An Off-Line Electronic Payment Scheme based on Publicly Verifiable Secret Sharing

Mustapha Hedabou

ENSA de Safi

Route Sidi Bouzid BP 63
46000 Safi. Morocco

ABSTRACT

In this paper, we introduce a new efficient technique allowing to render an off-line e-cash system traceable without need to a trusted party. The main idea is the use of the publicly verifiable secret sharing technique in order to revoke the anonymity of double spending users. The anonymity of honest users is still provided. Security analysis shows that the proposed technique does not undermine the security requirements of a traceable off-line e-cash scheme, including anonymity. A concrete construction of a traceable off-line e-cash system based on a particular blind signature scheme combined with the proposed technique is also given.

General Terms

Identity Based Cryptography, Electronic Payment.

Keywords

E-cash; Blind signature; Threshold secret sharing.

1. INTRODUCTION

Recently, there have been many electronic cash (e-cash) protocols proposed with rapid improvement of information technologies and widespread diffusion of communication networks. David Chaum [6] proposed the first electronic payment system based on the technique of blind signatures in order to guarantee the anonymity of clients. How-ever, the complete anonymity of electronic cash system gives rises to the problem of blackmailing and money laundering. Many extended systems which provide valuable functionalities such as anonymity, double spending prevention, unforgeability, untraceability, and efficiency, have been proposed [2, 10]. In the most cases, the main participants in an e-cash system are client, merchant and bank. Based on whether the bank is required to be on-line or not during the transaction, the e-cash systems are classified into on-line e-cash systems [6, 13] and off-line systems [7].

In on-line e-cash systems, the validity of an e-coin is checked before the bank consents its use. Due to the explosive growth of the maintaining database size, the real time validation of an e-coin may cause the service blockage. To overcome this limitation, off-line e-cash systems have been proposed. The transactions are conducted without a prior agreement of a bank. The payment is accepted and a check for a double spending is performed latter by the bank. A blacklist of double spending users is then issued by the bank and the merchant is responsible for checking all received payment slips against their local copies of the blacklist during a payment protocol. The traceability of dishonest users is a major concern for off-line e-cash systems.

The bank and the merchant cannot obtain the identities of clients by themselves since the e-cash systems are designed to provide the anonymity of users. Many works have been proposed in order to obtain a compromise between the need of the privacy protection of clients and effectively preventing the misuse by dishonest users. The concept of fair electronic cash system has been proposed independently by Brickell [4] and Stadler [16]. Only a trusted party is able to trace the identity of users, which is not suitable in the practice. This mechanism has also another problem, called the fair-tracing-problem: No one is able to control the legal usage of tracing, leading to the possibility of illegal tracing.

Camenisch, Maurer and Stadler [17] and independently Frankel et al. [18] proposed fair e-cash schemes with an off-line passive authority: the participation of the trustee is only required in the set-up of the system and for anonymity revocation. The efficiency and the security of these schemes have been improved in [9, 11]. Unfortunately, the unforgeability of the coins relies, in these schemes, on non-standard assumptions. In [12], Kgler and Vogt introduced a new mechanism, called optimistic fair tracing. Their approach doesn't prevent completely the illegal tracing but makes it detectable after-wards by the traced users. However, the decision whether the coins should be traceable or not must be made at the withdrawal phase.

In this paper, we propose a new technique allowing to trace the identity of double spending users on off-line e-cash systems. For this purpose, we suggest to use of publicly verifiable secret sharing technique in order to revoke the anonymity of a double spending user. The identity of client, which acts as a dealer, is split into pieces. At each transaction, one piece is shared with the merchant. The obtained scheme fulfills the security requirements of a traceable off-line e-cash system. This will be achieved in two stages. First, we combine this technique with the ID-based blind signature proposed in [17] to design a concrete traceable e-cash scheme. The general construction showing how this technique can be combined with any blind signature scheme to reveal the identity of double spending users is introduced latter.

This paper is organized as follows. In section 2, we give an introduction to blind signatures and threshold secret sharing schemes. A new off-line e-cash system based on Zang and Kim's blind signature scheme [17] is presented in section 3. Section 4 explains how the publicly verifiable secret sharing technique can be combined with any blind signature to obtain a traceable off-line scheme. In section 5, we analyze the security of the proposed technique and we conclude in section 6.

2. RELATED WORK

In this section, we give an overview of blind signatures, based on bilinear pairing, and threshold secret sharing. Before, we introduce basic facts about bilinear pairing and provide definitions of some mathematical problems. Let G_1, G_2 be two cyclic groups of prime order q, P be a generator of G_1 and H: $\{0, 1\}^* \rightarrow G_1$ be a secure cryptographic hash function. Let e be an admissible map from $G_1 \times G_2$ to G_2, which satisfies the following properties:

- Bilinearity: for any $u, v \in G_1$ and $a, b \in Z_q^*$, we have $e(u^a, v^b) = e(u, v)^{ab}$
- Non-degenerate: there exist $P, Q \in G_1$ such that: $e(P, Q) \neq 1$
- Computability: there is an efficient algorithm to compute $e(u, v)$ for $u, v \in G_1$.

We first introduce the following problems in G_1:

- Discrete logarithm problem (DLP). Given $P, Q \in G_1$, find an integer r such that $Q = rP$.
- Computational Diffie-Hellman problem (CDHP). Given P, aP, bP, compute abP for $a, b \in Z_q^*$.
- Decisional Diffie-Hellman problem (DDHP). Given P, aP, bP, cP, decide whether $c = ab$ for $a, b, c \in Z_q^*$.
- ROS problem. Given an oracle access to a random function F: $Z_q^l \rightarrow Z_q$, find coefficients $a_{k,i} \in Z_q^*$ and a solvable system of $l + 1$ equations in the unknowns $c_1, c_2, \cdots, c_l$ over Z_q^* : $a_{k,1}c_1 + \cdots + a_{k,l}c_l = F(a_{k,1}, \cdots, a_{k,l})$ for $k = 1, 2, \cdots, t, t \geq l + 1$.

G_1 is a gap Diffie-Hellman group if the Decisional Deffie-Hellman problem (DDHP) can be solved in polynomial time but there is not polynomial time algorithm to solve the computational Deffie-Hellman problem (CDHP) and Discrete logarithm problem (DLP). More details can be found in [3].

2.1 Blind signature schemes

Blind signature, firstly introduced by Chaum [6] in 1982, plays the central role in cryptographic protocols to provide the anonymity of users in e-cash or e-voting systems. In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a user and a signer. It allows the user to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. Several blind signature schemes based on pairings have been proposed [5, 17, 18]. In this paper we highlight the ID-based blind signature scheme proposed by Zhang and Kim [17] in Asiacrypt 2002. The security of this scheme depends on the intractability of the ROS-problem.

First the PKG (public key generator) picks a random integer s, compute $P_{pub} = sP$ and sets the public parameters $< p, G_1, G_2, P, P_{pub}, e, H >$, where G_1 is a gap Diffie-Hellman group. The public key of the PKG is P_{pub} and s is its private key (master key). For each signer with identity ID, the PKG sets its private key as $S_{ID} = sQ_{ID}$, where $Q_{ID} = H(ID)$. The blind signature of a message m is performed as follows:

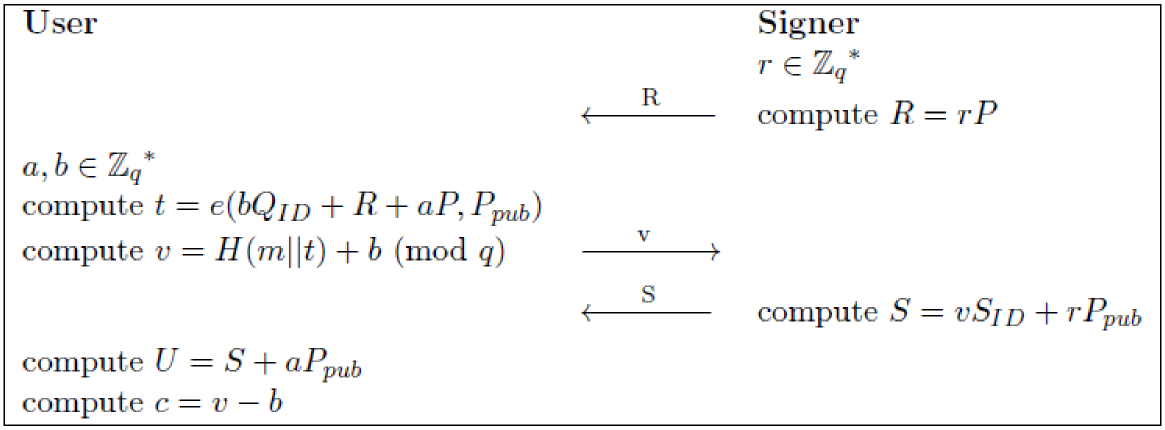
User
Signer
$r \in \mathbb{Z}_q^*$
R
compute $R = rP$
$a, b \in \mathbb{Z}_q^*$
compute $t = e(bQ_{ID} + R + aP, P_{pub})$
compute $v = H(m||t) + b \pmod q$
v
S
compute $S = vS_{ID} + rP_{pub}$
compute $U = S + aP_{pub}$
compute $c = v - b$

Fig 1: Zhang and Kim's Blind signature scheme

The blind signature of the message m is (m, U, c).

• Verification: the signature is valid if the following equation holds

$$c = H(m||e(U, P)e(Q_{ID}, P_{pub})^{-c})$$

2.2 Threshold secret sharing

The aim of threshold cryptography is to protect a key by sharing it amongst a number of entities in such a way that only a subset of minimal size, namely the threshold $t + 1$, can use the key. No information about the key can be learnt from t or less shares. The setup of a threshold scheme typically involves a Distributed Key Generation (DKG) protocol. In a DKG protocol, a group of entities cooperate to jointly generate a key pair and obtain shares of the private key. These shares can then be used to sign or decrypt on behalf of the group. The benefits of a threshold scheme are increased security, because an adversary can compromise up to t devices, and resilience, since any subset of $t + 1$ devices is sufficient. The entity responsible of sharing the secret parts is called dealer. Shamir's early idea [14] of distributing shares of a secret as evaluations of a polynomial has become a standard building block in threshold cryptography. The scheme is based on polynomial interpolation. Given k couples (x_i, y_i), with distinct x_i's, there is one and only one polynomial $q(x)$ of degree k–1 such that $q(x_i) = y_i$ for all i. Without loss of generality, we can assume that the secret D is a number. To divide it into pieces D_i, we pick a random k–1 degree polynomial $q(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ in which $a_0 = D$, and evaluate:

$$D_1 = q(1), \cdots, D_i = q(i), \cdots, D_n = q(n).$$

Given any subset of k of these D_i values (together with their identifying indices), we can find the coefficients L_i of $q(x)$ by interpolation, and then evaluate

$$D = q(0) = \sum_{i=1}^{k-1} L_i D_i, \text{ where } L_i = \prod_{i \neq j}\left(\frac{x_j}{(x_j - x_i)}\right)$$

On the other hand, the Knowledge of just k–1 of D_i does not suffice to recover D.

The basic secret sharing scheme will have some flows if some participants are dishonest [8]. For withstanding malicious participants, a new type of secret sharing scheme was proposed by Fieldman [8], called the verifiable secret sharing (VSS) scheme. The coefficients of this polynomial hidden in the exponent of the generator of a group, in which the discrete-log assumption holds, are published. This allows that the participants can validate correctness only of their own shares distributed by the dealer in the distribution phase. In [15], Stadler introduced the publicly verifiable secret sharing (PVSS) scheme that allows that anyone can verify the validity of shares without revealing any secret information.

3. A NEW OFF-LINE TRACEABLE E-CASH SYSTEM

Now, we introduce an off-line e-cash system based on Zang and Kim's blind signature scheme combined with the publicly verifiable secret sharing technique. The secret identity of the client is split into pieces. The client, who acts as a dealer, shares one piece with the merchant at each transaction. The merchant is able to check the validity of the share. Thus, if an e-coin is spent at least twice, the bank will have at least 2 shares and then be able to reconstruct the secret identity of the client.
The particular choice of the blind signature scheme proposed by Zang and Kim is made as an example to show how the publicly verifiable secret sharing technique can be used to achieve an off-line traceable e-cash system. This choice is not justified by any security or efficiency reasons.

The parameters of the proposed e-cash scheme are $< p, G_1, G_2, P, P_{pub}, e, H >$ as described in the previous section. In our scheme, the central bank, acts like a PKG, authorizes a bank to issue e-coins. For this purpose, the central bank generates the private key of the bank $S_{ID} = sQ_{ID}$, where $Q_{ID} = H(ID)$ and ID is identity of the bank.

To achieve a transaction, four sub protocols are required: withdrawal protocol, payment protocol, deposit protocol and tracing protocol, which is performed only when an e-coin is spent twice.

• **Withdrawal protocol**: A client with identity id sends information about his account and a request for a blindly signed e-coins m to the bank. The withdrawal protocol is done as follows:

The bank chooses randomly an integer $r \in Z_q^*$, computes $R = rQ_{ID}$ and sends R to the client.

The client chooses randomly two integers $a, b \in Z_q^*$, and sets $q(x) = id + ax + bx^2$. Computes $A_0 = idP, A_1 = aP, A_2 = bP, t = e(bQ_{ID} + R + aP, P_{pub})$ and

$v = H(m||A_0||A_1||A_2||t) + b \pmod q$, and sends v to the bank.

The bank computes $S = vS_{ID} + rP_{pub}$ and sends it back to the client.

The client computes $U = S + aP_{pub}$, $c = v - b$ and verifies the validity of the blind signature by checking whether the following equality holds:

$$c = H(m||A_0||A_1||A_2||e(U, P)e(Q_{ID}, P_{pub})^{-c})$$

If the above equality does not hold, the blind signature (m, U, c) is not a valid blind signature of the e-coin m. Otherwise, the client has withdrawn a $cash = (m, U, c, A_0, A_1, A_2)$. The client stores $(cash, a, b)$.

• **Payment protocol**: The client executes the payment protocol with the merchant as follows:

1. The client sends *cash* to the merchant.

2. The merchant checks the validity of the coins. If the coin is valid, the merchant continues the next step,

otherwise, refuses the coin.

3. The merchant generates a challenge $ch \in \{0, 1\}^*$ and sends it to the client.

4. The client computes $q(ch)$ and sends it to the merchant.

5. The merchant verifies the transaction record (*cash, ch, q*(*ch*)) by checking the validity of the share. This is done by checking whether the following equality holds.

$$e(q(ch)P, Q) = \prod_{i=0}^{i=3} e(A_i, Q)^{ch^i}$$

If the equality holds, then the merchant agrees to transact with the client. Otherwise, the merchant refuses the transaction with the client.

The verification of the validity of a share requires only the public information. The correctness of the verification equality is justified by the following equations:

$$\begin{aligned}\prod_{i=0}^{i=3} e(A_i, Q)^{ch^i} &= e(A_0, Q)e(A_1, Q)^{ch}e(A_2, Q)^{ch^2}\\ &= e(idP, Q)e(aP, Q)^{ch}e(bP, Q)^{ch^2}\\ &= e(idP, Q)e(a.chP, Q)e(b.ch^2P, Q)\\ &= e(idP + a.chP + b.ch^2P, Q)\\ &= e(q(ch)P, Q)\end{aligned}$$

- **Deposit protocol**: Involves the merchant and the bank. First, the merchant sends the transaction record (*cash, ch, q*(*ch*)) to the bank. The bank searches the database to check whether cash has existed. If the cash is new, the bank deposits the value to the merchant's account and stores (*cash, ch, q*(*ch*)) in its database. Otherwise, the bank traces the double-spending client.

- **Tracing protocol**: The anonymity of a double spending user will no longer be assured. Indeed, if an e-coin is spent at least twice, then there will be two transaction records (*cash*, ch_1, $q(ch_1)$), and (*cash*, ch_2, $q(ch_2)$), with two different challenges ch_1 and ch_2. Since $q(x) = id + ax + bx^2$, we have

$$id = \sum_{i=1}^{i=2} L_i\, q(ch_i),$$

where L_i denotes the appropriate Lagrange coefficients.

4. THE GENERAL CONSTRUCTION

To render an off-line e-cash system traceable, we use the (2, *n*) publicly verifiable secret sharing technique (PVSS). The client acts as a dealer and splits his secret identity into pieces. At each transaction, the client shares a piece of his identity with the merchant. The use of PVSS allows the merchant to check the validity of the share. If an e-coin is used twice, there will be 2 verifiable shares available. Since a (2, *n*) threshold secret sharing is used, the secret identity of the double spending client can be recovered. Here under, we describe how a (2, *n*) publicly verifiable secret sharing technique can be combined with any blind signature scheme to revoke the anonymity of a double spending user.

- First the client chooses two random integers $a, b \in Z_q^*$, and sets

$$q(x) = id + ax + bx^2$$

- During the Withdrawal protocol, the client uses the chosen random integers *a, b* in the blinding phase to compute the public information allowing to verify the validity of a share. The public information must be concatenated with the message *m* before the use of the hash function.

- In the payment protocol, for every merchant's challenge *ch*, the client computes a share *q*(*ch*) and sends it back to the merchant.

The only change that depends on the used blind signature scheme is the computation of the public information that allows to verify publicly the shares issued in the payment protocol. In fact, it doesn't depend on the blind signature scheme but rather on the underlying mathematical problems. In the previous section, DLP and CDHP are used but the proposed technique can be easily adapted to other mathematical problems. Let's suppose that the discrete log problem is used on a group Z_q^* with a generator *g*. In this case, the public information are $A_0 = g^{id}, A_0 = g^a, A_0 = g^b$. The validity of a share *q*(*ch*) is verified by the following equation:

$$\prod_{i=0}^{i=3} A_i^{ch^i} = g^{q(ch)}$$

The tracing protocol is the same as in the previous section.

5. SECURITY ANALYSIS

In this section, we discuss the effect of the proposed technique on the security of e-cash systems. The process introduced does not change the behavior of the used blind signature scheme. Thus, the obtained off-line e-cash system provides the security functionalities satisfied by the blind signature scheme on which it is based. The anonymity is also satisfied. Indeed, the user identity is hidden into the public information A_0 and cannot be revealed unless an intractable mathematical problem, such as discrete logarithm problem, is solved.
The security of the blind signature scheme proposed by Cha and Cheon is based on the intractability of the ROS problem. When choices are made in such way that the ROS problem is intractable, then the proposed scheme in section 3 meets the security requirements of an off-line e-cash system. The anonymity of honest users is still provided. Indeed, when the bank receives a payment deposit (*cash, ch, q*(*ch*)) it could not link it with the identity of the client. The only information available for the bank is $A_0 = idP$, where *id* is the user's identity. Thus, the only way to uncover the identity of an honest user is to solve the discrete logarithm problem on elliptic curves.

When the discrete logarithm problem is used, as suggest in the general construction, the identity of the client is hidden in $A_0 = g^{id}$. Solving the discrete logarithm problem is then the only way to recover the identity of an honest user.

Consequently, the e-cash scheme obtained by combining the use of the publicly verifiable secret sharing technique with a secure blind signature scheme fulfills the security requirements of an off-line traceable e-cash system.

Furthermore, unlike the others e-cash systems with revocable anonymity, our system doesn't require a trusted party which is clearly an advantage. Indeed, the trusted party is lead to deal with sensitive personal data it has to be totally protected which may causes additional expensive costs. In general, clients are not willing to pay for such extra costs. Others arguments against trusted party, such key escrow, key recovery can be found in [1]. In addition, with our approach, the illegal tracing cannot be a problem anymore since only the anonymity of dishonest users can be revoked.

On the other hand, the proposed technique cannot prevent blackmailing, money laundering or illegal purchases.

6. CONCLUSION

In this paper we have introduced a new technique, based on the use publicly verifiable secret sharing technique, in order to make an off-line e-cash system traceable without need of a trusted party. First, we have used the proposed technique to achieve a traceable off-line e-cash system based on the blind signature of Zhang and Kim. A general construction allowing to combine the proposed technique with any blind signature scheme is also introduced. The security analysis shows that the obtained scheme sill provides the security requirements of a traceable off-line e-cash system.

7. REFERENCES

[1] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, and B. Schneier. *The risks of key recovery, key escrow, and trusted third-party encryption.* Online, available at http://www.cdt.org/crypto/risks98, 1998.

[2] M. Au, W. Susilo, Y. Mu. *Practical anonymous divisible e-cash from bounded accumulators.* In: Proceedings of Financial Cryptography and Data Security, Lecture Notes in Computer Science 5143. Springer-Verlag, pp. 287-301, 2008 .

[3] D. Boneh, M. Franklin. *Identity based encryption from the Weil pairing.* In: Journal of Computing, Vol. 32(3), pp. 586-615, 2003.

[4] P. Brickell, P. Gemmel, and D. Kravitz. *Extensions to anonymous cash and the making of anonymous change.* In: Proceedings of The 6th ACM-SIAM, pp. 457-466, 1995.

[5] J.C. Cha and J.H. Cheon. *An identity-based signature from gap Diffie-Hellman groups.* In: Public Key Cryptography-PKC 2003, LNCS 2139, pp. 18-30, Springer-Verlag, 2003.

[6] D. Chaum. *Blind signatures for untraceable payments.* In: Advances in Cryptology-CRYPTO 82, New York: Plemum Press, pp. 199-203.

[7] D. Chaum, A. Fiat, and M. Naor. *Untraceable electronic cash.* In: Advances in Cryptology-CRYPTO 88, Lecture Notes in Computer Science, 403, Springer Verlag, 1988, pp. 319327.

[8] P. Fieldman. *A practical scheme for non-interactive verifiable secret sharing.* In: 28th Annual Symposium on Foundations of Computer Science, 1987: pp. 427-437.

[9] Y. Frankel, Y. Tsiounis, M. Young. *Fair Off-Line e-cash Made Easy.* In: Asiacrypt98, volume 1514 of LNCS, pages 257-270. Springer-Verlag, 1998.

[10] C. Fun. *Awnership-attached unblinding of blind signatures for untraceable electronic cash.* In: Information Science, 176(3), pp. 263-284, 2006.

[11] M. Gaud, J. Traore. *On the Anonymity of Fair Off-Line e-Cash Systems.* In:Financial Crypto 2003, LNCS 2742, pp. 34-50, 2003.

[12] D. Kgler and H. Vogt. *Fair Tracing without Trustees.* In: Financial Crypto 2001, LNCS 2339, pp. 136-148, 2002.

[13] C. Popescu. *A Fair Off-line Electronic Cash System Based on Elliptic Curve Discrete Logarithm Problem.* In: Studies in Informatics and Control, Volume 14, No. 4, 2005, pp. 291-298.

[14] A. Shamir. *How to share a secret.* In: Communications of the ACM, 22(11): pp. 612-613, 1979.

[15] M. Stadler. *Public verifiable secret sharing.* In: EUROCRYPT, LNCS 1996, 1070: pp. 190-199.

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

[17] F. Zhang and K. Kim. *ID-based blind signature and ring signature from pairings.* In: Asiacrpt2002, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.

[18] F. Zhang and K. Kim. *Efficient ID-based blind signature and proxy signature from bilinear pairings.* In: ACISP 2003. LNCS, vol. 2727, pp. 312-323. Springer, Heidelberg (2003)