Fair tracing based on VSS and blind signature without Trustees

ByeongGon Kim SungJun Min Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications Univ.(ICU),
58-4 Hwa-am Dong, Yuseoung Gu, Daejeon, Korea 305-732

{virus, sjmin, kkj}@icu.ac.kr

Abstract 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 tracing and depositing in bank. But in this scheme, illegal tracing done by bank alone is impossible. We propose a marking mechanism based on a variant of an Okamoto-Schnorr blind signature and Verifiable Secret Sharing scheme. And we put a merchant in this protocol instead of Trustees. This scheme is able to defend against blackmailing, kidnapping, bank robbery and money laundering.

1 Introduction

As the core to realizing the electronic commerce, the electronic cash(e-cash) demand will increase. 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 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 the 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.

In this paper, however, we propose a withdrawal-based real fair tracing and show that it has an enhanced computational complexity.

2 Related Works

2.1 KV-Scheme

Kügler and Vogt [KV01] proposed a marking mechanism based on a variant of an Okamoto-Schnorr Blind Signature [Oka92] in combination with a Chaum-van Antwerpen undeniable signature [Cha90].

2.1.1 Notations

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.

$v = g_1^{s_1} g_2^{s_2} (\text{mod } p)$ is the public key of the bank for blind signature.

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

$y = g_3^x (\text{mod } p)$ is the public key of the bank for undeniable signature.

2.1.2 Protocol

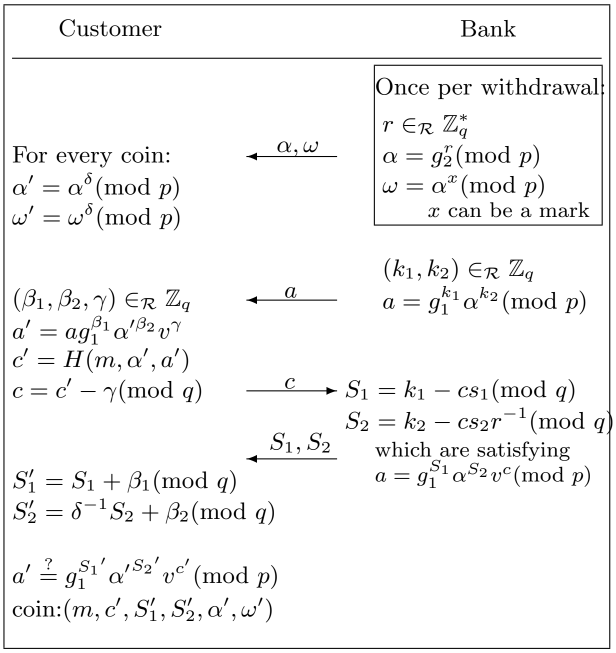
Customer
Bank
Once per withdrawal:
$r \in_{\mathcal{R}} \mathbb{Z}_q^*$
$\alpha = g_2^r (\text{mod } p)$
$\omega = \alpha^x (\text{mod } p)$
x can be a mark
α, ω
For every coin:
$\alpha' = \alpha^\delta (\text{mod } p)$
$\omega' = \omega^\delta (\text{mod } p)$
$(k_1, k_2) \in_{\mathcal{R}} \mathbb{Z}_q$
$a = g_1^{k_1} \alpha^{k_2} (\text{mod } p)$
a
$(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$
$a' = a g_1^{\beta_1} \alpha'^{\beta_2} v^\gamma$
$c' = H(m, \alpha', a')$
$c = c' - \gamma (\text{mod } q)$
c
$S_1 = k_1 - cs_1 (\text{mod } q)$
$S_2 = k_2 - cs_2 r^{-1} (\text{mod } q)$
which are satisfying
$a = g_1^{S_1} \alpha^{S_2} v^c (\text{mod } p)$
S_1, S_2
$S_1' = S_1 + \beta_1 (\text{mod } q)$
$S_2' = \delta^{-1} S_2 + \beta_2 (\text{mod } q)$
$a' \overset{?}{=} g_1^{S_1'} \alpha'^{S_2'} v^{c'} (\text{mod } p)$
coin:$(m, c', S_1', S_2', \alpha', \omega')$

Figure 1: KV-scheme of fair tracing

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

2. *Customer* blinds the value α and ω. For every coin, he selects $\delta \in_{\mathcal{R}} \mathbb{Z}_q^*$ and calculates $\alpha' = \alpha^\delta$ (mod p),
$\omega' = \omega^\delta = \alpha^{x\delta} = \alpha'^x$ (mod p).

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 $a = g_1^{k_1} \alpha^{k_2}$ (mod p) to *Customer*.

4. *Customer* chooses $(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$ and calculates $a' = a g_1^{\beta_1} \alpha'^{\beta_2} v^\gamma$ (mod p) where v is the public key of the bank for blind signature. And he also calculates $c' = H(m, \alpha', a')$ and sends $c = c' - \gamma$ (mod q) to the *Bank*.

5. *Bank* calculates $S_1 = k_1 - cs_1 (\text{mod } q)$, $S_2 = k_2 - cs_2 r^{-1} (\text{mod } q)$ which satisfies $a = g_1^{S_1} \alpha^{S_2} v^c (\text{mod } p)$. 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 a' and $g_1^{S_1'} \alpha'^{S_2'} v^{c'} (\text{mod } p)$.

8. coin: $(m, c', S_1', S_2', \alpha', \omega')$.

2.1.3 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).

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

But if the customer tries to check whether his coin has been traced or not, he needs additional information Sig_{bank}=(α, ω, *customerID*, *coin generation*).

One of the merits in this protocol is that the tracing capability can be transferred to a separate tracing authority.

2.1.4 Weak points

One of the drawbacks of this KV-scheme of fair tracing 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 marking key and certification of judge. In audit phase, the bank has to publish all marking key and certifications of judge.

Other major 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 $\omega = \alpha'^{x'} (\text{mod } p)$. If he cannot find any matched x or x_M, he can argue that the coin was illegally traced.

2.2 VSS (Verifiable Secret Sharing)

Feldman proposed a non-interactive verifiable secret sharing scheme, 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 user of secret sharing.

2. *Distributor* chooses a random polynomial
$f(x) = s + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$ $(\text{mod } q)$.

3. *Distributor* distributes $f(j)$ to each user j.

4. *Distributor* chooses p such that $q|(p-1)$, and generator $g \in_{\mathcal{R}} \mathbb{Z}_p^*$ of order q. And he also calculates

$$\begin{aligned} c_0 &= g^s (modp) \\ c_1 &= g^{a_1} (modp) \\ &\cdots \\ c_{k-1} &= g^{a_{k-1}} (modp) \end{aligned}$$

5. *Distributor* 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.

$$\begin{aligned} g^{f(j)} &\stackrel{?}{=} c_0 c_1^j c_2^{j^2} \cdots c_{k-1}^{j^{k-1}} \\ &= g^s g^{a_1 j} g^{a_2 j^2} \cdots g^{a_{k-1} j^{k-1}} \\ &= g^{s + a_1 j + a_2 j^2 + \cdots + a_{k-1} j^{k-1}} \end{aligned}$$

7. User j can recover secret s from $f(j)$ by using Lagrange interpolation.

3 Proposed Scheme

In this section we describe a protocol which combines VSS and modification of Kügler and Vogt scheme based on Okamoto-Schnorr blind signature in order to make a practical e-cash system.

3.1 Main idea

We consider 3-parties, customer, merchant and bank. Among them, customer will make mark x and undeniable signature $\omega = \alpha^x (\text{mod } p)$. The secret value 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.

3.2 Protocol

3.2.1 Notations

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 blind signature private key of the bank.

$v = g_1^{s_1} g_2^{s_2} (\text{mod } p)$ is the blind signature public key of the bank.

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

3.2.2 Initial step

In this step, *Customer* will make a secret mark and distribute it partially. This work also can be done by trusteed third party(TTP). But we will not assume the existence of TTP.

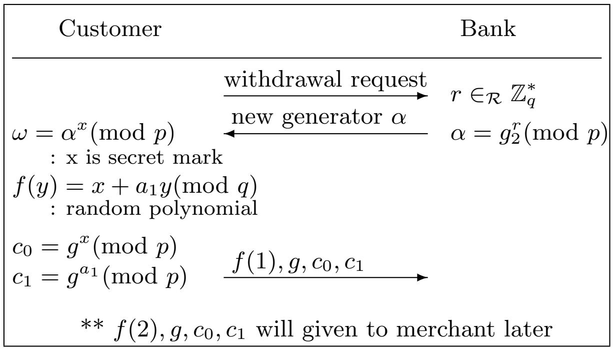
Customer
Bank
withdrawal request
$r \in_{\mathcal{R}} \mathbb{Z}_q^*$
new generator α
$\omega = \alpha^x(\bmod p)$
$\alpha = g_2^r(\bmod p)$
: x is secret mark
$f(y) = x + a_1 y(\bmod q)$
: random polynomial
$c_0 = g^x(\bmod p)$
$c_1 = g^{a_1}(\bmod p)$
$f(1), g, c_0, c_1$
** $f(2), g, c_0, c_1$ will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

Figure 2: Initial step of proposed scheme

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*.
3. *Customer* chooses a random number x as a secret mark and calculate $\omega = \alpha^x$ $(\bmod p)$.
4. *Customer* selects a random polynomial $f(y) = x + a_1 y$ $(\bmod q)$ and calculate $c_0 = g^x$ $(\bmod p)$, $c_1 = g^{a_1}$ $(\bmod p)$.
5. *Customer* sends $f(1), g, c_0$, and c_1 to the *Bank* according to the VSS scheme.
6. *Customer* will send $f(2), g, c_0$, and c_1 to the *Merchant* later.
7. The secret mark x can be recovered by $f(1)$ and $f(2)$ using VSS. As a result, *Bank* doesn't know the x. And α, ω are given to the *Customer* similar to the KV-scheme.

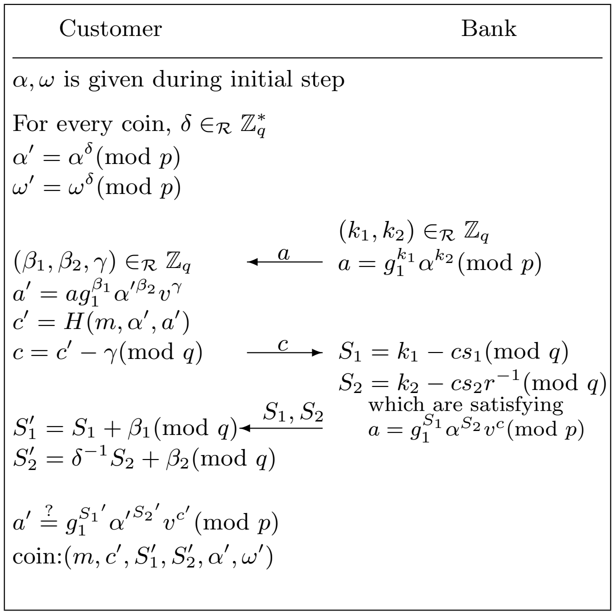
Customer
Bank
α, ω is given during initial step
For every coin, $\delta \in_{\mathcal{R}} \mathbb{Z}_q^*$
$\alpha' = \alpha^\delta(\bmod p)$
$\omega' = \omega^\delta(\bmod p)$
$(k_1, k_2) \in_{\mathcal{R}} \mathbb{Z}_q$
$(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$
a
$a = g_1^{k_1}\alpha^{k_2}(\bmod p)$
$a' = a g_1^{\beta_1}\alpha'^{\beta_2}v^\gamma$
$c' = H(m, \alpha', a')$
$c = c' - \gamma(\bmod q)$
c
$S_1 = k_1 - cs_1(\bmod q)$
$S_2 = k_2 - cs_2 r^{-1}(\bmod q)$
which are satisfying
S_1, S_2
$S_1' = S_1 + \beta_1(\bmod q)$
$a = g_1^{S_1}\alpha^{S_2}v^c(\bmod p)$
$S_2' = \delta^{-1}S_2 + \beta_2(\bmod q)$
$a' \overset{?}{=} g_1^{S_1'}\alpha'^{S_2'}v^{c'}(\bmod p)$
coin:$(m, c', S_1', S_2', \alpha', \omega')$

Figure 3: Withdrawal step of proposed scheme

3.2.3 Withdrawal step

In this step, the protocol is almost same as the KV-scheme. In other words, this step uses the variation of Okamoto-Schnorr blind signature.

1. For every coin, *Customer* select $\delta \in_{\mathcal{R}} \mathbb{Z}_q^*$ and calculate $\alpha' = \alpha^\delta(\bmod p)$, $\omega' = \omega^\delta(\bmod p)$.
2. *Bank* selects $(k_1, k_2) \in_{\mathcal{R}} \mathbb{Z}_q$ and sends $a = g_1^{k_1}\alpha^{k_2}(\bmod p)$ to *Customer*.
3. *Customer* chooses $(\beta_1, \beta_2, \gamma) \in_{\mathcal{R}} \mathbb{Z}_q$ and calculates $a' = a g_1^{\beta_1}\alpha'^{\beta_2}v^\gamma(\bmod p)$ where v is the blind signature public key of the bank.
   And he also calculates $c' = H(m, \alpha', a')$ and sends $c = c' - \gamma(\bmod q)$ to the *Bank*.
4. *Bank* calculates $S_1 = k_1 - cs_1$ $(\bmod q)$, $S_2 = k_2 - cs_2 r^{-1}$ $(\bmod q)$ which satisfies $a = g_1^{S_1}\alpha^{S_2}v^c(\bmod p)$.
   And *Bank* sends them to *Customer*.
5. *Customer* calculates $S_1' = S_1 + \beta_1$ (mod q), $S_2' = \delta^{-1}S_2 + \beta_2(\bmod q)$.
6. Anyone can verify the blind signature by comparing a' and $g_1^{S_1'}\alpha'^{S_2'}v^{c'}(\bmod p)$.
7. *coin* :$(m, c', S_1', S_2', \alpha', \omega')$.

3.2.4 Pay, Deposit and Verification step

When *Customer* gives coin to *Merchant*, he has to give $f(2), g, c_0, c_1$ also. Then *Merchant* can verify the truth of the shared secret using VSS.

$$g^{f(2)} \overset{?}{=} c_0 c_1^2 = g^x g^{2a_1} = g^{x+2a_1}$$

When *Merchant* deposit the received coin, the tracing mechanism can be performed. *Bank* can check the depositing coin with

$$\omega' = \alpha'^x (\bmod p)$$

if he knows the secret mark x. *Customer* revels x to *Bank* when he was blackmailed. If *Customer* is suspected as a criminal, *Bank* and *Merchant* can extract the secret value x using their own value $f(1)$ and $f(2)$ revealing under the permission of lawyer.

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

4 Comparisons

Compared with any other protocols, 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 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 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 informations. 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.

5 Conclusions

Anonymity and legal tracing capability is one of the important features of e-cash system. We propose tracing mechanism based on a variant of an Okamoto-Schnorr blind signature and VSS scheme.

Even though the fair tracing of e-cash is important, there is not an universal protocol to realize. Because there are many other requirements to consider in the real world. For example, divisibility, off-line usage and so on. Therefore, a new protocol only meet with partial requirements of e-cash, we have to try to come up with a new protocol using known cryptographic primitives and protocols. Combining various method or protocols, we can develop a good e-cash system someday.

References

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

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

[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.

[DFTY97] G. Davida, Y. Frankel, Y. Tsiounis, and M. Yung, "Anonymity control in e-cash systems", *Financial Cryptography - FC97*, LNCS 1318, Springer-Verlag,pp.1–16,1997.

[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.

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

[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.

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

[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