

การปรับปรุงประสิทธิภาพของระบบเงินสดดิจิทัล Improved Efficiency on Electronic Cash Scheme

อมรรัตน์ พรประสิทธิ์

บัณฑิตภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี

มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต ปทุมธานี 12121

พันธุ์ปิติ เปี่ยมสง่า

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

บทคัดย่อ

ระบบเงินสดดิจิทัล (Electronic Cash Scheme) เป็นระบบการชำระเงินที่ให้ความสำคัญเป็นส่วนตัวแก่ผู้บริโภค โดยใช้วิทยาการการเข้ารหัสข้อมูลเป็นพื้นฐาน และมีการทำงานร่วมกับสมาร์ตการ์ดที่มีระบบความปลอดภัยทางกายภาพ แต่มาตรฐานความปลอดภัยของวิทยาการการเข้ารหัสที่ใช้ในปัจจุบันทำให้ระบบเงินสดดิจิทัลต้องใช้ข้อมูลมากขึ้นเป็นเท่าตัว อีกทั้งด้วยขีดจำกัดในเรื่องของหน่วยความจำและการประมวลผลของสมาร์ตการ์ด ส่งผลให้ระบบเงินสดดิจิทัลมีประสิทธิภาพลดลง จุดประสงค์ของงานวิจัยคือการปรับปรุงระบบเงินสดดิจิทัลเพื่อเพิ่มประสิทธิภาพในการทำงานโดยการลดขนาดข้อมูลในส่วนของเงินสดดิจิทัล โดยใช้วิธีการลงลายมือลับแบบใหม่ที่ใช้มาตรฐานความปลอดภัยในปัจจุบัน ระบบที่นำเสนอสามารถลดขนาดของเงินสดดิจิทัลที่ใช้ส่งผ่านเครือข่ายในขั้นตอนการชำระเงินคิดเป็นร้อยละ 32.73 โดยเทียบจากระบบเดิมที่นำมาปรับปรุง ช่วยลดข้อมูลที่จัดเก็บในสมาร์ตการ์ดคิดเป็นร้อยละ 29.19 และลดข้อมูลที่ใช้ในการส่งผ่านเครือข่ายในขั้นตอนการฝากเงินคิดเป็นร้อยละ 30 เพื่อให้ความมั่นใจแก่ผู้ใช้ว่าระบบเงินสดดิจิทัลเป็นระบบการชำระเงินที่มีความปลอดภัยที่ได้มาตรฐาน และมีประสิทธิภาพในการทำงานบนเครือข่ายอินเทอร์เน็ต

Abstract

Electronic cash scheme is an electronic payment scheme to provide the customer's privacy. The protocol is based on cryptography techniques and working with a smart card, which has a physical security unit. Unfortunately, with the security standard of cryptography, the scheme must increase size of data two times, and with the limitation of the memory and processing resources of smart card, the efficiency and effectiveness of the existing scheme are decreased. The objective of this paper was to improve the electronic cash scheme to reduce size of data in order to increase the efficiency and effectiveness of the system. Using a new blind signature protocol, it reduced the size of cash which was transmitted in payment protocol by 32.73 percent as compared with the previous scheme and also reduced the size of data stored in the smart card by 29.19 percent. Furthermore, it reduced the data transmission in deposit protocol by 30 percent. The results can be noticed to the customer's confidentiality that the electronic cash is a secure and an efficient payment system to be used on the Internet.

1. คำนำ

เทคโนโลยีการชำระเงินผ่านระบบอิเล็กทรอนิกส์เป็นส่วนประกอบที่สำคัญในระบบพาณิชย์อิเล็กทรอนิกส์ แต่เมื่อพาณิชย์อิเล็กทรอนิกส์ขยายไปสู่เครือข่ายอินเทอร์เน็ตส่งผลให้เกิดความไม่ปลอดภัยของข้อมูลเพิ่มขึ้น รวมไปถึงการละเมิดสิทธิส่วนบุคคลของผู้บริโภค เนื่องจากมีกลไกที่สามารถค้นหาข้อมูลพฤติกรรมการซื้อของผู้บริโภค จึงมีความเป็นไปได้ที่บุคคลบางกลุ่ม ผู้ซึ่งสนใจในการค้นหาข้อมูลส่วนตัวเหล่านี้สามารถทราบถึงการไหลเวียนของเงินในระบบ และรายละเอียดของการชำระเงินเพื่อใช้เป็นประโยชน์ต่อไป แต่กิจกรรมการอุปโภคบริโภคนั้นเป็นข้อมูลส่วนบุคคล และเป็นสิทธิที่ผู้บริโภคควรได้รับการคุ้มครอง

ในปัจจุบัน มีชำระเงินแบบหนึ่งที่สามารถให้ความปลอดภัยกับลูกค้าจากปัญหาดังกล่าวได้ คือระบบเงินสด เนื่องจากลูกค้าสามารถใช้เงินสดกับร้านค้าโดยไม่ต้องมีการแสดงตัวว่าตนเป็นใคร ดังนั้นจึงมีนักวิจัยออกแบบระบบการชำระเงินที่มีคุณลักษณะเดียวกับระบบเงินสดมีชื่อเรียกว่า “ระบบเงินสดดิจิทัล”

ระบบเงินสดดิจิทัลสามารถแบ่งได้เป็น 2 ประเภทคือ ระบบออนไลน์ [1] และระบบออฟไลน์ [2, 3, 4, 5, 6] ระบบออนไลน์นั้นในขั้นตอนการชำระเงินระหว่างลูกค้ากับร้านค้า ต้องมีธนาคารทำหน้าที่อนุมัติรายการการชำระเงิน ระบบออนไลน์ต้องมีการติดต่อกับฐานข้อมูลที่ทันสมัยอยู่ตลอดเวลาเพื่อตรวจสอบเงินอิเล็กทรอนิกส์ว่าถูกใช้ไปแล้วหรือไม่ จึงอาจก่อให้เกิดปัญหาในเรื่องของเวลาที่ใช้ในการตรวจสอบ อีกทั้งหากระบบของธนาคารเกิดขัดข้องจะไม่สามารถทำการต่อไปได้ ในส่วนของระบบออฟไลน์นั้นในขั้นตอนการชำระเงินไม่ต้องมีธนาคารอนุมัติรายการการชำระเงิน ร้านค้าเป็นผู้ตรวจสอบเหรียญด้วยตนเอง แต่ระบบนี้อาจเกิดกรณีลูกค้าใช้เงินซ้ำ (Double Spending) ขึ้น ร้านค้าไม่สามารถตรวจสอบการใช้เงินซ้ำได้เอง จะทราบก็ต่อเมื่อนำเงินไปฝากกับธนาคาร

ระบบเงินสดดิจิทัลอาศัยวิทยาการการเข้ารหัสข้อมูลแบบ Public Key Cryptography [7, 8, 9, 10 11, 12] ในการทำงาน โดยใช้การลงลายมือชื่อดิจิทัล (Digital Signature) บนเหรียญดิจิทัล (Digital Coin) วิธีลงลายมือชื่อดิจิทัลช่วยให้ร้านค้า และธนาคารสามารถตรวจสอบเงินว่าเป็นเงินที่ถอนออกมาอย่างถูกต้องหรือไม่ มีการใช้โปรโตคอลลงลายมือชื่อดิจิทัลลับหรือที่เรียกว่า “Blind Signature” [13] บนเหรียญดิจิทัล

ซ่อนข้อมูลมิให้ธนาคารมองเห็นลักษณะข้อมูลของเหรียญดิจิทัลที่แท้จริง เพื่อสร้างความเป็นส่วนตัวให้กับลูกค้า นอกจากนี้ระบบเงินสดดิจิทัลมีการใช้อุปกรณ์อิเล็กทรอนิกส์ที่มีคุณสมบัติ Tamper-Resistant เช่น สมาร์ทการ์ดที่สามารถป้องกันการดึงข้อมูลอย่างไม่ต้องต้องการเพื่อป้องกันการใช้เงินซ้ำ [3] ลูกค้าจะไม่สามารถดึงข้อมูลในบัตรได้ หากไม่ได้รับความยินยอมจากบัตร

อย่างไรก็ตาม ด้วยเหตุที่ใช้ Public Key Cryptography ออกแบบ ระบบเงินสดดิจิทัลในปัจจุบันต้องการความปลอดภัยในการทำงานเพิ่มขึ้น ตามมาตรฐานในปัจจุบันความยาวของกุญแจส่วนบุคคล (Private Key) และกุญแจสาธารณะ (Public Key) ต้องไม่น้อยกว่า 160 และ 1024 บิตตามลำดับ [7] โดยที่ความยาวของกุญแจสาธารณะต้องเพิ่มจากเดิม 512 บิต เป็น 1024 บิต จะเห็นว่าความยาวนั้นเพิ่มขึ้นเป็นเท่าตัว แต่เนื่องจากอุปกรณ์สมาร์ตการ์ดมีหน่วยความจำไม่มากนักอีกทั้งมีข้อจำกัดในด้านการประมวลผล หากใช้โปรโตคอลที่มีอยู่จะทำให้ประสิทธิภาพของระบบลดลง ดังนั้นจึงควรมีการพัฒนาปรับปรุงระบบเงินสดดิจิทัล ที่มีระบบความปลอดภัยที่ได้มาตรฐาน และมีประสิทธิภาพเหมาะกับการทำงานร่วมกับสมาร์ตการ์ด

ระบบเงินสดดิจิทัลที่น่าสนใจในงานวิจัยนี้เป็นการปรับปรุงระบบเงินสดดิจิทัลจากงานวิจัยของ Brands [3] ที่มีชื่อว่า “Untraceable Off-line Cash in Wallets with Observers” ซึ่งเป็นระบบเงินสดดิจิทัลประเภทออฟไลน์ที่เป็นที่ยอมรับว่ามีประสิทธิภาพในการทำงาน และมีความปลอดภัย โดยนำผลงานวิจัยที่มีชื่อว่า “Blind Signature Based on Discrete Logarithm Problem” [14] นำมาประยุกต์แทน Blind Signature ของเดิม เพื่อลดขนาดข้อมูลในส่วนของเงินดิจิทัล รวมถึงมีความปลอดภัยตามมาตรฐานของ Public Key Cryptography ในปัจจุบัน เพื่อให้ความมั่นใจแก่ผู้ใช้ว่าระบบเงินสดดิจิทัล เป็นระบบการชำระเงินที่มีความปลอดภัยและมีประสิทธิภาพในการทำงานบนเครือข่ายอินเทอร์เน็ต

2. ผลงานวิจัยที่เกี่ยวข้อง

ระบบเงินสดดิจิทัลที่ให้ความเป็นส่วนตัวแก่ลูกค้านี้ เริ่มต้นจากงานวิจัยของ “Chaum” [13] ที่คิดค้นเทคนิคการลงลาย

มือชื่อลับบน RSA [15] ซึ่งเป็นเทคนิคที่สำคัญต่อระบบการชำระเงินที่มีคุณสมบัติให้ความเป็นส่วนตัวในด้านข้อมูลแก่ลูกค้า จึงถือได้ว่างานวิจัยการลงลายมือชื่อลับนี้เป็นจุดเริ่มต้นของระบบการชำระเงินที่ให้ความเป็นส่วนตัวในด้านข้อมูล

จากนั้นงานวิจัยพัฒนาเทคนิคการลงลายมือชื่อลับของ Chaum และ Pedersen [6] ได้นำโปรโตคอลของ Schnorr [1 b6] มาดัดแปลงเป็นการลงลายมือชื่อลับซึ่งเหมาะสมสำหรับการใช้ร่วมกับบัตรเครดิต ต่อมางานวิจัยของ Cemenisch และคณะ [14] ได้นำเสนอการลงลายมือชื่อลับโดยนำลายมือชื่อดิจิตอลมาตรฐานที่เรียกว่า DSA (Digital Signature Algorithm) [17] มาดัดแปลงให้เป็นการลงลายมือชื่อลับ โดยสร้างลายมือชื่อลับขนาด 320 บิต ซึ่งสั้นกว่าการลงลายมือชื่อลับของ Chaum และ Pederson เมื่อนำมาเปรียบเทียบกัน ดังนั้นงานของ Cemenisch และคณะจึงเหมาะสมที่จะนำไปใช้กับบัตรเครดิตมากกว่า

ผู้เสนอโปรโตคอลเงินสดดิจิตอลเป็นครั้งแรกคือ Chaum, Fiat และ Noar [4] โดยนำเอาเทคนิคการลงลายมือชื่อลับมาพัฒนา ความปลอดภัยของระบบนี้อยู่บนสมมติฐานที่ตั้งขึ้นอย่างกว้าง ๆ ที่ยังไม่มีการพิสูจน์อย่างเป็นทางการ ระบบนี้เป็นพื้นฐานสำคัญสำหรับระบบเงินสดดิจิตอลหลาย ๆ ระบบต่อมา

มีการเสนอระบบเงินสดดิจิตอลออกมาอย่างต่อเนื่อง งานของ Ferguson [18] พัฒนาเทคนิคจากงาน [4] แต่ระบบที่ได้มีการทำงานที่ซับซ้อนมาก งานของ Brands [3] นำงานของ [4, 6] มาพัฒนาทำให้ได้ระบบเงินสดดิจิตอลอย่างสมบูรณ์ มีโครงสร้างเรียบง่ายและมีประสิทธิภาพมากกว่างานวิจัยอื่น ๆ อาศัยเทคนิคของ Schnorr Signature Protocol [16] และ Representation Problem [2] ทำให้ธนาคารไม่สามารถติดตามการใช้ข้อมูลของลูกค้าได้ไม่ว่ากรณีใด ๆ โปรโตคอลของ Brands เป็นโปรโตคอลแรกที่สามารถป้องกันการใช้เหรียญซ้ำได้ โดยออกแบบให้ทำงานร่วมกับสมาร์ตการ์ดงานวิจัยนี้ของ Brands เป็นโปรโตคอลของระบบเงินสดดิจิตอลที่งานวิจัยฉบับนี้นำมาเป็นปรับปรุงเพื่อสร้างระบบเงินสดดิจิตอลระบบใหม่ที่มีประสิทธิภาพมากขึ้น

3. การปรับปรุงโปรโตคอลเงินสดดิจิตอล

โปรโตคอลของงานวิจัยนี้นำเอางาน [3] มาปรับปรุงโดยผู้เกี่ยวข้องในระบบเงินสดดิจิตอลประกอบด้วย ธนาคาร แสดงแทนด้วย B ลูกค้า แสดงแทนด้วย U และร้านค้า แสดงแทนด้วย S การคำนวณทุกขั้นตอนต้องมีการทำ Modulo ทุกครั้งตามวิธีการของ Public Key Cryptography

3.1 ขั้นตอนการติดตั้งระบบ ธนาคาร B กำหนดค่าตัวแปรที่ใช้ในระบบเงินสดดิจิตอล ตามมาตรฐานของระบบ DSA [25] ดังนี้ p คือเลขจำนวนเฉพาะ ขนาด 1,024 บิต q คือเลขจำนวนเฉพาะที่สามารถหาร $(p-1)$ ลงตัว ขนาด 160 บิต g, g_1, g_2 คือ Generator ที่มี Order $q \pmod{p}$ B สุ่มเลือก $x \in_R Z_q$ คือกุญแจส่วนตัวของ B และคำนวณ $y = g^x \pmod{p}$ คือกุญแจสาธารณะของ B H_1, H_0 คือ แฮชฟังก์ชันตามมาตรฐาน SHA-1 [17] โดยกำหนดความสัมพันธ์ตามสมการ (1) และ (2) ตามลำดับ

$$H_1: G_q \times G_q \times G_q \times G_q \times G_q \rightarrow Z_q \quad (1)$$

$$H_0: G_q \times G_q \times G_q \times \text{Date/Time} \rightarrow Z_q \quad (2)$$

B ประกาศค่าตัวแปร $p, q, g, g_1, g_2, y, H_1$ และ H_0 ให้ U และ S ทราบ ส่วนตัวแปร x นั้น B จะเก็บไว้เป็นความลับ นอกจากนี้ B จะสร้างฐานข้อมูลผู้ถือบัญชีเพื่อเก็บข้อมูลลูกค้า อาทิ ชื่อ ที่อยู่ เบอร์โทรศัพท์ติดต่อ และฐานข้อมูลที่เก็บข้อมูลอิเล็กทรอนิกส์ของเหรียญที่ใช้แล้ว

3.2 ขั้นตอนการเปิดบัญชี เมื่อ U ต้องการเปิดบัญชีกับ B นั้น U ต้องแสดงตัวกับ B ว่า U เป็นผู้ร้องขอเปิดบัญชีจริงและมีตัวตนจริง เมื่อ B ตรวจสอบหลักฐานว่าถูกต้อง B จะเปิดบัญชีให้แก่ U ดังนี้

1. U เลือกตัวแปร $u \in_R Z_q$ ซึ่งเป็นกุญแจส่วนตัวของ U ที่ U เก็บไว้เป็นความลับ จากนั้น U คำนวณค่า $I = g, u \pmod{p}$ ซึ่งเป็น กุญแจสาธารณะของ U จากนั้นส่งค่า I_u ให้ B

2. B คำนวณค่า $z' = (Ig_2)^x \pmod{p}$ แล้วส่งให้ U ส่วน I ร่วมกับข้อมูลอื่น ๆ ของ U ไว้ในฐานข้อมูลลูกค้า

3.3 ขั้นตอนการถอนเงิน เมื่อ U ต้องการถอนเงินจาก B นั้น U ต้องพิสูจน์ตัวตนต่อ B ว่าเป็นเจ้าของบัญชีจริง จากนั้นการถอนเงินจึงเกิดขึ้นดังนี้

1. B เลือกตัวเลข $k \in_R Z_q$ จำนวน $a' = g^k \pmod{p}$ และตรวจสอบ $\gcd(a', q) = 1$ ถ้าเป็นเท็จ ต้องย้อนกลับไปเลือกค่า k ใหม่ ถ้าเป็นจริง B จำนวน $b' = (Ig_2)^k \pmod{p}$ และส่งค่า a', b' ให้ U

2. เมื่อ U ได้รับ a' และ b' แล้วตรวจสอบ $\gcd(a', q) = 1$ ถ้าเป็นเท็จ U จะปฏิเสธการถอนเงิน และให้ B ย้อนกลับไปทำขั้นตอน 1 ใหม่ ถ้าสมการเป็นจริง U เลือกตัวเลข $v, \alpha, \beta \in_R Z_q$ แล้วคำนวณสมการ (3) ถึง (6) จากนั้น สุ่มเลือก $x_1, x_2 \in_R Z_q$ แล้วคำนวณ $B = g_1^{x_1} g_2^{x_2} \pmod{p}$ จากนั้นคำนวณ challenge m ตามสมการ (7) แล้ว Blind ด้วยสมการ (8) เพื่อซ่อนข้อมูลจาก B จากนั้นจึง m' ส่งให้ B

$$A = (Ig_2)^v \pmod{p} \quad (3)$$

$$z = z'^v \pmod{p} \quad (4)$$

$$a = a'^\alpha g^\beta \pmod{p} \pmod{q} \quad (5)$$

$$b = a'^\alpha A^\beta \pmod{p} \pmod{q} \quad (6)$$

$$m = H_1(A, B, a, b, z) \quad (7)$$

$$m' = \alpha m a'^{-1} \quad (8)$$

3. B จำนวน $s' = km' + a'x \pmod{q}$ แล้วส่งให้

U

4. U ตรวจสอบสมการ (9) และ (10) ถ้าเป็นเท็จ แสดงว่าลายมือชื่อของ B ไม่ถูกต้อง U ยกเลิกการถอนเงิน แต่ถ้าสมการเป็นจริง U คำนวณตาม $s = s'aa'^{-1} + \beta m \pmod{q}$

$$a' = (g'^y)^{m'} \pmod{p} \quad (9)$$

$$b' = ((Ig_2)^z z'^{-a'})^{m'} \pmod{p} \pmod{q} \quad (10)$$

U จัดเก็บข้อมูล $(A, B, (a, b, z, s))$ ซึ่งเป็น Representation ของเหรียญดิจิทัลไว้ในบิตร็อกเกอร์หรือนิกส์ รวมทั้งเก็บข้อมูล v, x_1, x_2 ไว้เป็นความลับเพื่อพิสูจน์ความเป็นเจ้าของเหรียญในขั้นตอนการชำระเงิน

3.4 ขั้นตอนการชำระเงิน เมื่อ U ต้องการใช้เหรียญที่ร้านค้า S ขั้นตอนการชำระเงินจึงเกิดขึ้นดังนี้

1. U ส่ง $(A, B, (a, b, z, s))$ ให้ S

2. S จำนวน $m_p = H_0(A, B, I_s, \text{Date/Time})$

เป็น Challenge ส่งให้กับ U โดย I_s คือ Shop-ID ที่ระบุได้ว่า

ร้านค้านั้นเป็นร้านใด และ Date/Time คือวัน และเวลาของการชำระเงิน

3. U จำนวน $r = A \pmod{q}$, $s_1 = vm_p + rx_1 \pmod{q}$ และ $s_2 = vm_p + rx_2 \pmod{q}$ โดยนำค่า v, x_1, x_2 มาคำนวณเพื่อแสดงความเป็นเจ้าของเหรียญดิจิทัลนั้น แล้วจึงส่ง s_1 และ s_2 ให้ S

4. S ตรวจสอบลายมือชื่อของ B บนเหรียญว่าถูกต้องหรือไม่จากสมการ (11) และ (12) หากสมการเป็นจริงแสดงว่าเป็นเหรียญนั้นถูกเบิกออกมาจากธนาคาร B จึงทำการตรวจสอบความเป็นเจ้าของเหรียญต่อไปโดยดำเนินการคำนวณตามสมการ (13) ถ้าสมการเป็นเท็จ แสดงว่า U ไม่ใช่เจ้าของเหรียญนั้น S จะยกเลิกการชำระเงิน ถ้าสมการเป็นจริง n S จึงมอบสินค้าให้ U และ เก็บข้อมูลของเหรียญ รวมทั้งวัน และเวลาของการชำระเงินไว้เพื่อนำไปฝากเงินกับธนาคารต่อไป

$$a = (g'^y)^{m'} \pmod{p} \pmod{q} \quad (11)$$

$$b = (A' z'^{-a})^{m'} \pmod{p} \pmod{q} \quad (12)$$

$$r = (g_1^{s_1} g_2^{s_2} B^{-r})^{m_p^{-1}} \pmod{p} \pmod{q} \quad (13)$$

3.5 ขั้นตอนการฝากเงิน หลังจากที่ S เก็บเหรียญดิจิทัลไว้ เมื่อครบกำหนดจึงนำไปฝากเงินกับ B มีขั้นตอนดังต่อไปนี้

1. S ส่งข้อมูลเกี่ยวกับการขายซึ่งประกอบด้วย $A, B, (a, b, z, s), (s_1, s_2), \text{Date/Time}$ ให้ B

2. B ตรวจสอบลายมือชื่อบนเหรียญตามสมการ (10) และ (11) ถ้าเป็นเท็จแสดงว่าเหรียญดังกล่าวทาง B ไม่ได้เป็นผู้ออกให้ B จะทำการยกเลิกการฝากเงิน ของ S แต่ถ้าสมการเป็นจริง B ตรวจสอบเหรียญว่าเป็นเหรียญที่มีมูลค่าหรือไม่ นั่นคือนำ A ไปตรวจสอบในฐานข้อมูลเหรียญที่ใช้แล้ว จะเกิดกรณีใดกรณีหนึ่งดังต่อไปนี้

- A ไม่อยู่ในฐานข้อมูลเหรียญที่ใช้แล้ว กรณีนี้แสดงว่าเหรียญมีมูลค่ายังมีเคอยู่ใช้มาก่อน สามารถนำมาฝากเงินได้ B จะทำการเก็บข้อมูลที่เกี่ยวข้องด้วย $(A, B, a, b, z, s, \text{Date/Time}, s_1, s_2)$ โดย S เป็นผู้นำฝาก และ B เพิ่มจำนวนเงินในบัญชีตามมูลค่าของเหรียญ

- หากค้นพบ A อยู่ในฐานข้อมูลเหรียญที่ใช้แล้ว กรณีนี้แสดงว่าเกิดการฉ้อโกงขึ้น ถ้าข้อมูลในฐานข้อมูลระบุว่า S

เป็นผู้นำฝาก และ Date/Time ในฐานข้อมูลมีค่าเดียวกันกับเหรียญใหม่ แสดงว่า S พยายามนำเหรียญเดิมมาฝากเงินซ้ำ แต่ถ้าข้อมูลในฐานข้อมูลไม่ได้รับว่า S เป็นผู้นำฝาก ค่า Challenge (s_1 และ s_2) ของเหรียญกับ Challenge ในฐานข้อมูลย่อมต่างกัน แสดงว่าลูกค้าใช้เหรียญซ้ำ B จึงนำข้อมูล (s_1 , s_2) ที่อยู่ในฐานข้อมูล กับข้อมูล (s_1 , s_2) ของเหรียญมาคำนวณหากุญแจส่วนบุคคลของผู้ใช้เหรียญซ้ำตามสมการ (13) จากนั้นเมื่อนำมาคำนวณตามสมการ (14) B จะรู้ว่าใครเป็นผู้ใช้เหรียญซ้ำเนื่องจาก B รู้ค่า I ซึ่งเป็นข้อมูลแทนหมายเลขบัญชีของ U

$$\frac{(s_1 - s_1')}{(s_2 - s_2')} = u \pmod{q} \quad (14)$$

$$g_1^{(s_1 - s_1')/(s_2 - s_2')} = I \pmod{p} \quad (15)$$

4. การป้องกันการใช้เหรียญซ้ำในโพรโตคอล

ในหัวข้อนี้ได้อธิบายถึงวิธีการเพิ่มประสิทธิภาพในการป้องกันปัญหาการใช้เหรียญซ้ำของลูกค้าในระบบเงินสดดิจิทัลแบบใหม่ โดยออกแบบให้ทำงานร่วมกับอุปกรณ์ Observer ที่เก็บข้อมูลลับของเหรียญร่วมกับลูกค้า ซึ่งมีคุณสมบัติ Tamper-Resistance อาทิ สมาร์ตการ์ด ช่วยป้องกันการกล่อบดข้อมูลอย่างไม่ต้อง นอกจากนั้นหากแม้ผู้ที่สามารถดึงข้อมูลจากอุปกรณ์ Observer ได้ และนำเหรียญไปใช้ซ้ำ โพรโตคอลนี้ยังสามารถระบุผู้กระทำผิดได้เช่นเดียวกัน

4.1 ขั้นตอนการเปิดบัญชีร่วมกับ Observer

1. U เลือกตัวแปร $u \in_R Z_q$ ซึ่งเป็นกุญแจส่วนบุคคลของ U จากนั้น U คำนวณค่า $I_u = g_1^u \pmod{p}$ ซึ่งเป็นกุญแจสาธารณะของ U จากนั้นส่งค่า I_u ให้ B

2. B สร้าง O โดยเลือกตัวแปร $o_1 \in_R Z_q$ โดยค่า o_1 มีเพียง B และ O เท่านั้นที่รู้ จากนั้น B คำนวณค่า I_o ตามสมการ (3.29) เป็น กุญแจสาธารณะของ O ที่มีขนาด 1,024 บิต จากนั้นคำนวณค่า $I_o = g_1^{o_1} \pmod{p}$ และคำนวณค่า z' ตามสมการ (3.5) แล้วจึงส่งค่า I_o และ z' ให้ U ส่วน B เก็บ o_1 และ I ร่วมกับข้อมูลอื่น ๆ ของ U ไว้ในฐานข้อมูลลูกค้า

4.2 ขั้นตอนการถอนเงินร่วมกับ Observer

1. B เลือกตัวเลข $k \in_R Z_q$ คำนวณ $a' = g^k \pmod{p}$ และตรวจสอบ $\gcd(a', q) = 1$ ถ้าเป็นเท็จ ต้องย้อน

กลับไปเลือกค่า k ใหม่ ถ้าเป็นจริง B คำนวณ $b' = (Ig_2)^k \pmod{p}$ และส่งค่า a', b' ให้ U

2. O สุ่มเลือกตัวเลข $o_2 \in_R Z_q$ แล้วคำนวณ $B_o = g_1^{o_2} \pmod{p}$ เพื่อเป็นข้อมูลลับของเหรียญดิจิทัลพร้อมกับข้อมูลลับของ U

3. เมื่อ U ได้รับ a' และ b' แล้วตรวจสอบสมการ $\gcd(a', q) = 1$ ถ้าเป็นเท็จ U จะปฏิเสธการถอนเงิน และให้ B ย้อนกลับไปทำขั้นตอน 1 ใหม่ ถ้าสมการเป็นจริง U เลือกตัวเลข $v, \alpha, \beta \in_R Z_q$ แล้วคำนวณสมการ (3) ถึง (6) จากนั้น สุ่มเลือก $x_1, x_2 \in_R Z_q$ แล้วคำนวณ $B = g_1^{x_1} g_2^{x_2} I_o^{v\alpha} B_o \pmod{p}$ จากนั้นคำนวณ challenge m ตามสมการ (7) แล้ว Blind ด้วยสมการ (8) แล้วจึง m' ส่งให้ B

4. B คำนวณ $s' = km' + a'x \pmod{q}$ ส่งให้ U

5. B ตรวจสอบสมการ (9) และ (10) ถ้าเป็นเท็จ แสดงว่าลายมือชื่อของ B ไม่ถูกต้อง U ยกเลิกการถอนเงิน แต่ถ้าสมการเป็นจริง U คำนวณ $s = sa'a'^{-1} + \beta m \pmod{q}$

4.3 ขั้นตอนการชำระเงินร่วมกับ Observer

1. U ส่ง $(A, B, (a, b, z, s))$ ให้ S

2. S คำนวณ $m_p = H_0(A, B, I_s, \text{Date/Time})$ เป็น Challenge ส่งให้กับ U

3. U คำนวณ $r = A \pmod{q}$ และนำค่า r มาคำนวณค่า Challenge m'_p โดยนำข้อมูลลับ v, ε ในขั้นตอนการถอนเหรียญมาคำนวณ $m'_p = v(m_p + r\varepsilon) \pmod{q}$ แล้วส่ง m'_p, r ให้ O ทำการคำนวณค่า Response

4. O ตรวจสอบว่ามี o_2 อยู่ในหน่วยความจำหรือไม่ ถ้าไม่มีแสดงว่า U พยายามใช้เหรียญซ้ำ O จึงปฏิเสธการส่งข้อมูลให้ U แต่ถ้าพบค่า o_2 O จะคำนวณสมการ $s_o = m'_p o_1 + r o_2 \pmod{q}$ แล้วส่ง s_o ให้ U

5. S ตรวจสอบลายมือชื่อของ B บนเหรียญว่าถูกต้องหรือไม่ จากสมการ (11) และ (12) หากสมการเป็นจริง S จึงทำการตรวจสอบความเป็นเจ้าของเหรียญต่อไปโดยตรวจสอบสมการ (13) ถ้าสมการเป็นเท็จ S จะยกเลิกการชำระเงิน ถ้าสมการเป็นจริง S จึงมอบสินค้าให้ U และ เก็บข้อมูลของเหรียญ รวมทั้งวัน และเวลาของการชำระเงินไว้เพื่อนำไปฝาก

เงินกับธนาคารต่อไป

ในขั้นตอนการฝากเงิน กระทำเช่นเดียวกับโปรโตคอลพื้นฐาน หากมีลูกค้าทำการใช้เหรียญแล้วธนาคารสามารถระบุได้ว่าเป็นผู้ใด โดยคำนวณตามสมการที่ 14 ได้ค่า $o_1 + u$ แต่ธนาคารเก็บค่า o_1 ไว้กับข้อมูลลูกค้า ธนาคารจึงสามารถคำนวณค่า u ซึ่งเป็นกุญแจส่วนบุคคลของ U ได้ และทำให้ U ไม่สามารถใช้ระบบเงินสดดิจิทัลได้อีกต่อไป

5. ผลการออกแบบ และประสิทธิภาพในการทำงาน

5.1 การวิเคราะห์ความปลอดภัยในโปรโตคอล ระบบเงินสดดิจิทัลแบบใหม่ควรครอบคลุมเงื่อนไขดังนี้

1. Unforgeability สามารถป้องกันการสร้างเหรียญปลอมโดยอาศัยการลงลายเซ็นบนเหรียญ โดยธนาคารนำกุญแจส่วนบุคคล x ลงลายเซ็นบนตัวแปร $m = H_1(A, B, a, b, z)$ ถ้า U ต้องการปลอมแปลงเหรียญ เขาต้องรู้ค่า x โดยการแก้ปัญหาคือ Discrete Logarithm จากค่า y ซึ่งเป็น กุญแจสาธารณะ แต่ปัญหานี้เป็น Uncomputable Problem (NP Complete) [7, 10] ดังนั้น U จึงไม่สามารถหาค่า x เพื่อสร้างเหรียญปลอมได้

โปรโตคอลนี้ยังป้องกันการฉ้อโกงที่ลูกค้าเจ้าของเหรียญทำการเปลี่ยนแปลงค่าตัวแปรบางตัวที่เป็นข้อมูลลับของลูกค้าเพื่อนำเหรียญไปใช้ซ้ำ ถ้า U เปลี่ยนแปลงพารามิเตอร์บางตัวในเหรียญดิจิทัล แล้วตัวแปร $m = H_1(A, B, a, b, z)$ ย่อมเปลี่ยนค่าไปเป็น $m' = H_1(A', B', a', b', z')$ โดยอาศัยคุณสมบัติของฟังก์ชัน Hash คือ Collision-Freeness ซึ่งระบุอยู่ในงานวิจัยของ Brands [3] เพื่อสร้าง Message Integrity ทำให้ตัวแปร $m \neq m'$ อย่างแน่นอน ดังนั้นลายเซ็นบนเหรียญจึงมีค่าเปลี่ยนไปจากเดิม ร้านค้าจึงสามารถตรวจสอบความถูกต้องของเหรียญได้ทุกครั้ง

2. Untraceability สามารถป้องกันการติดตามการใช้เงินจากธนาคารโดยอาศัยเทคนิคการลงลายมือชื่อลับเพื่อให้ธนาคารสร้างลายเซ็นบนข้อมูลที่ได้รับจากลูกค้า โดยไม่สามารถทราบได้ว่าข้อมูลนั้น จะกลายเป็นเหรียญดิจิทัลที่มีลักษณะเป็นอย่างไร เพื่อป้องกันธนาคารติดตามพฤติกรรมการใช้เงินของลูกค้า นอกจากนี้ยังเพิ่มความมั่นใจให้กับลูกค้า ว่าทางธนาคารไม่มีทางปฏิเสธการทำรายการถอนเหรียญของลูกค้าได้

(Nonrepudiation) เพราะลายเซ็นบนเหรียญเป็นเครื่องยืนยันว่าธนาคารสามารถสร้างได้แต่เพียงผู้เดียว

3. Unreusability สามารถป้องกันการใช้เหรียญซ้ำ โดยอาศัยคุณสมบัติ Tamper-Resistance จากสมาร์ตการ์ด ข้อมูลในหน่วยความจำส่วนนั้นไม่สามารถเข้าถึงได้โดยง่าย ต้องใช้อุปกรณ์อ่านที่ได้รับอนุญาตเท่านั้น ข้อมูลที่อยู่ในนั้นคือรหัสลับของเหรียญ o_2 ที่ใช้ในการตรวจสอบความเป็นเจ้าของเหรียญร่วมกับรหัสลับที่ลูกค้าเก็บไว้ส่วนหนึ่ง ถ้าเหรียญนั้นใช้แล้วรหัสลับนี้จะถูกลบทิ้งออกจากหน่วยความจำ เมื่อมีการใช้เหรียญครั้งต่อไป ลูกค้าจึงไม่สามารถใช้เหรียญนั้นซ้ำได้

5.2 การวิเคราะห์ประสิทธิภาพในการทำงาน ได้ทำการทดลองโดยการพัฒนาโปรแกรมด้วยภาษาจาวา (Java) ทำงานภายใต้ระบบปฏิบัติการวินโดวส์ 2000 (Windows 2000) บนเครื่องคอมพิวเตอร์ส่วนบุคคลรุ่นเพนเทียม 150 MHz โดยกระทำตั้งแต่ขั้นตอนการติดตั้งระบบ จนถึงขั้นตอนการฝากเงินในการเลือกข้อมูลที่ใช้ในโปรโตคอลใช้การเลือกสุ่มข้อมูลแบบ Cryptographically Strong Pseudo-Random Number Generator (CSPRNG) โดยข้อมูลที่สุ่มทั้งหมดคือกุญแจส่วนบุคคล และกุญแจลับขนาด 160 บิต ในการทำการทดลองเพื่อวิเคราะห์การทำงานของโปรโตคอลนั้นใช้เกณฑ์ดังต่อไปนี้

1. ขนาดของข้อมูลที่ใช้ในโปรโตคอล จากโปรแกรมระบบเงินสดดิจิทัลที่พัฒนาขึ้น ได้ทำการถอนเงินดิจิทัลจากโปรโตคอลของ Brand และงานวิจัยนี้จำนวนทั้งสิ้น 40 เหรียญ และวัดขนาดของข้อมูล พร้อมทั้งหาค่าเฉลี่ย ตารางที่ 1 แสดงค่าเฉลี่ยของขนาดของเงินดิจิทัลของงานวิจัยของ Brands และงานวิจัยนี้จากการทดลอง

ตารางที่ 1 ค่าเฉลี่ยของขนาดเงินดิจิทัลจากการทดลอง

โปรโตคอล	ค่าเฉลี่ย (บิต)		
	Mean	Median	Mode
Brands	5272.65	5274	5274
งานวิจัยนี้	3543.03	3542.5	3546
เปอร์เซ็นต์ความแตกต่าง	32.80%	32.83%	32.76%

ตารางที่ 2 ค่าเฉลี่ยของเวลาที่ใช้ในการคำนวณ Modular Exponentiation

ค่าเฉลี่ยเวลาในการทำงานในงานวิจัยของ Brands [3] (วินาที)				ค่าเฉลี่ยเวลาในการทำงานในงานวิจัยนี้(วินาที)			
Modular Exponentiation	Mean	Median	Mode	Modular Exponentiation	Mean	Median	Mode
$a = g^w \pmod{p}$	0.3873	0.38	0.38	$a' = g^k \pmod{p}$	0.5053	0.39	0.39
$b = (Ig_2)^w \pmod{p}$				$\gcd(a', q) = 1$			
				$b' = (Ig_2)^k \pmod{p}$			
$A = (Ig_2)^s \pmod{p}$	1.557	1.54	1.54	$A = (Ig_2)^v \pmod{p}$	1.5535	1.54	1.54
$z' = z^v \pmod{p}$				$z = z'^v \pmod{p}$			
$a' = a^u g^v \pmod{p}$				$a = a'^\alpha g^\beta \pmod{p} \pmod{q}$			
$b' = b^{su} A^v \pmod{p}$				$b = a'^{\alpha v} A^\beta \pmod{p} \pmod{q}$			
$B = g_1^{x_1} g_2^{x_2} \pmod{p}$				$B = g_1^{x_1} g_2^{x_2} \pmod{p}$			
$g' = h^{c'} a'$	0.9195	0.88	0.83	$a = (g' y^{-a})^{m^{-1}} \pmod{p} \pmod{q}$	0.8663	0.85	0.88
$A' = z'^{c'} b'$				$b = (A' z^{-a})^{m^{-1}} \pmod{p} \pmod{q}$			
$g_1^{t_1} g_2^{t_2} = A^d B$	0.6483	0.63	0.66	$r = (g_1^{s_1} g_2^{s_2} B^{-r})^{m p^{-1}} \pmod{p} \pmod{q}$	0.6468	0.66	0.66

จากตารางที่ 1 ขนาดของเงินดิจิทัลของงานวิจัยนี้น้อยกว่างานวิจัยของ Brands คิดเป็นร้อยละ 32.73 ด้วย ขนาดของเงินดิจิทัลที่ลดลง ส่งผลให้ข้อมูลที่ต้องเก็บในสมาร์ตการ์ดประกอบด้วย เงินดิจิทัล และข้อมูลลับประกอบด้วย (v, x_1, x_2, e) ลดลงร้อยละ 29.19 และลดขนาดของข้อมูลที่ร้านค้าต้องเก็บเพื่อนำไปขึ้นเงินกับทางธนาคาร ในขั้นตอนของการฝากเงินได้แก่ $(A, B, a, b, z, s, Date/Time, s_1, s_2)$ คิดเป็นร้อยละ 30

2. เวลาที่ใช้ในการทำงาน ในโปรโตคอลเงินสดดิจิทัลทั้งของ Brands และงานวิจัยนี้ใช้หลักการทำงานที่อยู่บน

พื้นฐานของ Discrete Logarithm [3, 7, 9, 12] ซึ่งใช้ q ความยาว 160 บิต และใช้ p ความยาว 1024 บิต โดยโปรโตคอลเงินสดดิจิทัลทั้งสองงานวิจัยมีการทำ Modular Exponentiation บน Z_p ทั้งหมด $(g^x \pmod{p})$ ดังนั้นงานวิจัยของ Brands และงานวิจัยนี้จึงใช้เวลาในการทำงานโดยเฉลี่ยเท่ากัน ซึ่งเท่ากับ $O((\log q)(\log p)^2)$ [9, 11]

การประมาณค่า CPU-time ในโปรแกรมของระบบเงินสดดิจิทัลจากการทดลองนั้นได้วัดเวลาที่ใช้การทำ Modular

Operations ต่างๆจากการทำการทดลอง 40 ครั้ง ซึ่งผลที่ได้นั้น สอดคล้องกับ Complexity ผลดังตารางที่ 2

จากตารางที่ 2 ค่าเฉลี่ยที่ได้นั้นจะเห็นว่าค่าใกล้เคียงกัน สอดคล้องกับการคำนวณค่า Complexity ที่สรุปว่าโปรโตคอล ทั้งสองมีการทำงานโดยเฉลี่ยเท่ากัน

6. สรุปผลการวิจัย

โปรโตคอลแบบใหม่สำหรับระบบเงินสดดิจิทัล ที่ป้องกันผู้ฉ้อโกงเหรียญดิจิทัลไปใช้ชำระเงินซ้ำได้ล่วงหน้า ที่ได้นำเสนอในหัวข้อที่ 4 นั้นมีประสิทธิภาพที่ดีขึ้นเมื่อนำมาเปรียบเทียบกับงานวิจัยของ Brands [3] โดยเมื่อทำการวิเคราะห์เปรียบเทียบขนาดของเงินสดดิจิทัลแล้ว งานวิจัยนี้สามารถลดข้อมูลที่เป็นเงินสดดิจิทัลได้ 32.73 เปอร์เซ็นต์ ลดข้อมูลที่เก็บในสมาร์ตการ์ดได้ประมาณ 29.19 เปอร์เซ็นต์ และช่วยลดข้อมูลที่ใช้ในการฝากเงินได้ 30 เปอร์เซ็นต์ ในส่วนเวลาที่ใช้ในการทำงานนั้นใช้เวลาโดยเฉลี่ยเท่ากัน จึงสรุปได้ว่างานวิจัยนี้ทำให้ประสิทธิภาพในการทำงานของโปรโตคอลเงินสดดิจิทัลดีขึ้น รวดเร็วขึ้น และยังคงไว้ซึ่งความมั่นคงในการรักษาความลับของข้อมูล สำหรับบุคคล และกฎเกณฑ์สาธารณะ อาจให้คนกลางที่ที่หน้าที่เป็น Certificate Authority เป็นผู้ออกให้ อาจเป็นหน่วยงานของรัฐหรือหน่วยงานที่น่าเชื่อถือ ซึ่งจะทำให้ระบบเงินสดดิจิทัลมีความปลอดภัยในการใช้งานและมีความน่าเชื่อถือมากขึ้น

7. เอกสารอ้างอิง

- [1] Chaum, D., Security without identification: Transaction systems to make big brother obsolete, Communications of the ACM : 1030-1044, 1985.
- [2] Brands, S., An Efficient Off-line Electronic Cash System Based on The Representation Problem, Technical Report CS-R9323, CWI (April 1993): 77 p., 1993.
- [3] Brands, S., Untraceable Off-line Cash in Wallets with Observers, Advances in Cryptology - Proceeding of CRYPTO'93 : 302-318, 1993.
- [4] Chaum, D., Fiat, A. and Naor, M., Untraceable electronic cash, Advances in Cryptology- Proceeding of CRYPTO '88 : 319-327, 1988.
- [5] Chaum, D. and Pedersen, T. P., Transferred Cash Grows in Size, Advances in Cryptology - Proceeding of EUROCRYPT '92 : 390-470, 1993.
- [6] Chaum, D. and Pedersen, T. P., Wallet DataBases with Observers, Advances in Cryptology - Proceeding of CRYPTO'92 : 89-105, 1993.
- [7] IEEE P1363, Standard Specifications for Public Key Cryptography, Institute of Electrical and Electronics Engineers, Inc., New York, 238 p., 1999.
- [8] Schneier, B., Applied Cryptography Protocol, Algorithms, and Source Code in C, 2 ed., John Wiley & Sons, Inc., New York, 759 p., 1996.
- [9] Stalling, W., Cryptography and Network Security: Principles and Practice, 2 ed., Prentice Hall International, Inc., New Jersey, 379 p., 1995,
- [10] Stinson, D. R., Cryptography Theory and Practice, CRC Press, Florida, 434 p., 1995.
- [11] Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A., Handbook of Applied Cryptography, CRC Press, Florida, 780 p., 1996.
- [12] Diffie, W. and Hellman, M. E., Multiuser cryptographic techniques, Proceedings AFIPS 1976 National Computer Conference : 109-112, 1976.
- [13] Chaum, D., Blind Signatures for Untraceable Payments, Advances in Cryptology - Proceeding of CRYPTO'82 : 199-203, 1982.
- [14] Camenisch, J., Piveteau, J. and Stadler, M., Blind Signature Based on the Discrete Logarithm Problem, Advances in Cryptology-EUROCRYPT'94 : 428-432, 1994.

- [15] Rivest, R. L., Shamir, A. and Adelman, L. M., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communication of the ACM : 120-126, 1978.
- [16] Schnorr, C. P., Efficient Signature Generation by Smart Cards, Journal of Cryptology : 161-174, 1991.
- [17] NIST, Digital Signature Standard (DSS), Federal Information Processing Standards Publications (FIPS PUB 186), 1994.
- [18] Ferguson, Niels., Single Term Off-line Coins, Advances in Cryptology - EUROCRYPT'93 : 318-328, 1993.