การออกแบบและสร้างรหัสรักษาความปลอดภัยสำหรับกระบวนการตรวจสอบและยืนยันตัวตนของระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ

Design and Implementation of Security Code for the Identification and Authentication Process of Electronic Toll Collection System

ปราชญ์ อัศวนรากุล[1] และอำนวย เรืองวารี[1*]
Prach Asavanarakul[1] and Amnoiy Ruengwaree[1*]

Received: June 20, 2019; Revised: August 26, 2019; Accepted: September 3, 2019

บทคัดย่อ

การขับเคลื่อนวิสัยทัศน์ประเทศไทย 4.0 ด้านอุตสาหกรรมการบินและโลจิสติกส์ไปสู่ความสำเร็จจำเป็นต้องใช้เทคโนโลยีที่รวดเร็ว ปลอดภัย และน่าเชื่อถือสูง อาร์เอฟไอดีเป็นเทคโนโลยีสำคัญที่นำมาประยุกต์ใช้ในระบบคมนาคมขนส่งเพื่อตรวจสอบและยืนยันตัวตนของผู้โดยสาร ยานพาหนะ และสินค้า อย่างไรก็ตาม การนำอาร์เอฟไอดีมาประยุกต์ใช้ยังพบปัญหาด้านการรักษาความลับหรือความปลอดภัยของข้อมูลรหัสที่ใช้ตรวจสอบและยืนยันตัวตน บทความวิจัยนี้นำเสนอวิธีการเพิ่มความปลอดภัยในการนำอาร์เอฟไอดีมาประยุกต์ใช้ในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ โดยการออกแบบและสร้างรหัสรักษาความปลอดภัยที่เรียกว่า Meta_ID และโพรโทคอลยืนยันตัวตนของเครื่องอ่านและป้ายอาร์เอฟไอดี จำลองสถานการณ์ระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่ใช้รหัส Meta_ID และโพรโทคอลที่นำเสนอ เปรียบเทียบกับระบบดั้งเดิมที่โปรแกรมรหัสลงบนป้ายของผู้ใช้งานแบบตายตัว กรณีมีจำนวนผู้ใช้ป้ายในระบบ 10,000 100,000 และ 1,000,000 ป้าย ผลการจำลองพบว่าระบบที่นำเสนอมีค่าความน่าจะเป็นของความสำเร็จในการล้วงรหัสต่ำกว่าระบบดั้งเดิมทั้ง 3 กรณี จึงสรุปได้ว่าระบบที่นำเสนอมีสมรรถนะด้านการรักษาความลับหรือความปลอดภัยดีกว่าระบบดั้งเดิม

คำสำคัญ : อาร์เอฟไอดี; เลขสุ่มเทียม; ระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ: อีทีซี; โลจิสติกส์

[1] *คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี*
[1] *Faculty of Engineering, Rajamangala University of Technology Thunyaburi*
[*] *Corresponding Author E - mail Address: amnoiy.r@en.rmutt.ac.th*

Abstract

To drive aviation and logistics in Thailand 4.0, it is necessary to use a fast, safe and reliable technology. Radio Frequency Identification (RFID) has adopted into the transportation system in order to identify and authenticate the passengers, vehicles and goods. However, The RFID in transport application still has some problem about the security of ID data. This article presents a method for increasing security in applying RFID to be used in electronic toll collection system. By design and create a security code called Meta_ID and authentication protocol of the RFID reader and tag. Simulate an electronic toll collection system that uses the Meta_ID code and proposed protocol, compared with the original system that uses the fix security code, in the case of 10,000, 100,000 and 1,000,000 user's tags. The simulation results show that the proposed system has a lower probability of hacking success than the original system in all 3 cases. Therefore, concluded that the proposed system has the security performance better than original system.

Keywords: RFID; Pseudo Random Number; Electronic Toll Collection System: ETC; Logistics

บทนำ

ในปี พ.ศ. 2558 รัฐบาลไทยได้กำหนดวิสัยทัศน์เชิงนโยบายที่เรียกว่า ประเทศไทย 4.0 (Thailand 4.0) เพื่อพัฒนาเศรษฐกิจของประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน ด้วยการพัฒนาอุตสาหกรรม 10 กลุ่ม หนึ่งในนั้นซึ่งถือว่ามีความสำคัญคืออุตสาหกรรมการบินและโลจิสติกส์ (Aviation and Logistics) กลไกสำคัญในการขับเคลื่อนอุตสาหกรรมกลุ่มนี้คือ การขนส่งและบริการด้านโลจิสติกส์ที่ต้องการความรวดเร็ว ปลอดภัย และมีความน่าเชื่อถือสูง ทั้งการคมนาคมทางอากาศ และภาคพื้นดิน การนำเทคโนโลยีเข้ามาพัฒนาปรับใช้ในกระบวนการตรวจสอบและยืนยันตัวตนในการผ่านทาง การผ่านด่าน และการขนส่งสินค้าจึงถือว่าจำเป็นอย่างยิ่ง ปัจจุบันประเทศไทยพัฒนาการคมนาคมขนส่งไปสู่ระบบอัตโนมัติ เพื่อรองรับปริมาณประชากร ยานพาหนะ และการขนส่งสินค้าที่เพิ่มขึ้น การบ่งชี้หรือระบุเอกลักษณ์วัตถุด้วยคลื่นความถี่วิทยุ (Radio Frequency Identification) เรียกสั้น ๆ ว่า อาร์เอฟไอดี (RFID) เป็นเทคโนโลยีสำหรับการบ่งชี้เอกลักษณ์วัตถุหรือสิ่งของด้วยคลื่นความถี่วิทยุเพื่อการยืนยันตัวตนของวัตถุหรือสิ่งของนั้น (Identification and Authentication) ปัจจุบันได้ถูกนำไปประยุกต์ใช้อย่างกว้างขวางในกิจการคมนาคมขนส่งและโลจิสติกส์ [1] – [2]

การประยุกต์ใช้อาร์เอฟไอดีในกิจการคมนาคมขนส่งและโลจิสติกส์ อย่างเช่น ระบบผ่านทางและตั๋วโดยสารอิเล็กทรอนิกส์ (E-ticket) ยังมีปัญหาด้านการชนกันของข้อมูล (Collision) รวมถึงการรักษาความปลอดภัยของข้อมูล (Security) ในกระบวนการยืนยันตัวตน เช่น การถอดแบบหรือโคลนนิ่งรหัสหรือบัตรป้ายเพื่อใช้ซ้ำ (Cloning Problem) การดักจับรหัสและข้อมูลลับระหว่างการรับส่งในกระบวนการตรวจสอบรหัส (Tracking Problem) เป็นต้น มีบทความวิจัยหลายบทความได้เสนอการพัฒนาอาร์เอฟไอดี

ให้มีความปลอดภัยของข้อมูลเพื่อนำไปใช้ในงานด้านต่าง ๆ ยกตัวอย่างเช่น [3] ได้เสนอการวิเคราะห์โพรโทคอล (Protocol) ป้องกันการชนกันของข้อมูลสำหรับการชี้เฉพาะสินค้าด้วยคลื่นความถี่วิทยุในระบบการจัดการโลจิสติกส์ โดยสรุปไว้ว่า ระบบอาร์เอฟไอดีที่ใช้โพรโทคอล ABS หรือ AQS มีความเหมาะสมที่จะนำไปประยุกต์ใช้ในการคมนาคมขนส่งและโลจิสติกส์ [4] ได้เสนอการออกแบบระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่ใช้งานร่วมระหว่างอาร์เอฟไอดีกับการประมวลผลภาพ [5] ได้เสนอโพรโทคอลอาร์เอฟไอดีที่ป้องกันการถอดแบบ [6] ได้เสนอการสร้างกุญแจรหัสที่มีความปลอดภัยในการส่งผ่านข้อมูล [7] ได้เสนอการพัฒนาประสิทธิภาพของระบบอาร์เอฟไอดีโดยใช้การสื่อสารแบบ Frame ALOHA [8] ได้เสนอโพรโทคอลน้ำหนักเบาสำหรับการสื่อสารด้วยอาร์เอฟไอดีที่มีคุณสมบัติการยืนยันตัวตนแบบสองทาง รวมถึงงานวิจัย [9] – [11] ที่เสนอโพรโทคอลที่มีความปลอดภัยในการตรวจสอบและยืนยันตนของระบบอาร์เอฟไอดี

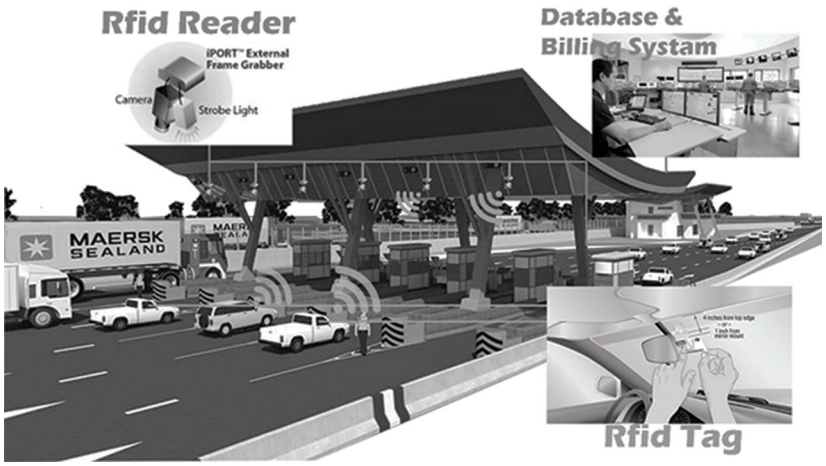
อย่างไรก็ตาม โพรโทคอลที่มีความปลอดภัยสูงย่อมมีความสลับซับซ้อนและต้องการทรัพยากรสูงตามไปด้วย อาทิเช่น ความสามารถประมวลผลของไมโครชิพ หน่วยความจำ และแหล่งพลังงานของอาร์เอฟไอดี ทำให้เกิดอุปสรรคในการนำไปใช้งานจริงในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ ตั๋วโดยสารและโลจิสติกส์ ซึ่งใช้อาร์เอฟไอดีชนิดต้นทุนต่ำ (Low-Cost RFID) เป็นทรัพยากรหลัก ดังนั้นจึงเป็นที่มาของวัตถุประสงค์การวิจัยนี้คือ (1) ออกแบบและสร้างรหัส Meta_ID สำหรับการรักษาความปลอดภัยที่ยากต่อการลอกเลียนแบบหรือทำซ้ำ (2) ทดสอบใช้งานในสถานการณ์จำลองกระบวนการตรวจสอบรหัสลับและยืนยันตัวตนของเครื่องอ่านและป้ายอาร์เอฟไอดีชนิดต้นทุนต่ำที่ใช้ในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ (3) ประเมินผลด้านการรักษาความปลอดภัยของระบบที่นำเสนอเปรียบเทียบกับระบบเดิม

วิธีดำเนินการวิจัย

1. **ศึกษาการประยุกต์ใช้งานอาร์เอฟไอดีในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ**

การบ่งชี้หรือระบุเอกลักษณ์วัตถุด้วยคลื่นความถี่วิทยุหรืออาร์เอฟไอดีเป็นเทคโนโลยีที่พัฒนาต่อเนื่องมาจากรหัสแท่งหรือบาร์โค้ด (Barcode) ที่ใช้อย่างแพร่หลายในระบบขนส่งสินค้า ระบบจัดเก็บและตรวจสอบสินค้าคงคลัง การตรวจสอบสินค้าในห้างสรรพสินค้าและร้านสะดวกซื้อ รวมถึงในระบบตั๋วโดยสาร เช่น ตั๋วรถไฟ ตั๋วเครื่องบิน เป็นต้น ระบบบาร์โค้ดใช้วิธีประมวลผลภาพรหัสแท่งในการยืนยันตัวตน การใช้งานบาร์โค้ดจึงต้องระมัดระวังไม่ให้แผ่นป้ายรหัสแท่งเกิดความเสียหาย อีกทั้งยังต้องระมัดระวังเรื่องการลอกเลียนหรือทำซ้ำซึ่งสามารถทำได้โดยง่าย เช่น การถ่ายภาพรหัสแท่งด้วยโทรศัพท์มือถือและนำไปใช้ซ้ำ เป็นต้น ปัจจุบันได้มีการพัฒนาอาร์เอฟไอดีมาใช้ในงานที่ต้องการความปลอดภัยสูงกว่าบาร์โค้ด เนื่องจากมีข้อดีกว่าหลายประการ เช่น (1) ประสิทธิภาพการระบุสินค้าหรือสิ่งของที่ดีกว่าเดิมจากการส่งสัญญาณคลื่นความถี่วิทยุโต้ตอบกันของเครื่องอ่าน (Reader) กับป้าย (Tag) ที่บรรจุรหัสลับ (Code) ที่ใช้ในการตรวจสอบและยืนยันตัวตนของสินค้าหรือสิ่งของ (2) ป้ายอาร์เอฟไอดีฝังอยู่ในตัวสินค้าหรือหีบห่อไม่มีการสัมผัสกับเครื่องอ่าน ไม่ต้องมองเห็น อาศัยการส่งสัญญาณคลื่นความถี่วิทยุระยะไกลพอประมาณ ทำให้มีความทนทานและคล่องตัวกว่าระบบเดิม สามารถอ่านรายการสินค้าในโกดังหรือตู้ขนส่งสินค้าได้โดยไม่จำเป็นต้องมองเห็นสิ่งของหรือสินค้านั้น ๆ ด้วยเหตุนี้ อาร์เอฟไอดีจึงเป็นที่นิยมนำมาใช้ในกิจการต่าง ๆ ที่ต้องการความมั่นคงปลอดภัย ซึ่งหนึ่งในนั้นคือ ระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ (Electronic Toll Collection System: ETC) ดังแสดงในรูปที่ 1 ปัจจุบันการทางพิเศษแห่ง

ประเทศไทยได้นำระบบเก็บค่าผ่านทางพิเศษอัตโนมัติมาใช้ในหลายเส้นทางในพื้นที่กรุงเทพมหานครและปริมณฑล อาทิเช่น เส้นทางพิเศษฉลองรัช เส้นทางพิเศษบางพลี-สุขสวัสดิ์ เส้นทางบูรพาวิถี เส้นทางมอเตอร์เวย์บางนา-บางประอิน และอื่น ๆ ทั้งนี้เพื่อเพิ่มประสิทธิภาพการจัดเก็บค่าผ่านทาง และลดเวลาในแถวหรือคิว (Queue) รอจ่ายค่าผ่านทาง



รูปที่ 1 ระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ

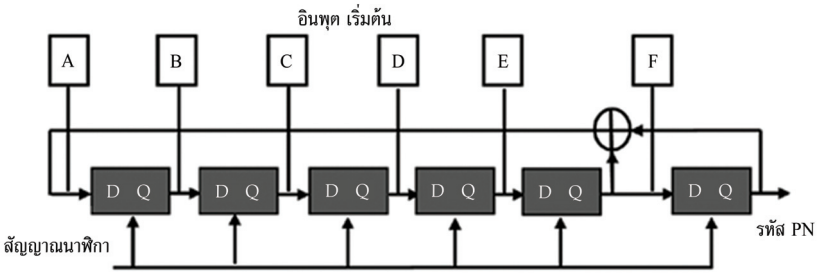
องค์ประกอบของอาร์เอฟไอดีในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติมี 3 ส่วนที่สำคัญแสดงดังรูปที่ 1 คือ (1) ป้ายอาร์เอฟไอดี (RFID Tag) เป็นตัวเก็บรหัสหรือหมายเลข ID ที่ใช้สำหรับการตรวจสอบและยืนยันตัวตน โดยทั่วไปแล้วป้ายอาร์เอฟไอดีแบ่งออกเป็น 2 ประเภทคือ ป้ายพาสซีพ (Passive Tag) เป็นป้ายที่ไม่มีแบตเตอรี่ในตัวเอง ทำงานโดยอาศัยพลังงานจากการเหนี่ยวนำสนามแม่เหล็กไฟฟ้าจากเครื่องอ่าน มีวิสัยการรับส่งข้อมูลระยะสั้น ๆ ใช้กับช่องทางจ่ายเงินสด และป้ายแอคทีพ (Active Tag) เป็นป้ายที่มีแบตเตอรี่ในตัวเอง ทำงานโดยอาศัยพลังงานแบตเตอรี่และพลังงานไฟฟ้าจากการเหนี่ยวนำสนามแม่เหล็กไฟฟ้าจากเครื่องอ่านข้อมูล วิสัยการรับส่งข้อมูลมีระยะไกล สามารถติดตั้งบริเวณกระจกหน้ายานพาหนะได้ (2) เครื่องอ่านข้อมูล (RFID Reader) ประกอบด้วย วงจรกำเนิดสนามแม่เหล็กไฟฟ้า วงจรรับส่งข้อมูลและอ่านรหัสหรือหมายเลข ID จากป้ายที่เข้ามาในวิสัยทำการ เครื่องอ่านข้อมูลจะติดตั้งบริเวณทางเข้าช่องผ่านทางอัตโนมัติ และ (3) ระบบฐานข้อมูลและการเรียกเก็บเงิน (Database and Billing System) ทำหน้าที่เก็บข้อมูลของผู้ใช้งานทั้งเลขรหัสสำหรับการยืนยันตัวตน ยอดเงินในบัญชี การคำนวณค่าผ่านทางและการตัดยอดบัญชีอัตโนมัติ ระบบฐานข้อมูลจะติดตั้งในอาคารสำนักงานควบคุมด่านผ่านทาง และเชื่อมต่อผ่านโครงข่ายสื่อสารไปยังฐานข้อมูลกลางเพื่อให้บริการครอบคลุมได้หลายเส้นทาง

2. ออกแบบและสร้างรหัสรักษาความปลอดภัย

กุญแจรหัสเพื่อการรักษาความปลอดภัย คือ รหัสลับข้อมูลที่ใช้ในกระบวนการยืนยันตัวตนของอาร์เอฟไอดี ซึ่งจะต้องมีหนึ่งเดียวในระบบ (Uniqueness) รหัสนี้จะถูกกำหนดขึ้นเพื่อบ่งบอกข้อมูลเฉพาะตัวในกระบวนการตรวจเอกลักษณ์และการยืนยันตน (Identification and Authentication) เครื่องอ่านจะทำการติดต่อกับป้ายอาร์เอฟไอดี เมื่อเครื่องอ่านสามารถอ่านข้อมูลรหัสจากป้ายและเปรียบเทียบ

ตรงกับฐานข้อมูลรหัสได้ เครื่องอ่านจะยืนยันตัวตนของป้ายหรืออีกนัยหนึ่งคือยืนยันผู้ใช้นั่นเอง อย่างไรก็ตาม ข้อมูลรหัสนี้จะต้องเป็นความลับระหว่างเครื่องอ่านและป้ายนี้เท่านั้น ทั้งนี้เพื่อป้องกันการแทรกแซง หรือการล้วงข้อมูล หรือการโจมตีเพื่อล้วงรหัส (Hacking) จากผู้ไม่ประสงค์ดี

บทความนี้นำเสนอวิธีการสร้างรหัสลับจากวงจรอิเล็กทรอนิกส์ที่เรียกว่า Maximum Length Sequence Pseudo-Random Noise Generation เรียกสั้น ๆ ว่ารหัส PN [12] แสดงในรูปที่ 2



รูปที่ 2 วงจรสร้างรหัสเลขสุ่มเทียมแบบ Maximum Length Sequence Pseudorandom Noise [12]

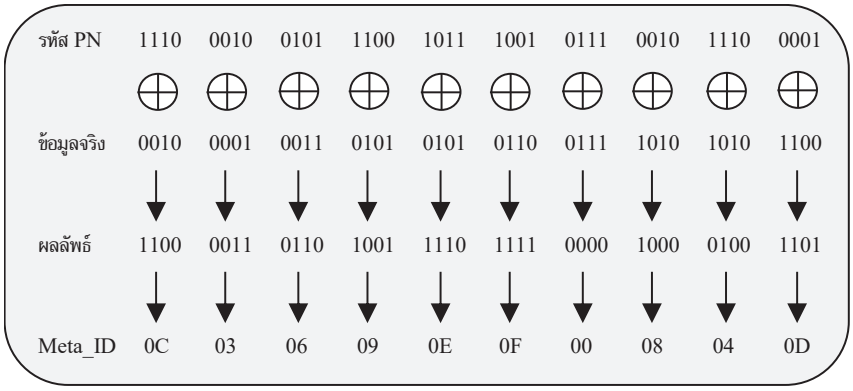
รหัส PN เป็นรหัสที่สร้างขึ้นจากวงจรอิเล็กทรอนิกส์ที่ประกอบด้วย ชิพต์รีจิสเตอร์ (Shift Register) จำนวนหนึ่งที่ต่อเชื่อมกันแบบอนุกรมเพื่อทำหน้าที่เป็นองค์ประกอบการประวิง (Delay Element) และมีการป้อนกลับของสัญญาณจากชิฟต์รีจิสเตอร์ (Feedback Loop) อย่างน้อย 2 ตำแหน่งกลับไปยังทางด้านขาเข้าของชิฟต์รีจิสเตอร์ตัวแรก ชุดวงจรนี้สามารถสร้างลำดับความยาวสูงสุด (Maximum-Sequence หรือ M-Sequence) ได้เท่ากับ $2^n - 1$ เมื่อ n คือ จำนวนของชิฟต์รีจิสเตอร์ที่ใช้ทั้งหมด อย่างไรก็ตาม การให้ได้มาซึ่งรหัสที่มีความแตกต่างกันนั้นขึ้นอยู่กับค่าเริ่มต้นของ Delay Element และตำแหน่งแท็ป (Taps) ของ Feedback Loop ดังรูปที่ 2 ซึ่งเขียนอยู่ในรูปโพลิโนเมียลได้ดังสมการที่ (1)

$$X^n + ... + X^4 + X^3 + X^2 + X + 1 \tag{1}$$

เมื่อ

X^n คือ ตำแหน่งของชิพต์รีจิสเตอร์ที่ทำการแท็ปสัญญาณทางด้านขาออกอย่างน้อย 2 ตำแหน่งที่นำมารวมกันตามกฎมอดูโล 2 (Modulo2) แทนด้วยเครื่องหมาย $\oplus$ ในรูปที่ 2

เมื่อนำรหัส PN ที่ออกแบบและสร้างขึ้นไปรวมแบบมอดูโล 2 กับข้อมูลจริง จะได้รหัสลับที่เรียกว่า Meta_ID ซึ่งเป็นรหัสที่จะนำไปเขียนลงหน่วยความจำในไมโครชิพของป้ายอาร์เอฟไอดี ความสลับซับซ้อนหรือความยากในการแก้รหัสจะขึ้นอยู่กับการออกแบบ Feedback Loop รวมถึงข้อมูลค่าเริ่มต้นใน Delay Element ที่กำหนดโดยผู้สร้าง ตัวอย่างเช่น ข้อมูลจริงที่ต้องการบันทึกในป้ายคือ 2135567AAC แปลงเป็นเลขฐานสองแล้วนำไปรวมกับรหัส PN ที่สร้างขึ้น จากนั้นแปลงผลลัพธ์เลขฐานสองเป็นฐานสิบหก จะได้รหัส Meta_ID ที่จะเขียนลงหน่วยความจำในไมโครชิพของป้ายดังรูปที่ 3



รูปที่ 3 ผลรวมแบบมอดูโล 2 ของรหัส PN กับข้อมูลจริง

3. ออกแบบโพรโทคอลอาร์เอฟไอดี

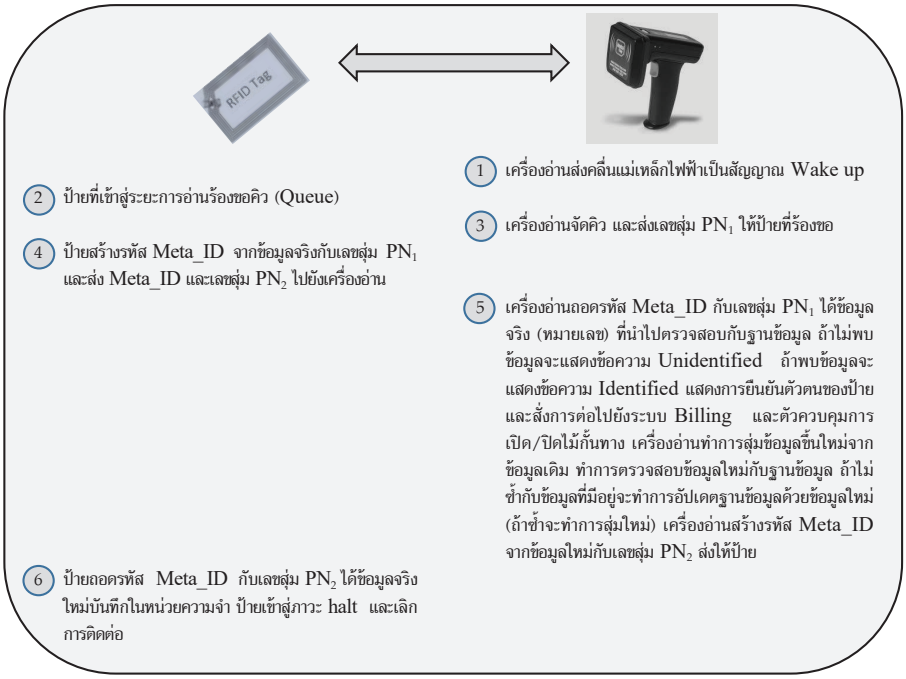
ลำดับขั้นตอนและข้อกำหนดในกระบวนการติดต่อสื่อสารกันระหว่างเครื่องอ่านข้อมูล (รวมทั้งฐานข้อมูล) กับป้ายเรียกว่า โพรโทคอล (Protocol) มีกระบวนการโดยรวมคือ เมื่อป้ายเข้ามาในวิสัยทำการของเครื่องอ่าน เครื่องอ่านจะทำการจัดคิวอ่านป้ายเพื่อป้องกันการชนกันของข้อมูล กรณีมีป้ายปริมาณมาก ๆ อยู่ในวิสัยทำการของเครื่องอ่าน ซึ่งจะส่งผลให้การยืนยันตนเกิดความผิดพลาด โดยเฉพาะการยืนยันตนของป้ายบัตรโดยสาร หรือกรณีการประยุกต์ใช้กับสินค้าที่อยู่บนสายพานลำเรียงหรือสินค้าที่บรรจุในตู้คอนเทนเนอร์เคลื่อนที่ บทความวิจัยนี้ได้นำโพรโทคอลป้องกันการชนกันของข้อมูลมาประยุกต์ใช้เพื่อทดสอบกับป้ายอาร์เอฟไอดีชนิด 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Standard [13] จากนั้นทำการออกแบบโพรโทคอลการสื่อสารและการยืนยันตัวตนของอาร์เอฟไอดีสำหรับระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่ใช้รหัสรักษาความปลอดภัยที่นำเสนอ ขั้นตอนต่าง ๆ สามารถแสดงดังรูปที่ 4

จากรูปที่ 4 กระบวนการติดต่อสื่อสารระหว่างเครื่องอ่านและป้ายอาร์เอฟไอดีจะผ่านการเข้ารหัสลับเพื่อรักษาความปลอดภัยสำหรับระบบเก็บค่าผ่านทางพิเศษอัตโนมัติทั้งขาไปและขากลับ รหัสลับที่ใช้ติดต่อสื่อสารจะสร้างจากเลขสุ่มด้วยวงจรอิเล็กทรอนิกส์ที่เรียกว่า Maximum Length Sequence Pseudo-Random Noise Generator ดังแสดงในหัวข้อ 2. รหัสลับดังกล่าวมีเฉพาะเครื่องอ่านกับป้ายที่กำลังติดต่อสื่อสารเท่านั้นที่รู้จัก อีกทั้งรหัสลับที่ใช้ติดต่อสื่อสารในแต่ละครั้งถูกสร้างขึ้นเพื่อใช้เพียงครั้งเดียว จึงเป็นการยากที่จะติดตามแกะรอยข้อมูลจริงได้ในเวลาอันสั้น ซึ่งในการติดต่อสื่อสารแต่ละครั้งจะใช้เวลาเพียงไม่กี่มิลลิวินาทีเท่านั้น [3]

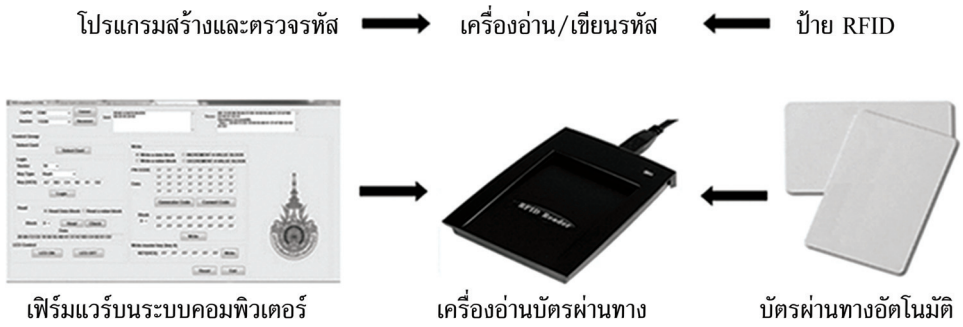
4. จำลองสถานการณ์

การจำลองสถานการณ์ระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ ในส่วนของการออกแบบและสร้างรหัส Meta_ID ตั้งแต่การสร้างรหัส PN การรวมแบบมอดูโล 2 การแปลงเลขฐาน และการยืนยันตัวตนของป้าย (การเข้ารหัส ถอดรหัส และตรวจสอบรหัสข้อมูล) จะดำเนินการอยู่บนเฟิร์มแวร์ (Firmware) ที่เขียนขึ้นด้วยโปรแกรม Microsoft Visual Studio ส่วนการติดต่อสื่อสารระหว่างเครื่องอ่าน/เขียนข้อมูลกับป้ายอาร์เอฟไอดี จะทำการเชื่อมต่อผ่าน RFID 13.56 MHZ Read/Write Mifare Module ซึ่งเป็นไปตามข้อกำหนดมาตรฐาน 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag

Interface Standard สำหรับการจำลองการทดสอบการทำงานของอาร์เอฟไอดีชนิดต้นทุนต่ำที่ใช้ในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติสามารถแสดงดังรูปที่ 5 ซึ่งประกอบด้วย 3 ส่วนหลัก ได้แก่ ส่วนที่หนึ่งคือ โปรแกรมที่ใช้สร้าง ตรวจสอบ และยืนยันตัวตนจะทำงานอยู่บนระบบคอมพิวเตอร์ ส่วนที่สองคือ เครื่องอ่าน/เขียนรหัสเลือกใช้ตัวเทียบเท่ากับเครื่องอ่านบัตรผ่านเข้า/ออกของด่านผ่านทางพิเศษ และส่วนสุดท้ายคือ ป้ายอาร์เอฟไอดีเลือกใช้แบบเดียวกับบัตรผ่านทางพิเศษอัตโนมัติ พารามิเตอร์สำหรับการจำลองสถานการณ์กำหนดไว้ดังตารางที่ 1



รูปที่ 4 โพรโทคอลการสื่อสารและยืนยันตัวตนระหว่างเครื่องอ่านข้อมูลกับป้ายอาร์เอฟไอดี



รูปที่ 5 การจำลองสถานการณ์รหัส Meta_ID สำหรับอาร์เอฟไอดีชนิดต้นทุนต่ำในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ

ตารางที่ 1 พารามิเตอร์สำหรับการจำลองสถานการณ์

พารามิเตอร์	รายละเอียด
Standard	ISO/IEC 14443 Type A
Device	RFID 13.56 MHz Read/Write Mifare Module
Meta_ID length (HEX)	10 บิต
Delay element	64
PN maximum length	18446744073709551615

ผลการวิจัยและการอภิปรายผล

ทำการทดสอบโปรแกรมรหัส (เลข ID) ตัวอย่าง 7D 74 DB 66 9A ลงในป้ายอาร์เอฟไอดีของผู้ใช้งานด้วยโปรแกรมที่ใช้สร้างรหัส Meta_ID และโพรโทคอลที่นำเสนอแล้วนำไปอ่านและยืนยันตัวตนตามสถานการณ์จำลองในรูปที่ 5 จำนวน 5 ครั้ง ได้ผลดังตารางที่ 2 พบว่าข้อมูลที่อ่านได้มีค่าตรงกับฐานข้อมูลแต่มีค่าเปลี่ยนไปทุกรอบการอ่าน เนื่องจากมีการอัปเดตรหัสใหม่ทุกครั้งที่ประสบผลสำเร็จ สถานะของการยืนยันตัวตนคือ Identified แสดงถึงการยืนยันตัวตนสำเร็จ จากนั้นนำป้ายอาร์เอฟไอดีเดียวกันนี้มาโปรแกรมรหัสตัวอย่าง 7D 74 DB 66 9A อีกครั้ง แล้วนำไปอ่านด้วยเครื่องอ่านอาร์เอฟไอดีแบบดั้งเดิม ได้ผลดังตารางที่ 3 พบว่า เครื่องอ่านทำการอ่านข้อมูลซ้ำหลายครั้ง แต่ข้อมูลที่อ่านได้ไม่ตรงกับรหัส (หมายเลข) ในฐานข้อมูล สถานะของการยืนยันตัวตนคือ Unidentified แสดงถึงการยืนยันตัวตนไม่สำเร็จ

ตารางที่ 2 ผลการยืนยันตัวตนของป้ายด้วยเครื่องอ่านอาร์เอฟไอดีที่ใช้โพรโทคอลที่นำเสนอ

ครั้งที่	ข้อมูลรหัส (เลข **ID**) ที่เขียนลงป้ายและฐานข้อมูล	ข้อมูลที่อ่านได้จากตัวอ่านอาร์เอฟไอดีที่นำสนอ	สถานะ (**Status**)
1	7D 74 DB 66 9A	7D 74 DB 66 9A	Identified
2	1A 26 12 C1 70	1A 26 12 C1 70	Identified
3	D8 40 E9 91 26	D8 40 E9 91 26	Identified
4	08 7A 52 64 f2	08 7A 52 64 f2	Identified
5	87 36 3C DA 60	87 36 3C DA 60	Identified

ผลการทดสอบในตารางที่ 2 แสดงให้เห็นว่า การเขียน/อ่านข้อมูลในป้ายอาร์เอฟไอดีด้วยเครื่องอ่านที่ใช้รหัส Meta_ID ตามโพรโทคอลที่นำเสนอสามารถยืนยันตัวตนของป้ายได้ร้อยละ 100 ส่วนตารางที่ 3 แสดงให้เห็นว่า เครื่องอ่านอาร์เอฟไอดีแบบดั้งเดิมไม่สามารถอ่านและยืนยันตัวตนป้ายอาร์เอฟไอดีที่ใช้รหัส Meta_ID ตามโพรโทคอลแบบใหม่ที่นำเสนอได้

ตารางที่ 3 ผลการยืนยันตัวตนของป้ายด้วยเครื่องอ่านอาร์เอฟไอดีแบบดั้งเดิม

ครั้งที่	ข้อมูลรหัส (เลข ID) ที่เขียนลงป้ายและฐานข้อมูล	ข้อมูลที่อ่านได้โดยตัวอ่านอาร์เอฟไอดีแบบดั้งเดิม	สถานะ (Status)
1	7D 74 DB 66 9A	FF FF E8 13 9E 26 AF C5 72 44 BC 6D 78 50 66 2F 66 8F 95 67 45 40 35 DF 54 56 7D 1D A0 10 8F BE 40 0B FF FF	Unidentified
2	7D 74 DB 66 9A	FF FF 8E 4F A0 34 03 7C 72 20 46 12 BD 7B 74 BE F7 38 F3 3B 7B 52 99 66 54 32 87 62 65 3B 9D 2F D1 BC FF FF	Unidentified
3	7D 74 DB 66 9A	FF FF 11 9D E6 03 8B 4F CC 42 16 A7 D0 8D 9B 7D 9E 10 6C E9 3D 65 11 55 EA 50 D7 D7 08 CD 72 EC B8 94 FF FF	Unidentified
4	7D 74 DB 66 9A	FF FF 36 9D 38 35 76 31 A3 23 54 74 1E C1 16 D3 18 59 4B E9 E3 53 EC 2B 85 31 95 04 C6 81 FF 42 3E DD FF FF	Unidentified
5	7D 74 DB 66 9A	FF FF FB DF 2A 7B E4 2B 0D D3 A0 B2 0F 9A E9 7E C8 0E 86 AB F1 1D 7E 31 2B C1 61 C2 D7 DA 00 EF EE	Unidentified

การวิเคราะห์ความปลอดภัยของระบบที่นำเสนอจากค่าพารามิเตอร์ที่กำหนดในตารางที่ 1 ป้ายอาร์เอฟไอดีที่ใช้เป็นแบบ Mifare Classic 1K สามารถบันทึกข้อมูลซ้ำได้ 100,000 ครั้ง บนมาตรฐาน ISO/IEC 14443 Type A เป็นป้ายอาร์เอฟไอดีที่มีต้นทุนต่ำมีความยาวของรหัสเท่ากับ 10 บิต (HEX) โดยในหนึ่งระบบสามารถกำหนดรหัส (เลข ID) ที่ไม่ซ้ำกันได้ทั้งหมด 16^{10} = 1,099,511,627,776 หรือประมาณ 1 ล้านล้านรหัส ข้อแตกต่างของระบบที่นำเสนอกับระบบดั้งเดิมคือ ระบบดั้งเดิมเมื่อทำการโปรแกรมรหัส (เลข ID) ลงในป้ายของผู้ใช้งานใด ๆ แล้วจะไม่สามารถนำมาใช้ซ้ำได้อีก รหัส (เลข ID) ได้จากการสุ่มเลือกและเขียนลงในหน่วยความจำของป้ายเมื่อเปิดใช้งาน ความน่าจะเป็นของความสำเร็จในการล้วงรหัส (Probability of Hacking Success: $p(N_A)$) จะขึ้นอยู่กับจำนวนผู้ใช้ในระบบ และจำนวนครั้งของความพยายามโจมตีเพื่อล้วงรหัส (Number of Attraction) ความน่าจะเป็นของความสำเร็จในการล้วงรหัสกำหนดดังสมการที่ (2)

$$p(N_A) = \frac{N_A \cdot N_L}{16^{10}} \tag{2}$$

โดยที่

N_A คือ จำนวนครั้งที่พยายามโจมตี

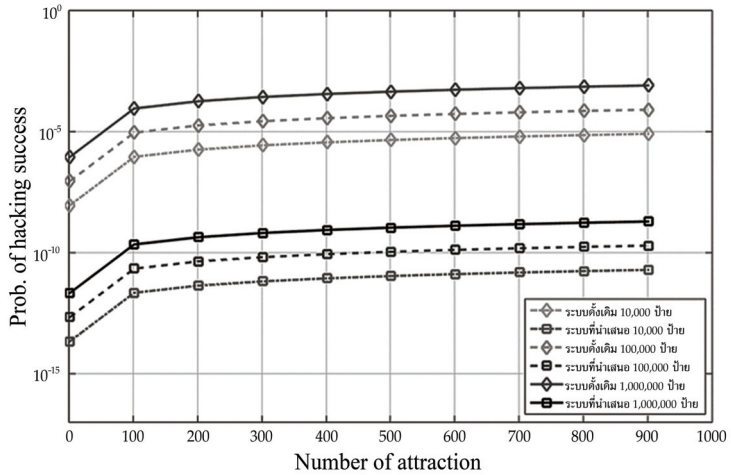
N_L คือ จำนวนผู้ใช้หรือป้าย

ในบทความนี้กำหนดองค์ประกอบการประวิง (Delay Element) จำนวน 64 ตัว สามารถสร้างรหัสที่มีความยาวรอบเท่ากับ $2^{64} - 1 = 18,446,744,073,709,551,615$ หรือประมาณ 18×10^{18} ชิพ ระบบจะทำการสุ่มตัดรหัสครั้งละ 40 ชิพจากทั้งหมดเพื่อรวมกับข้อมูลจริง (เลข ID ของป้าย) 10 หลักแบบมอดูโล 2 การรวมเป็นแบบบิตต่อบิต นอกจากนี้ระบบมีการดำเนินการอัปเดตรหัสใหม่ทุกครั้งที่มีการยืนยันตัวตนสำเร็จ รหัสลับที่ใช้ติดต่อสื่อสารเป็นเลขสุ่มขึ้นมา และเปลี่ยนทุกครั้งที่ทำการสื่อสารทั้งขาไปและขากลับตามโพรโทคอลที่นำเสนอในหัวข้อ 3. ทำให้ความน่าจะเป็นของความสำเร็จในการล้วงรหัสยากขึ้นไปอีก ความน่าจะเป็นของความสำเร็จในการล้วงรหัสดังกล่าวสามารถกำหนดดังสมการที่ (3)

$$p(N_A) = \frac{N_A \cdot N_L}{\left(2^{64} - 1\right)/40} \tag{3}$$

ทำการวิเคราะห์เปรียบเทียบความน่าจะเป็นของความสำเร็จในการล้วงรหัสระหว่างระบบเก็บค่าผ่านทางพิเศษอัตโนมัติแบบดั้งเดิมที่ใช้อาร์เอฟไอดีที่โปรแกรมรหัส (เลข ID) ลงในป้ายของผู้ใช้งานแบบตายตัวเมื่อเปิดใช้งานกับระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่ใช้รหัส Meta_ID และอัปเดตรหัสทุกครั้งที่ใช้งานและมีการยืนยันตัวตนสำเร็จตามโพรโทคอลที่นำเสนอดังรูปที่ 5 ผลการวิเคราะห์เปรียบเทียบแสดงดังรูปที่ 6

จากรูปที่ 6 ผลการจำลองสถานการณ์และวิเคราะห์ระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่ใช้ RFID แบบดั้งเดิมที่ใช้อาร์เอฟไอดีที่โปรแกรมรหัสลงบนป้ายของผู้ใช้งานแบบตายตัว (แทนด้วยสัญลักษณ์ ◊) เทียบกับแบบใหม่ที่ใช้รหัส Meta_ID และอัปเดตรหัสทุกครั้งที่ใช้งานและมีการยืนยันตัวตนสำเร็จตามโพรโทคอลที่นำเสนอ (แทนด้วยสัญลักษณ์ □) ในสถานการณ์ที่มีจำนวนป้ายหรือผู้ใช้ป้ายในระบบ 3 กรณี คือ 10,000 100,000 และ 1,000,000 ป้าย/ผู้ใช้ และใช้ความพยายามโจมตีเพื่อล้วงรหัสจำนวน 1 100 200 300 400 500 600 700 800 900 ครั้ง จะพบว่ากราฟความน่าจะเป็นของความสำเร็จในการล้วงรหัสของแบบที่นำเสนอมีค่าต่ำกว่าแบบดั้งเดิมทุกกรณี



รูปที่ 6 ผลการเปรียบเทียบความน่าจะเป็นของความสำเร็จในการล้วงรหัสระหว่างระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่ใช้อาร์เอฟไอดีแบบดั้งเดิมกับแบบที่นำเสนอ

สรุป

บทความวิจัยนี้ได้เสนอวิธีการแก้ปัญหาการรักษาความปลอดภัยในการนำอาร์เอฟไอดีมาใช้ในระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ โดยการออกแบบรหัสรักษาความปลอดภัยที่เรียกว่า Meta_ID เพื่อประยุกต์เข้ากับโพรโทคอลยืนยันตัวตนของเครื่องอ่านและป้ายอาร์เอฟไอดีของระบบเก็บค่าผ่านทางพิเศษอัตโนมัติ การจำลองสถานการณ์ของระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่มีจำนวนป้ายหรือผู้ใช้ป้ายในระบบ 3 กรณีคือ 10,000 100,000 และ 1,000,000 ป้าย/ผู้ใช้ พบว่าระบบเก็บค่าผ่านทางพิเศษอัตโนมัติที่ใช้รหัส Meta_ID และอัปเดตรหัสทุกครั้งที่ใช้งานตามโพรโทคอลที่นำเสนอมีค่าความน่าจะเป็นของความสำเร็จในการล้วงรหัสต่ำกว่าระบบดั้งเดิมที่ใช้อาร์เอฟไอดีที่โปรแกรมรหัสลงบนป้ายของผู้ใช้งานแบบตายตัวทั้ง 3 กรณี จากข้อมูลดังกล่าวสามารถยืนยันได้ว่าระบบที่นำเสนอมีสมรรถนะด้านการรักษาความลับหรือความปลอดภัยดีกว่าระบบดั้งเดิม รหัส Meta_ID ที่ออกแบบและสร้างขึ้นสามารถโปรแกรมลงในไมโครชิพของป้ายอาร์เอฟไอดีชนิดต้นทุนต่ำที่ใช้เป็นบัตรผ่านทางพิเศษได้ อย่างไรก็ตาม การนำไปใช้งานในสถานการณ์จริงต้องปรับปรุงเฟิร์มแวร์ของเครื่องอ่านและเขียนข้อมูลของระบบเดิมเป็นระบบที่นำเสนอในบทความนี้

กิตติกรรมประกาศ

ขอขอบคุณผู้ทรงคุณวุฒิที่ให้คำวิจารณ์อันทรงคุณค่าสำหรับบทความวิจัยนี้ และขอบคุณคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ที่สนับสนุนการวิจัยให้สำเร็จลุล่วงด้วยดี

References

[1] Syed Ahson and Mohammed Ilyas. (2008). **RFID Handbook: Applications, Technology, Security and Privacy**, N.Y.: CRC Press.

[2] Kovinthaweewattana, P., Cheunta, W., Kuankid, S., Baongam, W., and Dinsakul, H. (2009). **Radio Frequency Identification (RFID) System**. National Science and Technology Development Agency (NSTDA.). (in Thai)

[3] Vaodee, S., Dabbang, P., and Oncheanjit, J. (2010). Anti-Collision Protocol Analysis for Radio Frequency Identification in Logistics Management System. In **Proceedings of the Industrial Engineering Network 2010**. Ubonratchathani. (in Thai)

[4] Tang Z. (2016). The Design of ETC System Based on RFID and Image Identification. In **Proceedings of the 2016 International Conference on Energy, Power and Electrical Engineering**. pp. 236-240. Shenzhen, China. DOI: 10.2991/epee-16.2016.53

[5] Dimitriou, T. (2005). A lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks. In **First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)**. Athens, Greece. pp.59-66. DOI: 10.1109/SECURECOMM.2005.4

[6] Kungpisdan, S. and Metheekul, S. (2009). A Secure Offline Key Generation with Protection Against Key Compromise. In **WMSCI 2009: 13th World Multi-Conference on Systemics, Cybernetics and Informatics**. 10-13 July 2009, Orlando, Florida. pp. 63-67

[7] Mungmee, S. and Sittichivapak, S. (2009). Development Efficiency of RFID System in Frame ALOHA Communication. **Ladkrabang Engineering Journal**. Vol. 26, No. 2, pp. 7-12 (in Thai)

[8] Pechto, S. and Kungpisadan, S. (2010). Design and Development of a Lightweight RFID Security Protocol Offering Mutual Authentication. In **Proceedings of the 3rd National Conference on Information Technology (NCIT2010)**. Bangkok. (in Thai)

[9] Lee, Y. K. and Verbauwhede, I. (2005). **Secure and Low-Cost RFID Authentication Protocols**. Access (4 June 2019). Available (https://www.researchgate.net/publication/250139714_Secure_and_ Low-cost_RFID_Authentication_Protocols)

[10] Khan, G. N. and Moessner, M. B. (2011). Secure Authentication Protocol for RFID Systems. In **Proceedings of the 20th International Conference on Computer Communications and Networks (ICCCN)**. Mauri, Hawaii. pp. 379-384

[11] Peng, P. and Zhao, Y. (2012). Anti-Cloning and Secure RFID Mutual Authentication Protocols. In **Proceedings of the 4th IEEE Conference on Broadband Network and Multimedia Technology**. Shenzhen, China. pp. 379-384

[12] Dabbang, P. (2003). **Performance Analysis of Hybrid DS/SFH SSMA in Multi-user and Multi-rate Environment**. M. Eng. Dissertation King Mongkut's University of Technology Ladkrabang.

[13] GS1 EPC global. (2011). **Specification for EPC HF RFID Air Interface**. Access (4 June 2019). Available (https://www.gs1.org/sites/default/files/docs/epc/epcglobal_hf_2_0_3-standard-20110905r3.pdf)