A Thesis for the Degree of Master

A Study on Fair Electronic Cash System with and without TTP

Yan Xie

School of Engineering

Information and Communications University

2004

A Study on Fair Electronic Cash System with and without TTP

A Study on Fair Electronic Cash System with and without TTP

Advisor : Professor Kwangjo Kim

by

Yan Xie
School of Engineering
Information and Communications University

A thesis submitted to the faculty of Information and Communications University in partial fulfillment of the requirements for the degree of Master of Science in the School of Engineering

Daejeon, Korea
January. 11. 2004
Approved by

(signed)

Professor Kwangjo Kim
Major Advisor

A Study on Fair Electronic Cash System with and without TTP

Yan Xie

We certify that this work has passed the scholastic standards required by the Information and Communications University as a thesis for the degree of Master

January. 11. 2004

Approved:

Chairman of the Committee
Kwangjo Kim, Professor
School of Engineering

Committee Member
Daeyoung Kim, Assistant Professor
School of Engineering

Committee Member
C.Pandu Rangan, Invited Professor
School of Engineering

M.S. Yan Xie

2001825

A Study on Fair Electronic Cash System with and without TTP

School of Engineering, 2004, 48p.
Major Advisor : Prof. Kwangjo Kim.
Text in English

Abstract

The research on off-line electronic cash(e-cash) schemes has drawn much attention since Chaum *etc* [8] presented the first off-line anonymous electronic cash scheme in 1988. However, anonymous electronic cash schemes also facilitate fraud and criminal activities [32], such as money laundering, blackmailing and illegal purchases. Frankel *etc* [13]. first introduces the concept of fair electronic cash scheme in 1996, fair off-line e-cash (FOLC) schemes extend off-line anonymous electronic cash scheme to allow a qualified trust third party(TTP) to revoke the anonymity of the user under a warrant. The research on FOLC scheme has been one of the hottest topics on electronic cash since then.

In this thesis, we propose two off-line fair E-cash schemes: a fair e-cash protocol with the limited power of TTP and a fair e-cash system without TTP.

We first present a fair e-cash scheme with the limited power of TTP, which is normally used in several fair e-cash systems in order to conduct tracing mechanism. Generally user should send his withdrawal information to TTP before he withdraws the money from bank. In our protocol, bank first gives the signature on user's coin by using the blind

signature protocol. After TTP verifies the validity of the e-coin, and ensures that each dubious coin and user can be traced if required. He gives his signature in the e-coin, which means he has the traceability for each e-cash during tracing protocol. So there are two signatures on a coin: The signature of the bank ensures that no entity is able to forge a coin, and the signature of the TTP ensures that each dubious user and coin can be traced with the cooperation of bank. We make the interaction between user and TTP after the withdrawal protocol, then TTP only knows information about coin. In this protocol TTP can't trace user's identity by himself. Even if he has the coin of user, there is not linkage to user's identity. and in case of coin tracing, since coin is provided by user anonymously, without bank or user's help, TTP can't distinguish which coin will be illegal. The tracing mechanism only can be carried out under the cooperation of bank's. The misuse of tracing mechanism of TTP can be prevented.

In our second e-cash system, an ID-based distributed "magic ink" signature is introduced to build a fair e-cash system without TTP. ID-based signature simplifies the certification of public key of bank, the bilinear pairings used to construct ID-based signature also reduces the size of public keys of signers. The fairness of our e-cash system is satisfied by the distributed "magic ink" signature, which gives the user a blind signature on his coin during withdrawal protocol to protect user's privacy, and detects any prefect crimes later. The tracing mechanism can be implemented without the help of TTP, in case of the tracing information are distributed by a set of signers of the bank through a (n, n) threshold secret sharing, only under the cooperation of n signers of bank the tracing protocol can achieve. The bank's tracing ability is well controlled. The additional computation and communications of TTP are omitted, the misbehavior of tracing, which is undesired by the user and the bank are prevented.

The security analysis and comparisons of our protocols are also discussed.

Contents

List of Tables

List of Figures

List of Abbreviations

e-cash electronic cash

ID-based Identity based

TTP Trust Third Party

DLP Discrete Logarithm Problem

DDHP Decision Diffle-Hellman Problem

CDHP Computational Diffle-Hellman Problem

GDHP Gap Diffle-Hellman Problem

DMIS Distributed “magic ink” signature

IDDMIS ID-based distributed “magic ink” signature

List of Notations

B Bank

M Merchant

U User

DSA Digital Signature Algorithm

$VerDSA$ Verification Algorithm of Digital

H Collision-resistant one-way hash function

$||$ Concatenation of messages

$SKREP$ Signature of knowledge of a representation

I. Introduction

1.1 Electronic Cash System

As an important electronic payment system, electronic cash (or e-cash) system obtains more and more consideration due to the wild application and rapid development of electronic commerce in e-society. It can be considered as an imitation of analog money, but more convenient and economical.

In the early stage of designing an e-cash system, protecting user's privacy is a basic requirement. The anonymity of user in e-cash was firstly achieved by Chaum's paper [8]. Compared with on-line e-cash system, which means that during payment protocol bank should be online to cooperate with merchant, An off-line system is more efficient. The research on off-line electronic cash schemes has drawn much attention since Chaum *etc.* presented the first off-line anonymous electronic cash scheme [7] in 1988. However, anonymous electronic cash schemes also facilitate fraud and criminal activities [32], such as money laundering, blackmailing and illegal purchases. Frankel *etc.* first introduced the concept of fair off-line electronic cash(FOLC) scheme [13] in 1996, FOLC schemes extend off-line anonymous electronic cash scheme to allow a qualified trust third party(TTP) to revoke the anonymity of the user under a warrant. The research on FOLC scheme has been one of the hottest topics on electronic cash since then. In such kind of system, a tracing mechanism, which consists of owner tracing protocol and coin tracing protocol to prevent money laundering and blackmailing respectively, was added to achieve fairness requirement. Recently several schemes were gradually proposed to improve fairness and efficiency, most of them need the cooperation of TTP for tracing, but the extra computation and communication cost of TTP are not desirable to both user and bank, and the misuse of tracing ability from TTP is hard to prevent or detect, So designing a fair off-line e-cash system with limited power of TTP or without TTP is discussed in our thesis respectively.

According to the properties of fair off-line e-cash system, we propose two fair e-cash systems.

1.2 Our Contribution

In our thesis, we study on e-cash system, specially on fair off-line e-cash system. We also provide two schemes to give some idea about designing fair off-line e-cash system. The summarizations of our contribution are as follows:

A fair e-cash scheme based on the limited power of TTP

Normally, in a fair e-cash system, a TTP is used to ask user to send some information related with his identity before withdrawal protocol, so that the tracing mechanism can be cooperated by bank and TTP. But if TTP holds the valid coin of user, even he can make tracing mechanism by himself, specially in user tracing protocol. This kind of misuse tracing is undetectable and undesirable to legal user. In order to limit the illegal tracing power of TTP, we proposed a revocable e-cash system with the limited power of TTP. In our protocol bank first gives the signature on cash by using the blind signature protocol. After TTP verifies the validity of the e-coin, and ensures that each e-coin can be traced if required, TTP gives his signature on the e-coin, which means that he has the traceability of each coin with cooperation from bank during tracing protocol. So there are two signatures in a coin: the signature of the bank ensures that no entity is able to forge a coin, and the signature of the TTP achieves that each dubious user and coin can be traced. We process the interaction between user and TTP after the withdrawal protocol, then TTP only knows information about coin. In this protocol TTP can't trace user's identity by himself. Even if TTP has the coin of user, there is not linkage with user's identity. In case of coin tracing, since coin is provided by user anonymously, without bank or user's help, TTP can't distinguish which coin will be illegal. So each tracing only can be carried out under the cooperation of bank. So the misuse of tracing mechanism of TTP can be prevented.

A fair e-cash without TTP

Most of works in fair e-cash system introduced a TTP to cooperate with bank during tracing protocol to detect prefect crime. But it also increases extra computation and communication costs, and the misuse of tracing is difficult to be detected or prevented. In our scheme, we suggest a solution to provide a fair off-line e-cash system without the involvement of TTP, our scheme is constructed on the ID-based "magic ink" signature, the idea of ID-based signature here is to reduce the certification and management of bank's public key. Due to the application of bilinear pairing, the sizes of pubic key of signer smaller. "Magic ink" signature can provide a receiver a blind signature, which can be revoked later, Since a single signer's traceability can't be controlled, we use a (n, n) threshold security sharing scheme to distribute the tracing information in n signers, so if we use this property in a fair e-cash system, bank can give the user a blind signature on his coin to keep his privacy, the prefect crime is detected by n distinguished signers of bank, but they should work together to revoke the tracing information, so that the traceability is well controlled. Our scheme avoids the additional costs and prevents the misuse tracing of TTP, the smaller size of public key also save the storage resource of user.

1.3 Organization of Thesis

We introduce overview of e-cash System and related works, as well as some relative basic cryptographic primitives in Chapter II. Chapter III shows our fair e-cash system based on the limited power of TTP. A fair e-cash system without TTP is given in chapter IV. The additional coats are saved, it also can prevent the undetectable tracing without permission. Final conclusions and future works are made in chapter V.

II. Preliminaries

We begin this chapter with an overview of e-cash systems. Then some properties of fair e-cash system and related works are presented. Finally we describe basic cryptographic primitives which are used through our protocols

2.1 Overview of Electronic Cash Systems

2.1.1 Electronic Cash System

A electronic cash system is a set of parties with their interactions, which conduct a exchange of money between parties.

A typical e-cash system consists of three parties:

- *User:* purchases goods or services from merchant by using e-cash.
- *Merchant:* exchanges goods and e-cash with user, and deposits e-cash to bank.
- *Bank:* issues e-cash and maintains bank account for users and merchants.

In some fair e-cash system a trust third party(TTP) is required to help bank to achieve revocability. Basically there are three protocols included in a e-cash system: **Withdrawal**, **Payment**, and **Deposit**.
Fig.2.1 shows the basic model of e-cash system.

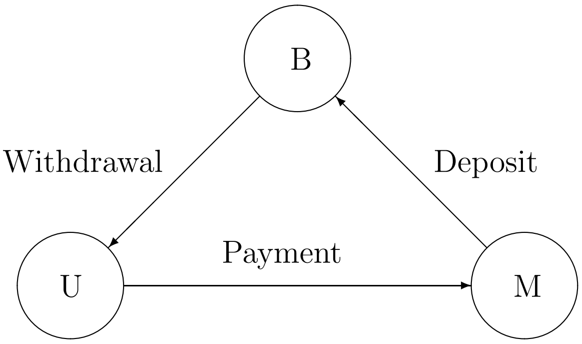

Figure 2.1: Basic model of e-cash system

2.1.2 Properties of E-cash System

In designing an efficient ideal e-cash system, several properties are required:

- **Anonymity:** system should provide anonymities of the coin and the identity of the user.
- **Unforgeability:** the valid e-cash can't be forged by user.
- **Double spending prevention:** each coin can be only used once, any double spending should be prevented or detected.
- **Divisibility**: user can divide one coin to several small piece of coins, the total value will not be changed.
- **Unlinkability:** it should be impossible to determine whether any two coins originate from same user or not.
- **On-line versus off-line:** the notion on-line and off-line refer to a property of the payment protocol. In many systems merchant is required to contact bank before accepting a coin, in this case,

the system is called an on-line e-cash system; the communication between a merchant and bank isn't efficient. If such a contact is not required during payment protocol, the system is called off-line.

2.2 Fair E-Cash System and Related Works

In order to let the user get the signature of his message without revealing his message from signer, Chaum introduced a blind signature [8], which can be used to protect the privacy of the user. But some malicious person can abuse such perfect anonymity provided by this scheme to commit perfect crimes [32]. For those reasons a e-cash system should achieve anonymity and revocability, which are denoted as fairness.

A tracing mechanism is developed to conduct the revocability. There are two kinds of tracing protocols: **User Tracing Protocol** and **Coin Tracing Protocol**.

- **User Tracing Protocol:** The user tracing protocol is used to determine the identity of the user in a specific payment transaction. In this protocol, bank gives the view of a deposit coin to TTP, and TTP returns some specific information, which allows the bank to identify the user through the database of user account. Money laundering can be prevented from detecting the identity of the illegal user in this protocol.

- **Coin Tracing Protocol:** The coin tracing protocol is considered to determine the e-coin in deposit protocol. Bank gives TTP user's withdrawal information, and TTP returns some information, which enables bank to find and freeze the corresponding coin in deposit transaction. Blackmailer normally forces some legal user to withdraw some anonymity coin for him, so that he can use it without being detected, but with the withdrawal report of the victim; the blackmailing crime can be detected in this protocol.

Both of two tracing protocols should be provided in a Fair e-cash system, due to different crime cases. For example, if a system just supports user tracing protocol, when the blackmailing occurs, the TTP should break all the coins of deposit protocol to find the original coin in withdraw protocol, on the contrary if a system just provides coin tracing, in order to prevent money laundering TTP should break all the coin of withdrawal protocol. Due to the absence of each tracing mechanism contradicts selectivity requirement of the fair e-cash system ; user tracing and coin tracing protocol must be included together.

Many fair anonymity schemes are suggested, by using different technologies, such as: fair blind signature [9, 11, 33], indirect discourse proofs [13], magic ink signature [1, 19], group signature [35, 38], and message authentication code [20], and etc [34].

Brickell [5] and Stadler [33] independently introduced a tracing mechanism based on trust third party(TTP) in e-cash system, with the help of TTP, bank can reveal the anonymity of some special user to prevent or detect the perfect crime.

Brickell proposed two ideas in his paper, one is based on Schorr blind signature scheme, which needs the interactive proof between bank and TTP, the other idea is based on RSA blind signature and *cut-and-choose* protocol. Stadler introduced the conception of fair blind signature, this scheme develops the e-cash system by Chaum *etc.* However, in Brickell and Stadler's schemes only user tracing is achieved, also the TTP should be online, the efficiency is a little high. Jacksson and Yung [18] introduced the notion of "challenge semantics" to prevent the revealing of private signature key of bank, but in this scheme TTP still needs to be online during withdrawal and payment protocol. Later Camenish [9] introduced the coin tracing mechanism in e-cash system, also Frankel [13] independently proposed a off-line fair e-cash system. In their works, TTP is not online, but complex modular exponential computation is required, so the efficiency also needs to be improved. Davida *etc* [11] provided a off-line revocable e-cash scheme based on schnorr blind signature, TTP is off-line, and it improved the efficiency of user and coin tracing by using proof of equality of logarithms.

The idea of trusted third party tracing was abandoned by recent approaches [34, 29, 21] for fair e-cash systems, but they only protect against blackmailing and lack support for coin and owner tracing. In [22, 23] show that coin and owner tracing also can be implemented without any trusted third party by introducing an audit concept. But these payment systems require the bank to be on-line at payment protocol.

kügler in his paper [24] shows that coin and owner tracing can be implemented off-line without any trusted third party, he proposed a concept of auditable tracing, which means that user can detect whether his spent coins have been traced or not and whether this tracing has performed with the permission of a judge or the user him self at a certain of time. This scheme provides better protection of user's privacy than unconditional TTP based tracing.

2.3 Cryptographic Background

In this section we introduce some cryptographic primitives used in upcoming protocols. The central concept to construct secure schemes is based on number-theoretic hard problems, which means attacker is difficult to solve those problems in polynomial time or needs to spend expensive resource to break the schemes in a certain period.

2.3.1 The Discrete Logarithm Problem

The difficulty of computing discrete logarithm is a foundation for the work presented in this thesis. We give a definition for this problem, please refer to the paper [25] for more detail.

Definition 2.3.1 *The discrete logarithm problem(DLP) is the following: given a finite cyclic group G, a generator g of G, and an element α, find the integer x, $0 \leq x \leq |G| - 1$, such that $\alpha = g^x$ holds.*

2.3.2 Bilinear Pairing

Bilinear paring namely the Weil pairing and Tate pairing of algebraic curves was first used to analyze the discrete logarithm problem in cryptography, such as MOV attack [26] and FR attack [14]. Now a variety of cryptographic applications based on bilinear pairing [3, 4, 17, 36] are proposed, it is also introduced to construct several ID-based signature schemes [6, 16, 28, 37].

We assume G_1 and G_2 are two cyclic groups of order q for a large prime q, G_1 is an additive group and G_2 is a multiplicative group, A map is a bilinear pairing, if it satisfies following properties:

1. Bilinear: $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$ and $e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$.

2. Non-degenerate: there exits $P, Q \in G_1$, $e(P, Q) \neq 1$.

3. Computability: If $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

We can find following arithmetic hard problems in G_1:

Definition 2.3.2 *Discrete Logarithm Problem (DLP): It means that if there are two groups Q and P, it is difficult to find an integer n, which can satisfy $P = nQ$.*

Definition 2.3.3 *Decision Diffle-Hellman Problem (DDHP): Given P, aP, bP, cP, and $a, b, c \in Z_q^*$, determine whether $c \equiv ab$ mod q.*

Definition 2.3.4 *Computational Diffle-Hellman Problem (CDHP): Given P, aP, bP, $a, b \in Z_q^*$, computes abP.*

Definition 2.3.5 *Gap Diffle-Hellman Problem (GDHP): A class of problems, when the DDHP is easy, but the CDHP is hard.*

We let CDHP and DLP are intractable, that means there is no polynomial time algorithm to solve CDHP and DLP with nonnegligible probability. We call a group G a Gap Diffle-Hellman group, when the DDHP is easy and CDHP is hard on that group. Such group can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear pairing can be derived from the Weil or Tate pairing.

2.3.3 Digital Signature

The digital signature involves only two parties: signer and user. It is assumed that the user knows the public key of the signer. A digital signature is formed by encrypting the entire message with the sender's private key or by encrypting a hash code of the message with sender's private key.

A digital signature consists of a triple algorithm (G, S, V)

Definition 2.3.6 *Key generation algorithm G is a probabilistic polynomial time algorithm, which inputs a security parameter and outputs a pair (p, s) of a public key and a private key.*

Definition 2.3.7 *The signing algorithm S is a probabilistic polynomial time algorithm, which inputs a secret key s, a message m to be signed and outputs a signature of a message $\sigma(m)$.*

Definition 2.3.8 *A verification algorithm V is a deterministic polynomial tim algorithm, which inputs a public p a message m and a signature $\sigma(m)$ and outputs accept/reject.*

2.3.4 Blind Signature

Blind signature is a special type of signature, which is introduced by chaum in 1982. The goal of blind signature is to prevent the signer from observing the original message of user and the resulting signature, so he can't link the signature with user.

A blind digital signature scheme consists three steps described as follows.

- There is a probabilistic polynomial time key generation algorithm, which inputs a security parameter and outputs a pair (p, s) of a public key and a private key.
- User blinds his original message$m$ to m' and sends m' to signer, the $Signer$ uses his private S to signs the message m', and transfers this signature to user.
- User computers signer's valid signature on m by unblinding the signature on m'

2.3.5 Hash Function

A way of authentication is to sign each transmitted message digitally, but digital signature is costly procedures and its' size must be efficient for message transmission. In order to solve this problem, the sender can compute and sign a hash of each message and the receiver can compute the hash again and verify the signature.

The role of a hash function is to compress its input, so that none can efficiently find two inputs that compress to the same string. There are several features of hash functions show as follows:

- It is a Compression algorithm, which inputs a arbitrary bitlength of number x, output a fixed bitlength of number y.
- It is a one-way function, which by given a $y = h(x)$, it is infeasible to find x.
- It guarantees that given a value x it is computationally infeasible to find a $y \neq x$ such that $h(x) = h(y)$.

Hash function is major building block for several cryptographic protocols including pseudorandom generators, digital signatures, and message authentication.

III. A Fair E-cash System Based On the Limited Power of TTP

3.1 The Approach of Our Protocol

The solution of controlling the anonymity is the involvement of the Trusted Third Party(TTP), which can revoke the anonymity of the user or the coin with the cooperation of bank to detect the prefect crime. Bank doesn't has any power to reveal user's privacy. Normally, such system can provide revocability from two kinds of tracing mechanisms, user tracing and coin tracing. User tracing is for identifying the owner of the coin; coin tracing is for identifying the coin. Both of them should be included in a revocable e-cash system to handle different crimes and achieve the system requirement of selectivity.

But the unlimited tracing power of TTP is difficult to control, for example, if TTP gets the coin, he can trace the identity of user by himself. Those misuse of tracing from TTP may break the legal user's privacy. In this chapter, we propose a new revocable e-cash system with the limited power of TTP. By changing the convention protocol process, we try to limit the information that TTP can collect from user, so the tracing can't be done without help from bank. Finally we also verify the security requirements.

3.2 Requirements of Our Scheme

Usually there are four participants in an anonymity controlled e-cash system, which are user(U), bank(B), merchant(M) and TTP; both user and merchant can have a bank account beforehand. There are five protocols consist in this system, three of them are the same as the anonymity e-cash system: a withdraw protocol which user withdraws electronic coin from bank, a payment protocol which user pays the electronic coin to merchant, and a deposit protocol which merchant deposits his electronic coins to the bank. In addition anonymity controlled e-cash system contains two extra protocols acted between bank and TTP: user tracing and coin tracing.

There are 5 requirements of our fair e-cash system, which is described as follows:

- Anonymity: System should provide anonymity of the coin and the identity of the legal user, along with the detection of the double spending.
- Revocation: Due to the prefect crime of the unconditional anonymity e-cash system, TTP should reveal the anonymity of either the coin or the identity of the user.
- Limitation of the tracing: Only TTP has the privilege of tracing the coin and the user's identity, they should not have the ability of forging the valid coin or impersonating a user.
- No framing: In case of the collusion between bank and TTP, a fair e-cash system should ensure that bank could not impersonate a legal user and his/her activities.
- Selectivity: The revocation only can be done under the warrant of an authorized judge, the anonymity of the other legal user, even different transaction of the same user should be protected.

3.3 Our Scheme

In conventional anonymity controlled e-cash system, user should first register to TTP, and TTP embeds the tracing information into the e-coin, and then user withdraws money from bank and gets bank's valid blind signature at the same time. Contrary to the previous protocols, in our scheme bank first gives the signature on user's coin by using the blind signature protocol. After TTP verifies the validity of the e-coin, and ensures that each e-coin can be traced if required, he gives his signature on the e-coin, which means he has the traceability to revoke each dubious coin or identity of user during tracing protocol. So there are two signatures in a coin: The signature of the bank ensures that no entity is able to forge a coin, and the signature of the trustee ensures that each dubious user and coin can be traced. bank can trace the coin or the user only under the help of TTP, and the privacy of honest users will be protected. Further the tracing power of TTP is controlled.

3.3.1 System Setup

System Parameters:

A large prime p and a large number q such that $q|p-1$. A generator g of a subgroup G_q of the multiplicative group Z_p^*.

User and TTP independently create DSA signature system using system parameters, they select $x_u, x_{ttp} \in G_q$ randomly as their private keys, then calculate $h_u = g^{x_u}$ and $h_{ttp} = g^{x_{ttp}}$ as their public keys and publish them respectively.

Bank creates blind DSA signature system by selecting $x_b \in G_q$ randomly as his private key, and calculates as his public key $h_b = g^{x_b}$ and publishes it.

We use $DSA(m)$ to express the DSA signature of entity on the message m , and $VerDSA(m)$ to express the DSA verification algorithm by using entity's DSA public key.

Count Open:

User and merchant open their accounts in bank, and get their identities.

3.3.2 Withdrawal Protocol

Withdrawal protocol contains two steps, first, user gets the blind signature form bank, and second, user gets the signature from TTP:

Step 1

- User should prove his identity to bank; user sends his e-cash requirement , which denotes: $withdrawal\ require||\ 80 bits\ random\ string||\ time.$ and provides his signature on m, which is $S_u = DSA_u(m)$ by his DSA private key. then user sends the pair(m, S_u) to bank.
- Bank verifies user's signature by $VerDSA(S_u, m)$.
- Bank uses blind DSA signature to sign the e-coin, selects $r \in Z_q^*$ and calculates $R = g^r \bmod p$ with his signature $T_b = DSA_b(R)$ and sends them to user, and stores R linked with user's ID as a pair (R, ID_u, m, S_u).
- User establishes a coin c and lets Δ denote as the money value user wants to withdraw and the valid payment period, which can be accepted by bank, then he selects α, $\beta \in_R Z_q^*$, calculates $R' = R^\alpha g^\beta \bmod P$, and blinds cash date by computing $c' = \alpha c(R'||\Delta)^{-1} \bmod q$, then sends c' to bank.

- Then bank computes $c'' = c'H(R||\Delta)$ and $S' = rc'' + Rx_(b)$ mod q and forwards s' and c'' to user.
- User verifies the signature based on following equations:

$$g^{s'} = R^{c''} h_u^{H(R||\Delta)}$$

$$c'' = c'H(R||\Delta)$$

- After the verification passes, user computes

  $S = S'(R'||\Delta)H(R||\Delta)^{-1} + \beta c \bmod q$.

  The Pair (S, R') is user's valid cash signature, which is dedicated as S_b.

The protocol is shown in Fig.3.1.

Step 2

- User should send $(c, R, T_b, S_b, SKREP[\alpha, \beta : R' = R^\alpha g^\beta])$ to TTP, here $SKREP[\alpha, \beta : R' = R^\alpha g^\beta]$ is a signature of knowledge of a representation of R to the bases R' and g, on this signature refer to [10].

  Then TTP should check $verDSA_b(R, T_b)$ and verify the signature of blinded coin through the equation

$$g^s h_b^{-(R'||\Delta)} = R'^c$$

  After this, TTP sends user $S_{ttp} = DSA_{ttp}(c)$ by his DSA private key and as the same time records the pair (R, c) . So finally the e-cash can be expressed as follow: $(\Delta, c, S_b, S_{ttp})$.

3.3.3 Payment Protocol

After verifying the signatures (S_b, S_{ttp}) of bank and TTP on e-coin c, merchant will accept the user's coin and transfer the goods to user.

$$
\begin{array}{ccc}
\textbf{User} & & \textbf{Bank} \\
m & & \\
S_u = DSA_u(m) & \xrightarrow{(m,\ S_u)} & \\
 & & r_i \in_R Z_q^* \\
 & & R = g^r \\
 & \xleftarrow{(R, T)} & T_b = DSA_b(R) \\
\alpha, \beta \in_R Z_q^* & & \\
R' = R^{\alpha} g^{\beta} & & \\
c' = \alpha c(R'||\Delta)^{-1} & & \\
 & \xrightarrow{c'} & \\
 & & c'' = c'H(R||\Delta) \\
 & & S' = rc'' + H(R||\Delta) \\
 & \xleftarrow{(S', c'')} & \\
S = S'(R'||\Delta)H(R||\Delta)^{-1} & & \\
+\alpha\beta & & \\
(S, R') & &
\end{array}
$$

Figure 3.1: Withdrawal protocol

3.3.4 Deposit Protocol

Bank holds a record of spent cash to prevent double spending of e-cash. After receiving *coin* $= (\Delta, c, S_b, S_{ttp})$ from merchant for deposit, bank will verify the validate of the coin, and then check whether the coin has been double spent, if not, bank will deposit the cash to the merchant's account.

3.3.5 User Tracing Protocol

The illegal activities such as money laundering, illegal purchase and double spending can be traced by user tracing protocol. Bank sends e-coin to TTP. Then, TTP finds the R, which is linked with c, and sends R to bank. Based on the previous database saved in withdrawal protocol, bank can find the corresponding user from his database.

3.3.6 Coin Tracing Protocol

When blackmailing occurs, bank and TTP should find the coin. After withdrawal protocol blackmailed user should send his identity ID_u to bank, according to the database of (R, ID_u, m, S_u), bank finds R and passes it to TTP. TTP finds the corresponding c and sends it to bank, then bank can determine and freeze the money.

3.4 Security Analysis

Correctness

We prove the correctness of bank's blind signature as follows:

$$\begin{array}{rcl}
g^S h_b^{-(R'||\Delta)} & = & g^{S'(R'||\Delta)H(R||\Delta)^{-1}+\beta c} h_b^{-(R'||\Delta)} \\
 & = & g^{[(rc''+H(R||\Delta)x_b)](R'||\Delta)H(R||\Delta)^{-1}} h_b^{-(R'||\Delta)} g^{\beta c} \\
 & = & g^{rc''(R'||\Delta)H(R||\Delta)} g^{x_b(R'||\Delta)} g^{-x_b(R'||\Delta)} g^{\beta c} \\
 & = & g^{rc''(R'||\Delta)H(R||\Delta)^{-1}} g^{\beta c} \\
 & = & g^{rc'(R'||\Delta)H(R||\Delta)H(R||\Delta)^{-1}} g^{\beta c} \\
 & = & g^{rc'(R'||\Delta)} g^{\beta c} \\
 & = & g^{rc\alpha(R'||\Delta)^{-1}(R'||\Delta)} g^{\beta c} \\
 & = & g^{rc\alpha} g^{\beta c} \\
 & = & (R^{\alpha} g^{\beta})^c \\
 & = & R'^c
\end{array}$$

Anonymity for legal user

The identity of a legal user is anonymous and cannot be linked with the e-cash. However, one who makes a double spending will be traced only by bank. For a legal user, the DSA blind signature will be used when he withdraws e-coin from bank, so that the bank know nothing about the e-coin, and can not trace the e-cash from the deposit protocol. When user makes payment transaction, merchant can only verify the user's e-cash.

Revocation

TTP records each (R, c) in withdrawal step, and the T_b ensure that R is linked with user's ID by bank, and $SKERP[\alpha, \beta : R' = R^{\alpha} g^{\beta}]$ guarantees R sent by bank is actually used in blind DSA signature of bank on coin. when a tracing requirement is requested, he can easily find out the tracing information and provides it to bank, either user tracing and coin tracing achieves.

Money Value and Payment Period

During withdrawal protocol, Bank should make sure that the value of money of valid electronic cash is same as the value, which is required by user. So that user can't over spend the money. In our protocol we denote Δ as the value of money and payment period. value of money dedicates the money user wants to withdraw, and the payment period dedicates the valid payment time that the money can be spent, because if some person double spent dead person's coin, even we handle this by user tracing mechanism, the malicious person's identity still can't be revealed. Bank embeds Δ in his blind signature on user's coin, the user first can check whether bank give the correct information about money value and payment period on his coin, from verifying $c'' = c'H(R||\Delta)$, any modification in money value or payment period is detectable by user in withdrawal protocol. A valid e-cash in our system should include c; Δ, and S_b, so in payment protocol and deposit protocol, both merchant and bank can verify the validity of e-coin by the public key of bank's blind signature, also they can check the value of money and the period of payment based on Δ linked with coin. If user makes any cheating to modify the value of money or changes the period of payment, the value of Δ will be different from original one, the changed value denoted as Δ' can't pass the verification equation: $g^s h_b^{-(R'||\Delta)} = R'^c$. So both bank and user must make honest information on the value of money and payment period, otherwise any cheating will be detected.

No framing

Even bank colludes with TTP, he cannot frame a legitimate user, because they cannot obtain the user's secret key x_u so that they cannot get the withdrawal counterfeit with the user's signature. If bank forges a cash of the user to fraud him, user can easily detect this by checking the payment records on his account. The counterfeit in the records corresponds a certain of cash, while forging a counterfeit means the bank can forge the user's signature. This is similar to in physical world, the bank must answer for that others withdraw your money without checking up the identity of the withdrawer.

Selectivity

The revocable information is linked with each user's specific coin per withdrawal time, only when bank gives some requirement and information for tracing, TTP may help him to trace the user or the cash, the other user's privacy is kept secret.

Unforgeability

If an illegal user tries to forge a valid e-coin, he must generate a valid blind signature of bank, since a public key pair of bank is (x_b, g^{x_b}) , and solving a discrete logarithm problem under group is infeasible. Then the probability for an attack to get the secret of bank is $1/q$, if q is larger, We can say the forgeability is impossible.

Limited Power of TTP

In this scheme, the tracing power of TTP is controlled. In some previous scheme, TTP know the identity of user's, if he get the coins, he can make illegal tracing by himself, but in our protocol, TTP get the information after user's withdraw the money from bank, if user can provide a valid signature from bank, he doesn't need to reveal his identity to TTP, then his signature can be signature by TTP anonymously. The information he gets from user is not enough to make tracing. Tracing mechanism can be achieved only after bank sends linked tracing information to him. Also we can let it be tamper resistant equipment over Internet, it works 24 hours a day only with the abilities of verification, signature, and tracing, then the tracing power of TTP can be limited in legal activities.

3.5 Summary

Obviously due to requirement of being similar to analog money and detecting perfect crime, we provided a fair e-cash system with limited TTP in this chapter. Since in previous schemes it is difficult to prevent misuse of TTP, we change the protocol process to limit the tracing information, which TTP can get from user, The tracing mechanism only can be achieved with the help of bank, the security requirements of the proposed scheme are also analyzed.

IV. A Fair E-cash System without TTP

4.1 Our Model and Assumption

Payment systems with TTP can provide both tracing mechanisms efficiently, but also have several shortcomings. Firstly, the involvement of TTP spends additional computation and communication costs, which both bank and merchants are not willing to pay. Also the misbehavior of tracing by TTP is difficult to be detected.

In this chapter, we introduce a fair e-cash system without TTP. We used the ID-based distributed "magic ink" signature to implement withdrawal protocol. The advantage of ID-based signature is the simplification of key distribution and certification management; a signer can directly use his identity as his public key instead of an arbitrary number, thus at the same time he can prove his identity rather than providing a certificate from CA. We combined the conception of "magic ink" to achieve the requirement of tracing. The "magic ink" signature provides a revocable anonymity solution, which means that the signer has some capability to revoke a blind signature to investigate the original user in case of abnormal activity, while keeping the legal user's privacy anonymous. A single signer of the bank in "magic ink" signature can easily trace the original user or coin of e-cash without any limitation; this scheme can't satisfy anonymity for a legal user in e-cash system, so we use n signers of the bank to sign the message through a (n, n) threshold secret sharing to distribute the commitment during the signature procedure, single signer's revocability is limited, only under the agreement and cooperation of a set of n singers, the user's identity can be discovered.

Physically “magic ink” signature can be described as follows: a user writes some message on an envelope using magic ink, simultaneously this message also is copied on a blank paper through carbon paper in this envelope, then the signer writes down his signature on the envelope, this signature also will appear on the inside paper, finally the signer and user keep the envelop and signed inside paper respectively. Normally the message is invisible on the envelop, but in some case(criminal activity) signer can discover this invisible message. The “magic ink” signature provides a revocable anonymity solution, which means that the signer has some capability of revealing a blind signature to investigate the abnormal activity, whilst keeps the legal action anonymous. The first “magic ink” signature [19] is based on digital signature standard; this scheme approaches a revocable anonymity from a set of distributed servers through threshold cryptosystem instead of the enrollment of the trust third party in “fair blind signature”. It achieves more security and availability.

In traditional CA-based public key cryptosystem, each participant should provide a digital certificate to prove the validity of his identity and public key; this procedure obviously exhausts huge system resource. In 1984, Shamir proposed an ID-based encryption and signature scheme [30], which directly utilizes user’s identity as his public key. So this scheme could simplify the key distribution and certification management process.

We suggested an ID-based distributed “magic ink” signature scheme in a fair off-line e-cash system by combining a distributed “magic ink” signature with an ID-based signature from bilinear pairing. This scheme can be used in some revocable e-cash system or credential certificates applications. In case of a single signer can easily trace the original user of the message without any limitation; we can use a (n, n) threshold to share the commitment during the signature procedure. Only under the agreement and cooperation of n signers of the bank, the tracing mechanism can be conducted.

We first introduce the structure and the basic idea of ID-based "magic ink" signature, and present our scheme by upgrading n signers of banks, finally we give analysis of our protocol.

4.2 ID-Based "Magic Ink" Signature

An ID-based "magic ink" signature scheme consists of three parties and five steps, which is described as follows:

- Three parties are Trust Authority(TA), signer and receiver.
- **Setup** is a randomized algorithm, which generates system parameters and a master key by inputting a security parameter to TA.
- In **Extract** step, TA inputs system parameters, master key and an arbitrary $ID \in \{0,1\}^*$, and outputs a private key S_{ID}. Here ID is the signer's identity, which is treated as the signer's public key.
- **Signature** is a signature generation protocol engaged by receiver and a signer, signer outputs a blind signature, and receiver finally produces a valid or failed signature. Signer records a signature-view variant in their database to indicate each blind signature.
- **Verification** is a randomized algorithm that takes message m with its signature and signer's identity as an input, and outputs acceptation or rejection.
- **Tracing** occurs in case of illegal activities, signer searches his database of signature-view invariant to find a value, which can be

linked to the valid signature. From this value, signer can find the original signature receiver.

4.2.1 Basic Protocol of ID-Based "Magic Ink" Signature

ID-based "magic ink" signature can be thought as a combination of ID-based signature with a revocable blind signature. We will describe the basic idea of ID-based "magic ink" signature of a single signer. First set G_1 to be a cyclic additive group and G_2 to be a multiplicative group, both of groups have a same prime order q, our scheme is built on GDHP Group . We view the bilinear map as $e : G_1 \times G_1 \rightarrow G_2$.

At the beginning of this protocol, the **TA** operates Setup and Extract, during the generation of private key of the signer, we can use n **TA** with a (n, n) threshold security sharing to share the master key, in order to control the power of **TA**.

Setup

Let P be a generator of G_1, randomly choose a number $s \in Z_q^*$ as a master key of trust authority, set $P_{pub} = sP$. Construct two cryptographic hash functions $H : \{0, 1\}^* \rightarrow Z_q$ and $H_1 : \{0, 1\}^* \rightarrow G_1$. Then the system parameters are : $\{q, P, P_{pub}, G_1, G_2, e, H, H_1\}$.

Extract

Assume that the signer's identity is his ID, we can calculate the public key as $Q_{ID} = H_1(ID)$, and the private key of signer is $S_{ID} = sQ_{ID}$.

Signature

- The signer randomly chooses a number $r \in Z_q^*$, and computers

$R = rP$, then sends R to the receiver.

- A number $a \in Z_q^*$ will be chosen randomly by receiver as a blind factor, then receiver computes $t = e(aP_{pub}, R)$ and $c = H(m, t)$ with his message m, sends blinded c by computing $c' = a^{-1}c$ mod q to signer.
- After receiving c', signer uses his private key S_{ID} to produce the blind signature by computing $S' = c'S_{ID} + rP_{pub}$, and sends the S' to the receiver.
- S' is unblinded by factor a, then the final signature of message m is (S, t, m), where $S = S'a$.

The protocol is showed in Fig.4.1.

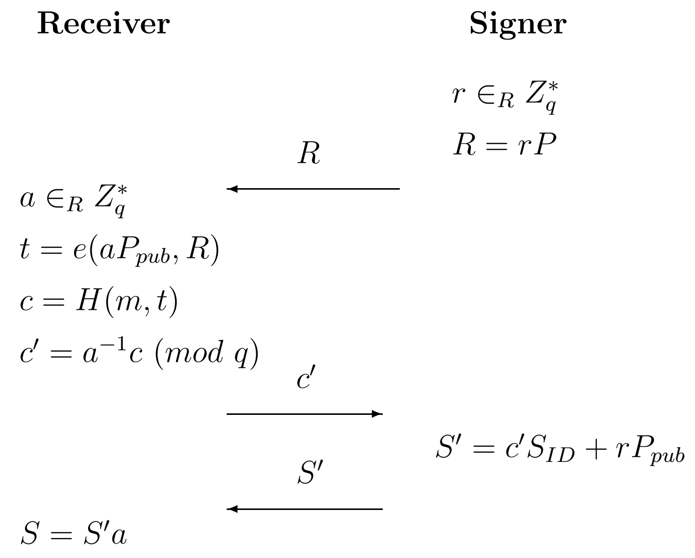

Figure 4.1: ID-based “magic ink” signature protocol

Verification
Receiver can verify whether the signature is valid or not by using signer's public key to check:

$$e(S, P) = e(Q_{ID}, P_{pub})^{H(m,t)}t.$$

Receiver accepts the signature, if the above equation holds.

Tracing
Let $(c^{-1}S)$ identifies a valid signature (m, t, S), and (c', S') can be viewed by the signer during the signature session, so it can be noted as a signature-view invariant. In each signature, we have $c'^{-1}S' = c^{-1}S$, since:

$$c'^{-1}S' = c^{-1}a \times Sa^{-1} = c^{-1}S.$$

From a valid signature (m, t, S), signer can easily calculate $c^{-1}S$, here $c = H(m, t)$. So if any illegal receiver needs to be discovered, signer can compare the value of $c^{-1}S$ with the database of signature-view invariant. If signer can find the same value in the database, the original receiver can be identified.

In the ID-based single signer "magic ink" signature, signer can easily get the signature-view invariant during the signature session to trace the original receiver without any limitation.

4.3 Our Protocols

In our fair e-cash system, we can treat bank as signers, and user as a receiver, during the withdrawal protocol, user first randomly chooses a message m as his e-coin, and gets the valid ID-based distributed "magic ink" signature to his coin from bank, bank assigns n different parties to sign this coin and as the same time stores each part of signature-view variant to their database. During payment protocol, a merchant simply verifies whether the coin is valid or not by checking bank's signature. If the coin is valid, the merchant will deposit it to bank. When bank detects some illegal activities such as blackmailing or money laundering. He can search the database of signature-view invariant to find the corresponding user. Also if bank cooperates with user, he can act coin tracing to calculate the final coin and signature. But because of the use of distributed signature, the revocability of bank is limited, Only under the cooperation of all n parties, bank can get the signature-view invariant. In some previous fair e-cash system scheme, a trust third party(TTP) was used to send the pseudonym in signature put by user during the signature procedure to bank, in order to help bank to make tracing, but our scheme doesn't need the enrollment of the TTP. It obviously reduces the protocol complexity and saves the system resource, as well as enhance the security level.

Since the single signer can't support privacy requirement, so we introduce a threshold scheme to the fair e-cash system. the goal of threshold cryptography is to replace one signer of a bank during withdrawal protocol to a group of signers of bank to share the same secret. We will provide a (n, n) threshold scheme by modifying our previous construction in a single signer case, which means a signer will be replaced by n signers in a way that key generation and signature generation require collaboration of at least n singers of the bank, whilst no subgroup of less than n participants can forge a signature.

We assume during the withdrawal protocol, the valid coin must be signed with the cooperation of n signers of the bank. We set n signers to individually sign the coin through using their own private keys and send them to user through point-to-point communication, and user combines those signatures to an ID-based "magic ink" signature and gets his valid coin. The advantage of ID-based distributed "magic ink" signature is that it can hide the signature-view invariant to each signer of the bank, also it satisfies the original ID-based blind signature requirement. So without the agreement and cooperation of n signers, the coin can't be revoked. The protocol of the fair e-cash system from ID-based distributed "magic ink" signature is described as follow:

Set G_1 as a cyclic additive group and G_2 as a multiplicative group, both of groups have a same prime order q. We view the bilinear group as $e : G_1 \times G_1 \to G_2$.

Computation and Communication

We assume: there are a set of n signers in bank, all of them are polynomial-time randomized Turing Machines. In communication model, we also assume: any user can build point to point communication channel with each signer through a secure channel. An adversary can corrupt up to $n-1$ among the n signers.

Setup

Let P be a generator of G_1, randomly choose a number $s \in Z_q^*$ as a master key of trust party, set $P_{pub} = sP$. Construct two cryptographic hash functions $H : \{0,1\}^* \to Z_q$ and $H_1 : \{0,1\}^* \to G_1$. Then the system parameters are : $\{q, P, P_{pub}, G_1, G_2, e, H, H_1\}$.

Extract

Assume each signer's identity is ID_i. We can express the public key of each signer as: $Q_{IDi} = H_1(ID_i)$, and the private key of signer is $S_{IDi} = sQ_{IDi}$, so the public key of the bank is $Q_{ID} = \sum_{i=1}^{n} Q_{IDi}, i = 1, 2...n$.

Withdrawal Protocol

- n signers obtain a (n, n) secret sharing $(r_1, r_2, \ldots r_n)$ of a randomly chosen number $r \in Z_q^*$ by letting $r = \sum_{i=1}^{n} r_i$, each signer computes $R_i = r_i P$, and sends R_i to user.

- User computers $R = \sum_{i=1}^{n} R_i$, a integer $a \in Z_q^*$ is chosen randomly by user as a blind factor. User computes $t = e(aP_{pub}, R)$ and $c = H(m, t)$ with his coin m , sends blinded c by computing $c' = a^{-1}c \bmod q$ to each signer.

- Each signer individually generates the signature $S_i' = c' S_{IDi} + r_i P_{pub}$, and secretly sends it to receiver.

- After receiving all the signature S_i', user combines those signature to get blinded signature S', where $S' = \sum_{i=1}^{n} S_i' = c' \sum_{i=1}^{n} S_{IDi} + \sum_{i=1}^{n} r_i P_{pub}$. then user unblinds the S' by computing $S = S'a$, so the (S, t, m) will be the valid coin.

  Fig.4.2 shows the withdrawal protocol.

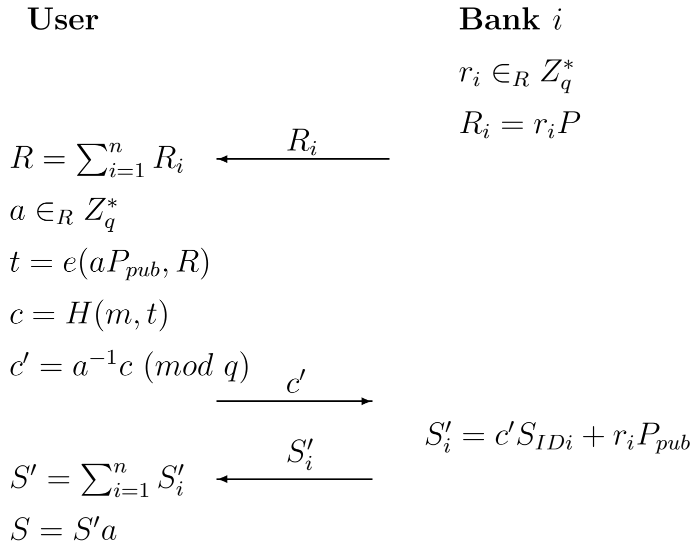

Figure 4.2: Withdrawal protocol

Payment Protocol

After the merchant get the user's payment, he only needs to verify the validity of coin. The verification is similar to the previous verification, Merchant uses public key Q_{ID} of bank to check whether it is a valid coin from equation:

$$e(S, P) = e(Q_{ID}, P_{pub})^{H(m,t)}t$$

If above equation is hold, merchant will accept user's coin.

Deposit Protocol

At the time that merchant tries to deposit his coin to bank, bank firstly should check the validity of coin by verifying the signature of coin. Then bank needs to check for double spending, from his database he can look for whether there exists a same coin. If he find a same coin, he can deny the request for deposit, If the coin has not been spent before, he will store the coin to his database and deposit the money to merchant's account.

Tracing Protocol

Since S' is blind to each signer of bank, and each S'_i is secretly sent to user, so any signer can't know S' without cooperating with another $n-1$ signers of bank. Only n signers of bank work together to compute S' from $S' = \sum_{i=1}^{n} S'_i$, then the signature-view invariant will be revoked. so those cooperation can be controlled by some authority in bank, in order to prevent the misuse of tracing.

User Tracing Protocol

After deposit protocol bank get the coin (S, t, m) and computes $c = H(t, m)$, then get the value of Sc^{-1}, from comparing the value of $S'c'^{-1}$, he can find a equal number, which can refer to the identity of user

Coin Tracing Protocol

After withdrawal, bank can get the value Sc^{-1} which refers to the blackmailed coin. So during deposit protocol, bank can easily find the coin.

4.4 Analysis of Our Protocol

Our analysis is mainly focused on the correctness, blindness, unforgeable security, robustness and comparison and efficiency of ID-based distributed "magic ink" signature, since our fair e-cash system is highly related with this.

4.4.1 Correctness

For the properties of bilinear pairings, we can declare that this is a valid signature; the proof of verification equation is as follow:

$$\begin{aligned}
e(S,P) &= e(S'a,P) = e(\sum_{i=1}^{n} S'_i a, P) \\
&= \prod_{i=1}^{n} e(ac'S_{IDi} + ar_i P_{pub}, P) \\
&= \prod_{i=1}^{n} e(cS_{IDi}, P) \prod_{i=1}^{n} e(ar_i P_{pub}, P) \\
&= e(S_{ID}, P)^c \prod_{i=1}^{n} e(aP_{pub}, P)^{r_i} \\
&= e(sQ_{ID}, P)^c \prod_{i=1}^{n} e(aP_{pub}, r_i P) \\
&= e(sQ_{ID}, P)^c \prod_{i=1}^{n} e(aP_{pub}, R_i) \\
&= e(sQ_{ID}, P)^c e(aP_{pub}, R) = e(Q_{ID}, sP)^c t \\
&= e(Q_{ID}, P_{pub})^{H(m,t)} t
\end{aligned}$$

4.4.2 Blindness Revocability

Under the requirement of protecting legal user's privacy, this scheme basically can achieve blindness, because the coin sent to n signers of the bank will be blinded previously by randomly chosen integer $a \in Z_q^*$ and each signer just signs the blinded cion c', after receiving the blinded signature, the user can unblind this signature by using blind factor a and get the valid signature, but the signer can't find any relationship between S' and S, signer just has a probability of $1/q$ to correctly guess the unblinded signature, so we can say this scheme is blind.

4.4.3 Revocable Anonymity

A valid magic ink signature means that the scheme should be revocable anonymity, this scheme also supports such function, so that in a e-cash system any illegal activities can be traced. each signer receives c' and S_i' during withdrawal protocol, when bank needs to trace the identity of user or coin under legal authority, he can compute the value of Sc^{-1} from the signature (S, t, m), and compare with the value $S'c'{-}1$ from the cooperation of n signers. Since the signature view invariant, tracing mechanism can be easily reach. So the revocable property is maintained. The tracing mechanism of distributed magic ink should be cooperated by n signers, each signer can't get S' by himself. The revocability of bank can be well controlled in our e-cash system.

4.4.4 Unforgeable Security

We consider the following fame: assume that an adversary can cooperate $n-1$ signers without loss of generality. Let the identities of these $n-1$ signer are $Q_{ID_i}, i = 1, 2 \ldots n$. So adversary can get S_{ID_i} to compute S_i'. If he can compute S_{ID_n}, he can forge a valid ID-based distributed

	DMIS	IDDMIS
Number of costs(reciever)	$(2n+1)$**E**+ 4**m**+ 2**I**	1**P**+**M**+2**m**+1**I**+ $(2n-2)$**A**
Number of cost(each signer)	2**E**+ 2**m**+**I**	3**M**+ 1**A**
Private key size(bit)	160bit	161bit
Public key size(bit)	1024bit	161bit
Threshold	(n,t)	(n,n)
Based Problem	DLP	CDHP

Table 4.1: Comparison with Distributed "Magic Ink" Signature

"magic ink" signature. However it is equivalent to solve CDHP in G_1 for computing $sH(ID_n)$ with sP and $H(ID_n)$.

4.4.5 Robustness

If the signature can't pass the verification, there exists some dishonest signers. Since each signer should send his partial signature S_i' to the user, user can check each signature by verifying whether $e(S_i,P) = e(Q_{IDi},P_{pub})^{H(m,t)}e(aP_{pub},R_i)$, here $S_i = S_i'a$. If one of the signatures doesn't pass, we can declare that this signer made some mistake or cheating.

4.4.6 Comparison and Efficiency

Jakobsson first proposed a distributed "magic ink" signature [19] in 1997. The comparison with our proposed scheme is showed in Table.4.1 . We denote:

DMIS the distributed "magic ink" signature[19]

IDDMIS the ID-based distributed "magic ink" signature

M the cost of point multiplication over G_1

A the point addition over G_1

e the cost of weil pairing computation in G_1

m the cost of multiplication over a finite field

E the cost of exponent over a finite field

I the cost of inverse over a finite field

n the number of signers

According to[2, 12], if we let **m** denote other computations, we have following relations:

$$M \approx 700m; A \approx 16m; P \approx 300m; E \approx 800mI \approx 20m$$

From Table 4.1, the total computation costs of each signature can be presented as follows:

$$user\ of\ DMIS = (2n+1)800m + 4m + 40m = 1600nm + 844m$$

$$user\ of\ IDDMIS = 3000m+700m+2m+20m+(2n-2)16m = 3690m+32nm$$

$$signer\ of\ DMIS = 1600m + 3m = 1603m$$

$$signer\ of\ IDDMIS = 2100m + 16m = 2116m$$

First we compare the computation costs of user's side between two schemes. From Table.4.2, we can find that if n, which denotes the number of distributed signers, is not less than 2, the computational costs in user side of our scheme is lower than previous scheme. If the system use a mount of distributed signers, our scheme will be more efficient as the mount of n increases. For example, according to [2], on PIII 1GHz one multiplication over a finite field costs 0.006 milliseconds, when n=20, in previous scheme each user takes 197 milliseconds, when n=20, in previous scheme each user takes 197milliseconds, however our protocol for each user takes 25milliseconds. For mobil user, who has

	DMIS	IDDMIS
n=2	4044m	3754m
n=3	5644m	3786m
...	...	...
n=10	16844m	4010m
n=20	32844m	4330m

Table 4.2: Computation Comparison between user's in DMIS and ID-DMIS

limited computation resource, this advantage will improve convenience of wireless application in e-cash system.

In our protocol, each signer should compute 2116m, in DMIS scheme, each signer should compute 1621m. Since the computation time of multiplication over a finite field is very quick, so 495m more computation takes 2.97 milliseconds.

The advantage of our protocol are described as follows:

- Due to the ID-based signature, $n$signers of bank can directly use their identities such as an e-mail address related with their unique information instead of an arbitrary number. This property simplifies the key distribution and management in our e-cash scheme. Without been certificated by CA, the public keys of bank can be directly sent to users and merchants, and users and merchants don't have to save any certification of public keys of bank, neither take the process to authenticate bank's public keys.

- Bilinear pairings, which is constructed to ID-based signature, reduce public key size. So the users and merchants can save their storage space for public keys. As a tendency of wireless e-payment application, e-cash system also should provide service to mobile user, which has limited communication and computation resource.

The smaller data storage requirement will be helpful.

- In our fair e-cash system, the revocation can be achieved with the involvement of TTP. The TTP's interactions between user and bank increase the additional communication and computation costs, which are not desirable to both bank and user. Also any misuse of tracing by the TTP can't be detected. In our scheme the bank also has the power to perform coin and owner tracing. However the application of tracing is restricted by using (n, n) threshold security sharing.

4.5 Summary

We proposed a fair off-line e-cash system, which is based on ID-based distributed "magic ink" signature, it has the ability to reveal the blind signature give by signer of bank. However revocability limitation also should be considered, so we introduced a (n, n) threshold secret sharing to bank's side by designing (n, n) threshold secret sharing of bank, it means that the valid signature of each signer is anonymous, even it is impossible for less than n signers work together to link the signed coin to original user. Only n signers can reach the revocability. The ID-based signature also simplifies the public key certification and management, and makes the size of public key of signer shorter.

V. Conclusions and Future Works

In this thesis, we studied on a fair off-line e-cash system, first of all we gave an overview of the e-cash system, including its properties and security requirements. Specially we emphasized several reasons of applying a fair off-line e-cash system, which not only protects the privacy of user, but also achieves the requirement of tracing perfect crime in real e-payment applications. Several previous works on fair e-cash systems also were briefly introduced. We mainly suggested two schemes in designing a fair off-line e-cash system, and avoided some disadvantages appeared in related schemes.

We first presented a fair off-line e-cash system with the limited power of TTP, which is normally used in several fair e-cash systems in order to conduct tracing mechanism. Generally user should send his withdrawal to TTP before he withdraws the money from bank, in our protocol, bank first gives the signature on user's coin using the blind signature protocol. Then TTP verifies the validity of the e-coin, and ensures that each e-coin can be traced if required. After that TTP gives his signature on the e-coin, which means he has the traceability of each coin during tracing protocol. So there are two signatures in a coin: The signature of the bank ensures no entity able to forge a coin, and the signature of the trustee ensures each dubious user and coin can be traced. The improvement of our scheme is that the traceability of TTP is controlled. In order to prevent illegal tracing of TTP, The tracing mechanism only can by achieved by the cooperation of bank. The privacy of honest users are protected.

In our second e-cash system without TTP, an ID-based distributed "magic ink" signature is introduced to achieve fairness, which protects legal user's privacy and prevents prefect crime without the help of TTP. ID-based signature simplifies the certification of public key of signer, the certification procedure is skipped, and the storage space also is saved, those advantage will improve user's efficiency, specially for wireless users, who have limited communication and computation resources. The bilinear pairing used to construct ID-based signature also reduces the size of public keys of signers from banks, public key normally should be stored by users and merchants to verify the blind signature from bank, a short length of public key will save uses's storage resource. The fairness of our e-cash system is satisfied by the distributed "magic ink", which gives the user a blind signature on his coin during withdrawal protocol to protect user's privacy, and detects any prefect crime later. The tracing mechanism can be implemented without the help of TTP, However in case of the tracing information are distributed by a set of signers of the bank through a (n, n) threshold secret sharing, The bank's traceability is well controlled. The additional computation and communications of TTP, which is undesired by the user and the bank are skipped, and the misbehavior of tracing is prevented..

In our further works, it is valuable to simulate our protocol to a practical fair e-cash system, and evaluate the efficiency. We also need to enhance our protocol proofs in sense of provable security. A better solution, which preserves all requirements is hopefully to be designed.

References

1. F. Bao and R. Deng, “A New Type of “Magic Ink” Signature towards Transcript-Irrelevant Anonymity Revocation”, *PKC’99*, LNCS 1560, pp.1-11, Springer-Verlag, Berlin Heidelberg 1999.

2. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, “Efficient Algorithms for Pairing-Based Cryptosystems”, *Advances in Cryptology-Crypto’2002*, LNCS 2442, pp.354-368, Springer-Verlag, 2002.

3. D. Boneh and M. Franklin, “Identity-based Encryption from The Weil Pairing”, *Advances in Cryptology-Crypto’2001*, LNCS 2139, PP.213-29, Spring-Verlag, 2001.

4. D. Boneh, B. Lynn, and H. Shacham, “Short Signatures from the Weil Pairing”, *Advances in Cryptology-Asiacrypt 2001*, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

5. E. brickell, P. Gemmell and D. Kravitz. “Trustee-based Tracing Extension to Anonymous Cash and the Marking of Anonymous Change”, *Proc. 6th Annual ACM-SIAM Symposium on Discrete Algorithms(SODA)*, pp.457-466, 1995.

6. J.C. Cha and J.H. Cheon, “An Identity-based Signature from Gap Diffie-Hellman Groups”, *PKC’03*, LNCS 2567, pp. 18-30, Spring-Verlag, 2003.

7. D. Chaum, A. Fiat, M. Naor, ”Untraceable Electronic Cash,” Crypto’88, LNCS 1000, pp.84-95, Springer-Verlag, 1996,.

8. D. Chaum, “Blind Signatures for Untraceable Payments”, *Advanced in Cryptology-Crypto’82*, pp.199-203, 1983.

9. J. Camenisch, U. Maurer, M. Stadle, “Digital Payment System with Passive Anonymity Revocable trustees”, *Computer Security Esorics’96*, LNCS 1146, pp. 33-43, Springer-Verlag, 1996.

10. J. Camenish and M. Stadler, “Efficient Grouop Signatures Schemes for Large Groups”. *Crypto’97*, LNCS1294, pp. 410-424, 1997.

11. G. Davida, Y. Fankel, Y. Tsiounis, and M. Yung, “Anonymity Control in E-cash Systems” *Financial Cryptography’97*, LNCS 1318, pp.1-16, Spring-Verlag, 1997.

12. K. Eisentraeger, K. Lauter, P.L. Montgomery, “An Efficient Procedure to Double and Add Points on an Elliptic Curve,” /em Cryptology ePrint Archive.

13. Y. Frankel, Y. Tsiounis, M. Yung, “Indirect Discourse Proofs: Achieving Efficient Fair Off-line E-cash”, *Advanced in Cryptology-Asiacrypt’96*, LNCS 1163, pp.286-300, Springer-verlag, 1996.

14. G. Frey and H. Rück, “Remark Concerning m-Divisibility and the Discrete Logarithm in The Divisor Class Group of Curves”, *Mathematics of Computation*, 62, pp.865-874, 1994.

15. S. D. Galbraith, K. Harrison, and D. Soldera, “Implementing the Tate Pairing”, *ANTS 2002*, LNCS 2369, pp.324-337, Springer-Verlag, 2002.

16. F. Hess, “Efficient Identity Based Signature Schemes Based on Pairings”, *9th Annual International Workshop SAC’02*, LNCS 2595, pp. 310-324, Spring-Verlag, 2002.

17. A. Joux, “The Weil and Tate Pairing as Building Blocks for Public Key Cryptosystem”, *ANTS 2002*, LNCS 2369, PP.20-32, Springer-verlag, 2002.

18. M. Jackbosson, M. Yung, “Revocable and Versatile Elcetronic Cash”, *3rd ACM Conference on Computer and Communications Security*, ACM press, pp.76-87, 1996.

19. M. Jakobsson and M. Yung, “Distributed Magic Ink Signatures”, *Advances in Cryptology-EUROCRYPT’97*, LNCS 1233, PP.450-464, Spring-Velag, 1997.

20. A. Juel, “Trusten token: Simple and practical anonymous digital coin tracing”, *in FC’99*, LNCS 1648, pp. 29-45, 1999.

21. D. Kügler and H. Vogt, “Marking: A Privacy Protecting Approach Against Blackmailing”, *PKC’2001*, LNCS 1992, pp. 137-152, Spring-Verlag, 2001.

22. D. Kügler and H. Vogt, “Fair Tracing without Trustees”, *Financial Cryptograhpy’2001*, LNCS2339, pp. 136-148, Spring-Verlag, 2001.

23. D. Kügler and H, Vogt, “Auditable Tracing with Unconditional Anonymity”, *WISA’2001*, pp. 108-120. Seoul, Korea, 2001

24. D. Kügler and H, Vogt, “Offline Payments with Auditable Tracing, *Financial Cryptography 2002*, LNCS 2357, pp. 269-281, Springer, 2002.

25. K.S. McCurley, “The Discrete Logarithm Problem”, *Symposia in Applied Mathematics*, Vol. 42, PP. 49-74, American Mathematical Society, 1990.

26. A. Menezes, T. Okamoto, and S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in A Finite Field", *IEEE Transaction on Information Theory*, pp.1639-1646, 1993.

27. Y. Mu, K.Q. Nguyen, and V. Varadharajan, "A Fair Electronic Cash Scheme", *ISEC2001*, LNCS 2040, pp.20-32, Springer-verlag, 2001.

28. K.G. Paterson, "ID-based Signatures from Pairings on Elliptic Curves", *Cryptology ePrint Archive*, available at http://eprint.iacr.org/2002/004/.

29. B. Pftzmann and A.-R. Sadeghi. "Self-escrowed Cash Against User Blackmailing" *Financial Cryptograhpy'2000.* LNCS 1962, pp. 42-52. Spring-Verlag, 2001.

30. A. Shamir, "Identity-based Cryptosystems and Signature Schemes", *Advances in Cryptology-Crypto'84*, LNCS 196, pp.47-53, Springer-Verlag, 1984.

31. B. Schoenmakers, "Basic Security of the ecash Payment System", *State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography,* LNCS 1528, pp. 338-352, Springer-Verlag, 1997

32. B.V. Solms and D. Naccache, "On Blind Signatures and Perfect Crimes", *Computers and security*, 11(6):581-583, 1992.

33. M. Stadler, J.M.Piveteau and J. Camenisch, "Fair Blind Signature", *Eurocrypt'95*, LNCS 921, pp.209-219, Springer-Verlag, 1995.

34. T. Sander, and A. TaShma, "Auditable, Anonymous Electronic Cash", *Crypto '99*, LNCS 1648, pp, 555-572, 1999.

35. J. Traor, “Group Signature and Their Relevance to Privacy-Protecting Off-line Electronic Cash Systems”, *Proc. of ASISP99*, LNCS 1587, pp.228-243, Springer-verlag, 1999.

36. F. Zhang, S. Liu and K. Kim, “ID-based One Round Authenticated Tripartite Key Agreement Protocol with Pairings”, *Cryptology ePrint Archive*, available at http://eprint.iacr.org/2002/122/.

37. F. Zhang and K. Kim, “ID-based Blind Signature and Ring Signature from Pairings”, *Asiacrypt2002*, LNCS 2501, pp.533-547, Springer-verlag, 2002.

38. F. Zhang, F.T. Zhang and Y. Wang, “Fair Electronic Cash Systems with Multiple Banks”, *SEC 2000*, pp.461-470, Kluwer, 2000.

Acknowledgement

I would like to express my sincere gratitude to Prof. Kwangjo Kim, my academic advisor,As a foreign student, I wish to express my gratitude deeply and sincerely, his constant inspiration and encouragement for my research and life in ICU will be remembered by me forever. Specially thanks also goes to Prof. Daeyoung Kim and Prof. C.Pandu Rangan for their generosity and agreeing to serve as committee members of my thesis.

I would like to appreciate all members in CAIS Lab: Hyungki Choi, Kyusuk Han, Zeen Kim, Sangwon Lee, Byunggon Kim, Songwon Lee, Hwasun Chang, Jaehyk Park, Soogil Choi, Chuljoon Choi, Joongman Kim, Sungjoon Min, Jeongkyu Yang, Seokkyu Kang, Vo Duc Liem, Dang Nguyen Duc, Divyan, and my native friends Dr. Zhang Fang Guo, Dr. Cheng Xiao Feng and Wang Ping for their kindly advice and help during my study and life in ICU korea.

I also would like to give my thanks to Jeongbae Park, and Jinki Hong of CN Lab, and Dongwon Lee of DBLab for their great help.

In addition, I am also grateful our former lab members: Gookwhan An, ByoungCheon Lee, Manho Lee, Jinho Kim, Jaegwan Park, Myungsun Kim, Jongseong Kim, Wooseok Ham, and Hyunrok Lee for their encouragement and advice.

My sincerely thanks also goes to my parents, my uncle and aunt for their devotion and support, specially I would like to thank my cousin Ms. Min Sha, and her husband Mr. James Wang, their unconditional encouragement and trust, happy smile, and unbounded optimism.

Finally, I will never forget my life in ICU Korea, It filled up my poor knowledge and made me a grown-up person.

Curriculum Vitae

Name : Yan Xie

Date of Birth : Sep. 09. 1974

Sex : Male

Nationality : Chinese

Education

2001.5–2003.8	Cryptology and Information Security Engineering Information and Communications University (M.S.)

Career

2001.6–2002.7	Graduate Research Assistant Development of Electronic Voting System for World-Cup 2002 Information Research center for Information Security, ICU

Publications

(1) 2002.11 Yan Xie, Fangguo Zhang and Kwangjo Kim, New Revocable E-cash based on the limited power of TTP, 2002 *Information Security Conference*, pp. 266-269, Korea.

(2) 2003.2 Yan Xie, Fangguo Zhang, Kwangjo Kim, ID-Base Distributed "Magic Ink" Signature, 2002 *Workshop of Korea Institute of Information Security* , pp.19-23, 2002 Korea.

(3) 2003.5 Yan Xie, Fangguo Zhang, Kwangjo Kim, ID-Base Distributed "Magic Ink" Signature From Pairings, to be appeared in *ICICS2003*

(4) 2002.8 Wooseok Ham, Hyungki Choi, Yan Xie, Misung Lee and Kwangjo Kim, Secure One-way Mobile Payment System Keeping Low Computation in Mobile Devices, *The 3rd International Workshop on Information Security Applications*, pp.287-301, Jeju, Korea