International Journal of Hybrid Information Technology
Vol.9, No.1 (2016), pp. 431-442
http://dx.doi.org/10.14257/ijhit.2016.9.1.38

An Untraceable Off-Line Electronic Cash Scheme without Merchant Frauds

Baoyuan Kang and Danhui Xu

School of Computer science and software
Tianjin polytechnic university, Tianjin, 300387, China
baoyuankang@aliyun.com, mixueren123123@sina.com

Abstract

In an electronic cash scheme, there are three participants, the bank, the spender and the merchant. First, a spender opens an account in a bank. Then, he withdraws electronic cash from his account and pays it to a merchant. After checking the electronic cash's validity, the merchant accepts it and deposits it to the bank. There are a number of requirements for an electronic cash scheme, such as, anonymity, unforgeability, unreusability, date attachability, divisibility, transferability and portability. In this paper, we show a recently proposed electronic cash scheme is suffering from some faults in anonymity, expiration date and merchant frauds. To improve the scheme, we propose a new untraceable off-line electronic cash scheme and give a security analysis for it.

Keywords*: Electronic cash, Payment system, Anonymity, Signature scheme, Cryptography*

1. Introduction

Due to the fast progress of computer networks and Internet, information technology is used in electronic commerce. Electronic payment is one of the key issues of electronic commerce development. To realize the digitalization of traditional cash, in 1983, Chaum suggested the first electronic cash scheme [1]. Popularly, in an electronic cash scheme, there are three participants, the bank, the spender and the merchant. First, a spender opens an account in a bank. Then, he withdraws electronic cash from his account and pays it to a merchant. After checking the electronic cash's validity, the merchant accepts it and deposits it to the bank. For security and efficiency, there are a number of requirements for electronic cash scheme, such as, anonymity, unforgeability, unreusability, date attachability, divisibility, transferability and portability [2]. Some of them are listed below:

Anonymity: The spender of a cash must be anonymous. As long as the coin is spent legitimately, neither the merchant nor the bank can identify the spender of the coin.

Unforgeability: Only authorized banks can generate electronic cash.

Unreusability: The electronic cash cannot be reused. The scheme can detect the malicious spenders, who spend the cash twice.

Date attachability: Electronic cash must embody the dates of withdrawing, paying and depositing. These dates can are used to check the expiration date and charge for interest.

Electronic cash schemes can be divided into two categories: online and off-line. In online schemes, as paying a coin to a merchant, the bank must attend to validate the coin and detect its reuse. But, in off-line schemes, double spending can only be figured out when the merchant deposits the coin to the bank in the next phase. After Chaum's scheme, a lot of electronic cash schemes [3-8] have been proposed based on blind signature and restrictive blind signature [9]. Afterward, many more complex schemes have been proposed [10-13]. Recently, Eslami and Talebi proposed an untraceable electronic cash scheme [2] and claimed that their scheme satisfies all main security

ISSN: 1738-9968 IJHIT

requirements, such as, anonymity, unreusability and date attachability. However, Baseri, *et al.*, [14] showed that Eslami and Talebi's scheme is subjected to some weaknesses in perceptibility of double spender, unforgeability and date attachability. Baseri, *et al.*, also contributed an electronic cash scheme and claimed that their scheme is immune to the weaknesses of Eslami and Talebi's scheme. But, as we show in this paper, Baseri, *et al.*,'s scheme is suffering from some faults in anonymity, expiration date and merchant frauds. To improve Baseri, *et al.*,'s scheme, we also propose a new untraceable off-line electronic cash scheme. The new scheme not only possesses the features, such as anonymity, unforgeability, unreusability, but also possesses the feature of avoiding merchant frauds.

The remainder of this paper is organized as follows. Some basic concepts are introduced in Section 2. In Section 3, we review Baseri, *et al.*,'s scheme and show its weaknesses. In Section 4 we propose a new electronic cash scheme. Security analysis of our scheme is covered in Section 5. Performance comparisons are shown in Section 6. We finally conclude in Section 7.

2. Preliminaries

2.1 RSA Cryptosystem

A RSA cryptosystem [15] can be determined by a set (p,q,n,e,d). Where p and q are two large prime numbers, $n=pq$ and $ed=1(\mathrm{mod}\,\phi(n))$. Here $\phi(n)=(p-1)(q-1)$. $(p,q,d)$are private while (n,e) are public. For encrypting the plain text m, one calculates the cipher c as $c=m^e(\mathrm{mod}\,n)$. For decrypting c, one calculates the plain text m as $m=c^d(\mathrm{mod}\,n)$.

2.2 Blind Signatures

In 1983, Chaum proposed a blind signature scheme [1] based on the RSA cryptosystem. Blind signatures can be applied to preserve the anonymity of users against leaking user information to the signer, such as, in electronic cash payment and electronic voting schemes. A typical blind signature scheme involves two participants: a signer and a signature requester. The signature requester need the signature of the signer on one message m. But the requester does not wish to leak the content of m to the signer. Hence, the requester chooses a random number b as a blinding factor and sends $b^e m$ (e is the signer's public key in RSA cryptosystem) to the signer. The signer computes $(b^e m)^d$ (d is the signer's private key related to public key e). Since $(b^e m)^d = bm^d$, the requester can obtain the signature m^d on m by multiplying $(b^e m)^d$ by b^{-1}.

3. Baseri et al.'s Scheme and its Failures

In this section, we first review Baseri et al.'s scheme [14]. Then we show its failures.

3.1 Baseri, *et al.*,'s scheme

There are four participants in the scheme: a Central Authority, the Bank, the Spender and the Merchant. The scheme contains five phases: initialization, withdrawal, payment, deposit and exchange.

3.1.1 Initialization: In this phase, the central authority should set some public parameters. There parameters include two publicly known elements, g_1, g_2, of the same

large prime order, l in Z_n^*. Here $n = pq$ and p , q are two large prime numbers. H is a one-way hash function. In addition, each authenticated participant involved in the system should determine his own parameters and get a certificate for its own public key from certification authority. The required parameters of the bank are two RSA public/private key pairs $((e_B, n), 1/e_B)$ and $((e_B{}', n), 1/e_B{}')$ such that $e_B > e_B{}'$.

3.1.2 Opening an Account: To open an account, the customer should identify himself to the bank. Authenticating the customer, the bank stores his identity information in its account database. This process is done in the following steps.

Step 1. The customer:

(a) Identifies himself by means of official documents, like a passport or some other identification.

(b) Generates a random number, $u \in_R Z_n^*$, and keeps it as his own secret identity information which is unknown to any other, unless he spends a coin more than one time.

(c) Computes:
$ID_c = g_1^u (\mathrm{mod}\, n)$ as his identity, such that $g_1^u g_2 \neq 1 (\mathrm{mod}\, n)$.

(d) Send ID_c to the bank.

(e) Provides a zero knowledge proof that he knows the discrete logarithm of ID_c, which respect to g_1.

Step 2. The bank B:

(a) Checks the identity and the zero knowledge proof offered by the customer.

(b) Stores the identity information of the customer in the account database.

(c) Computes A and O_1 as its own signature on A:
$A = ID_C g_2 (\mathrm{mod}\, n)$,
$O_1 = A^{1/e_B} (\mathrm{mod}\, n)$.

(d) Sends A and O_1 to the customer.

3.1. 3. Withdrawal: Before withdrawing and asking for a coin, the spender should prove his/her ownership of the account to the bank. The spender should prove his identity in a similar way to the withdrawal of classical cash from an account (*i.e.,* by offering his passport or driving license). In addition, he should refer to a bulletin board in which the bank periodically publishes the fresh time by two parameters, t and $e_B * t (\mathrm{mod}\, \phi(n))$. Time t is constant during the period and used to synchronize customers and the bank in the withdrawing process and to determine the validation time of coins. Note that $t * e_B$ plays the role a public key for the bank and is chosen in such a way that its reverse (*i.e.,* $1/(e_B * t) (\mathrm{mod}\, \phi(n))$) exists. The coin is represented by a five-tuple (A', B, s_1, s_2, s_3) constructed in the following steps

Step 1. The spender S:

(a) Chooses three random numbers, $x_1, x_2 \in_R Z_{e_B'}^*$ and $s \in_R Z_n^*$, and two blinding factors $b_1, b_2 \in Z_n^*$.

(b) Computes:

- $A' = A^s \left(\mathrm{mod}\, n\right)$,
- $B = g_1^{x_1} g_2^{x_2} \left(\mathrm{mod}\, n\right)$,

- $\omega_1 = Bb_1^{e'_B} \pmod n$,
- $\omega_2 = (A' + B) b_2^{(e_B * t)} \pmod n$.

(c) Sends ω_1, ω_2, t to the bank.

Step 2. The bank B:

(a) Checks the validity of the Date/Time slip.

(b) Signs ω_1 and ω_2 by computing:

- $O_2 = \omega_1^{1/e_B^1} \pmod n$,
- $O_3 = \omega_2^{1/(e_B * t)} \pmod n$.

(c) Sends O_2 and O_3 to the spender.

Step 3. The spender S:

(a) Verifies the signatures of the bank on A, ω_1, ω_2.

(b) Obtains the signatures of the bank on A', B and $A' + B$, which are signed with private keys $1/e_B$, $1/e'_B$ and $(1/(e_B * t))$, respectively:

- $s_1 = O_1^s \pmod n = sign_B(A')$,
- $s_2 = O_2 / b_1 \pmod n = sign_B(B)$,
- $s_3 = O_3 / b_2 \pmod n = sign_B(A' + B)$.

The $Coin$ is $(A', B, s_1, s_2, s_3, t)$.

3.1.4 Payment: When the spender wants to spend his coin at the shop, the following steps are done:

Step 1. The spender S:

(a) Sends A', B, s_1, s_2, s_3, t to the merchant M.

Step 2. The merchant M:

(a) Verifies if $A' \neq 0$.

(b) Checks the expiration date of the coin.

(c) Verifies the signatures, s_1, using the public key, e_B, s_2 using the public key, e'_B and s_3, and using the public key $(e_B * t)$.

(d) Computes:

- The challenge $d = H(A', B, ID_M, date \| time)$ in which H is the hash function determined in the initialization phase, ID_M is the identity of the merchant and $date \| time$ represents the date and time of the transaction.

(e) Sends d to the spender.

Step 3. The spender S:

(a) Computes:

- $r_1 = dus + x_1 \pmod{e_B}$,
- $r_2 = ds + x_2 \pmod{e_B}$.

(b) Sends r_1 and r_2 to the merchant.

Step 4. The merchant M:

(a) Accepts the coin if $g_1^{r_1} g_2^{r_2} = A'^d B$.

3.1.5 Deposit: In this phase, the following process is done between the bank B and the merchant M:

Step 1. The merchant M:

Sends the transcript of each electronic coin (i.e. $Coin$, r_1, r_2) to the bank.

Step 2. The bank B:

(a) Checks the authenticity of the merchant and verifies the transcript of the received coin.

(b) Checks whether the coin exists in its deposit or exchange tables or not. If the coin exists, it runs the double spender detection procedure, else, accepts the coin, stores it in the deposit table and transfers money to the merchant.

3.1.5.1. Double Spender Detection Procedure: Suppose that a malicious spender spends the same coin twice or more. Suppose that the malicious spender first spender the coin, along with d', r_1' and r_2', the bank finds out that the coin already exists in its tables. At that time, using the relation between r_1, r_2, d and consequently between r_1', r_2', d', it computes the identity of the malicious spender by the following equations:

- $u = \frac{r_1 - r_1'}{r_2 - r_2'} \left(\mathrm{mod}\, e_B\right)$,
- $ID_C = g_1^u \left(\mathrm{mod}\, n_B\right)$.

3.1.6 Exchange: In this phase, referring to the bank, the customer can exchange his old coin (which is not outdated) with new coins and update the expiration date of his own coin. To control the size of its database, this affair is undertaken by the following procedure:

Step 1. The customer:

(a) Offers his coin, besides his identity, to the bank.

Step 2. The Bank B:

(a) Checks deposit and exchange tables to ensure that the coin has nit already been exchanged or spent.
(b) Checks the authenticity of the customer and verification of the coin similar to the validation checking of the payment phase.
(c) Runs the withdrawal phase of the protocol.
(d) Updates the exchange table by inserting the information of the customer and the old coin.

3.2 Weaknesses of Baseri, *et al.*,'s scheme

In this subsection, we show some weaknesses of Baseri et al.'s scheme.

3.2.1 First Fault: Attacking Expiration Date: During time t period, after successfully withdrawing a coin $\left(A', B, s_1, s_2, s_3, t\right)$, the spender can forgery a coin

$$\left(A'^*, B^*, s_1^*, s_2^*, s_3^*, t'\right)$$

in time t' period. Here

$$A'^* = A',\ B^* = B,\ s_1^* = s_1, s_2^* = s_2, s_3^* = s_3^{t/t'}.$$

Since

$$s_3^* = s_3^{t/t'} = ((A' + B)^{1/e_B * t})^{t/t'} = (A' + B)^{1/e_B * t'} = (A'^* + B^*)^{1/e_B * t'}.$$

So, s_1^*, s_2^* and s_3^* are the signatures of the bank on A'^*, B^* and $A'^* + B^*$ in time t' period, which are signed with private keys $1/e_B$, $1/e'_B$ and $\left(1/\left(e_B * t'\right)\right)$, respectively. Furthermore, in payment, the spender computes r_1^* and r_2^* using same number s, x_1 and x_2 in withdrawing the coin $\left(A', B, s_1, s_2, s_3, t\right)$. Let $d^* = H\left(A'^*, B^*, ID_M, date \| time\right)$. Obviously, $g_1^{r_1^*} g_2^{r_2^*} = A'^{*d^*} B^*$ holds. Hence, $\left(A'^*, B^*, s_1^*, s_2^*, s_3^*, t'\right)$ is valid coin in time t' period.

Note 1 This attack is only an expiration date attack. If the spender spends $\left(A', B, s_1, s_2, s_3, t\right)$ in time t period, and also spends $\left(A'^*, B^*, s_1^*, s_2^*, s_3^*, t'\right)$ in time t' period, the bank can finds out the malicious spender. But if the spender only spends the coin $\left(A'^*, B^*, s_1^*, s_2^*, s_3^*, t'\right)$ in time t' period, the bank cannot finds out the malicious spender

3.2.2 Second Fault: Fault on Preventing Merchants Frauds: In practice, there are always many merchants from different shops. When merchant M_1 receives a coin $\left(A', B, s_1, s_2, s_3, t\right)$ from a spender who wants to buy goods from the merchant M_1, malicious merchant M_1 may send $\left(A', B, s_1, s_2, s_3, t\right)$ to a merchant M_2 to spend. When M_2 sends $d = H\left(A', B, ID_{M_2}, date \| time\right)$ to M_1, M_1 sends d to the spender . After receiving (r_1, r_2) from the spender, M_1 sends (r_1, r_2) to M_2. Since (r_1, r_2) satisfies $g_1^{r_1} g_2^{r_2} = A'^d B$. So, malicious merchant M_1 can spend the spender's coin $\left(A', B, s_1, s_2, s_3, t\right)$ to another merchant M_2. Due to lacking necessary authentication, in the above process, the spender cannot find any fraud. When the spender asks goods to M_1, M_1 can refuse him by saying something is wrong with the verification in payment phase. So, M_1 successfully carries out fraud. Baseri et al.'s scheme is not a practical scheme.

3.2.3 Third Fault: Fault on Anonymity: First we note that in Baseri, *et al.*,'s scheme coins have format $\left(A' = A^s, B, s_1, s_2, s_3, t\right)$. Now we define coin $\left(A^m, B, s_1, s_2, s_3, t\right)$, $m \in Z_n$ as same roots coins with same B determined by random numbers $x_1, x_2 \in {}_R Z^*_{e'_B}$. When a spender send two same roots coins $\left(A^{m_1}, B, s_1, s_2, s_3, t\right)$ and $\left(A^{m_2}, B, s_1^*, s_2, s_3^*, t'\right)$ to a merchant. Assumed $t' > t$ .The merchant may deliberately send

$$d = d_2 = d_1 = H\left(A^{m_1}, B, ID_M, date \| time\right)$$

to the spender. When the merchant receives (r'_1, r'_2) , he can compute the private key u of the spender using (r_1, r_2) related to d_1. Sine

$$r_1 = m_1 du + x_1 \left(\bmod e_B\right),\ r_2 = m_1 d + x_2 \left(\bmod e_B\right)$$

$$r_1' = m_2 du + x_1 \left(\bmod e_B\right),\ r_2' = m_2 d + x_2 \left(\bmod e_B\right).$$

The merchant can obtain the spender secret identity information $u = \frac{r_1 - r_1'}{r_2 - r_2'} \left(\mathrm{mod}\, e_B\right)$.
This violates the anonymity requirement of electronic cash.

Note 2 This attack is different from double spender detection, because

$$\left(A^{m_1}, B, s_1, s_2, s_3, t\right) \neq \left(A^{m_2}, B, s_1^*, s_2, s_3^*, t'\right)$$

They are different coins. This attack indicates that among the random numbers, $x_1, x_2 \in {}_R Z_{e_B'}^*$ and $s \in {}_R Z_n^*$ in Baseri et al.'s scheme , x_1, x_2 are useful to protect the anonymity , but s is almost no use. For security, spenders must choose different x_1, x_2 every time.

4. The Proposed Scheme

To overcome the weaknesses of Baseri, *et al.*,'s scheme, we proposed an improved electronic cash scheme. In our scheme there are also four participants: a Central Authority, the Bank, the Spender and the Merchant and the improved scheme contains five phases: initialization, withdrawal, payment, deposit and exchange. Initialization, deposit and exchange are as same as that of Baseri, *et al.*,'s scheme. Here we only describe the withdrawal and payment phases.

Withdrawal phase

To withdrawing and asking for a coin (A', B, s_1, s_2, s_3) the following process is done:

Step 1. The spender S:

(a) Randomly Chooses $x_1, x_2 \in {}_R Z_{e_B'}^*$ and $s, b_1, b_2 \in {}_R Z_n^*$

(b) Calculates: $A' = A^s \left(\mathrm{mod}\, n\right)$, $B = g_1^{x_1} g_2^{x_2} \left(\mathrm{mod}\, n\right)$,

$$\omega_1 = B^{t+s} b_1^{e_B'} \left(\mathrm{mod}\, n\right), \quad \omega_2 = \left(A' + B^{t+s}\right) b_2^{(e_B * t)} \left(\mathrm{mod}\, n\right).$$

(c) Sends t, ω_1, ω_2 to the bank.

Step 2. The bank B:

(a) Checks the validity of the Date/Time.

(b) Signs ω_1 , ω_2 by generating:

$$O_2 = \omega_1^{1/e_B'} \left(\mathrm{mod}\, n\right), \; O_3 = \omega_2^{1/(e_B * t)} \left(\mathrm{mod}\, n\right).$$

(c) Sends O_2 and O_3 to the spender.

Step 3. The spender S:

(a) Verifies the following equations

$$O_2^{e_B'} = \omega_1 \left(\mathrm{mod}\, n\right) \; , \; O_3^{e_B * t} = \omega_2 \left(\mathrm{mod}\, n\right)$$

(b) Gains the three signatures s_1, s_2, s_3 of the bank on A' , B^{t+s} and $A' + B^{t+s}$, respectively.

$$s_1 = O_1^s \left(\mathrm{mod}\, n\right), s_2 = O_2 / b_1 \left(\mathrm{mod}\, n\right), s_3 = O_3 / b_2 \left(\mathrm{mod}\, n\right).$$

The *Coin* is $\left(A', B^{t+s}, s_1, s_2, s_3, t\right)$.

Payment phase

To spend a coin at the shop, the following steps are done

Step 1. The spender S:

(a) Sends $\left(A', B^{t+s}, s_1, s_2, s_3, t\right)$ to the merchant M.

Step 2. The merchant M:

(a) Checks the expiration date of the coin.

(b) Verifies the three signatures, s_1, s_2, s_3 of the bank on A', B^{t+s} and $A'+B^{t+s}$, respectively, via the following formulas

$$s_1^{e_B} = A', \quad s_2^{e_B'} = B^{t+s}, \; s_3^{e_B \cdot t} = A' + B^{t+s}$$

(c) Computes $d = H\left(A', B^{t+s}, ID_M, date \| time\right)^{1/e_M}$, Here H is the hash function determined in the initialization phase, e_M is the public key of the merchant, ID_M is the identity of the merchant and $date \| time$ represents the date and time of the transaction.

(d) Sends d and $date \| time$ to the spender.

Step 3. The spender S:

(a) Verifies the signature d of the merchant, using the public key e_M of the merchant M via the following formulas

$$d^{e_M} = H\left(A', B^{t+s}, ID_M, date \| time\right)$$

(b) Computes

$$r_1 = dus + (t+s)x_1 \left(\bmod e_B\right), \; r_2 = ds + (t+s)x_2 \left(\bmod e_B\right).$$

(c) Sends r_1 and r_2 to the merchant.

Step 4. The merchant M accepts the coin if and only if $g_1^{r_1} g_2^{r_2} = A'^d B^{t+s}$.

5. Security Analysis

5.1 Immunity to the Proposed Attacks

The improved scheme is not subjected to the proposed attacks on Baseri, *et al.*,'s scheme.

Firstly, to avoid expiration date attack, we set $\omega_2 = \left(A' + B^{t+s}\right) b_2^{(e_B * t)} \left(\bmod n\right)$ and $s_3 = O_3 / b_2 \left(\bmod n\right)$. So, s_3 is the sign of the bank on $A' + B^{t+s}$. Now, if the spender computes $s_3^{t/t'}$, he can get $(A' + B^{t+s})^{1/e_B * t'}$. But, he cannot get $(A' + B^{t'+s})^{1/e_B * t'}$. So, the improved scheme is not subjected to expiration date attack.

Secondly, in improved scheme, when the spender sends $\left(A', B^{t+s}, s_1, s_2, s_3, t\right)$ to the merchant, the merchant computes $d = H\left(A', B^{t+s}, ID_M, date \| time\right)^{1/e_M}$, not computing $d = H\left(A', B^{t+s}, ID_M, date \| time\right)$. When the merchant sends d to the spender, the spender first verifies the signature d of the merchant, using the public key e_M of the merchant M. If d does not satisfy the verification equation, the spender does not send r_1 and r_2 to the merchant. So, the improved is not subjected to merchants fraud attack.

Thirdly, in the improved scheme the coin $(A', B^{t+s}, s_1, s_2, s_3, t)$ is different from the coin $(A', B, s_1, s_2, s_3, t)$ in Baseri, *et al.*,'s scheme. B^{t+s} is not only related to random numbers x_1, x_2, but also related to time t and random number s. So, the number of same root coins can be largely reduced in improved scheme. The anonymity of electronic cash in new scheme can be efficiently protected.

5.2 Anonymity

In the first place, while obtaining the signatures s_2, s_3 of the bank on B^{t+s}, $A'+B^{t+s}$ respectively, the spender blind B^{t+s} and $A'+B^{t+s}$ by blinding factors. So, the attacker cannot get spender's identity information in the withdrawal phase. Furthermore, no one can know the identity of the spender by the information of payment phase. The information in the payment phase of the scheme includes the coin $(A', B^{t+s}, s_1, s_2, s_3, t)$ and (r_1, r_2). Although $A' = A^s$, due to the difficulty in computing discrete logarithm, the attacker cannot get s from A', and in the equations to compute r_1, r_2, there are r_1, r_2, x_1, x_2, s, five unknown numbers and time parameter t. It reveals no information to the attacker.

5.3 Double Spender Detection

In the case that a spender spends a coin twice or more, the identity information of the malicious spender can be obtained from the equations:

$$u = \frac{r_1 - r_1'}{r_2 - r_2'},\ ID_C = g_1^u (\mathrm{mod} n_B)$$

Here (r_1, r_2) and (r_1', r_2') are information the spender sends to the merchant in payment phase in twice consumption, respectively. In fact,

$$r_1 = dus + (t+s)x_1 \left(\mathrm{mod}\, e_B\right)$$

$$r_1' = d'us + (t+s)x_1 \left(\mathrm{mod}\, e_B\right)$$

$$r_2 = ds + (t+s)x_2 \left(\mathrm{mod}\, e_B\right)$$

$$r_2' = d's + (t+s)x_2 \left(\mathrm{mod}\, e_B\right)$$

So,

$$u = \frac{r_1 - r_1'}{r_2 - r_2'}$$

Further, one can obtain the identify information of the malicious spender by

$$ID_C = g_1^u (\mathrm{mod}\, n_B)$$

5.4 Unforgeability

If an adversary intends to forge a coin $(A'^*, (B^{t+s})^*, s_1^*, s_2^*, s_3^*, t^*)$, he must generate three signatures s_1^*, s_2^*, s_3^* for $A'^*, (B^{t+s})^*, (A'+B^{t+s})^*$, respectively. The adversary may get the two signatures s_1^*, s_2^* for $A'^*, (B^{t+s})^*$, respectively. But, he cannot get the signature s_3^* for $(A'+B^{t+s})^*$.

After get a cion $(A', B^{t+s}, s_1, s_2, s_3, t)$, the adversary can choose a random number $a \in_R Z_n^*$, and let

$$A'^* = A'^a,\ (B^{t+s})^* = (B^{t+s})^a,\ s_1^* = s_1^a,\ s_2^* = s_2^a.$$

Now, s_1^*, s_2^* are signatures for $A'^*, (B^{t+s})^*$, respectively. But the adversary cannot obtain the signature s_3^* for $(A'+B^{t+s})^*$.

On the other hand, if the adversary lets $s_3^* = s_3$, $(A' + B^{t+s})^* = A' + B^{t+s}$, and divides $(A' + B^{t+s})^* = A' + B^{t+s} = A'^* + (B^{t+s})^*$, $A'^* \neq A', (B^{t+s})^* \neq B^{t+s}$ Due to the hardness of discrete logarithm problem, the adversary cannot compute the signatures s_1^*, s_2^* for $A'^*, (B^{t+s})^*$, respectively. So, the adversary cannot generate new coin by forgery.

6. Performance Comparison

Baseri, *et al.*, compared their scheme with some other related scheme [2, 12, 16]. The comparison showed that Baseri, *et al.*,'s scheme cost less computation time. But we show Baseri, *et al.*,'s scheme is subjected to some weaknesses. For developing immunity from attacks, we propose a new scheme. Here we just compare our scheme with Baseri, *et al.*,'s scheme. Compared with Baseri, *et al.*,'s scheme, the new scheme just increases two modular multiplications in withdrawal phase and payment phase, respectively. But our scheme is more secure. So, from security and efficiency, our scheme needs less computation and communication costs.

7. Conclusion

Electronic payment is one of the key issues of electronic commerce development. Electronic cash is special electronic payment. There are a number of requirements for secure electronic cash schemes, such as, anonymity, unforgeability, unreusability, date attachability, divisibility, transferability and portability. In this paper, we show Baseri, *et al.*,'s electronic cash scheme is suffering from some weaknesses in anonymity, expiration date and merchant frauds. To improve Baseri, *et al.*,'s scheme, we propose a new off-line electronic cash scheme. We also discuss the security properties of our scheme, such as, anonymity, double spender detection and unforgeability. It is worthy to be mentioned that the new scheme not only possesses the features, such as anonymity, unforgeability, unreusability, but also possesses the feature of avoiding merchant frauds.

Acknowledgements

This work was supported by the Research Programs of Applied Basic and Advanced Technology of Tianjin (No. 15JCYBJC15900).

References

[1] D. Chaum, "Blind signatures for untraceable payments", In Crypto 82, Plenum Press, New York, **(1983)**, pp. 199-203.
[2] Z. Eslami and M. Talebi, "A new untraceable off-line electronic cash system", Electronic Commerce Research and Application, vol. 10, **(2011)**, pp. 59-66.
[3] R. Anderson, C. Manifavas and C. Sutherland, "NetCar-A practical electronic cash system", In Security Protocols, Springer, **(1997)**, pp. 49-57.
[4] G. Davida, Y. Frankel, Y. Tsiounis and M. Yung, "Anonymity control in e-cash systems", In Financial Cryptography, Springer, **(1997)**, pp. 1-16.
[5] G. Maitland and C. Boyd, "Fair electronic cash based on a group signature scheme", Information and Communication Security, **(2001)**, pp. 461-465.
[6] D. Chaum and S. Brands, "Minting electronic cash", Spectrum, IEEE, vol. 34, no. 2, **(2002)**, pp. 30-34.
[7] J. Camenisch, S. Hohenberger and A. Lysyanskaya, "Compact e-cash", Advances in Cryptology, EUROCRYPT, **(2005)**, pp. 302-321.
[8] H. Wang and Y. Zhang, "Untraceable off-line electronic cash flow in e-commerce", 24th Australasian Computer Science Conference Proceedings. IEEE, **(2002)**, pp. 191-198.
[9] S. Brands, "Untraceable off-line cash in wallet with observers", In Advances in Cryptology-CRYPTO'93, Springer, **(1994)**, pp. 302-318.

[10] C. Ku, C. Tsao, Y. Lin and C. Chen, "An escrow electronic cash system with limited traceability", Information Science, vol. 164, no. 1-4, **(2004)**, pp. 17-30.
[11] T. Cao, D. Lin and R. Xue, "A randomized RSAbased partially blind signature scheme for electronic cash", Computer &Security, vol. 24, no. 1, **(2005)**, pp. 44-49.
[12] W. Juang, "D-cash: a flexible pre-paid e-cash scheme for date-attachment", Electronic Commerce Research and Applications, vol. 6, no. 1, **(2007)**, pp. 74-80.
[13] C. Fan and W. Sun, "Efficient encoding scheme for date attachable electronic cash", The 24th Workshop on Combinatorial Mathematics and Computation Theory, **(2007)**, pp. 405-410.
[14] Y. Baseri, B. Takhtaei and J. Mohajeri, "Secure untraceable off-line electronic cash system", Scientia Iranica, vol. 20, no. 3, **(2013)**, pp. 637-646.
[15] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, **(1978)**, pp. 120-126.
[16] R. Martinez-Pelaez, F. Rico-Novella, and C. Satizabal, "Tomin: trustworthy mobile cash with expiration-date attached". Journal of Software, vol. 5, no. 6, **(2010)**, pp. 579-584.

Authors

Baoyuan Kang, received M.S. in algebra from the shanxi University, and ph.D. in cryptography from Xidian University, People's Republic of China in 1993 and 1999, respectively. From 1993 to 1999, he taught mathematics in Northwestern Polytechnic University. Since 1999 he has taught mathematics and computer science in Central South University. Now he is a professor at Tianjin Polytechnic University. His current research interests are cryptography and information security.

Danhui Xu, received B.S. in Computer Science from the Tianjin Polytechnic University, China in 2013. Now he is a postgraduate student at Tianjin Polytechnic University. His current research interests are cryptography and information security.