บัตร RFID ชนิด MIFARE Classic 1k

เก่ง จันทร์นวล

---

1. บทนำ

บัตร RFID หรือคีย์การ์ด RFID เป็นเทคโนโลยีที่นิยมนำมาใช้ในงานระบุตัวตนโดยใช้คลื่นความถี่วิทยุ ตัวอย่างเช่น ใช้เป็นบัตรเข้าออกประตู กุญแจรถยนต์อัจฉริยะ บัตรประตัวพนักงาน/นักศึกษา แท็กติดกับตัวสินค้า บัตรคูปองอาหาร เป็นต้น MIFARE Classic 1k เป็นบัตรชนิดที่สามารถส่งข้อมูลระหว่างอุปกรณ์อ่านบัตรแบบไม่ต้องสัมผัสเพียงแค่นำบัตรและอุปกรณ์อ่านบัตรอยู่ในระยะที่เหมาะสมก็สามารถทำได้ นอกจากนั้นบัตรชนิดนี้ยังสามารถเก็บข้อมูลที่เป็นตัวอักขระได้นักพัฒนาสามารถนำไปประยุกต์ใช้กับระบบงานต่างๆ ได้อย่างหลากหลาย

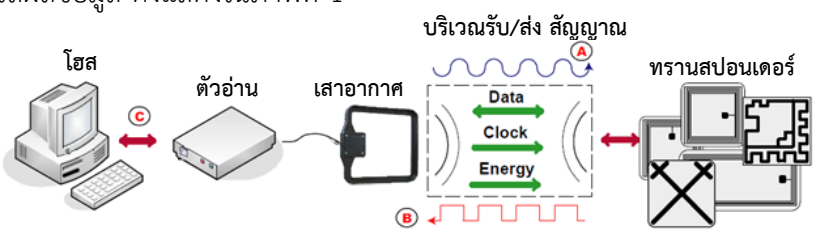
ดังนั้นเอกสารฉบับนี้ จึงได้ศึกษาเกี่ยวกับบัตร RFID ชนิด MIFARE Classic 1k รวมถึงได้ทำการทดลองอ่านข้อมูลและเขียนข้อมูลลงบนบัตร ด้วยบอร์ด RFID-RC522 ซึ่งเป็นอุปกรณ์ที่สามารถอ่านข้อมูลจากบัตรและเขียนข้อมูลลงบนบัตรชนิดนี้ได้ โดยการศึกษาค้นคว้าครั้งนี้มีวัตถุประสงค์เพื่อเป็นแนวทางนำเอาเทคโนโลยี RFID มาประยุกต์ใช้กับระบบงานจริงที่กำลังพัฒนาอยู่ รวมถึงนิสิตนักศึกษา และผู้ที่สนใจ สามารถนำมาศึกษาเรียนรู้ เพื่อพัฒนาระบบและประยุกต์ใช้กับงานในส่วนที่เกี่ยวข้องได้อีกด้วย

2. ระบบ RFID

ระบบ RFID (Radio Frequency Identification System) เป็นเทคโนโลยีระบุตัวตนอัตโนมัติ ซึ่งเป็นการนำเอาอุปกรณ์อิเล็กทรอนิกส์ไปใช้เพื่อระบุเอกลักษณ์ของรายการหรือวัตถุ

2.1 องค์ประกอบของระบบ RFID

โดยทั่วไประบบ RFID จะประกอบด้วย 1) ทรานสปอนเดอร์ (Transponder) หรือเรียกว่า แท็ก (Tag) ทำหน้าที่ส่งสัญญาณหรือข้อมูลที่บันทึกอยู่ในแท็ก 2) ตัวอ่าน (Reader) ทำหน้าที่การรับข้อมูลที่ส่งมาจากแท็ก แล้วทำการตรวจสอบความผิดพลาดของข้อมูล ถอดรหัสข้อมูล และ 3) โฮส หมายถึงเครื่องคอมพิวเตอร์ที่ทำหน้าที่คอยประมวลผลข้อมูล ดังแสดงในภาพที่ 1



3. ตัวอ่านทำการถอดรหัสและส่งต่อไปยังโฮส (C)
1. ตัวอ่านส่งคลื่นแม่เหล็กไฟฟ้าไปยังทรานสปอนเดอร์ (เพื่อเป็นพลังงาน)
2. ทรานสปอนเดอร์ส่งหมายเลขประจำตัว/ข้อมลกลับไปยังตัวอ่าน (B)

ภาพที่ 1 องค์ประกอบของระบบ RFID

หลักการทำงานเบื้องต้นของระบบคือ ตัวอ่านจะส่งคลื่นแม่เหล็กไฟฟ้าออกมาตลอดเวลา และคอยตรวจจับว่ามีทรานสปอนเดอร์เข้ามาอยู่ในบริเวณสนามแม่เหล็กไฟฟ้าหรือไม่ หรืออีกนัยหนึ่งก็คือการคอยตรวจจับว่ามีการมอดูเลตสัญญาณเกิดขึ้นหรือไม่ เมื่อมีทรานสปอนเดอร์เข้ามาอยู่ในบริเวณสนามแม่เหล็กไฟฟ้า ทรานสปอนเดอร์จะได้รับพลังงานไฟฟ้าที่เกิดจากการเหนี่ยวนำของคลื่นแม่เหล็กไฟฟ้าที่ส่งมาจากตัวอ่าน เมื่อทรานสปอนเดอร์ได้รับพลังงานจะเริ่มต้นทำงานคือจะส่งข้อมูลในหน่วยความจำที่ผ่านการมอดูเลตกับคลื่นพาหะแล้วออกมาทางสายอากาศที่อยู่ภายในทรานสปอนเดอร์ ตัวอ่านข้อมูลจะคอยตรวจจับความเปลี่ยนแปลงของคลื่นพาหะที่เกิดจากการมอดูเลตแล้วทำการถอดรหัสเพื่อนำข้อมูลและส่งต่อให้กับโฮสเพื่อนำไปใช้งานต่อไป

การสื่อสารข้อมูลที่เกิดขึ้นในระบบ RFID จะทำการส่งข้อมูลผ่านคลื่นวิทยุ ข้อมูลที่เก็บในทรานสปอนเดอร์จะประกอบด้วย หมายเลขบัตร รหัสรักษาปลอดภัย รหัสสินค้า และข้อมูลอื่นๆ ที่จำเป็น ตัวอ่านจะมีระบบป้องกันเหตุการณ์การอ่านข้อมูลจากทรานสปอนเดอร์เดิมซ้ำ เรียกว่าระบบ "Hands Down Polling" โดยตัวอ่านข้อมูล จะสั่งให้ในทรานสปอนเดอร์หยุดการส่งข้อมูลในกรณีเกิดเหตุการณ์ดังกล่าว หรืออาจมีบางกรณีที่มีหลายในทรานสปอนเดอร์อยู่ในบริเวณสนามแม่เหล็กไฟฟ้าพร้อมกัน หรือที่เรียกว่า "Batch Reading" ตัวอ่านข้อมูลควรมีความสามารถที่จะจัดลำดับการอ่านทรานสปอนเดอร์ทีละตัวได้

2.2 ประเภทของทรานสปอนเดอร์

ทรานสปอนเดอร์มีหลากหลายมากทั้งรูปร่าง ขนาด ความสามารถ และวัสดุที่ใช้ อาจมีขนาดเล็กเท่าปลายดินสอหรือเมล็ดข้าว หรือมีขนาดใหญ่ถึง 6 นิ้ว ซึ่งถูกสร้างขึ้นมามีรูปร่างหลากหลายเช่น กุญแจ บัตรเครดิต แคปซูล แผ่นจาน แถบ เป็นต้น ทรานสปอนเดอร์สามารถมีเสาส่งสัญญาณแบบโลหะที่ติดตั้งไว้ภายในตัวเอง หรือติดตั้งไว้อยู่ภายนอก หรือแบบใหม่จะเป็นเสาส่งสัญญาณแบบแผ่นวงจรพิมพ์

ทรานสปอนเดอร์มีอยู่สองแบบคือแบบพาสซีฟ (Passive) ทำงานโดยไม่ต้องมีแหล่งจ่ายกระแสไฟฟ้าอยู่ภายใน และแบบแอคทีฟ (Active) ต้องมีแหล่งจ่ายกระแสไฟฟ้าอยู่ภายในตัวเอง ซึ่งทรานสปอนเดอร์จะมีความสามารถทั้งอ่านข้อมูลอย่างเดียวหรือทั้งอ่าน/เขียนข้อมูลได้ ส่วนระยะการตรวจจับสัญญาณระหว่างทรานสปอนเดอร์และตัวอ่านสามารถแตกต่างกันได้อาจมีระยะอ่านได้ไม่กี่เซ็นติเมตรไปจนถึงระยะอ่านได้ห่างเป็นเมตรขึ้นอยู่กับกำลังไฟฟ้า ความถี่ของสัญญาณวิทยุที่ใช้ และประเภทและขนาดของเสาส่งสัญญาณ

ย่านความถี่หรือการแพร่พลังงานสำหรับระบบ RFID ถูกจำกัดไว้โดยหน่วยงานรัฐบาล [FCC 2001] ดังนั้นการเลือกใช้ความถี่ใดขึ้นอยู่กับความต้องการของการประยุกต์ใช้งาน เทคโนโลยี RFID ในปัจจุบันที่ได้รับความนิยมใช้งานและคุณลักษณะทั่วไปสามารถแสดงดังตารางที่ 1

ตารางที่ 1 เทคโนโลยี RFID ที่นิยมใช้งานและคุณลักษณะทั่วไป

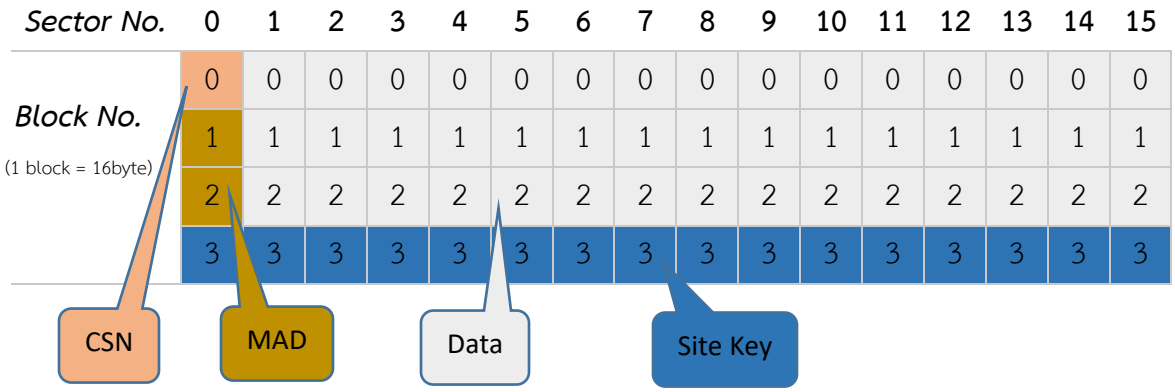
ย่านความถี่	ช่วงอ่าน	คุณลักษณะทั่วไป	การประยุกต์ใช้งาน	RFID โปรโตคอล
Low 100 – 500 kHz	สูงถึง 4-6 นิ้ว	- ช่วงอ่านระยะสั้นถึงปานกลาง - ราคาถูก - ความเร็วอ่านต่ำ - สามารถอ่านข้อมูลผ่านของเหลวได้	- บัตรผ่านเข้า-ออกประตู - ติดตามเฝ้าดูสัตว์ - ควบคุมสินค้าคงคลัง - กุญแจอัจฉริยะของรถยนต์	ISO/IEC 18000-2
High 10 - 15 MHz	สูงถึง 8 ฟุต	- ช่วงอ่านระยะสั้นถึงปานกลาง - ราคาค่อนข้างไม่แพง - ความเร็วอ่านข้อมูลระดับกลาง - สามารถอ่านข้อมูลผ่านของเหลวได้	- บัตรผ่านเข้า-ออกประตู - สมาร์ทการ์ด (บัตรประจำตัวประชาชน บัตรเครดิต) - ติดตามสิ่งของ - อุปกรณ์อิเล็กทรอนิกส์รักษาความปลอดภัย	ISO/IEC 18000-3 EPC HF Class 1 ISO/IEC 15693 ISO 14443 (A/B) I-Code, Tag-It, Hitag, MiFare
Ultra-high 850 – 950 MHz	10-20 ฟุต	- ช่วงอ่านระยะยาว - ความเร็วการอ่านสูง - ลดโอกาสของการเกิดการชนกันของสัญญาณ - เกิดปัญหากับของเหลวและโลหะ	- เฝ้าติดตามการขนส่งสินค้าทางตู้สินค้า - ระบบเก็บเงินค่าผ่านทาง - ใช้ในระบบห่วงโซ่อุปทาน - ติดตามสิ่งของ	ISO 18000-6 EPC Class 0, Class 1
Microwave 2.4 – 5.8 GHz	น้อยกว่า 3 ฟุต	- ช่วงอ่านปานกลาง - มีโอกาสเกิดการชนกันของสัญญาณ - มีอัตราการถ่ายโอนข้อมูลสูงมาก - เกิดปัญหากับของเหลวและโลหะ	- เฝ้าติดตามการขนส่งสินค้าทางตู้สินค้า - ระบบเก็บเงินค่าผ่านทาง - ติดตามสัมภาระของสายการบิน	ISO/IEC 18000-4

3. บัตร MIFARE Classic 1k

MIFARE เป็นเทคโนโลยีที่ถูกพัฒนาภายใต้มาตรฐาน ISO/IEC 14443 Type A ซึ่งส่งด้วยสัญญาณวิทยุที่ความถี่ HF 13.56 MHz

3.1 โครงสร้างหน่วยความจำ

บัตร MIFARE Classic 1K เป็นบัตรที่มีหน่วยความจำ โดยแบ่งออกเป็นเซกเตอร์ แต่ละเซกเตอร์แบ่งออกเป็นบล็อก บล็อกละ 16 ไบต์ เซกเตอร์ของหน่วยความจำภายในบัตรมีทั้งหมด 16 เซกเตอร์ ซึ่งแต่ละเซกเตอร์จะถูกแบ่งออกเป็น 4 บล็อก ดังนั้นเราสามารถคำนวณโครงสร้างของหน่วยความจำได้ดังนี้ 16 ไบต์ (1 บล็อก) x 4 บล็อก x 16 เซกเตอร์ = 1024 ไบต์



ภาพที่ 2 โครงสร้างหน่วยความจำที่อยู่ในบัตร MIFARE Classic 1K

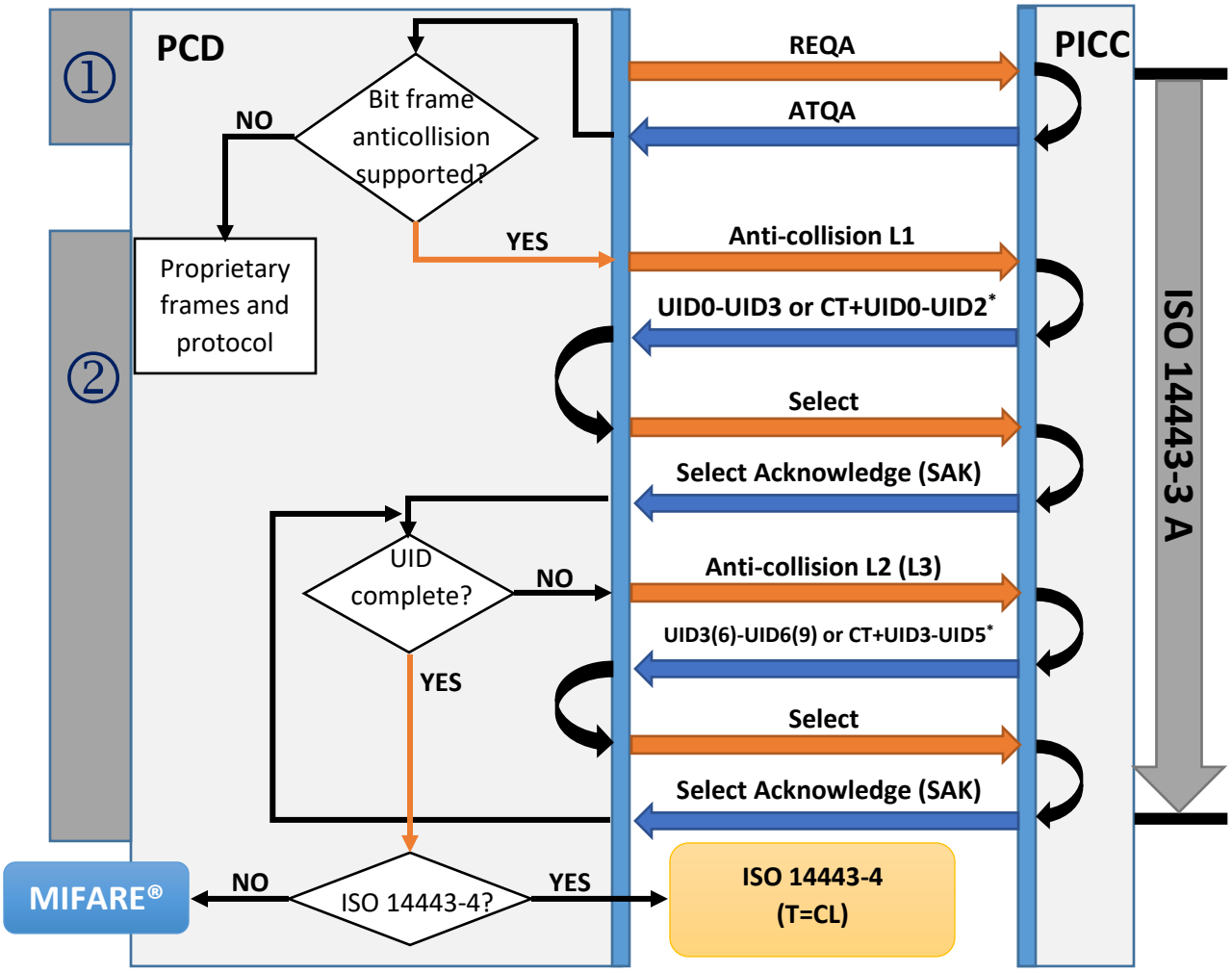
จากรูปภาพ เซกเตอร์ 0 บล็อก 0 ขนาด 16 ไบต์ จะไม่นำมาใช้งานเพราะว่าส่วนนี้จะใช้เก็บข้อมูลผู้ผลิตและหมายเลขบัตร (Card Serial Number: CSN) ซึ่งจะถูกกำหนดและบันทึกไว้ในบัตรตั้งแต่มาจากโรงงานผู้ผลิต อาจเรียกบล็อกนี้ว่า “Manufacturer Block” ส่วนบล็อก 1 และ 2 ของเซกเตอร์ 0 ก็เช่นเดียวกันโดยทั่วไปส่วนนี้จะสงวนไว้เป็นโครงสร้างข้อมูลที่เก็บค่าต่าง ๆ (MIFARE Application Directory: MAD) ไว้ใช้ร่วมกันในแต่ละเซกเตอร์เพื่อให้การจัดการแต่ละเซกเตอร์เป็นอย่างถูกต้องและปลอดภัย (สามารถนำมาใช้เก็บข้อมูลได้)

จากทั้งหมด 16 เซกเตอร์ บล็อกที่ 4 (บล็อกหมายเลข 3) ของแต่ละเซกเตอร์คือไซต์คีย์ (Site Key) มีขนาด 16 ไบต์ จะแบ่งออกเป็น 2 คีย์ คือ คีย์ A และ คีย์ B แต่ละคีย์ใช้หน่วยความจำขนาด 6 ไบต์ (ปกติจะเก็บค่าเป็นเลขฐานสิบหกจำนวน 6 คู่) คีย์ A จะใช้สำหรับต้องการข้อมูลในเซกเตอร์นั้น ส่วนคีย์ B จะใช้สำหรับต้องการเขียนข้อมูลลงบนเซกเตอร์นั้น ซึ่งคีย์ทั้งสองนี้จะคล้ายกับรหัสลับที่นำมาใช้สำหรับการป้องกันข้อมูลจากการอ่านหรือแก้ไขแบบไม่ได้รับอนุญาตและในแต่ละเซกเตอร์จะมีคีย์ A และ B แยกกัน บัตร MIFARE สามารถนำไปใช้เก็บข้อมูลที่เข้ารหัสแล้วจากหลายแอปพลิเคชันหรือหลายผู้พัฒนาได้ แต่ละแอปพลิเคชันที่มีการเก็บข้อมูลลงบนบัตรเดียวกันสามารถทำการป้องกันข้อมูลของตนเองจากแอปพลิเคชันอื่น ๆ ได้โดยการใช้คีย์ลับซึ่งเป็นคีย์ที่ไม่เปิดเผย ซึ่งในที่นี้จะหมายถึงคีย์ B ดังภาพที่ 3

byte 15							byte 8	byte 7							
s	e	c	R	e	t	C1	88	77	78	a5	a4	a3	a2	a1	a0
key B						GPB	access bit			key A					

ภาพที่ 3 โครงสร้างบล็อกไซต์คีย์

3.2 กระบวนการทำงานระหว่างอุปกรณ์อ่านและบัตร



* CT (Cascade Tag, Type A) คือตำแหน่งไบต์ที่เก็บค่าแสดงถึง UID ที่ได้รับแต่ incompletely ใช้เพื่อให้ทำงานใน anticollision ระดับที่สูงขึ้นเพื่อให้ได้ค่า UID ที่ completed ถ้า CT มีค่า 0x88 ใช้สำหรับ UID0 ให้ทำการตรวจจับการชนกัน

ภาพที่ 4 กระบวนการเริ่มทำงานระหว่างอุปกรณ์อ่านและบัตร RFID

จากภาพเป็นการแสดงกระบวนการทำงานระหว่างอุปกรณ์อ่านบัตรและบัตร RFID ซึ่งจะเกิดเมื่อบัตร RFID เข้ามาในบริเวณสนามแม่เหล็กไฟฟ้าของอุปกรณ์อ่านข้อมูล ซึ่งในที่นี้จะอธิบายโดยเน้นเฉพาะเมื่อมีบัตร RFID ชนิด MIFARE Classic 1k เข้ามาในบริเวณสนามแม่เหล็กดังนี้

① อุปกรณ์อ่านบัตร (Proximity Coupling Device: PCD) เริ่มต้นการสื่อสารด้วยการส่ง REQA (Request Command, Type A) เมื่อบัตร RFID (Proximity Integrated Circuit: PICC) จะทำการส่ง ATQA (Answer to Request, Type A) กลับ ซึ่งสัญญาณที่ส่งกลับจะร่วมข้อมูลดังนี้

- ข้อมูลที่บอกว่า PICC สนับสนุนบิตเฟรม anticollision หรือไม่สนับสนุน
- ข้อมูลที่เกี่ยวกับขนาดของ UID
- ข้อมูลรหัสสิทธิบางอย่าง (เพื่อสั่งให้ PCD ทำงานข้ามขั้นตอนบางอย่าง)

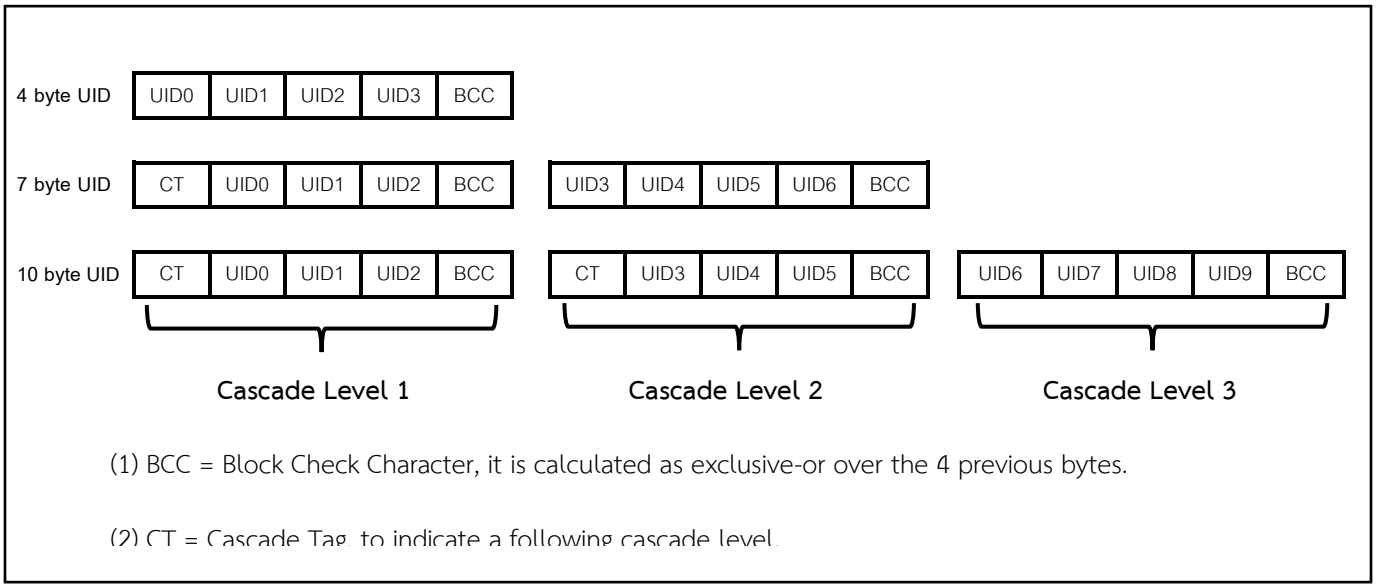
② ภายหลังที่เกิดกระบวนการ anticollision และ select ซึ่งขณะนี้ PCD เป็นผู้ควบคุมขั้นตอนโดยส่งคำสั่ง “ANTICOLLISON” ไป ซึ่ง PICC จะส่งค่ากลับโดยแบ่งออกได้ 3 กรณีดังนี้

- ในกรณีที่ 1 Cascade Level 1 (UID มีขนาด single UID (ใช้ 4 ไบต์)) ส่งค่ากลับดังนี้
  - ค่าทั้งหมด 4 ไบต์ที่เป็นค่า UID (UID0...UID3) และอีก 1 ไบต์เป็นค่า BCC หรือ
  - ค่า CT (Cascade Tag) ตามด้วยค่า 3 ไบต์แรกของ double UID (UID0...UID2) และอีก 1 ไบต์ BCC

โดยทั่วไปถ้าบัตร RFID เป็นชนิด MIFARE Classic 1k จะเกิดแค่ Cascade Level 1 ก็จะได้รับ UID ที่ complete และ PCD สามารถเริ่มต้นการสื่อสารตามโปรโตคอลที่ได้รับการสนับสนุน โดยข้าม Cascade Level 2 และ 3 แต่ถ้าเป็นบัตร RFID ที่ UID มีขนาด double UID หรือ triple UID จะต้องกระทำ anticollision และ selection ตามลำดับ

- ในกรณีที่ 2 Cascade Level 2 (UID มีขนาด double UID (ใช้ 7 ไบต์)) ส่งค่ากลับดังนี้
  - ค่าทั้ง 4 ไบต์หลังสุด ได้แก่ double UID (UID3...UID6) และอีก 1 ไบต์ BCC หรือ
  - ค่า CT (Cascade Tag) ตามด้วยค่า 3 ไบต์ถัดไปของ triple UID (UID3...UID5) และอีก 1 ไบต์ BCC
- ในกรณีที่ 3 Cascade Level 3 (UID มีขนาด triple UID (ใช้ 10 ไบต์)) ส่งค่ากลับดังนี้
  - ค่าทั้ง 4 ไบต์หลังสุดของ triple UID (UID6...UID9) และอีก 1 ไบต์ BCC

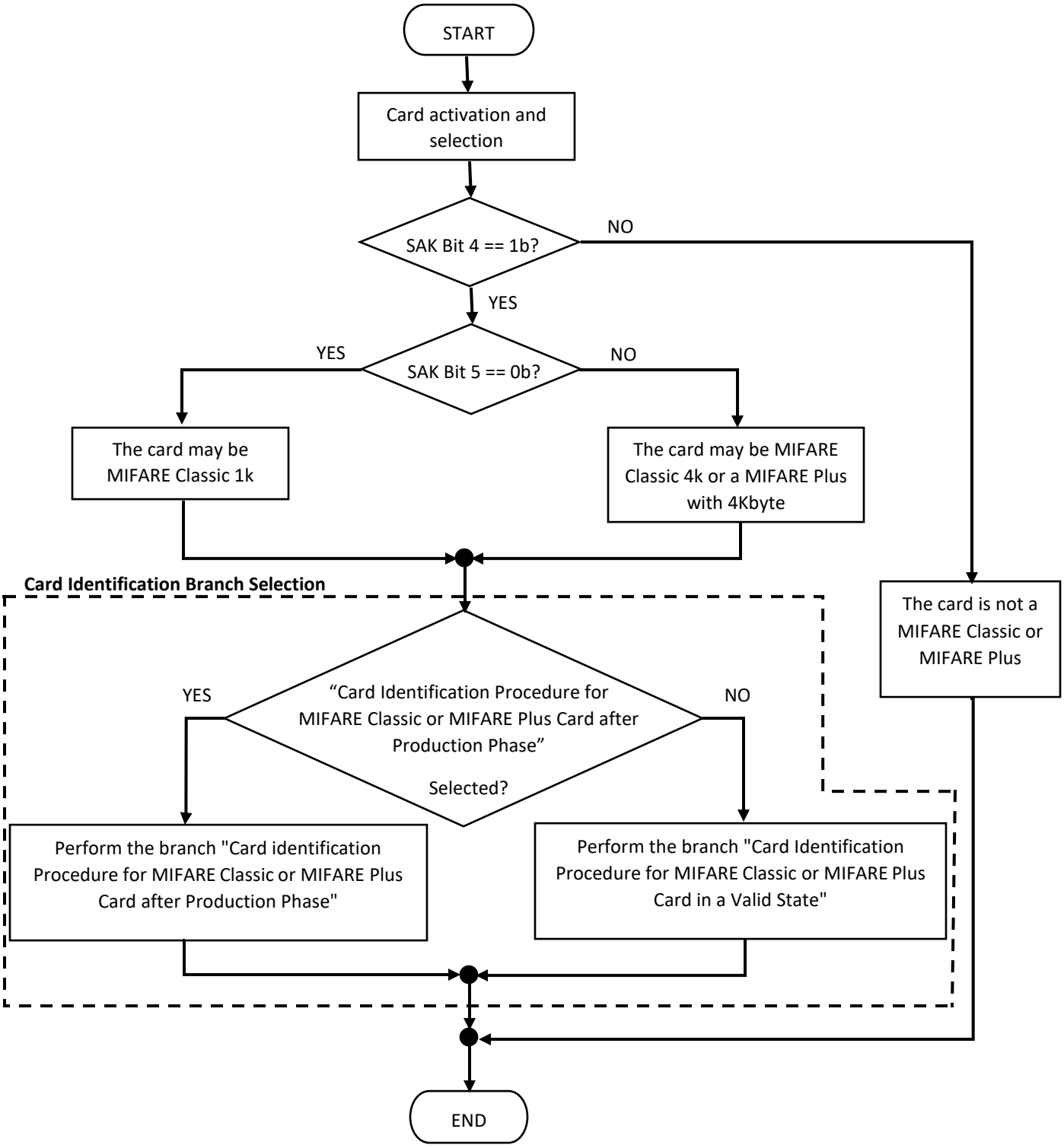
Cascade Level 3 PICC จะคืนค่า SAK ซึ่งแสดงถึงชนิดของบัตร รวมถึงการสนับสนุน T= CL



ภาพที่ 5 แสดง UID ตามมาตรฐาน ISO/IEC 14443

3.3 กระบวนการระบุชนิด MIFARE Classic 1k

หัวข้อนี้เป็นการอธิบายกระบวนการระบุตัวตนของบัตรซึ่งเป็นขั้นตอนการทำงานของอุปกรณ์อ่านบัตรเพื่อระบุชนิดของบัตรว่าเป็นชนิด MIFARE Classic (ตัวอย่างที่ใช้ทดลอง) หรือ MIFARE Plus



ภาพที่ 6 กระบวนการระบุชนิดของบัตร MIFARE Classic 1k

จากภาพที่ 6 กระบวนการระบุชนิดของบัตรจะเกิดขึ้นที่อุปกรณ์อ่านบัตรซึ่งสามารถเขียนอธิบายขั้นตอนดังกล่าวดังนี้

1. ตรวจสอบบิตที่ 4 ของ Selection Acknowledge (SAK, ดูเพิ่มเติม [ISOIEC 14443-3]) มีค่าเท่ากับ 1b และ
2. ตรวจสอบบิตที่ 5 ของ Selection Acknowledge (SAK, ดูเพิ่มเติม [ISOIEC 14443-3]) ซึ่งเป็นบิตแสดงถึงขนาดหน่วยความจำของบัตรชนิด MIFARE Classic หรือ MIFARE Plus
    - บิตที่ 5 มีค่าเท่ากับ 0b แสดงว่าเป็นบัตรชนิด MIFARE Classic 1k และ
    - บิตที่ 5 มีค่าเท่ากับ 1b แสดงว่าเป็นบัตรชนิด MIFARE Classic 4k หรือ MIFARE Plus with 4Kbyte

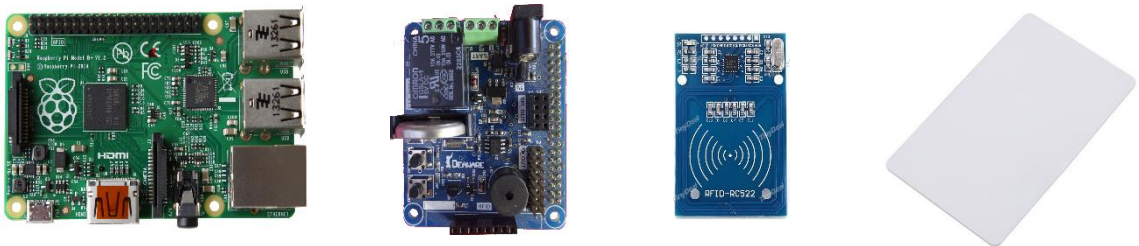
ถ้าหากกระบวนการระบุชนิดบัตรกระทำเสร็จสิ้นก่อนสองขั้นตอนดังกล่าวแสดงว่าไม่สามารถระบุได้ว่าบัตร RFID นี้เป็นชนิด MIFARE Classic หรือ MIFARE Plus ดังนั้นอุปกรณ์อ่านบัตรจะต้องส่งไปยังกระบวนการตรวจสอบเพิ่มเติมเพื่อพิสูจน์ว่าบัตรเป็นชนิด MIFARE Classic 1k หรือ 4k

ในส่วนของการดำเนินการขั้นตอน After Production Phase (บัตรว่างเปล่า) จะเกี่ยวข้องกับคีย์ A และคีย์ B ซึ่งขั้นตอนนี้จะทำการตรวจสอบหากพบว่าเป็น After Production Phase จริงอุปกรณ์อ่านบัตรจะดำเนินการฟอร์แมตบัตรเพื่อเตรียมโครงสร้างข้อมูลของให้บัตรให้สามารถใช้งานได้ ส่วนที่สองคือ Valid State ก่อนที่จะใช้งานโดยการเขียนหรืออ่านในแต่ละเซกเตอร์ ซึ่งจะต้องทำการรับรองโดยการอ้างถึงคีย์ A หรือคีย์ B ของเซกเตอร์นั้นๆ ว่าสามารถกระทำได้หรือไม่

4. การอ่าน/เขียน ข้อมูลบนบัตร MIFARE Classic 1k

สำหรับหัวข้อนี้ผู้เขียนบทความต้องการทดลองอ่านข้อมูลจากบัตรและเขียนข้อมูลลงบัตร เพื่อเป็นแนวทางในการนำไปประยุกต์ใช้งานต่อไป โดยการทดลองประกอบด้วยอุปกรณ์ทดลองดังนี้

1. บอร์ด Raspberry PI B+
2. บอร์ด Pulee เวอร์ชัน 1a
3. บอร์ด RFID-RC522
4. มีทรานสปอนเดอร์ (หรือ แท็ก) แบบบัตร ชนิด MIFARE Classic 1k



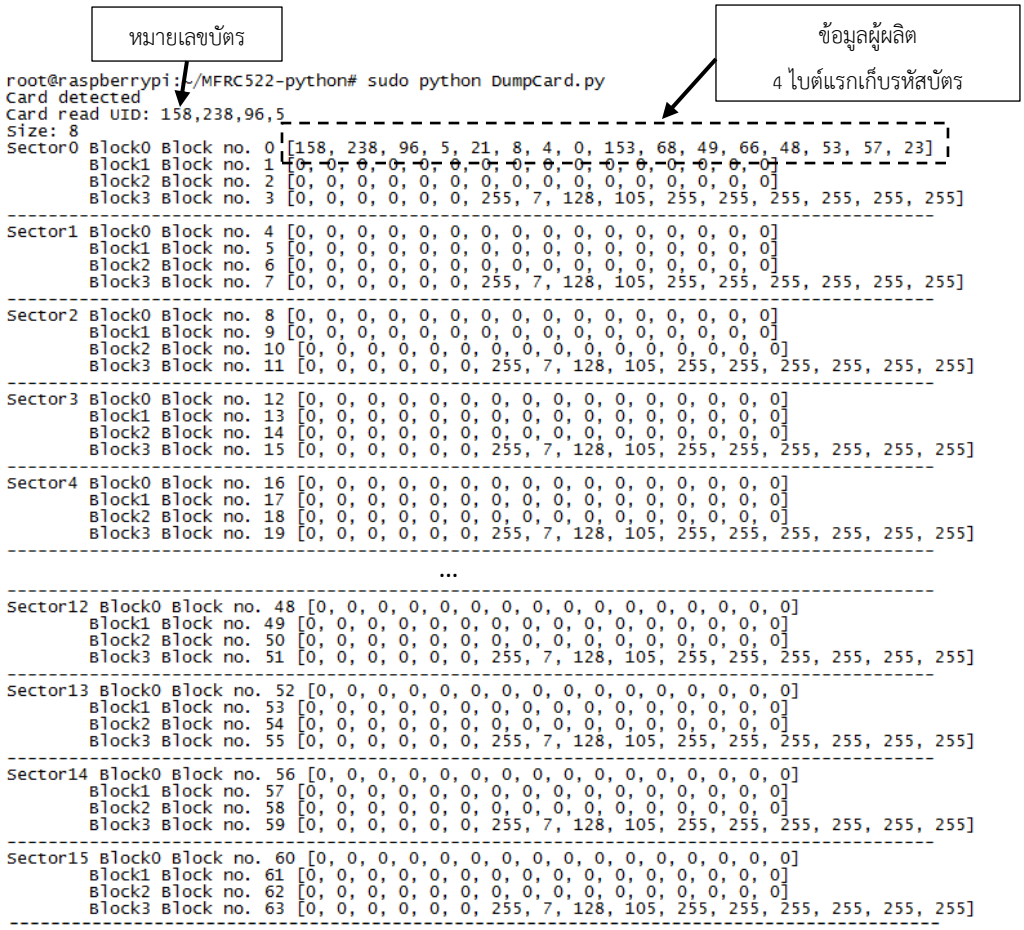
1) Raspberry 4) Pulee v.1a 2) RFID-RC522 3) MIFARE Classic 1k

ภาพที่ 7 อุปกรณ์ที่ใช้ในการทดลอง

การทดลองการอ่าน/เขียนบัตรโดยการเขียนโค้ดโปรแกรมภาษา python ซึ่งเป็นภาษาที่สามารถทำงานอยู่บนชุดทดลองได้อย่างมีประสิทธิภาพ โดยได้ผลลัพธ์ดังนี้

4.1 การอ่านข้อมูลจากบัตร

เป็นการอ่านข้อมูลทั้งหมดจากบัตรซึ่งบัตร RFID ที่ทดลองนั้นเป็นบัตรใหม่ยังไม่มีการใช้งาน มีโครงสร้างที่ประกอบด้วย 16 เซกเตอร์ เซกเตอร์ละ 4 บล็อก จำนวนบล็อกทั้งหมด 64 บล็อก แต่ละบล็อกมี 16 ไบต์ ดังนี้



ภาพที่ 8 โครงสร้างและข้อมูลที่ถูกอ่าน

บล็อกที่ 4 (Block3) ของแต่ละเซกเตอร์เรียกว่า “sector trailer” ประกอบด้วยข้อมูลที่ใช้สำหรับเงื่อนไขควบคุมการเข้าถึงข้อมูลของเซกเตอร์นั้น ๆ และกุญแจลับประกอบด้วยคีย์ A ถูกเก็บที่ 6 ไบต์แรก และคีย์ B เก็บที่ 6 ไบต์ท้ายสุดของบล็อก ซึ่งตอนนี้คีย์ B มีค่าเป็น 255 255 255 255 255 255 หรือ 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF โดยคีย์ทั้งคู่ใช้พิสูจน์ตัวตนเข้าใช้งานเซกเตอร์และจะต้องใช้ร่วมกับ Access bit ที่ถูกเก็บที่ไบต์ 6 – 8 (ไบต์แรกคือไบต์ที่ 0) ว่าการการเข้าถึงข้อมูลในเซกเตอร์นั้นสามารถทำงานอ่านได้อย่างเดียวหรือสามารถเขียนข้อมูลลงบัตรได้

ในส่วนของไบต์ที่ 9 ของบล็อกที่ 4 ในแต่ละเซกเตอร์เรียกว่า General Purpose Byte (GPB) และบล็อกอื่น ๆ ที่มีค่าเท่ากับ 0 (ศูนย์) หมายถึงบล็อกว่างเปล่าสามารถนำมาใช้งานได้

4.2 การเขียนข้อมูลลงบัตร

การทดลองจะทำการเขียนข้อมูลลงบัตรโดยเลือกเขียนข้อมูลที่เซกเตอร์ 1 (Block no. 4) โดยบล็อกที่ 0 (ศูนย์) จะใช้เก็บหมายเลขรหัสบัตรหรือรหัสแอปพลิเคชันเป็นรหัสที่ผู้ที่พัฒนาระบบกำหนดเองโดยจะต้องไม่ซ้ำกันและจะเก็บข้อมูลชื่อองค์กร ส่วนบล็อกที่ 1 เก็บรหัสนักศึกษา และทดลองเปลี่ยนคีย์ A เป็น 0x95 0x51 0xF8 0xF9 0x25 0x34 เปลี่ยนคีย์ B จาก 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF เป็น 0x29 0x27 0xD3 0x6C 0x42 0x30 ดังนี้

Block 0 = [0x32 0x35 0x35 0x38 0x30 0x30 0x30 0x21 0x02 0x49 0x54 0x42 0x52 0x55 0x03 0x23]

Block 1 = [0x35 0x37 0x30 0x31 0x31 0x32 0x34 0x31 0x37 0x30 0x34 0x32 0xFF 0xFF 0xFF 0xFF]

Block 3 = [0x95 0x51 0xF8 0xF9 0x25 0x34 0x78 0x77 0x88 0x00 0x29 0x27 0xD3 0x6C 0x42 0x30]

ข้อระวังการเปลี่ยนคีย์ควรเปลี่ยนคีย์เมื่อได้ทำการเขียนข้อมูลลงเซกเตอร์นั้นเรียบร้อยแล้วไม่มีการเปลี่ยนแปลงข้อมูลใดๆ และต้องทำความเข้าใจกับ Access bit ก่อนเพราะคีย์ (A,B) ทำงานร่วมกับ Access bit หากกำหนดค่า Access bit ผิดพลาดอาจทำให้เราไม่สามารถเข้าถึงข้อมูลหรือจัดการข้อมูลในเซกเตอร์นั้นได้อีกเลย หลังจากทำการเปลี่ยนคีย์ใหม่คือคีย์ A และ B ค่าคีย์ทั้งสองระบบจะถูกซ่อนไว้ไม่ให้เห็น ดังภาพที่ 9

```
root@raspberrypi:~/MFRC522-python# sudo python DumpCard.py
Card detected
Card read UID: 158,238,96,5
Size: 8
Sector0 Block0 Block no. 0 [158, 238, 96, 5, 21, 8, 4, 0, 153, 68, 49, 66, 48, 53, 57, 23]
        Block1 Block no. 1 [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
        Block2 Block no. 2 [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
        Block3 Block no. 3 [0, 0, 0, 0, 0, 0, 120, 119, 136, 0, 0, 0, 0, 0, 0, 0]
------------------------------------------------------------------------------
Sector1 Block0 Block no. 4 [50, 53, 53, 56, 48, 48, 48, 33, 2, 73, 84, 66, 82, 85, 3, 35]
        Block1 Block no. 5 [53, 55, 48, 49, 49, 50, 52, 49, 55, 48, 52, 50, 255, 255, 255, 255]
        Block2 Block no. 6 [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
        Block3 Block no. 7 [0, 0, 0, 0, 0, 0, 120, 119, 136, 0, 0, 0, 0, 0, 0, 0]
------------------------------------------------------------------------------
```

ภาพที่ 9 โครงสร้างและข้อมูลที่ถูกเขียน

สังเกตบล็อกที่ 4 (Block3) ของเซกเตอร์ที่ 1 คีย์ A และ คีย์ B จะถูกซ่อนถ้าไม่ทราบคีย์ก็จะไม่สามารถเข้าถึงหรือแก้ไขข้อมูลในเซกเตอร์นี้ได้ทำให้ข้อมูลมีความปลอดภัยจากผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล และจากตัวอย่างการทดลองเปลี่ยนแปลงคีย์ A และคีย์ B มีเงื่อนไขคือคีย์ A สามารถอ่านข้อมูลได้อย่างเดียว ส่วนคีย์ B สามารถอ่านและเขียนข้อมูลในเซกเตอร์นี้ได้

5. บทสรุป

บัตร RFID ชนิด MIFARE Classic 1k เป็นบัตรที่ใช้ระบบ RFID ซึ่งในปัจจุบันเป็นระบบที่นำมาใช้กันอย่างแพร่หลายเพื่อให้เกิดประสิทธิภาพสูงสุดในการทำงานรวมถึงมีความปลอดภัยในการรักษาข้อมูล บัตร RFID ชนิดนี้มีสามารถเก็บข้อมูลสูงสุดถึง 1024 ไบต์ แต่นำมาใช้งานจริงได้เพียง 752 ไบต์ เนื่องจากต้องใช้เก็บ เลขรหัสบัตร เลขรหัสผูผลิต สิทธิการใช้งาน สิทธิในการอ่าน/เขียนบัตร ซึ่งมีความปลอดภัยค่อนข้างสูง ทำให้เราสามารถใช้ในการกำหนดการรักษาความปลอดภัยของบัตรได้ นอกจากนั้นยังถูกผลิตให้มีรูปร่างที่หลากหลายรองรับลักษณะการใช้งานที่แตกต่างกันที่สำคัญคือต้นทุนที่ไม่แพงเหมาะสำหรับนักพัฒนา นักศึกษา ในการนำมาศึกษาและทดลองระบบที่เกี่ยวกับ RFID นอกจากนั้นบัตรชนิดนี้ยังสามารถนำไปประยุกต์ใช้กับระบบงานจริงได้

บทความฉบับนี้ได้ศึกษา ค้นคว้า รวบรวม เนื้อหาที่เกี่ยวข้องกับบัตร MIFARE Classic 1k และได้นำมาทดลองใช้งานทำให้ได้เข้าใจและเห็นปัญหาที่เกิดขึ้นจริง ซึ่งเนื้อหาอาจยังไม่ครอบคลุมรายละเอียดทั้งหมดในแต่ละหัวข้อแต่ก็เพียงพอในการนำมาเป็นแนวทางในการพัฒนาระบบงานจริงได้และผู้เขียนก็หวังว่าเอกสารฉบับนี้จะเป็นประโยชน์แก่ผู้ที่เริ่มต้นศึกษา นักพัฒนาระบบ ที่เกี่ยวกับระบบ RFID ได้เป็นอย่างดี

6. อ้างอิง

B. S. Prabhu, Xiaoyong Su, Harish Ramamurthy, Chi-Cheng Chu, Rajit Gadh UCLA. (2005). **WinRFID – A Middleware for the enablement of Radio Frequency Identification (RFID) based Applications**. เข้าถึงได้: http://wireless.ucla.edu/techreports2/UCLA-WinRFID.PDF, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

NXP Semiconductors. (2014). **MIFARE Type Identification Procedure.** [ออนไลน์]. เข้าถึงได้ : http://www.nxp.com/documents/application_note/AN10833.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

NXP Semiconductors. (2013). **MIFARE and handling of UIDs.** [ออนไลน์]. เข้าถึงได้ : http://www.nxp.com/documents/application_note/AN10927.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

NXP Semiconductors. (2013). **MIFARE Application Directory (MAD).** [ออนไลน์]. เข้าถึงได้ : http://www.nxp.com/documents/application_note/AN10787.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

NXP Semiconductors. (2012). **MIFARE Classic as NFC Type MIFARE Classic Tag.** [ออนไลน์]. เข้าถึงได้ : http://www.nxp.com/documents/application_note/AN1305.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

NXP Semiconductors. (2012). **NFC Type MIFARE Classic Tag Operation.** [ออนไลน์]. เข้าถึงได้ : http://www.nxp.com/documents/application_note/AN1304.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

NXP Semiconductors. (2011). **MIFARE Classic 1K - Mainstream contactless smart card IC for fast and easy solution development.** [ออนไลน์]. เข้าถึงได้ : http://www.nxp.com/documents/data_sheet/MF1S503x.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

Philips Semiconductor. (2004). **mifare Interface Platform Type Idenfification Procedure.** [ออนไลน์]. เข้าถึงได้ : http://dl.shibby.fr/Documents/Access%20Control/13.560MHz/MIFARE/m018413.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)

ScreenCheck BV. (n.d.). **Mifare Keyfile Manual.** [ออนไลน์]. เข้าถึงได้ : http://screencheck.com/wp-content/uploads/manuals/mifare-plugin/SCMifareKeyfile_Generator.pdf, (วันที่ค้นข้อมูล 1 มิถุนายน 2558)