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.