A FAIR OFF-LINE ELECTRONIC CASH SYSTEM WITH ANONYMITY REVOKING TRUSTEE

by
Constantin Popescu
Horea Oros

Abstract: In this paper we present a new fair off-line electronic cash system which is able of coin tracing and owner tracing. The anonymity of the system can be revokable under certain conditions by an off-line trusted third party. In our scheme the trusted third party verifies the bank's signature of the e-coin and then records the tracing information, which is different from conventional electronic cash system.

Keywords: Cryptography, electronic cash system, revokable anonymity, blind signatures.

1. Introduction

Chaum [7] proposed in 1982 the first electronic payment system based on the technique of blind signatures in order to guarantee the privacy of customers. This complete anonymity of electronic cash system can be used for blackmailing or money laundering. Von Solms and Naccache showed in [14] that anonymity could be used for blackmailing or money laundering by criminals without revealing their identities.

The concept of fair electronic cash system was put forth independently by Brickell [2] and Stadler [15]. It offers a compromise between the need of the privacy protection of customers and effectively preventing the misuse by criminals. On one hand, the bank and the merchant can not obtain the identities of customers by themselves. On the other hand, in the cases where there are suspect criminal activities (e.g. blackmailing or money laundering), the trusted third party, with the help of the bank, can revoke the anonymity of the customer or the coin.

Based on the system of Brands [1], Brickell proposed a fair electronic cash system [2], in which a trustee must be involved in the transactions. Camenisch extended his anonymous payment system [3] to be a fair payment system [5]. Frankel, Tsiounis and Yung proposed a fair off-line electronic cash system [8] which need more communication among the bank, the customers and the merchants.

Also, electronic payment systems with revocable anonymity have been proposed in [6], [10], [11], [13]. In these payment systems trusted third parties are able to revoke the anonymity of the customers in case of suspicious transactions. When illegal acts like blackmailing are disclosed, the trusted third party can block various attacks on payment systems by tracing the coins or the customer.

In this paper, we propose a new fair off-line electronic cash system. The anonymity of users can be revoked in our double spending resistant system and our system has the ability to trace both the electronic coin and the owner of the electronic coin.

This paper is organized as follows. In section 2, we present our fair off-line electronic payment system. Furthermore, we discuss the security of this system in section 3. Finally, we conclude the work of this paper in the last section.

2. Our fair off-line electronic cash system

An electronic cash system is composed of a set of protocols in which three participants are involved: a customer, a merchant and a bank. Basically, three protocols are included in an electronic cash system: withdrawal protocol involving the customer and the bank, payment protocol involving the customer and the merchant and deposit protocol involving the merchant and the bank. In our payment system will be added one more party, the trusted third party, and two more protocols acted between the bank and the trusted third party: customer tracing protocol and coin tracing protocol.

2.1. System parameters

The system parameters consist of a large prime *p*, a large prime factor *q* of *p-1* and an element $g \in \mathbf{Z}_p^*$ of order *q*.

The Trusted Third Party:

The trusted third party executes the following to setup his parameters:

1. Select random secret $x_t \in \mathbf{Z}_q$.

2. Calculate $y_t = g^{x_t} (\bmod p)$.
3. The public key of the trusted third party is y_t.
4. The corresponding secret key is x_t.

The Bank:
The bank executes the following to setup his parameters:

1. Select random secret $x_b \in \mathbf{Z}_q$.
2. Calculate $y_b = g^{x_b} (\bmod p)$
3. The public key of the bank is y_b.
4. The corresponding secret key is x_b.

The Customer:
The customer executes the next steps to setup his parameters:

1. Select random secret $x_u \in \mathbf{Z}_q$
2. Calculate $y_u = g^{x_u} (\bmod p)$
3. The public key of the customer is y_u
4. The corresponding secret key is x_u

2.2.The Withdrawal Protocol

The withdrawal protocol involves the customer and the bank in which the customer withdraws an electronic coin from the bank.
The customer must to perform the following subprotocol with the bank:

1. The customer sends his electronic cash requirement $m = H(withdrawal\, require \,||\, ID \,||\, time)$ to the bank, where *ID* is the identity of the customer and *H* is a collision-resistant hash function. Then, the customer sign the message *m* using the signature scheme of Nyberg-Rueppel [12]: $r = mg^k (\bmod p)$, $s = x_u r + k (\bmod q)$, where $k \in \mathbf{Z}_q$. The customer sends the signature *(r,s)* to the bank.
2. The bank checks that the following equality holds: $m = g^{-s} y_u^r r (\bmod p)$. Then, the bank uses blind Nyberg-Rueppel signature [4] to sign the e-coin: selects $\bar{k} \in \mathbf{Z}_q$ and computes $\bar{r} = g^{\bar{k}} (\bmod p)$. Also, the bank sends $\bar{r}$ to the customer and stores $\bar{r}$ linked with the customer's identity.

3. The customer establishes a coin c, randomly selects $\alpha, \beta \in \mathbf{Z}_q$, computes $r_b = cg^{\alpha}\overline{r}^{\beta} (\bmod p)$ and blind the e-coin by computing $c' = r_b \beta^{-1} (\bmod q)$. The customer sends the value c' to the bank.
4. The bank computes $\overline{s} = c' x_b + \overline{k} (\bmod q)$ and forwards $\overline{s}$ to the customer.
5. The customer computes $s_b = \overline{s}\beta + \alpha (\bmod q)$. The pair (r_b, s_b) is a valid e-coin signature issued by the bank.

The customer has to perform the following subprotocol with the trusted third party:

1. The customer sends $(c, \overline{r}, r_b, s_b)$ to the trusted third party.
2. The trusted third party verifies the signature of blinded coin: $g^{-s_b} y_b^{r_b} r_b = c (\bmod p)$. The trusted third party chooses a random number $k_t \in \mathbf{Z}_q$ and computes: $r_t = cg^{k_t} (\bmod p)$, $s_t = x_t r_t + k_t (\bmod q)$. Finally, the trusted third party sends the pair (r_t, s_t) to the customer.

The e-cash is represented by the tuple (c, r_b, s_b, r_t, s_t).

2.3.The Payment Protocol

The payment protocol involves the customer and the merchant in which the customer pays the electronic coin to the merchant.

1. The customer sends the tuple $(c, \overline{r}, r_b, s_b)$ to the merchant.
2. The merchant verifies the validity of the signature (r_b, s_b) by checking that the following equality holds:
$$g^{-s_b} y_b^{r_b} r_b = c (\bmod p) \qquad (1)$$
3. The merchant verifies the validity of the signature (r_t, s_t) by checking that the following equality holds:
$$g^{-s_t} y_t^{r_t} r_t = c (\bmod p) \qquad (2)$$

If the equalities (1) and (2) hold, then the merchant will accept the coin from the customer.

2.4. The Deposit Protocol

The deposit protocol involves the merchant and the bank as follows (the merchant deposits his electronic coins to the bank):

1. The merchant sends the e-cash (c, r_b, s_b, r_t, s_t) to the bank.
2. The bank verifies the validity of the e-coin using the same operations as the merchant (see steps 2 and 3 from subsection 2.3).
3. The bank checks whether the coin has been double spent. If the coin was not deposited before, the bank accepts the coin and will deposit the e-cash to the account of the customer. Then the merchant sends the goods to the customer.

If the coin was deposited before, then the bank requests the trusted third party that the identity of the dishonest customer to be revoked.

2.5. The Customer Tracing Protocol

The customer tracing protocol involves the bank and the trusted third party. This protocol is used to determine the identity of the customer in a specific payment transaction. Money laundering can be prevented from detecting the identity of the illegal customer in this protocol.

The customer tracing protocol is as follow:

1. The bank sends the e-coin (c, r_b, s_b, r_t, s_t) to the trusted third party.
2. The trusted third party verifies the validity of the e-coin using the same operations as the merchant (see steps 2 and 3 from subsection 2.3) and then sends $\bar{r}$ to the bank. Note that $\bar{r}$ is linked with the coin *c*.
3. The bank can find the corresponding customer from his database (saved in the withdrawal protocol).

2.6. The Coin Tracing Protocol

The coin tracing protocol involves the bank and the trusted third party. This protocol determines the e-coin in the case when the blackmailing occurs. The blackmailing can be prevented in this protocol.

The coin tracing protocol is as follow:

1. The customer sends his identity, *ID*, to the bank.
2. The bank sends $\bar{r}$ to the trusted third party.
3. The trusted third party finds the corresponding coin *c* and then sends the coin *c* to the bank.

4. The bank can reject the coin *c*.

3. Security Analysis

We will analyze the security of the proposed fair off-line electronic cash system in this section.

Theorem 1. *If the blind signature scheme is secure against forgery then the proposed e-cash system is secure against forgery of the coin.*

Proof. If a dishonest customer tries to forge a valid e-coin, he must to generate a valid blind signature of the bank, (r_b, s_b). Since solving a discrete logarithm problem is infeasible (i.e. from the public key of the bank, $g^{x_b} (\text{mod } p)$, the customer can not compute the secret key of the bank, x_b) we can say that the forgeability of the coin is impossible.

Theorem 2. *The anonymity of customers can be removed with the cooperation between the bank and the trusted third party in certain special cases.*

Proof. The trusted third party records each pair $(c, \bar{r})$ in the withdrawal protocol and $\bar{r}$ is linked with the identity of the customer. He can checks in his database the tracing information and provides it to the bank.

Theorem 3. *The proposed fair off-line electronic cash system can protect the customer's privacy and keep the system anonymous.*

Proof. Since the blind Nyberg-Rueppel signature (r_b, s_b) can not give any information for the coin *c*, the bank can not link the blind coin with the identity of the customer. Therefore, it is infeasible for the bank to trace honest customers without the help of the trusted third party. Also, in the payment protocol, the merchant can only verify the e-coin of the customer and the identity of the customer is anonymous.

4. Conclusion

In this paper we proposed a new fair off-line electronic cash system with anonymity revoking trustee. Customer's anonymity can be removed by proceeding owner tracing and coin tracing under cooperating of the bank and the trusted third party. The security of our system is based on the discrete logarithm problem.

References:

[1] **S. Brands**, *Untraceable off-line cash in wallet with observers*, Advances in Cryptology-CRYPTO'93, Lecture Notes in Computer Science, vol. 773, Springer-Verlag, pp. 302-318, 1993.

[2] **E. Brickell, P. Gemmel, and D. Kravitz**, *Trustee-based tracing extensions to anonymous cash and the making of anonymous change*, Proceedings of The 6th ACM-SIAM, pp. 457-466, 1995.

[3] **J. Camenisch, J. Piveteau, M. Stadler**, *An efficient payment system protecting privacy*, Proceedings of ESORICS'94, Lecture Notes in Computer Science, vol. 875, Springer-Verlag, pp. 207-215, 1994.

[4] **J. Camenisch, J. Piveteau, M. Stadler**, *Blind Signatures Based on the Discrete Logarithm Problem*, Advances in Crypology - EUROCRYPT '94, LNCS, vol. 950, Springer Verlang, pp. 428-432, 1995.

[5] **J. Camenisch, J. Piveteau, M. Stadler**, *An efficient fair payment system*, Proceedings of ACM Conference on Computer and Communications Security, pp. 88-94, 1996.

[6] **J. Camenisch, U. Maurer, M. Stadler**, *Digital Payment Systems with Passive Anonymity-Revoking Trustees*, Journal of Computer Security, vol. 5, number 1, IOS Press, 1997.

[7] **D. Chaum**, *Blind signatures for untraceable payments*, Proceedings of EUROCRYPT'82, pp. 199-203, 1983.

[8] **Y. Frankel, Y. Tsiounis, M. Yung**, *Indirect discourse proofs: Achieving efficient fair off-line e-cash*, Advances in Cryptology-ASIACRYPT'96, Lecture Notes in Computer Science, vol. 1163, Springer-Verlag, pp. 286-300, 1996.

[9] **A. Juels**, *Trustee tokens: Simple and practical anonynous digital coin tracing*, Lecture Notes in Computer Science, vol. 1648, Springer-Verlag, pp. 33-43, 1999.

[10] **M. Lee, G. Ahn, J. Kim, J. Park, B. Lee, K. Kim, and H. Lee**, *Design and implementation of an efficient fair off-line e-cash system based on elliptic curve discrete logarithm problem*, Journal of Communications and Networks, vol. 4(2), pp. 81-89, 2002.

[11] **G. Maitland, C. Boyd**, *Fair electronic cash based on a group signature scheme*, Proceedings of ICICS 2001, Lecture Notes in Computer Science, Springer-Verlag, pp. 461-465, 2001.

[12] **K. Nyberg, R.A. Rueppel**, *A new signature scheme based on the DSA giving message recovery*, Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 58-61, 1993.
[13] **C. Popescu**, *An Off-line Electronic Cash System with Revokable Anonymity*, Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference, Dubrovnik, Croatia, pp. 763-767, 2004.
[14] **B. von Solms, D. Naccache**, *On blind signatures and perfect crimes*, Computers and Security, 11(6), pp. 581-583, 1992.
[15] **M. Stadler, J.M. Piveteau, and J. Camenisch**, *Fair blind signatures*, Proceedings of Eurocrypt'95, pp. 209-219, 1995.

Authors:

Constantin Popescu - University of Oradea, Romania, E-mail address: cpopescu@uoradea.ro
Horea Oros - University of Oradea, Romania, E-mail address: horos @uoradea.ro