A Thesis for the Degree of Master

Design of Fair Tracing E-cash System based on Blind Signature

ByeongKon Kim

School of Engineering

Information and Communications University

2004

Design of Fair Tracing E-cash System based on Blind Signature

Design of Fair Tracing E-cash System based on Blind Signature

Advisor : Professor Kwangjo Kim

by

ByeongKon Kim
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
Dec. 29. 2003
Approved by

(signed)

Professor Kwangjo Kim
Major Advisor

Design of Fair Tracing E-cash System based on Blind Signature

ByeongKon Kim

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

Dec. 29. 2003

Approved:

Chairman of the Committee
Kwangjo Kim, Professor
School of Engineering

Committee Member
Jae Choon Cha, Assistant Professor
School of Engineering

Committee Member
Soran Ine, Ph.D
NITZ Corp.

M.S. ByeongKon Kim
2002019

Design of Fair Tracing E-cash System based on Blind Signature

School of Engineering, 2004, 38p.
Major Advisor : Prof. Kwangjo Kim.
Text in English

Abstract

Many researches on the electronic cash (e-cash) system have been carried out with proliferation of electronic commerce. But there is no one outstanding system satisfying all requirements of e-cash efficiently, and researchers try to cover the requirements partially or totally. One of the requirements is *fair tracing* problem.

In e-cash system, a customer withdraws electronic *coins* from bank and pays the coins to a merchant in the off-line manner. Finally, the merchant deposits the paid coins to the bank. To protect the privacy of customer, each payment should be anonymous and it can be achieved by blind signature. However *unconditional anonymity* may be misused for untraceable blackmailing of customer, which is also called *perfect crime*. Furthermore, unconditional anonymity makes ease money laundering, illegal purchase, and bank robbery.

We propose a tracing scheme of e-cash which has not only fair tracing ability but also lower computational complexity for comparisons. Many other protocols allow *optimistic* fair tracing which means that illegal tracing can be found after deposits in a bank. But in this scheme, illegal tracing done by bank is impossible. We propose a marking mechanism based on an Okamoto-Schnorr blind signature and Verifiable Secret Sharing scheme.

Besides, for double spending prevention of e-cash, we adopted Schnorr's one-time signature scheme. If we only consider the anonymity problem, the system will be exposed by double spending threat. So, we are trying to solve this two problem simultaneously.

Finally, we will consider a variant of this scheme and compare it with other protocol.

Contents

List of Tables

List of Figures

List of Abbreviations

DB Data Base

DSA Digital Signature Algorithm

e-commerce Electronic Commerce

e-cash Electronic Cash

SSS Secret Sharing Scheme

TTP Trusted Third Party

VSS Verifiable Secret Sharing

List of Notations

$H()$ Collision-resistant one-way hash function

m message

P_k Public Key

S_k Secret Key

$Sig_{user}()$ Signature of *user*

T_v Expiration date of validity time

x, x_M, x' secret mark(key) of undeniable signature

$\mathbb{Z}_p$ integers modulo p

$\mathbb{Z}_p^*$ a group under multiplication modulo p

$a|b$ a divides b

$||$ Concatenation of message

I. Introduction

There have been many electronic cash(e-cash) protocols proposed with rapid improvement of information technologies and widespread diffusion of communication networks. A secure and efficient e-cash system plays an important role to support e-commerce safely as a trustful payment over the Internet.

In e-cash system, there are three basic entities, *customer*, *bank* and *merchant*. And there are also three activities, *withdrawal*, *payment* and *deposit*. A customer withdraws electronic *coins* from bank and pays the coins to a merchant in the off-line or on-line manner. Finally, the merchant deposits the paid coins to a bank. In this process, there are many requirements which are anonymity, anonymous revocation, double spending prevention, off-line usage, transferability, divisibility and so on.

1.1 Fair Tracing

To protect the privacy of customers, each payment should be anonymous and it can be achieved by blind signature. However von Solms and Naccache [vSN92] have shown that *unconditional anonymity* may be misused for untraceable blackmailing of customers, which is also called *perfect crime*. Furthermore, unconditional anonymity makes ease money laundering, illegal purchase, and bank robbery. Due to these anonymity related problems, tracing of payment systems with *revokable anonymity* [SPC95, DFTY97] have been invented.

There are two types of tracing mechanism: Coin tracing and Owner tracing. This mechanism of e-cash is better feature compared with physical cash. Because coin and owner tracing is almost impossible in real world. But these two tracing mechanisms have one common problem, called the *fair-tracing-problem*: No one is able to control the legal usage of tracing, leading to the possibility of illegal tracing.

Kügler and Vogt proposed a new kind of tracing mechanism [KV01] which guarantees stronger privacy than any other known approaches, although their fair coin tracing can be carried out by the bank without any help of trusted third parties. They called their *withdrawal-based* scheme as *optimistic fair tracing*, which means that the decision whether the coins should be traceable or not must be made at their withdrawal. This protocol cannot prevent illegal tracing, but can detect it afterwards by the traced person. If it turns out to be illegal, then he can prove it to a judge and the tracer(bank) will be prosecuted.

However, we propose a withdrawal-based real fair tracing protocol and show that it has an enhanced computational complexity.

1.2 Double Spending Prevention

Off-line digital cash systems are more preferable than on-line cash systems, since in off-line digital cash systems banks do not need to be involved in payment process. There have always been two major concerns for off-line systems : double-spending and customer's privacy. In particular, double-spending is a serious threat for off-line schemes [NMV97].

In on-line e-cash system, double spending prevention mechanism can be achieved easily. While spending, the coins are securely transferred to the merchant. The merchant verifies the coins by sending them to the bank. After ascertaining that the coins are not double spent, the bank credits the merchant's account and the coin is destroyed. If the coin is double spent, the bank sends an appropriate message to abort the transaction[AM00].

In this thesis, our protocol focused on anonymity and its revocation functions. Basically, our coin stream is blinded and anonymous. So, using only this coin stream, bank cannot differentiate each coins without revealing it's anonymity. So, it is hard for bank to prevent double spending. Therefore, we are trying to suggest a supplementary stream for this function. Until now, our protocol is not restricted on-line system. So, this double spending prevention mechanism can be used in off-line system also.

1.3 Our Contribution

Most of works in fair tracing scheme of e-cash introduced a TTP to cooperate with a bank during tracing protocol to detect perfect crime. But it also increases extra computation and communication costs, and the misuse of tracing is difficult to be detected or prevented.

In our protocol, we suggest a fair tracing mechanism for e-cash without TTP. And we can achieve perfect(not optimistic) fair tracing based on Okamoto-Schnorr Blind Signature [Oka92], Chaum-van Antwerpen undeniable signature [Cha90] and Verifiable Secret Sharing(VSS) Scheme. Besides, the number of comparison and data storage are much reduced.

On the other hand, our protocol also gives the double spending prevention mechanism using Schnor's one-time signature. Even in off-line e-cash system, this mechanism will be worked. And this is not hurt the anonymity and tracing mechanism.

Finally, we show that our protocol can adopt TTP, and we can transfer this marking mechanism to other agents or entities.

1.4 Organization of Thesis

The rest of this paper is organized as follows: We introduce some e-cash system requirements, relative basic cryptographic primitives in Section II. In Section III, we will analyze a fair tracing scheme and check it's drawbacks. We explain our new protocol and it's variant in Section IV, and analyze the properties of our payment system in Section V. Besides, we will compare it with other recent protocol also. Finally, we will end with concluding remarks.

II. Preliminaries

2.1 E-cash system

2.1.1 Overview

An e-cash system is a set of parties with their interactions, exchanging money and goods. A typical e-cash system has three parties :

- **Customer** : purchases goods or services from merchant using e-cash.
- **Merchant** : sells goods or services to customer, and deposits e-cash to bank.
- **Bank** : issues e-cash and maintains bank account for customers and merchants.

And there are also three activities, *withdrawal*, *payment* and *deposit*. A customer withdraws electronic coins from bank and pays the coins to a merchant. Finally, the merchant deposits the paid coins to the bank.

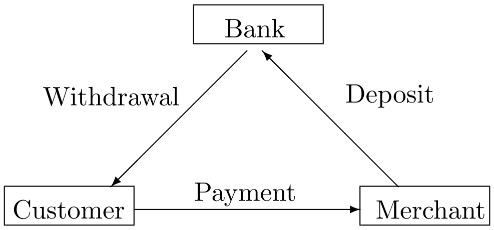


Figure 2.1: Basic model of e-cash system

2.1.2 Cryptographic Requirements

An ideal e-cash system must satisfy the following properties :

- Unforgeability : the valid e-cash cannot forged.
- Anonymity : anyone cannot trace e-cash owner and cannot know what the customer bought.
- Anonymous revocation : legal coin or owner tracing is possible to prevent crimes.
- Double spending prevention : the same e-cash must not allowed to spend twice.
- Off-line : when a customer gives e-cash to a merchant, it is not need to connect to the bank on-line.
- Transferability : when a customer receives an e-cash in a transaction, he may spend it without depositing the coin first and getting a new e-cash issued from bank.
- Divisibility : we can divide money into arbitrary part/fractions.

Some of these requirements is not absolute condition for use some kind of e-cash. For example, unforgeability and double spent prevention are essential conditions, but off-line is not.

Depending on the payment method in e-commerce, the requirements are changed. For example, credit-based electronic money, anonymity is not allowed.

2.1.3 Anonymity Problem

In 1982, Chaum [Cha82] showed how to build an anonymous electronic cash system by devising blind signature schemes. Chaum's scheme is provably anonymous: even an all powerful agent that collaborates with the bank and any coalition of the customers can not link payments to withdrawals, i.e. customers enjoy *unconditional anonymity.* In 1992 von Solms and Naccache [vSN92] discovered a serious attack on Chaum's payment system. Blackmailers could commit a perfect blackmailing crime by using anonymous communication channels and anonymous e-cash. Following that, further concerns were raised, e.g, it was argued that the ability to move money around anonymously at the speed of light may facilitate money laundering activities and tax evasion.

Due to these anonymity problems, e-cash with *revocable anonymity* has been requested by governments and banks, and tracing methods have been invented, where the withdrawal and the deposit of coins can linked by two complementary tracing mechanisms [SPC95]:

Coin tracing : Is the withdrawn coin is deposited?

Owner tracing : Who is the withdrawer of this deposited coin?

Tracing mechanism of e-cash can be achieved effectively by introducing trusted third party [DFTY97]. But that is a big assumption to realize of e-cash system, and that causes additional costs. To make matters worse, the achieved level of anonymity is uncertain and any misuse of tracing by TTP can not be detected.

Recent one example of them is escrowed cash system. In this system, payment transactions look anonymous from the outside (to customers, merchants, banks), while Trustees are able to revoke the anonymity of each individual payment transaction. But in this scheme, criminals may still be able to hide their suspicious activities in an escrowed system in a way that is hard to detect. Sander and Ta-Shma [ST99] argue that escrowed cash is not a natural solution to some of the major attacks on electronic cash systems (blackmailing and bank robbery) that are caused not by the anonymity feature but rather stem from the fact that most anonymous cash systems are implemented using signature based schemes.

Therefore, recent approaches are not use TTP tracing [ST99a, PS01]. But they only protect against blackmailing and lack support for coin and owner tracing. And these payment systems require the bank to be on-line at payment. Kügler and Vogt [KV01] proposed off-line payment system without TTP using marking mechanism. X. Chen et.al tried an off-line scheme using group blind signature [CZW03].

In this thesis, we analyze the Kügler's mechanism and propose a true fair tracing mechanism of e-cash. Fair tracing means that legal tracing is always possible, but illegal tracing is inhibited. In here, if the tracing has been permitted by judge or withdrawer(customer), then that tracing is legal, otherwise illegal.

2.2 Digital Signature

Digital signature is an electronic version of paper signature. One classification of them is signature with message appendix and signature with message recovery. Both cases, we can find out the original message which is associated with an originating entity. When a dispute arises whether a party signed on a document, a mediator can resolve the matter fairly verifying it without accessing secret information of the signer.

Characteristics of digital signature are unforgeability, non-repudiation, unalterable, not reusable, authentication of a signer and so on. And it mainly used one-way hash function. So, Many applications in information security, like the certificate of public keys, are adopting this technique to support desired security properties.

Digital signature schemes have several forms (blind, undeniable, proxy, one-time, etc) and each form addresses different goals. We can apply these signature variants according to circumstances to satisfy the requirements of cryptographic applications. Out of several digital signature schemes, blind signature schemes have been widely employed in e-commerce area.

2.3 Okamoto-Schnorr Blind Signature

Chaum [Cha82] proposed the notion of *blind digital signatures* as a key tool for constructing various anonymous electronic cash instruments. Informally, a blind digital signature scheme may be thought of as an abstract game between a customer and a bank. A customer has a secret document for which she needs to get the signature from a bank. She should be able to obtain this signature without revealing to the bank anything about her document except its length. On the other hand, the security of the signature scheme should guarantee that it is difficult for the customer to forge a signature of any additional document, even after getting from the bank a number of blind signatures. Blind/untraceable signatures have attracted considerable attention in the literature, and are used in many proposed e-cash systems.

Let's assume that the sender A(the customer) does not want the signer B(the bank) to be capable of associating a postiori message m and a signature $Sig_B(m)$ to a specific instance of the protocol. This may be important in electronic cash applications where a message m might represent a monetary value which A can spend. When m and $S_B(m)$ are presented to B for payment, B is unable to deduce which party was originally given the signed value. This allows A to remain anonymous so that spending patterns cannot be monitored.

A blind signature protocol required the following components [MOV96]:

1. A digital signature mechanism for signer B. $Sig_B(x)$ denotes the

signature of B on x.

2. Function f and g (known only to the sender) such that $g(Sig_B(f(m))) = Sig_B(m)$. f is called a *blinding function*, g an *unblinding function*, and $f(m)$ a *blinded message*.

Property 2 places many restrictions on the choice of Sig_B and g.

Okamoto [Oka92] suggested a blind signature scheme in Crypto'92 which is based on Schnorr signature scheme and DSA.

p and q are two large primes such that $q|(p-1)$.

g_1 and g_2 are elements of $\mathbb{Z}_p^*$ of order q.

$(s_1, s_2) \in_{\mathcal{R}} \mathbb{Z}_q$ is the private key of the bank(*Signer*) for blind signature.

$y = g_1^{s_1} g_2^{s_2} \mod p$ is the main element of bank's public key for blind signature. So, public key is (p, q, g_1, g_2, y).

Step 1 Bank(signer) picks random numbers $k_1, k_2 \in_{\mathcal{R}} \mathbb{Z}_q$, computes $x = g_1^{k_1} g_2^{k_2} \mod p$, and sends x to Customer.

Step 2 Customer picks random numbers $\beta, \gamma, \delta \in_{\mathcal{R}} \mathbb{Z}_q$, and computes
$\alpha = x g_1^{\beta} g_2^{\gamma} y^{\delta} \mod p$,
$e = H(m, \alpha) - \delta \mod q$
Customer sends e to the Bank. Here, m is a message to be signed.

Step 3 Bank compute (S_1, S_2) such that $S_1 = k_1 - es_1 \mod q$, and $S_2 = k_2 - es_2 \mod q$, and sends (S_1, S_2) to Customer.

Step 4 Customer compute $\rho = S_1 + \beta \mod q$, $\sigma = S_2 + \gamma \mod q$. (α, ρ, σ) is bank's signature of message m.

The verification equation of signature is

$$\begin{aligned}
\alpha &\overset{?}{=} g_1^{\rho} g_2^{\sigma} y^{H(m,\alpha)} \mod p \\
&= g_1^{S_1+\beta} g_2^{S_2+\gamma} y^{e+\delta} \mod p \\
&= (g_1^{S_1} g_2^{S_2} y^{e})(g_1^{\beta} g_2^{\gamma} y^{\delta}) \mod p \\
&= (g_1^{S_1} g_2^{S_2} y^{e})(\alpha/x) \mod p \\
&= (g_1^{k_1-es_1} g_2^{k_2-es_2} y^{e})(\alpha/x) \mod p \\
&= (g_1^{k_1} g_2^{k_2})(g_1^{-es_1} g_2^{-es_2} y^{e})(\alpha/x) \mod p \\
&= (x)((g_1^{s_1} g_2^{s_2})^{-e} y^{e})(\alpha/x) \mod p \\
&= x(y^{-e} y^{e})(\alpha/x) \mod p \\
&= x(\alpha/x) \mod p \\
&= \alpha \mod p.
\end{aligned}$$

2.4 Schnorr's One-time Signature

The security of Schnorr's signature scheme [Sch91] depends on the difficulty of calculating discrete logarithms. Users in the system can share a random number g and two prime numbers, p and q such that $q|(p-1)$, $q \neq 1$ and $g^q \equiv 1 \mod p$.

To generate a particular pair of private/public key, a customer(say, Alice) chooses a random number S_k as her private key, $0 < S_k < q$. customer then computes her public key P_k as

$$P_k = g^{-S_k} \mod p.$$

To sign a message m, Alice picks a random number $r \in_{\mathcal{R}} \mathbb{Z}_q^*$ and does the following computations:

$$\begin{aligned} x &= g^r \mod p \\ c &= H(m||x) \\ y &= (r + cS_k) \mod q \end{aligned}$$

The signature on the message m is the pair (c, y). To verify the signature, Bob checks

$$\begin{aligned} x &\overset{?}{=} g^y P_k^c \mod p \\ &= g^{(r+cS_k)}(g^{-S_k})^c \mod p \\ &= g^r \mod p \end{aligned}$$

and tests if c is equal to $H(m||x)$. If the test is OK, the signature is valid.

The value r must be treated as *on-time number*. It must not be used more than once to generate different signatures. If Alice has used r to sign two different messages m and m', then one has two signatures (c, y) and (c', y'). With there two signatures, one can compute Alice's private key S_k as follows:

$$\begin{aligned} S_k &= \frac{y - y'}{c - c'} \\ &= \frac{(r + cS_k) - (r + c'S_k)}{c - c'} \mod q \end{aligned}$$

Schnorr's scheme allows most of the computation for signature generation to be completed independent of the message being signed.

2.5 Verifiable Secret Sharing

Secret sharing schemes(SSS) were discovered independently by Blakley [Bla79] and Shamir [Sha79]. The motivation for secret sharing is secure key management. In some situations, there is usually one secret key that provides access to many important files. If such a key is lost (e.g., the person who knows the key becomes unavailable, or the computer which stores the key is destroyed), then all the important files become inaccessible. The basic idea in secret sharing is to divide the secret key into pieces and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key.

The general model for secret sharing is called an k-out-of-n scheme (or (k, n)-threshold scheme) for integers k, n. In the scheme, there is a dealer(or sender) and n participants. The dealer divides the secret into n parts and gives each participant one part so that any k parts can be put together to recover the secret, but any $k-1$ parts reveal no information about the secret. The pieces are usually called shares or shadows. Different choices for the values of k and n reflect the tradeoff between security and reliability. A secret sharing scheme is perfect if any group of at most $k-1$ participants (insiders) has no advantage in guessing the secret over the outsiders.

SSS is based on Lagrange interpolation. A trusted dealer uses the secret s to construct a $k-1$ degree polynomial $f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1x + a_0$. with $a_0 = s$ and $f(0) = s$. The rest of coefficients are picked at random from $\mathbb{Z}_q$, where q is a prime greater than s.

Then the dealer gives every party in the scheme a distinct point on the polynomial, except the point at 0 (Usually, gives $f(j)$ to customer j). k of those parties together can recover the secret, since k points uniquely identify a $k-1$ degree polynomial. Using Lagrange interpolation method, $s = f(0)$ can be recovered easily.

Good things about this scheme are efficient, security under no assumption and dealer can add new customers to the scheme. But this scheme needs trusted dealer and cannot verify correctness of shares.

Verifiable secret sharing(VSS) intends to fix these problems of Shamir's scheme. Feldman's scheme[Feld87] extends Shamir's by adding a public verifier function, and many other variations of VSS has been proposed. We use a simple one of them [OA97].

1. Let s be a secret value, k be a threshold, and $j(= 1, 2, \cdots, n)$ be the customer of secret sharing.
2. *Dealer* chooses a random polynomial $f(x) \equiv s + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \pmod q$.
3. *Dealer* distributes $f(j)$ to each customer j.
4. *Dealer* chooses p such that $q|(p-1)$, and generator $g \in_{\mathcal{R}} \mathbb{Z}_p^*$ of order q. And he also calculates
$$\begin{aligned} c_0 &= g^s \mod p \\ c_1 &= g^{a_1} \mod p \\ &\cdots \\ c_{k-1} &= g^{a_{k-1}} \mod p \end{aligned}$$
5. *Dealer* distributes $p, g, c_0, c_1, \cdots, c_{k-1}$ to all j.
6. User j can verify whether the distribution was well performed or not.
$$\begin{aligned} g^{f(j)} &\overset{?}{=} c_0 c_1^j c_2^{j^2} \cdots c_{k-1}^{j^{k-1}} \\ &= g^s g^{a_1 j} g^{a_2 j^2} \cdots g^{a_{k-1} j^{k-1}} \\ &= g^{s + a_1 j + a_2 j^2 + \cdots + a_{k-1} j^{k-1}} \end{aligned}$$
7. User j can recover secret s from $f(j)$ by using Lagrange interpolation.

III. Analysis of KV- Fair Tracing Scheme

3.1 KV-Scheme

Kügler and Vogt [KV01] proposed an e-cash tracing mechanism which used marking mechanism based on a variant of an Okamoto-Schnorr Blind Signature in combination with a Chaum-van Antwerpen undeniable signature [Cha90]. In this scheme, The truth of e-cash is guaranteed by blind signature. But the anonymity and traceability is obtained using undeniable signature. In other words, undeniable signature's secret key is used for marking.

p and q are large primes such that $q|(p-1)$.

g_1, g_2, and g_3 are elements of $\mathbb{Z}_p^*$ of order q.

$(s_1, s_2) \in_{\mathcal{R}} \mathbb{Z}_q$ is the private key of the bank for blind signature.

$v = g_1^{s_1} g_2^{s_2} \mod p$ is the main element of bank's public key for blind signature. So, public key is (p, q, g_1, g_2, v).

$x \in_{\mathcal{R}} \mathbb{Z}_q$ is the private key of the bank for undeniable signature.

$y = g_3^x \mod p$ is the public key of the bank for undeniable signature.

1. Once per withdrawal, *Bank* selects $r \in_{\mathcal{R}} \mathbb{Z}_q^*$, and makes a new random generator $\alpha = g_2^r \mod p$, undeniable signature $\omega = \alpha^x \mod p$. Then send α and ω to Customer.

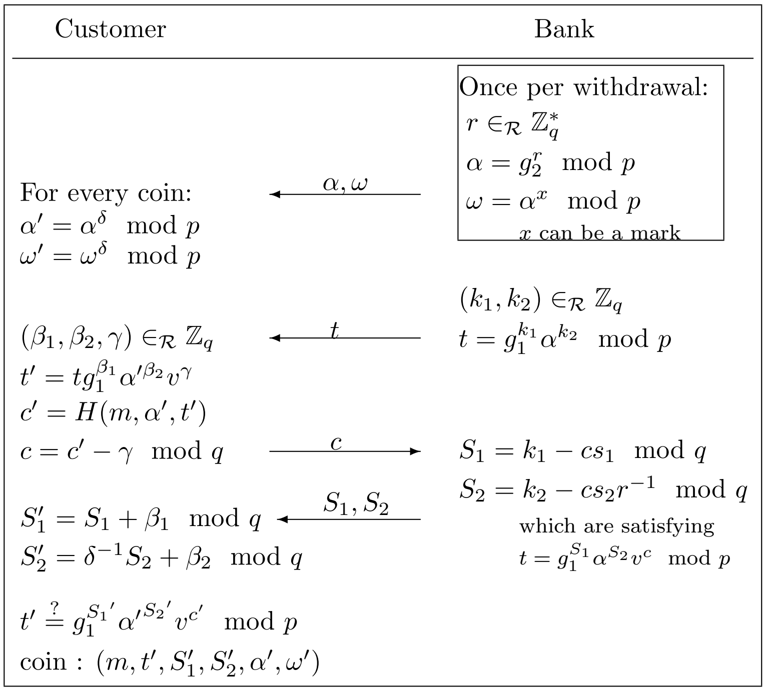

Customer
Bank
Once per withdrawal:
$r \in_{\mathcal{R}} \mathbb{Z}_q^*$
$\alpha = g_2^r \mod p$
$\omega = \alpha^x \mod p$
x can be a mark
α, ω
For every coin:
$\alpha' = \alpha^\delta \mod p$
$\omega' = \omega^\delta \mod p$
$(k_1, k_2) \in_{\mathcal{R}} \mathbb{Z}_q$
$t = g_1^{k_1} \alpha^{k_2} \mod p$
t
$(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$
$t' = t g_1^{\beta_1} \alpha'^{\beta_2} v^\gamma$
$c' = H(m, \alpha', t')$
$c = c' - \gamma \mod q$
c
$S_1 = k_1 - cs_1 \mod q$
$S_2 = k_2 - cs_2 r^{-1} \mod q$
which are satisfying
$t = g_1^{S_1} \alpha^{S_2} v^c \mod p$
S_1, S_2
$S_1' = S_1 + \beta_1 \mod q$
$S_2' = \delta^{-1} S_2 + \beta_2 \mod q$
$t' \overset{?}{=} g_1^{S_1'} \alpha'^{S_2'} v^{c'} \mod p$
coin : $(m, t', S_1', S_2', \alpha', \omega')$

Figure 3.1: KV-scheme of fair tracing

2. *Customer* blinds the value α and ω. For every coin, he selects $\delta \in_{\mathcal{R}} \mathbb{Z}_q^*$ and calculates

$$\begin{aligned} \alpha' &= \alpha^\delta \mod p \\ \omega' &= \omega^\delta = \alpha^{x\delta} = \alpha'^x \mod p \end{aligned}$$

3. Okamoto-Schnorr Blind Signature is started with the value g_1 and α. *Bank* selects $(k_1, k_2) \in_{\mathcal{R}} \mathbb{Z}_q$ and sends $t = g_1^{k_1} \alpha^{k_2} \mod p$ to *Customer*.

4. *Customer* chooses $(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$ and calculates $t' = t g_1^{\beta_1} \alpha'^{\beta_2} v^\gamma \mod p$ where v is the public key of the bank for blind signature. He also calculates $c' = H(m, \alpha', t')$ and sends $c = c' - \gamma \mod q$ to the *Bank*.

5. *Bank* calculates $S_1 = k_1 - cs_1 \mod q$, $S_2 = k_2 - cs_2 r^{-1} \mod q$ which satisfies $t = g_1^{S_1} \alpha^{S_2} v^c \mod p$. And *Bank* sends them to *Customer*.

6. *Customer* calculates

$$\begin{aligned} S_1' &= S_1 + \beta_1 \mod q \\ S_2' &= \delta^{-1} S_2 + \beta_2 \mod q \end{aligned}$$

7. Anyone can verify the blind signature by comparing t' and $g_1^{S_1{}'} \alpha'^{S_2{}'} v^{c'}$ mod p.

8. coin: $(m, t', S_1', S_2', \alpha', \omega')$.

3.2 Analysis

3.2.1 Tracing Capabilities

If the bank decides to issue marked coins, it simply chooses and stores a random undeniable signature key x_M, which can be used instead of x to compute the certificate $\omega = \alpha^{x_M} \mod p$. This situation can be made by request of customer or lawyer.

When a coin being deposited, such a marking will be detected, as the verification process will fail because of the wrong key. In this case, the bank tests $\omega' \overset{?}{=} \alpha'^{x_M} \mod p$ for all stored marking keys x_M.

But if the customer tries to check whether his coin has been traced or not, he must request for the bank to publish all marking keys x_M in audit phase. If he finds that marking key of his coin is neither x nor x_M, he can argue that his coin is traced illegally. But if the marking key is one of the x_M list, then he requests the proper permission of judge, who is responsible for this tracing.
(ex : $Sig_{judge}(y_M, customerID, coin\ generation)$, where $y_M = g_3{}^{x_M}$)

3.2.2 Weak Points

One of the drawbacks of this KV-scheme is that it needs too much additional information in legal coin tracing. Because marking has to be authorized by a judge, and the bank has to save all marking keys and certifications of judge. In audit phase, the bank has to publish all marking keys and unique undeniable signature key x. Therefore, for legal tracing, bank has to save all marking key list and judge's certifications as much as the number of suspected coins.

Other weakness is that customer needs too much computational power to check his coin. Because customer has to compare all x, x_M with x' using $\omega = \alpha'^{x'} \mod p$. If he cannot find any matched x or x_M, he can argue that the coin was illegally traced. So, customer has to have enough computing power for that operations.

Besides, when a customer try to do this operations, revealing all marking key lists will make another security problem. Customer will try to check using his computer. So, the bank must give the lists to the customer. In this case, the customer will know the all marking keys and can transfer the key lists to other suspected customers. And the criminals can check his coins in withdrawal stage. After all, legal tracing is impossible if the marking key was revealed.

The most important weak point is that this fair tracing is *optimistic*, which means that illegal tracing is possible, but later it can be found and prosecuted. Therefore, in this e-cash system, if the coin is not marked, then customer has the merits of perfects anonymity. But if the customer cannot trust his coin, he have to prove the illegal tracing by himself. If the most of customer don't trust the bank, they will request audit step to verify legal tracing and much computational power will be need. So, this protocol has some ideal assumptions in this case.

IV. Proposed Scheme

In this section we describe a protocol which combines VSS, Schnorr's one-time signature and Okamoto-Schnorr blind signature in order to make a more practical e-cash system.

4.1 Main Idea

We consider 3-parties, *customer*, *merchant* and *bank*. Among them, customer will make a mark x and undeniable signature $\omega = \alpha^x \mod p$. The secret value (mark x) will be shared by bank and merchant using VSS.

At first, bank cannot know the secret value, but she can get confidence that the shared-secret value is true. Later, customer gives the coin to merchant with the secret value.

Bank cannot trace coin by himself. This means that illegal coin tracing is impossible. But any two parties can cooperate to reveal the secret value x under the permission of lawyer. This means that legal coin tracing is possible. Therefore, bank and merchant can trace the coin for preventing customer's crime. Furthermore, bank and customer can trace the coin to block blackmailing and kidnapping.

Revealing of modified undeniable signature has no impact on Okamoto-Schnorr blind signature. Hence, even though the mark x is not given by the bank, the truth of the coin will be conserved by blind signature.

Finally, we use one-time signature to prevent coin double spending in payment stage.

4.2 Protocol

4.2.1 Notations

p and q are two large primes such that $q|(p-1)$.

g, g_1 and g_2 are elements of $\mathbb{Z}_p^*$ of order q.

$(s_1, s_2) \in_{\mathcal{R}} \mathbb{Z}_q$ is the blind signature private key of the bank.

$v = g_1^{s_1} g_2^{s_2} \mod p$ is the main element of bank's public key for blind signature. So, public key is (p, q, g_1, g_2, v).

$x \in_{\mathcal{R}} \mathbb{Z}_q$ is a secret mark.

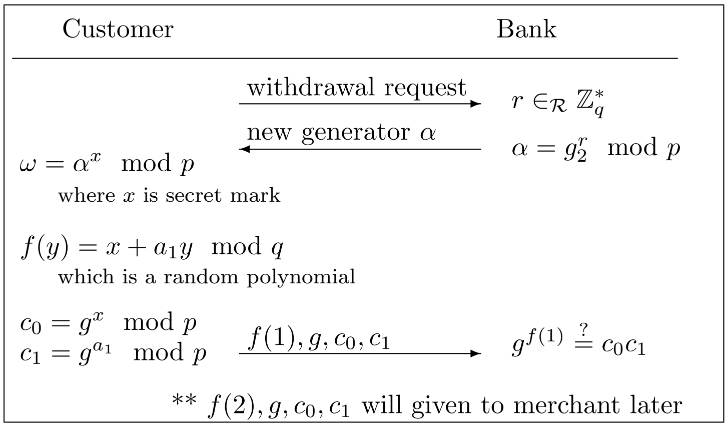
S_k is the secret key of Customer, $0 < S_k < q$.

P_k is the public key of Customer, $P_k = g^{-S_k} \mod p$.

4.2.2 Initial Stage

Customer will make a secret mark and distribute it partially. When the bank received the distributed values, she checks the correctness of the shared values. If the customer(withdrawer) is suspected as criminal, then she will save this shared values with the customer's ID for tracing. Otherwise she will not save them.

1. *Customer* requests coin withdrawal to the *Bank*.
2. *Bank* selects random number $r \in_{\mathcal{R}} \mathbb{Z}_q^*$, makes a new generator $\alpha = g_2^r \mod p$, and sends it to the the *Customer*.
3. *Customer* chooses a random number x as a secret mark and calculate $\omega = \alpha^x \mod p$.



Customer
Bank
withdrawal request
$r \in_{\mathcal{R}} \mathbb{Z}_q^*$
new generator α
$\alpha = g_2^r \mod p$
$\omega = \alpha^x \mod p$
where x is secret mark
$f(y) = x + a_1 y \mod q$
which is a random polynomial
$c_0 = g^x \mod p$
$c_1 = g^{a_1} \mod p$
$f(1), g, c_0, c_1$
$g^{f(1)} \overset{?}{=} c_0 c_1$
** $f(2), g, c_0, c_1$ will given to merchant later

Figure 4.1: Initial stage

4. *Customer* selects a random polynomial $f(y) = x + a_1 y \mod q$ and calculate $c_0 = g^x \mod p$, $c_1 = g^{a_1} \mod p$.

5. *Customer* sends $f(1), g, c_0$, and c_1 to the *Bank* according to the VSS scheme. Using these values, bank can check the correctness of the shared value.

$$g^{f(1)} \overset{?}{=} c_0 c_1 = g^x g^{a_1} = g^{x+a_1} = g^{f(1)}$$

   If this verification is failed, the request will be rejected. Because customer is trying to cheat the mark. If the customer is suspected as criminal, then she will save these values with the customer's ID for tracing.

6. *Customer* will send $f(2), g, c_0$, and c_1 to the *Merchant* later.

   The secret mark x can be recovered by $f(1)$ and $f(2)$ using VSS. As a result, *Bank* doesn't know the mark x. And α, ω are given to the *Customer*.

Customer		Bank
α, ω is given during initial step		
For every coin, $\delta \in_{\mathcal{R}} \mathbb{Z}_q^*$		
$\alpha' = \alpha^{\delta} \mod p$		
$\omega' = \omega^{\delta} \mod p$		
		$(k_1, k_2) \in_{\mathcal{R}} \mathbb{Z}_q$
$(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$	$\xleftarrow{t, T_v, Sig_{bank}(T_v)}$	$t = g_1^{k_1} \alpha^{k_2} \mod p$
$t' = t g_1^{\beta_1} \alpha'^{\beta_2} v^{\gamma}$		
$m' = m \vert\vert T_v \vert\vert Sig_{bank}(T_v)$		
$c' = H(m', \alpha', t')$		
$c = c' - \gamma \mod q$	$\xrightarrow{c}$	$S_1 = k_1 - cs_1 \mod q$
		$S_2 = k_2 - cs_2 r^{-1} \mod q$
		which are satisfying
		$t = g_1^{S_1} \alpha^{S_2} v^{c} \mod p$
$S_1' = S_1 + \beta_1 \mod q$	$\xleftarrow{S_1, S_2}$	
$S_2' = \delta^{-1} S_2 + \beta_2 \mod q$		
$t' \overset{?}{=} g_1^{{S_1}'} \alpha'^{{S_2}'} v^{c'} \mod p$		
coin : $(m', t', S_1', S_2', \alpha', \omega', c_0, c_1)$		

Figure 4.2: Withdrawal stage

4.2.3 Withdrawal Stage

In this stage, customer receives the expiration date of validity time T_v, makes coin message m', and takes blind signature on the coin from the bank. Finally, customer makes one coin stream.

1. For every coin, *Customer* selects $\delta \in_{\mathcal{R}} \mathbb{Z}_q^*$ and calculate

$$\alpha' = \alpha^{\delta} \mod p$$
$$\omega' = \omega^{\delta} \mod p.$$

   Customer has to transform α to α' using randomly chosen δ for every coin. Otherwise the bank could recognize coins at deposit of behalf of the generator α.

The value α' and ω' will be used for coin stream, and they keep the same relation with α and ω (i.e. $\omega = \alpha^x \mod p$).

$$\begin{aligned}\omega' &= \omega^\delta \mod p \\ &= (\alpha^x)^\delta \mod p \\ &= (\alpha^\delta)^x \mod p \\ &= \alpha'^x \mod p\end{aligned}$$

2. *Bank* selects $(k_1, k_2) \in_{\mathcal{R}} \mathbb{Z}_q$ and calculates $t = g_1^{k_1}\alpha^{k_2} \mod p$. Also, she decides expiration date of validity time T_v and signed on it.
   Then sends $t, T_v, Sig_{bank}(T_v)$ to $Customer$.

3. Blinding
   $Customer$ makes coin message $m' = m||T_v||Sig_{bank}(T_v)$.
   And he chooses $(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$ and calculates $t' = tg_1^{\beta_1}\alpha'^{\beta_2}v^\gamma \mod p$ where v is the blind signature public key of the bank.
   And he also calculates $c' = H(m', \alpha', t')$ and sends $c = c' - \gamma \mod q$ to the *Bank*.

4. Signing
   Bank calculates $S_1 = k_1 - cs_1 \mod q$, $S_2 = k_2 - cs_2r^{-1} \mod q$

which satisfies $t = g_1^{S_1}\alpha^{S_2}v^c \mod p$.

$$\begin{aligned}
g_1^{S_1}\alpha^{S_2}v^c &= g_1^{k_1-cs_1}\alpha^{k_2-cs_2r^{-1}}v^c \mod p \\
&= (g_1^{k_1}\alpha^{k_2})(g_1^{-cs_1}\alpha^{-cs_2r^{-1}})v^c \mod p \\
&= t(g_1^{-cs_1}\alpha^{-cs_2r^{-1}})v^c \mod p \\
&= t(g_1^{-cs_1})((g_2^r)^{-cs_2r^{-1}})v^c \mod p \\
&= t(g_1^{-cs_1})(g_2^{-cs_2})v^c \mod p \\
&= t(g_1^{s_1}g_2^{s_2})^{-c}v^c \mod p \\
&= t(v)^{-c}v^c \mod p \\
&= t \mod p
\end{aligned}$$

And *Bank* sends S_1, S_2 to *Customer*.

5. Unblinding

   Customer calculates

$$\begin{aligned}
S_1' &= S_1 + \beta_1 \mod q, \\
S_2' &= \delta^{-1}S_2 + \beta_2 \mod q.
\end{aligned}$$

   The *coin* is $(m', t', S_1', S_2', \alpha', \omega', c_0, c_1)$.

6. Reliance of coin

   The reliance of this coin can be achieved by blind signature verification. In this step, all necessary values can be extract from coin's stream and bank's public key. In other words, you can extract g_1, v from public key (p, q, g_1, g_2, v), and find out $t', {S_1}', {S_2}', \alpha'$ from coin stream, and can calculate c' from the equation $c' = H(m', \alpha', t')$ where the arguments can extract from coin stream.

   So, Anyone can verify the blind signature by comparing t' and

$g_1^{{S_1}'}{\alpha'}^{{S_2}'}v^{c'} \mod p$.

$$\begin{aligned} t' &\overset{?}{=} g_1^{{S_1}'}{\alpha'}^{{S_2}'}v^{c'} \mod p \\ &= (g_1^{S_1+\beta_1})({\alpha'}^{\delta^{-1}S_2+\beta_2})(v^{c'}) \mod p \\ &= (g_1^{S_1+\beta_1})({\alpha'}^{\delta^{-1}S_2})({\alpha'}^{\beta_2})(v^{c'}) \mod p \\ &= (g_1^{S_1+\beta_1})((\alpha^{\delta})^{\delta^{-1}S_2})({\alpha'}^{\beta_2})(v^{c'}) \mod p \\ &= (g_1^{S_1+\beta_1})(\alpha^{S_2})({\alpha'}^{\beta_2})(v^{c+\gamma}) \mod p \\ &= (g_1^{S_1}\alpha^{S_2}v^{c})(g_1^{\beta}{\alpha'}^{\beta_2}v^{\gamma}) \mod p \\ &= t(g_1^{\beta_1}{\alpha'}^{\beta_2}v^{\gamma}) \mod p \\ &= t' \mod p \end{aligned}$$

4.2.4 Payment Stage

In this stage, customer gives his coin and additional values to merchant. The values are :

- Coin : $(m', t', S_1', S_2', \alpha', \omega', c_0, c_1)$
- Shared values $f(2)$ and g for VSS
- $g' = g^{\delta} \mod p, \quad D = \delta + c'S_k$ for one-time signature, where random number δ is treated as one-time number

Then merchant can verify the truth of the shared secret using VSS.

$$g^{f(2)} \overset{?}{=} c_0c_1^2 = g^x g^{2a_1} = g^{x+2a_1} = g^{f(2)}$$

And merchant can verify the truth of one-time signature also.

$$\begin{aligned} g' &\overset{?}{=} g^D P_k^{c'} \mod p \\ &= g^{(\delta+c'S_k)}(g^{-S_k})^{c'} \mod p \\ &= g^{\delta} \mod p \end{aligned}$$

where $c' = H(m', \alpha', t')$ can calculate from coin stream $(m', t', S_1', S_2', \alpha', \omega', c_0, c_1)$.

4.2.5 Deposit and Verification Stage

In this stage, a merchant sends the coin to a bank simply. But sometimes, one more interaction can be performed for tracing or double spending prevention.

Fair Tracing

When a merchant deposits the received coin, the tracing mechanism can be performed.

If the bank knows the secret mark x, then he can check the depositing coin with

$$\omega' = \alpha'^{x} \mod p$$

from the coin stream $(m', t', S'_1, S'_2, \alpha', \omega', c_0, c_1)$.

But, as we have already mentioned, the bank doesn't know about the secret mark. So, illegal tracing is impossible. On the other hand, customer can revels x to bank when he was blackmailed. Then bank can check it easily.

If a customer is suspected as criminal, bank stored the shared values $f(1), g, c_0$ and c_1 to DB in initial stage. Then bank compare c_0 and c_1 of depositing coin with the stored values in DB. If the values are same, then bank request merchant to reveal shared value $f(2)$ under the permission of lawyer. After all, bank can extract the secret value x using $f(1)$ and $f(2)$, and acquires the usage of coin.

$$f(1) = x + a_1, f(2) = x + 2a_1$$
$$x = 2f(1) - f(2)$$

In this protocol, revealing shared value $f(2)$ to the bank, the merchant has no advantages. Therefore, bank cannot trace the coin without other's cooperation. So, we can say that this is a fair tracing.

Double Spending Prevention and Detection

Each coin has a time limit for usage. So, all coin must be deposited to the bank by expiration date T_v. And bank will maintain the spent coin until T_v.

In on-line e-cash system, when a merchant received a coin, he can request to the bank whether the coin is already on spent coin list or not. If the coin is in the spent list, the merchant will abort the transaction. So, merchant need not request the one-time signature of customer.

In off-line system, real time double spending prevention is impossible, but detection is possible using the same mechanism of on-line system through depositing coins on expiration date T_v. But we cannot know who is the criminal, because the shared value(c_0, c_1) is a only one clue, and bank doesn't save all this value lists.

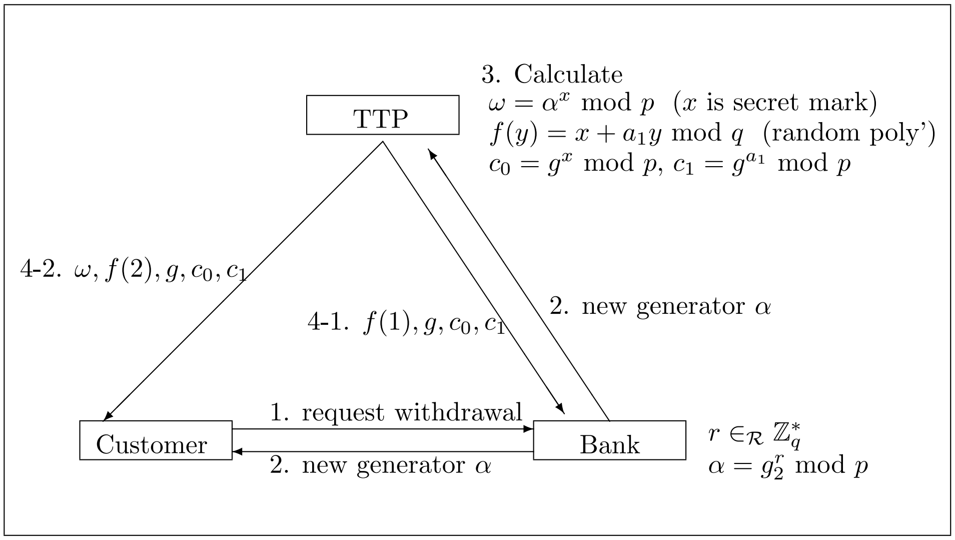
One-time signature can be a solution for this problem. In previous stage, customer choose unique one-time random number δ for each coins, and received the bank's blind signature. So, δ is a important blinding factor and combined with blind signature. So, if customer use it more than once for different coin message m', customer's secret key will be exposed.

$$\begin{aligned} D'' &= \delta + c''S_k \\ S_k &= \frac{D - D''}{c' - c''} \\ &= \frac{(\delta + c'S_k) - (\delta + c''S_k)}{c' - c''} \mod q \end{aligned}$$

So, customer will not try to use a coin more than once. Otherwise, on final date T_v, double spending can be detected, and bank can reveal the criminal in cooperation with the merchant.

4.3 Variant

Introducing TTP, we can achieve the same goal easily. At initial stage, TTP decides secret mark x and distributes the secret value to customer and bank. The other stage is not changed and the merits of our scheme is conserved. In this variants, we don't need to deliver the shared values to merchant. TTP will reveal the secret mark x, whenever it is needed and legally requested.



3. Calculate
$\omega = \alpha^x \bmod p$ (x is secret mark)
$f(y) = x + a_1 y \bmod q$ (random poly')
$c_0 = g^x \bmod p$, $c_1 = g^{a_1} \bmod p$
TTP
4-2. $\omega, f(2), g, c_0, c_1$
4-1. $f(1), g, c_0, c_1$
2. new generator α
1. request withdrawal
Customer
Bank
2. new generator α
$r \in_{\mathcal{R}} \mathbb{Z}_q^*$
$\alpha = g_2^r \bmod p$

Figure 4.3: Initial stage with TTP

1. *Customer* requests coin withdrawal to the *Bank*.

2. *Bank* selects random number $r \in_{\mathcal{R}} \mathbb{Z}_q^*$, makes a new generator $\alpha = g_2^r \bmod p$, and sends it to the the *Customer* and *TTP*.

3. *TTP* chooses a random number x as a secret mark and calculate $\omega = \alpha^x \bmod p$. Also, *TTP* selects a random polynomial $f(y) = x + a_1 y \bmod q$ and calculate $c_0 = g^x \bmod p$, $c_1 = g^{a_1} \bmod p$.

4. *TTP* sends $f(1), g, c_0, c_1$ to the *Bank* and $f(2), g, c_0, c_1$ to the *Customer* according to the VSS scheme.

5. The secret mark x can be recovered by $f(1)$ and $f(2)$ using VSS. As a result, *Bank* doesn't know the mark x. And α, ω are given to the *Customer*.

But, introducing TTP is a big assumption. So, if there is any legal authority, TTP can be replaced by it.

V. Analysis on Attack model and Comparison

Now, we will check how the proposed protocol can be applied to solve anonymity related problems.

5.1 Resistance Against Blackmailing and Kidnapping

Withdrawal based tracing initiated by customer can be used to blackmailing and kidnapping. The difference between blackmailing and kidnapping is that a kidnapper has physical control over his victim. Thus, all actions of the victim are observed by the kidnapper. In contrast to blackmailing, a kidnapper risks to be identified by his victim.

In both cases the customer reveals his secret mark to the bank, which will be detected at deposit. Depending on the choice of the customer the bank can accept or reject detected blackmailed marked coins at deposit. If the customer later instructs the bank to reject all his blackmailed coins, the bank will immediately refund all the unspent blackmailed coins to the customer. Then the bank can also prove with the disavowal protocol that the rejected coins have been blackmailed.

However, in the auditing case, the bank must be able to prove that the issued coins are not illegally traced. Therefore, the bank needs a certificate from the customer, which proves that tracing was initiated by the customer.

In the case of kidnapping, issuing such a certificate might be a problem, as the kidnapper observes the actions of the customer. This problem can be prevented, if the customer always has to issue a certificate $Sig_{customer}(y_M = g^{x_M}; customerID; coin\ generation)$ before a withdrawal. In case of an emergency, customer used this marking key x_M which has already known to the bank, otherwise used any random mark x. After all, Bank can know the customer's status and prevent the criminals.

5.2 Resistance Against Bank Robbery Attack

The ability to forge banknotes is a major threat for governments and banks, as a huge amount of forged banknotes will let the financial system of a country collapse. This situation is even worse with coin based anonymous electronic payment systems, as forged coins cannot be distinguished from regularly issued coins. This problem was first discovered by Jakobsson and Yung [JY96] who introduced the bank robbery attack, where the goal is to illegally obtain money from the bank: A robber can receive money either by gaining access to the bank's private signature keys, which are used to mint (unmarked) coins, or by blackmailing the bank to issue a number of coins in a non-regular withdrawal, so that tracing mechanisms will be circumvented by the blackmailer. The problem of bank robberies was already addressed in several papers (e.g. [JY96, PP97]).

However the previously proposed practical solutions rely on trust in a third party and thus offer only restricted privacy for the customers. Our payment system cannot guarantee that the marking mechanism can also be used in the case of bank robberies, because the robber may not give the shared secret value $f(1), g, c_0, c_1$ to the bank.

A basic assumption of our approach to prevent bank robberies is that they do not occur often. After a bank robbery, the bank will immediately finish the deposit stage of the affected coin generation to prevent spending of robbed coins. Then the customers have to redeem their coins with the secure redemption method and thus may exchange the legally withdrawn and unspent coins against new coins. The bank robber cannot redeem the robbed coins, as the bank always detects that these coins were not issued in a regular withdrawal, as their α will not be stored in the database of withdrawn coins and the secure redemption also prevents mapping of robbed coins to legally withdrawn and previously spent coins.

Another mechanism for minimizing this damage, we can use the T_v. If the bank used short term for validity time, and the robbed coins are used the same T_v, bank can examine all the depositing coin which has this value. After that, the bank can identify the one-time signature public key in cooperation with merchant. So, the number of candidate of bank robbery will be reduced.

5.3 Comparisons

Compared with KV-scheme, our protocol is much more efficient in terms of computational complexity and data storage.

If we assume that a mid-size bank has one million(10^6) customers or accounts, each customer withdraws and uses about one thousand coins, and 1% of customers are suspicious. In this case, 10^9 coins are issued. And you have to investigate all 10^9 key lists for owner tracing of one depositing coin. But in our scheme, mark x is not saved in the bank and only suspicious customer's information($CustomerID, f(1), g, c_0, c_1$) will be saved. In complexity of comparisons, our scheme is more efficient by 10^9 times per coin.

We have to estimate the real storage for coins and other necessary information. The required additional information is almost same as or smaller than previous scheme. Because previous scheme needs judge's certification and signed mark(marked or unmarked key) lists. But this new scheme needs some other information for VSS scheme.

The key point of this new scheme is that bank cannot trace illegally by itself. This means that perfect fair tracing can be achieved. Besides, in payment stage, we can introduce one-time signature and prevent double spending of e-cash. Moreover, this signature can be separated from main protocol, and revealing signature's private key will not affect the other signature scheme, but only revealed the customer's privacy. In other words, one-time signature doesn't affect the soundness of e-cash.

But there is a also small disadvantage. In our protocol, we assumed that 3 different parties, so we didn't consider that bank can be a merchant. This case is very rare, but bank can sell goods sometimes. In this case, customer must give all shared values to the bank, and bank can find out secret mark by himself. So, if the customer doesn't care the tracing capability of bank, he will use the coin which was issued by the same bank. Otherwise, he have to use other bank's coin.

VI. Conclusion

Anonymity and legal tracing capability is one of the important features of e-cash system. We proposed a fair tracing mechanism based on a variant of an Okamoto-Schnorr blind signature and VSS scheme. Besides we introduced the double spending prevention mechanism by Schnorr's one-time signature. And we show that our mechanism is able to defend against blackmailing, kidnapping and bank robbery attack.

As a future work, transferability is a related problem of anonymity and fair tracing ability. On-line transferability can be achieved easily by engaging e-cash issued bank. But off-line transferability may be lost the tracing capability. So, if we can devise this mechanism in this protocol, it will be a good and more realistic e-cash system.

Currently, many researchers trying to make a new protocol satisfying all requirements continuously. So, combining cryptographic primitives and some known e-cash protocols, we can develop a good and real e-cash system in the future.

공정한 추적이 가능한 은닉서명기반 전자화폐 시스템 설계

김병곤

전자상거래의 확산에 따라 전자화폐(e-cash)에 대한 연구가 많이 이루어져 왔다. 그러나 전자화폐의 모든 요구사항을 만족하는 효율적인 시스템은 보기 어려우며, 부분적 혹은 전체적인 요구사항을 만족하는 시스템을 만들기 위해 많은 사람들이 노력하고 있다. 그런 요구사항중의 하나가 *공정한 추적(Fair Tracing)* 문제이다.

전자화폐 시스템에서는 고객이 은행에서 코인(Coin)을 인출하고, 상인에게 오프라인(Off-line)으로 지불하며, 최종적으로 상인이 은행에 예치한다. 고객의 프라이버시를 보장하기 위하여 지불시 익명성이 보장되어야하며, 이는 은닉서명을 통하여 이루어질 수 있다. 그러나 무조건적인 익명성은 범죄에 남용될 위험이 있다. 즉, 돈세탁이나 불법적인 구매, 은행털이, 협박등의 범죄에 무조건적인 익명성이 보장된다면 완전 범죄가 가능해진다.

본 논문에서 제안하는 방식은 전자화폐에 추적성을 부여할 뿐 만 아니라 비교 연산에 있어서도 기존 추적 방식에 비해 우위를 가진다. 또한 기존 방식의 경우 불법 추적이 가능하지만 나중에 불법임을 밝혀낼 수 있다는 낙관적인 견해의 공정한 추적임에 반하여, 본 논문에서 제안하는 방식은 불법 추적이 아예 불가능한 공정한 추적 방식이다.

또한 이중사용방지를 위하여 일회용 서명을 도입하였다. 익명성 문제에만 치중된 프로토콜은 전자화폐의 이중사용이라는 취약점에 노출될 수 있다. 따라서 본 논문에서는 이 두가지 문제를 동시에 고려하였으며, 제안된 방식의 변형 가능성도 모색한다.

References

[Bla79] G.R. Blakley, "Safeguarding Cryptographic Keys", *Proceedings of AFIPS 1979 National Computer Conference*, Vol. 48, pp. 313–317, 1979.

[Sha79] A. Shamir, "How to share a secret", *Communications of the ACM, 22,11*, pp.612–613, 1979.

[Cha82] D. Chaum, "Blind signatures for untraceable payments", *Crypto 82*, pp.199–203, 1982

[Feld87] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", *In Proc. of the 28th IEEE Ann. Symp. on Foundations of Computer Science*, pp. 427–437, IEEE, 1987.

[CFN88] D. Chaum, A. Fiat and M. Naor, "Untraceable electronic cash", *Crypto '88*, pp.819–327, Springer-Verlag, 1988.

[Cha90] D. Chaum,"Zero-knowledge undeniable signatures", *Advances in Cryptology - EUROCRYPT '90*, LNCS 473, Springer-Verlag, pp.458–464, 1990.

[Sch91] C. Schnorr, "Efficient signature generation for smart cards", *Journal of Cryptology*, vol.4, no.3, pp.161–174, 1991.

[Oka92] T.Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes", *Advances in Cryptology-Crypto '92*, LNCS 740, Springer-Verlag,pp.31–53,1992.

[vSN92] B. Von Solms and D. Naccache, "On blind signatures and perfect crimes", *Computers and Security 11(6)*, pp.581–583, 1992.

[CFM94] B. Chor, A. Fiat and M. Naor, "Tracing traitors", *Advances in Cryptology - CRYPTO '94*, LNCS 839, pp.257–270, Springer-Verlag, 1994.

[SPC95] M. Stadler, J.M. Piveteau and J. Camenisch, "Fair blind signatures", *Advances in Cryptology - EUROCRYPT '95*, LNCS 921, Springer-Verlag, pp.209–219, 1995.

[MOV96] A.J. Menezes, P.v. Oorschot and S. Vanstone, " Handbook of Applied Cryptography", CRC press LLC, pp.475, 1996.

[JY96] M. Jakobsson and M. Yung, "Revokable and versatile electronic money", *3rd ACM Conference on Computer and Communications Security - CCS '96*, ACM Press, pp.76–87, 1996.

[OA97] T. Okamoto and H. Yamamoto, "Modern cryptography", Life&Power press, pp.227, 1997.

[DFTY97] G. Davida, Y. Frankel, Y. Tsiounis and M. Yung, "Anonymity control in e-cash systems", *Financial Cryptography - FC'97*, LNCS 1318, Springer-Verlag,pp.1–16,1997.

[NMV97] K.Q. Nguyen, Y. Mu, and V. Varadharajan, "One-Response Off-Line Digital Coins", *Proceedings of SAC '97*, 1997

[PP97] H. Petersen and G. Poupard, "Efficient scalable fair cash with off-line extortion prevention", *International Conference on Information and Communications Security - ICICS '97*, LNCS 1334, Springer-Verlag, pp. 463–477, 1997.

[ST99] T. Sander and A. Ta-Shma, "On Anonymous Electronic Cash and Crime", ISW, pp.202–206, 1999.

[ST99a] T. Sander and A. Ta-Shma, “Auditable, Anonymous Electronic Cash”, CRYPTO ’99, LNCS 1648, Springer-Verlag, pp.555–572, 1999

[AM00] R.Sai Anand and C.E. Veni Madhavan, “An Online, Transferable E-Cash Payment System”, *INDOCRYPT 2000*, LNCS1997, pp.93-103, 2000.

[ZW00] F.Zhang, Y. Wang, “Fair Electronic Cash Systems with Multiple Banks”, *IFIP TC11 16th Annual Working Conference on Information Security: Information Security for Global Information Infrastructures*, Kluwer Academic Publishers, pp.461-470, 2000.

[PS01] B. Pfitzmann and A. R. Sadeghi, “Slef-escrowed cash against user blackmailing”, *Financial Cryptography - FC 2000*, LNCS 1962, Springer-Verlag, pp.42–52, 2001

[KV01] D. Kügler and H. Vogt, “Fair tracing without trustees”, *Financial Cryptography - FC 2001*, Preproceedings, 2001.

[JKC01] Jinho Kim, Kwangjo Kim and Chulsoo Lee, “An Efficient and Provably Secure Threshold Blind Signature”, *ICISC 2001*, LNCS 2288, Springer-Verlag, pp.318–327, 2002.

[CZW03] X. Chen, F. Zhang and Y. Wang, “A New Approach to Prevent Blackmailing in E-Cash”, available from `http://eprint.iacr.org/2003/055/`, 2003

Acknowledgement

First, I would like to express my gratitude to Prof. Kwangjo Kim, my thesis advisor, for his constant direction and support. Without his guidance, I could never have carried out my research. Special thanks are also due to Prof. Jae Choon Cha and Dr. Soran Ine for their generosity and agreeing to serve as advisory committee members.

I would like to mention the close relationship of my colleagues in C&IS lab members. There were 6 graduates I have enjoyed ICU life together: Myungsun Kim, JongSeong Kim, WooSeok Ham, HyunRok Lee and HyungKi Choi, Dang Nguyen Duc. There are also many current members: Dr. Xiaofeng Chen, Vo Duc Liem, Nv Jigian, Ren Kui, Yan Xie, Wang Ping, Munirathnam M. Divyan, SongWon Lee, HwaSun Chang, Chuljoon Choi, SungJoon Min, SangWon Lee, JaeHyrk Park, JoongMan Kim, SuGil Choi, Zeen Kim, KyuSuk Han, SeokKyu Kang and JeongKyu Yang. Their kind and sincere support leads me to carry out this thesis and successful ICU life.

In addition, I would like to give my thanks JeongYun Lee, Sangbae Park, SeungHo Lee and many other students for their constant encouragement and affection.

Also I should mention my compnay SAMSUNG SDS and close colleagues SeungKook Lee, SungHo Cho, KiHyung Kim, JongJu Kim, GabSeong Son, JaeSik Son, IkJae Lee, TaeHun Lee, MeonSik Choi and many others in Koje Shipbuilding IS team. Their support make me come to this university. Besides I can remember my customers during in Koje island : KyuOk Hwang, HoYoung Yoon, SangHwan Cho, ChoWoo Lee, TaeSik Ahn and many others.

My love and thanks goes to my parents, my brothers and sisters for endless and profound affection and their devotion. Also many thanks to my wife's family, especially my mother-in-law always help my family with sweet heart.

Most of all, I have to give my thanks and love to my wife KiYoung Park for her endless encourage and devotion, and to my lovely son JeKwan and daughter Jihae. I dedicate this work to them.

Curriculum Vitae

Name : ByeongKon Kim

Date of Birth : July. 26. 1966

Sex : Male

Nationality : Korean

Education

1986.3–1993.2	Physics Yonsei University (B.S.)
2002.3–2004.2	Engineering Information and Communications University (M.S.)

Career

1993.8–2004.2	Senior Engineer HR Planning & Management Group, SAMSUNG SDS SHI Shipyard I.S. Team, SAMSUNG SDS
2002.3–2004.2	Graduate Research Assistant Cultivation of Top-Level IT Security Manpower Information Research center for Information Security, ICU

2002.3–2002.8	Graduate Research Assistant Development of Electronic Voting System for Worldcup 2002 Information Research center for Information Security, ICU
2003.2–2003.6	Graduate Teaching Assistant ICE514 Concrete Mathematics, ICU

Publications

International Papers (in English)

1. ByeongKon Kim, SungJun Min, and Kwangjo Kim, "Fair tracing based on VSS and blind signature without Trustees", Proc. of CSS2003, pp 37-42, Oct. 29 31,2003, Kitakyushu, Japan
2. SuGil Choi, Kwangjo Kim and ByeongKon Kim, "Practical Solution for Location Privacy in Mobile IPv6", In Pre-Proc. of WISA2003, pp.88-97, Aug. 25-27, 2003, Jeju Island, Korea

Domestic Papers (in Korean)

1. ByeongKon Kim and Kwangjo Kim, "VSS와 은닉서명에 기반한 공정한 추적 방식", 2003년도 한국정보보호학회 하계정보보호학술대회, pp.53-56, 2003.7.4, 배재대, 대전
2. ByeongKon Kim and Kwangjo Kim, "VSS를 이용한 신뢰기관 없는 공정한 추적 방식", 2003년도 한국정보보호학회 동계학술대회, pp.291-295, 2003.12.6, 한양대, 서울