FAIR CASH SCHEME BASED ON OKAMOTO'S DIVISIBLE ELECTRONIC CASH

PHITHA TANPAIROJ

A THESIS SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
1999

ISBN 974-662-495-4

3936999 SCCS/M : MAJOR : COMPUTER SCIENCE ; M.Sc. (COMPUTER SCIENCE)
KEY WORDS : FAIR DIVISIBLE ELECTRONIC CASH / CRYPTOGRAPHY VERIFIABLE SECRET SHARING / REVOCABLE BLIND SIGNATURE

PHITHA TANPAIROJ : FAIR CASH SCHEME BASED ON OKAMOTO'S DIVISIBLE ELECTRONIC CASH. THESIS ADVISORS : ASST. PROF. DAMRAS WONGSAWANG, Ph.D., ASSOC. PROF. SUPACHAI TANGWONGSAN. 81 P. ISBN 974-662-495-4

In the era of electronic information, many electronic services have been made available since the invention of the Internet. Electronic commerce is one of those services and it has been widely appreciated. Uncomplicated and widespread accessibility to the Internet also contributes to the growth of electronic commerce. Unfortunately, the Internet today provides inadequate security for all of its services especially in financial transactions. Many groups of researchers are creating new feasible methods to provide adequate security for electronic payment schemes, not only for use in the Internet but also for other types of media.

One of the most significant issues in electronic commerce is "payment techniques." Electronic payment is the vital starting point for electronic commerce. Electronic commerce will not be practically implemented unless suitable and secure payment techniques are established. Fortunately, several electronic payment standards exist today. SET is a standard for the payment scheme by using credit card via the Internet and FirstVirtual is a standard for financial transaction gateway. However, there is no standard for electronic cash system that is implemented in an on-line or off-line environments. On-line electronic cash systems have been being developed constantly for more than 10 years but off-line electronic cash is still in an immature state, even though it has existed since 1988.

The objective of this thesis is to build an electronic cash system which provides users with anonymity and, in specific circumstances, an ability to revoke any anonymity. The anonymity or privacy can be misused for criminal activities such as money laundry and blackmailing. Thus, in the presented scheme, all users have full privacy, but all coins and uses of anonymity can be revoked or suspended unconditionally, by the cooperation of all trusted agents. This scheme introduces techniques that utilize verifiable secret sharing and revocable blind signature to archive a desired balance between privacy and authenticity. Such coin requires a group of trusted agents in order to be produced or to be revoked. In other words, it guarantees that a bank cannot trace any coin without cooperation from all trusted agents.

3936999 SCCS/M : สาขาวิชา : วิทยาการคอมพิวเตอร์ ; วท.ม. (วิทยาการคอมพิวเตอร์)

พิธา ตัณฑ์ไพโรจน์ : การปรับปรุงแบบจำลองเงินอิเล็คโทรนิค ของ โอกาโมโต้ เพื่อให้มีความสมดุลย์ระหว่างความเป็นส่วนตัว และความปลอดภัยของระบบ (FAIR CASH SCHEME BASED ON OKAMOTO'S DIVISIBLE ELECTRONIC CASH). คณะกรรมการควบคุมวิทยานิพนธ์ ผศ. ดำรัส วงศ์สว่าง, Ph.D., รศ. ศุภชัย ตั้งวงศ์ศานต์, Ph.D. 81 หน้า. ISBN 974-662-495-4

ในยุคของข้อมูลอิเล็คโทรนิค มีบริการทางอิเล็คโทรนิคมากมายที่ได้รับการพัฒนานับตั้งแต่การก่อตั้งระบบอินเตอร์เน็ท การค้าอิเล็คโทรนิคก็เป็นหนึ่งในบริการเหล่านั้น และเป็นบริการที่ได้รับความยอมรับในวงกว้าง เนื่องจากความง่ายดาย และเครือข่ายที่แผ่ขยายไปในวงกว้างของระบบอินเตอร์เน็ท ได้สนับสนุนการเติบโตของการค้าอิเล็คโทรนิค แต่ว่าการรักษาความปลอดภัยบนระบบอินเตอร์เน็ทนั้นยังมีไม่เพียงพอโดยเฉพาะอย่างยิ่งการทำธุรกรรมทางการเงิน กลุ่มของนักวิจัยได้พยายามที่จะพัฒนาวิธีการที่มีความปลอดภัยสูงที่จะนำมาใช้ในระบบการชำระเงินผ่านระบบเครือข่ายซึ่งไม่จำกัดอยู่เพียง ระบบอินเตอร์เน็ทแต่ยังรวบระบบเครือข่ายอื่น ๆ ด้วย

หนึ่งในประเด็นที่มีความสำคัญที่สุดในระบบการค้าอิเล็คโทรนิคคือเทคโนโลยีการชำระเงิน การชำระเงินผ่านทางระบบอิเล็คโทรนิคเป็นจุดเริ่มต้นที่สำคัญของระบบการค้าอิเล็คโทรนิค เนื่องจากระบบการค้าอิเล็คโทรนิคคงจะไม่สามารถที่จะใช้งานได้อย่างมีประสิทธิภาพ โดยปราศจากระบบการชำระเงินที่มีความเหมาะสมและมีความปลอดภัยเพียงพอ ในปัจจุบันมีการกำหนดมาตรฐานการจ่ายเงินผ่านทางระบบอิเล็คโทรนิคอยู่หลายแบบด้วยกัน อย่างเช่นระบบ SET เป็นมาตรฐานของการจ่ายเงินโดยใช้บัตรเครดิตผ่านทางระบบอินเตอร์เน็ท FirstVirtual เป็นมาตรฐานการจ่ายเงินผ่านทางตัวกลางทางการเงิน อย่างไรก็ตามในปัจจุบันไม่มีมาตรฐานสำหรับระบบที่เป็นการใช้เงินสดแบบอิเล็คโทรนิค ทั้งที่เป็นแบบ On-line และ Off-line ระบบเงินสดอิเล็คโทรนิคที่เป็นแบบ On-line ได้มีการพัฒนาอย่างต่อเนื่องมาเป็นเวลามากกว่า 10 ปี แต่ระบบเงินสดอิเล็คโทรนิคที่เป็นแบบ Off-line ยังอยู่ในขั้นที่ไม่สมบูรณ์มากนัก แม้ว่ามันจะได้รับการเสนอมาตั้งแต่ปี 2531

จุดประสงค์ของวิทยานิพนธ์ คือการเสนอแนวคิดที่จะพัฒนาระบบเงินสดอิเล็คโทรนิค ที่ให้ความสมดุลย์ระหว่างความเป็นส่วนตัวของผู้ใช้ และความปลอดภัยของระบบ รวมถึงความสามารถในการถอดถอนความเป็นส่วนตัว เนื่องจากความเป็นส่วนตัวของระบบอาจจะถูกนำไปใช้ในทางที่ผิดเพื่อก่ออาชญากรรม ตัวอย่างเช่น การฟอกเงินหรือการข่มขู่เอาเงิน ดังนั้นระบบที่เสนอ ผู้ใช้ทุกคนจะได้รับความเป็นส่วนตัว แต่ว่าความเป็นส่วนตัวสามารถที่จะถูกถอดถอนได้อย่างไม่มีเงื่อนไข ด้วยความร่วมมือจากองค์กรที่เชื่อถือได้ โดยวิธีการนี้ได้นำเสนอวิธีที่ใช้การกระจายความลับที่สามารถที่จะตรวจสอบได้ (Verifiable Secret Sharing) และ การเซ็นชื่อแบบบอดที่สามารถจะถอดถอนได้ในภายหลัง (Revocable blind signature) เพื่อที่จะบรรลุความต้องการที่จะสร้างความสมดุลย์ระหว่างความปลอดภัยของระบบ กับความเป็นส่วนตัวของผู้ใช้ โดยที่การสร้างและถอดถอนความเป็นส่วนตัวของเหรียญต้องมีองค์กรที่เชื่อถือได้เข้าร่วม เพื่อที่จะให้ความมั่นใจว่าองค์กรที่เป็นผู้ออกเงินอิเล็คโทรนิค ไม่สามารถที่จะทำการถอดถอนความเป็นส่วนตัวโดยปราศจากความร่วมมือขององค์กรที่เชื่อถือได้