JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 34, 171-192 (2018)
DOI: 10.6688/JISE.2018.34.1.11

An Off-Line Payment Scheme for Digital Content via Subliminal Channel

BAO-YUAN KANG, MU WANG AND DONG-YA JING
School of Computer Science and Software
Tianjin Polytechnic University
Tianjin, 300387 P.R. China
E-mail: baoyuankang@aliyun.com; {463189225; 352427284}@qq.com

Now, more and more people have been purchasing digital contents through *e*-commerce. So, secure payment schemes are important issue. In a traditional electronic payment scheme there are three participants, a customer, a shop and a bank. To solve fairness and ownership issue, an arbiter is also needed. Recently, Chen *et al.* proposed a fair online payment system for digital content via subliminal channel and claimed that their scheme satisfies not only unforgeability and anonymity but also fairness and legal owner arbitration. Once demand, the arbiter can solve the fairness issue, and judge the ownership from the subliminal message provided by the customer. But in this paper, we point out that Chen *et al.*'s scheme is subjected to some attacks on anonymity, fairness and the customer's private key. Furthermore, combining techniques of blind signatures and verifiably encrypted signatures, we propose a fair off-line payment scheme for digital content via subliminal channel. In many respects we discuss the security, and show the formal proofs of unforgeability and anonymity of the proposed scheme. The comparisons show that the proposed scheme needs low computation and communication cost.

Keywords: electronic payment, fair exchange, anonymity, digital content, cryptography

1. INTRODUCTION

In recent years, more and more people have been purchasing digital content such as images, audio, and video through the Internet. Therefore, well-designed electronic payment schemes are important for digital content transactions over the Internet. In 1982, Chaum [1] proposed the concept of anonymous electronic payment. After that, many electronic payment schemes have been investigated by many researchers [2-12, 21-23].

In a traditional electronic payment scheme there are three participants, a customer, a shop and a bank. When a customer wants to buy goods from the shop, he first withdraws an *e*-cash from the bank. Then, he pays the cash to the shop. After verifying the valid of the cash, the shop sends the goods to the customer, and submits the cash to the bank, and the bank deposits money to the account of the shop. Schemes needing the bank being on line to verify the valid of *e*-cash are called as online payment schemes. Otherwise, they are called as off-line payment schemes. To prevent one of the participants in an electronic payment scheme from refusing to perform his duty, fairness must be satisfied. Of course, to keep customer's privacy, secure electronic payment schemes should satisfy not only unforgeability but also anonymity.

If the bank's participation becomes online, it will become a bottleneck of the system and make it impractical. So, several off-line payment schemes [16-20] were proposed. In

Received May 27, 2016; revised August 14, 2016; accepted September 8, 2016.
Communicated by Meng Chang Chen.

[17], Eslami and Talebi proposed an untraceable electronic payment scheme and claimed that their scheme satisfies anonymity, unreusability and date attachability. However, Baseri, *et al.*, [18] showed that the scheme [17] is subjected to some weaknesses in perceptibility of double spender, unforgeability and date attachability. Baseri, *et al*., also contributed an electronic payment scheme. But, Kang and Xu [19] showed that Baseri, *et al.*,'s scheme is suffering from anonymity, expiration date and merchant frauds. In [19] a new off-line electronic payment scheme avoiding merchant frauds was proposed. Anonymity property of electronic payment scheme can ensure the privacy of the customers. But, this property may be abused by criminals. In [16], Chen *et al.* proposed an electronic payment scheme with anonymity revocation. However, Kang and Xu [20] showed that Chen *et al.*'s scheme is suffering from forgeability and double spending owner tracing. In [20], a new off-line payment scheme with anonymity revocation was proposed, and the comparisons of security, communication efficiency and computation cost of the new scheme with several related schemes was shown.

In real life, sometimes a customer must prove to the authority that he is the legal owner of digital content. So, payment schemes with legitimacy arbitration are needed. Traditionally, ownership or copyright protections of digital content usually use the watermark insertion mechanism. However, the watermark insertion algorithm causes "reduced quality" for digital content. Recently Lin *et al.* [6] proposed an incentive-based electronic payment scheme for digital content, Chen and Liu [24] proposed a traceable *e*-cash transfer system against blackmail via subliminal channel, and Chen *et al.* [5] proposed a fair online payment system for digital content via subliminal channel. The subliminal channel can be used to send subliminal message to protect the customer's ownership to a digital content. In Chen *et al.*'s scheme [5] there is an arbiter responsible for the fair and legal owner arbitration. Chen *et al.* [5] claimed that their scheme satisfies not only unforgeability and anonymity but also fairness and legal owner arbitration. On demand, the arbiter can use the subliminal message from the customer to prove the legal ownership of the customer to the digital content. Compared with watermark mechanisms, their scheme not only provides legal ownership proving but also keeps quality of the digital content. But in this paper, we point out that Chen *et al.*'s scheme [5] is subjected to some flaws. The first flaw is the attack on the customer's private key by the bank. The second flaw is the attack on anonymity. The third flaw is the attack on fairness.

To contribute a secure and fair electronic payment scheme, based on Schnorr signature scheme [13], Fan *et al.*'s randomized blind signature scheme [14] and verifiably encrypted signatures technique [15], this paper proposes a fair off-line electronic payment scheme for digital content via subliminal channel. We discuss the security of the proposed scheme in many respects. Furthermore, we provide the formal proofs of unforgeability and anonymity. It is worth noting that compared with existing schemes our scheme needs low computation and communication cost.

The remainder of this paper is organized as follows. In the next section, we will review some primitives related to bilinear pairing. Section 3 reviews Chen *et al.*'s scheme. Shortcomings of Chen *et al.*'s scheme are shown in Section 4. Section 5 proposes a fair off-line payment scheme. Security analysis and proofs of the proposed scheme are covered in Section 6. The comparison is shown in Section 7. Finally conclusions are given in Section 8.

2. PRELIMINARY

2.1 The Bilinear Pairing

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order. Let e: $G_1 \times G_1 \rightarrow G_2$ be a pairing map which satisfies the following conditions:

1. Bilinearity: for any $P, Q, R \in G_1$, $e(P + Q, R) = e(P, R)e(Q, R)$. In particular, for any a, $b \in Z_q$, $e(aP, bP) = e(P, abP) = e(abP, P) = e(P, P)^{ab}$.
2. Non-degeneracy: There exists $P, Q \in G_1$, such that $e(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

2.2 The CDH Problem

Let G be a cyclic additive group of prime order q, P be a generator of G. The computational Diffie-Hellman (CDH) problem is to compute abP for given P, aP, $bP \in G$.

3. BRIEFLY REVIEW OF CHEN *ET AL.*'S SCHEME

Chen *et al.*' scheme [5] consists of four phases: the open account phase, the withdrawal phase, the payment phase and the arbitration phase. The system parameters consist of primes p and q such that $q|(p-1)$ and an element $g \in Z_p$ with order q. $H(\cdot)$ is one-way hash function. *Amount* is the amount of the digital content. x_C, x_S, x_B, x_j are the private keys of the customer, the shop, the bank and the arbiter, respectively. y_C, y_S, y_B, y_j are the public key of the customer, the shop, the bank and the arbiter, respectively. And $y_C = g^{x_C} \bmod p$, $y_S = g^{x_S} \bmod p$, $y_B = g^{x_B} \bmod p$, $y_J = g^{x_J} \bmod p$.

Open account phase

When a customer wants to buy the digital content via the Internet, he will go to the bank to apply for an account in advance.

Step 1: The customer sends his actual identity ID_C to the bank.

Step 2: Upon receiving ID_C from the customer, the bank chooses a random number u_1 to compute the parameters as follows:

$$V_1 = g^{u_1} \bmod p,\ I = (ID_C \cdot V_1) \bmod p,\ A_C = (I \cdot g)^{x_B} \bmod p$$

and sends back A_C to the customer, the bank stores (ID_C, V_1) as the customer's account.

Step 3: When the customer receives the above message A_C, he stores the message.

The withdrawal phase

Before processing the transaction, the customer needs to withdraw an *E*-cash from the bank.

Step 1: The customer sends an authentication message $M_C = (ID_C, A_C, amount)$ for the bank to verify and chooses a random number u_2 to compute the parameters (V_2, V_3, V_4)

$$V_2 = y_S^{u_2} \bmod p,\ V_3 = y_B^{u_2} \bmod p,\ V_4 = y_C^{u_2} \bmod p$$

and then computes the hash value of the withdrawal message C

$$C = H(ID_B || ID_{shop} || V_4 || amount)$$

and the anonymous withdrawal message C'.

$$C' = (C \cdot u_2^{-1} + x_C) \bmod q$$

and then sends (M_C, V_2, C', V_3) to the bank.

Step 2: After receiving the message, the bank checks

$$A_C \stackrel{?}{=} (V_1 \cdot ID_C \cdot g)^{x_B} \bmod p.$$

If it holds, the bank chooses a random number u_3 to compute the parameters (V'_2, V'_3, V''_3).

$$V'_2 = H((V_2)^{x_B u_3^{-1}} \bmod p),\ V'_3 = (V_3)^{u_3^{-1}},$$
$$V''_3 = V'_3 \cdot (H(amount))^{x_B} \bmod p$$

and the bank computes the withdrawal response message r.

$$r = (C' + u_3^{-1}) \cdot x_B) \bmod q$$

The bank stores (V'_3, V''_3) and sends (V'_2, V'_3, r) to the customer.

Step 3: The customer verifies r obtained from the bank.

$$g^r \stackrel{?}{=} y_B^{C'} \cdot V_3'^{u_2^{-1}} \bmod p.$$

If it holds, the customer transforms r into r'.

$$r' = ((r + x_C) \cdot u_2) \bmod q$$

Finally, the customer stores the messages (V_4, C, V'_2, V'_3, r').

The payment phase

When the customer wants to purchase digital content, he and the shop carry out the following steps.

Step 1: When the customer wants to buy the digital content, he generates a signature r_C of the subliminal message using the arbiter's public key y_J and transaction message M_P.

$$r_C = M_{CS} \cdot y_J^{x_C} y_S^{x_C}$$

$$M_P = (ID_C \cdot M_{CS} || ID_{shop} || ID_B || r_C || C || ID_{DC} || V_4 || V'_2 || V'_3 || T_C)$$

where ID_{DC} is identity of the digital content. The customer chooses a random number u_4 and a timestamp T_C to compute two message recovery parameters (r_{C1}, s_{C1}).

$$r_{C1} = M_p \cdot y_S^{u_4},\ S_{C1} = u_4 + x_C \cdot r_{C1} + T_C$$

and computes a parameter M'_P using one-way hash function:

$$M'_P = H(M_P || y_C).$$

Then the customer sends (y_C, r_{C1}, s_{C1}, T_C, M'_P) to the shop.

Step 2: After receiving (y_C, r_{C1}, s_{C1}, T_C, M'_P) at time T_V, the shop checks the validity of the timestamp T_C as follows:

$$T_V - T_C \,?\leq \tau.$$

Where τ denotes the expected transmission valid time interval between the customer and the shop, if it holds, the shop uses private key x_S, two parameters (r_{C1}, s_{C1}) of message recovery and T_C to recover the cipher message and checks M'_P as follows:

$$M'_P \,?= H(y^{-s_{C1}+T_C} \cdot y_C^{x_s \cdot r_{C1}} \cdot r_{C1} || y_C).$$

If it holds, the shop continues to check V'_2 and V'_3 as follows:

$$V'_2 \,?= H(V'^{x_s}_3).$$

If it holds, the shop checks whether V'_3 (extracted from M_P) exists in the shop's database or not. If V'_3 does exist, the shop stores it and verifies the challenge of withdrawal message as follows:

$$C \,?= H(ID_B || ID_{shop} || V_4 || DC\text{'s } amount).$$

If it holds, the shop uses the arbiter's public key Y_J, his private key x_s and the authorized code AUC_{DC} of the digital content to compute a parameter N as follows:

$$N = y_J^{x_s} \cdot AUC_{DC}.$$

It uses its private key x_s chooses a random number u_5 and then generates two signatures (r_N, s_N) as follows:

$$r_N = g^{u_5} \bmod p,$$
$$s_N = u_5 \cdot ID_C \cdot M_{cs} - x_s \cdot N \cdot ID_{DC} \bmod q.$$

Finally, the shop computes a parameter r_{MA} with digital content M and the authorized

code AUC_{DC} of the digital content as follows:

$$r_{MA} = M \cdot AUC_{DC} + y_J^{x_s}.$$

And then sends $(N, r_N, s_N, r_{MA}, H(N \| r_{MA} \cdot y_C^{x_s}))$ to the customer.

Step 3: Upon receiving the message, the customer checks whether a signature r_N is valid as follows:

$$(r_N)^{ID_C \cdot M_{CS}} ? = (g^{s_N} \cdot y_S^{N \cdot ID_{DC}}) \bmod p.$$

If it holds, he continuously checks r_{MA} and generates a certification message M_W as follows:

$$H(N \| r_{MA} \cdot y_C^{x_s}) ? = H(N \| r_{MA} \cdot y_C^{x_s}),\ M_W = r' \cdot y_S^{x_C} \bmod p.$$

The customer sends M_W and $H(M_P \| r')$ to the shop.

Step 4: Once receiving the message M_W, the shop verifies whether hash values is equal as follows:

$$M'_W = M_W \cdot y_C^{-x_s} \bmod p,\ H(M_P \| r') ?= H(M_P \| M'_W).$$

If it holds, the shop sends $(M'_W, C, V'_4, V'_3, amount)$ to the bank via the secure channel.

Step 5: After receiving the message $(M'_W, C, V_4, V'_3, amount)$, the bank needs to check whether V'_3 had been used in the database. If it is false, it continues to check whether the withdrawal message is valid as follows:

$$g^{r'} \cdot (H(amount))^{x_B} \bmod p ?= (y_B^C \cdot V_4^{x_B+1} \cdot V'_3) \bmod p.$$

If it holds, the bank marks V'_3 that it has been used in advance and stores the shop's identity ID_{shop}. The bank sends back a confirmation message Yes/No.

Step 6: If the shop receives a positive confirmation Yes message from the bank, it uses the signature of the subliminal message r_C (extracted from M_P) and private key x_S to compute M'_{cs} as follows:

$$M'_{cs} = r_C \cdot y_C^{-x_s}.$$

The shop generates two parameters of message recovery (r_M, s_M) with a random number u_6 and its private key x_S for the digital content as follows:

$$r_M = My_C^{x_S} \cdot g^{u_6},\ S_M = x_S \cdot r_M + u_6.$$

Finally, the shop generates the following three parameters $(S_{DC1}, S_{DC2}, r_{DC})$ with M'_{CS}

random number u_7, a parameter N and the digital content M as follows:

$$S_{DC1} = y_J^{x_s} \cdot u_7,\ S_{DC2} = x_S \cdot M'_{CS} - u_7,\ r_{DC} = H(M)^{x_S \cdot N + S_{DC1}} \bmod p$$

and users M'_{CS} and AUC_{DC} to compute a certification $Cert_M$ of the digital content as follows:

$$Cert_M = H(M)^{M'_{CS} + AUC_{DC}} \bmod p.$$

Then sends (r_M, S_M, S_{DC1}, S_{DC2}, r_{DC}, $Cert_M$) to the customer.

Step 7: Upon receiving the message, the customer computes a parameter M''_{CS} with a subliminal message M_{CS} as follows:

$$M''_{CS} = M_{CS} \cdot y_J^{x_C}$$

and he recovers the digital content with two parameters (r_M, S_M) of message recovery as follows:

$$M = g^{-S_M} \cdot y_S^{r_M} \cdot r_M \cdot y_S^{-x_C}.$$

Then he checks whether a certification of the digital content $Cert_M$ is valid as follows:

$$(Cert_M)^{S_{DC1}} \stackrel{?}{=} (r_{DC})^{M''_{CS}} \cdot H(M)^{-S_{DC2} \cdot N} \bmod p.$$

If it holds, the consumer completes this transaction; else the consumer proposes a fair arbitration request to the arbiter.

The fair arbitration phase

In the payment phase, if the customer does not receive a signature for the digital content or checks a signature is not held, he can propose the arbitration request to the arbiter.

Step 1: The customer sends message (ID_C, ID_B, ID_{Shop}, ID_{DC}, M_{CS}, V'_3, N, r_N, S_N, r_{MA}) to the arbiter.

Step 2: The arbiter verifies whether a signature (N, r_N, S_N) is valid or not as follows:

$$(r_N)^{ID_C \cdot M_{CS}} \stackrel{?}{=} (g^{s_N} \cdot y_S^{N \cdot ID_{DC}}) \bmod p.$$

If it does not hold, it means the customer is lying; otherwise checks next conditions.

Step 3: The arbiter sends V'_3 to the bank to check whether it has been used in its database or not. If it's false, it means the shop does not withdraw. It means that the customer is lying; otherwise the arbiter recalculates the correct certification to the customer as follows:

$AUC_{DC} = N \cdot y_S^{-x_J}$, $M = (r_{MA} - y_S^{x_J}) \cdot AUC_{DC}^{-1}$.

$M''_{CS} = M_{CS} \cdot y_C^{x_J} \bmod p$, $Cert_M = H(M)^{M''_{CS} + AUC_{DC}} \bmod p$ and sends to (M, $Cert_M$) to the customer.

The legal owner arbitration phase

When a consumer is suspected of possessing illegal digital content, he can provide the transaction messages to the arbiter. The arbiter, according to the transaction messages provided by the customer, verifies whether the customer is involved in the transaction and the digital content is authorized by the shop.

Step 1: The customer sends (ID_C, ID_{Shop}, M_{CS}, ID_{DC}, N, r_N, S_N, M, $Cert_M$) to the arbiter.
Step 2: Upon receiving these message from the customer, the arbiter uses the subliminal message M_{CS} provided by customer, $ID_C \cdot M_{CS}$ and ID_{DC} to verify signature N of the authorized code AUC_{DC} of digital content as follows:

$$(r_N)^{ID_C \cdot M_{CS}} ? = (g^{s_N} \cdot y_S^{N \cdot ID_{DC}}) \bmod p.$$

If it holds, it means the customer has been authorized by the shop; otherwise the customer is illegal.

Step 3: The arbiter uses a signature N and a private key x_J to compute the authorized code AUC_{DC} of the digital content.

$$AUC_{DC} = N \cdot y_S^{-X_j}$$

and uses M_{CS} to compute

$$M''_{CS} = M_{CS} \cdot y_J^{x_C} \bmod p.$$

Finally, use M''_{CS} and AUC_{DC} to verify the certification of the digital content as follows:

$$Cert_M ?= H(M)^{M''_{CS} + AUC_{DC}} \bmod p.$$

If it holds, it means the arbiter can determine that the customer is legal; otherwise the customer is illegal.

4. SHORTCOMINGS OF CHEN *ET AL.*'S SCHEME

In this section, we show that Chen *et al.*'s scheme [5] is subjected to three attacks.

4.1 The Bank Can Obtain the Private Key of the Customer

In the withdrawal phase of Chen *et al.*'s scheme, there are two equations

$$C' = (Cu_2^{-1} + x_C) \bmod q \tag{1}$$

and

$$r' = ((r + x_C)u_2) \bmod q \tag{2}$$

So, by Eqs. (1) and (2)

$$\begin{aligned} C'u_2 &= (C + x_C u_2) \bmod q \\ &= (C + r' - ru_2) \bmod q \end{aligned}$$

Then,

$$C'u_2 + ru_2 = (C + r') \bmod q$$

and

$$\begin{aligned} u_2 &= (C + r')(r + C')^{-1} \bmod q \\ u_2^{-1} &= (C + r')^{-1}(r + C') \bmod q \end{aligned}$$

So, by the Eq. (1), it holds

$$x_C = C' - Cu_2^{-1} = (C' - C(r + C')(r' + C)^{-1}) \bmod q$$

But, the bank can get r, C' in the withdrawal phase and get C, r' in payment phase, and C, C', r, r' can be traced by V_3, V'_3 obtained by the bank in the withdrawal phase of the system. So, the bank can compute the private of the customer.

4.2 Chen *et al.*'s System Does Not Satisfy the Anonymity

Chen *et al.* said their scheme satisfies anonymity, both the bank and the shop cannot know the customer's identity during the payment phase. But, in the withdrawal phase, the customer submits the information $M_C = \{ID_C, A_C, amount\}$, and the bank stores the information (V'_3, V''_3). So, in the payment phase, when the shop sends (M'_W, C^*, V_4, V'_3, $amount^*$) to the bank, the bank can trace the customer's identity ID_C by V'_3. So, Chen *et al.*'s scheme does not satisfy the anonymity.

4.3 In the Fair Arbitration Phase, the Customer May Not Get the Digital Content and Its Certification. So, Chen *et al.*'s Scheme Does Not Satisfy the Fairness.

In the payment phase of Chen *et al.*'s system, if the customer does not receive a signature for the digital content or checks a signature is not held, he can propose the arbitration request to the arbiter. The customer sends message (ID_C, ID_B, ID_{Shop}, ID_{DC}, M_{CS}, V'_3, N, r_N, S_N, r_{MA}) to the arbiter. But, the hostile shop may compute

$$r_{MA} = M^* \cdot AUC_{DC} + y_j^{x_s}$$

or

$r_{MA} = M \cdot AUC_{DC} + D$.

Here, $M^* \neq M$, $D \neq y_J^{x_S}$.

And in Chen *et al.*'s system, there is no the verification of r_{MA}. Such, the arbiter cannot compute the correct digital content. So, the hostile shop will succeed in cheating customer.

Of course, the hostile shop may compute N ($\neq y_J^{x_S} AUC_{DC}$). And there is not the verification of N in Chen *et al.*'s system. So, the arbiter cannot compute the correct authorized code AUC_{DC}.

So, Chen *et al.*'s scheme [5] is not fair to the customer.

5. THE PROPOSED SCHEME

In this section, combining techniques of blind signatures and verifiably encrypted signatures, we will propose a fair off-line payment scheme for digital content via subliminal channel. In the proposed scheme, there are four participants, a customer, a shop, a bank and an arbiter. When a customer wants to buy digital content from the shop, he first withdraws an *e*-cash from the bank. Then, with subliminal message, his identity information and the arbiter's public key, the customer generates a verifiably encrypted signature of the cash and sends it to the shop. After verifying the valid of the verifiably encrypted signature, the shop sends the digital content and its certification to the customer. If the verification of the digital content and its certification passes, the customer sends the cash to the shop. Later, when the shop submits the cash to the bank, the bank verifies it is validity and deposits money to the account of the shop. Once one of the participants refuses to fulfill his duty or it is necessary to check the ownership of digital content, the arbiter can carry out arbitration.

The proposed scheme consists of six phases: the initializing phase, the withdrawal phase, the payment phase, the deposit phase, the fair arbitration phase and the legal owner arbitration phase. Here any communication between any two entities should be encrypted, and this can be done by incorporating mutual authentication and key agreement protocols, like in [16]. Here, for brevity, we omit those encryptions in six protocols.

The following notations are used in our scheme.

x_1, x_2, Pub_1, Pub_2	the two private keys and two public keys of the bank, respectively, where $x_1, x_2 \in Z_q$, $Pub_1 = x_1P$, $Pub_2 = x_2P$
x_S, Y_S	the private key and public key of the shop, respectively. Where $Y_S = x_SP$
x_J, Y_J	the private key and public key of the arbiter, respectively. Where $Y_J = x_JP$
ID_K	the identity of the K
$H_1()$, $H_2()$	two one-way hash function
M	the digital content
amount	the price of digital content
ID_{DC}	the identity of digital content
$Cert_M$	the certification of digital content signed by the arbiter
M_{CS}	the subliminal message generated by the customer

5.1 The Initializing Phase

Given a security parameter η, the bank chooses a large prime q, a cyclic additive group G_1 generated by P, and a cyclic multiplicative group G_2 with the same order q, and a bilinear pairing map e: $G_1 \times G_1 \rightarrow G_2$. The bank also publishes two hash functions H_1: $\{0, 1\}^* \rightarrow Z_q$, H_2: $\{0, 1\}^* \rightarrow G_1$. The shop wanting to sell digital content over Internet must register its digital contents to the arbiter. The arbiter uses his private to generate a certification $Cert_M$ to each digital content M.

Assume the shop already has an account in the bank. When a customer wants to buy a digital content via the Internet, he will go to the bank to apply for an account in advance.

Step 1: The customer sends his actual identity ID_C to the bank.
Step 2: Upon receiving ID_C from the customer, the bank chooses a random number $u_1 \in Z_q^*$ to compute the parameters as follows:

$$V_1 = u_1 P$$
$$A_C = u_1 + H_1(ID_C \| V_1) x_1$$

And sends back A_C to the customer. The bank stores (ID_C, V_1) as the customer's account.
Step 3: When the customer receives the above message A_C, he stores the message.

5.2 The Withdrawal Phase

Before processing the transaction, the customer needs to withdraw an *e*-cash from the bank. To achieve unlinkability, the randomized blind signature technique [14] is used.

Step 1: The customer sends an authentication message $M_C = (ID_C, A_C, amount)$ for the bank.
Step 2: After receiving the message, the bank checks

$$A_C P ? = V_1 + H_1(ID_C \| V_1) Pub_1$$

If it holds, the bank chooses a random number $k \in Z_q^*$ to compute $K = kP$ and sends K to the customer.
Step 3: The customer chooses three random numbers $u_2, r_1, r_2 \in Z_q^*$ to compute

$$V_2 = u_2 K$$
$$\alpha_1 = r_1 H_2(ID_B \| ID_{Shop} \| amount \| V_2) + r_2 P$$
$$\alpha_2 = r_1 u_2 \bmod q$$

and sends (α_1, α_2) to the bank.
Step 4: The bank compute

$$T = x_1 \alpha_1 + x_2 \alpha_2 k H_1(amount) P$$

and sends T to the customer.

Step 5: The customer computes

$$S = r_1^{-1}(T - r_2 Pub_1)$$

and obtains an *e*-cash (S, V_2).

5.3 The Payment Phase

When the customer wants to purchase a digital content, with a selected subliminal message, his identity and the public key of the arbiter, the customer generates a verifiably encrypted signature of the cash and sends it to the shop. When the customer receives valid digital content and its certification from the shop, he sends the cash to the shop.

Step 1: The customer generates subliminal message M_{CS} and chooses a random numbers $u_3 \in Z_q^*$ to compute

$$V_3 = u_3 K$$
$$t = H_1(M_{CS} || ID_C)$$
$$S' = S + t u_3 Y_j$$

and sends (S', V_2, V_3, ID_{DC}, t) to the shop.

Step 2: After receiving (S', V_2, V_3, ID_{DC}, t), the shop checks whether V_2 exists in its database or not. If V_2 does not exist, the shop verifies

$$e(S', P) = e(H_2(ID_B || ID_{Shop} || DC\text{'s } amount || V_2), Pub_1) e(H_1(DC\text{'s } amount) V_2, Pub_2) e(Y_j, t V_3)$$

If it holds, the shop stores V_2 and chooses a random numbers $u_4 \in Z_q^*$ to compute

$$V_4 = u_4 P$$
$$w = u_4 + H_1(S' || t || M || V_4) x_s$$

and sends ($Cert_M$, M, w, V_4) to the customer.

Step 3: The customer computes $H_2(M)$ and uses the public key Y_j of the arbiter and $H_2(M)$ to verifies the certification $Cert_M$ of the digital content M. If the verification passes, the customer also verifies

$$wP = V_4 + H_1(S' || t || M || V_4) Y_s.$$

Step 4: The customer sends S to the shop.

Step 5: The shop verifies

$$e(S, P) = e(H_2(ID_B || ID_{Shop} || DC\text{'s } amount || V_2), Pub_1) e(H_1(DC\text{'s } amount) V_2, Pub_2).$$

If it holds, the shop receives a valid *e*-cash (S, V_2).

5.4 The Deposit Phase

When the shop wants to deposit the received *e*-cash (S, V_2) into his account in the bank, the following steps are done between the bank and the shop.

Step 1: The shop sends (ID_{Shop}, S, V_2, DC's *amount*) to the bank.
Step 2: The bank first checks whether the cash (S, V_2) exists in its deposit. If it does not exist, the bank verifies

$$e(S, P) = e(H_2(ID_B||ID_{Shop}||DC\text{'s } amount||V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2)$$

If it holds, the bank accepts the cash, stores it in the deposit table and transfers money to the shop.

5.5 The Fair Arbitration Phase

Arbitration 1: In the payment phase, if the shop does not receive a valid *e*-cash for the digital content after it sends ($Cert_M$, M, w, V_4) to the customer, the shop can propose the arbitration request to the arbiter.

Step 1: The shop sends message $\{(S', V_2, V_3, ID_{DC}, t), (Cert_M, M, w, V_4)\}$ to the arbiter.
Step 2: The arbiter first verifies the certification $Cert_M$ of the digital content M, and verifies

$$e(S', P) = e(H_2(ID_B||ID_{Shop}||DC\text{'s } amount||V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2)$$
$$e(Y_j, tV_3)$$

and

$$wP = V_4 + H_1(S'||t||M||V_4)Y_s.$$

If they hold, and V_2 does not exist in its database, the arbiter uses his private key x_J to compute

$$S = S' - tx_jV_3$$

and give S to the shop. The shop obtains a valid *e*-cash (S, V_2).

Arbitration 2: In the payment phase, if the customer does not receive the digital content and related information after he sends (S', V_2, V_3, ID_{DC}, t) to the shop, the customer can propose the arbitration request to the arbiter.

Step 1: The customer sends (S', V_2, V_3, ID_{DC}, t) to the arbiter.
Step 2: When the arbiter finds the record $\{(S', V_2, V_3, ID_{DC}, t), (Cert_M, M, w, V_4)\}$ in his database, he gives ($Cert_M$, M, w, V_4) to the customer.

In the payment phase, when the customer sends (S', V_2, V_3, ID_{DC}, t) to the shop, the shop may not send ($Cert_M$, M, w, V_4) to the customer for purposes that the shop wants to

stop the transaction or the shop maliciously wants to get *e*-cash through the arbitration 1. If the shop wants to stop the transaction, the shop does not propose the arbitration 1 request. So, when the customer proposes arbitration request in arbitration 2, the arbiter cannot find the record $\{(S', V_2, V_3, ID_{DC}, t), (Cert_M, M, w, V_4)\}$. Of course, the arbiter cannot give $(Cert_M, M, w, V_4)$ to the customer. The transaction really stops, the customer does not get $(Cert_M, M, w, V_4)$, and the shop does not get the *e*-cash.

If the shop maliciously wants to get the *e*-cash through the arbitration 1, the shop must send $\{(S', V_2, V_3, ID_{DC}, t), (Cert_M, M, w, V_4)\}$ to the arbiter. Then, the arbiter can compute S and then records $\{(S', V_2, V_3, ID_{DC}, t), (Cert_M, M, w, V_4)\}$, gives the *e*-cash to the shop. As a result, when the customer proposes arbitration request in arbitration 2, the arbiter can give $(Cert_M, M, w, V_4)$ to the customer. The transaction ends, the shop and the customer get the thing they wanted. In summary, the arbitration is feasible and fair.

5.6 The Legal Owner Arbitration Phase

When a consumer is suspected of possessing illegal digital content, he can provide the transaction messages to the arbiter. The arbiter checks whether the customer is involved in the transaction and the digital content is authorized by the shop.

Step 1: The customer sends $(ID_C, Cert_M, M, S', w, V_4, M_{CS}, Y_s)$ to the arbiter.
Step 2: The arbiter first verifies the certification $Cert_M$ of M. Then he computers $\bar{t} = H_1(M_{CS}||ID_C)$ and verifies

$$wP = V_4 + H_1(S'||\bar{t}||M||V_4)Y_s.$$

If it holds, the arbiter knows the customer is legal owner of the digital content M.

6. SECURITY ANALYSIS AND FORMAL PROOF OF THE PROPOSED SCHEME

In this section, we discuss the security of the proposed scheme on the following aspects.

6.1 Correctness

Firstly, we show when *amount* = *DC*'s *amount* the *e*-cash (S, V_2) can be verified by equation

$$e(S, P) = e(H_2(ID_B||ID_{Shop}||DC\text{'s } amount||V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2)$$

If fact,

$$\begin{aligned} &e(S, P) \\ &= e(r_1^{-1}(T - r_2Pub_1), P) \\ &= e(r_1^{-1}(x_1\alpha_1 + x_2\alpha_2 kH_1(amount)P - r_2Pub_1), P) \\ &= e(r_1^{-1}(x_1(r_1H_2(ID_B||ID_{Shop}||amount||V_2) + r_2P) + x_2r_1u_2kH_1(amount)P - r_2Pub_1), P) \end{aligned}$$

$= e(x_1H_2(ID_B||ID_{Shop}||amount||V_2) + r_1^{-1}x_1r_2P + x_2u_2kH_1(amount)P - r_1^{-1}r_2Pub_1, P)$
$= e(x_1H_2(ID_B||ID_{Shop}||amount||V_2) + r_1^{-1}r_2Pub_1 + x_2u_2kH_1(amount)P - r_1^{-1}r_2Pub_1, P)$
$= e(x_1H_2(ID_B||ID_{Shop}||amount||V_2) + x_2H_1(amount))V_2, P)$
$= e(H_2(ID_B||ID_{Shop}||amount||V_2), Pub_1)e(H_1(amount)V_2, Pub_2)$
$= e(H_2(ID_B||ID_{Shop}||DC\text{'s } amount||V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2)$

Secondly, we show that when *amount* = *DC*'s *amount*, (S', V_2, V_3, ID_{DC}, t) can be verified by equation

$$e(S', P) = e(H_2(ID_B||ID_{Shop}||DC\text{'s } amount||V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2) e(Y_j, tV_3)$$

Since

$$S' = S + tu_3Y_j$$

and above proven result

$$e(S, P) = e(H_2(ID_B||ID_{Shop}||DC\text{'s } amount||V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2)$$

So

$e(S', P)$
$= e(S + tu_3Y_j, P)$
$= e(S, P)e(tu_3Y_j, P)$
$= e(S, P)e(Y_j, tV_3)$
$= e(H_2(ID_B||ID_{Shop}||DC\text{'s } amount||V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2)e(Y_j, tV_3)$

Thirdly, we show the signature w generated by the shop can be verified by

$$wP = V_4 + H_1(S'||t||M||V_4)Y_s.$$

Since

$V_4 = u_4P$
$w = u_4 + H_1(S'||t||M||V_4)x_s$

So

$wP = (u_4 + H_1(S'||t||M||V_4)x_s)P$
$= u_4P + H_1(S'||t||M||V_4)x_s)P$
$= V_4 + H_1(S'||t||M||V_4)Y_s$

6.2 Double Spending Issue

Case 1: In the deposit phase, when the shop sends (ID_{Shop}, S, V_2, *amount*) to the bank, the bank first checks whether the cash (S, V_2) exists in its deposit or not. If the cash exists, it means the cash has been used in a past deal.

Case 2: In the payment phase, when the customer sends (S', V_2, V_3, ID_{DC}, t) to the shop, the shop firstly checks whether V_2 exists in the shop's database or not. If V_2 exists, the shop stops the deal.

6.3 Shop Cheat Issue

In the payment phase, when the information (S', V_2, V_3, ID_{DC}, t) passes the verification, the shop then sends digital content to the customer. So, when the shop receives (S', V_2, V_3, ID_{DC}, t) from the customer, the malicious shop may want to send (S', V_2, V_3, ID_{DC}, t) to another shop to buy goods for it. But the malicious shop cannot succeed, since in withdrawal phase, the customer mounts the shop information in α_1, S'cannot passes the verification in another shop.

6.4 Amount Consistency Issue

In withdrawal phase, the customer sends $M_C = (ID_C, A_C, amount)$ to the bank, and computes $\alpha_1 = r_1H_2(ID_B||ID_{Shop}||amount||V_2) + r_2P$. But the malicious customer may compute $\alpha_1 = r_1H_2(ID_B||ID_{Shop}||amount^*||V_2) + r_2P$. Here $amount^*$ may be more than $amount$ in M_C. But this bad intention can be prevented. Since the bank mounts the $amount$ got from M_C into T, so the wrong α_1 will cause that S' cannot passes the verification of the shop. Even the customer colludes with the shop, in deposit phase S cannot passes the verification of the bank. So, the bad intention of the customer can be prevented. Moreover, in our scheme the shop and the bank do not need keep additional information to verify the amount consistency issue.

6.5 Anonymity

In the payment phase, the customer can securely communicate with the shop by selecting a random number z and generating shared key zY_S. To do this, it is only necessary to send additional information zP when the customer sends (S', V_2, V_3, ID_{DC}, t) to the shop. No the customer's identity can be known by the shop. So, in the payment phase, the customer's identity is anonymous to the shop. As for the customer's identity anonymity to the bank in deposit phase, we will show formal security proof in unlinkability property.

6.6 Fairness Issue

In the payment phase, if the shop does not receive a valid *e*-cash for the digital content after the shop sends ($Cert_M$, M, w, V_4) to the customer, the shop can propose the arbitration request to the arbiter. The shop sends message {(S', V_2, V_3, ID_{DC}, t) and ($Cert_M$, M, w, V_4)} to the arbiter. Only the two information pass verification, the arbiter computes S and sends it to the shop and stores {(S', V_2, V_3, ID_{DC}, t) and ($Cert_M$, M, w, V_4)} in the arbiter's database. If the shop cheats the arbiter, that is when the shop receives (S', V_2, V_3, ID_{DC}, t) from the customer, the shop does not send ($Cert_M$, M, w, V_4) to the customer. Then, when the shop sends ($Cert_M$, M, w, V_4) to the arbiter in arbitration 1, the customer can get it from arbitration 2.

6.7 Owner Issue

Only the legal customer owns the subliminal message M_{CS} and the signature (w, V_4) on the digital content M. So, only the legal customer can pass the arbiter's verification. Even if the legal customer share M_{CS} and (w, V_4) with illegal customer, the identity information of the customer must be submitted in legal owner arbitration phase. And it is necessary to use the identity information to verify the signature. So, the identity information of illegal customer cannot pass the signature verification. Therefore, our system can solve the owner issue.

6.8 Formal Proof of Unlinkability

Theorem 1: The proposed Scheme satisfies the unlinkability property.

***Proof*:** Here unlinkability means that when the bank receives an *e*-cash (S, V_2) in deposit phase, by the view (K, α_1, α_2, T) of the bank in the withdrawal phase, the bank cannot know who withdraws the cash.

To proof the unlinkability property of our scheme, it is only needed to show that there always exists one and only one corresponding triple (u_2, r_1, r_2) for any cash (S, V_2) and any view (K, α_1, α_2, T).In fact, since $V_2 = u_2 kP$, so for given V_2, k, there is one and only one number u_2. Then, by equation $\alpha_2 = r_1 u_2 \bmod q$, there is one and only one number r_1. Finally, by equation $\alpha_1 = r_1 H_2(ID_B || ID_{Shop} || amount || V_2) + r_2 P$, there is one and only one number r_2. Furthermore, by the two equation

$$T = x_1\alpha_1 + x_2\alpha_2 kH_1(amount)P$$
$$S = r_1^{-1}(T - r_2 Pub_1)$$

and the correctness inference in section 6.1, the equation

$$e(S, P) = e(H_2(ID_B || ID_{Shop} || DC\text{'s } amount || V_2), Pub_1)e(H_1(DC\text{'s } amount)V_2, Pub_2)$$

always holds.

This completes the proof of the unlinkability property.

6.9 Formal Proof of Unforgeability

Theorem 2: If the Chosen-Target CDH assumption is hard, then the proposed scheme is secure against *e*-cash existential forgery attack.

***Proof*:** Following the technique in [14], we prove the unforgeability of our scheme. The thinking of proof is that if an adversary can forge an *e*-cash, the challenger will use the forged *e*-cash to solve the Chosen-Target CDH assumption [14].

Let (G_1, G_2, H_1, H_2, q, e, P, Pub_1, Pub_2) be the public parameters of our scheme, and (P, aP) be the challenge from the Chosen-Target CDH assumption. Assume the challenger know the partial private key x_2, where $Pub_2 = x_2 P$. But the challenger does not

know the partial private key x_1, where $Pub_1 = x_1P$. The challenger is allowed to access the oracles offered in the Chosen-Target CDH assumption. And the challenger will simulate two hash oracles and signature oracle for the adversary.

The challenger keeps two hash queries list. When the adversary queries the hashed value of $ID_B||ID_{Shop}||amount||V_2$ to hash H_2, if the query already appears on the H_2-list in a tuple ($ID_B||ID_{Shop}||amount||V_2$, Z), the challenger responds with $H_2(ID_B||ID_{Shop}||amount||V_2) = Z$. Otherwise, the challenger selects a random element $Z \in G_1$, and responds with $H_2(ID_B||ID_{Shop}||amount||V_2) = Z$ and records ($ID_B||ID_{Shop}||amount||V_2$, Z) in H_2-list. Similarly, the challenger answers the adversary's query to the hashed value of *amount* to hash H_1 with $H_1(amount) = z'$. When the adversary queries signature for (α_1, α_2), the challenger first queries to the oracles offered in the Chosen-Target CDH assumption and obtains $T_1 = a\alpha_1$. Then, the challenger computes $T = T_1 + x_2k\alpha_2z'P$ and returns T to the adversary.

After q_{H1}, q_{H2} and q_S queries to the H_1, H_2 and signature oracles, if he adversary can generate η valid *e*-cash (S_1, V_2^1), (S_2, V_2^2), …, (S_η, V_2^η). Then the challenger can compute

$$D_i = S_i - x_2z_i'V_2^i$$

and outputs (D_1, Z_1), (D_2, Z_2), …, (D_η, Z_η) as η valid instances in the Chosen-Target CDH assumption.

This completes the proof of the unforgeability.

7. COMPARISONS

Because schemes [5, 6] and our scheme are all payment schemes for digital content, in this section, we compare our scheme with [5, 6] in some features, communication efficiency and computation cost. The features are anonymity/unlinkability, unforgeability, verification, double-spending detection, uncheatability of merchant, customer private key security, fairness, owner arbitration. Our scheme satisfies all of above features. But, Chen *et al.*'s scheme does not satisfy anonymity, customer private key security and fairness, and there is no formal proof of the unforgeability in Chen *et al.*'s scheme. Lin *et al.*'s scheme does not satisfy fairness and owner arbitration, and there are no formal proofs of anonymity and unforgeability. We show the comparison result of the features in Table 1.

In Table 2, we compare the communication efficiency of our scheme with schemes [5, 6]. Chen *et al.*'s scheme and Lin *et al.*'s scheme are on-line payment schemes. Therefore they do not have deposit protocols. Lin *et al.*'s scheme also has no open account protocol and legal owner arbitration protocol. Although Lin *et al.*'s scheme has initializing protocol we do not compute its communication number of rounds for the sake of fair comparison. According to Table 2, our scheme demonstrates better communication efficiency under enhanced security.

Since there is no detail signature algorithm description in [6], in Table 3, we only compare the computation cost of our scheme with Chen *et al.*'s scheme. It is necessary to illustrate that Chen *et al.*'s scheme has no deposit protocol, and we mainly count the exponential operation, scalar multiplication, hash computation and bilinear pairings opera-

tion. According to [14], the computation cost of Chen *et al.*' scheme and our scheme are correspond approximately to 13852 scalar multiplication and 5210 scalar multiplication, respectively. Obviously, our scheme needs low computation cost.

Table 1. Comparison of features of our scheme with schemes [5, 6].

	F1	F2	F3	F4	F5	F6	F7	F8
Chen *et al.* [5]	No	–	Yes	Yes	Yes	No	No	Yes
Lin *et al.* [6]	–	–	Yes	Yes	Yes	Yes	No	No
Ours	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

F1: Anonymity/Unlinkability, F2: Unforgeability, F3: Verification, F4: Double spending detection, F5: Uncheatability of merchant, F6: Customer private key security, F7: Fairness, F8: Owner arbitration

Table 2. Required number of rounds for each protocol in compared schemes.

	P1	P2	P3	P4	P5	P6
Chen *et al.* [5]	2	2	6	–	2	1
Lin *et al.* [6]	–	4	7	–	2	–
Ours	2	4	3	1	4	1

P1: Initializing protocol, P2: Withdrawal protocol, P3: Payment protocol, P4: Deposit protocol, P5: Fair protocol, P6: Legal owner arbitration protocol

Table 3. Comparison of computation cost.

	P1	P2	P3	P4	P5	P6
Chen *et al.* [5]	2E+2S	9E+7S+3H	32E+28S+11H	–	7E+4S+H	6E+3S+H
Ours	E+S+H	7E+2S+3H	6E+2S+8H+7B	E+2H+3B	E+2S+3H+4B	E+2H

P1: Initializing protocol, P2: Withdrawal protocol, P3: Payment protocol, P4: Deposit protocol, P5: Fair protocol, P6: Legal owner arbitration protocol
E: Exponential operation, S: Scalar multiplication, H: Hash computation, B: bilinear pairings.

8. CONCLUSION

In this paper, we show that Chen *et al.*'s scheme is subjected to three attacks. Firstly, the bank can obtain the private key of the customer. Secondly, in the fair arbitration phase, the customer may not get the digital content and its certification. Also the bank can trace the customer's identity by the cash. Furthermore, we propose a fair off-line payment scheme for digital content via subliminal channel and discuss the security, show the formal proofs of unforgeability and anonymity of the proposed scheme.

ACKNOWLEDGEMENTS

We would like to thank the reviewers for their helpful comments. This work is supported by the Applied Basic and Advanced Technology Research Programs of Tianjin (No. 15JCYBJC15900) and the National Natural Science Foundation of China (No. 51378350).

REFERENCES

1. D. Chaum, "Blind signatures for untraceable payments," in *Proceedings of International Conference on Crypto*, 1983, pp. 199-203.
2. J. Luo, M. Yang, and S. Huang, "An unlinkable anonymous payment scheme based on near field communication," *Computers and Electrical Engineering*, Vol. 49, 2016, pp. 198-206.
3. J. Yang and P. Lin, "A mobile payment mechanism with anonymity for cloud computing," *The Journal of Systems and Software*, Vol. 116, 2016, pp. 69-74.
4. W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Computer Communications*, Vol. 35, 2012, pp. 188-195.
5. C. Chen and J. Liao, "A fair online payment system for digital content via subliminal channel," *Electronic Commerce Research and Applications*, Vol. 10, 2011, pp. 279-287.
6. S. Lin and D. Liu, "An incentive-based electronic payment scheme for digital content transactions over the internet," *Journal of Network and Computer Applications*, Vol. 32, 2009, pp. 589-598.
7. J. Isaac and S. Zeadally, "An anonymous secure payment protocol in a payment gateway centric model," *Procedia Computer Science*, Vol. 10, 2012, pp. 758-765.
8. P. Pourghomi, M. Saeed, and G. Ghinea, "A secure cloud-based NFC mobile payment protocol," *International Journal of Advanced Computer Science and Application*, Vol. 5, 2014, pp. 24-31.
9. J. Wang, J. Liu, X. Li, and W. Kou, "Fair *e*-payment protocol based on blind signature," *The Journal of China Universities of Posts and Telecommunications*, Vol. 16, 2009, pp. 114-118.
10. C. Fan, V. Huang, and Y. Yu, "User efficient recoverable off-line *e*-cash with fast anonymity revoking", *Mathematical and Computer Modelling*, Vol. 58, 2013, pp. 227-237.
11. W. Juang, "Ro-cash: An efficient and practical recoverable pre-paid off-line *e*-cash scheme using bilinear pairings," *The Journal of Systems and Software*, Vol. 83, 2010, pp. 638-645.
12. L. Zhang, "Provably-secure electronic cash based on certificateless partially-blind signatures," *Electronic Commerce Research and Applications*, Vol. 10, 2011, PP. 545-552.
13. C. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, Vol. 4, 1991, pp. 161-174.
14. C. Fan, W. Sun, and V. Huang, "Provably secure randomized blind signature scheme based on bilinear pairing," *Computer and Mathematics with Application*, Vol. 60, 2010, pp. 285-293.
15. B. Kang, "New types of verifiably encrypted signature schemes," *Advanced Materials Research*, Vol. 490-495, 2012, pp. 914-918.
16. Y. Chen, J. Chou, H. Sun, and M. Cho, "A novel electronic cash system with trustee-based anonymity revocation from pairing," *Electronic Commerce Research and Applications*, Vol. 10, 2011, pp. 673-682.

17. Z. Eslami and M. Talebi, "A new untraceable off-line electronic cash system," *Electronic Commerce Research and Application*, Vol. 10, 2011, pp. 59-66.
18. Y. Baseri, B. Takhtaei, and J. Mohajeri, "Secure untraceable off-line electronic cash system," *Scientia Iranica*, Vol. 20, 2013, pp. 637-646.
19. B. Kang and D. Xu, "An untraceable off-line electronic cash scheme without merchant frauds," *International Journal of Hybrid Information Technology*, Vol. 9, 2016, pp. 431-442.
20. B. Kang and D. Xu, "Secure electronic cash scheme with anonymity revocation," *Mobile Information Systems*, Vol. 2016, Article ID 2620141.
21. C. Chan and C. Chang, "A new scheme for the electronic coin," in *Proceedings of IEEE International Conference on E-business Engineering*, 2006, pp. 339-343.
22. C. Fan, Y. Liang, and B. Lin, "Fair transaction protocols based on electronic cash," in *Proceedings of the 7th International Conference on Parallel and Distributed Computing*, *Applications and Technologies*, 2006, pp. 383-388.
23. X. Hou and C. Tan, "On fair traceable electronic cash," in *Proceedings of the 3rd Annual Communication Networks and Services Research Conference*, 2005, pp. 39-44.
24. C. Chen and M. Liu, "A traceable e-cash transfer system against blackmail via subliminal channel," *Electronic Commerce Research and Applications*, Vol. 8, 2009, pp. 327-333.

Bao-Yuan Kang (亢保元) received his M.S. in Algebra from the Shanxi University, and Ph.D. in Cryptography from Xidian University, P.R. 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.

Mu Wang (王牧) received his 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.

Dong-Ya Jing (景东亚) received his 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.