New Revocable E-cash System Based on the Limited Power of TTP

Yan Xie, Fangguo Zhang, and Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

Abstract

As a simulation or replacement of analog money in cyber space, the e-cash was introduced by using cryptographic primitives. Since a perfect anonymity system causes some illegal activities, such as money laundering, blackmailing, and illegal purchase, a revocable electronic system was paid a great attention to control the anonymity. In general, Trust Third Party(TTP) is introduced to detect any dubious user and coin, namely user tracing and coin tracing. In this paper we propose a new revocable anonymity e-cash system, and verify the security requirement as well. In our scheme a user first withdraws the e-coin from bank by using blind signature, and then TTP verifies the bank's signature and records the tracing information.

I. Introduction

As an important electronic payment system, electronic cash (or e-cash) system gets more and more concern due to the rapid application and development of electronic commerce in e-society. It can be considered as an imitation of physical money, but more convenient and economical. One of the most important factors of e-cash system similar to the physical cash is the protection of the user's privacy. Chaum suggested the first e-cash scheme [2] in 1982. In this scheme the technique of blind signatures was used to guarantee the privacy of users. But this complete anonymity of e-cash can be used for criminal activities [10], such as money laundering or blackmailing. For this reason the e-cash of future should be controlled (or revocable). The solution of controlling the anonymity is the natural involvement of the Third Trusted Party(TTP), which can revoke the anonymity of the user or the coin with the cooperation of bank. 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.

In this paper, we present a new revocable e-cash system scheme, A user first withdraws the e-coin from bank by using blind signature, and then TTP verifies the bank's signature and records the tracing information. This sequence is different from conventional protocol.

The organization of this paper is as follows: In section 2 we introduce the security requirement of a revocable e-cash system briefly. In section 3 we present our new revocable e-cash system protocol. In section 4 the analysis of our e- cash system is discussed. We make the final conclusion in section 5.

II. Requirements of A Revocable E-cash System

Usually there are four participants in an anonymity controlled e-cash system, which are user(U), bank(B), shop(S) and TTP; both U and S 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 with which U withdraws electronic coin form B, a payment protocol with which U pays the electronic coin to S, and a deposit protocol with which S deposits his electronic coins to the B. 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 a revocable e-cash system, which is described as follows:

1). Anonymity: System should provide anonymity of the coin and the identity of the legal user, along with the detection of the double spending.

2). 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.

3). Limitation of the tracer: 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.

4). No framing: In case of the collusion between B and TTP, a revocable e-cash system should ensure that B could not impersonate a legal user and his/her activities

5). 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.

The user tracing protocol is used to determine the identity of the user in a specific payment transaction. In this protocol, B gives the view of a deposit coin to TTP, and TTP return some specific information, which allow the B to identify the U through the database of user account. Money laundering can be prevented from detecting the identity of the illegal user in this protocol.

The coin tracing protocol is considered to determine the e-coin in deposit protocol. B gives TTP some information in a withdraw protocol, and TTP returns some information, which enables B to find the corresponding coin in deposit transaction. Blackmailer normally forces some legal user to withdraw some anonymity coin for them, so that they can use it without being detected, but with the withdraw report of the victim; the blackmailing crime can be prevented in this protocol.

Both of two tracing protocols should be provided in a revocable 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 of the revocable e-cash system requirement; user tracing and coin tracing protocol must be included.

Many revocable anonymity schemes are suggested, by using different technology, such as: fair blind signature [3][5][11], Indirect discourse proofs [6], Magic ink signature [1][7], Group signature [12][13], and Massage authentication code [8], and etc [9].

III. Our Revocable E-cash Protocol

In conventional anonymity controlled e-cash system, U should first register to TTP, and TTP embeds the tracing information into the e-coin, and then U withdraws money from B and gets B's valid blind signature at the same time. Contrary to the previous protocols, in our scheme B first gives the signature for the cash information that user submitted using the blind signature protocol. Then TTP verifies the validity of the e-coin, the blind signature of the bank, and ensures that each e-coin can be traced if required. Then, the TTP gives his signature in the e-coin, which means he takes responsibility 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. B can trace the coin or the user only with the help of TTP, and the privacy of honest users will be protected.

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^*

U and TTP independently create DSA signature system using system parameter by selecting 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. B creates blind DSA signature system using system parameter by selecting $x_b \in G_q$ randomly as his private key, and calculates $h_b= g^{x_b}$ as his public key and publishes it.

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

Account open:

U and S open their account in bank, and get their identities.

2. Withdrawal Protocol

Withdrawal protocol contains two steps, first, U gets the signature form B, and second, U gets the signature from TTP:

Step 1

- U should prove his identity to B; U sends his e-cash requirement m which denots *withdrawal require*|| *80bits random string*|| *time*. and provides his signature on m, which is $S_u= DSA_u(m)$ by his DSA private key. then U sends the pair (m, S_u) to B.

- B verifies U's signature by $VerDSA_u(S_u, m)$.

- B uses blind DSA signature to sign the e-coin, selects $r \in_R Z_q^*$ and calculates $R= g^r \mathrm{mod} p$ with his signature $T_b= DSA_b(R)$ and sends them to U, and stores R linked with U's ID as a pair (R, ID_u, m, S_u).

- U establishes a coin c and selects $\alpha, \beta \in_R Z_q^*$, calculates $R' = R^\alpha g^\beta \mathrm{mod} p$, and blinds cash date by computing $c' = \alpha c R R'^{-1} \mathrm{mod} q$, then sends c' to B. Then B computes $S' = rc' + R x_b \mathrm{mod} q$ and forwards to U.

- After receiving B's signature, U computes $s = s' R' R^{-1} + \beta c \mathrm{mod} q$ The Pair (S, R') is U's valid cash signature, which is dedicated as S_b.

Step 2

- U 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 [4]. Then TTP should check $VerDSA_b(R, T_b,)$ and verify the signature of blinded coin through the equation $(g^S h_b^{-R})^{c^{-1}} = R' \mathrm{mod} p$, after this, TTP sends U $S_{ttp}= DSA_{ttp}(c)$ 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: (c, S_b, S_{ttp}).

3. Payment Protocol:

After verifying the signatures (S_b, S_{ttp}) of B and TTP for e-coin c, S will accept the U's coin.

4. Deposit Protocol:

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

5. User Tracing Protocol:

B sends e-coin to TTP. Then, TTP finds the R, which linked with c, and sends R to B. Based on the previous database saved in withdrawal protocol, B can find the corresponding user from his database.

6. Coin Tracing Protocol:

When Blackmailing occurs, U should send his ID to B, and then B sends R to TTP. Then, TTP finds the corresponding c and sends it to B, then B can freeze the money.

IV. Analysis

Anonymity for legal user: The identity of a legal U is anonymous and cannot be linked with the e-cash. However, one who makes a double spending will be traced only by B. 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 U makes payment transaction, the Identity of U is anonymous, and S can only verify the U's e-cash.

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

No framing: Even B colludes with TTP, he cannot frame a legitimate user, because they cannot obtain the U's secret key x_u so that they cannot get the withdrawal counterfeit with the Ur's signature. If B forges a cash of the U to fraud him, U 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 U'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 B 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 U tries to forge a valid e-coin, he must generate a valid blind signature of B, since a public key pair of B 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 B is $1/q$, if q is larger, We can say the forgeability is impossible.

V. Concluding

E-cash system is going to be an important issue and application in current E-commerce . Obviously due to requirement of being similar to analog money and protecting some illegal crime, a revocable e-cash system is discussed and recommended. We propose a new revocable e-cash scheme whose security is based on discrete logarithm problem. Also, the security requirements of the proposed scheme is analyzed, but the security proof in a provable security sense is required as a further work.

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, 1999.

[2] D. Chaum, *Blind signature for Untraceable payments,* EUROCRYPT'82, pp. 199-203, 1983.

[3] Jan. Camenisch, U. Maurer, and Markus Stadler, *Digital payment system with passive anonymity revoking trustee,* In Esorics'96, LNCS 1146, Italy, pp. 33-43, 1996,

[4] Jan. Camenish and M. Stadler, *Efficient Grouop Signatures Schemes for Large Groups.* Crypto'97, LNCS1294, pp. 410-424, 1997.

[5] G. Davida, Y. Frankel, Y. Tsiounis, and M.Yung. *Anonymity control in E-Cash systems,* FC'97, LNCS 1318, pp. 1-16, 1997.

[6] Y. Frankle, Y. Tsiounis, and M. Yung, *indirect discourse proofs: Achieving fair off-line e-cash,* Asiacrypt'96, LNCS1163, pp. 286-300, 1996.

[7] M. Jakobsson and M. Yung, *Distributed "magic ink" Signatures,* Eurocrypt'97, LNCS 1233, pp. 450-464, 1997.

[8] A. Juel, Trusten token: *Simple and practical anonymous digital coin tracing,* in FC'99, LNCS 1648, pp. 29-45, 1999.

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

[10] B.V. Solms and D. Naccache, *On blind signatures and perfect crimes,* Computers and security, pp. 581-583, 1992.

[11] M. Stadler, J. M.Piveteau, and Jan. Camenisch, *Fair blind signatures,* Eurocrypt'95, LNCS 921, pp. 209-219, 1995.

[12] J, Traor, *Group signature and their relevance to privacy-protecting on-line electronic cash systems,* ACISP99. LNCS 1587, pp. 228-243, 1999.

[13] F. Zhang, F. Zhang, and Y. Wang, *Fair Electronic Cash Systems with Multiple Banks,* SEC 2000, pp. 461-470, Kluwer, 2000.