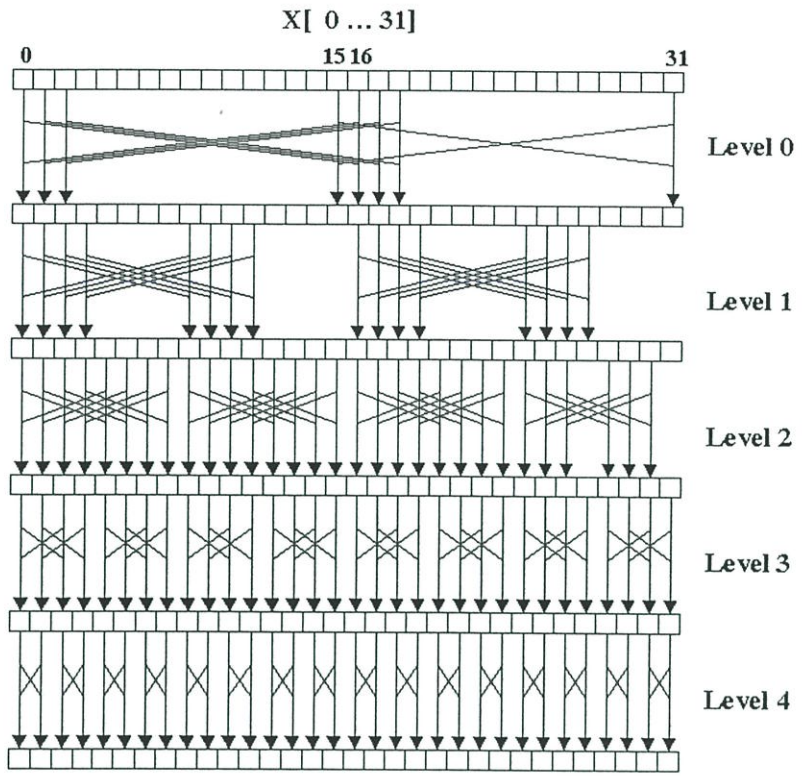


รูปที่ 3.13 สมาชิกในตารางระดับที่ 0 ของอัลกอริทึม A38

Ti[x] แทน สมาชิกของตารางระดับที่ i ที่มีดัชนี (Index) เท่ากับตัวแปร x สมาชิกในตารางจะนำไปแทนที่สมาชิกในอาร์เรย์ X โดยมีการจับคู่ กระบวนการผลิต RAND และ Kc มีอัลกอริทึมดังในรูปที่ 3.14

อัลกอริทึม A38 แบ่งการทำงานเป็น 5 ระดับตามตารางระดับ โดยแต่ละระดับมีการทำซ้ำๆ กัน (Iteration) ของอัลกอริทึม 16 รอบ การโหลด RAND ลงในอาร์เรย์ X นั้นจะทำเพียงครั้งแรกของการคำนวณเท่านั้น ส่วนการโหลด Ki นั้นจะทำทุกๆ รอบของการทำซ้ำในอัลกอริทึม A38

ค่าของสมาชิกในอาร์เรย์ X จะถูกจับคู่กันเพื่อคำนวณหาดัชนีของสมาชิกในตารางระดับแล้วนำค่าของสมาชิกในตารางระดับที่ค่าดัชนีเท่ากับที่คำนวณได้มาแทนลงในอาร์เรย์ X ทำซ้ำไปจนครบ 5 ระดับดังแสดงในรูปที่ 3.14



รูปที่ 3.14 Butterfly Compression

```
for j = 0 to 4 do
{
  for k = 0 to 2^j − 1 do
  {
    for l = 0 to 2^(4−j) − 1 do
    {
      m = 1 + k × 2^(5−j)
      n = (m + 2^(4−j))
      y = (X[m] + 2 × X[n]) mod 2^(9−j))
      z = (2 × X[m] + X[n]) mod 2^(9−j))
      X[m] = T_j[y]
      X[n] = T_j[z]
    }
  }
}
```

รูปที่ 3.15 อัลกอริทึมในการคำนวณค่าของอาร์เรย์ X ของอัลกอริทึม A38

เมื่อได้อาร์เรย์ X ที่ผ่านการทำการบีบอัดแบบ Butterfly แล้วนำอาร์เรย์ X มาคำนวณหา SRES และ Kc โดยใช้อัลกอริทึมดังแสดงในรูปที่ 3.15

```
for i=0 to 3 do
        {
         RAND[i] = (X[2×i] << 4) OR X[(2×i)+1)];
        }
for i=0 to 5 do
{
    Kc[i] = (X[(2×i)+18]<<6) OR (X[(2×i)+19]<<2) OR (X[(2×i)+20]>>2);
{
Kc[6] = (X[30]<<6) OR (X[31]<<2);
Kc[7] = 0;
```

รูปที่ 3.16 การคำนวณหาค่าของ SRES และ Kc ของอัลกอริทึม A38

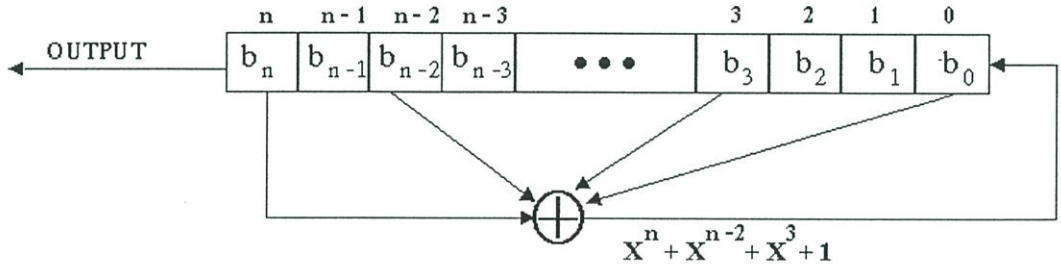
X[i] << x แทนการ Shift สมาชิกในอาร์เรย์ X ที่มีดัชนีเท่ากับตัวแปร i ไปทางซ้าย x บิต และ X[i] >> x แทนการ Shift สมาชิกในอาร์เรย์ X ที่มีดัชนีเท่ากับตัวแปร i ไปทางขวา x บิต สมาชิกในอาร์เรย์ X ที่มีดัชนีตั้งแต่ 0 ถึง 7 จะถูกใช้ในการผลิต SRES รอบละ 1 ไบต์ทั้งหมด 4 รอบ โดยในแต่ละรอบสมาชิกในอาร์เรย์ X จะถูกนำมาคำนวณเป็นคู่ๆ โดยใช้โอเปอร์เรชั่น OR และ Left Shift ส่วนสมาชิกในอาร์เรย์ X ที่มีดัชนีตั้งแต่ 18 ถึง 31 จะถูกใช้ในการผลิต Kc รอบละ 1 ไบต์ทั้งหมด 6 รอบ โดยในแต่ละรอบสมาชิกในอาร์เรย์ X จะถูกนำมาคำนวณเป็นคู่ๆ โดยใช้โอเปอร์เรชั่น OR, Right และ Left Shift ส่วนใน Kc ไบต์ที่ 7 นั้นได้จากการคำนวณสมาชิกในอาร์เรย์ X ที่มีดัชนีเป็น 30 และ 31 โดยใช้โอเปอร์เรชั่น OR และ Left Shift ส่วน Kc ไบต์สุดท้ายถูกเซ็ตให้เป็น 0 เสมอ ดังแสดงในอัลกอริทึมของรูปที่ 3.16

3.2.2 อัลกอริทึม A5

อัลกอริทึม A5 เป็นอัลกอริทึมในการเข้าและรหัสลับแบบ Secret Key โดยมีลักษณะเป็น Stream Cipher ในการเข้าและถอดรหัสลับจะผลิตคีย์ต่อเนื่อง (Key Stream) แล้วนำไป XOR กับ Plaintext ของผู้ใช้เพื่อทำการผลิต Ciphertext โดยการผลิตคีย์ต่อเนื่องนั้นจะผลิตคีย์เป็นรอบๆละ 228 บิต [16-18]

3.2.2.1 Linear Feedback Shift Register (LFSR)

LFSR เป็นการสร้างคีย์ต่อเนื่องแบบหนึ่งประกอบด้วย Shift Register และลำดับของการป้อนกลับ (Feedback Sequence) โดย Shift Register บิตซ้ายสุดของ Register จะเป็นเอาท์พุตของ LFSR ซึ่งแต่ละรอบของการผลิตเอาท์พุต Register จะเลื่อนไปทางซ้าย 1 บิต นำบิตตามลำดับของการป้อนกลับมา XOR กันเพื่อแทนบิตขวาสุดที่ถูกเลื่อนไป ลำดับของการป้อนกลับสามารถเขียนอยู่ในรูปแบบเลขยกกำลัง (Polynomial) โดย x ยกกำลัง n แทน บิตที่ n จะถูกป้อนกลับ เครื่องหมายบวกแทนการ XOR ของบิตที่ถูกป้อนกลับกลับมาที่บิตแรกดังแสดงในรูปที่ 3.17



รูปที่ 3.17 LFSR ที่เขียนอยู่ในรูปแบบเลขยกกำลังได้ $X^n + X^{n-2} + X^3 + 1$

LFSR ขนาด n+1 บิตจะสามารถสร้างลำดับของบิต (Bit Sequence) โดยมีรูปแบบของบิต (Bit Pattern) ไม่ซ้ำกับรูปแบบเดิมจำนวน 2^n รูปแบบ [19]

จากตัวอย่างในรูปที่ 3.17 จะเห็นได้ว่า LFSR จะทำการป้อนกลับบิตที่ n, n-2, 3, และ 0 โดยจะนำมา XOR กันก่อนที่จะป้อนกลับยังบิตแรกแล้ว Register จะถูกเลื่อนไปทางซ้าย 1 บิตโดยบิตสุดท้ายของ Register จะเป็นเอาท์พุตของ LFSR

3.4.2.2 Threshold Generator

อัลกอริทึม A5 มี Threshold Generator ทำหน้าที่ในคำนวณหาคีย์ที่ต่อเนื่อง (Key Stream) เพื่อนำไป XOR กับ Plaintext ก็จะได้ Ciphertext ภายใน Threshold Generator ประกอบด้วย LFSR 3 ตัว R1, R2, และ R3 โดยมีขนาด 19 บิต, 22 บิต, และ 23 บิตตามลำดับ C1, C2, และ C3 บิตตรงกลางของ LFSR ทุกตัวเรียกว่า "Majority Bit" ดังแสดงในรูปที่ 3.18 Majority Control ทำหน้าที่ควบคุมการป้อนกลับ (Feedback) ของ LFSR ทั้ง 3 ตัวในแต่ละรอบของการคำนวณ Threshold วิธีควบคุมการป้อนกลับว่า LFSR แต่ละตัวจะทำการป้อนกลับ (Move) หรือหยุดการป้อนกลับ (Stop) ทำได้โดยการคำนวณ Majority bit ของ LFSR ทั้ง 3 ตัว

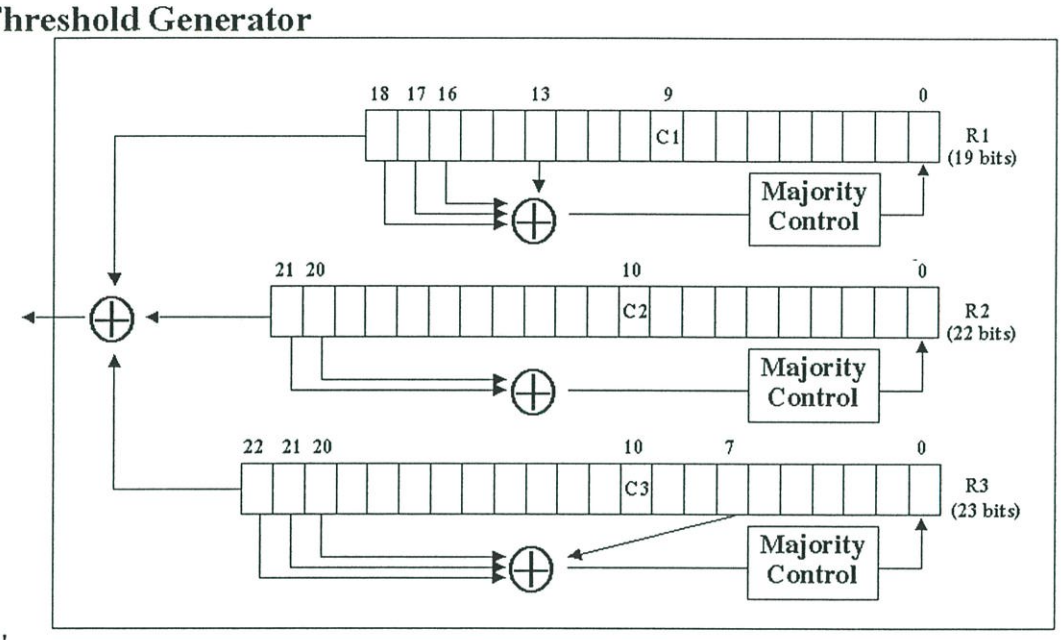
ถ้า $C1 = C2 \neq C3$ แล้ว R1, R2 ป้อนกลับ แต่ R3 หยุดป้อนกลับ

ถ้า $C1 = C3 \neq C2$ แล้ว R1, R3 ป้อนกลับ แต่ R1 หยุดป้อนกลับ

ถ้า C2 = C3 ≠ C1 แล้ว R2, R3 ป้อนกลับ แต่ R1 หยุดป้อนกลับ

ถ้า C1 = C2 = C3 แล้ว R1, R2, และ R3 ป้อนกลับ

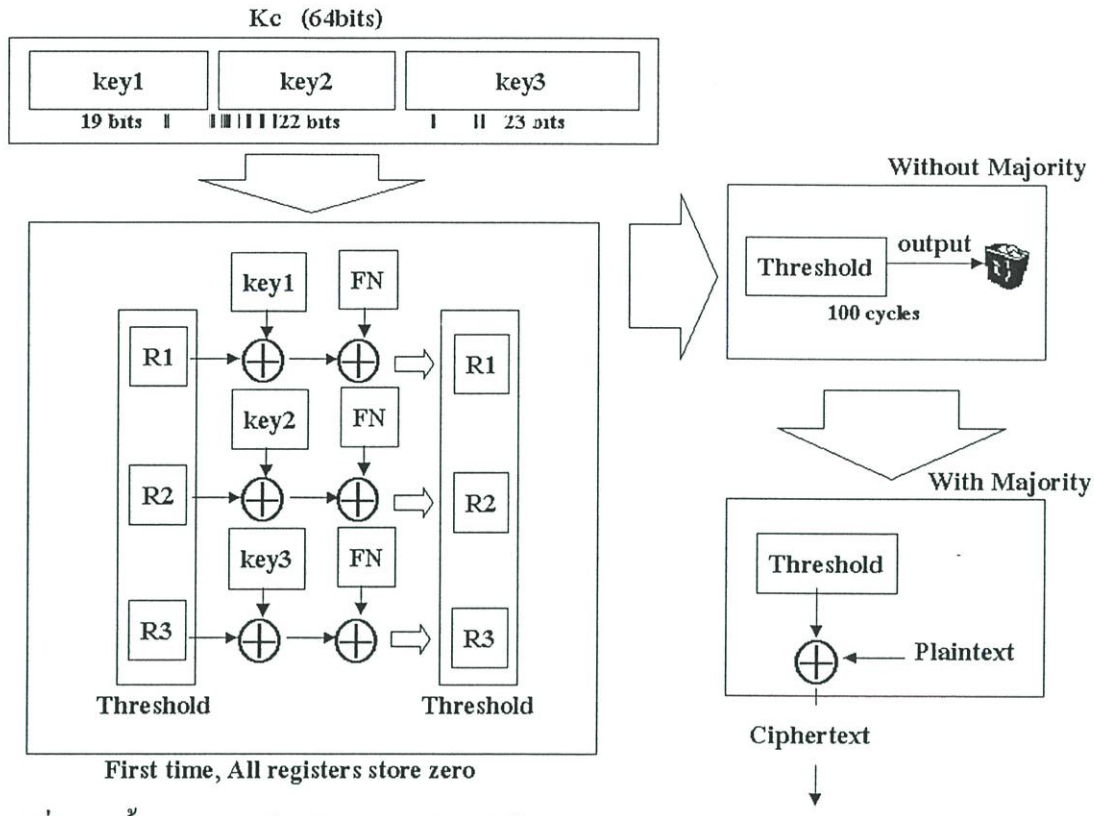
การควบคุมการป้อนกลับของ LFSR ทุกตัวมีความน่าจะเป็นที่จะป้อนกลับข้อมูลเป็น 0.75



รูปที่ 3.18 Threshold Generator

3.4.2.3 ขั้นตอนการเข้ารหัสลับ

ขั้นตอนการเข้ารหัสลับของอัลกอริทึม A5 ดังแสดงในรูปที่ 3.19 ในตอนเริ่มการเข้ารหัสลับจะนำ Kc ขนาด 64 บิตที่ได้รับมาจากอัลกอริทึม A8 มาแบ่งตามขนาดของ R1, R2, และ R3 คือ 19 บิต, 22 บิต, และ 23 บิตตามลำดับ เมื่อเริ่มทำการสร้างคีย์ต่อเนื่อง ทุกๆ บิตของ Register ทุกตัวใน Threshold จะถูกเซตให้เป็น 0 นำ Register ทุกตัวไปจับคู่ XOR กับ Kc ที่ถูกแบ่งเอาไว้ตามขนาดของ Register ทำการรัน Threshold 100 รอบซึ่งในแต่ละรอบจะไม่มีการควบคุมการป้อนกลับของ Register ดังนั้น Register ทุกตัวจะทำการป้อนกลับตลอดใน 100 รอบนี้ หลังทำการผลิตคีย์ต่อเนื่องจำนวน 228 บิตแล้วนำไป XOR กับ Plaintext ของผู้ใช้เพื่อทำการผลิต Ciphertext



รูปที่ 3.19 ขั้นตอนการเข้ารหัสลับของอัลกอริทึม A5

ก่อนที่จะทำการผลิตคีย์ต่อเนื่อง 228 ถัดไปจะต้องทำการรัน Threshold 100 รอบซึ่งในแต่ละรอบจะไม่มีการควบคุมการป้อนกลับของ Register แล้วจึงจะนำ Threshold ไปทำการผลิตคีย์ต่อเนื่องจำนวน 228 บิตถัดไป

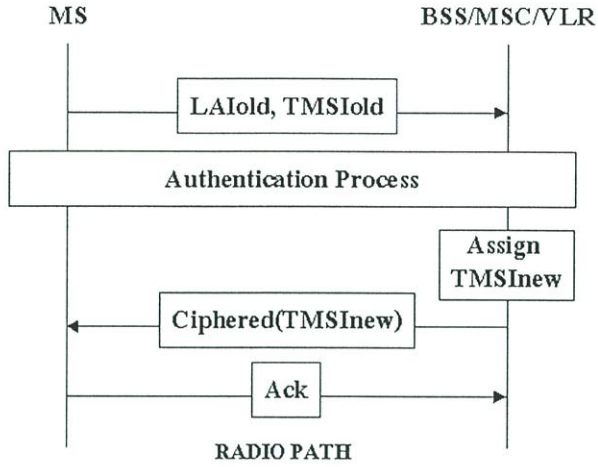
3.3 บริการรักษาความปลอดภัยของเครือข่าย GSM

ปัญหาสำคัญของการสื่อสารเคลื่อนที่ (Mobile Communication) อย่างหนึ่งคือ ความจำเป็นที่จะต้องสื่อสารข้อมูลผ่านช่องสัญญาณวิทยุซึ่งเป็นสื่อกลางแบบเปิด (Open Medium) เครือข่าย GSM จัดเตรียมบริการต่างๆในการรักษาความปลอดภัยให้กับผู้ใช้ ทำให้ผู้ใช้บริการของเครือข่ายสามารถที่จะมั่นใจได้ว่าทรัพยากรของเครือข่ายหรือข้อมูลของผู้ใช้จะไม่ถูกลักลอบไปใช้อย่างไม่ถูกต้อง บริการในการรักษาความปลอดภัยต่างๆ แบ่งออกเป็น 4 บริการดังนี้ [8]

3.3.1 บริการป้องกันหมายเลขประจำตัวผู้ใช้ (Anonymity Service)

บริการป้องกันหมายเลขประจำตัวผู้ใช้ (Anonymity Service) เป็นบริการที่เครือข่ายจัดเตรียมการป้องกัน IMSI ซึ่งเป็นหมายเลขประจำตัวของผู้ใช้ เครือข่าย GSM จัดเตรียมให้มีการกำหนดหมายเลขประจำตัวชั่วคราว TMSI ให้กับผู้ใช้เมื่อผู้ใช้กำลังอยู่ในพื้นที่ในการจัดการของ MSC เมื่อผู้ใช้ต้องการสื่อสารกับเครือข่ายก็จะใช้ TMSI ที่ได้รับแทน IMSI ทำให้ผู้ใช้ไม่ต้องส่ง

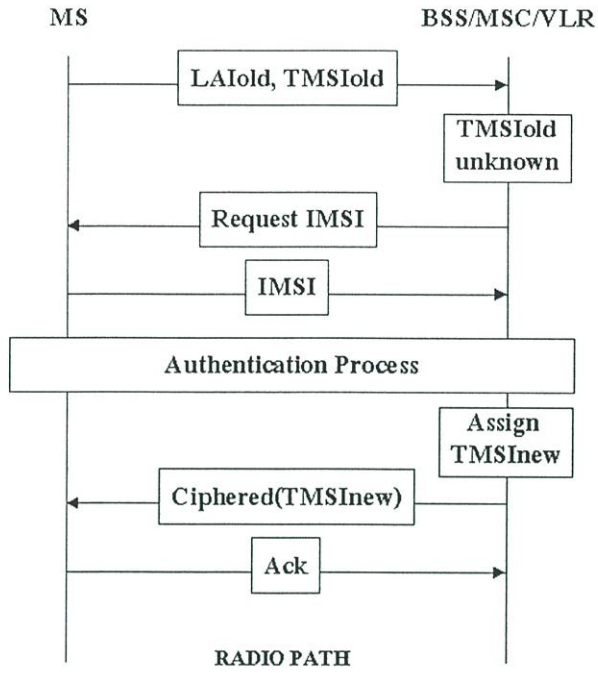
IMSI ผ่านช่องสัญญาณวิทยุ (Radio Channel) ซึ่งเป็นสื่อกลางในการสื่อสาร (Transmission Medium) ที่ง่ายที่จะถูกผู้ไม่ประสงค์ดีลับลอบนำหมายเลขประจำตัวของผู้ใช้ไปใช้ประโยชน์อย่างไม่ถูกต้อง ดังแสดงในรูปที่ 3.20



รูปที่ 3.20 การป้องกันหมายเลขประจำตัวผู้ใช้ของเครือข่าย GSM

ในการปรับปรุงตำแหน่งที่อยู่ (Location Updating) ของผู้ใช้ MS จะส่ง TMSI อันเดิมและ LAI ปัจจุบันของผู้ใช้ให้กับเครือข่าย เครือข่ายจะทำการปรับปรุงตำแหน่งที่อยู่ของผู้ใช้และเริ่มกระบวนการตรวจสอบผู้ใช้ (Authentication Process) เพื่อทำให้แน่ใจว่าเป็นผู้ใช้ที่ถูกต้อง หลังจากนั้นเครือข่ายจะทำการผลิต TMSI ใหม่ให้กับผู้ใช้ โดยการส่ง TMSI ใหม่นี้ให้กับผู้ใช้จะต้องทำการเข้ารหัสลับ TMSI ก่อนที่จะส่งให้กับผู้ใช้ [9]

ในกรณีที่ VLR เกิดไม่ทราบ TMSI หรือเกิดการสูญหายของ TMSI เครือข่ายจะร้องขอ IMSI ของผู้ใช้ก่อนที่จะทำการกำหนด TMSI ใหม่ให้กับผู้ใช้ โดย IMSI ที่จะถูกส่งจะถูกส่งออกมาโดยไม่มีการเข้ารหัสลับดังแสดงในรูปที่ 3.21



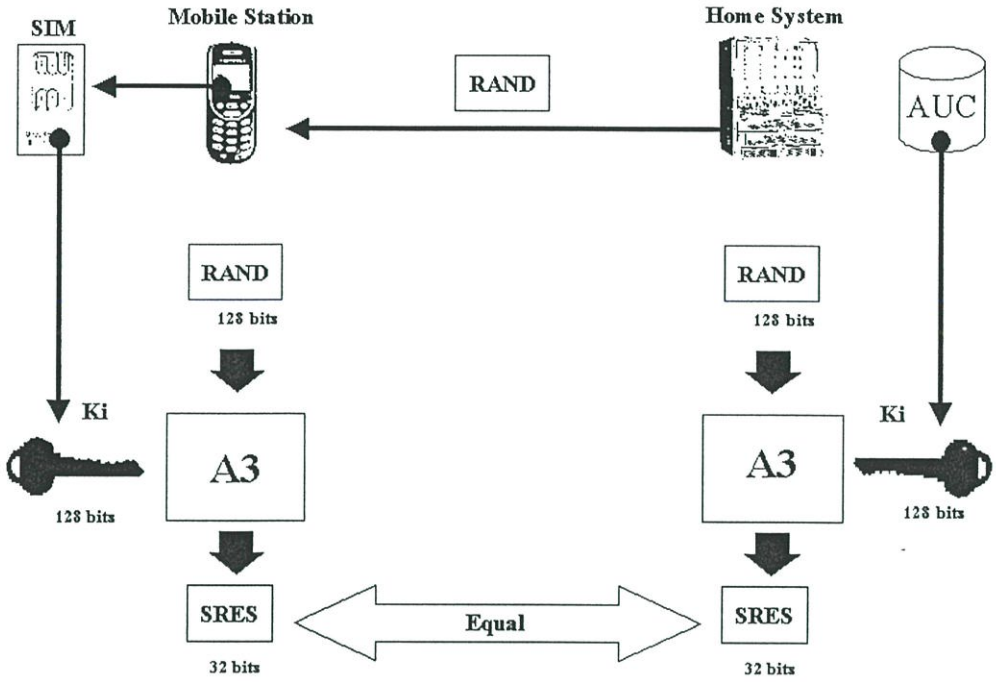
รูปที่ 3.21 การป้องกันหมายเลขประจำตัวผู้ใช้กรณีที่ VLR ไม่ทราบค่า TMSI ที่ได้รับ

3.3.2 บริการตรวจสอบผู้ใช้ (Authentication Service)

บริการตรวจสอบผู้ใช้ (Authentication Service) คือบริการที่ป้องกันไม่ให้ทรัพยากรของเครือข่ายถูกลักลอบโดยผู้ที่ไม่ได้รับการลงทะเบียนใช้งานกับเครือข่ายอย่างถูกต้อง (Unauthorized Party) โดยเครือข่าย GSM ใช้วิธีการในการตรวจสอบผู้ใช้แบบ Challenge-Response โดยเครือข่ายจะส่ง Challenge ของเครือข่ายให้กับผู้ใช้ ผู้ใช้จะนำ Challenge คำนวณหา Response ของผู้ใช้แล้วส่งกลับไปให้เครือข่าย เครือข่ายจะตรวจสอบความถูกต้องของ Response ของผู้ใช้ที่ได้รับเพื่ออนุมัติให้ผู้ใช้สามารถใช้บริการกับเครือข่ายได้ [10]

รูปที่ 3.22 แสดงขั้นตอนการตรวจสอบผู้ใช้ของเครือข่าย GSM โดยทางฝั่งของเครือข่ายจะส่ง RAND (Random Number) ขนาด 128 บิตเป็น Challenge ของเครือข่าย ผู้ใช้และเครือข่ายจะทำการคำนวณ RAND กับอัลกอริทึม A3 โดยใช้ Ki (Authentication Key) ขนาด 128 บิตเพื่อหา SRES (Signature Response) ขนาด 32 บิตเพื่อใช้เป็น Response ของผู้ใช้ในการตรวจสอบผู้ใช้

Ki เป็นคีย์ในการคำนวณหา SRES โดย Ki จะถูกเก็บไว้ทั้งใน SIM ของผู้ใช้และฐานข้อมูล AuC ของเครือข่ายในตอนที่ผู้ใช้ลงทะเบียนใช้งานกับเครือข่าย ทำให้ผู้ใช้และเครือข่ายมีคีย์ที่ตรงกันในการคำนวณหา SRES



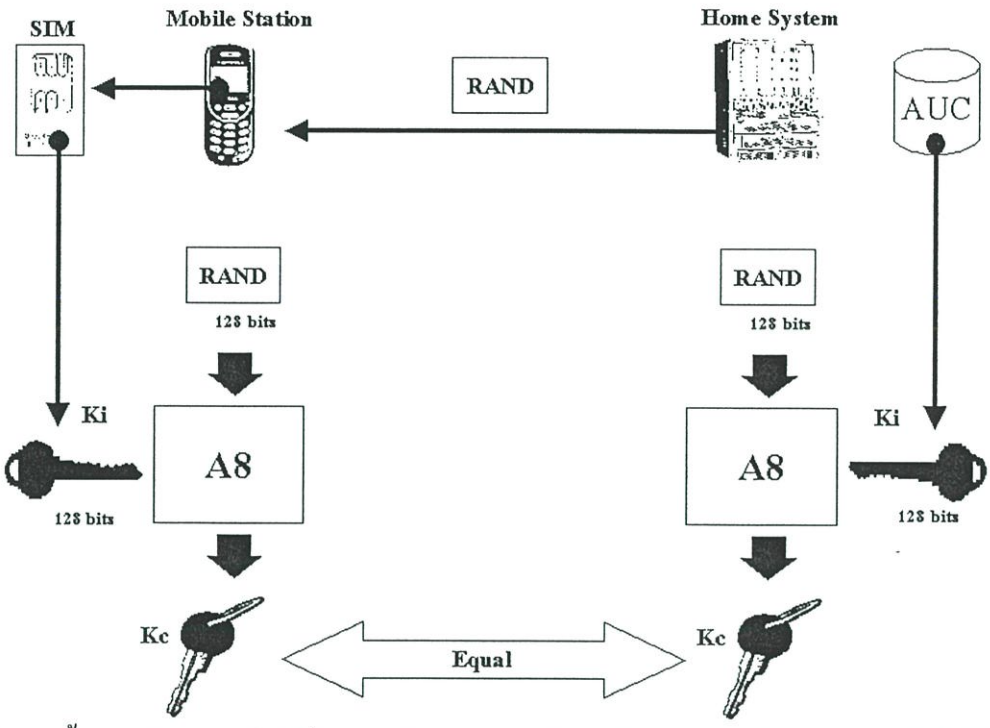
รูปที่ 3.22 ขั้นตอนการตรวจสอบผู้ใช้ของเครือข่าย GSM

3.3.3 บริการจัดส่งคีย์ในการเข้ารหัสลับ (Key Distribution)

สำหรับการเข้ารหัสลับข้อมูลที่ใช้คีย์เหมือนกันในการเข้าและถอดรหัสลับข้อมูล (Secret Key Encryption) นั้นการทำให้ผู้ส่งและผู้รับใช้ คีย์ที่ตรงกันในการเข้าและถอดรหัสลับข้อมูลเป็นหัวใจสำคัญในการรักษาความปลอดภัย นำไปสู่บริการในการรักษาความปลอดภัยอีกบริการหนึ่งของเครือข่าย GSM คือบริการจัดส่งคีย์ในการเข้ารหัสลับ (Key Distribution) [11]

เครือข่าย GSM ใช้ประโยชน์จากการตรวจสอบผู้ใช้ (Authentication) ทุกครั้งที่มีการตรวจสอบผู้ใช้ เครือข่ายและผู้ใช้จะทำการสร้างคีย์ที่จะใช้ในการเข้าและถอดรหัสลับร่วมกันระหว่างผู้ใช้กับเครือข่าย (Session Secret Key)

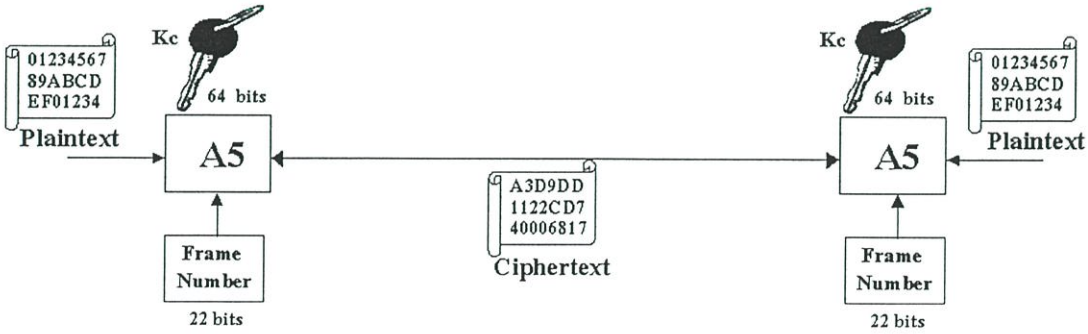
รูปที่ 3.23 แสดงขั้นตอนในการสร้างคีย์ที่จะใช้ในการเข้าและถอดรหัสลับร่วมกันของเครือข่าย GSM กับผู้ใช้ RAND ขนาด 128 บิตและ Ki ขนาด 128 บิตถูกใช้เป็นอินพุตเหมือนการตรวจสอบผู้ใช้ ใช้อัลกอริทึม A8 ในการสร้างคีย์ที่จะใช้ในการเข้าและถอดรหัสลับ หลังจากทำการคำนวณอัลกอริทึม A8 เสร็จเรียบร้อยแล้วจะได้ Kc ขนาด 64 บิตใช้เป็นคีย์ในการเข้าและถอดรหัสลับข้อมูลระหว่างผู้ใช้กับเครือข่าย



รูปที่ 3.23 ขั้นตอนในการสร้างคีย์ในการเข้าและถอดรหัสลับข้อมูลของเครือข่าย GSM กับผู้ใช้

3.3.4 บริการรักษาความลับของผู้ใช้ (Confidentiality Service)

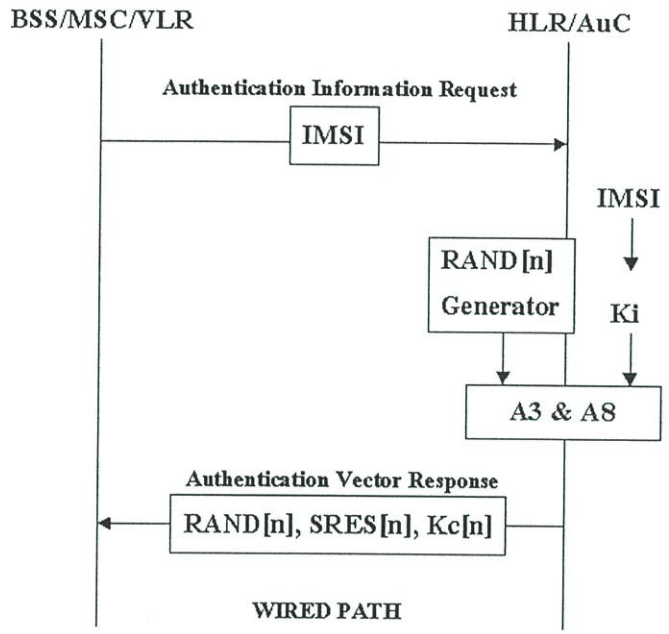
เครือข่าย GSM ได้จัดเตรียมบริการในการรักษาความลับของผู้ใช้ (Confidentiality Service) โดยจัดเตรียมให้ผู้ส่งจะใช้อัลกอริทึม A5 เข้ารหัสลับข้อมูลดั้งเดิมที่ต้องการส่ง (Plaintext) ก่อนที่จะส่งผ่านช่องสัญญาณวิทยุในรูปของข้อมูลที่เข้ารหัสลับเรียบร้อยแล้ว (Ciphertext) โดยใช้ Kc (Cipher Key) ขนาด 64 บิตเป็นคีย์ในการเข้าและถอดรหัสลับ นอกจากนี้ในการเข้าและถอดรหัสลับจะต้องทำการคำนวณหมายเลขของเฟรมข้อมูล Fn (Frame Number) ขนาด 22 บิตด้วยดังแสดงใน รูปที่ 3.24



รูปที่ 3.24 การเข้าและถอดรหัสลับข้อมูลของเครือข่าย GSM

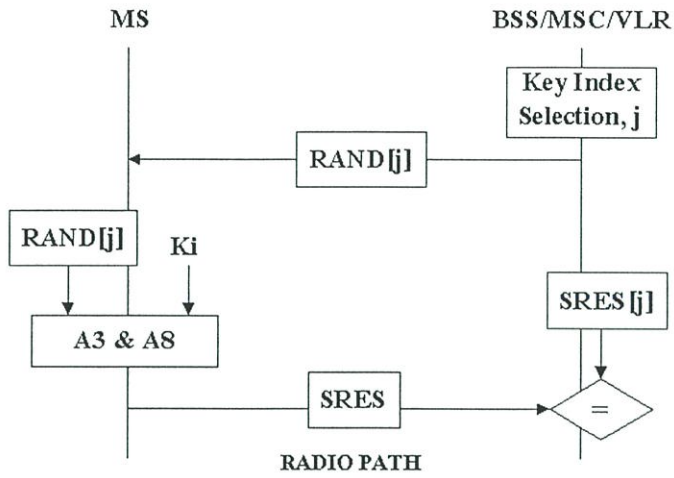
3.3.5 การผลิตข้อมูลในการรักษาความปลอดภัย (Security Data Generating)

ทางฝั่งเครือข่ายจะไม่ทำการผลิตข้อมูลในการรักษาความปลอดภัย 3 ตัวคือ RAND, SRES, และ Kc ทุกครั้งที่มีการตรวจสอบผู้ใช้ AuC จะทำการผลิตข้อมูลทั้ง 3 ตัวนั้นตัวละ n ชุด ดังแสดงในรูปที่ 3.25



รูปที่ 3.25 การผลิตข้อมูลในการรักษาความปลอดภัย

MSC จะส่ง IMSI เป็นการร้องขอข้อมูลในการตรวจสอบผู้ใช้จาก AuC ทางฝั่ง AuC จะนำ IMSI ไปค้นหา Ki ของผู้ใช้แล้วทำการผลิต RAND ทั้งหมด n ตัว แล้วคำนวณหา SRES และ Kc จำนวน n ตัวเช่นกัน แล้วส่งชุดข้อมูล 3 ตัวนี้ให้กับ MSC เมื่อ MSC ได้ชุดข้อมูล 3 ตัวนี้จะทำการบันทึกข้อมูลลงในฐานข้อมูล VLR เมื่อเครือข่ายต้องการทำการตรวจสอบผู้ใช้ จะส่งเลือก RAND เพียง 1 ตัวใน RAND[n] นั้นไปทำการตรวจสอบผู้ใช้ดังแสดงในรูปที่ 3.26



รูปที่ 3.26 การตรวจสอบผู้ใช้จากชุดข้อมูล RAND[n]

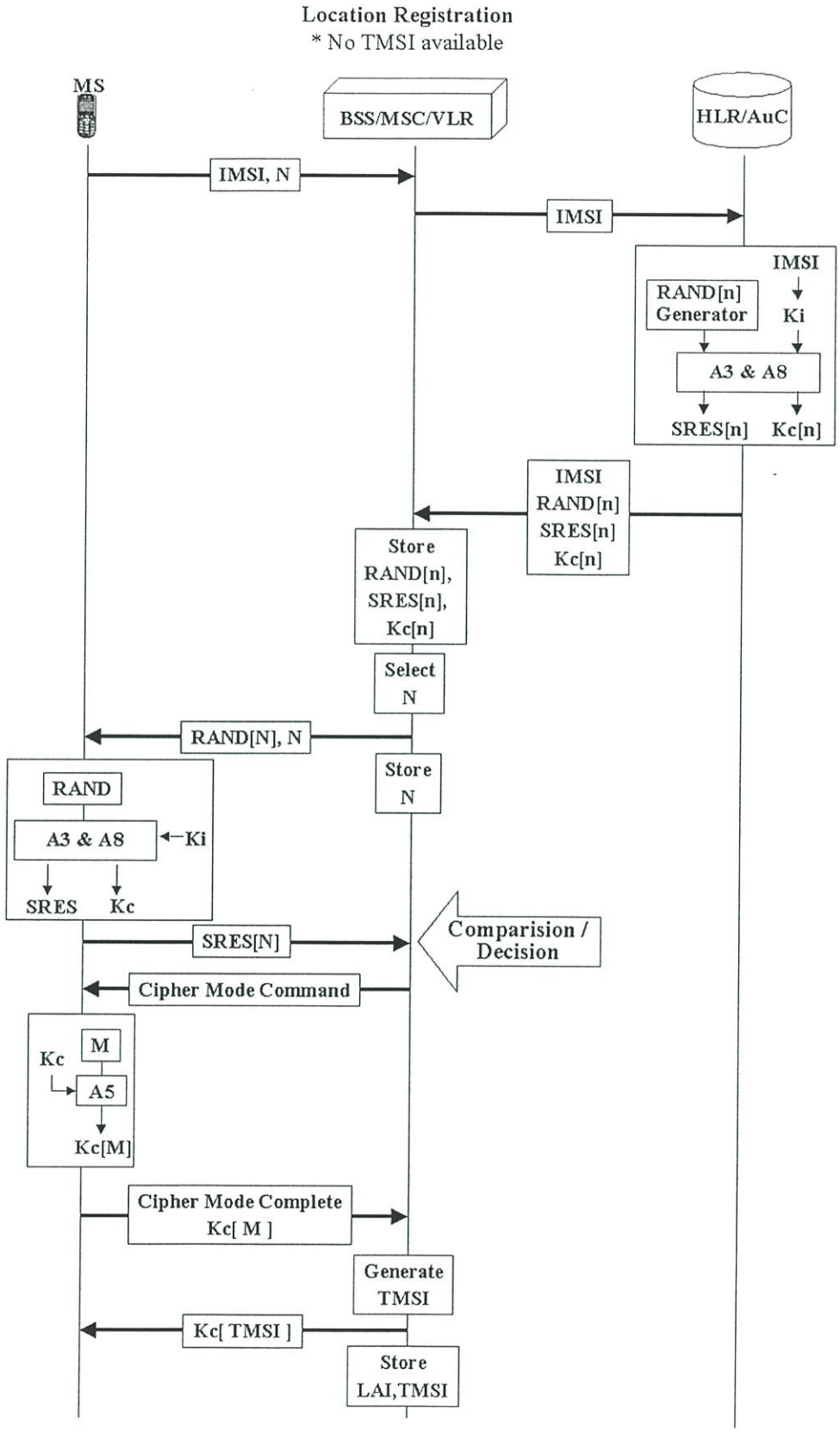
3.4 โพรโตคอลการสื่อสารของเครือข่าย GSM

โพรโตคอลการสื่อสารในเครือข่าย GSM จัดเตรียมให้ผู้ใช้ถูกเครือข่ายตรวจสอบผู้ใช้เพื่อป้องกันการถูกผู้ไม่ประสงค์ดีลับลอบเข้ามาใช้ทรัพยากรของเครือข่ายได้ รูปแบบของโพรโตคอลที่มีการตรวจสอบผู้ใช้นั้นประกอบด้วย การลงทะเบียนตำแหน่งที่อยู่ (Location Registration), การปรับปรุงตำแหน่งที่อยู่ (Location Updating), การสร้างโทรศัพท์เข้าออก (Call Setup) [12]

3.4.1 โพรโตคอลการลงทะเบียนตำแหน่งที่อยู่ (Location Registration Protocol)

สำหรับการสื่อสารในเครือข่าย GSM ผู้ใช้แต่ละคนเมื่อเริ่มใช้งานโทรศัพท์เคลื่อนที่ จะต้องการลงทะเบียนตำแหน่งที่อยู่ (Location Registration) ปัจจุบันของตนกับ MSC ที่ผู้ใช้จะทำการลงทะเบียน โดยโพรโตคอลการลงทะเบียนตำแหน่งที่อยู่นั้นจะมีขั้นตอนดังแสดงในรูปที่ 3.27

ผู้ใช้จะส่ง IMSI และหมายเลขคีย์ (Key Number), N ให้กับ MSC โดยผ่าน BSS, MSC จะส่ง IMSI ให้กับ AuC โดยผ่าน HLR เมื่อ AuC ได้รับ IMSI ก็จะทำการผลิตอาร์เรย์ของ RAND ที่มีสมาชิกจำนวน n ตัว แล้วทำการคำนวณหาอาร์เรย์ของ SRES และ Kc จำนวน n ตัวเช่นกัน แล้วส่งชุดข้อมูล 4 ตัวคือ นำ IMSI, อาร์เรย์ของ RAND, SRES, และ Kc กลับไปให้ MSC โดยผ่าน HLR เมื่อ MSC ได้รับข้อมูลในการรักษาความปลอดภัยจะนำข้อมูลบันทึกลงในฐานข้อมูล VLR หลังจากนั้น MSC จะทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RAND ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RAND[N] และหมายเลขคีย์ที่เลือก N ให้กับผู้ใช้ ผู้ใช้จะทำการคำนวณหา SRES[N] แล้วส่งกลับให้ VLR เพื่อตรวจสอบ ถ้า SRES[N] ของผู้ใช้ ตรงกันกับ SRES[N] ที่เก็บอยู่ในฐานข้อมูล การตรวจสอบผู้ใช้ก็เป็นอันเสร็จสมบูรณ์



รูปที่ 3.27 โพรโตคอลการทำ Location Registration ของเครือข่าย GSM

MSC จะทำการผลิต TMSI แล้วส่งคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Command) ให้กับผู้ใช้เป็นการแจ้งให้ผู้ใช้ทราบว่าการส่งข้อมูลหลังจากนี้จะเป็นข้อมูลที่ถูกเข้ารหัสลับ MS จะเข้ารหัสลับข้อมูล M ด้วยอัลกอริทึม A5 เพื่อเป็นการตอบรับคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Complete) เมื่อMSC ได้รับTMSI การตอบรับคำสั่งสภาวะการเข้ารหัสลับจากผู้ใช้จะนำ Kc[N] เข้ารหัสลับ TMSI ด้วยอัลกอริทึม A5 แล้วส่งให้กับผู้ใช้ ผู้ใช้จะใช้ TMSI ที่ได้รับเก็บไว้ใน SIM เพื่อใช้แทน IMSI ต่อไป ทางฝั่ง MSC จะเก็บ TMSI และ LAI ผู้ใช้ไว้ในฐานข้อมูล VLR ในการส่งสัญญาณควบคุมทั้งหมดของการลงทะเบียนตำแหน่งที่อยู่นี้จะใช้ช่องสัญญาณควบคุม SDCCH

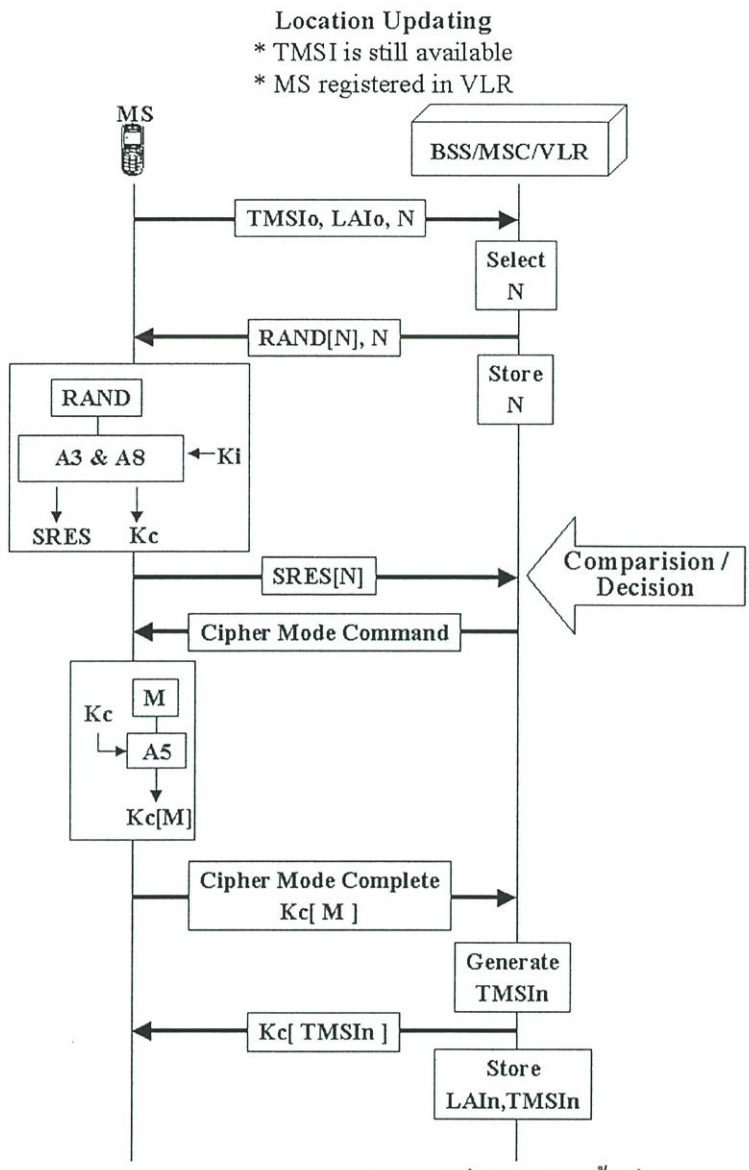
3.4.2 โพรโตคอลการปรับปรุงตำแหน่งที่อยู่ (Location Updating Protocol)

ผู้ใช้ในเครือข่าย GSM จะต้องทำการปรับปรุงตำแหน่งที่อยู่ของตนกับเครือข่ายอย่างสม่ำเสมอ เพื่อทำให้เครือข่ายทราบว่าผู้ใช้อยู่ในพื้นที่การจัดการตำแหน่งใดของ MSC โดยปกติแล้วการปรับปรุงตำแหน่งที่อยู่ของผู้ใช้จะเกิดขึ้นทุกๆ 5 วินาที [13] โพรโตคอลการปรับปรุงตำแหน่งที่อยู่ของผู้ใช้แบ่งเป็น 2 กรณีคือ กรณีที่ผู้ใช้อยู่ในพื้นการจัดการของ MSC เดิม กับกรณีที่ผู้ใช้อยู่ในพื้นการจัดการของ MSC ใหม่ ดังแสดงในรูปที่ 3.28 และรูปที่ 3.29 ตามลำดับ

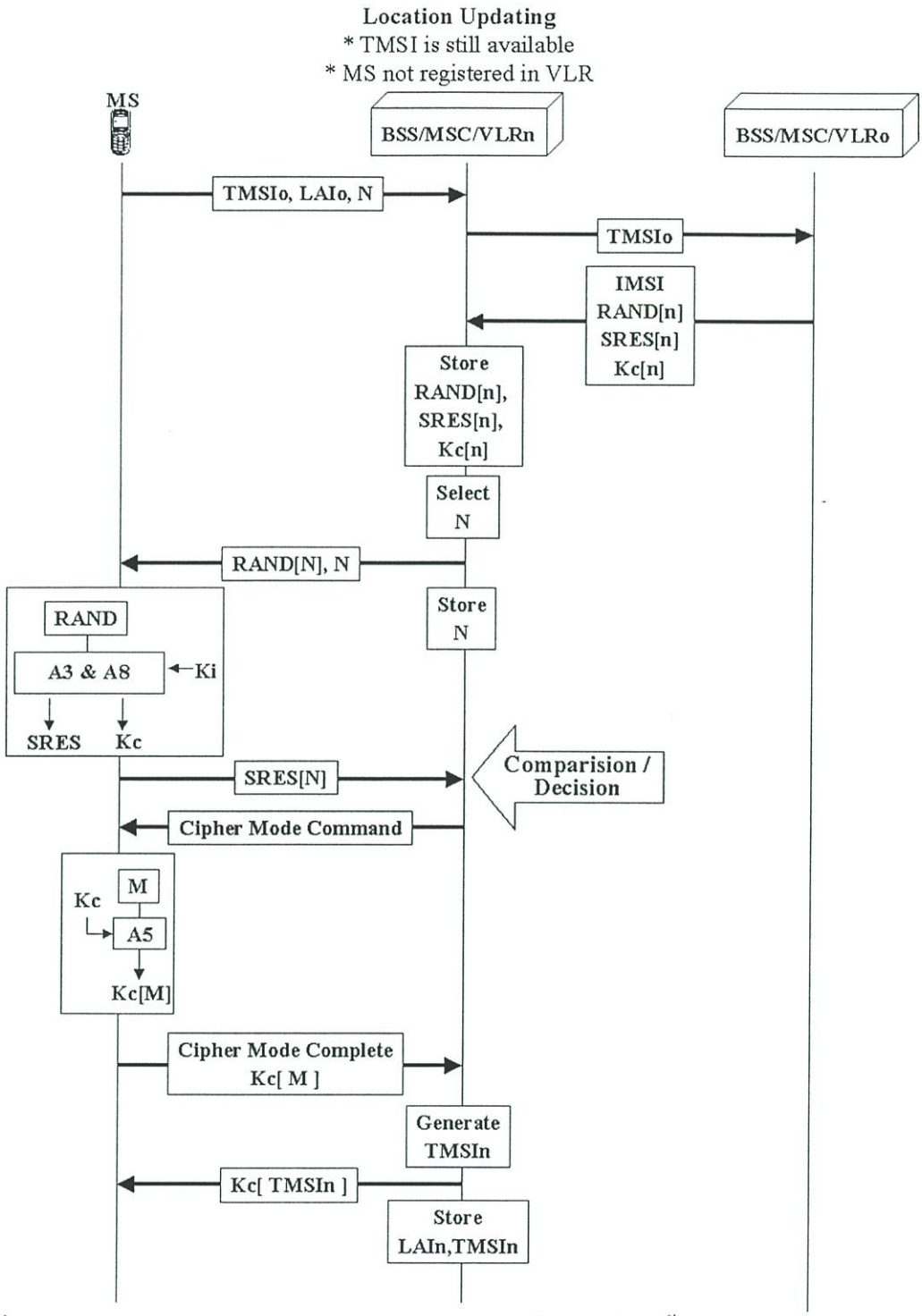
การปรับปรุงตำแหน่งที่อยู่ของผู้ใช้จะไม่ทำการร้องขอข้อมูลความปลอดภัยใหม่โดยจะใช้ชุดข้อมูลในการรักษาความปลอดภัยเดิมที่ได้รับในตอนที่ทำการลงทะเบียนตำแหน่งที่อยู่ของผู้ใช้ เมื่อผู้ใช้จะทำการปรับปรังตำแหน่งที่อยู่จะส่ง TMSI และ LAI ของตนให้กับ MSC เป็นการร้องขอการปรับปรุงตำแหน่งที่อยู่ (Location Updating Request) เมื่อ MSC ได้รับข้อมูลจะทำการตรวจสอบ LAI ถ้า LAI ที่ได้รับเป็นพื้นที่การจัดการของ MSC จะทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RAND ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RAND[N] และหมายเลขคีย์ที่เลือก ผู้ใช้จะทำการคำนวณหา SRES[N] แล้วส่งกลับให้ VLR เพื่อตรวจสอบ ดังแสดงในรูปที่ 3.28

ในกรณีที่ MSC ตรวจสอบ LAI ของผู้ใช้แล้วไม่ได้เป็นพื้นที่การจัดการของตน จะส่ง TMSI ของผู้ใช้เพื่อร้องขอข้อมูลในการรักษาความปลอดภัยจาก MSC เดิมซึ่งจะได้รับชุดข้อมูลในการรักษาความปลอดภัย 4 ตัวคือ RAND[n], SRES[n], Kc[n], และ IMSI แล้ว MSC จะใช้ข้อมูลในการรักษาความปลอดภัยชุดนี้ตรวจสอบผู้ใช้ดังแสดงในรูปที่ 3.29

หลังจากทำการตรวจสอบผู้ใช้เสร็จสมบูรณ์แล้ว MSC จะทำการผลิต TMSI ใหม่ให้กับผู้ใช้ โดยการส่ง TMSI ให้กับผู้ใช้ TMSI จะถูกเข้ารหัสลับเหมือนในโพรโตคอลของการลงทะเบียนตำแหน่งที่อยู่



รูปที่ 3.28 โพรโตคอลการทำ Location Updating ในกรณีที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC เดิม

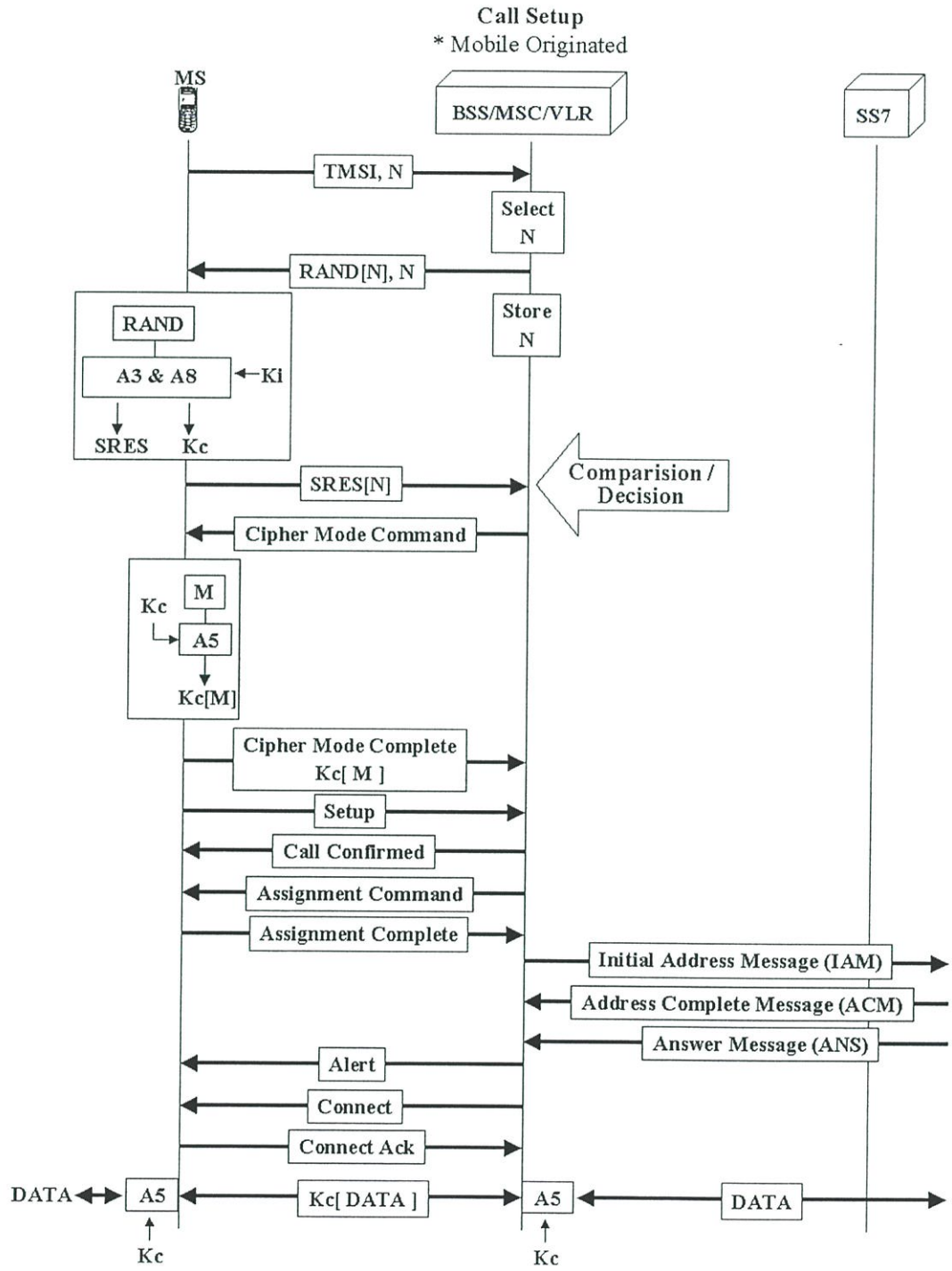


รูปที่ 3.29 โพรโตคอลการทำ Location Updating ในกรณีที่ผู้ใช้เปลี่ยนพื้นที่การจัดการของ MSC

3.4.3 โพรโตคอลการสร้างโทรศัพท์เข้าออก (Call Setup Protocol)

ในการโทรศัพท์เข้าและออกของผู้ใช้ ผู้ใช้จะต้องผ่านการตรวจสอบผู้ใช้ก่อน และการสื่อสารข้อมูลแต่ละครั้งข้อมูลที่จะสื่อสารจะถูกเข้ารหัสลับก่อนที่จะส่งผ่านช่องสัญญาณวิทยุ

โพรโตคอลการโทรศัพท์เข้าและออกแบ่งเป็น 2 ส่วนคือ โพรโตคอลการโทรศัพท์ออก (Mobile Originated Protocol) และโพรโตคอลการโทรศัพท์เข้า (Mobile Terminated Protocol)



รูปที่ 3.30 โพรโตคอลการทำ Call Setup ในกรณี Mobile Originated

3.4.3.1 โพรโตคอลการโทรศัพท์ออก (Mobile Originated Protocol)

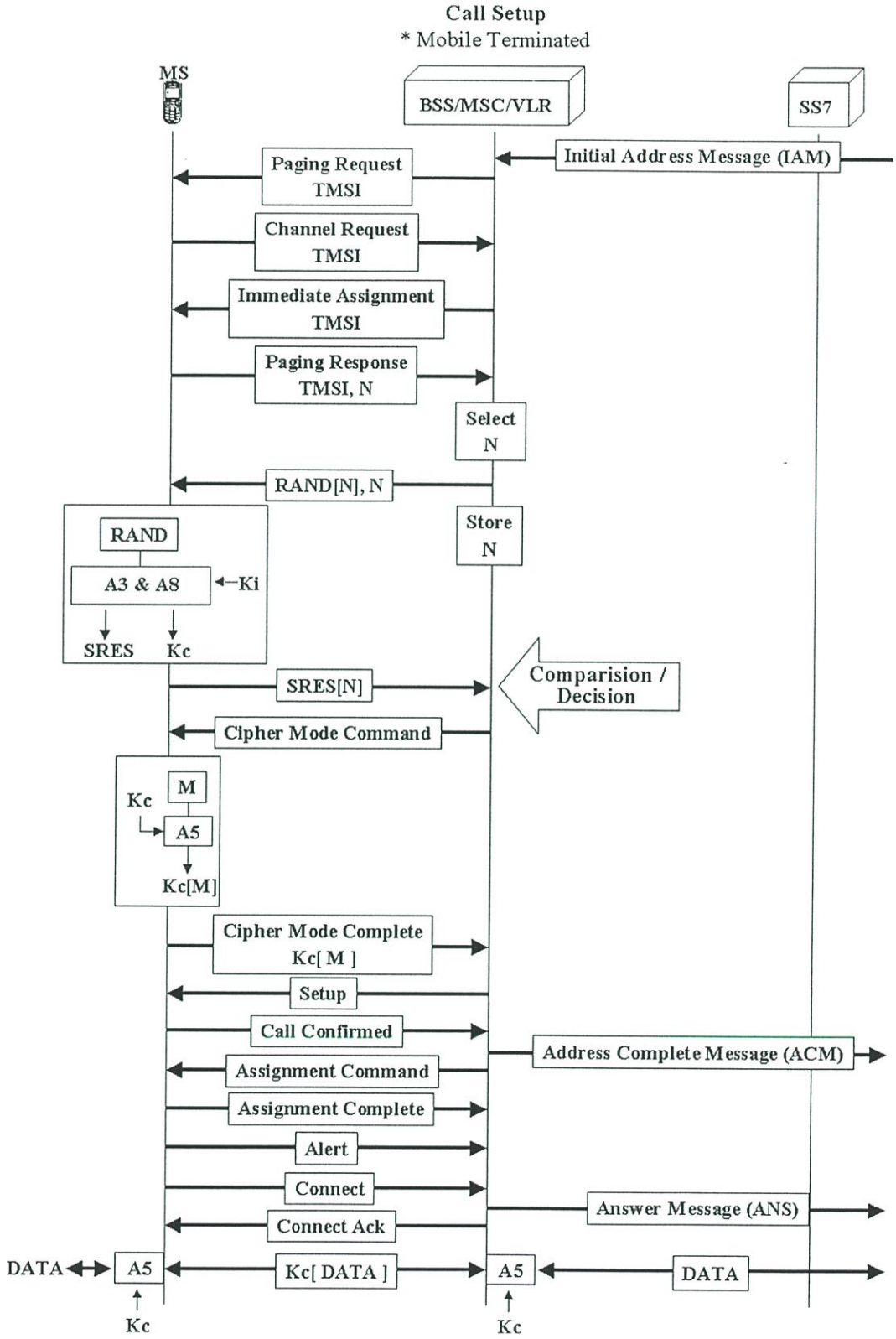
การโทรศัพท์ออก (Mobile Originated) คือ การที่ผู้ใช้ต้องการสร้างการติดต่อกับโทรศัพท์เคลื่อนที่หรือเครือข่ายใช้สายอื่นๆ โดยการกดเลขหมายของโทรศัพท์ที่ต้องการติดต่อบนโทรศัพท์เคลื่อนที่ของตน [14] ขั้นตอนของโพรโตคอลการโทรศัพท์ออกของผู้ใช้ดังแสดงในรูปที่ 3.30

ผู้ใช้จะส่ง TMSI และหมายเลขคีย์ (Key Number), N ให้กับ MSC โดยผ่าน BSS เป็นการแจ้งให้ MSC ทราบว่าต้องการจะโทรศัพท์ออก MSC จะทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RAND ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RAND[N] และหมายเลขคีย์ที่เลือก ผู้ใช้จะทำการคำนวณหา SRES[N] แล้วส่งกลับให้ VLR เพื่อตรวจสอบ

MSC จะส่งคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Command) ให้กับผู้ใช้เป็นการแจ้งให้ผู้ใช้ทราบว่าการส่งข้อมูลหลังจากนี้จะเป็นข้อมูลที่ถูกเข้ารหัสลับ MS จะเข้ารหัสลับข้อมูล M ด้วยอัลกอริทึม A5 เพื่อเป็นการตอบรับคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Complete) หลังจากนั้นผู้ใช้จะทำการร้องขอการโทรศัพท์ออก (Call Request) โดยการส่งเมสเสจ Setup ให้กับเครือข่าย เพื่อแจ้งให้ทราบว่าจะส่งข้อมูลไปที่ใดและลักษณะของบริการที่ต้องการ ถ้าบริการที่ร้องขอมานั้นเหมาะสม เครือข่ายจะส่งเมสเสจ Call Confirmed ให้กับ MS หลังจากนั้นเครือข่ายจะส่งเมสเสจ Assignment Command ให้กับผู้ใช้เพื่อหยุดการส่งสัญญาณควบคุมใน SDCCH ผู้ใช้จะส่งเมสเสจ Assignment Complete ผ่านช่องสัญญาณ FACCH เพื่อตอบรับการหยุดใช้ช่องสัญญาณควบคุม MSC จะส่งเมสเสจ IAM เพื่อร้องขอการติดต่อกับโทรศัพท์ปลายทางซึ่งจะผ่านเครือข่าย SS7 (Signalling System Number 7) โดยเครือข่าย SS7 จะทำหน้าที่ในการเปลี่ยนสัญญาณควบคุมของเครือข่าย GSM ให้เข้ากันกับเครือข่ายปลายทางที่ต้องการติดต่อ โทรศัพท์ปลายทางจะส่งเมสเสจ ACM กลับมาให้ MSC เพื่อจองช่องสัญญาณในการสื่อสารและเมื่อโทรศัพท์ปลายทางพร้อมที่จะทำการสื่อสารจะส่งเมสเสจ ANS ให้กับ MSC เมื่อได้รับเมสเสจ ANS แล้ว MSC จะส่งเมสเสจ Alert โดยผ่าน FACCH แจ้งให้ผู้ใช้ทราบว่าการโทรศัพท์ได้รับตอบรับแล้ว (Call Accept) เครือข่ายจะทำการจองช่องสัญญาณ TCH ให้กับผู้ใช้แล้วส่งเมสเสจ Connect ให้กับผู้ใช้เมื่อผู้ใช้ส่งเมสเสจ Connect Ack ผ่านช่องสัญญาณ FACCH ให้กับเครือข่าย ผู้ใช้ก็จะสามารถสื่อสารข้อมูลได้โดยข้อมูลที่จะสื่อสารจะต้องทำการเข้ารหัสลับก่อน เมื่อเครือข่ายได้รับข้อมูลจะทำการถอดรหัสลับข้อมูลก่อนที่จะส่งไปให้กับโทรศัพท์ปลายทางตามต้องการ

3.4.3.2 โพรโตคอลการโทรศัพท์เข้า (Mobile Terminated Protocol)

การโทรศัพท์เข้า (Mobile Terminated) คือ การที่ผู้ใช้ได้รับการติดต่อกับโทรศัพท์เคลื่อนที่หรือเครือข่ายใช้สายอื่นๆ ขั้นตอนของโพรโตคอลการโทรศัพท์เข้าของผู้ใช้ดังแสดงในรูปที่ 3.31



รูปที่ 3.31 โพรโตคอลการทำ Call Setup ในกรณี Mobile Terminated

โทรศัพท์เคลื่อนที่หรือเครือข่ายใช้สายอื่นๆจะส่งเมสเสจ IAM เพื่อร้องขอการติดต่อกับผู้ใช้โดยผ่านเครือข่าย SS7 (Signalling System Number 7) โดยเครือข่าย SS7 จะทำหน้าที่ในการ

เปลี่ยนสัญญาณควบคุมของเครือข่ายภายนอกให้เข้ากันกับเครือข่าย GSM เมื่อ MSC ได้รับ IAM ก็จะส่ง TMSI เพื่อเรียกหาผู้ใช้โดยผ่านช่องสัญญาณ PCH ผู้ใช้จะส่ง TMSI โดยผ่านช่องสัญญาณ RACH ให้กับเครือข่ายเพื่อร้องขอการจองช่องสัญญาณ SDCCH เครือข่ายจะส่ง TMSI โดยผ่านช่องสัญญาณ AGCH เพื่อเป็นการกำหนดช่องสัญญาณ SDCCH ให้กับผู้ใช้ ผู้ใช้จะส่ง TMSI และหมายเลขคีย์ (Key Number), N ให้กับ MSC โดยผ่าน BSS เป็นการแจ้งให้ MSC ทราบว่าต้องการจะโทรศัพท์ออก MSC จะทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RAND ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RAND[N] และหมายเลขคีย์ที่เลือก ผู้ใช้จะทำการคำนวณหา SRES[N] แล้วส่งกลับให้ VLR เพื่อตรวจสอบ

MSC จะส่งคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Command) ให้กับผู้ใช้เป็นการแจ้งให้ผู้ใช้ทราบว่าการส่งข้อมูลหลังจากนี้จะเป็นข้อมูลที่ถูกเข้ารหัสลับ MS จะเข้ารหัสลับข้อมูล M ด้วยอัลกอริทึม A5 เพื่อเป็นการตอบรับคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Complete) หลังจากนั้นเครือข่ายจะทำการร้องขอการโทรศัพท์เข้าโดยการส่งเมสเสจ Setup ให้กับผู้ใช้ เพื่อแจ้งให้ผู้ใช้ทราบว่าลักษณะของบริการ ถ้าบริการที่ร้องขอมานั้นเหมาะสม ผู้ใช้จะส่งเมสเสจ Call Confirmed ให้กับ MSC เมื่อผู้ใช้ยืนยันการรับโทรศัพท์แล้ว MSC จะส่งเมสเสจ ACM ให้กับโทรศัพท์ต้นทางพร้อมทั้งจองช่องสัญญาณในการสื่อสารกับโทรศัพท์ต้นทางให้กับผู้ใช้ หลังจากนั้นเครือข่ายและผู้ใช้จะส่งเมสเสจ Assignment Command กับเมสเสจ Assignment Complete เพื่อหยุดการส่งสัญญาณควบคุมใน SDCCH ผู้ใช้จะส่งเมสเสจ Alert โดยผ่าน FACCH แจ้งให้ MSC ทำการจองช่องสัญญาณ TCH ให้กับผู้ใช้แล้วส่งเมสเสจ Connect ให้กับเครือข่ายเพื่อแจ้งให้ MSC ทราบว่าพร้อมจะรับบริการ MSC จะส่งเมสเสจ ANS และ Connect Ack ให้กับโทรศัพท์ต้นทางและผู้ใช้ตามลำดับ เพื่อแจ้งให้ทราบว่าสามารถสร้างการติดต่อถูกสร้างเรียบร้อยแล้ว โทรศัพท์ต้นทางก็จะสามารถสื่อสารข้อมูลได้โดยข้อมูลก่อนที่จะถูกส่งให้ผู้ใช้ MSCจะต้องทำการเข้ารหัสลับก่อน เมื่อผู้ใช้ได้รับข้อมูลจะทำการถอดรหัสลับข้อมูลเพื่อที่จะทราบเนื้อหา (Content) ที่โทรศัพท์ต้นทางต้องการส่งให้ตามต้องการ

บทที่ 4

การออกแบบระบบรักษาความปลอดภัย

การรักษาความปลอดภัยของเครือข่ายต่างๆนั้นจะมีค่าใช้จ่ายที่เกิดขึ้นเมื่อทำการรักษาความปลอดภัย สำหรับการสื่อสารเคลื่อนที่นั้นมีข้อจำกัดของในเรื่องของเวลาค่อนข้างมาก ดังนั้นการรักษาความปลอดภัยจึงไม่ควรที่มีค่าใช้จ่ายที่สูงจนเกินไป แต่ในการลดค่าใช้จ่ายต่างๆเหล่านี้จะต้องพิจารณาถึงประสิทธิภาพของการรักษาความปลอดภัยด้วย การลดค่าใช้จ่ายจึงไม่ควรทำให้ประสิทธิภาพของความปลอดภัยลดลง

ในงานวิจัยนี้ทำการปรับปรุงบริการต่างๆในการรักษาความปลอดภัยของเครือข่าย GSM เพื่อลดค่าใช้จ่ายที่จะเกิดขึ้นในการรักษาความปลอดภัย และออกแบบอัลกอริทึมที่จะใช้เข้าและถอดรหัสลับข้อมูลเพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของเครือข่าย GSM

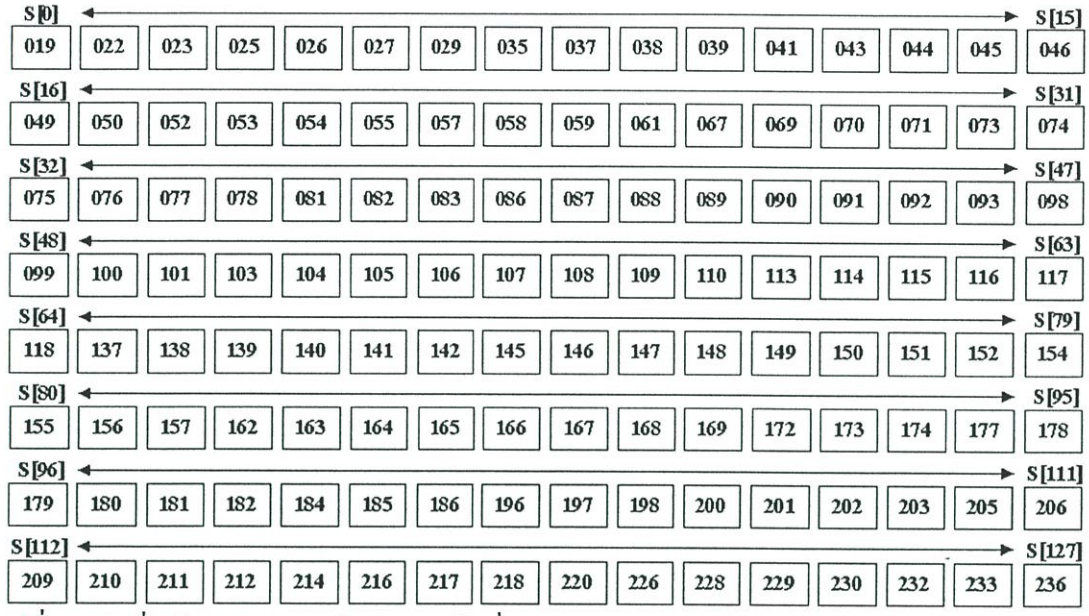
4.1 การออกแบบอัลกอริทึมที่ใช้เข้ารหัสลับข้อมูลสำหรับเครือข่าย GSM

งานวิจัยนี้ทำการออกแบบอัลกอริทึมที่จะใช้เข้าและถอดรหัสข้อมูลของผู้ใช้เครือข่าย GSM โดยทำการพัฒนาอัลกอริทึม RC4 ให้มีประสิทธิภาพยิ่งขึ้น อัลกอริทึมที่นำเสนอนี้สามารถเลือกใช้ขนาดของคีย์ที่จะใช้ในการเข้าและถอดรหัสลับได้ตามต้องการเหมือนกับอัลกอริทึม RC4 โดยประกอบ 2 ส่วนหลักคือ การจัดตารางคีย์ (Key Scheduling) และ การผลิตคีย์ต่อเนื่อง (Key Stream Generator) เช่นเดียวกับอัลกอริทึม RC4

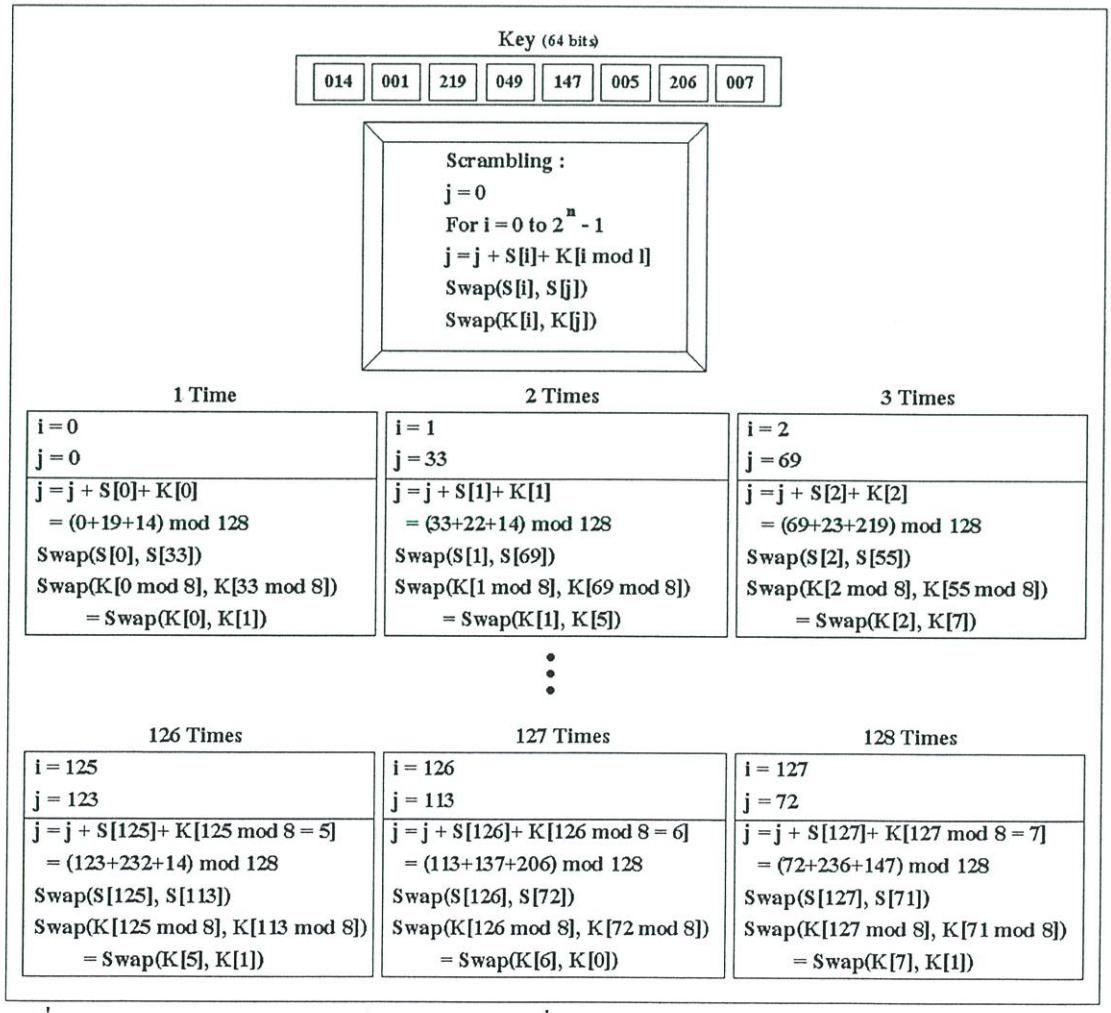
4.1.1 การจัดตารางคีย์ที่นำเสนอ (The Proposed Key Scheduling)

อัลกอริทึมที่นำเสนอนี้ถูกออกแบบโดยทำการลดของ S-Box ของอัลกอริทึม RC4 จากเดิม 256 ไบต์ลงเหลือ 128 ไบต์ โดยในตอนเริ่มต้นของการเข้าและถอดรหัสลับข้อมูลของอัลกอริทึมที่นำเสนอนี้ สมาชิกแต่ละตัวใน S-Box ดังแสดงในรูปที่ 4.1

ในการจัดตารางคีย์ที่นำเสนอนี้จะนำคีย์ที่ใช้เข้าและถอดรหัสลับข้อมูลมาใส่ลงไปในอาร์เรย์ K โดยอาร์เรย์ K มีจำนวนสมาชิกทั้งหมดตามขนาดของคีย์ที่เลือกใช้และสมาชิกแต่ละตัวจะมีขนาด 1 ไบต์ เช่นเดียวกับการจัดตารางคีย์ของอัลกอริทึม RC4



รูปที่ 4.1 ค่าเริ่มต้นของ S-Box ในอัลกอริทึมที่นำเสนอ

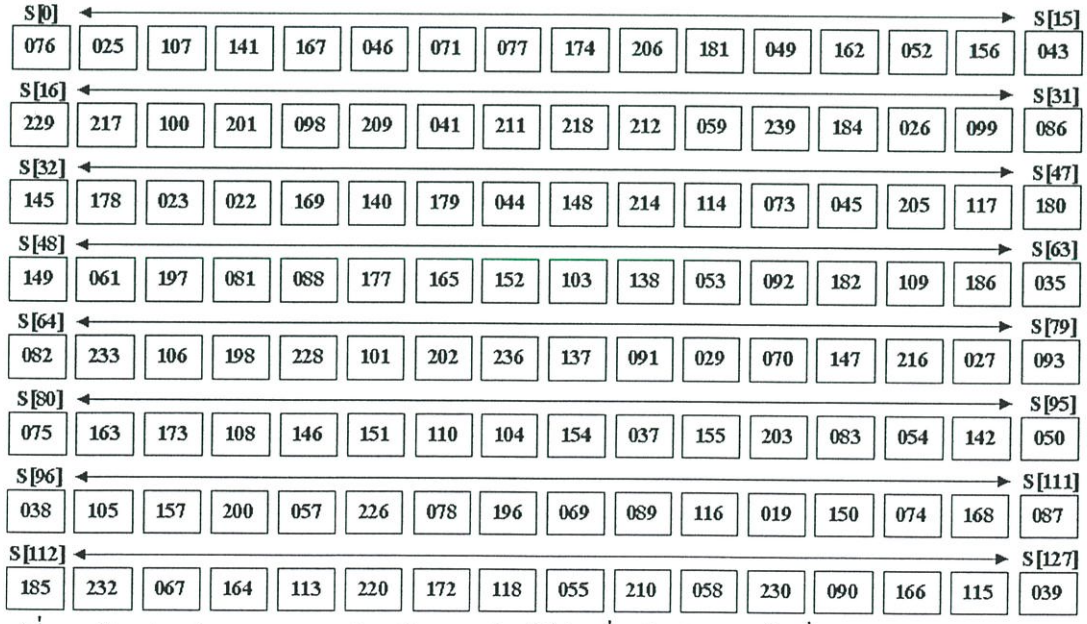


รูปที่ 4.2 ตัวอย่างการจัดตารางคีย์ของอัลกอริทึมที่นำเสนอ

ทำการกวนตารางคีย์ (Key Scrambling) เพื่อสลับเปลี่ยนค่าของสมาชิกใน S-Box โดยใช้คีย์ในการเข้าและถอดรหัสลับเป็นตัวควบคุมตำแหน่งการสลับสับเปลี่ยน ขั้นตอนการกวนตารางคีย์นี้จะทำการสลับเปลี่ยนค่าของสมาชิกใน S-Box ทั้งหมด 128 ครั้ง ในการสลับเปลี่ยนค่าของสมาชิกใน S-Box จะทำการสลับเปลี่ยนโดยมีขั้นตอนการคำนวณดังแสดงในรูปที่ 4.2

ขั้นตอนการจัดตารางคีย์ที่นำเสนอนี้ประกอบด้วยตัวแปร 2 ตัวคือ ตัวแปร i และตัวแปร j ค่าของตัวแปร i จะถูกเพิ่มขึ้นทีละ 1 ทุกรอบของการสลับเปลี่ยนโดยค่าตัวแปร i มีค่าเริ่มต้นเป็น 0 ค่าของตัวแปร j ซึ่งมีค่าเริ่มต้นเป็น 0 เช่นเดียวกับค่าตัวแปร i จะถูกนำไปบวกกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i และค่าของสมาชิกในอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วยจำนวนสมาชิกในอาร์เรย์ K หลังจากการนั้นนำค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วย 128 สลับเปลี่ยนกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร j หารเอาเศษ (Modulo) ด้วย 128

ในการจัดตารางคีย์ที่นำเสนอนี้นอกจากจะทำการสลับเปลี่ยนค่าของสมาชิกต่างๆ ใน S-Box แล้วยังทำการสลับเปลี่ยนค่าของสมาชิกต่างๆในอาร์เรย์ K อีกด้วย โดยจะสลับเปลี่ยนค่าของสมาชิกของอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วยจำนวนสมาชิกในอาร์เรย์ K สลับเปลี่ยนกับค่าของสมาชิกของอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร j หารเอาเศษ (Modulo) ด้วยจำนวนสมาชิกในอาร์เรย์ K

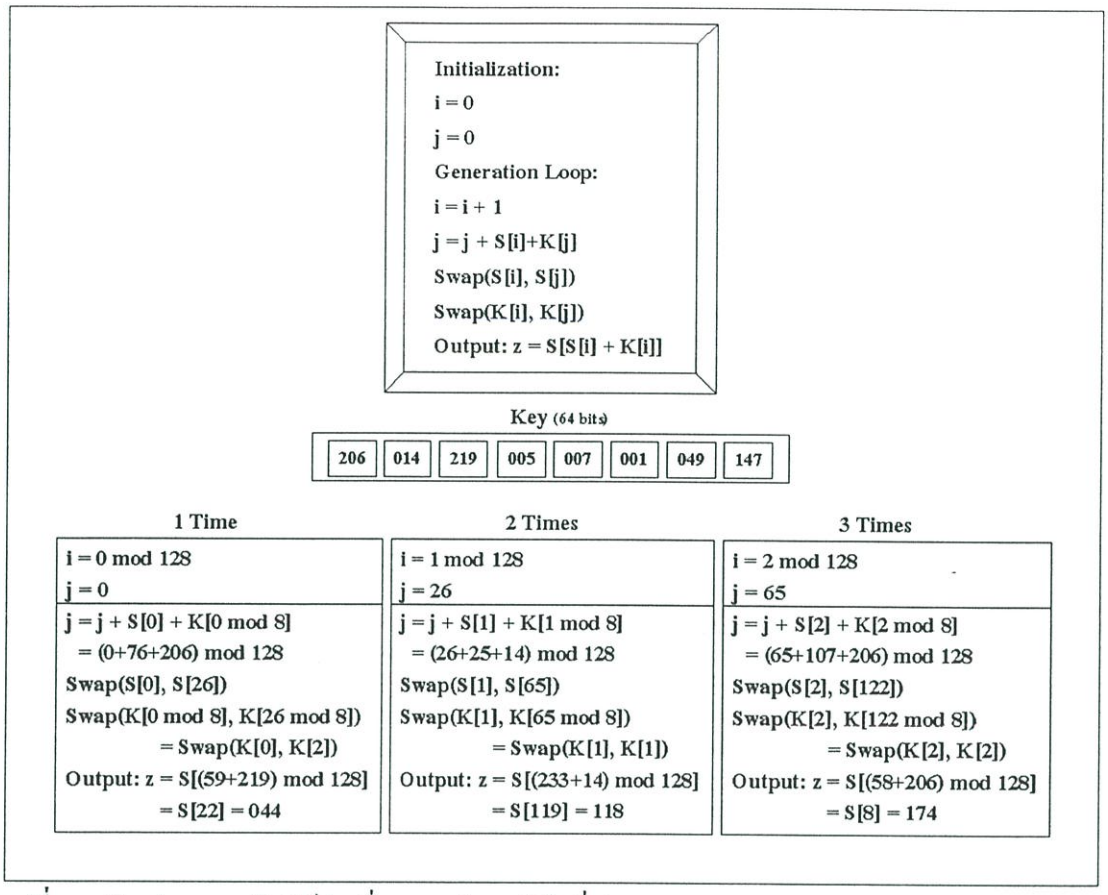


รูปที่ 4.3 ตัวอย่างค่าของ S-Box สำหรับการผลิตคีย์ต่อเนื่องในอัลกอริทึมที่นำเสนอ

4.1.2 การผลิตคีย์ต่อเนื่องที่นำเสนอ (The Proposed Key Stream Generator)

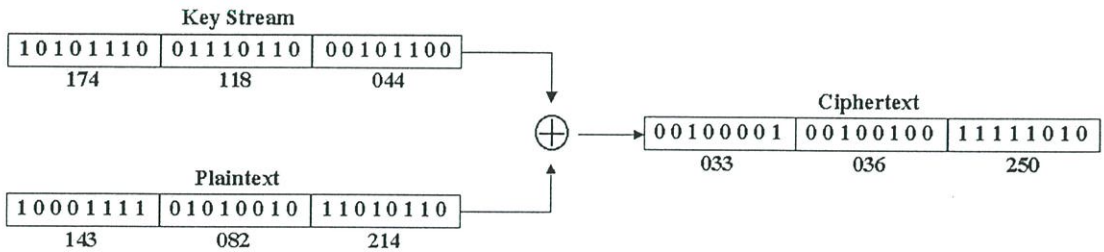
การผลิตคีย์ต่อเนื่องที่นำเสนอนั้นจะนำเอา S-Box ที่ได้ผ่านการจัดตารางคีย์มาแล้ว ดังแสดงในรูปที่ 4.3 มาคำนวณหาคีย์ต่อเนื่อง (Key Stream) โดยคีย์ต่อเนื่องจะถูกผลิตเป็นรอบๆ ละ 8 บิต โดยแต่ละรอบของการผลิตจะทำการสลับเปลี่ยนค่าของสมาชิกใน S-Box เช่นเดียวกับอัลกอริทึม RC4 นอกจากนั้นยังทำการสลับเปลี่ยนค่าของสมาชิกในอาร์เรย์ K อีกด้วย การสลับเปลี่ยนทั้งสองส่วนนี้จะทำในทุกๆรอบของการผลิตคีย์ต่อเนื่อง

ขั้นตอนการผลิตคีย์ต่อเนื่องที่นำเสนอประกอบด้วยตัวแปร 2 ตัวคือ ตัวแปร i และตัวแปร j เหมือนการผลิตคีย์ต่อเนื่องของอัลกอริทึม RC4 ค่าของตัวแปร i จะถูกเพิ่มขึ้นทีละ 1 แล้วหารเอาเศษด้วย 128 ทุกรอบของการผลิตคีย์ต่อเนื่องโดยค่าตัวแปร i มีค่าเริ่มต้นเป็น 0 ค่าของตัวแปร j ซึ่งมีค่าเริ่มต้นเป็น 0 เช่นเดียวกับค่าตัวแปร i จะถูกนำไปบวกกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วย 128 และบวกกับค่าของสมาชิกของอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วยจำนวนสมาชิกในอาร์เรย์ K หลังจากการนั้นนำค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วย 128 สลับเปลี่ยนกับค่าของสมาชิกของ S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร j หารเอาเศษ (Modulo) ด้วย 128 และทำการสลับเปลี่ยนค่าของสมาชิกของอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร i หารเอาเศษ (Modulo) ด้วยจำนวนสมาชิกในอาร์เรย์ K สลับเปลี่ยนกับค่าของสมาชิกของอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร j หารเอาเศษ (Modulo) ด้วยจำนวนสมาชิกในอาร์เรย์ K เอาท์พุตของการผลิตคีย์ต่อเนื่องในแต่ละรอบคือ สมาชิกใน S-Box ที่มีดัชนีเท่ากับค่าของสมาชิกใน S-Box ที่มีดัชนีเท่ากับค่าของตัวแปร i บวกกับค่าของสมาชิกในอาร์เรย์ K ที่มีดัชนีเท่ากับค่าของตัวแปร j ดังแสดงในรูปที่ 4.4



รูปที่ 4.4 ตัวอย่างการผลิตคีย์ต่อเนื่องของอัลกอริทึมที่นำเสนอ

เอาท์พุตของการผลิตคีย์ต่อเนื่องในแต่ละรอบจะถูกนำไป XOR กับ Plaintext เพื่อทำการสร้าง Ciphertext ตัวอย่างลำดับของบิต (Bit Sequence) ใน Plaintext กับลำดับของบิตใน Ciphertext ดังแสดงในรูปที่ 4.5



รูปที่ 4.5 การเข้ารหัสลับข้อมูลของอัลกอริทึมที่นำเสนอ

4.2 การปรับปรุงบริการรักษาความปลอดภัยของเครือข่าย GSM

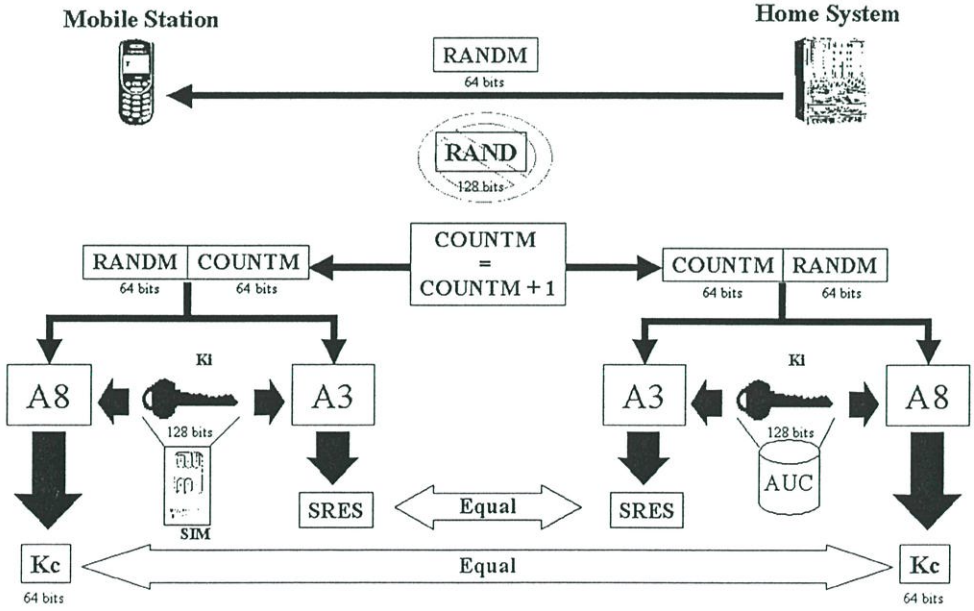
ในงานวิจัยนี้ทำการลดขนาดค่าสุ่ม (Random Number), RAND ขนาด 128 บิต โดยใช้ ค่าสุ่มของโทรศัพท์เคลื่อนที่ (Mobile Random Number), RANDM ขนาด 64 บิตแทน เนื่องจากค่าของ

RAND จะถูกใช้ในบริการรักษาความปลอดภัยต่างๆ ในเครือข่าย GSM ดังนั้นการปรับเปลี่ยนค่าของ RAND จึงมีผลกระทบกับหลายๆ บริการ

การปรับปรุงบริการตรวจสอบผู้ใช้และการจัดส่งคีย์ในการเข้ารหัสลับ มีขั้นตอนดังแสดงในรูปที่ 4.6 เปลี่ยนการส่ง RAND ขนาด 128 บิตเป็น RANDM ขนาด 64 บิต เมื่อทางฝั่งผู้ใช้ได้รับ RANDM จะนำไปคำนวณกับอัลกอริทึม A3 และ A8 เพื่อหา SRES และ Kc ตามลำดับ แต่เนื่องจากอัลกอริทึม A3 และ A8 ต้องการอินพุตขนาด 64 บิต ทำให้ไม่สามารถนำ RANDM ไปใช้เป็นอินพุตได้เพียงลำพัง เพื่อที่จะทำให้อินพุตมีขนาด 128 บิต ผู้ใช้และเครือข่ายจะนำ RANDM ไปรวม (Concatenate) กับ COUNTM (Mobile Counter) ขนาด 64 บิต

COUNTM คือ จำนวนครั้งที่ผู้ใช้คนนั้นทำการตรวจสอบ (Authentication) กับเครือข่าย ผู้ใช้และเครือข่ายจะสร้างตัวนับ (Counter) ขึ้นมาเพื่อนับจำนวนครั้งที่ผู้ใช้ทำการตรวจสอบกับเครือข่าย ทำให้ผู้ใช้และเครือข่ายมีค่าของ COUNTM ที่เท่ากันโดยไม่จำเป็นจะต้องส่ง COUNTM แลกเปลี่ยนกันระหว่างผู้ใช้และเครือข่าย

หลังจากทำการรวม COUNTM กับ RANDM เสร็จแล้ว นำไปคำนวณกับอัลกอริทึม A3 และ A8 โดยใช้ Ki เป็นคีย์ในการคำนวณเพื่อหา SRES ขนาด 32 บิต และ Kc ขนาด 64 บิต ตามลำดับ



รูปที่ 4.6 การปรับปรุงบริการรักษาความปลอดภัย

4.3 โพรโตคอลการสื่อสารที่นำเสนอ

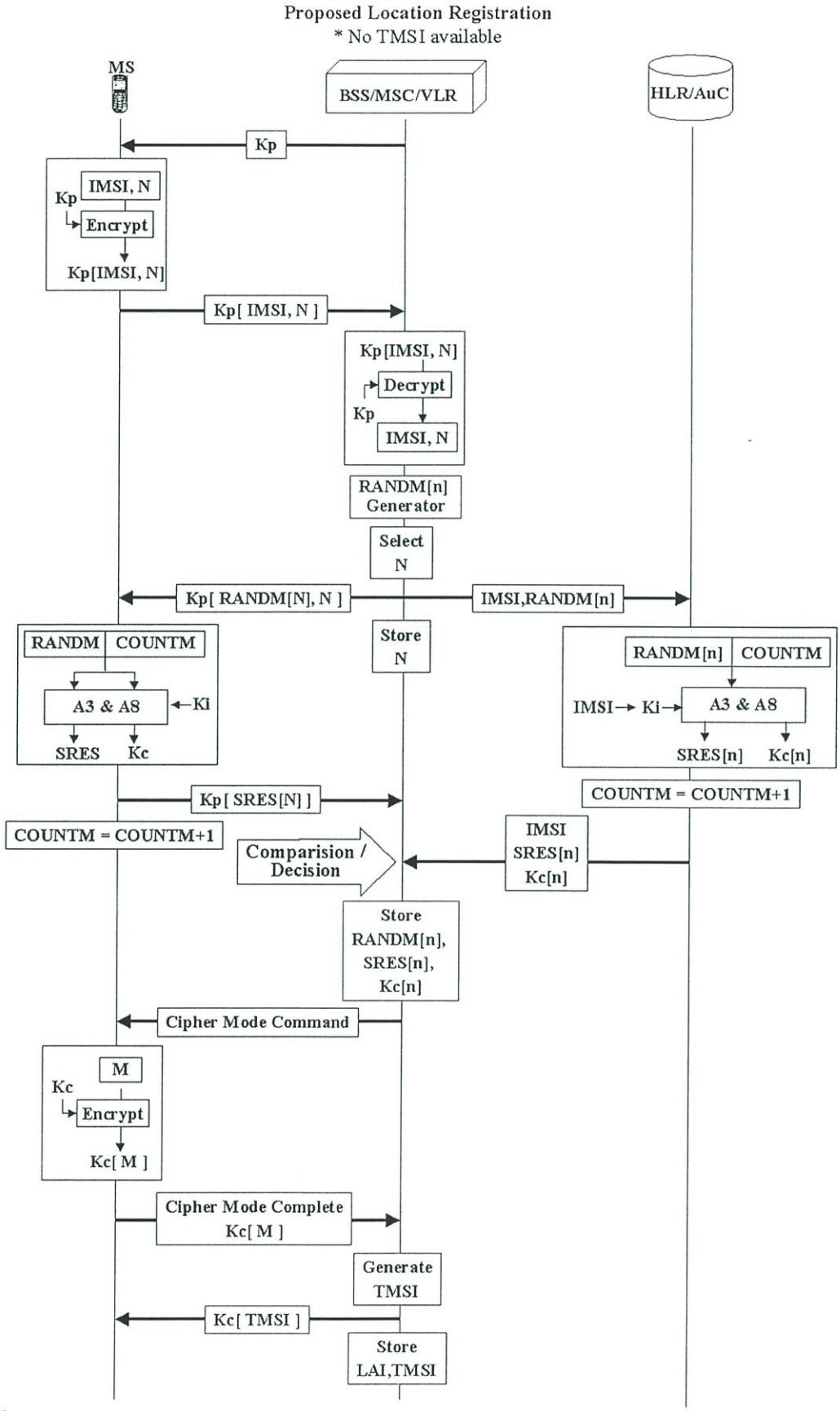
เนื่องจากการสื่อสารเคลื่อนที่มีความจำเป็นที่จะต้องสื่อสารข้อมูลผ่านช่องสัญญาณวิทยุซึ่งเป็นสื่อกลางที่ง่ายแก่การถูกผู้ไม่ประสงค์ดีลักลอบนำข้อมูลต่างๆของผู้ใช้ หรือปลอมตัวเข้ามาใช้ทรัพยากรของเครือข่าย งานวิจัยนี้ทำการออกแบบโพรโตคอลการสื่อสารของเครือข่าย GSM ใหม่

โดยจัดเตรียมการป้องกันข้อมูลที่จะถูกส่งผ่านช่องสัญญาณวิทยุและเปลี่ยนหน่วยงานที่จะทำการผลิตค่าสุ่ม (Random Number) เพื่อที่จะสามารถลดค่าใช้จ่ายของการรักษาความปลอดภัยของเครือข่าย GSM รายละเอียดของโพรโตคอลที่นำเสนอนั้นแบ่งออกเป็น 3 ส่วนคือ การลงทะเบียนตำแหน่งที่อยู่ที่นำเสนอ (The Proposed Location Registration), การลงทะเบียนตำแหน่งที่อยู่ที่นำเสนอ (The Proposed Location Updating), การสร้างการโทรศัพท์เข้าออกที่นำเสนอ (The Proposed Call Setup)

4.3.1 โพรโตคอลการลงทะเบียนตำแหน่งที่อยู่ที่นำเสนอ (The Proposed Location Registration Protocol)

การลงทะเบียนตำแหน่งที่อยู่ของผู้ใช้เครือข่าย GSM แต่ละครั้งจะต้องทำการสร้างข้อมูลในการรักษาความปลอดภัยขึ้นใหม่และจะต้องทำการส่งข้อมูลในการรักษาความปลอดภัยให้กับหน่วยงานต่างๆ ที่จำเป็น ดังนั้นการออกแบบโพรโตคอลจำเป็นต้องคำนึงถึงหน้าที่และข้อจำกัดต่างๆของแต่ละหน่วยงานในเครือข่าย ขั้นตอนของโพรโตคอลการลงทะเบียนตำแหน่งที่อยู่ที่นำเสนอดังแสดงในรูปที่ 4.7

MSC จะส่ง (Broadcast) Kp ให้กับผู้ใช้ทุกคนใน LA ของตนทุกๆ นาทีโดยผ่านทางช่องสัญญาณ BCCH เมื่อผู้ใช้จะทำการลงทะเบียนตำแหน่งที่อยู่จะนำ Kp เข้ารหัสลับข้อมูลที่จะส่งโดยใช้อัลกอริทึมที่นำเสนอ ทางฝั่ง MSC จะถอดรหัสลับข้อมูลโดยใช้ Kp และอัลกอริทึมที่นำเสนอ หลังจากนั้น MSC จะทำการผลิต RANDM จำนวน n ตัว แล้วทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RANDM ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RANDM[N] และหมายเลขคีย์ที่เลือก N ให้กับผู้ใช้โดยก่อนที่จะส่งจะต้องทำการเข้ารหัสลับก่อน ในขณะเดียวกันจะส่ง IMSI กับอาร์เรย์ RANDM ทั้งหมดให้กับ AuC โดยผ่าน HLR เมื่อ AuC ได้รับ IMSI และอาร์เรย์ของ RANDM ที่มีสมาชิกจำนวน n ตัว จะทำการคำนวณหาอาร์เรย์ของ SRES และ Kc จำนวน n ตัวเช่นกัน โดยก่อนที่จะนำ RANDM ไปคำนวณกับอัลกอริทึม A3 และ A8 จะต้องนำ RANDM ไปรวมกับ COUNTM ก่อน เมื่ออาร์เรย์ของ SRES และ Kc ได้แล้วส่งชุดข้อมูล 3 ตัวคือ นำ IMSI, อาร์เรย์ของ SRES, และ Kc กลับไปให้ MSC โดยผ่าน HLR ทางฝั่งผู้ใช้ก็จะนำ RANDM[N] ที่ได้รับไปถอดรหัสลับและนำไปรวมกับ COUNTM ที่เก็บไว้ใน SIM ทำการคำนวณหา SRES[N] และ Kc[N] ทำการเข้ารหัสลับ SRES[N] ก่อนที่จะส่งให้ MSC เมื่อ MSC ได้รับ SRES ของผู้ใช้จะทำการถอดรหัสข้อมูลแล้วทำการเปรียบเทียบกับอาร์เรย์ SRES ที่ได้รับจาก AuC ถ้าตรงกันการตรวจสอบผู้ใช้เป็นอันเสร็จสมบูรณ์



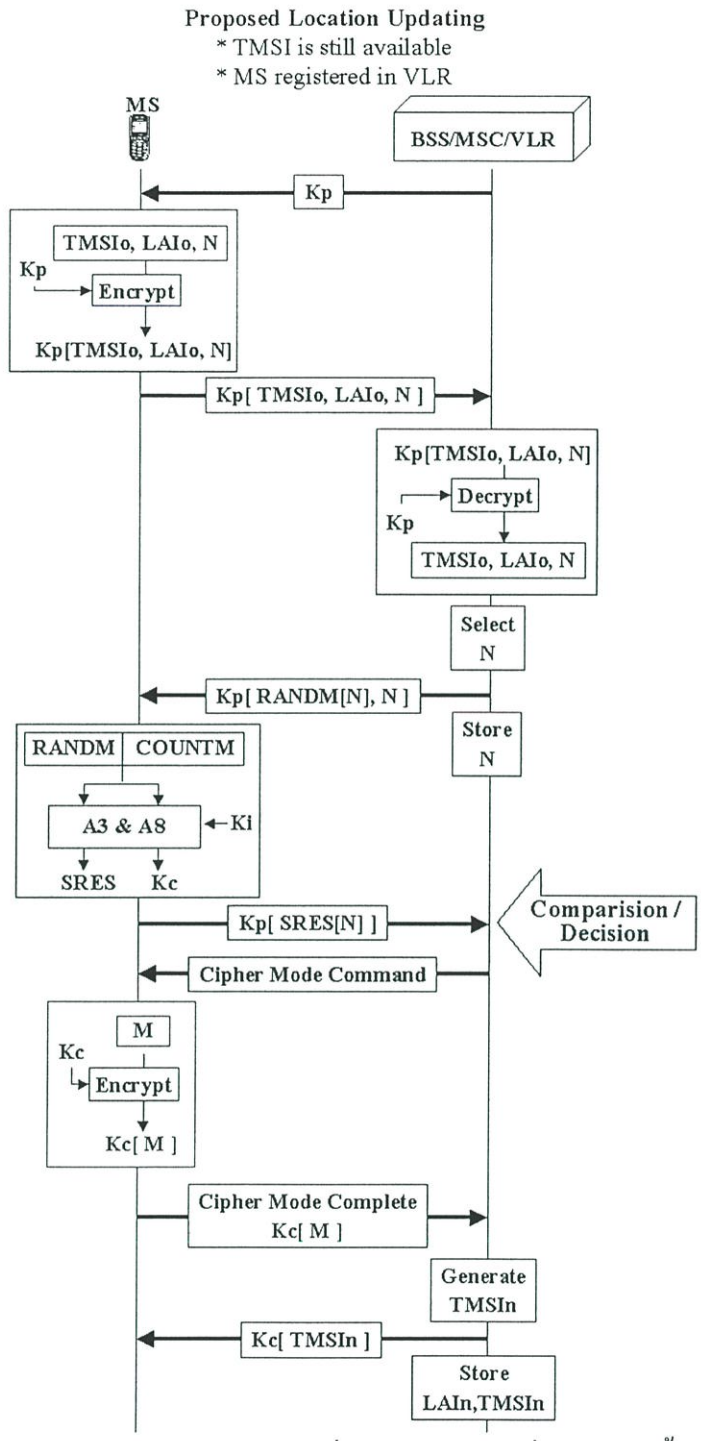
รูปที่ 4.7 โพรโตคอลการทำ Location Registration ที่นำเสนอ

MSC จะทำการผลิต TMSI แล้วส่งคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Command) ให้กับผู้ใช้เป็นการแจ้งให้ผู้ใช้ทราบว่าการส่งข้อมูลหลังจากนี้จะเปลี่ยนการเข้ารหัสลับโดยใช้ Kc แทน Kp ผู้ใช้จะเข้ารหัสลับข้อมูล M ด้วยอัลกอริทึมที่นำเสนอ เพื่อเป็นการตอบรับคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Complete) เมื่อ MSC ได้รับ TMSI การตอบรับคำสั่งสภาวะการเข้ารหัสลับจากผู้ใช้จะนำ Kc[N] เข้ารหัสลับ TMSI ด้วยอัลกอริทึมที่นำเสนอแล้วส่งให้กับผู้ใช้ ผู้ใช้จะใช้ TMSI ที่ได้รับเก็บไว้ใน SIM เพื่อใช้แทน IMSI ต่อไป ทางฝั่ง MSC จะเก็บ TMSI และ LAI ผู้ใช้ไว้ในฐานข้อมูล VLR ในการส่งสัญญาณควบคุมทั้งหมดของการลงทะเบียนตำแหน่งที่อยู่นี้จะใช้ช่องสัญญาณควบคุม SDCCH

4.3.2 โพรโตคอลการปรับปรุงตำแหน่งที่อยู่ที่นำเสนอ (The Proposed Location Updating Protocol)

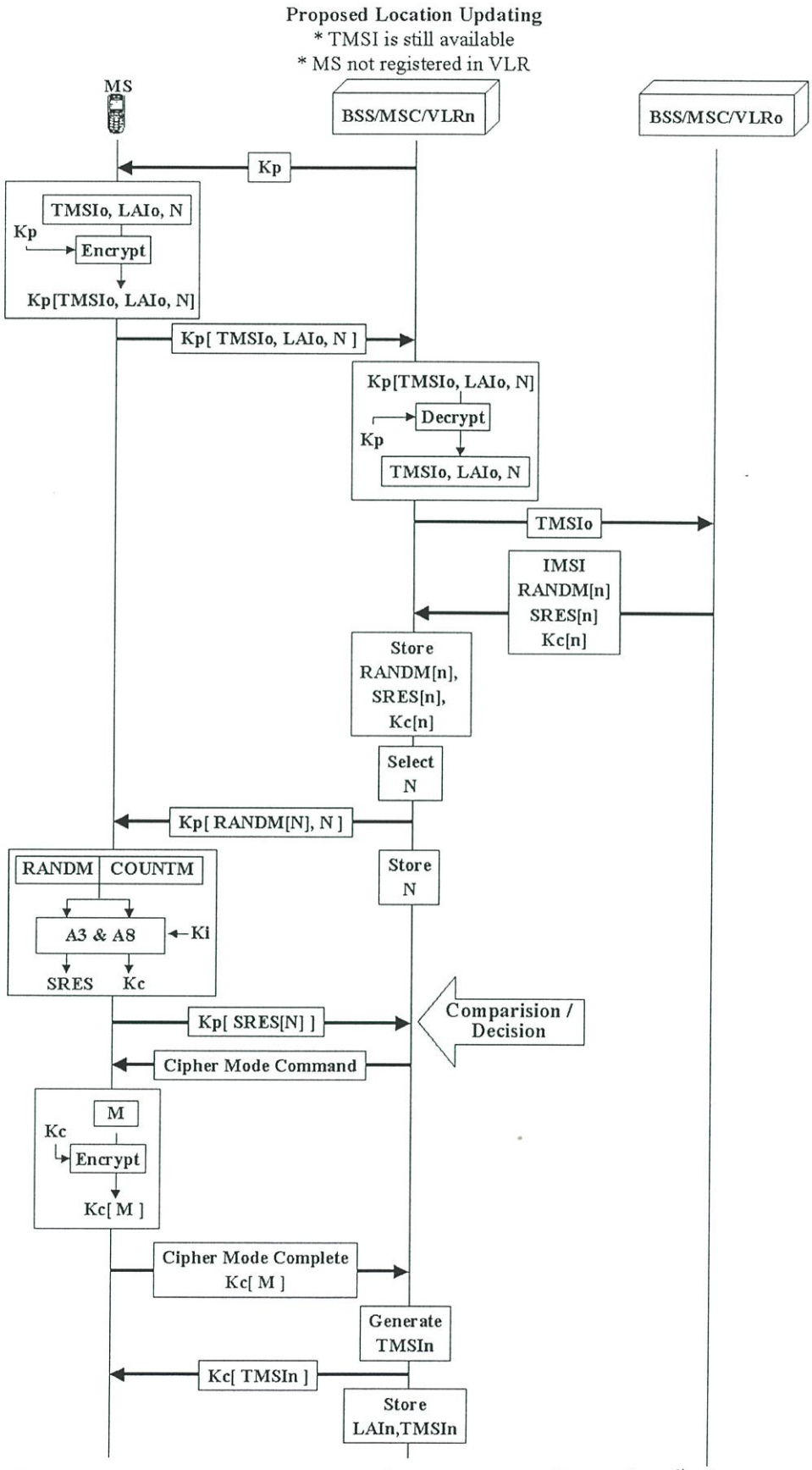
จากการปรับเปลี่ยนวิธีการรักษาความปลอดภัยและโพรโตคอลในการลงทะเบียนตำแหน่งที่อยู่ทำให้จำเป็นต้องทำการออกแบบโพรโตคอลที่ใช้ในการปรับปรุงตำแหน่งที่อยู่ของผู้ใช้ในเครือข่าย GSM ด้วย โพรโตคอลการปรับปรุงตำแหน่งที่อยู่ของผู้ใช้ที่นำเสนอนี้แบ่งเป็น 2 กรณีคือ กรณีที่ผู้ใช้อยู่ในพื้นการจัดการของ MSC เดิม กับกรณีที่ผู้ใช้อยู่ในพื้นการจัดการของ MSC ใหม่ ดังแสดงในรูปที่ 4.8 และรูปที่ 4.9 ตามลำดับเช่นเดียวกับโพรโตคอลเดิมของเครือข่าย GSM

การปรับปรุงตำแหน่งที่อยู่ของผู้ใช้ที่นำเสนอนี้จะไม่ทำการร้องขอข้อมูลความปลอดภัยใหม่โดยจะใช้ชุดข้อมูลในการรักษาความปลอดภัยเดิมที่ได้รับในตอนที่ทำการลงทะเบียนตำแหน่งที่อยู่ของผู้ใช้ ก่อนที่ผู้ใช้จะส่งข้อมูลจะนำ Kp ที่ได้จากช่องสัญญาณ BCCH มาเข้ารหัสลับข้อมูลที่ต้องการส่ง เมื่อผู้ใช้จะทำการปรับปรังตำแหน่งที่อยู่จะส่ง TMSI และ LAI ของตนให้กับ MSC เป็นการร้องขอการปรับปรุงตำแหน่งที่อยู่ (Location Updating Request) เมื่อ MSC ได้รับข้อมูลจะทำการตรวจสอบ LAI ถ้า LAI ที่ได้รับเป็นพื้นที่การจัดการของ MSC จะทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RANDM ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RANDM[N] และหมายเลขคีย์ที่เลือก ผู้ใช้จะทำการคำนวณหา SRES[N] แล้วส่งกลับให้ VLR เพื่อตรวจสอบผู้ใช้ โดยการคำนวณนั้นจะต้องนำ RANDM[N] ไปรวมกับ COUNTM ก่อนดังแสดงในรูปที่ 4.8



รูปที่ 4.8 โพรโตคอลการทำ Location updating ที่นำเสนอในกรณีที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC เดิม

ในกรณีที่ MSC ตรวจสอบ LAI ของผู้ใช้แล้วไม่ได้เป็นพื้นที่การจัดการของตน จะส่ง TMSI ของผู้ใช้เพื่อร้องขอข้อมูลในการรักษาความปลอดภัยจาก MSC เดิมซึ่งจะได้รับชุดข้อมูลในการรักษาความปลอดภัย 4 ตัวคือ RANDM[n], SRES[n], Kc[n], และ IMSI แล้ว MSC จะใช้ข้อมูลในการรักษาความปลอดภัยชุดนี้ตรวจสอบผู้ใช้ดังแสดงในรูปที่ 4.9



รูปที่ 4.9 โพรโตคอลการทำ Location updating ที่นำเสนอในกรณีที่ผู้ใช้เปลี่ยนพื้นที่การจัดการของ MSC

หลังจากทำการตรวจสอบผู้ใช้เสร็จสมบูรณ์แล้ว MSC จะทำการผลิต TMSI ใหม่ให้กับผู้ใช้ โดยการส่ง TMSI ให้กับผู้ใช้ TMSI จะถูกเข้ารหัสลับเหมือนในโพรโตคอลของการลงทะเบียนตำแหน่งที่อยู่ที่นำเสนอ โดยการเข้ารหัสลับในส่วนนี้จะใช้ Kc แทน Kp จากนั้น MSC จะทำการบันทึก LAI และ TMSI ใหม่ลงในฐานข้อมูล VLR เพื่อปรับปรุงตำแหน่งที่อยู่ของผู้ใช้ให้ถูกต้อง

4.3.3 โพรโตคอลการสร้างการโทรศัพท์เข้าออกที่นำเสนอ (The Proposed Call Setup Protocol)

ในการโทรศัพท์เข้าและออกของผู้ใช้ที่นำเสนอนี้ออกแบบให้ผู้ใช้ผ่านการตรวจสอบผู้ใช้ก่อน และการสื่อสารแต่ละครั้งข้อมูลที่จะสื่อสารจะถูกเข้ารหัสลับโดยใช้อัลกอริทึมที่นำเสนอก่อนที่จะส่งผ่านช่องสัญญาณวิทยุ โพรโตคอลการสร้างโทรศัพท์เข้าและออกที่นำเสนอนี้แบ่งเป็น 2 ส่วนคือ โพรโตคอลการโทรศัพท์ออกที่นำเสนอ (The Proposed Mobile Originated Protocol) และโพรโตคอลการโทรศัพท์เข้าที่นำเสนอ (The Proposed Mobile Terminated Protocol)

4.3.3.1 โพรโตคอลการโทรศัพท์ออกที่นำเสนอ (The Proposed Mobile Originated Protocol)

โพรโตคอลการโทรศัพท์ออกที่นำเสนอนี้ออกแบบให้มีการเข้ารหัสลับข้อมูลที่จะสื่อสารผ่านช่องสัญญาณวิทยุโดยการใช้ Kp ร่วมกับอัลกอริทึมที่นำเสนอ ขั้นตอนของโพรโตคอลการโทรศัพท์ออกของผู้ใช้ดังแสดงในรูปที่ 4.10

ก่อนผู้ใช้จะส่ง TMSI และหมายเลขคีย์ (Key Number), N ให้กับ MSC จะนำข้อมูลที่จะส่งมาเข้ารหัสลับโดยใช้ Kp ผ่าน BSS เป็นการแจ้งให้ MSC ทราบว่าต้องการจะโทรศัพท์ออก MSC จะทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RANDM ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RANDM[N] และหมายเลขคีย์ที่เลือกให้กับผู้ใช้ ผู้ใช้จะทำการคำนวณหา SRES[N] แล้วส่งกลับให้ VLR เพื่อตรวจสอบ โดยก่อนการคำนวณนั้นจะต้องนำ RANDM ไปรวมกับ COUNTM ก่อน

MSC จะส่งคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Command) ให้กับผู้ใช้เป็นการแจ้งให้ผู้ใช้ทราบว่าการส่งข้อมูลหลังจากนี้จะเป็นข้อมูลที่ถูกเข้ารหัสลับโดยใช้ Kc ที่ได้จากการตรวจสอบผู้ใช้ MS จะเข้ารหัสลับข้อมูล M ด้วยอัลกอริทึมที่นำเสนอ เพื่อเป็นการตอบรับคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Complete) หลังจากนั้นผู้ใช้จะทำการร้องขอการโทรศัพท์ออก (Call Request) โดยการส่งเมสเสจ Setup ให้กับเครือข่าย เพื่อแจ้งให้ทราบว่าจะส่งข้อมูลไปที่ใดและลักษณะของบริการที่ต้องการ ถ้าบริการที่ร้องขอมานั้นเหมาะสม เครือข่ายจะส่งเมสเสจ Call Confirmed ให้กับ MS หลังจากนั้นเครือข่ายจะส่งเมสเสจ Assignment Command ให้กับผู้ใช้เพื่อหยุดการส่งสัญญาณควบคุมใน SDCCH ผู้ใช้จะส่งเมสเสจ Assignment Complete ผ่านช่องสัญญาณ FACCH เพื่อตอบรับการหยุดใช้ช่องสัญญาณควบคุม MSC จะส่งเมสเสจ IAM เพื่อร้องขอ

การติดต่อกับโทรศัพท์ปลายทาง โทรศัพท์ปลายทางจะส่งเมสเสจ ACM กลับมาให้ MSC เพื่อจองช่องสัญญาณในการสื่อสารและเมื่อโทรศัพท์ปลายทางพร้อมที่จะทำการสื่อสารจะส่งเมสเสจ ANS ให้กับ MSC เมื่อได้รับเมสเสจ ANS แล้ว MSC จะส่งเมสเสจ Alert โดยผ่าน FACCH แจ้งให้ผู้ใช้ทราบว่าการโทรศัพท์ได้รับตอบรับแล้ว (Call Accept) เครือข่ายจะทำการจองช่องสัญญาณ TCH ให้กับผู้ใช้แล้วส่งเมสเสจ Connect ให้กับผู้ใช้เมื่อผู้ใช้ส่งเมสเสจ Connect Ack ผ่านช่องสัญญาณ FACCH ให้กับเครือข่าย ผู้ใช้ก็จะสามารถสื่อสารข้อมูลได้โดยข้อมูลที่จะสื่อสารจะต้องทำการเข้ารหัสลับก่อน เมื่อเครือข่ายได้รับข้อมูลจะทำการถอดรหัสลับข้อมูลก่อนที่จะส่งไปให้กับโทรศัพท์ปลายทางตามต้องการ

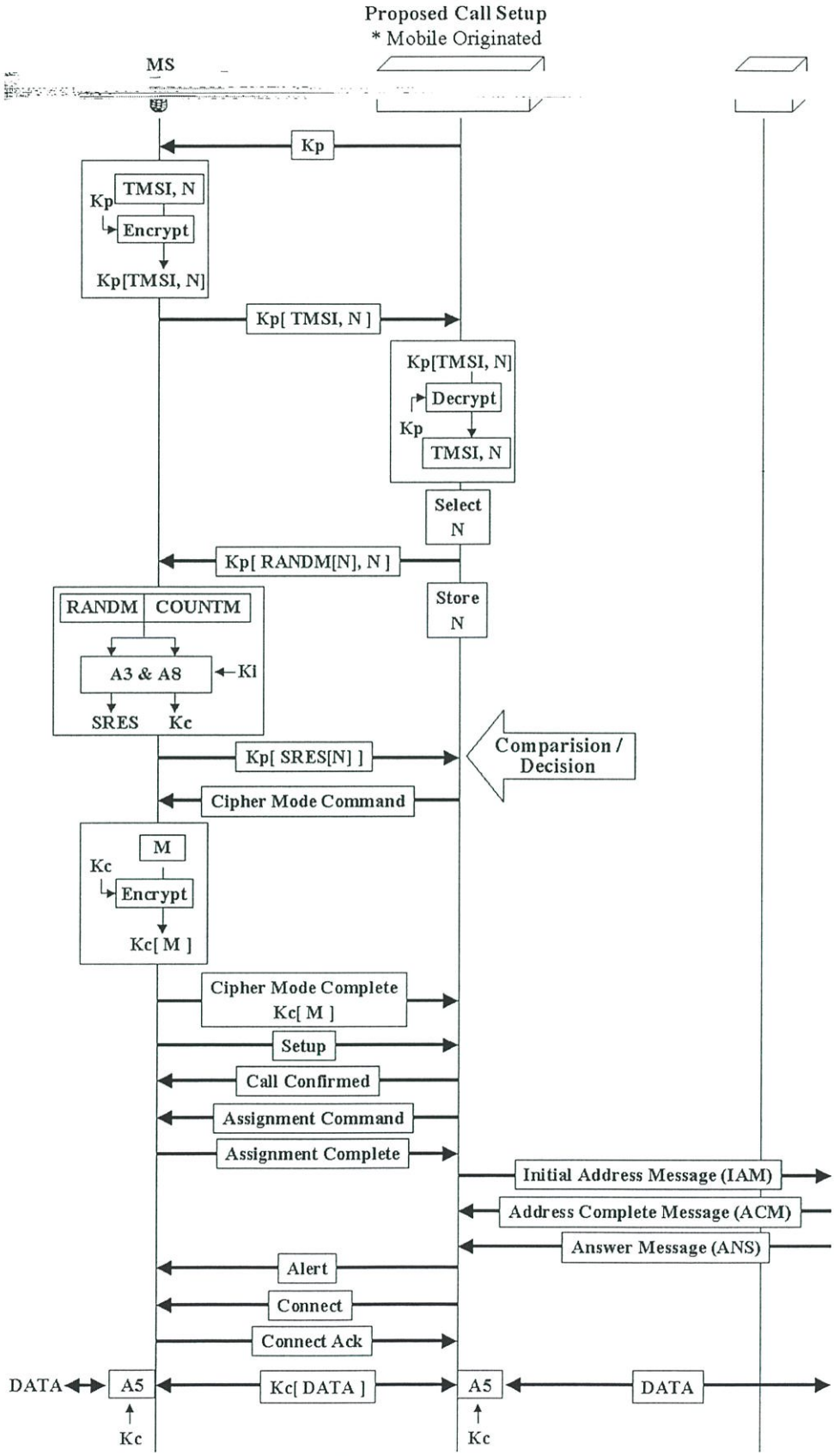
4.3.3.2 โพรโตคอลการโทรศัพท์เข้าที่นำเสนอ (The Proposed Mobile Terminated Protocol)

รายละเอียดของโพรโตคอลการโทรศัพท์เข้าที่นำเสนอดังแสดงในรูปที่ 4.11

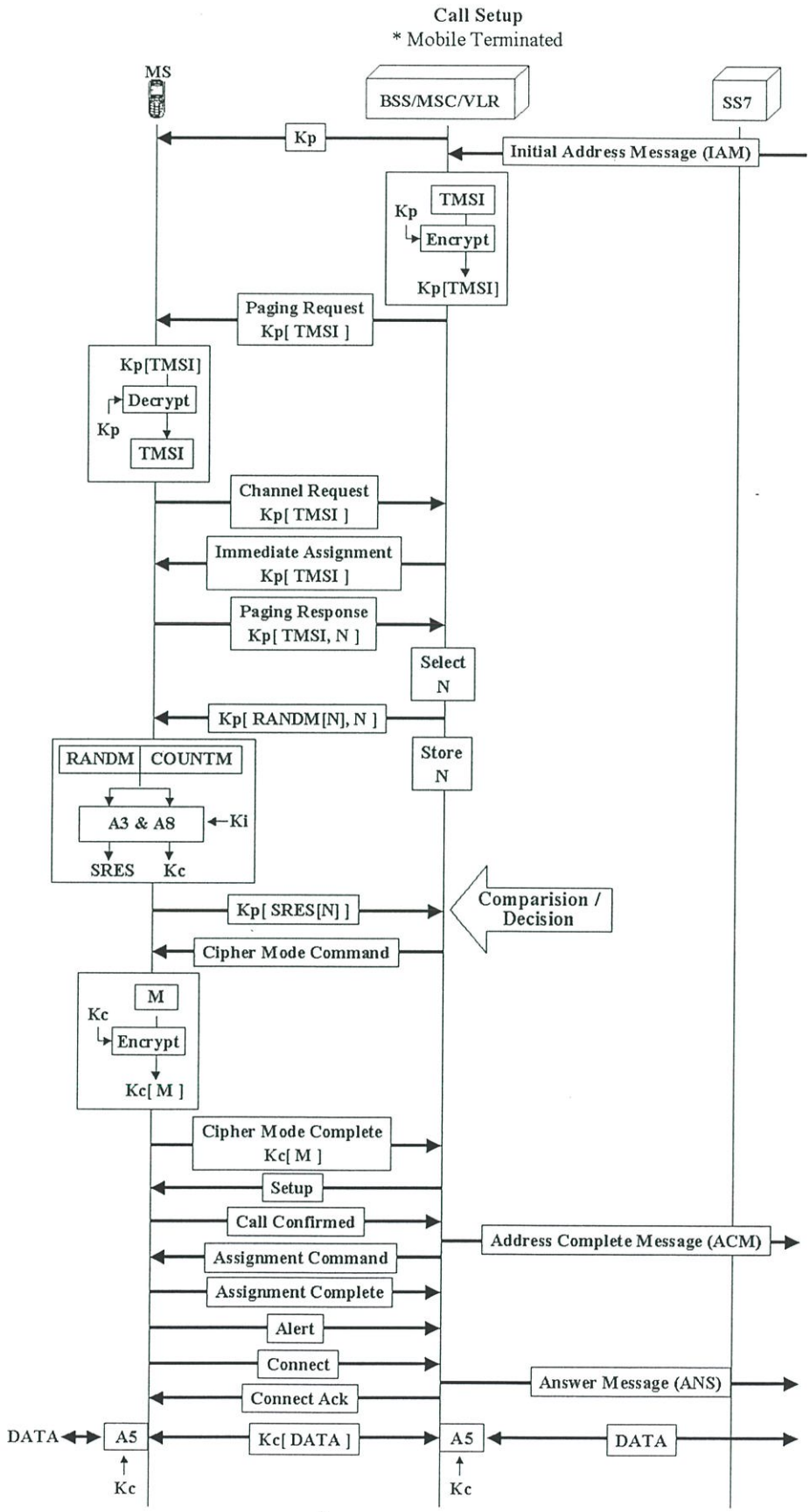
โทรศัพท์เคลื่อนที่หรือเครือข่ายใช้สายอื่นๆจะส่งเมสเสจ IAM เพื่อร้องขอการติดต่อกับผู้ใช้ MSC เมื่อได้รับการร้องขอจะส่ง TMSI เพื่อเรียกผู้ใช้โดยผ่านช่องสัญญาณ PCH โดยข้อมูลที่จะส่งนี้จะถูกเข้ารหัสลับโดยใช้อัลกอริทึมที่นำเสนอกับ Kp ผู้ใช้จะส่ง TMSI โดยผ่านช่องสัญญาณ RACH ให้กับเครือข่ายเพื่อร้องขอการจองช่องสัญญาณ SDCCH เครือข่ายจะส่ง TMSI โดยผ่านช่องสัญญาณ AGCH เพื่อเป็นการกำหนดช่องสัญญาณ SDCCH ให้กับผู้ใช้ ผู้ใช้จะส่ง TMSI และหมายเลขคีย์ (Key Number), N ให้กับ MSC โดยผ่าน BSS เป็นการแจ้งให้ MSC ทราบว่าต้องการจะโทรศัพท์ออก MSC จะทำการสุ่มเลือกหมายเลขคีย์ที่มีค่าตั้งแต่ 0 ถึง n แล้วส่งสมาชิกของอาร์เรย์ RANDM ที่มีดัชนีเท่ากับหมายเลขคีย์ที่สุ่มได้ (N), RANDM[N] และหมายเลขคีย์ที่เลือก ผู้ใช้จะทำการคำนวณหา SRES[N] แล้วส่งกลับให้ VLR เพื่อตรวจสอบเหมือนกับการตรวจสอบผู้ใช้ของโพรโตคอลการโทรศัพท์ออกที่นำเสนอ

MSC จะส่งคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Command) ให้กับผู้ใช้เป็นการแจ้งให้ผู้ใช้ทราบว่าการส่งข้อมูลหลังจากนี้จะเป็นข้อมูลที่ถูกเข้ารหัสลับโดยใช้ Kc ได้จากการตรวจสอบผู้ใช้ MS จะเข้ารหัสลับข้อมูล M ด้วยอัลกอริทึมที่นำเสนอ เพื่อเป็นการตอบรับคำสั่งสภาวะการเข้ารหัสลับ (Cipher Mode Complete) หลังจากนั้นเครือข่ายจะทำการร้องขอการโทรศัพท์เข้าโดยการส่งเมสเสจ Setup ให้กับผู้ใช้ เพื่อแจ้งให้ผู้ใช้ทราบว่าลักษณะของบริการ ถ้าบริการที่ร้องขอมานั้นเหมาะสม ผู้ใช้จะส่งเมสเสจ Call Confirmed ให้กับ MSC เมื่อผู้ใช้ยืนยันการรับโทรศัพท์ MSC จะส่งเมสเสจ ACM ให้กับโทรศัพท์ต้นทางพร้อมทั้งจองช่องสัญญาณในการสื่อสารกับโทรศัพท์ต้นทางให้กับผู้ใช้ หลังจากนั้นเครือข่ายและผู้ใช้จะส่งเมสเสจ Assignment Command กับเมสเสจ Assignment Complete เพื่อหยุดการส่งสัญญาณควบคุมใน SDCCH ผู้ใช้จะส่งเมสเสจ Alert โดยผ่าน FACCH แจ้งให้ MSC ทำการจองช่องสัญญาณ TCH ให้กับผู้ใช้แล้วส่งเมสเสจ

Connect ให้กับเครือข่ายเพื่อแจ้งให้ MSC ทราบว่าพร้อมจะรับบริการ MSC จะส่งเมสเสจ ANS และ Connect Ack ให้กับโทรศัพท์ต้นทางและผู้ใช้ตามลำดับ เพื่อแจ้งให้ทราบว่าสามารถสร้างการติดต่อถูกสร้างเรียบร้อยแล้ว โทรศัพท์ต้นทางก็จะสามารถสื่อสารข้อมูลได้ตามต้องการ



รูปที่ 4.10 โพรโตคอลการทำ Call Setup ที่นำเสนอในกรณี Mobile Originated



รูปที่ 4.11 โพรโตคอลการทำ Call Setup ที่นำเสนอในกรณี Mobile Terminated

4.4 การวิเคราะห์ประสิทธิภาพของอัลกอริทึม

การวิเคราะห์ความปลอดภัยของอัลกอริทึมที่นำเสนอเปรียบเทียบกับอัลกอริทึม A5 ของเครือข่าย GSM การวิเคราะห์แบ่งเป็น 2 ส่วนคือ การวิเคราะห์คีย์ต่อเนื่อง (Key Stream Analysis), การวิเคราะห์ Ciphertext (Ciphertext Analysis), และการวิเคราะห์ค่าใช้จ่ายในการคำนวณ

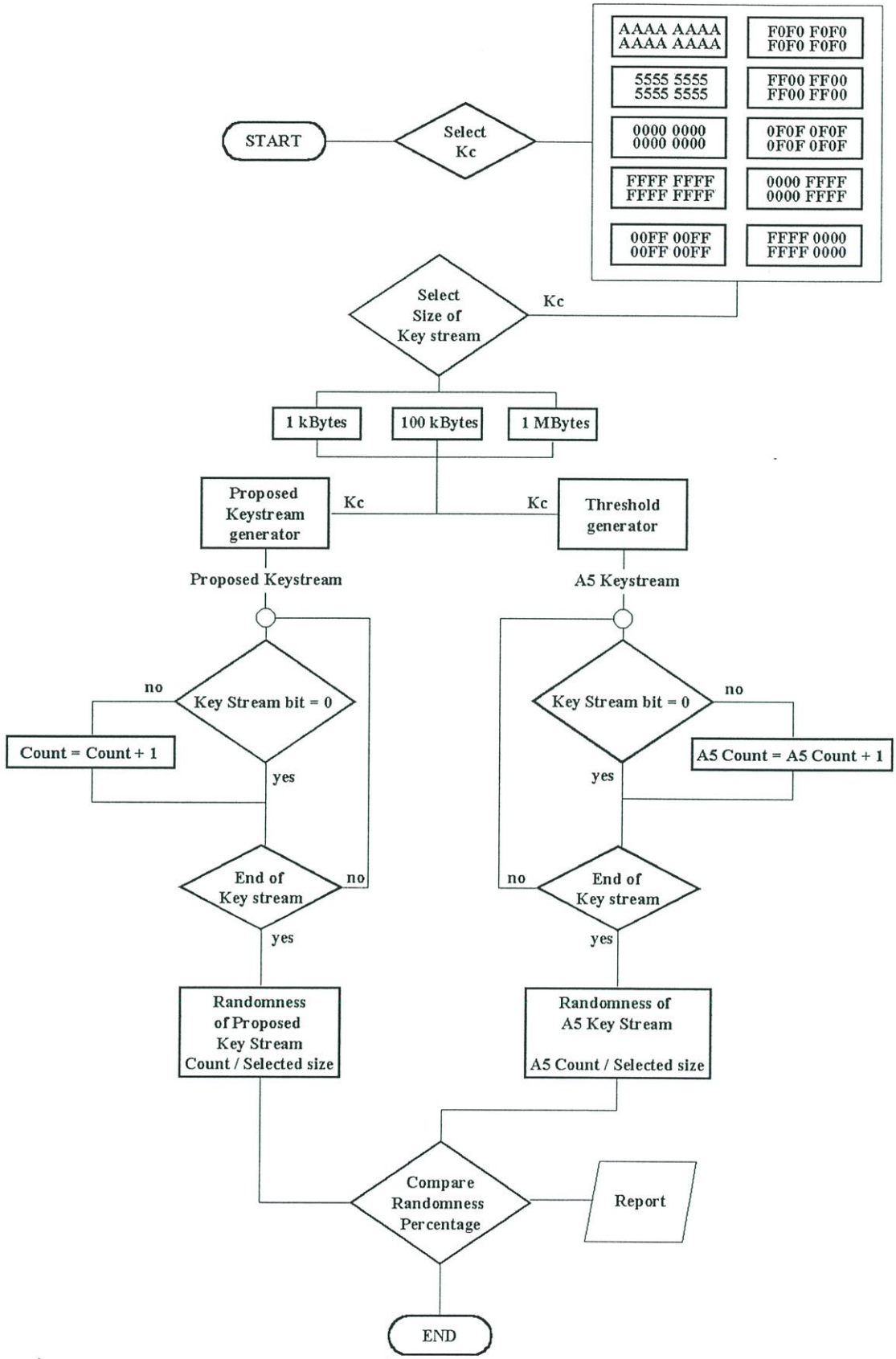
4.4.1 การวิเคราะห์คีย์ต่อเนื่อง (Key Stream Analysis)

สำหรับทั้งอัลกอริทึมที่นำเสนอและอัลกอริทึม A5 ของเครือข่าย GSM นั้นมีการผลิตคีย์ต่อเนื่องแล้วนำคีย์ต่อเนื่องนั้นไป XOR กับ Plaintext เพื่อคำนวณหา Ciphertext เหมือนกัน ดังนั้นการวิเคราะห์ประสิทธิภาพของคีย์ต่อเนื่องจึงเป็นดัชนีตัวหนึ่งที่สามารถใช้วัดประสิทธิภาพของอัลกอริทึมทั้งสองนี้อัลกอริทึมนี้ พารามิเตอร์ที่ถูกเลือกมาใช้วัดความปลอดภัยของคีย์ต่อเนื่องคือ Randomness

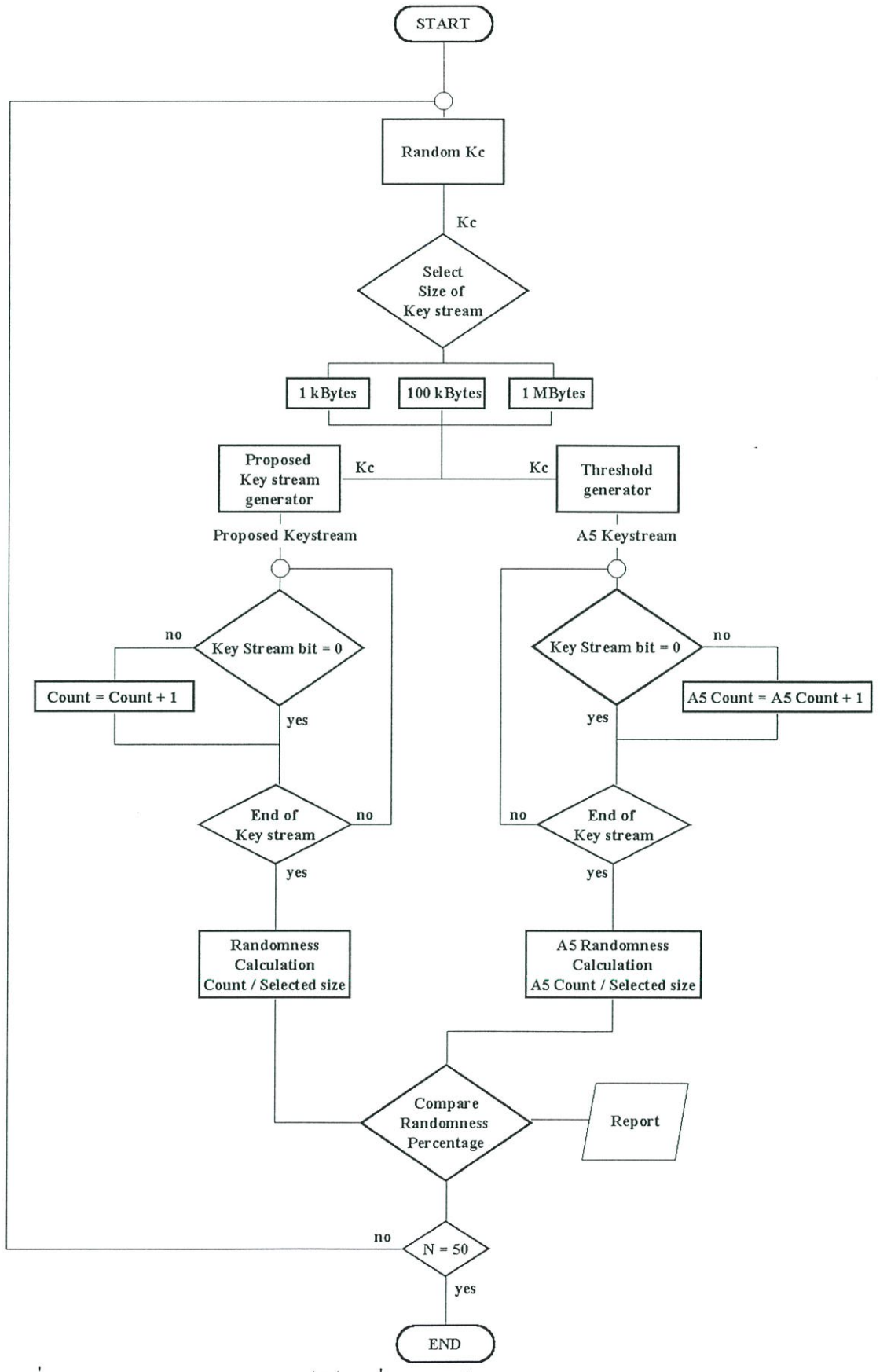
Randomness คือ การที่คีย์ต่อเนื่องมีคุณสมบัติการสุ่ม (Random) เนื่องจากคีย์ต่อเนื่องที่ดีไม่ควรจะสามารถคาดเดาได้ ดังนั้นอัตราส่วนระหว่างบิต 0 และ บิต 1 ของคีย์ต่อเนื่องที่ดีควรจะใกล้เคียง 0.5 มากที่สุดเท่าที่จะเป็นไปได้ [20]

การออกแบบการวิเคราะห์ Randomness นี้จะทำการวิเคราะห์ Randomness ของคีย์ต่อเนื่องของอัลกอริทึมที่นำเสนอเปรียบเทียบกับ Randomness ของคีย์ต่อเนื่องที่ได้จาก Threshold ของอัลกอริทึม A5 การวิเคราะห์จะแบ่งเป็น 2 ส่วนคือการใช้ Kc ที่จากชุด Kc ที่เป็น weak key ดังแสดงในรูปที่ 4.12 และการใช้ Kc ที่จากการสุ่มดังแสดงในรูปที่ 4.13

หลังจากทำการเลือก Kc เรียบร้อยแล้วจะนำ Kc ที่ถูกเลือกนี้ใช้เป็นอินพุตของการผลิตคีย์ต่อเนื่อง จะทำการเลือกขนาดของคีย์ต่อเนื่องที่จะนำมาวิเคราะห์โดยมี 3 ขนาด คือ 1026 ไบต์, 102600 ไบต์, และ 1050624 ไบต์ ทำการผลิตคีย์ต่อเนื่องตามขนาดที่เลือกแล้วนำคีย์ต่อเนื่องที่ผลิตได้นี้นับจำนวน บิต 1 ของคีย์ต่อเนื่อง แล้วนำจำนวนบิต 1 ไปคำนวณหาเปอร์เซ็นต์ของบิต 1 ใช้เป็นพารามิเตอร์ในการวิเคราะห์ Randomness ในส่วนของการวิเคราะห์ Randomness โดยใช้ Kc จากการสุ่มนั้นจะทำการสุ่ม Kc ทั้งหมด 50 รอบ



รูปที่ 4.12 Flow Chart การวิเคราะห์คีย์ต่อเนื่องโดยใช้ Kc จากกลุ่ม Weak Key



รูปที่ 4.13 Flow Chart การวิเคราะห์คีย์ต่อเนื่องโดยใช้ Kc จากการสุ่ม

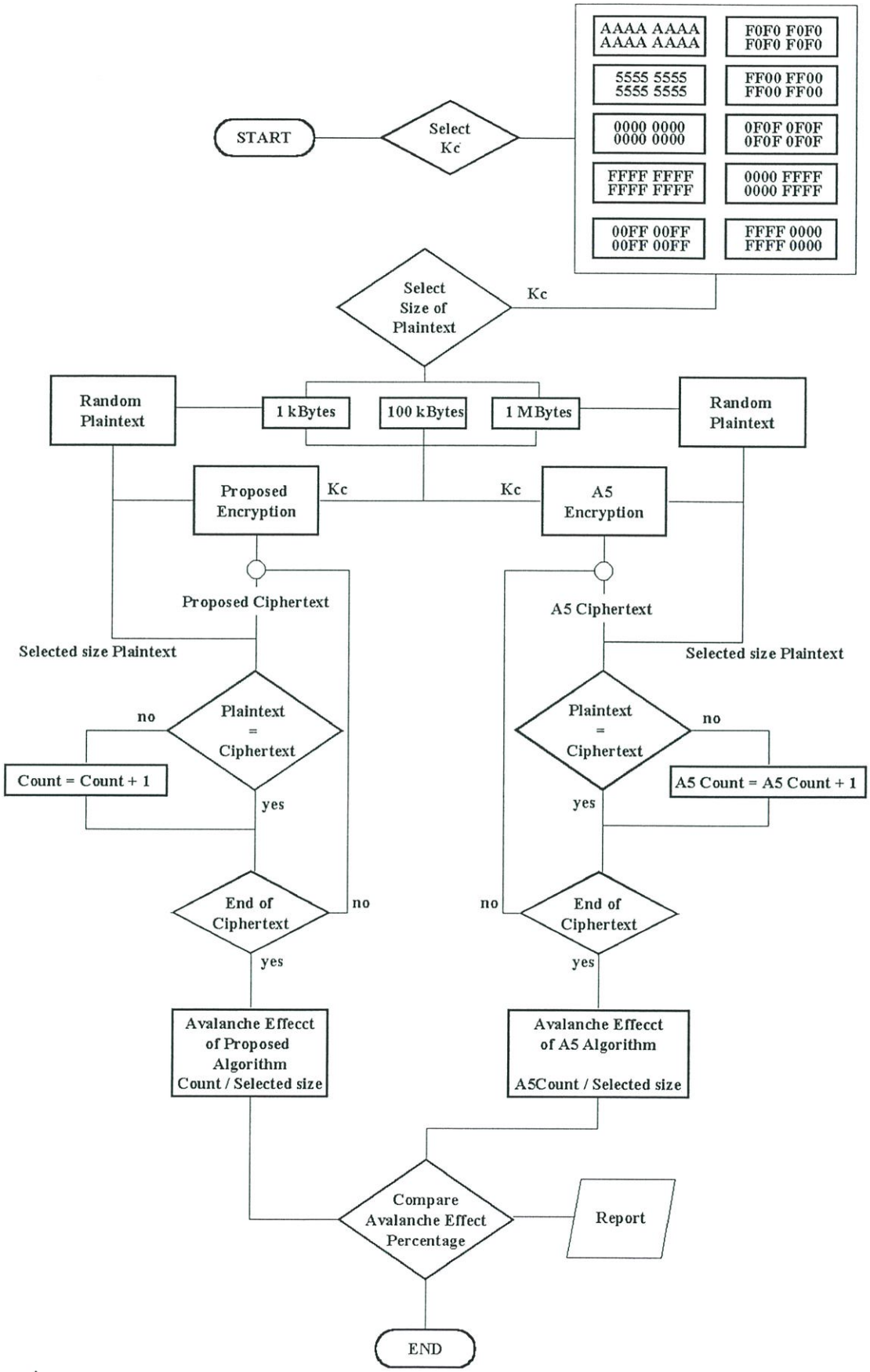
4.4.2 การวิเคราะห์ Ciphertext (Ciphertext Analysis)

Ciphertext คือ ข้อมูลที่จะถูกเข้ารหัสลับแล้วส่งผ่านช่องสัญญาณวิทยุเพื่อปกปิดเนื้อหาสารที่ผู้ใช้ต้องการจะส่งจริงๆ ดังนั้น Ciphertext ควรจะต้องมีลักษณะเปลี่ยนไปจาก Plaintext มากที่สุดทำที่จะเป็นไปได้ ในการวิเคราะห์ความปลอดภัยของอัลกอริทึมที่ใช้เข้ารหัสลับข้อมูลนั้น Ciphertext ของอัลกอริทึมการเข้ารหัสลับเป็นดัชนีอีกหนึ่งที่ใช้ในการวัดประสิทธิภาพของอัลกอริทึมการเข้ารหัสลับ พารามิเตอร์ที่ถูกเลือกใช้ในการวัดคุณภาพของ Ciphertext ในงานวิจัยนี้คือ Avalanche Effect

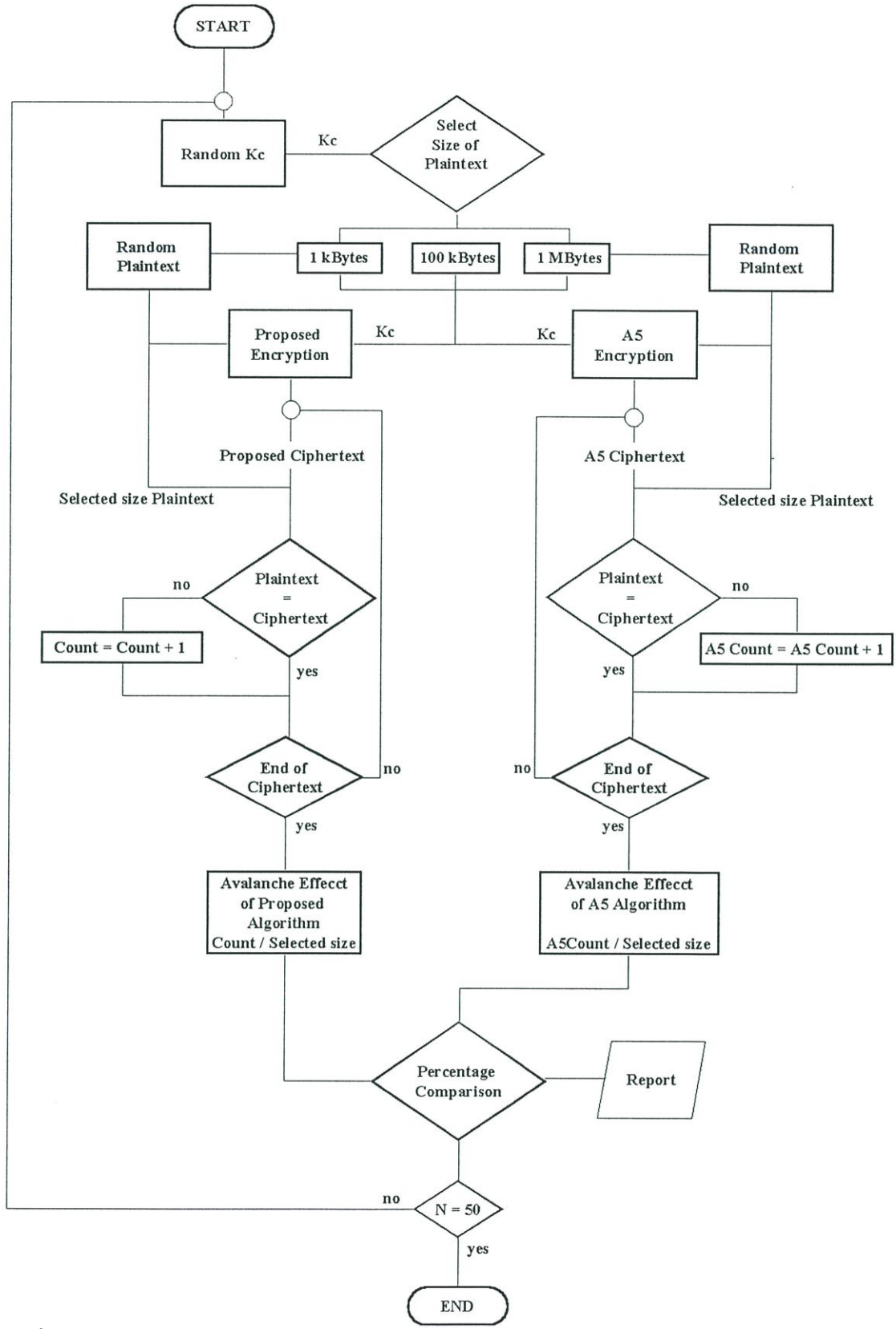
Avalanche Effect คือ ปรากฏการณ์ที่ค่าของบิตในข้อมูลชุดหนึ่งเปลี่ยนไปจากเดิมเมื่อนำชุดนั้นผ่านกระบวนการเข้ารหัสลับ [6]

การออกแบบการวิเคราะห์ Avalanche Effect นี้จะทำการวิเคราะห์ Avalanche Effect ของอัลกอริทึมที่นำเสนอเปรียบเทียบกับ Avalanche Effect ของอัลกอริทึม A5 การวิเคราะห์จะแบ่งเป็น 2 ส่วนคือการใช้ Kc ที่จากชุด Kc ที่เป็น Weak Key ดังแสดงในรูปที่ 4.14 และการใช้ Kc ที่จากการสุ่มดังแสดงในรูปที่ 4.15

หลังจากทำการเลือก Kc เรียบร้อยแล้วจะนำ Kc ที่ถูกเลือกนี้ใช้เป็นอินพุตของการผลิตคีย์ต่อเนื่อง จะทำการเลือกขนาดของคีย์ต่อเนื่องที่จะนำมาวิเคราะห์โดยมี 3 ขนาด คือ 1026 ไบต์, 102600 ไบต์, และ 1050624 ไบต์ ทำการผลิตคีย์ต่อเนื่องตามขนาดที่เลือกแล้วทำการสุ่มเลือก Plaintext ตามขนาดของคีย์ต่อเนื่องเช่นกัน นำคีย์ต่อเนื่องที่ผลิตได้ XOR กับ Plaintext แล้วคำนวณหาว่าจำนวนบิตที่เปลี่ยนไประหว่าง Plaintext กับ Ciphertext แล้วนำไปคำนวณหาเปอร์เซ็นต์ของบิตที่เปลี่ยนไปนี้ใช้เป็นพารามิเตอร์ในการวิเคราะห์ Avalanche Effect ในส่วนของการวิเคราะห์ Avalanche Effect โดยใช้ Kc จากการสุ่มนั้นจะทำการสุ่ม Kc ทั้งหมด 50 รอบ



รูปที่ 4.14 Flow Chart การวิเคราะห์ Ciphertext โดยใช้ Kc จากกลุ่ม Weak Key



รูปที่ 4.15 Flow Chart การวิเคราะห์ Ciphertext โดยใช้ Kc จากการสุ่ม

4.4.3 การวิเคราะห์ค่าใช้จ่ายการเข้ารหัสลับ

การวิเคราะห์ค่าใช้จ่ายการเข้าและถอดรหัสลับของอัลกอริทึมที่นำเสนอเปรียบเทียบกับอัลกอริทึม A5 ของ GSM นั้นจะต้องพิจารณาขนาดของข้อมูลที่จะนำมาวิเคราะห์ให้เหมาะสมเนื่องจากอัลกอริทึมทั้งสองอัลกอริทึมนี้มีลักษณะการเข้ารหัสลับที่แตกต่างกัน โดยอัลกอริทึม A5 นั้นเข้ารหัสลับข้อมูลรอบละ 114 บิต ส่วนอัลกอริทึมที่นำเสนอนั้นจะทำการผลิตคีย์ต่อเนื่องครั้งละ 8 บิต จึงจำเป็นที่จะต้องเลือกขนาดของข้อมูลที่จะใช้ให้เหมาะสม เช่น จำนวนผลคูณของ 114 กับ 8 เป็นต้น การวิเคราะห์ค่าใช้จ่ายการเข้าและถอดรหัสลับกำหนดเป็นสมการต่างๆดังนี้

$$C_{wos} = \frac{8(D + \frac{D}{456}H)}{R_b} \tag{4.1}$$

$$C_{proposed} = \frac{8(D + \frac{D}{456}H)}{R_b} + \frac{8(D + \frac{D}{456}H)T_{Proposed}}{64} \tag{4.2}$$

$$C_{A5} = \frac{8(D + \frac{D}{456}H)}{R_b} + \frac{8(D + \frac{D}{456}H)T_{A5}}{114} \tag{4.3}$$

เมื่อ C_{wos} คือ ค่าใช้จ่ายที่เกิดขึ้นเมื่อไม่มีการเข้ารหัสลับข้อมูล (หน่วยเป็น Sec)

$C_{Proposed}$ คือ ค่าใช้จ่ายของการเข้ารหัสลับด้วยอัลกอริทึมที่นำเสนอ (หน่วยเป็น Sec)

C_{A5} คือ อัตราเร็วในการสื่อสารข้อมูลระหว่าง MS และ VLR (Sec/bit)

$T_{Proposed}$ คือ เวลาที่ใช้ในการเข้ารหัสลับข้อมูล 64 บิตของอัลกอริทึมที่นำเสนอ (Sec)

T_{A5} คือ เวลาที่ใช้ในการเข้ารหัสลับข้อมูล 114 บิตของอัลกอริทึม A5 (Sec)

R_b คือ อัตราเร็วในการสื่อสาร (bps)

D คือ ขนาดของข้อมูล (ไบต์)

H คือ ขนาดของ Header (ไบต์)

4.5 แบบจำลองวิเคราะห์ค่าใช้จ่ายของการตรวจสอบผู้ใช้

แบบจำลองวิเคราะห์ค่าใช้จ่ายของผู้ใช้ในเครือข่ายถูกสร้างขึ้นเพื่อคำนวณค่าใช้จ่ายที่ใช้เมื่อมีการตรวจสอบผู้ใช้ (Authentication) ในโพรโตคอลที่นำเสนอโดยเปรียบเทียบกับการตรวจสอบผู้ใช้ในโพรโตคอลของ GSM จะพบว่าสำหรับการตรวจสอบผู้ใช้ในโพรโตคอลต่างๆ จะมีการตรวจ

สอบผู้ใช้อยู่ 3 แบบที่แตกต่างกันคือ การตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Registration, การตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Updating ในกรณีที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC เดิม, และการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Updating ในกรณีที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC ใหม่ ส่วนการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Call Setup นั้นจะมีการตรวจสอบผู้ใช้เหมือนกับการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Updating

4.5.1 การเปรียบเทียบค่าใช้จ่ายการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Registration

ค่าใช้จ่ายของโพรโตคอลการทำ Location Registration ของโพรโตคอลที่นำเสนอดังแสดงในสมการที่ 4.4 และค่าใช้จ่ายของโพรโตคอลการทำ Location Registration ของ GSMดังแสดงในสมการที่ 4.5

$$C_{Auth}^{Proposed} = \begin{cases} 240A + 352T_{crypt} + T_{randm} + T_{Secure}^{Proposed} & ;(4.6) \\ 136A + 2688B + 144T_{crypt} + T_{randm} + T_{Secure}^{Proposed} & \text{elsewhere} \end{cases} \quad (4.4)$$

$$C_{Auth}^{GSM} = 240A + 3172B + T_{rand} + T_{Secure}^{GSM} \quad (4.5)$$

$$104A + 108T_{crypt} \geq 2688B \quad (4.6)$$

เมื่อ $C_{Auth}^{Proposed}$ คือ ค่าใช้จ่ายในการตรวจสอบผู้ใช้ที่นำเสนอ (หน่วยเป็น Sec)

C_{Auth}^{GSM} คือ ค่าใช้จ่ายในการตรวจสอบผู้ใช้ที่นำเสนอ (Sec)

A คือ อัตราเร็วในการสื่อสารข้อมูลระหว่าง MS และ VLR (Sec/bit)

B คือ อัตราเร็วในการสื่อสารข้อมูลระหว่าง VLR และ HLR (Sec/bit)

T_{crypt} คือ อัตราเร็วในการเข้าและถอดรหัสลับของอัลกอริทึมที่นำเสนอ (Sec/bit)

$T_{Secure}^{Proposed}$ คือ เวลาที่ใช้ในการคำนวณ COUNTM และทำการผลิต SRES และ Kc (Sec)

T_{Secure}^{GSM} คือ เวลาที่ใช้ในการคำนวณหา SRES และ Kc (Sec)

T_{rand} คือ เวลาที่ใช้ในการผลิต RAND ขนาด 128 บิต (Sec)

T_{randm} คือ เวลาที่ใช้ในการผลิต RANDM ขนาด 64 บิต (Sec)

ในการคำนวณหาเวลาที่ใช้ในการตรวจสอบผู้ใช้จะทำการนำขนาดของข้อมูลที่ใช้สื่อสาร ดังแสดงในตารางที่ 4.1 คูณกับอัตราเร็วในการสื่อสารซึ่งแบ่งเป็น 2 ช่วงดังแสดงในสมการที่ 4.5 และ 4.6 ภายในสมการที่ 4.5 จะแบ่งเป็น 2 กรณีเนื่องจากมีการส่งข้อมูลออกไปพร้อมกันทั้ง 2 ทาง ในการคำนวณจะนำค่าใช้จ่ายของฝั่งที่ใช้เวลามากกว่ามาคำนวณเป็นค่าใช้จ่ายของการตรวจสอบผู้ใช้ [21]

ตารางที่ 4.1 ขนาดของข้อมูลในโพรโตคอลต่างๆ

ชนิดของข้อมูล	ขนาดของข้อมูล	ชนิดของข้อมูล	ขนาดของข้อมูล
IMSI	64 บิต	SRES[N]	32 บิต
TMSI	32 บิต	N	8 บิต
LAI	40 บิต	RAND[n]	128n บิต
RAND[N]	128 บิต	RANDM[n]	64n บิต
RANDM[N]	64 บิต	SRES[n]	32n บิต

4.5.2 การเปรียบเทียบค่าใช้จ่ายการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Updating

สำหรับการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Updating ในกรณีที่อยู่ในพื้นที่การจัดการของ MSC เดิมซึ่งมีค่าใช้จ่ายดังแสดงในสมการที่ 4.7 และสมการที่ 4.8 โดยสมการที่ 4.4 เป็นค่าใช้จ่ายของโพรโตคอลที่นำเสนอ ส่วนสมการที่ 4.7 เป็นค่าใช้จ่ายของโพรโตคอลของ GSM

$$C_{Auth}^{Proposed} = 248A + 368T_{crypt} + T_{Secure}^{Proposed} \tag{4.7}$$

$$C_{Auth}^{GSM} = 248A + T_{Secure}^{GSM} \tag{4.8}$$

สำหรับการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Updating ในกรณีที่อยู่ในพื้นที่การจัดการของ MSC ใหม่ซึ่งมีค่าใช้จ่ายดังแสดงในสมการที่ 4.9 และสมการที่ 4.10 โดยสมการที่ 4.9 เป็นค่าใช้จ่ายของโพรโตคอลที่นำเสนอ ส่วนสมการที่ 4.10 เป็นค่าใช้จ่ายของโพรโตคอลของ GSM

$$C_{Auth}^{Proposed} = 248A + 2720B + 368T_{crypt} + T_{Secure}^{Proposed} \tag{4.9}$$

$$C_{Auth}^{GSM} = 248A + 3712B + T_{Secure}^{GSM} \quad (4.10)$$

สำหรับค่าใช้จ่ายการตรวจสอบผู้ใช้ของโพรโตคอลการทำ Call Setup ทั้งในแบบ Mobile Originated และ Mobile Terminated นั้นมีค่าใช้จ่ายเหมือนกับการตรวจสอบผู้ใช้ในโพรโตคอลการทำ Location Updating ในกรณีที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC เดิม เนื่องจากมีการตรวจสอบใช้ในลักษณะเดียวกัน

บทที่ 5

ผลการทดลอง

ในบทนี้เป็นผลการทดลองวัดประสิทธิภาพและค่าใช้จ่ายที่เกิดขึ้นเมื่อใช้วิธีการรักษาความปลอดภัยที่นำเสนอและเปรียบเทียบกับวิธีการรักษาความปลอดภัยแบบเดิมของเครือข่าย GSM

5.1 ประสิทธิภาพของอัลกอริทึมที่นำเสนอ

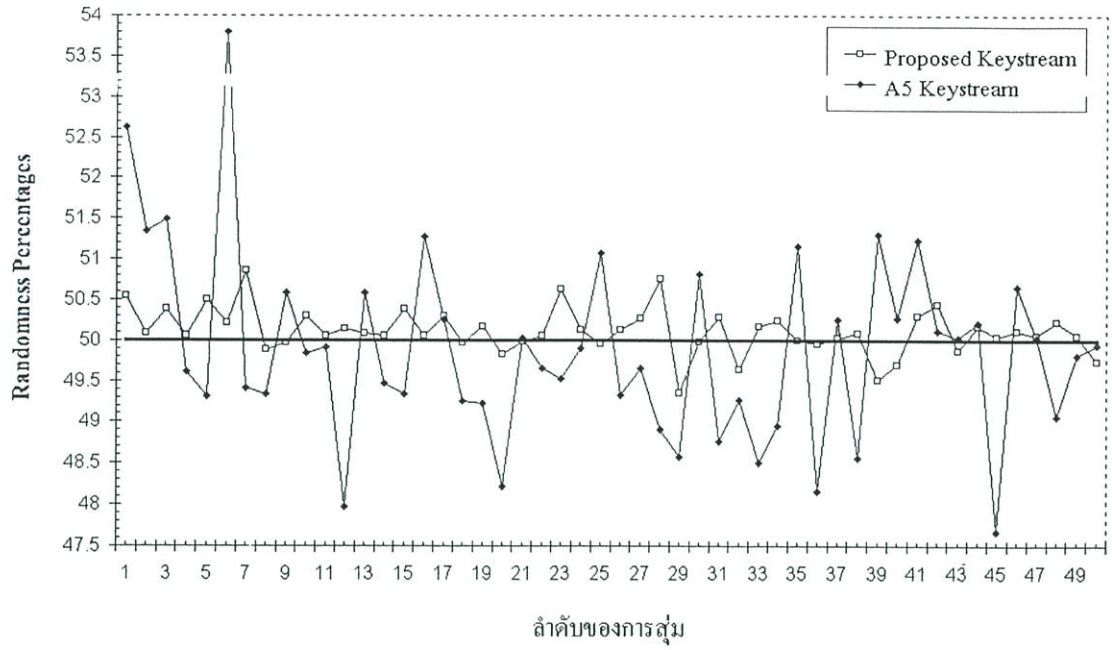
การทดลองวิเคราะห์ความปลอดภัยของอัลกอริทึมที่นำเสนอเปรียบเทียบกับอัลกอริทึม A5 ของ GSM แบ่งผลการทดลองออกเป็น 2 ส่วนคือ การคำนวณคุณสมบัติ Randomness ของคีย์ต่อเนื่องและการคำนวณคุณสมบัติ Avalanche Effect ของ Ciphertext

5.1.1 ผลการคำนวณหาคุณสมบัติ Randomness ของคีย์ต่อเนื่อง

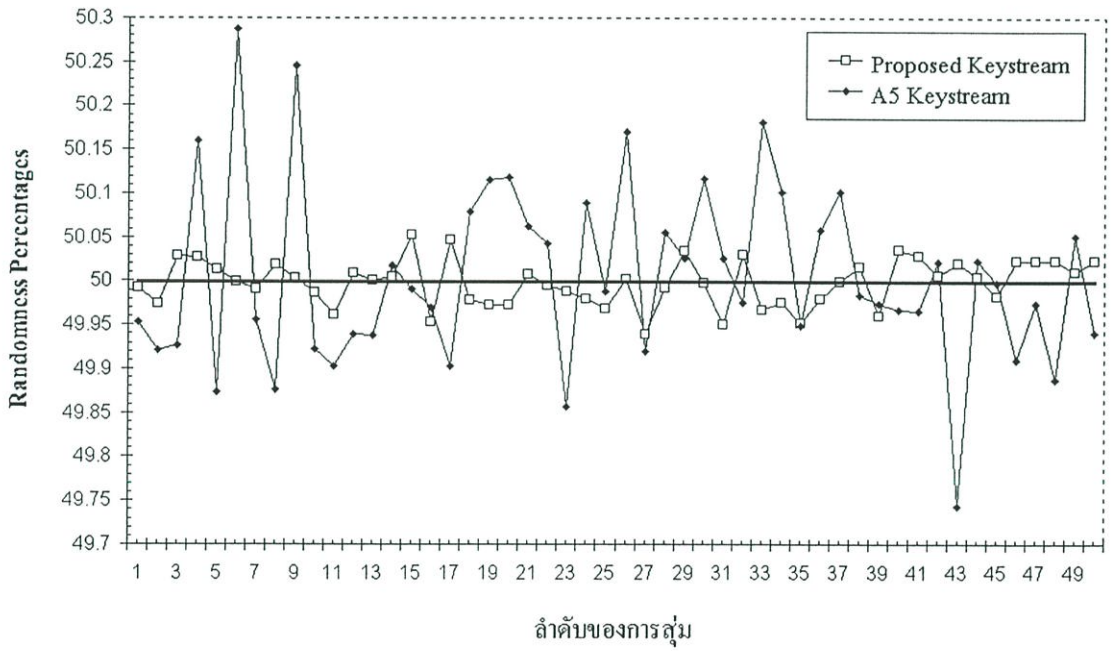
การคำนวณหาคุณสมบัติ Randomness ของคีย์ต่อเนื่องที่ได้จากอัลกอริทึมที่นำเสนอเปรียบเทียบกับคีย์ต่อเนื่องที่ได้จาก Threshold Generator ของอัลกอริทึม A5 นั้นจะแบ่งได้เป็น 2 ส่วนตามลักษณะการได้มาซึ่ง Kc คีย์ที่ใช้ในการเข้ารหัสลับข้อมูล คือ ส่วนแรกเป็นการสุ่มเลือก Kc ขึ้นมา และในส่วนที่ 2 เป็นการใช้ Kc ที่เป็น Weak Key

5.1.1.1 Randomness เมื่อใช้ Kc จากการสุ่ม

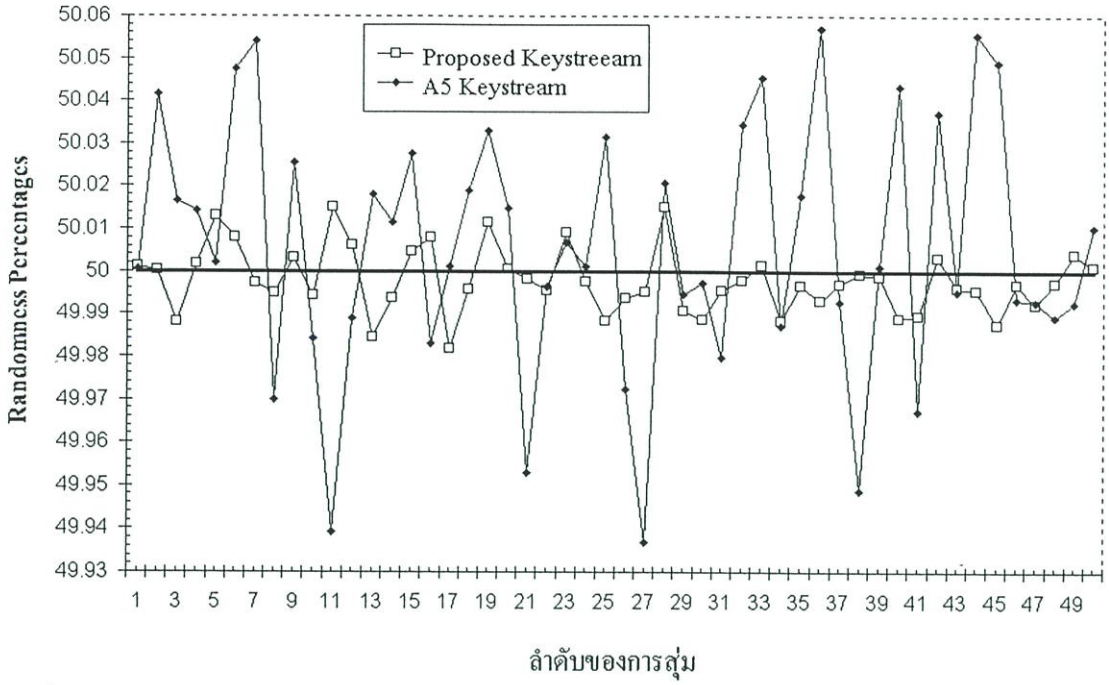
จากการสุ่มค่าของ Kc ขนาด 64 บิตจำนวน 50 ค่าแล้วนำค่า Kc ที่ได้จากการสุ่มนี้ไปคำนวณหาคีย์ต่อเนื่องโดยใช้อัลกอริทึมที่นำเสนอและ Threshold Generator ของอัลกอริทึม A5 โดยขนาดของคีย์ต่อเนื่องจะทำการผลิตเป็น 3 ขนาดคือ 1026 ไบต์, 102600 ไบต์, และ 1050624 ไบต์ ผลการคำนวณหา Randomness ของคีย์ต่อเนื่องทั้งสองอัลกอริทึมดังแสดงในรูปที่ 5.1, 5.2, และ 5.3 ตามลำดับ



รูปที่ 5.1 กราฟเปรียบเทียบ Randomness ของคีย์ต่อเนื่องขนาด 1026 ไบต์เมื่อใช้ Kc จากการสุ่ม



รูปที่ 5.2 กราฟเปรียบเทียบ Randomness ของคีย์ต่อเนื่องขนาด 102600 ไบต์เมื่อใช้ Kc จากการสุ่ม



รูปที่ 5.3 กราฟเปรียบเทียบ Randomness ของคีย์ต่อเนื่องขนาด 1050624 ไบต์เมื่อใช้ Kc จากการสุ่ม

เมื่อนำค่าเปอร์เซ็นต์ของการ Randomness ของทั้งสองอัลกอริทึมในแต่ละขนาดมาทำการหาค่าทางสถิติพื้นฐานคือ ค่าเฉลี่ย, ความแปรปรวน, และส่วนเบี่ยงเบนมาตรฐาน จะได้ผลการคำนวณดังแสดงตารางที่ 5.1, 5.2, และ 5.3

ตารางที่ 5.1 การคำนวณหาค่าทางสถิติของ Randomness สำหรับคีย์ต่อเนื่องขนาด 1026 ไบต์โดยใช้ Kc จากการสุ่ม

พารามิเตอร์ทางสถิติ	Randomness ของคีย์ต่อเนื่องขนาด 1026 ไบต์			
	Proposed Key Stream		A5 Key Stream	
	bit 1	Percentage	bit 1	Percentage
ค่าเฉลี่ย	4113.18	50.111842	4095.5	49.884259
ความแปรปรวน	522.2276	0.0775149	8893.69	1.3202014
ส่วนเบี่ยงเบนมาตรฐาน	22.8523	0.278415	94.30636	1.1489567

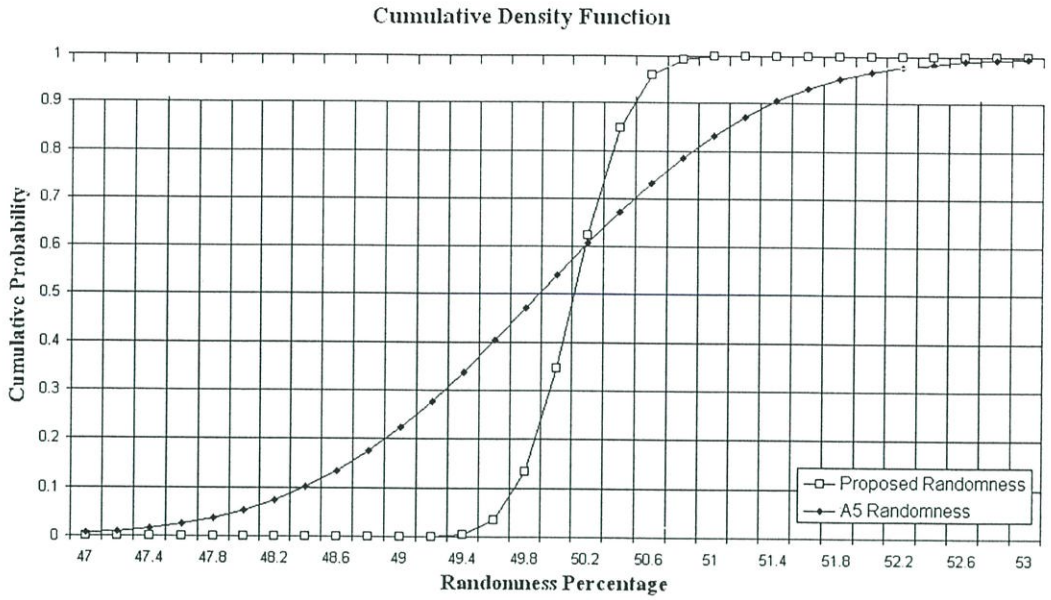
ตารางที่ 5.2 การคำนวณหาค่าทางสถิติของ Randomness สำหรับคีย์ต่อเนื่องขนาด 102600 ไบต์โดยใช้ Kc จากการสุ่ม

พารามิเตอร์ทางสถิติ	Randomness ของคีย์ต่อเนื่องขนาด 102600 ไบต์			
	Proposed Key Stream		A5 Key Stream	
	bit 1	Percentage	bit 1	Percentage
ค่าเฉลี่ย	410387.2	49.998187	410441.4	50.005044
ความแปรปรวน	47890.48	0.0006954	709157.6	0.0105261
ส่วนเบี่ยงเบนมาตรฐาน	218.8389	0.0263696	842.115	0.1025969

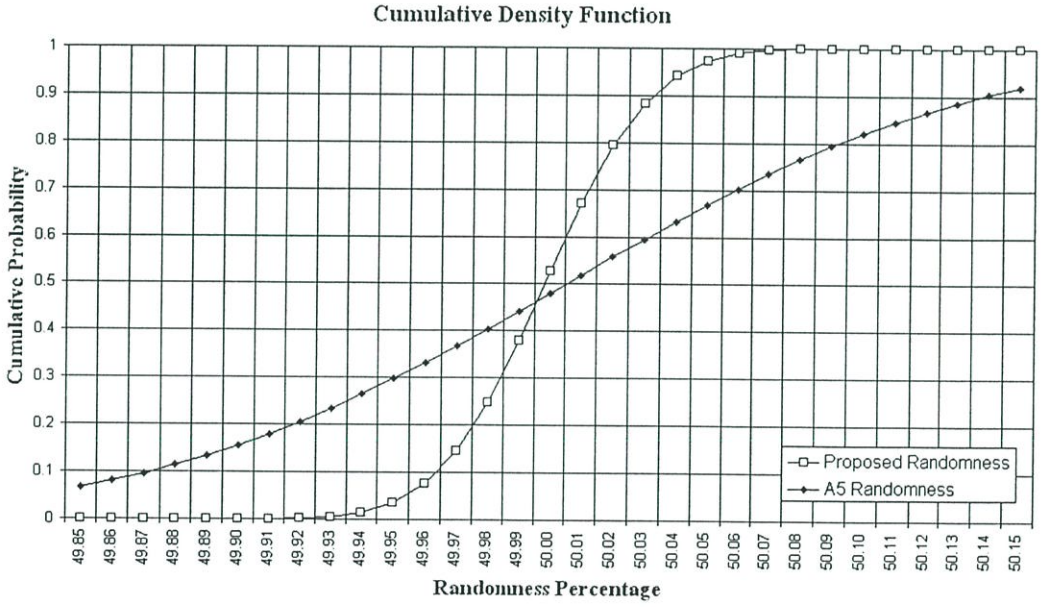
ตารางที่ 5.3 การคำนวณหาค่าทางสถิติของ Randomness สำหรับคีย์ต่อเนื่องขนาด 1050426 ไบต์โดยใช้ Kc จากการสุ่ม

พารามิเตอร์ทางสถิติ	Randomness ของคีย์ต่อเนื่องขนาด 1050624 ไบต์			
	Proposed Key Stream		A5 Key Stream	
	bit 1	Percentage	bit 1	Percentage
ค่าเฉลี่ย	4202317.74	49.997879	4202987.94	50.005853
ความแปรปรวน	407405.35	5.76701E-5	6109465.57	0.0008648
ส่วนเบี่ยงเบนมาตรฐาน	138.2831	0.0075941	2471.733	0.0294079

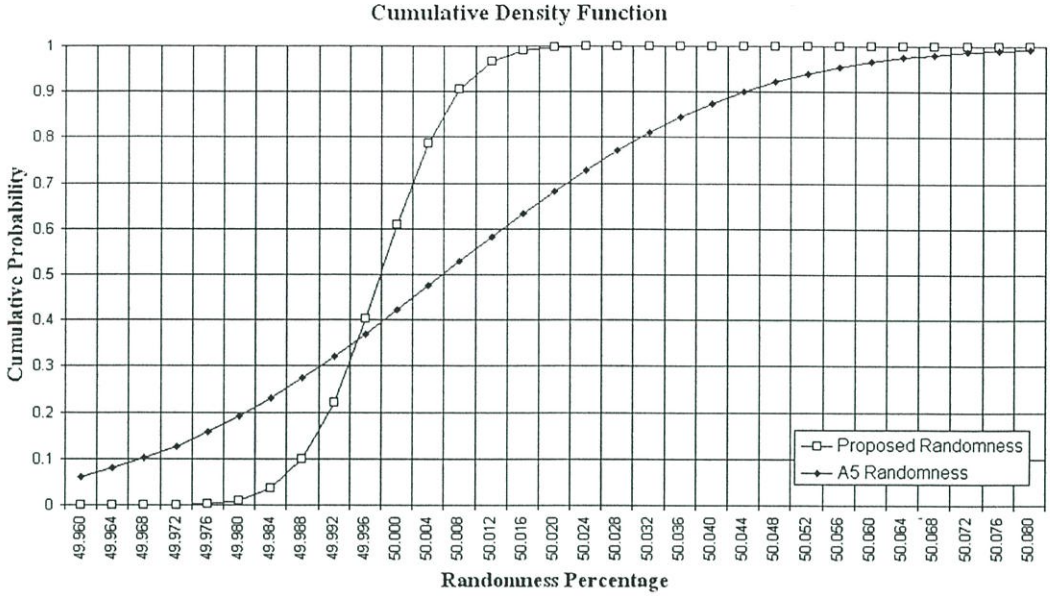
จากข้อมูลที่ได้รับจากกราฟและตารางทั้ง 3 นี้เมื่อนำค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของข้อมูล 1026 ไบต์, 102600 ไบต์, และ 1050624 ไบต์ มาพิจารณาเป็นกราฟการแจกแจงแบบปกติสะสมดังแสดงในรูปที่ 5.4, 5.5, และ 5.6 ตามลำดับ จะเห็นได้ว่าเมื่อพิจารณาค่าเฉลี่ยของเปอร์เซ็นต์ Randomness ของคีย์ต่อเนื่องทั้งสองอัลกอริทึมนี้จะมีความแตกต่างไม่มากนัก แต่เมื่อพิจารณาความแปรปรวนและส่วนเบี่ยงเบนมาตรฐาน ผลลัพธ์ข้อมูลการ Randomness ของคีย์ต่อเนื่องที่ได้รับจาก Threshold Generator จะมีค่าความแปรปรวนและส่วนเบี่ยงเบนมาตรฐานสูงกว่าผลลัพธ์ข้อมูลการ Randomness ของคีย์ต่อเนื่องที่ได้รับจากอัลกอริทึมที่นำเสนอค่อนข้างมาก ทำให้กราฟของคีย์ต่อเนื่องของ Threshold Generator นั้นมีเปอร์เซ็นต์ของ Randomness ห่างจาก 50% มากกว่าคีย์ต่อเนื่องที่นำเสนอ



รูปที่ 5.4 กราฟการแจกแจงแบบปกติสะสมของ Randomness สำหรับคีย์ต่อเนื่องขนาด 1026 ไบต์



รูปที่ 5.5 กราฟการแจกแจงแบบปกติสะสมของ Randomness สำหรับคีย์ต่อเนื่องขนาด 102600 ไบต์



รูปที่ 5.6 กราฟการแจกแจงแบบปกติสะสมของ Randomness สำหรับคีย์ต่อเนื่องขนาด 1050624 ไบต์

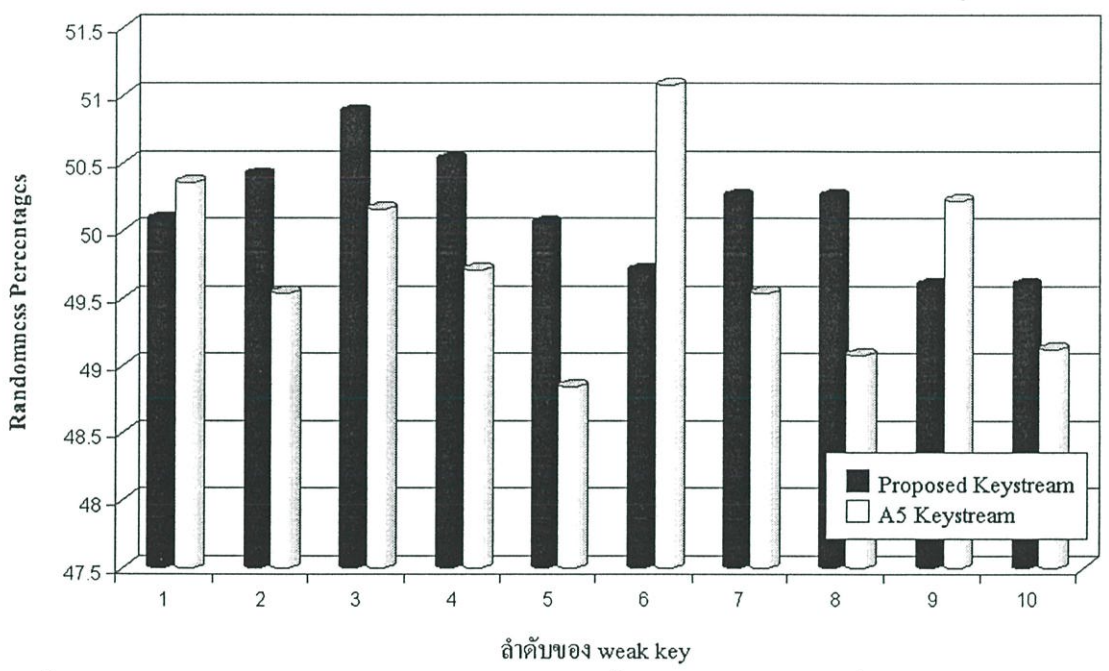
ตารางที่ 5.4 ลำดับของบิตในกลุ่มของ Weak Key

ลำดับ Weak Key	ลำดับของบิตขนาด 64 บิต (เลขฐาน 16)
1	0xAAAA AAAA AAAA AAAA
2	0x5555 5555 5555 5555
3	0x0000 0000 0000 0000
4	0xFFFF FFFF FFFF FFFF
5	0x00FF 00FF 00FF 00FF
6	0xF0F0 F0F0 F0F0 F0F0
7	0xFF00 FF00 FF00 FF00
8	0x0F0F 0F0F 0F0F 0F0F
9	0x0000 FFFF 0000 FFFF
10	0xFFFF 0000 FFFF 0000

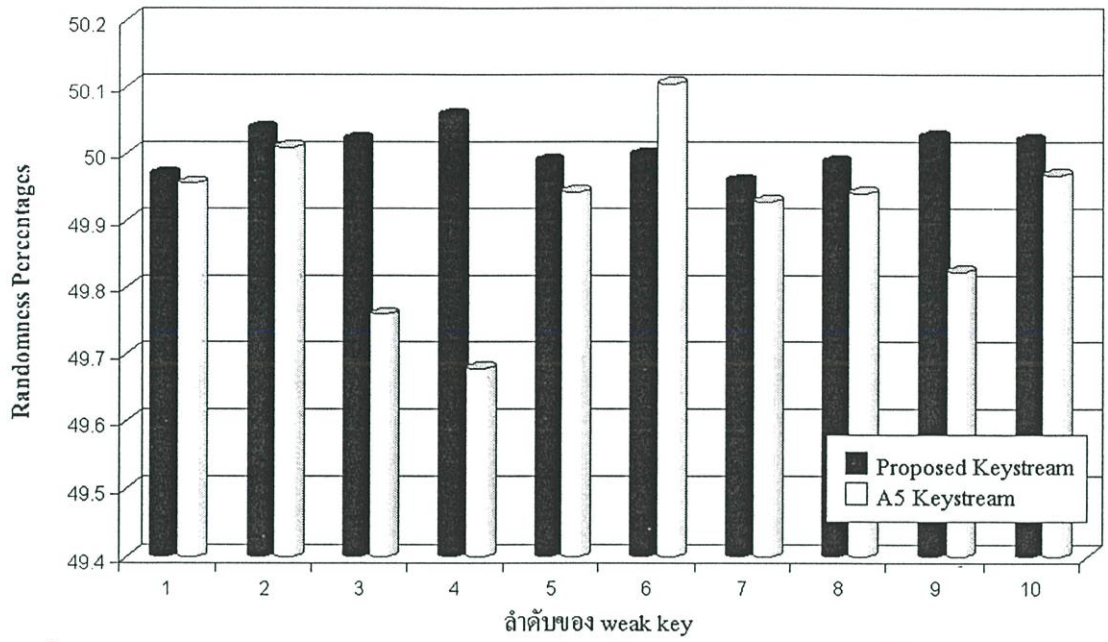
5.1.1.2 Randomness เมื่อใช้ Kc จากกลุ่ม Weak Key

ในการทดลองนี้นำ Kc จากกลุ่ม Weak Key ในตารางที่ 5.4 มาคำนวณหาคีย์ต่อเนื่องโดยใช้อัลกอริทึมที่นำเสนอและ Threshold Generator เพื่อคำนวณหาประสิทธิภาพของอัลกอริทึมว่ามีประสิทธิภาพเพียงไร เมื่อใช้คีย์ในการเข้ารหัสลับที่มีลำดับของบิตที่ที่มีรูปแบบของบิตที่สามารถเข้าใจได้อย่างง่ายๆ

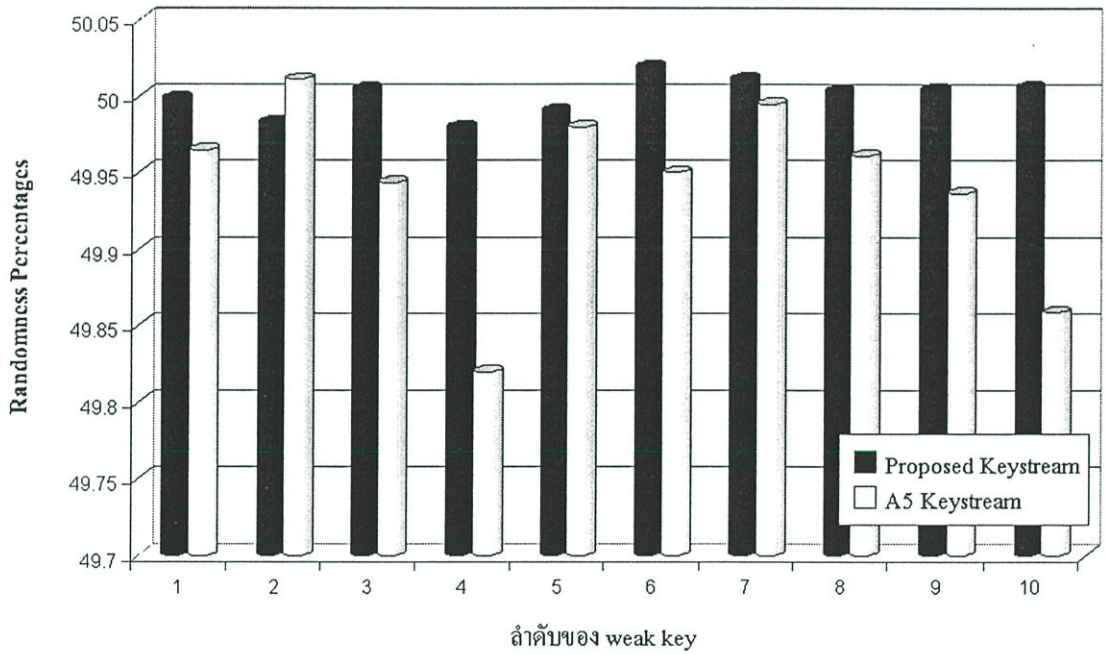
จากผลการทดลองดังแสดงในแผนภูมิแท่งรูปที่ 5.7, 5.8, และ 5.9 พบว่าเมื่อคีย์ต่อเนื่องที่นำเสนอมีเปอร์เซ็นต์ Randomness ใกล้เคียง 50% มากกว่าคีย์ต่อเนื่องของ Threshold โดยมีความคลาดเคลื่อนจาก 50 % ไปไม่เกิน –0.5 ถึง 1% สำหรับคีย์ต่อเนื่องที่นำเสนอและความคลาดเคลื่อนจาก 50 % ไปไม่เกิน –1.5 ถึง 1.5% สำหรับคีย์ต่อเนื่องของ Threshold ในทุกขนาดของคีย์ต่อเนื่อง



รูปที่ 5.7 แผนภูมิเปรียบเทียบ Randomness ของคีย์ต่อเนื่องขนาด 1026 ไบต์เมื่อใช้ Kc จากกลุ่ม Weak Key



รูปที่ 5.8 แผนภูมิเปรียบเทียบ Randomness ของคีย์ต่อเนื่องขนาด 102600 ไบต์เมื่อใช้ Kc จากกลุ่ม Weak Key



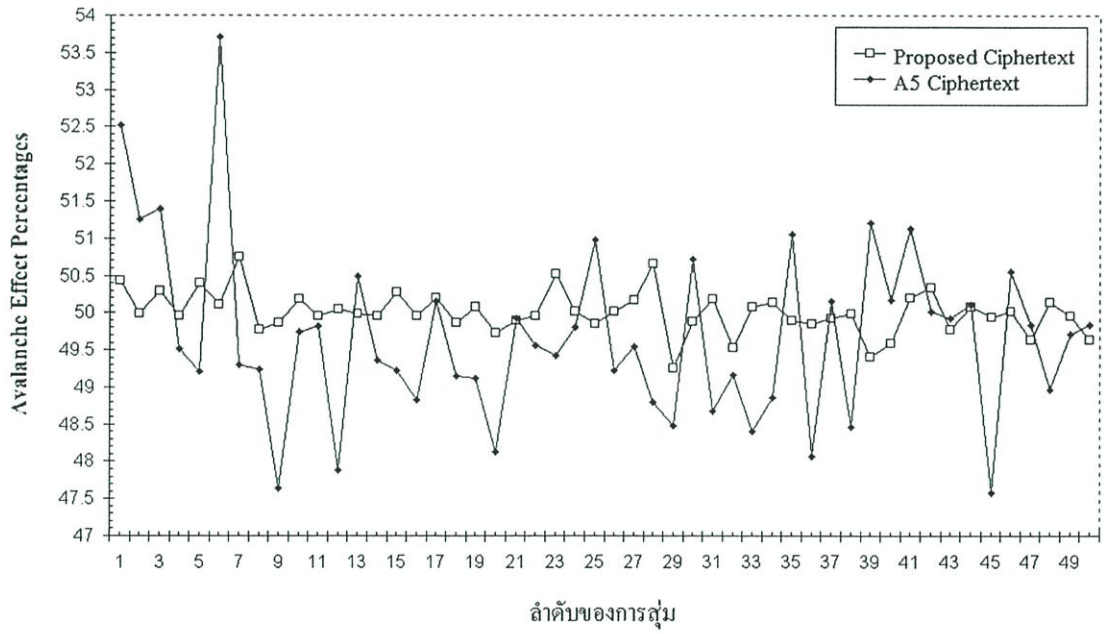
รูปที่ 5.9 แผนภูมิเปรียบเทียบ Randomness ของคีย์ต่อเนื่องขนาด 1050624 ไบต์เมื่อใช้ Kc จากกลุ่ม Weak Key

5.1.2 ผลการคำนวณหาคุณสมบัติ Avalanche Effect ของ Ciphertext

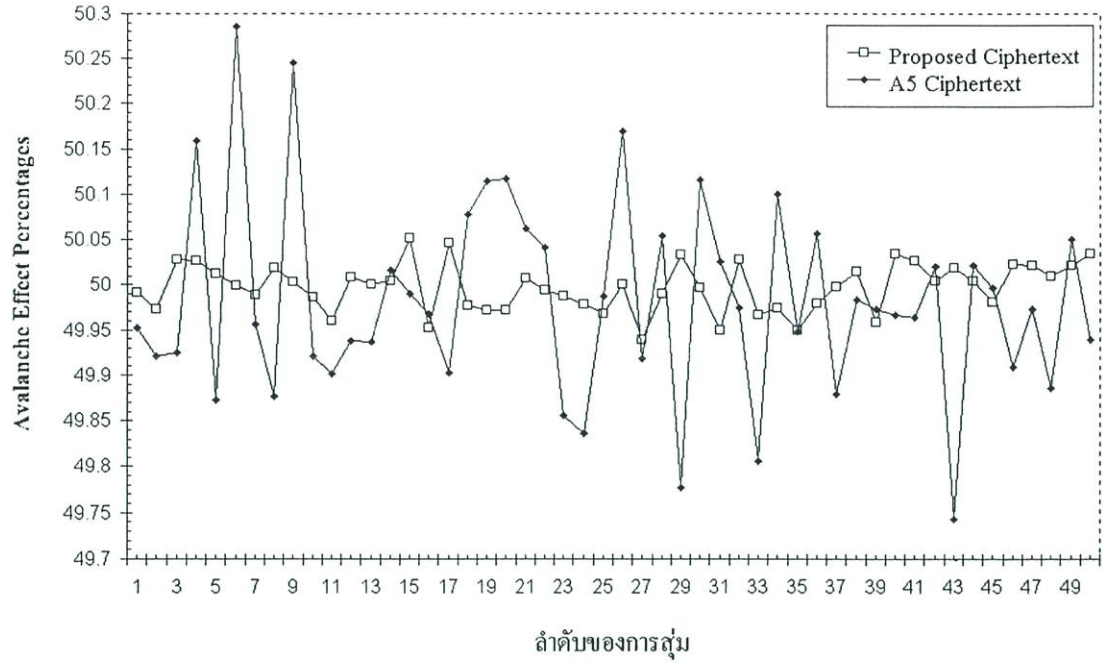
การคำนวณหาคุณสมบัติ Avalanche Effect ของ Ciphertext ที่ได้จากอัลกอริทึมที่นำเสนอเปรียบเทียบกับ Ciphertext ของอัลกอริทึม A5 โดยแบ่งได้เป็น 2 ส่วนตามลักษณะการได้มาซึ่ง Kc คีย์ที่ใช้ในการเข้ารหัสลับข้อมูล คือ ส่วนแรกเป็นการสุ่มเลือก Kc ขึ้นมา และในส่วนที่ 2 เป็นการใช้ Kc ที่อยู่ในกลุ่ม Weak Key

5.1.2.1 Avalanche Effect เมื่อใช้ Kc จากการสุ่ม

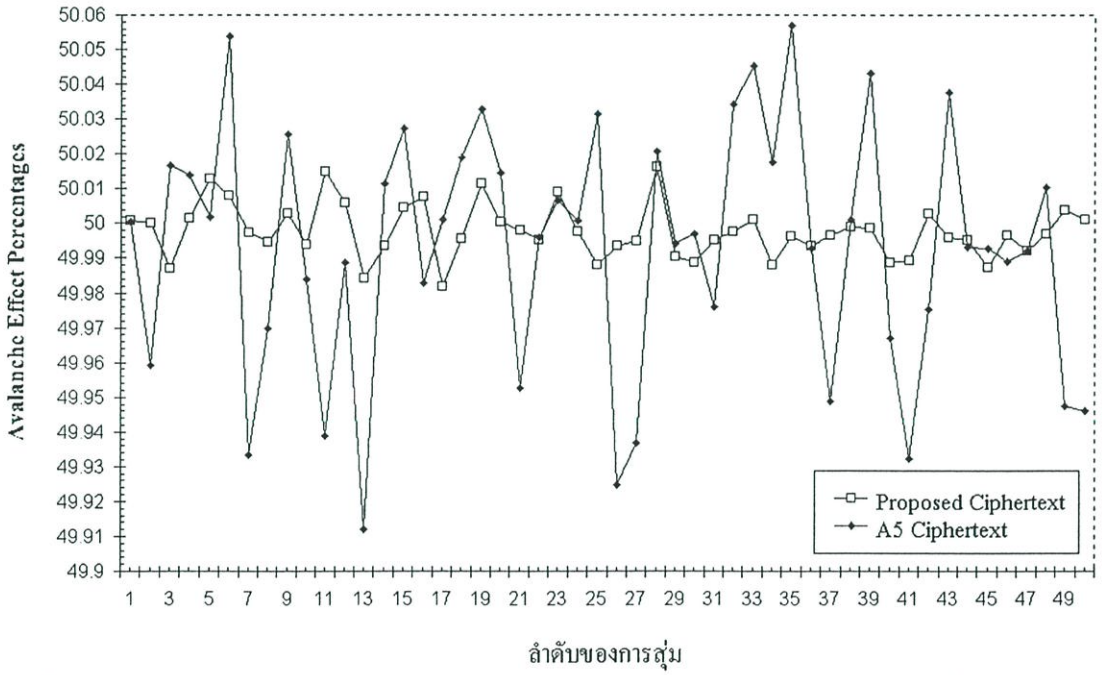
จากการสุ่มค่าของ Kc ขนาด 64 บิตจำนวน 50 ค่าแล้วนำค่า Kc ที่ได้จากการสุ่มนี้ไปคำนวณหาคีย์ต่อเนื่องโดยใช้อัลกอริทึมที่นำเสนอและ Threshold Generator ของอัลกอริทึม A5 โดยขนาดของคีย์ต่อเนื่องจะทำการผลิตเป็น 3 ขนาดคือ 1026 ไบต์, 102600 ไบต์, และ 1050624 ไบต์ แล้วนำคีย์ต่อเนื่องที่คำนวณได้ไป XOR กับ Plaintext ที่ได้จากการสุ่มตามขนาดข้อมูลคีย์ต่อเนื่องทำการคำนวณหา Avalanche Effect ของคีย์ต่อเนื่องทั้งสองอัลกอริทึมดังแสดงในรูปที่ 5.10, 5.11, และ 5.12 ตามลำดับ



รูปที่ 5.10 กราฟเปรียบเทียบ Avalanche Effect ของ Ciphertext ขนาด 1026 ไบต์เมื่อใช้ Kc จากการสุ่ม



รูปที่ 5.11 กราฟเปรียบเทียบ Avalanche Effect ของ Ciphertext ขนาด 102600 ไบต์เมื่อใช้ Kc จากการสุ่ม



รูปที่ 5.12 กราฟเปรียบเทียบ Avalanche Effect ของ Ciphertext ขนาด 1050624 ไบต์เมื่อใช้ Kc จากการสุ่ม

เมื่อนำค่าเปอร์เซ็นต์ของการ Avalanche Effect ของทั้งสองอัลกอริทึมในแต่ละขนาดข้อมูลมาทำการหาค่าทางสถิติพื้นฐานคือ ค่าเฉลี่ย, ความแปรปรวน, และส่วนเบี่ยงเบนมาตรฐาน จะได้ผลการคำนวณดังแสดงตารางที่ 5.5, 5.6, และ 5.7

ตารางที่ 5.5 การคำนวณหาค่าทางสถิติของ Avalanche Effect สำหรับ Ciphertext ขนาด 1026 ไบต์ โดยใช้ Kc จากการสุ่ม

พารามิเตอร์ทางสถิติ	Avalanche Effect ของ Ciphertext ขนาด 1026 ไบต์			
	Proposed Algorithm		A5 Algorithm	
	Differ bits	Percentage	Differ bits	Percentage
ค่าเฉลี่ย	4102.82	50.088041	4130.02	49.68129
ความแปรปรวน	552.2276	0.802812	9243.6196	1.371352
ส่วนเบี่ยงเบนมาตรฐาน	22.8523	0.283339	96.14374	1.171048

ตารางที่ 5.6 การคำนวณหาค่าทางสถิติของ Avalanche Effect สำหรับ Ciphertext ขนาด 102600 ไบต์โดยใช้ Kc จากการสุ่ม

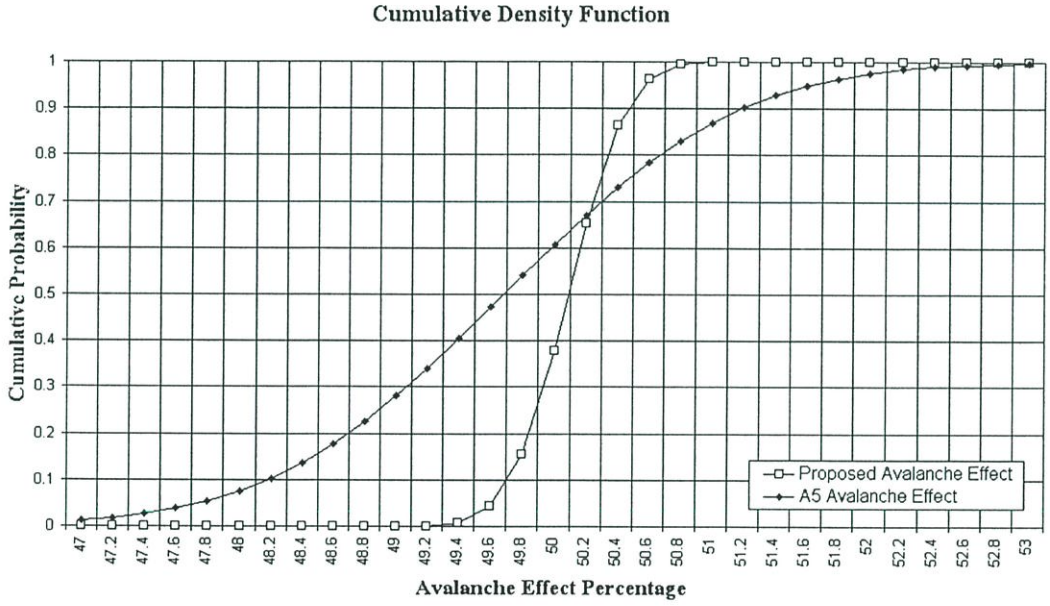
พารามิเตอร์ทางสถิติ	Avalanche Effect ของ Ciphertext ขนาด 102600 ไบต์			
	Proposed Algorithm		A5 Algorithm	
	Differ bits	Percentage	Differ bits	Percentage
ค่าเฉลี่ย	410420.8	49.997466	410546.34	49.982171
ความแปรปรวน	47890.4799	0.000711	794020.5844	0.011786
ส่วนเบี่ยงเบนมาตรฐาน	218.83896	0.026662	891.078326	0.108562

ตารางที่ 5.7 การคำนวณหาค่าทางสถิติของ Avalanche Effect สำหรับ Ciphertext ขนาด 1050426 ไบต์โดยใช้ Kc จากการสุ่ม

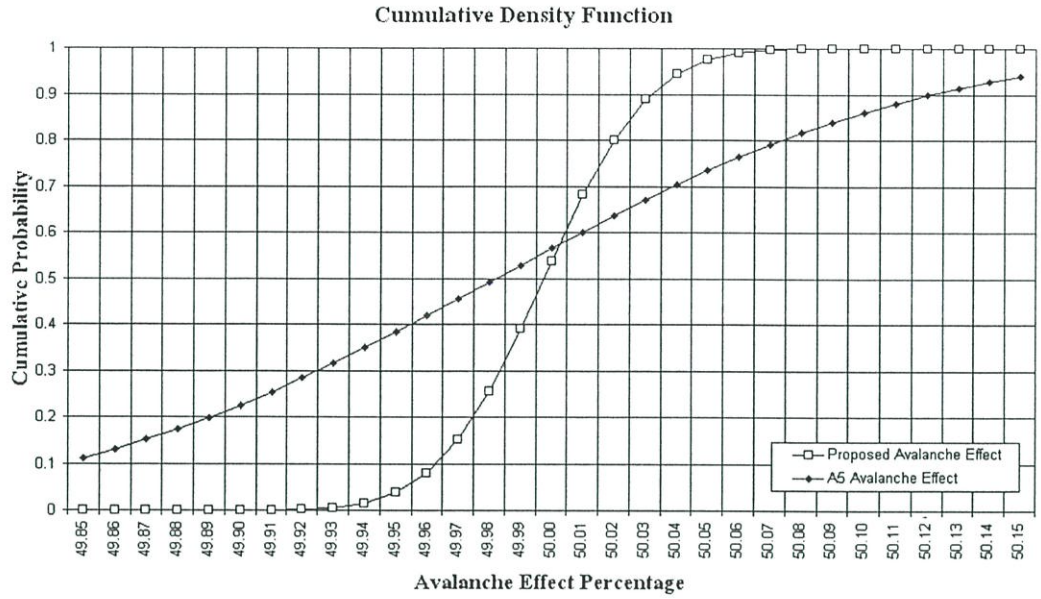
พารามิเตอร์ทางสถิติ	Avalanche Effect ของ Ciphertext ขนาด 1050624 ไบต์			
	Proposed Algorithm		A5 Algorithm	
	Differ bits	Percentage	Differ bits	Percentage
ค่าเฉลี่ย	4202680.26	49.997808	4203084.58	49.992997

ความแปรปรวน	414450.87	5.8667E-05	8792917.52	0.001245
ส่วนเบี่ยงเบนมาตรฐาน	643.77859	0.0076595	2965.2854	0.0352801

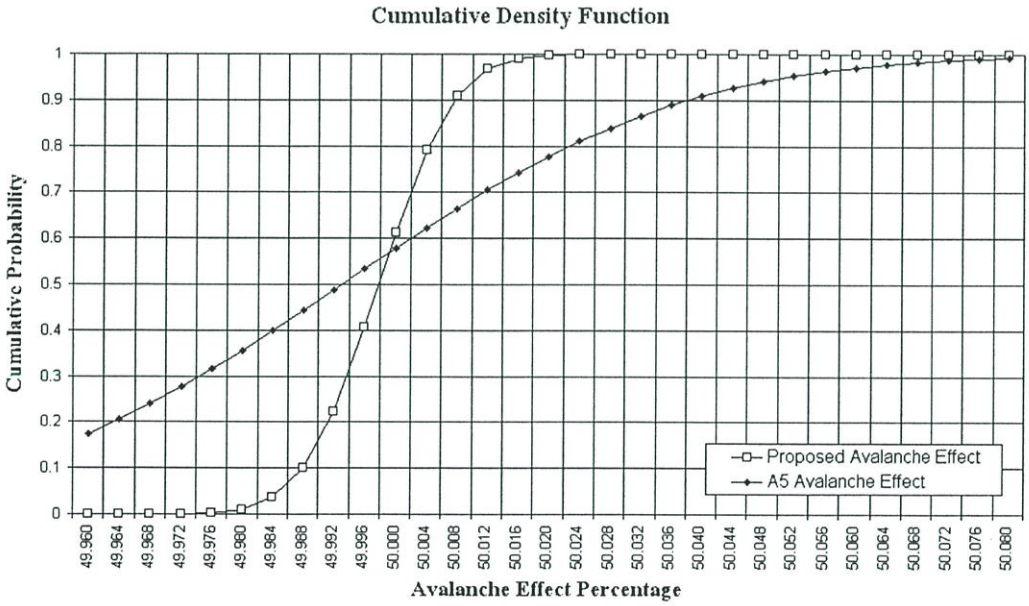
จากข้อมูลที่ได้รับจากกราฟและตารางทั้ง 3 นี้ เมื่อนำค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของข้อมูล 1026 ไบต์, 102600 ไบต์, และ 1050624 ไบต์ มาพิจารณาเป็นกราฟการแจกแจงแบบปกติสะสมดังแสดงในรูปที่ 4.5, 4.6, และ 4.7 ตามลำดับ จะเห็นได้ว่าเมื่อพิจารณาค่าเฉลี่ยของเปอร์เซ็นต์ Avalanche Effect ของ Ciphertext สำหรับทั้งสองอัลกอริทึมนี้ พบว่าอัลกอริทึมที่นำเสนอมีเปอร์เซ็นต์ Avalanche Effect ที่สูงกว่าอัลกอริทึม A5 เมื่อพิจารณาความแปรปรวนและส่วนเบี่ยงเบนมาตรฐาน ผลลัพธ์เปอร์เซ็นต์ Avalanche Effect ของ Ciphertext สำหรับอัลกอริทึม A5 จะมีค่าความแปรปรวนและส่วนเบี่ยงเบนมาตรฐานสูงกว่าผลลัพธ์เปอร์เซ็นต์ Avalanche Effect ของ Ciphertext สำหรับอัลกอริทึมที่นำเสนอค่อนข้างมาก



รูปที่ 5.13 กราฟการแจกแจงแบบปกติสะสมของ Avalanche Effect สำหรับ Ciphertext ขนาด 1026 ไบต์



รูปที่ 5.14 กราฟการแจกแจงแบบปกติสะสมของ Avalanche Effect สำหรับ Ciphertext ขนาด 102600 ไบต์

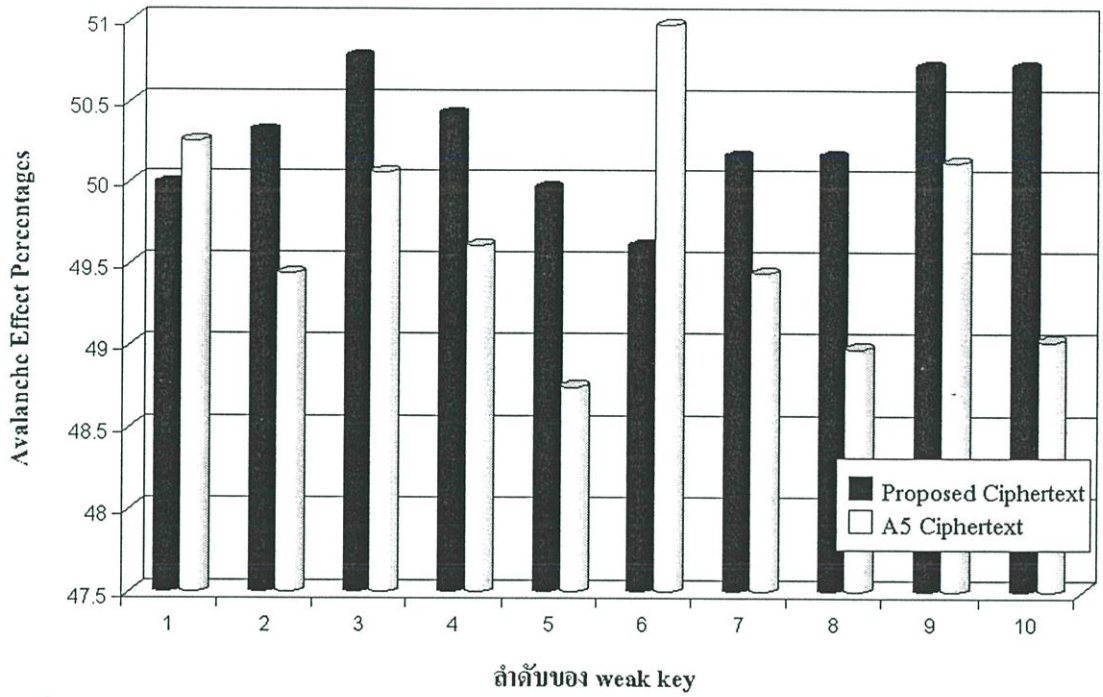


รูปที่ 5.15 กราฟการแจกแจงแบบปกติสะสมของ Avalanche Effect สำหรับ Ciphertext ขนาด 1050624 ไบต์

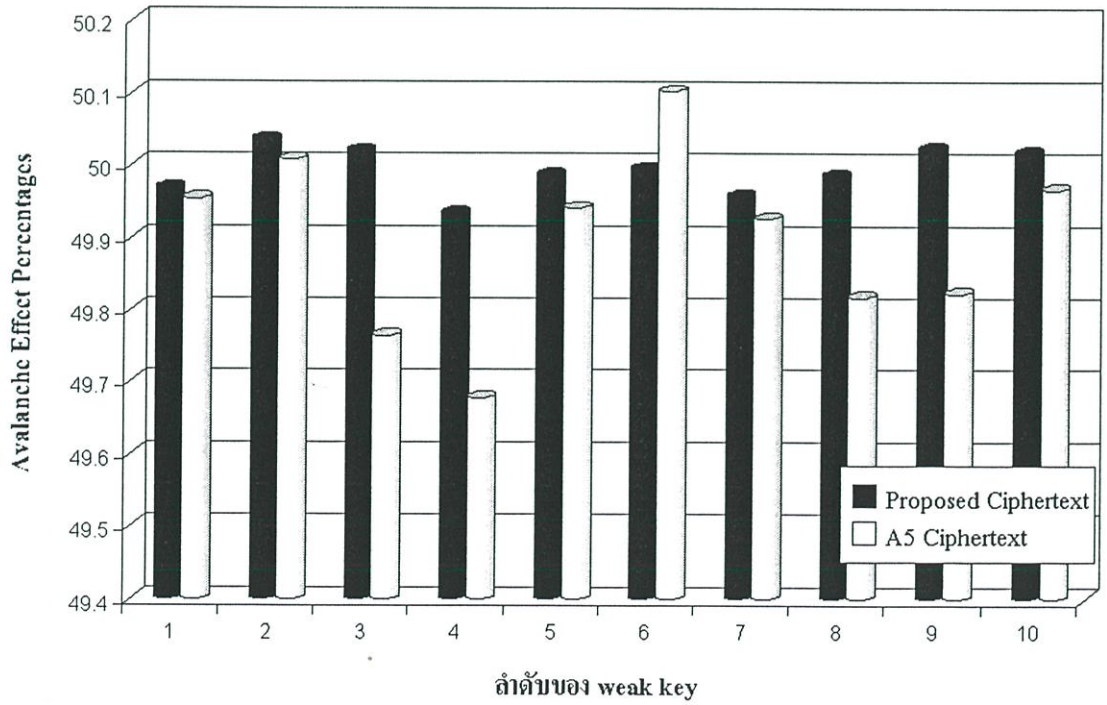
5.1.2.2 Avalanche Effect เมื่อใช้ Kc จากกลุ่ม Weak Key

ในการทดลองนี้นำ Kc จากกลุ่ม Weak Key ในตารางที่ 5.4 มาคำนวณหา Ciphertext ของอัลกอริทึมที่นำเสนอและอัลกอริทึม A5 เพื่อคำนวณหาจำนวนของบิตที่เปลี่ยนไปของ Ciphertext

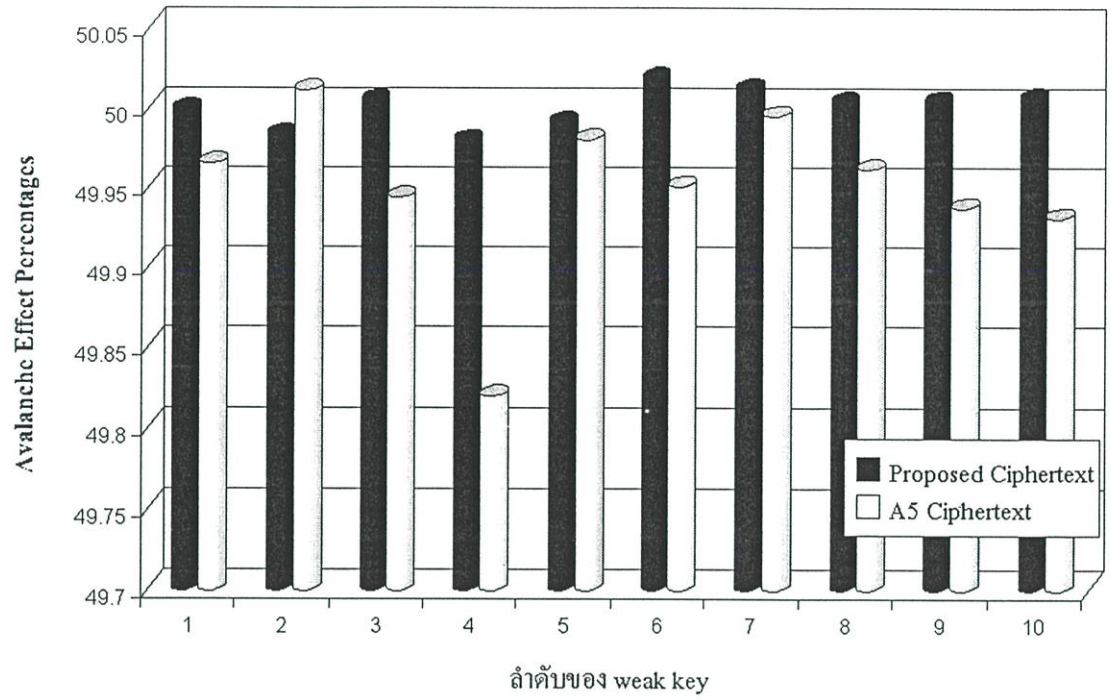
เมื่อเทียบกับ Plaintext ของอัลกอริทึมเมื่อใช้คีย์ในการเข้ารหัสลับที่มีลำดับของบิตที่ที่มีรูปแบบของบิตที่สามารถเข้าใจได้อย่างง่ายๆ



รูปที่ 5.16 แผนภูมิเปรียบเทียบ Avalanche Effect ของ Ciphertext ขนาด 1026 ไบต์เมื่อใช้ Kc จากกลุ่ม Weak Key



รูปที่ 5.17 แผนภูมิเปรียบเทียบ Avalanche Effect ของ Ciphertext ขนาด 102600 ไบต์เมื่อใช้ Kc จากกลุ่ม Weak Key



รูปที่ 5.18 แผนภูมิเปรียบเทียบ Avalanche Effect ของ Ciphertext ขนาด 1050624 ไบต์เมื่อใช้ Kc จากกลุ่ม Weak Key

จากผลการทดลองดังแสดงในแผนภูมิแท่งรูปที่ 5.16, 5.17, และ 5.18 พบว่าส่วนใหญ่แล้ว Ciphertext ของอัลกอริทึมที่นำเสนอมีเปอร์เซ็นต์ Avalanche Effect สูงกว่า Ciphertext ของอัลกอริทึม A5 โดยมีเพียง 13.33% ของ Weak Key ทั้งหมดที่ Ciphertext ของอัลกอริทึมที่ให้เปอร์เซ็นต์ Avalanche Effect สูงกว่าอัลกอริทึมที่นำเสนอ

5.1.3 ค่าใช้จ่ายในการเข้ารหัสลับข้อมูล

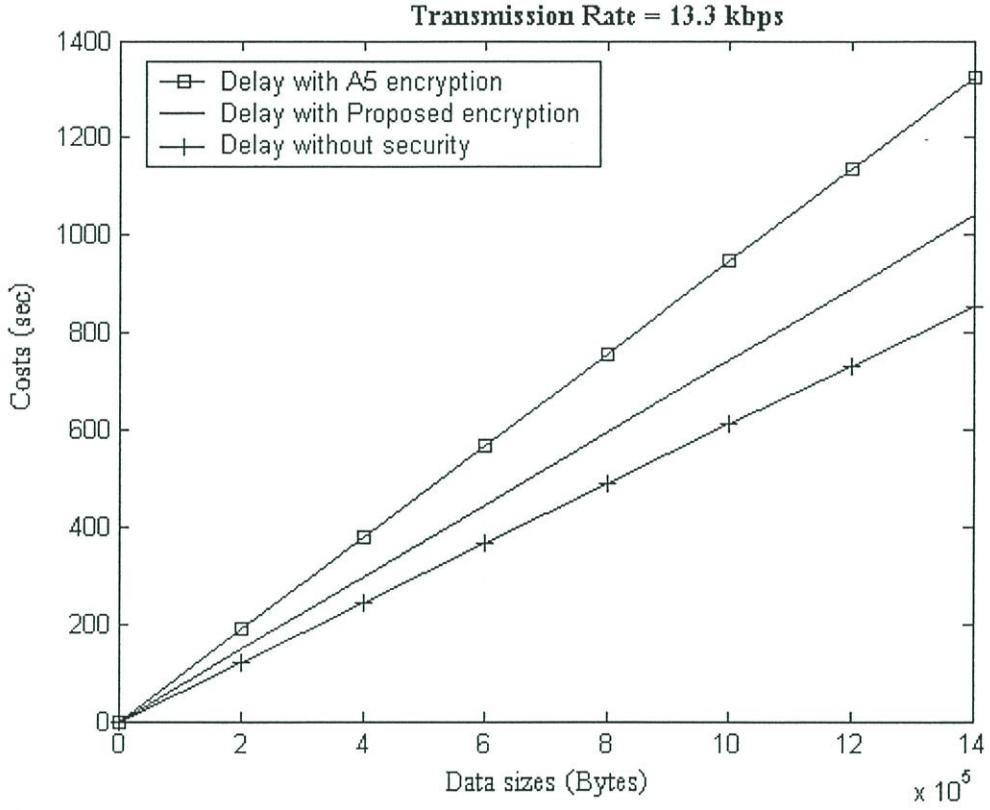
การทดลองใช้โปรแกรม Borland C++ บน PC ที่มี CPU เป็น Pentium II 266 MHz โดยมี RAM ขนาด 128 ไบต์ทำการคำนวณหาเวลาที่ใช้ในการเข้ารหัสลับของอัลกอริทึมที่นำเสนอเปรียบเทียบกับอัลกอริทึม A5 โดยการทดลองเข้ารหัสลับข้อมูลทั้งหมด 50 ครั้งแล้วนำมาหาค่าเฉลี่ย ดังแสดงในตารางที่ 5.8

ตารางที่ 5.8 เวลาที่ใช้ในการเข้ารหัสลับข้อมูล

ขนาดของข้อมูล	เวลาที่ใช้ในการเข้ารหัสลับ	
	อัลกอริทึมที่นำเสนอ	อัลกอริทึม A5
102600 ไบต์	5.156251 msec	23.203125 msec
1050624 ไบต์	258.103125 msec	1159.059374 msec

จากตารางที่ 5.8 พบว่าอัลกอริทึมที่นำเสนอใช้เวลาในการเข้ารหัสลับข้อมูลเร็วกว่าอัลกอริทึม A5 ประมาณ 77.74%

ในการทดลองคำนวณหาค่าใช้จ่ายของการเข้ารหัสลับข้อมูลเปรียบเทียบการเข้ารหัสลับโดยใช้อัลกอริทึมที่นำเสนอเปรียบเทียบกับอัลกอริทึม A5 ทำการทดลองโดยใช้โปรแกรม MATHLAB ทำการคำนวณค่าใช้จ่ายในสมการที่ 4.1 ถึง 4.3 ได้ผลลัพธ์ดังแสดงในรูปที่ 5.19 และรูปที่ 5.20

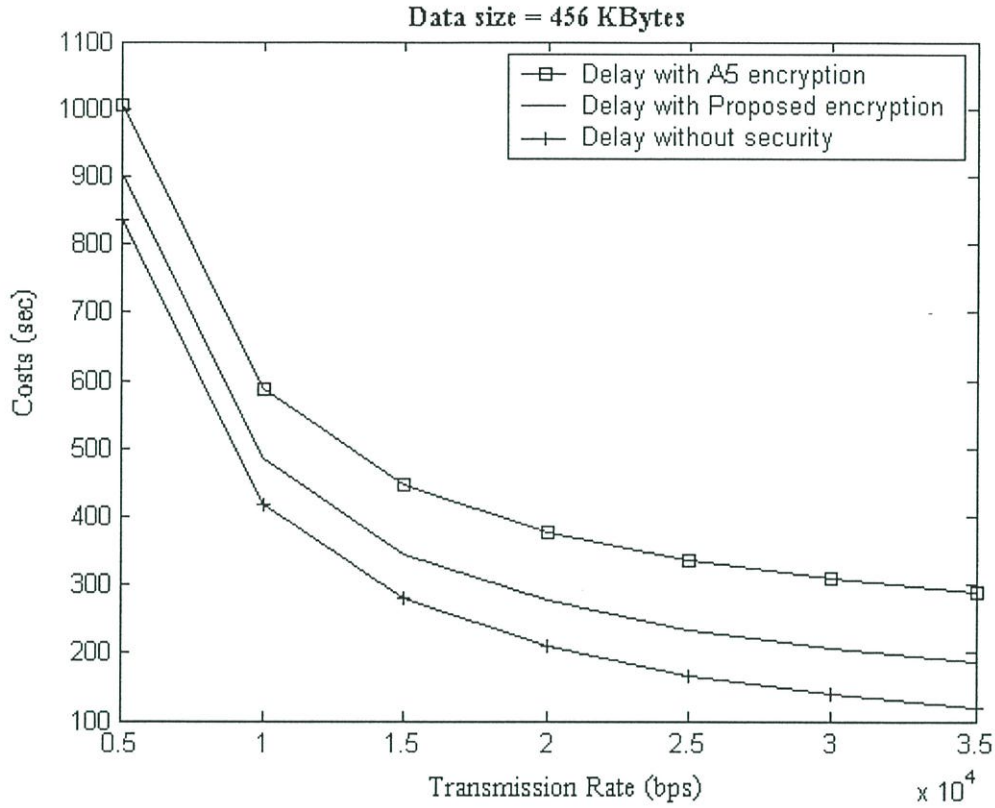


รูปที่ 5.19 กราฟเปรียบเทียบค่าใช้จ่ายการเข้ารหัสลับโดยมีอัตราการสื่อสารข้อมูลคงที่ 13.3 กิโลบิตต่อวินาที

จากกราฟในรูปที่ 5.19 เป็นการพิจารณาความสัมพันธ์ระหว่างค่าใช้จ่ายในการเข้ารหัสลับข้อมูลกับขนาดของข้อมูลที่ถูกเข้ารหัสลับ พบว่าค่าใช้จ่ายการเข้ารหัสลับที่นำเสนอมีค่าใช้จ่ายต่ำกว่าอัลกอริทึม A5 สำหรับขนาดข้อมูล 1 เม็กกะไบต์ อัลกอริทึมที่นำเสนอมีค่าใช้จ่ายน้อยกว่าอัลกอริทึม A5 ประมาณ 21.39% และ อัลกอริทึมที่นำเสนอมีค่าใช้จ่ายมากกว่าค่าใช้จ่ายที่เกิดจากการส่งข้อมูลเพียงอย่างเดียวไม่มีการเข้ารหัสลับข้อมูลก่อนประมาณ 17.9%

จากกราฟในรูปที่ 5.20 เป็นการพิจารณาความสัมพันธ์ระหว่างค่าใช้จ่ายในการเข้ารหัสลับข้อมูลกับอัตรเร็วในการสื่อสารข้อมูล พบว่าค่าใช้จ่ายการเข้ารหัสลับที่นำเสนอมีค่าใช้จ่ายต่ำกว่า

อัลกอริทึม A5 สำหรับอัตราเร็วในการสื่อสารข้อมูล 13.3 Kbps อัลกอริทึมที่นำเสนอมีค่าใช้จ่ายน้อยกว่าอัลกอริทึม A5 ประมาณ 13.04% และ อัลกอริทึมที่นำเสนอมีค่าใช้จ่ายมากกว่าค่าใช้จ่ายที่เกิดจากการส่งข้อมูลเพียงอย่างเดียวไม่มีการเข้ารหัสลับข้อมูลก่อนประมาณ 9.85%



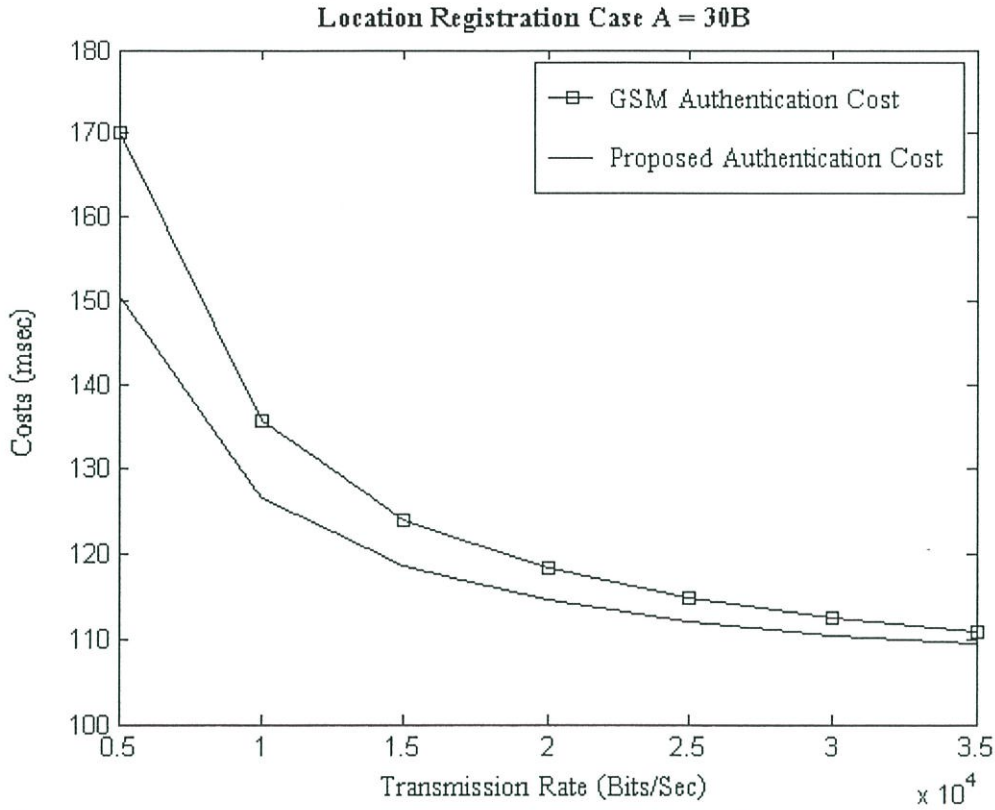
รูปที่ 5.20 กราฟเปรียบเทียบค่าใช้จ่ายการเข้ารหัสลับโดยมีขนาดข้อมูลคงที่ 456 กิโลไบต์

5.2 การคำนวณค่าใช้จ่ายการตรวจสอบผู้ใช้

ในการทดลองคำนวณหาค่าใช้จ่ายของการตรวจสอบผู้ใช้ (Authentication) ในโพรโตคอลที่นำเสนอเปรียบเทียบกับโพรโตคอลของ GSM ทำการทดลองโดยใช้โปรแกรม MATHLAB ทำการคำนวณค่าใช้จ่ายในสมการที่ 4.1 ถึง 4.7 ที่เป็นค่าใช้จ่ายได้จากโพรโตคอลในกรณีต่างๆ

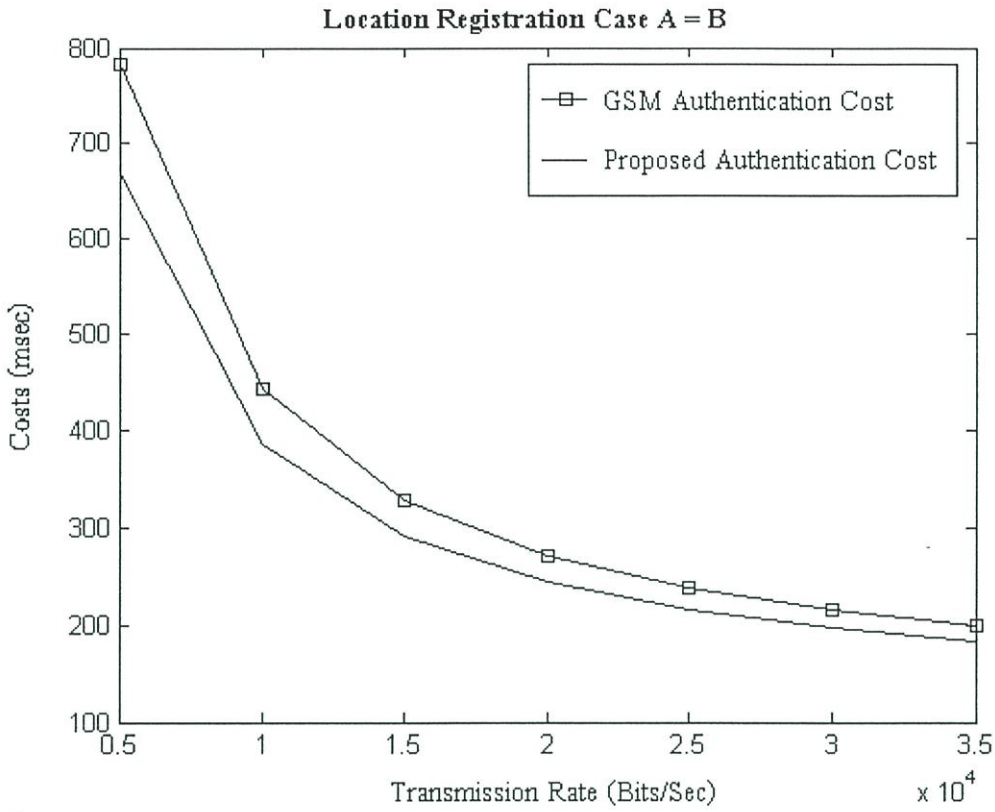
5.2.1 ค่าใช้จ่ายตรวจสอบผู้ใช้เมื่อมีการทำ Location Registration

ค่าใช้จ่ายการตรวจสอบผู้ใช้เมื่อมีการ Location Registration มีผลลัพธ์ดังแสดงในกราฟรูปที่ 5.21 และ 5.22 การสมมุติพารามิเตอร์ A และ B ถูกแบ่งเป็น 2 กรณีคือ A = 30B และ A = B เนื่องจากสมการที่ 3.1 ค่าใช้จ่ายออกเป็น 2 กรณี



รูปที่ 5.21 กราฟเปรียบเทียบค่าใช้จ่ายของการตรวจสอบผู้ใช้ในกรณีที่ผู้ใช้ทำ Location Registration และอัตราเร็วในการสื่อสาร A = 30B

จากกราฟในรูปที่ 5.15 พบว่าค่าใช้จ่ายของโพรโตคอลที่นำเสนอในกรณีที่ผู้ใช้ทำ Location Registration นั้นมีค่าใช้จ่ายต่ำกว่าโพรโตคอลของ GSM โดยพิจารณาอัตราเร็วในการสื่อสารระหว่าง MS กับ MSC เร็วกว่าอัตราเร็วในการสื่อสารระหว่าง MSC กับ HLR 30 เท่า ที่ความเร็วในการสื่อสาร 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM 6.78%, ที่ความเร็วในการสื่อสารน้อยกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM ประมาณ 11.52%, และที่ความเร็วในการสื่อสารมากกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM ประมาณ 5.04%

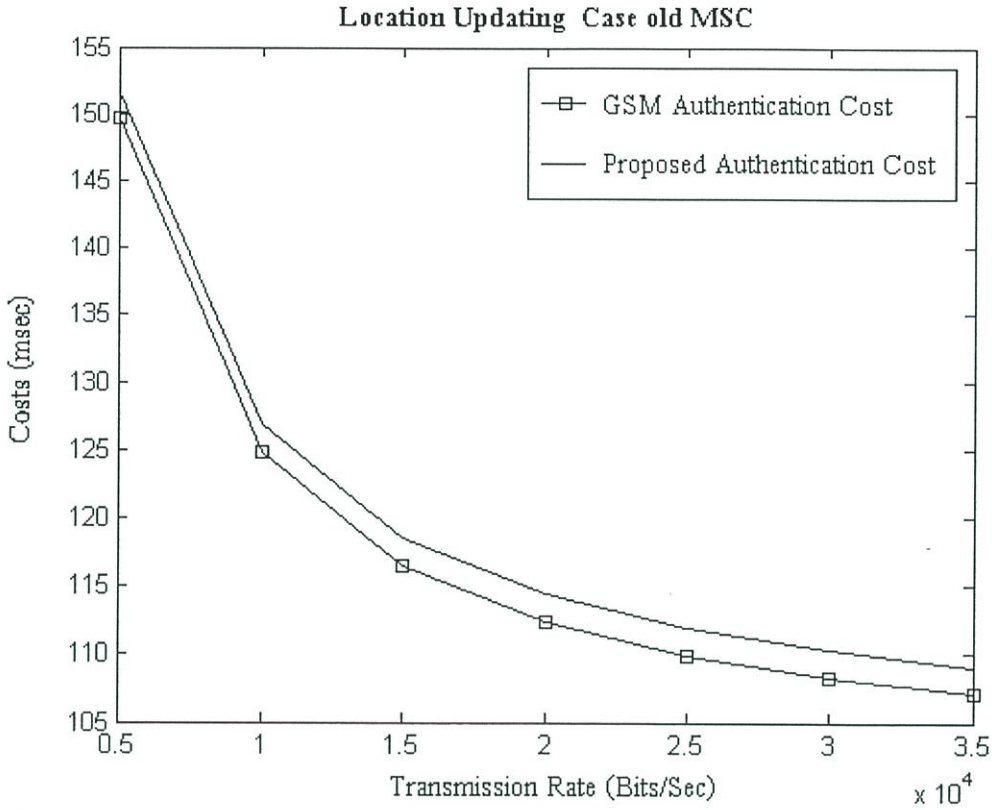


รูปที่ 5.22 กราฟเปรียบเทียบค่าใช้จ่ายของการตรวจสอบผู้ใช้ในกรณีที่ผู้ใช้ทำ Location Registration และอัตราเร็วในการสื่อสาร A = B

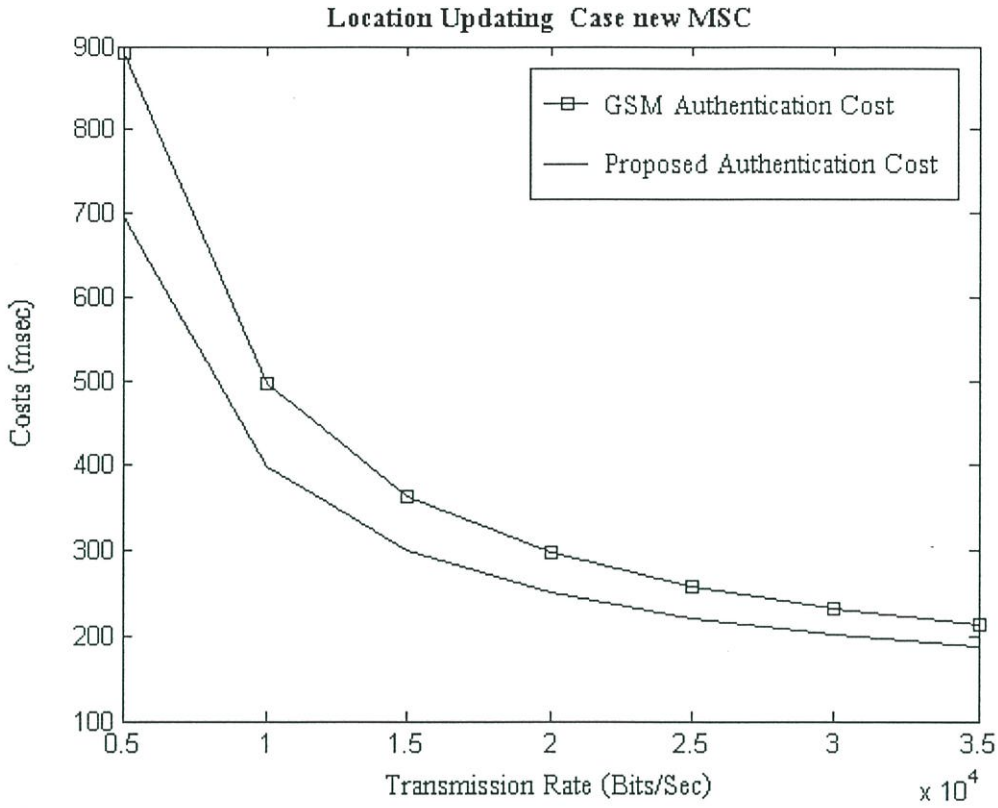
จากกราฟในรูปที่ 5.16 พิจารณาอัตราเร็วในการสื่อสารระหว่าง MS กับ MSC เท่ากับอัตราเร็วในการสื่อสารระหว่าง MSC กับ HLR พบว่าค่าใช้โพรโตคอลที่นำเสนอนั้นยังคงมีค่าใช้จ่ายต่ำกว่าโพรโตคอลของ GSM โดยที่ความเร็วในการสื่อสาร 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM 11.94%, ที่ความเร็วในการสื่อสารน้อยกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM ประมาณ 14.94%, และที่ความเร็วในการสื่อสารมากกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM ประมาณ 8.09%

5.2.2 ค่าใช้จ่ายตรวจสอบผู้ใช้เมื่อมีการทำ Location Updating

ค่าใช้จ่ายการตรวจสอบผู้ใช้เมื่อมีการ Location Updating มีผลลัพธ์แบ่งออกเป็น 2 กรณีคือ การทำ Location Updating เมื่ออยู่ในพื้นที่การจัดการของ MSC เดิมและ MSC ใหม่ ดังแสดงในกราฟรูปที่ 5.23 และ 5.24 ตามลำดับ



รูปที่ 5.23 กราฟเปรียบเทียบค่าใช้จ่ายของการตรวจสอบผู้ใช้เมื่อผู้ใช้ทำ Location Updating ในกรณีที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC เดิม



รูปที่ 5.24 กราฟเปรียบเทียบค่าใช้จ่ายของการตรวจสอบผู้ใช้เมื่อผู้ใช้ทำ Location Updating ในกรณีที่ผู้ใช้เปลี่ยนพื้นที่การจัดการของ MSC

พิจารณาอัตราเร็วในการสื่อสารระหว่าง MS กับ MSC เท่ากับอัตราเร็วในการสื่อสารระหว่าง MSC กับ HLR จากผลการทดลองพบว่าในกรณีผู้ใช้ทำ Location Updating กับ MSC เดิมนั้น ค่าใช้โพรโตคอลที่นำเสนอนั้นมีค่าใช้จ่ายสูงกว่าโพรโตคอลของ GSM ดังแสดงในรูปที่ 5.23 แต่ในกรณีผู้ใช้ทำ Location Updating กับ MSC ใหม่นั้น ค่าใช้โพรโตคอลที่นำเสนอนั้นมีค่าใช้จ่ายต่ำกว่าโพรโตคอลของ GSM ดังแสดงในรูปที่ 5.24

สำหรับค่าใช้จ่ายในกราฟรูปที่ 5.23 ที่ความเร็วในการสื่อสาร 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอสูงกว่าของโพรโตคอลของ GSM 1.66%, ที่ความเร็วในการสื่อสารน้อยกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอสูงกว่าของโพรโตคอลของ GSM ประมาณ 1.32%, และที่ความเร็วในการสื่อสารมากกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอสูงกว่าของโพรโตคอลของ GSM ประมาณ 1.83%

สำหรับค่าใช้จ่ายในกราฟรูปที่ 5.24 ที่ความเร็วในการสื่อสาร 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM 18.25%, ที่ความเร็วในการสื่อสารน้อยกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM ประมาณ 22.02%,

และที่ความเร็วในการสื่อสารมากกว่า 13.3 Kbps ค่าใช้จ่ายของโพรโตคอลที่นำเสนอต่ำกว่าของโพรโตคอลของ GSM ประมาณ 12.96%

5.2.3 Transmission Loads ในการตรวจสอบผู้ใช้

ในการตรวจสอบผู้ใช้หนึ่งครั้งของเครือข่าย เครือข่ายจะมีปริมาณทราฟฟิคเพิ่มขึ้นตามจำนวนข้อมูลที่โพรโตคอลถูกออกแบบให้มีการแลกเปลี่ยนข้อมูลซึ่งกันและกันในแต่ละหน่วยงานของเครือข่าย จากการทดลองเปรียบเทียบจำนวน Transmission Loads ที่ใช้ในโพรโตคอลที่นำเสนอกับโพรโตคอลของ GSM ได้ผลลัพธ์ดังแสดงในตารางที่ 5.9

ตารางที่ 5.9 การเปรียบเทียบ Transmission Loads

ชนิดของโพรโตคอลในการตรวจสอบผู้ใช้	จำนวน Transmission Loads	
	โพรโตคอลที่นำเสนอ	โพรโตคอลของ GSM
Location Registration	366 ไบต์	494 ไบต์
Location Updating by old MSC	31 ไบต์	31 ไบต์
Location Updating by new MSC	363 ไบต์	491 ไบต์

จากผลการทดลองพบว่าโพรโตคอลที่นำเสนอเมื่อมีการตรวจสอบผู้ใช้หนึ่งครั้งจะทำให้เครือข่ายมีปริมาณทราฟฟิคเพิ่มขึ้นน้อยกว่าโพรโตคอลของ GSM โดยโพรโตคอลที่นำเสนอนั้นใช้ Transmission Loads น้อยกว่าโพรโตคอลของ GSM 128 ไบต์ ยกเว้นในกรณีที่ผู้ใช้ทำ Location Updating กับ MSC เดิม Transmission Loads ของทั้งสองโพรโตคอลนั้นจะเท่ากัน

บทที่ 6
บทสรุป

6.1 สรุปผลการทดลอง

กระบวนการรักษาความปลอดภัยของเครือข่ายมีความสำคัญสำหรับการสื่อสารข้อมูลของเครือข่ายที่ใช้อุปกรณ์โทรศัพท์เคลื่อนที่เป็นอย่างยิ่ง เนื่องจากจะสามารถทำให้ผู้ใช้ของเครือข่ายมั่นใจได้ว่าข้อมูลของผู้ใช้หรือทรัพยากรของเครือข่ายจะไม่ถูกลักลอบนำไปใช้โดยพลการ

สำหรับการปรับปรุงโพรโตคอลการตรวจสอบผู้ใช้ (Authentication Protocol) โดยการลดขนาดของ RAND จาก 128 บิต มาใช้ RANDM ขนาด 64 บิตซึ่งจะถูกใช้งานร่วมกับ COUNTM ขนาด 64 บิตนั้นสามารถลดค่าใช้ง่ายในการตรวจสอบผู้ใช้ของเครือข่ายได้ทั้งในกรณีที่ผู้ใช้ทำ Location Registration, Location Updating ขณะที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC ใหม่, และการทำ Call Setup ทั้งในกรณีที่เป็น Mobile Originated และ Mobile Terminated สำหรับการตรวจสอบผู้ใช้ในกรณีผู้ใช้ทำ Location Updating ขณะที่ผู้ใช้อยู่ในพื้นที่การจัดการของ MSC เดิมนั้นค่าใช้จ่ายของโพรโตคอลที่นำเสนอใหม่จะสูงกว่าโพรโตคอลเดิมของเครือข่าย GSM แต่ข้อมูลของผู้ใช้จะได้รับการเข้ารหัสลับก่อนที่จะส่งผ่านช่องสัญญาณวิทยุขณะที่โพรโตคอลเดิมของเครือข่าย GSM มิได้จัดเตรียมไว้ให้

การรักษาความปลอดภัยของข้อมูลผู้ใช้นั้นการเข้าและถอดรหัสลับข้อมูลเป็นกลไกที่สำคัญที่สุดอันหนึ่งในระบบการรักษาความปลอดภัยปัจจุบัน การเข้าและถอดรหัสลับข้อมูลมีจุดประสงค์หลักคือการปกปิดเนื้อหาสาระของข้อมูลที่ผู้ส่งต้องการจะส่งให้ผู้รับ ซึ่งผู้รับที่ถูกต้องเท่านั้นจึงจะสามารถถอดรหัสลับข้อมูลได้ สำหรับอัลกอริทึมการเข้าและถอดรหัสลับที่นำเสนอนั้นเป็นการเข้ารหัสลับแบบ Secret Key โดยมีลักษณะการเข้ารหัสลับเป็นแบบ Stream Cipher ซึ่งจะทำการผลิตคีย์ต่อเนื่อง (Key Stream) โดยจะนำไป XOR กับข้อมูลของผู้ใช้เพื่อปกปิดเนื้อหาของข้อมูล จากการทดลองเปรียบเทียบคีย์ต่อเนื่องที่นำเสนอกับคีย์ต่อเนื่องของอัลกอริทึม A5 ที่เครือข่าย GSM ใช้เข้ารหัสลับอยู่เดิมนั้นพบว่า คีย์ต่อเนื่องที่นำเสนอนั้นมีคุณสมบัติการสุ่ม (Randomness) ดีกว่าและเมื่อนำข้อมูลที่เข้ารหัสลับเรียบร้อยแล้วทำการนับจำนวนบิตที่เปลี่ยนไปเมื่อเทียบกับข้อมูลเดิมก่อนที่จะเข้ารหัสลับ จะเห็นได้ว่าอัลกอริทึมที่นำเสนอนั้นมีค่าเฉลี่ยของจำนวนบิตที่เปลี่ยนไปสูงกว่าอัลกอริทึม A5 ของเครือข่าย GSM และจากผลการทดลองในหัวข้อที่ 5.1.3 แสดงในเห็นว่าอัลกอริทึมในการเข้ารหัสลับที่นำเสนอนี้มีความเร็วในการเข้ารหัสลับข้อมูลสูงกว่าอัลกอริทึม A5 อีกด้วย

6.2 ปัญหาและข้อเสนอแนะ

การเข้าและถอดรหัสลับข้อมูลนั้นอัลกอริทึมแบบ Secret Key อาจจะมีความเร็วในการเข้าและถอดรหัสลับข้อมูลสูงกว่าเมื่อเปรียบเทียบกับอัลกอริทึมการเข้ารหัสลับแบบ Public Key แต่ถ้ามองถึงคุณสมบัติต่างๆ เกี่ยวกับความปลอดภัยแล้วอัลกอริทึมการเข้ารหัสลับแบบ Public Key อาจจะให้ความน่าเชื่อถือเกี่ยวกับความปลอดภัยสูงกว่า ดังนั้นการออกแบบอัลกอริทึมการเข้ารหัสลับแบบ Public Key ที่มีค่าใช้จ่ายการเข้าและถอดรหัสลับข้อมูลไม่สูงมากนักจึงเป็นอีกทางเลือกหนึ่งที่น่าสนใจสำหรับผู้ออกแบบระบบการรักษาความปลอดภัยของเครือข่ายการสื่อสารเคลื่อนที่

เอกสารอ้างอิง

[1] Jörg Eberapächer, Hans-Jörg Vögel, Christian Bettstetter. **GSM: Switching, Service and Protocol.** 2nd Ed. New York: John Wiley & Sons, Inc 2001.

[2] ETSI TS 100 522 V7.1.0 (2000-02) "Digital cellular telecommunications system (Phase 2+); Network Architecture" (GSM 03.02 version 7.13.0 Release 1998) France, European Telecommunications Standards Institute 2000, 2000.

[3] ETSI TS 100 927 V7.5.0 (2000-07) "Digital cellular telecommunications system (Phase 2+); Numbering, Addressing and Identification" (GSM 03.03 version 7.5.0 Release 1998) France, European Telecommunications Standards Institute 2000, 2000.

[4] ETSI EN 300 908 V8.5.1 (2000-11) "Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path" (GSM 05.02 version 8.5.1 Release 1999) France, European Telecommunications Standards Institute 2000, 2000.

[5] Moe Rahnema, "Overview of the GSM system and protocol architecture", IEEE Communication Magazine, pp 92-100, April 1993

[6] William Stallings. **Cryptography and Networks Security: Principle and Practice.** 2nd Ed. New Jersey: Prentice Hall, Inc 1999

[7] R. L. Rivest, "The RC4 encryption algorithm", RSA Data Security, Inc Mar. 1992

[8] ETSI TS 300 920 V7.1.1 (2000-08) "Digital cellular telecommunications system (Phase 2+); Security aspects" (GSM 03.20 version 7.1.1 Release 1998) France, European Telecommunications Standards Institute 2000, 2000.

[9] ETSI TS 100 614 V8.0.0 (2001-02) "Digital cellular telecommunications system (Phase 2+); Security management" (GSM 12.03 version 8.0.0 Release 1999) France, European Telecommunications Standards Institute 2001, 2001.

[10] Al-tawil Khalid, Ali Akrami, and Habib Youssef, "A new authentication protocol for GSM networks", IEEE Annual Conference on Local Computer Networks, LCN'98, pp 21-30, 1998.

[11] Larry L. Peterson and Bruce S. Davie. **Computer Networks: A Systems Approach.** 2nd Ed. San Francisco: Morgan Kaufmann Publishers, 2000

[12] ETSI TS 100 929 V8.0.0 (2000-10) "Digital cellular telecommunications system (Phase 2+); Security related network function" (GSM 03.20 version 8.0.0 Release 1999) France, European Telecommunications Standards Institute 2000, 2000.

[13] Gregory P. Polini and David J. Goodman, "Signaling system performance evolution for personal communications", IEEE Communication Magazine, pp. 60-65, June 1995

[14] Yi-Bing Lin, Imrich Chlamtac. **Wireless and Mobile Network Architectures.** New York: John Wiley & Sons, Inc 2001.

[15] Min-Shiang Hwang,Yuan-Liang Tang, and Cheng-Chi Lee, "An Efficient Authentication Protocol for GSM Networks", EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA , 2000 pp 326 –329

[16] Alex Birykov, Adi Shamir, David Wagner. Real Time Cryptanalysis of A5/1 on a PC. Presented at the Fast SoftwareEncryptionWorkshop, April 10-12, 2000, New York,NY.

[17] E. Biham, O. Dunkelman, "Cryptanalysis of the A5/1 GSM stream Cipher", Lecure Notes in Computer Science, vol. 1977, 2000, pp. 43–51, (Indocrypt 2000).

[18] Jovan Dj. Golic. Cryptanalysis of Alleged A5 Stream Cipher. In Proc. Eurocrypt'97, pp. 239–255, Springer Verlag 1997

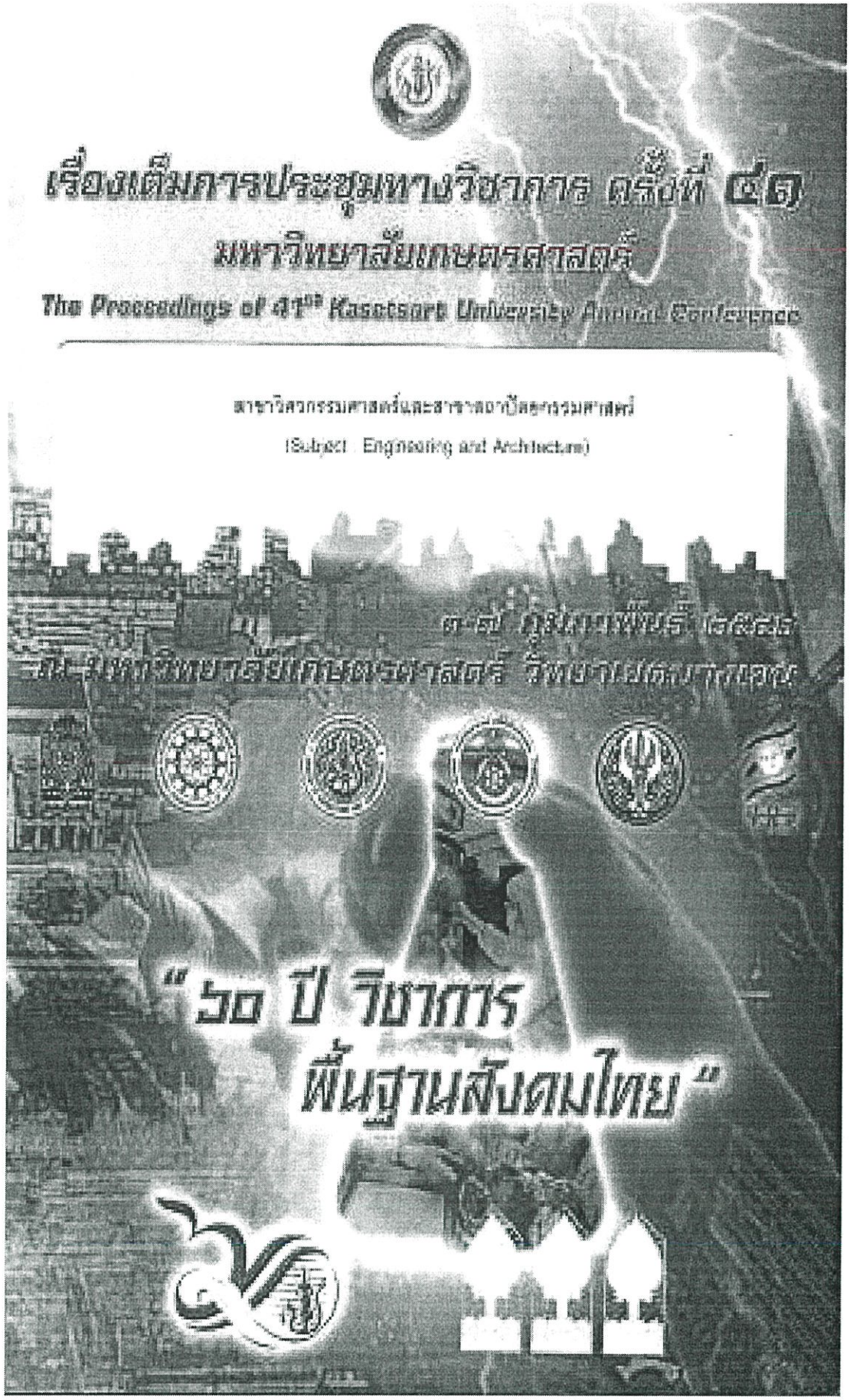
[19] B.Scheier. **Applied Cryptography: Protocol, Algorithms and Source Code in C.** 2nd Ed. John Wiley & Sons, Inc 1996

[20] Thomas F. La Porta, Malathi Veeraraghran, and Richard W. Buslens, "Comparision of signaling loads for PCS systems", IEEE/ACM Transactions on Networking, vol. 4, pp 840-855, Dec 1996

[21] Kencheng Zeng et al, "Psuedorandom Bit Generator in Stream Cipher Cryptography" IEEE Computer, Vol. 24, No. 2, Febuary 1991, pp.8-17

ภาคผนวก ก

ผลงานวิจัยในระหว่างการศึกษาที่ได้รับการตีพิมพ์เผยแพร่


เรื่องเต็มการประชุมทางวิชาการ ครั้งที่ ๔๑
มหาวิทยาลัยเกษตรศาสตร์
The Proceedings of 41st Kasetsart University Annual Conference
สาขาวิศวกรรมศาสตร์และสาขาสถาปัตยกรรมศาสตร์
(Subject Engineering and Architecture)
"๖๐ ปี วิชาการ
พื้นฐานสังคมไทย"

ฉลับรองว่าผลงานวิจัย

เรื่อง

การสื่อสารอย่างปลอดภัยสำหรับเครือข่าย GSM โดยใช้การเข้ารหัสลับแบบ Secret Key

โดย

กัมพล พรหมจิระประวัติ และบรรจง ปิยะอ่วง

ได้นำเสนอพิจารณาของคณะกรรมการผู้ทรงคุณวุฒิ สาขาวิศวกรรมศาสตร์
และได้นำเสนอในการประชุมทางวิชาการของมหาวิทยาลัยเกษตรศาสตร์ ครั้งที่ 44
ระหว่างวันที่ 3-5 กุมภาพันธ์ 2549

(ศาสตราจารย์ ดร.สุภมาศ พนิชศักดิ์พัฒนา)
รองอธิการบดีฝ่ายวิชาการ
ประธานคณะกรรมการดำเนินการจัดการประชุมทางวิชาการ ครั้งที่ 44

ผู้ทรงคุณวุฒิ
สาขาวิศวกรรมศาสตร์

1.	พีรยุทธ์	ชาญเศรษฐิกุล	2.	กรกฎ	โพนน้ำเที่ยง
3.	พีรวัฒน์	วัฒนพงศ์	4.	ปัญญา	เหล่าอนันต์ธนา
5.	ธัญญา	นิยมาภา	6.	ไพศาล	กองดาอุบาสาย
7.	เบญจพล	เวทศรีวรรณ	8.	กฤษณะ	ไวทยะ
9.	เกียรติยุทธ	กวีญาณ	10.	ปฐมาภรณ์	ศรีนพคุณวาวณ
11.	พีระยศ	แสนโภชน์	12.	วุฒิพงศ์	อารีกุล
13.	เพียงใจ	พานิชกุล	14.	เอกสิทธิ์	โตสิตสกุลชัย
15.	วิชัย	ศิวะโกศิษฐ	16.	บุษบากร	ศรีวงศ์ตานนท์
17.	วิไล	เจียมไชยศรี	18.	วรศักดิ์	สมพบ
19.	สมเจตน์	พัชราพันธ์	20.	นวพัตน์	ก้องสมุทร
21.	ผนิดา	วิญญวงศ์	22.	จันทร์เพ็ญ	อุดมโชติพฤกษ์

การสื่อสารอย่างปลอดภัยสำหรับเครือข่าย GSM โดยใช้การเข้ารหัสลับแบบ secret key

Secured communication for GSM networks using secret key encryption

กัมพล พรหมจิระประวัติ [1] และ รศ. บรรจง ปิยะธำรง [1]

Kamphol Promjiraprawat [1] and Assc. Prof. Bunjong Piyatamrong [1]

บทคัดย่อ

ในไม่กี่ปีมานี้การสื่อสารไร้สายเป็นที่นิยมกันอย่างมากทั่วโลกและมีจำนวนผู้ใช้เพิ่มขึ้นอย่างรวดเร็ว ระบบการสื่อสาร GSM ถูกพัฒนาขึ้นในระหว่างปี 1980 เป็นมาตรฐานเครือข่ายเคลื่อนที่ไร้สายที่ใช้อยู่ทั่วไปในทวีปยุโรป ปัจจุบันนี้ GSM ถูกใช้งานมากกว่า 100 ประเทศโดยมีผู้ปฏิบัติงานเครือข่ายมากกว่า 220 ราย งานวิจัยมากมายถูกนำเสนอขึ้นเพื่อที่จะทำให้การสื่อสารไร้สายมีการพัฒนามากขึ้น อย่างไรก็ตาม ความปลอดภัยของการสื่อสารเคลื่อนที่ยังคงเป็นเรื่องที่น่าเป็นห่วงมากเนื่องจากข้อมูลของผู้ใช้ถูกส่งออกไปโดยผ่านช่องสัญญาณวิทยุทำให้เครือข่ายเกิดความไม่มั่นคงที่จะถูกลักลอบดักฟัง งานวิจัยนี้เสนอวิธีการรักษาความปลอดภัยแบบใหม่บนพื้นฐานของการเข้ารหัสลับแบบ Secret Key ซึ่งไม่เพียงแต่ทำให้การจราจรของเครือข่ายลดลงเท่านั้นยังลดเวลาในการทำ Call Setup อีกด้วย ยิ่งไปกว่านั้นวิธีการที่นำเสนอยังมีความปลอดภัยอย่างมาก

ABSTRACT

In the recent years, wireless communication become popular in the worldwide, number of subscribers and users are increased rapidity. The Global System for Mobile Communication (GSM) was developed during the 1980s. GSM is the Pan-European wireless mobile system standard. Nowadays, GSM is used in more than 100 country and by over 220 network operators. A lot of research has been proposed to make the wireless communication more advantageous. However, security of the mobile communication is still major concern because the subscriber information is transmitted through radio channel, the network is vulnerable to eavesdropping. This paper presents new security method based on symmetric encryption, which is able not only to reduce the network traffic, but also to reduce call setup time. Moreover, the proposed method is highly secure.

---

1 ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

คำนำ

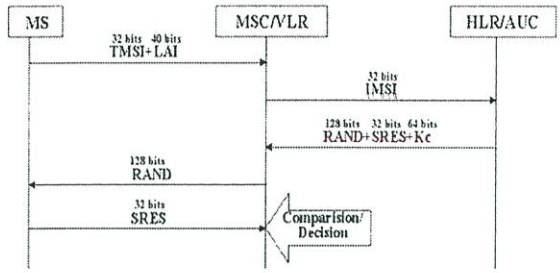
GSM (The Global System for Mobile Communication) เป็นหนึ่งในเครือข่ายเคลื่อนที่ไร้สายที่เจริญเติบโตอย่างรวดเร็วในไม่กี่ปีที่ผ่านมานี้ ผู้ใช้บริการของเครือข่าย GSM สามารถที่จะแลกเปลี่ยนข้อมูลข่าวสารต่างๆโดยปราศจากข้อจำกัดในเรื่องของเวลา, สถานที่, แม้กระทั่งเครือข่ายที่จะใช้งานอีกทั้ง Multimedia Service ซึ่งกำลังจะถูกผลักดันให้เกิดขึ้นในการสื่อสารไร้สายในยุคที่สาม (Third Generation wireless communications) เพื่อเพิ่มประโยชน์ในการใช้งานแก่ผู้ใช้บริการ อย่างไรก็ตามความปลอดภัยของการสื่อสารยังคงเรื่องสำคัญที่ต้องให้ความสนใจเนื่องจากการสื่อสารไร้สายจำเป็นต้องส่งข้อมูลผ่านทางช่องสัญญาณวิทยุซึ่งเป็นสื่อกลางที่ง่ายแก่การถูกลักลอบนำข้อมูลไปใช้อย่างไม่ถูกต้อง[7] ในงานวิจัยนี้นำเสนอวิธีการใหม่ในการจัดการเกี่ยวกับความปลอดภัยบนเครือข่าย GSM โดยมีแนวความคิดหลักๆ คือ

- เพิ่มความปลอดภัยในการป้องกันข้อมูลของผู้ใช้ไป
- ลด Transmission Load ที่ใช้ในการทำ Authentication
- ลด Delay Time ที่เกิดขึ้นเมื่อทำ Authentication
- ลด Delay Time ที่เกิดจากการเข้าและถอดรหัสลับโดยการใช้การเข้ารหัสลับแบบ Secret Key

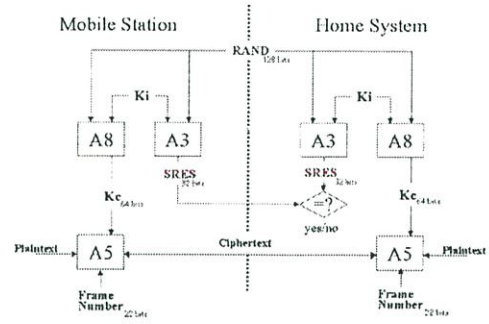
ปัญหาการรักษาความปลอดภัยสำหรับเครือข่าย GSM

สำหรับเครือข่ายไร้สายผู้ใช้บริการอุปกรณ์ไร้สายสามารถที่จะแลกเปลี่ยนข้อมูลข่าวสารต่างๆได้ปราศจากข้อจำกัดในเรื่องของเวลา, สถานที่, และเครือข่ายที่จะใช้งานซึ่งแตกต่างจากเครือข่ายใช้สายที่ถูกยึดติดอยู่กับคู่สายและเครือข่ายที่เฉพาะเจาะจง เนื่องจากความสามารถในการเคลื่อนที่ไปได้อย่างเป็นอิสระ ตำแหน่งที่อยู่ของผู้ใช้อาจถูกพิจารณาเป็นข้อมูลที่มีค่าซึ่งอาจจำเป็นที่จะต้องเก็บเป็นรักษาความลับเพื่อรักษาความเป็นส่วนตัวของผู้ใช้ ในรูปที่ 1 และ 2 แสดงลักษณะของสถาปัตยกรรมการรักษาความปลอดภัยในเครือข่าย GSM โดยในส่วนของ Authentication Protocol ซึ่งใช้วิธีการ request/response ในการตรวจสอบ Identity ของผู้ใช้ สำหรับเครือข่าย GSM ผู้ใช้จำเป็นจะต้องมีการทำ Authentication ทุกๆ 5 วินาทีระหว่างโทรศัพท์เคลื่อนที่ของผู้ใช้ (Mobile Station) กับสถานีฐาน (Base Stations) ทำให้เกิดการจราจรของข้อมูลบนเครือข่ายสูงมาก[5,6] อีกทั้งในตอนเริ่มการทำ Authentication ทางฝั่ง MS (Mobile Station) จะส่ง LAI (Location Area Identity) ซึ่งเป็นตัวระบุตำแหน่งที่อยู่ของผู้ใช้ และ TMSI (Temporary Mobile Subscriber Identity) ซึ่งเป็น Identity ชั่วคราวที่เครือข่ายกำหนดให้กับผู้ใช้ขณะที่ผู้ใช้อยู่ใน Location Area (กลุ่มของ Cell Site ต่างๆ) นั้นๆผ่านช่องสัญญาณวิทยุโดยปราศจากการป้องใดๆ ทำให้ง่ายแก่การถูกผู้ไม่ประสงค์ดีลักลอบเอาข้อมูลไปใช้ได้

จากปัญหาต่างๆที่ได้กล่าวไว้ข้างต้นนี้ งานวิจัยนี้ทำการจัดเตรียมการรักษาความลับของตำแหน่งที่อยู่และ Identity ของผู้ใช้ที่จะส่งผ่านช่องสัญญาณวิทยุใน Authentication Protocol และพยายามที่จะลด Cost ต่างๆ เกิดจากการรักษาความปลอดภัยในเครือข่าย GSM



รูปที่ 1 GSM Authentication Protocol



รูปที่ 2 GSM Security Algorithms

การปรับปรุงกระบวนการรักษาความปลอดภัยสำหรับเครือข่าย GSM

วิธีการรักษาความปลอดภัยที่นำเสนอนี้แบ่งออกเป็น 2 ส่วนคือ Authentication Protocol และการเข้า/ถอดรหัสลับของข้อมูล

Authentication Protocol

ในรูปที่ 3 แสดงลำดับขั้นตอนของ Authentication Protocol ที่นำเสนอ แนวทางในการวิจัยพยายามที่จะลด Delay Time และ Transmission Load ที่ใช้ในการทำ Authentication ในขณะเดียวกันยังสามารถเพิ่มความปลอดภัยให้กับผู้ใช้โทรศัพท์เคลื่อนที่

Authentication Protocol ที่นำเสนอมีขั้นตอนต่างๆ ดังนี้คือ

ขั้นตอนที่ 1 VLR (Visited Location Register) จะส่ง Krc (RC5 session key) ให้กับ MS ทุกๆนาที

ขั้นตอนที่ 2 MS เมื่อต้องการทำ Authentication ก็จะนำ Authentication Request ซึ่งประกอบด้วย TMSI และ LAI มาเข้ารหัสลับก่อนที่จะส่งไปให้ VLR จากรูปที่ 3 EKrc (X) แทน การเข้ารหัสลับข้อมูล X โดยใช้อัลกอริทึม RC5 และมี Krc เป็น Key ในการเข้าและถอดรหัสลับ หลังจากนี้เป็นต้นไปการติดต่อระหว่าง MS กับ VLR จะต้องทำการเข้ารหัสลับข้อมูลที่จะส่งโดยใช้ Krc เป็น Key ในการเข้าและถอดรหัสลับ

ขั้นตอนที่ 3 VLR จะถอดรหัสข้อมูลที่ได้รับโดยใช้ Krc แล้ว VLR ก็จะทราบ IMSI (International Mobile Subscriber Identity) ของผู้ใช้ได้จาก TMSI

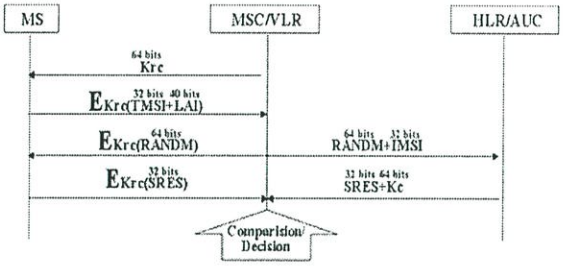
ขั้นตอนที่ 4 VLR ทำการสร้าง RANDM (Mobile Random Number) แล้ว ส่งให้ทั้ง MS และ HLR พร้อมๆกันโดยข้อมูลในส่วนที่จะส่งให้ HLR (Home Location Register) ก็จะส่ง IMSI ไปด้วย

ขั้นตอนที่ 5 ทั้ง HLR และ MS จะคำนวณหา SRES (Signature Response ขนาด 32 bits) และ Kc (Cipher Key) โดยการใช้ Ki (Authentication Key) และ RANDM ดังแสดงในรูปที่ 4 ทางฝั่ง MS จะส่ง

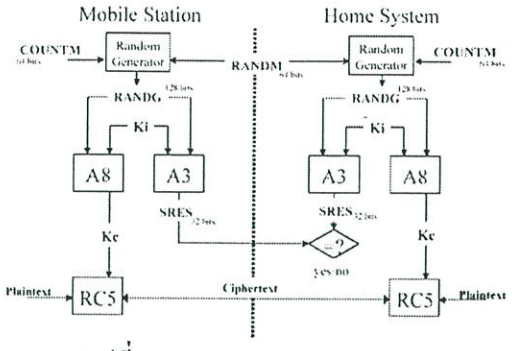
SRES ไปให้ VLR โดยจะเก็บ Kc ไว้ใช้ต่อไป ส่วนทางฝั่ง HLR ก็จะส่งทั้ง SRES และ Kc กลับไปให้ VLR

ขั้นตอนที่ 5 VLR จะทำการเปรียบเทียบ SRES ที่ได้รับจาก MS และ HLR ถ้าตรงกันการทำ Authentication เป็นอันสิ้นสุด

ความแตกต่างระหว่าง Protocol ที่นำเสนอกับ GSM Protocol จะเห็นได้ว่ามีการรักษาความปลอดภัยที่ดีขึ้นสำหรับข้อมูลที่จะถูกส่งออกไปโดยผ่านทางช่องสัญญาณคลื่นวิทยุ อย่างไรก็ตามวิธีการที่นำเสนอนี้จำเป็นที่จะต้องมีหน่วยความจำเพิ่มขึ้นทั้งทางฝั่ง MS และทางฝั่งเครือข่ายเพื่อที่จะทำให้การทำ Authentication สมบูรณ์



รูปที่ 3 Proposed Authentication Protocol



รูปที่ 4 Proposed Security Algorithms

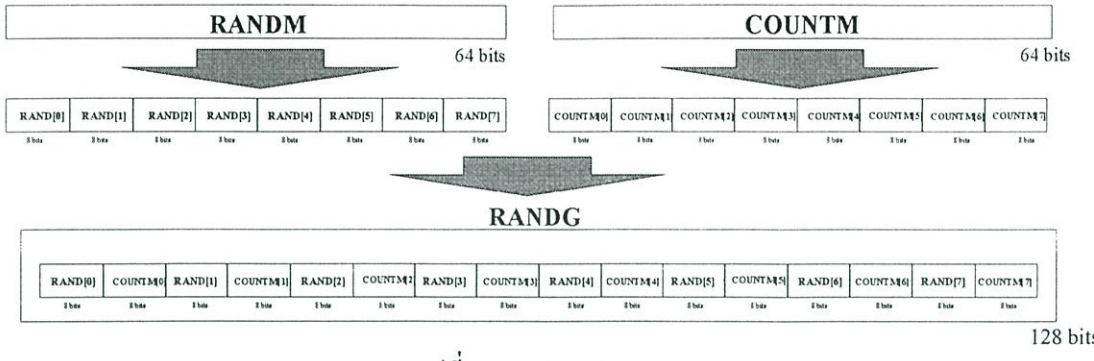
การเข้าและถอดรหัสลับ

การเข้ารหัสแบบ Secret Key คือการเข้าและถอดรหัสลับผู้สื่อสารใช้ Key อันเดียวกันในการเข้าและถอดรหัสลับ โดยปกติแล้วการเข้ารหัสแบบ Secret Key จะมีความเร็วของการเข้าและถอดรหัสลับค่อนข้างสูง[2,3]

ในงานวิจัยนี้พิจารณาเลือกใช้อัลกอริทึม RC5 แทนที่อัลกอริทึม A5 ในการเข้า/ถอดรหัสลับของข้อมูล อัลกอริทึม RC5 เป็นการเข้าและถอดรหัสลับแบบ Secret Key ถูกคิดค้นโดย Ron L. Rivest ในปี 1995 อัลกอริทึม RC5 มีความยืดหยุ่นสูงมากในการเลือกใช้ขนาดของคีย์ในการเข้ารหัสลับและจำนวนรอบที่ใช้การเข้ารหัสลับ อีกทั้งยังมีความเร็วสูงในการเข้าและถอดรหัสลับ[4]

งานวิจัยนี้ยังนำเสนอการใช้ "Mobile user events counter" (COUNTM) เพื่อลด Transmission Load และ Delay Time ในการทำ Authentication ดังแสดงใน รูปที่ 4 โดยที่ COUNTM เป็นค่าทางสถิติของเครือข่าย GSM ซึ่งถูกเก็บไว้ 2 ชุดเหมือนกันที่ MS และ AUC (Authentication Center) ทุกครั้งเมื่อมีการทำ Authentication ข้อมูล COUNTM ทั้ง 2 ชุดจะถูก update ให้เหมือนกันตลอดเวลา

ในรูปที่ 5 แสดงให้เห็นวิธีการสร้าง RANDG (Generated Random Number) โดยใช้ Random Generator เพื่อที่จะนำ RANDG ไปใช้ในคำนวณหา SRES และ Kc ต่อไป



รูปที่ 5 Random Generator

แบบจำลองการวิเคราะห์และผลการทดลอง

งานวิจัยนี้ทำการวิเคราะห์เกี่ยวกับ Transmission Load และเวลาที่ใช้ในการทำ Authentication รวมไปถึง Delay Time ที่เกิดจากการเข้าและถอดรหัสลับข้อมูล แล้วนำผลลัพธ์ที่ได้เปรียบเทียบกันระหว่างวิธีการที่นำเสนอกับวิธีการของ GSM

ก่อนที่จะทำการวิเคราะห์จำเป็นที่จะต้องตั้งข้อสมมุติเกี่ยวกับระบบเพื่อที่จะหา Cost ที่ใช้ในการทำ Authentication และการเข้าและถอดรหัสลับที่นำเสนอดังนี้

1. อัตราเร็วในการสื่อสาร (Transmission Rate) เป็น 13.3 Kbps เหมือนกันหมดทุกๆการเชื่อมต่อ
2. เวลาที่ใช้เข้า/ถอดรหัสลับของข้อมูล 64 bits โดยใช้อัลกอริทึม RC5 เป็น 0.61 msec[4] บน 50 MHz chip และเวลาที่ใช้เข้า/ถอดรหัสลับของข้อมูล 64 bits โดยใช้อัลกอริทึม A5 เป็น 4.6 msec[1]
3. ความเร็วในการสื่อสาร (Communication Speed) เป็นความเร็วเฉลี่ยที่จะส่งข้อมูลจากที่หนึ่งไปยังเป้าหมาย
4. สมมุติให้เวลาที่ใช้ในการคำนวณที่ VLR และ HLR ต่างจากที่ MS ใช้เพียงเล็กน้อย

งานวิจัยนี้แบ่งการทดลองเป็น 4 การทดลองดังนี้

ผลการทดลองที่ 1: การทดลองนี้จะพิจารณาที่ความสัมพันธ์ระหว่างเวลาที่ใช้ในการทำ Authentication กับอัตราเร็วในการสื่อสารข้อมูล ทำการวิเคราะห์เวลาที่ใช้ในการทำ Authentication แล้วกำหนดเป็นสมการต่างๆ ดังนี้

$$Taut_{gsm} = 232A + 256B \qquad (1)$$

$$Taut_{our} = \begin{cases} 136A + 192B + 144T_{crypt} ; 192B \geq 96A + 192T_{crypt} \\ 232A + 336T_{crypt} \qquad \text{elsewhere} \end{cases} \qquad (2)$$

โดยที่ $Taut_{gsm}$ แทน เวลาที่ใช้ในการทำ Authentication Protocol เมื่อใช้วิธีการของ GSM (หน่วยเป็นวินาที)

$Taut_{our}$ แทน เวลาที่ใช้ในการทำ Authentication Protocol เมื่อใช้วิธีการที่นำเสนอ (หน่วยเป็นวินาที)

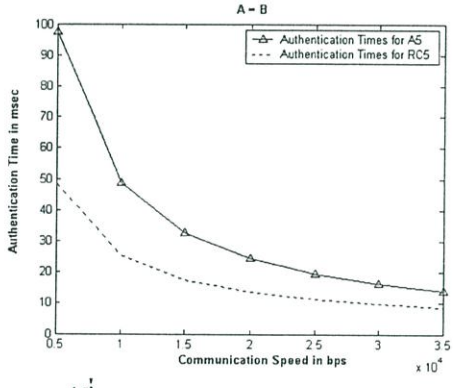
A แทน ความเร็วในการสื่อสารข้อมูล (Communication Speed) ระหว่าง MS กับ VLR (หน่วยเป็นวินาที/bit)

B แทน ความเร็วในการสื่อสารข้อมูล (Communication Speed) ระหว่าง VLR กับ HLR (หน่วยเป็นวินาที/bit)

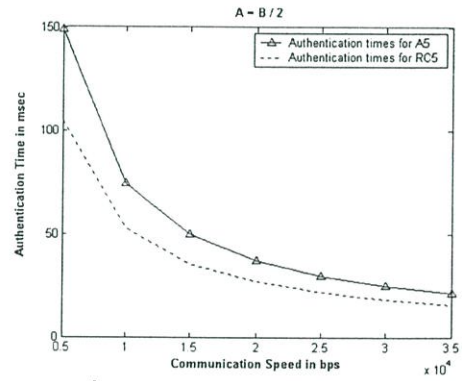
T_{crypt} แทน เวลาที่อัลกอริทึม RC5 ใช้ในการเข้าหรือถอดรหัสลับข้อมูล (หน่วยเป็นวินาที/bit)

การพิจารณาความเร็วในการสื่อสารระหว่าง MS กับ VLR และความเร็วในการสื่อสารระหว่าง VLR กับ HLR แบ่งเป็น 2 กรณีคือเมื่อ $2A = B$ และ $A = B$ ดังแสดงใน รูปที่ 6 และ 7 ตามลำดับ

ที่ความเร็วในการสื่อสารสูงๆเวลาที่ใช้ในการทำ Authentication ของวิธีการที่นำเสนอกับวิธีการของ GSM อาจจะมีความแตกต่างไม่มากนัก แต่เมื่อพิจารณาความเร็วในการสื่อสารปกติ (13.3 Kbps) เวลาที่ใช้ในการทำ Authentication ของวิธีการที่นำเสนอจะเร็วกว่าวิธีการของ GSM ในทั้ง 2 กรณี เมื่อคิดเป็น percentage แล้วเวลาที่ใช้ในการทำ Authentication ของวิธีการที่นำเสนอจะเร็วกว่าวิธีการของ GSM ประมาณ 28.7 % (กรณี $2A = B$) และ 47 % (กรณี $A = B$)



รูปที่ 7 Authentication times (A = B)



รูปที่ 6 Authentication times (2A = B)

ผลการทดลองที่ 2: การทดลองนี้จะพิจารณาที่ความสัมพันธ์ระหว่าง Delay Time ที่เกิดขึ้นจากการรักษาความปลอดภัยกับอัตราเร็วในการสื่อสารข้อมูล สมมุติให้ขนาด Packet เป็น 1422 Bytes (รวม Header ขนาด 54 bytes) โดยที่มีขนาดข้อมูลเป็น 1368 Bytes เนื่องจากขนาด block ในอัลกอริทึมการเข้ารหัสลับของ RC5 และ A5 มีขนาดไม่เท่ากัน คือ 64 bits และ 114 bits ตามลำดับ จึงจำเป็นต้องเลือกขนาดของข้อมูลให้มีความเหมาะสม เช่น จำนวนผลคูณของ 114 กับ 64 เป็นต้น ทำการวิเคราะห์ Delay Time ที่เกิดขึ้นจากการรักษาความปลอดภัยแล้วกำหนดเป็นสมการต่างๆ ดังนี้

$$D_{wos} = \frac{8(D + \frac{D}{1368}H)}{R_b} \qquad (3)$$

$$D_{wrc5} = \frac{8(D + \frac{D}{1368}H)}{R_b} + \frac{8(D + \frac{D}{1368}H)T_{rc5}}{64} \quad (4)$$

$$D_{wa5} = \frac{8(D + \frac{D}{1368}H)}{R_b} + \frac{8(D + \frac{D}{1368}H)T_{a5}}{114} \quad (5)$$

โดยที่ D_{wos} แทน Delay Time ที่เกิดขึ้นเมื่อไม่มีการรักษาความปลอดภัย

D_{wa5} แทน Delay Time ที่เกิดขึ้นเมื่อใช้อัลกอริทึม A5 เข้าและถอดรหัสข้อมูลในการรักษาความปลอดภัย

D_{wrc5} แทน Delay Time ที่เกิดขึ้นเมื่อใช้อัลกอริทึม RC5 เข้าและถอดรหัสข้อมูลในการรักษาความปลอดภัย

D แทน ขนาดของข้อมูล (หน่วยเป็น Bytes)

H แทน Header (หน่วยเป็น Bytes)

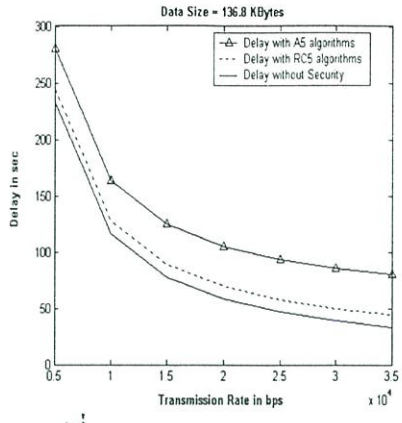
R_b แทน อัตราเร็วในการสื่อสารข้อมูล (หน่วยเป็น bps)

T_{rc5} แทน เวลาที่อัลกอริทึม RC5 ใช้เข้า/ถอดรหัสลับข้อมูล 64 bits

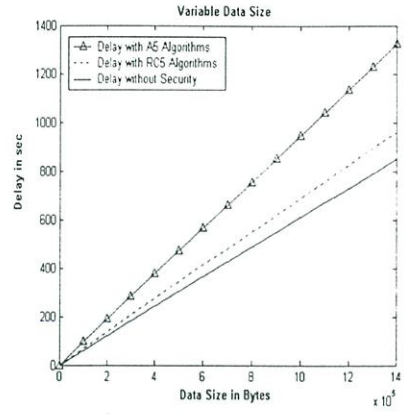
T_{a5} แทน เวลาที่อัลกอริทึม A5 ใช้เข้า/ถอดรหัสลับข้อมูล 114 bits

ดังแสดงใน รูปที่ 8, Delay Time (หน่วยเป็นวินาที) ในการส่งข้อมูลขนาด 136.8 Kbytes ผ่านช่องสัญญาณที่มีอัตราเร็วในการสื่อสารข้อมูลต่างๆ แบ่งเป็น 3 กรณี คือ กรณีที่ 1 คือไม่มีการรักษาความปลอดภัย กรณีที่ 2 คือใช้อัลกอริทึม RC5 ในการรักษาความปลอดภัย กรณีที่ 3 คือใช้อัลกอริทึม A5 ในการรักษาความปลอดภัย

เมื่อพิจารณาที่ความเร็วในการสื่อสารต่ำ (เช่น 13.3 Kbps) ความแตกต่างของ Delay Time ระหว่างการใช้อัลกอริทึม RC5 ในการรักษาความปลอดภัยกับไม่มีการรักษาความปลอดภัยประมาณ 11.1 วินาที, ความแตกต่างของ Delay Time ระหว่างการใช้อัลกอริทึม RC5 กับการใช้อัลกอริทึม A5 ในการรักษาความปลอดภัยประมาณ 35.9 วินาที และความแตกต่างของเวลาระหว่างการใช้อัลกอริทึม A5 ในการรักษาความปลอดภัยกับไม่มีการรักษาความปลอดภัยประมาณ 47 วินาที ถ้าทำการเทียบความแตกต่างเหล่านี้ในรูปแบบ Percentage จะพบว่าการใช้อัลกอริทึม RC5 ในการรักษาความปลอดภัยใช้เวลามากกว่าไม่มีการรักษาความปลอดภัย 4.77%, อัลกอริทึม A5 ในการรักษาความปลอดภัยใช้เวลามากกว่าไม่มีการรักษาความปลอดภัย 20.18% และอัลกอริทึม A5 ในการรักษาความปลอดภัยใช้เวลามากกว่าอัลกอริทึม RC5 ในการรักษาความปลอดภัย 14.71% สำหรับในการสื่อสารความเร็วสูง (เช่น 32 Kbps) Percentage ที่กล่าวมานี้จะเพิ่มขึ้นอย่างรุนแรงเป็น 80.89%, 141.23%, และ 33.36% ตามลำดับ



รูปที่ 8 Delay versus Transmission Rate



รูปที่ 9 Delay versus Data Sizes

ผลการทดลองที่ 3: เหมือนการทดลองที่ 2 โดยเปลี่ยนมาพิจารณาที่ความสัมพันธ์ระหว่าง Delay Time กับขนาดของข้อมูลส่งผ่านช่องสัญญาณ

ดังแสดงใน รูปที่ 9 เป็นการแสดง Delay Time (หน่วยเป็นวินาที) เปรียบเทียบกับขนาดของข้อมูลโดยการใช้อัตราเร็วในการสื่อสารข้อมูลคงที่คือ 13.3Kbps สำหรับข้อมูลขนาด 1 Mbytes อัลกอริทึม RC5 ใช้เวลามากกว่าไม่มีการรักษาความปลอดภัย 83.11 วินาที, อัลกอริทึม A5 ใช้เวลามากกว่าไม่มีการรักษาความปลอดภัย 351.85 วินาที ซึ่งมากกว่าประมาณ 4.23 เท่าของเวลาที่อัลกอริทึม RC5 ใช้ สำหรับข้อมูลขนาดเล็กอาจจะมีความแตกต่างไม่มากนัก อย่างไรก็ตามสำหรับการสื่อสารในอนาคต การส่งข้อมูลขนาดใหญ่ๆ (ในหน่วย MBytes) ก็จะมีความจำเป็นมากขึ้นสำหรับบริการ Multimedia และ GPRS (General Packet Radio Service)[12] ดังนั้นวิธีการที่นำเสนอน่าจะเป็นคำตอบที่ดีในการรักษาความปลอดภัยในเครือข่าย GSM

ผลการทดลองที่ 4: การทดลองนี้จะพิจารณาที่ Transmission Load ที่ใช้สำหรับการทำ Authentication เปรียบเทียบกันระหว่างวิธีการที่นำเสนอกับวิธีการของ GSM

Transmission Load ที่ใช้ใน Authentication Protocol ของ GSM คือ (TMSI+LAI) + IMSI + 2RAND + 2SRES = 424 bits

Transmission Load ที่ใช้ใน Authentication Protocol ที่นำเสนอคือ (TMSI + LAI) + IMSI + 2RANDM + 2SRES = 296 bits

โดยที่ TMSI, IMSI, และ SRES มีขนาด 32 bits

LAI มีขนาด 40 bits

RAND มีขนาด 128 bits

RANDM มีขนาด 64 bits

เพื่อที่จะรองรับการเจริญเติบโตอย่างรวดเร็วของจำนวนผู้ใช้ในเครือข่าย GSM และป้องกันปัญหาการเกิด Overload ของเครือข่าย วิธีการที่นำเสนอแสดงให้แล้วว่าช่วยทำให้ Transmission Load ในการทำ Authentication ลดลงได้เป็นอย่างดี

บทสรุป

ในงานวิจัยนี้นำเสนอวิธีการรักษาความปลอดภัยแบบใหม่สำหรับเครือข่าย GSM ซึ่งมี cost ต่างๆ ในการทำออเธนทิเคชั่นและการเข้า/ถอดรหัสลับต่ำกว่าเมื่อเปรียบเทียบกับวิธีการของ GSM อีกทั้ง Authentication Protocol ที่นำเสนอจัดเตรียมการรักษาความปลอดภัยที่สูงขึ้นสำหรับข้อมูลที่จะถูกส่งผ่านทางช่องสัญญาณวิทยุ ยิ่งไปกว่านั้นยังสามารถลด Transmission Load ของการทำ Authentication ได้เป็นอย่างดีอีกด้วย ดังนั้นวิธีการที่นำเสนอน่าจะเป็นอีกทางเลือกที่น่าสนใจในการรักษาความปลอดภัยสำหรับเครือข่าย GSM

เอกสารอ้างอิง

[1] ETSI TS 100 929 V8.1.0 (2001-07) "Digital cellular telecommunications system (Phase 2+); Security related network functions" (GSM 03.20 version 8.1.0 Release 1999)

[2] B.Scheier, "Applied Cryptography: Protocol, Algorithms and Source Code in C"; second edition, John Wiley & Sons, Inc 1996

[3] W.Stallings, "Cryptography and Network Security"; second edition, Prentice Hall, Inc 1999

[4] Ronald L. Rivest, "The RC5 Encryption Algorithm", In Proceedings of the Second International Workshop on Fast Software Encryption, pp 86-96, Leuven Belgium, Dec 1994.

[5] Gregory P. Polini and David J. Goodman, "Signaling system performance evolution for personal communications", IEEE Communication Magazine, pp. 60-65, June 1995

[6] Thomas F. La Porta, Malathi Veeraraghran, and Richard W. Buslens, "Comparision of signaling loads for PCS systems", IEEE/ACM Transactions on Networking, vol. 4, pp 840-855, Dec 1996

[7] M.J. Beller, L.F. Chang, and Y. Yacobi. "Privacy and Authentication on a Portable communications System" IEEE J. Select. Areas Commun, vol 11, no. 6, pp. 821-829, Aug. 1993

[8] Al-tawil Khalid, Ali Akrami, and IIabib Youssef, "A new authentication protocol for GSM networks", IEEE Annual Conference on Local Computer Networks, LCN'98, pp 21-30, 1998.

[9] Min Xu and Shambhu Upadhyaya, "Secure Communication in PCS", Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd , 2001 pp 2193 -2197 vol.3

[10] Min-Shiang Hwang, Yuan-Liang Tang, and Cheng-Chi Lee, "An Efficient Authentication Protocol for GSM Networks", EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA , 2000 pp 326 -329

[12] Jörg Eberapächer, Hans-Jörg Vögel, and Christian Bettstetter, "GSM: Switching, Service and Protocol"; second edition, John Wiley & Sons, Inc 2001

ภาคผนวก ข

ตัวอย่างแฟ้มข้อมูลที่ถูกเข้ารหัสลับขนาด 1026 ไบต์และแฟ้มข้อมูลที่ถูกถอดรหัสลับและคีย์ขนาด 64 บิตที่ใช้เข้าและถอดรหัสลับโดยการใช้อัลกอริทึมที่นำเสนอ

ตัวอย่างแฟ้มข้อมูลขนาด 1026 ไบต์ก่อนที่จะทำการเข้ารหัสลับโดยใช้อัลกอริทึมที่นำเสนอ

B1424DABB9$20B7BA56$25BFDE7F9C$E92DDC6F45FBE9$A745643308CA2EB25D6FF7324E53B223
9D2643CF2A51A02$266328D797BF43$10D$43C$CA3BD5BF23$CA4735EF0E9AC4E5DBC57D329A27
43223F6911B5EC1D3F54E49714D6B30A$EB39CE76D$7437386CA9BA746CE134C$5FAFC57$D453E$
26AF63C2D749A04741B46BB91F30E4$7300C640A043F$124$$52674AB62410DAC9A6964B694E708D0
346$01FCDE7C77D5CB4FA16$8BA6F152DB1D7D1BAA9FB1D3662633EB$BB517566E9345E047C926
CE7EDE96B737D106A2205$F1617A5$$22D66A5$33372FB$93E643D5EF646ECAF9$B2EBF7465F71A
B71EC4FA735EC64D$F4335E2B3760B3B7C1ACDE26F5F2DF696AFEED9CCC1A7E37F6D67A774D1
$BB0C6065C$04BD6ED3F716DEF074956398AC7CFB5E5D018$1F00269775039631554747A7935DE4CFB
454A27593EA208FB210D00740B4129EABBE6402664BC52EFC2969035693A425492D11176343029AF73
E2D42666$945AB1E1B4FA3CE1F367E53044AB45E31C7545589A33E574F26E491C1B6505F2B9EDAA
514C$$91$B9BC5E7625BD$F9C42579C2CB9701B2F5C$C3C1A0F2A9B4C95A10AF06$4E5FCC19500
1AB60$C00AB095E$D5805EBA613E5C5276C30A450C67507ADFB24$16FBB9D19826A29D0F1D467
B996D4995$BC6$6D2817DBB71A44271E33C1E2FE976B0DFEE76A$$0A7A0$40EE923$BAFCAC$071
FFCFAC65D6615D39704F3715300B559E011CE36FC15565DC7EA$ED1E792AF77FD$7F$964$5BF792
9$9416E977C66A6E92F2B$C66D1FC9204737F0394B24D9$FFA2B93E4D5$$E1F74E4BBD7EF1722E67
CF4$4C502BFD90456$$761B932B$DDC7ECA0E4A95A256B7990E1FF2$1A3C9$BC6DCBA1CEEE4
4430192FA4AF4$65396AD9F03DD316B2E92360FF5DE4B5D41E54633CF37EE177D93EA10D3E4E9C7
D57613DF077$B091C2B$18$CB79ADA0CC1593039EF$2A3C2D2ADFBBA037F69B2F9DDF$18097231
D0BE640E115C5221$1AF91059419A$0522DB090C47A312CD$05744330321C20B5FBB0DF054FCFF77
F5A4059CFC64A16C6E311FF56FCA976B67$8239B5766629576502D960FB09$349F372DCD2AE96431
DE6C67$EEB91049CA223F20ACCF04$294D163D$FA9017AFB701$170D5BFEBAAAA2358AF721052
B$66C22$571BD$6D1E1DA5AE$ECBB3724275997$5DB5FF2C300BEF6B30BC5E7$18EDFA3F5AFB3
6C9CC1D94FF903C32A344129$8B6C83C0201C3$671E9$29370126E65ADEB2421533B$57BA6B70525
A00DC5963275F51CBFC46A24D7B37BC93000219BEBE24EB204B3$EF41AD9DCA261F5C72AE550C
62$01$2D$BD1F645F15B2393F34701$3200D59C6F94D5CF7BC4E0544FEC1CD5ABFEDEADBACB6A
D6E792EC14FEC6B663$724BC9E60F64D7299A113839575 4EDC5EB64D9C4$E62EDFCA55D6EB99E
C339C06

ตัวอย่างแฟ้มข้อมูลขนาด 1026 ไบต์ที่ถูกเข้ารหัสลับโดยใช้อัลกอริทึมที่นำเสนอ

54A03$096A954DF71735335B702E79D37A47507ACD0BF114E$0A02666C07C1BB7CC55067F60A904B
170F2940B415430BDB3FE6$CF59F9C7$D$6F45D520F35C025CAB72$$1387EA0001E$5E0F5F00A540
291AB$AC054EDD1273FA3733145CS45A25835733D2FE902$F2$E28177FC2F03169$41C$FD6275$B01
F3A25C95E67FE73ECE3E43F2B6096025D7A1F2ED92659CF1CDFEBA9D9340D1A$D6C7DC4$342FE
FDE5CB3A4112A0F2622D$1EF6$$2F66EC99BB7E0EE190B050DAB$1C7F$DE2427F9910235EFBC0A
C$49FD0524A2577311115 52AE79C0F$137FDD9A$39D22DAB3D2E6AABF28766D22E26AB0$37A5090
49E7E32935F3553B905$A615CF7C520B31AEFCE$4D91927E447344D9A4BA2DB406F3F9F76BC182F
DA0770CCDF$BFF21554$4$31CF3$$F0EA$D6E$$9301CDE$B52FA9AAEDA46$CD63C2B905C175C$
E9FBCE60F94A314$5C36E29622F12DD7ACC9$FB02E0C$3E1E5B514137EA091374A2FF16AB9$A13
E24F1377144CD67187BD3976A0D60D2367E0F2536FE705$0BEC22E9F26F9F0990F526389E2024393B$
$E219CCA04256BBD7EF0ECF4962602758 7F361A244$AD829DBEE30D$A37B2991522AB542519A$6E
442C97$AF19E7626BAE9F6750D035FE$3$2EDA7CC1476D93E$C13$A9D4372E60178693CFDD35E
$CE930DFA0FB2A7250$6DA07769D53A255DBBA044C49454DABE1CE215 1$52$475457B6C2C1493C$
29A47$710$31FE5E664C1ED1C6E0440B77FB64BFE5235C5C7769$$FE3DD03E5EFC94$D5E70$E3
A0B30D4E$E3BAA4C0D54DBE7B$ABBA5$2A1B7E66703FEE131F0B39FCB6A25FC05$9A$60D4E0D
1BA2A00C3EEAAF31CBC9D2DD075$3B1B30E9B$A0DE$AE3$14$9CD6D04A3D941$8$E1F6182B3FA
56F9FD3B49$ED5DDBE0E736C915EB27$F3441$0B691B31635A$20017DD99E7B4A50A1FC7C1BA9A
EA56D13C193$EE5FD$CD11A$2B79B2E73$0$2F50B$C$794EE7$BC3F75CFB62C04$8436C2EDC554
6FBBA$3AE3B25C7CAE44C0B04C3A394B143F03D64273629D6951$6C302AB987F799F7975521F$4$3
AA14C$AA00$7256C34A$A03FA6F5B900BC92A4E903CC53E$41C0706E93552C300654C1A7AFC7D5
C337BE5A$$FBB2FB75D4439$44159075DACBEC064B6AE345$043A7E42D$3E969A4CB94$AD76E9C
322231C3FF30BC22C0009587FF$CC455C07D4$CB001E4D07E97A1F963D5A6D57$0CC14AB5A0F63F
91E5A77DD570C5F29BFC9453F7CA13$A31F694AF$B2ABC3BC5BFE659D7D1E7B6$DF21D3D5FCE
9D1A73F3FB9C4CADF4DBA69031E$1B1E61D11C64D5C9860AC269D466C0E218539343 7FFE$42D6B
FC4D269C75$B1F436B0$C2CDF7AB230B77465E5B1B67AE4ACCB76709B732EDD5BA7$5FF1E7$20
F0F62A3E0FAE15ADE3A952EB0CA4D55152D43F7CACA0$6236045E0DF73A$4$7AADB7C3D37A0$
D9B2F2B$B9B295400

ตัวอย่างคีย์ที่ใช้ในการเข้าและถอดรหัสลับ (Kc) ขนาด 64 บิต

$CBC62F4AE0E$2AD

ประวัติผู้เขียน

นายกัมพล พรหมจิระประวัติ เกิดวันที่ 14 มกราคม พ.ศ. 2519 ที่จังหวัดกรุงเทพมหานคร จบการศึกษาวิทยาศาสตร์บัณฑิต สาขาคณิตศาสตร์ประยุกต์ คณะวิทยาศาสตร์ประยุกต์ จากสถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ ปีการศึกษา 2542 หลังจากนั้นเข้าศึกษาต่อในระดับบัณฑิตศึกษา หลักสูตรวิศวกรรมศาสตร์มหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2544

ผลงานทางวิชาการที่ได้รับการตีพิมพ์

กัมพล พรหมจิระประวัติ และ รศ. บรรจง ปิยธำรง "การสื่อสารอย่างปลอดภัยสำหรับเครือข่ายGSM โดยใช้การเข้ารหัสลับแบบ secret key" การประชุมวิชาการของมหาวิทยาลัยเกษตรศาสตร์ ครั้งที่ 41 3-7 กุมภาพันธ์ 2546

Kamphol Promjiraprawat and Assoc.Prof. Bunjong Piyatamrong "Secured Communications for GSM Networks" International Conference on Telecommunications 2003 (ICT'2003) February 23- March 1, 2003 Tahiti, Papeete-French Polynesia