Electronic Commerce Research and Applications 10 (2011) 59–66

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/ecra

A new untraceable off-line electronic cash system

Ziba Eslami *, Mehdi Talebi

Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran

ARTICLE INFO

Article history:
Received 28 January 2009
Received in revised form 10 August 2010
Accepted 10 August 2010
Available online 18 September 2010

Keywords:
Electronic cash
Payment system
Blind signature
ElGamal signature scheme
Cryptography
Discrete logarithm

ABSTRACT

Digital content transactions through e-commerce will grow tremendously in the coming years. In this respect, well-designed electronic payment schemes and high-quality digital contents are two critical factors. Untraceable electronic cash schemes make it possible for customers to pay the e-cash to the merchants through communication networks under privacy protection. Therefore, there is a need to invent new electronic payment protocols with strong cryptographic algorithms that will eventually replace present day paper-based cash schemes. There have been two types of electronic cash schemes, namely on-line and off-line. In general off-line schemes are more efficient than on-line ones. The two fundamental issues with any off-line electronic cash scheme have been the detection of double-spending and provision of anonymity. This paper proposes a new untraceable off-line electronic cash scheme which can maintain anonymity and double spender detection and possesses strong fraud control capabilities. Moreover, the proposed scheme attaches expiration date to coins so that the banking system can manage its databases more efficiently. The scheme is based on cryptographic techniques such as ElGamal and blind signatures. The coins produced by the scheme can be transferred through computer networks into storage devices and vice versa so that portability is assured.

1. Introduction

Due to the fast progress of computer technologies, the efficiency of data processing and the speed of information generation have been greatly improved. Advanced network services, taking advantage of the new techniques, largely shorten the communicating time among distributed entities. Among these services, untraceable electronic cash (e-cash) is a popular one since it realizes the digitalization of traditional cash. These schemes make it possible to pay electronic money to the merchants through communication networks under privacy protection (Abe and Fujisaki 1996, Camenisch et al. 1994, Chaum 1983, Chaum et al. 1988, Fan and Lei 1998, Fan et al. 1999, Ferguson 1994, Okamoto and Ohta 1991, Pfitzmann and Waidner 1997, Westland et al. 1997). However, in spite of the benefits that electronic payments seem to have, except for the widely recognized credit/debit systems, it is still early days in the world of digital money and we are within a transition period towards a globally acceptable electronic cash scheme. One reason might be that there should be a substantial investment on required infrastructures so that the deployment of new payment mechanisms in several environments offers comparative advantage over credit cards or traditional cash. Therefore, there is definitely a need to invent new electronic payment protocols with strong cryptographic algorithms which have the potential to replace present day cash schemes. There are a number of features that one might expect from an electronic cash scheme. We outline some of them below.

Anonymity: The spender of the cash must remain anonymous. If the coin is spend legitimately, neither the recipient nor the bank can identify the spender.

Unreusability: The digital cash cannot be copied and reused. Then we have to minimize the risks for forgery and establish a good authenticity system.

Unforgeability: Only authorized parties (i.e. the bank) can produce digital coins.

Off-line Payment: The transaction can be done off-line, meaning no communication with the central bank is needed during the transaction.

Transferability: Electronic coins can be circulated among people regardless of whether the transactions are on-line of off-line.

Divisibility: Digital cash can be divided into smaller amounts.

Portability: The security and use of digital cash is not dependent on any physical location. The cash can be transferred through computer networks into storage devices and vice versa.

In spite of the vast amount of ongoing research on digital cash, a universal e-cash scheme has yet to be devised. So far, many cash schemes have been proposed which tend to focus only on a limited

* Corresponding author.
E-mail addresses: z_eslami@sbu.ac.ir (Z. Eslami), mahdi.talebi@gmail.com (M. Talebi).

1567-4223/$ - see front matter © 2010 Published by Elsevier B.V.
doi:10.1016/j.elerap.2010.08.002

subset of expected properties. Only few of the proposed schemes are actually being used for on-line payment without the underlying support of some other electronic payment methods such as credit/debit cards. To date, research on e-cash has been directed primarily towards addressing security requirements through the design of suitable security protocols and mechanisms. The challenge is that approaches which try to satisfy all the above requirements end up to introduce very complex mathematics, heavy network traffic, and/or inefficient or risky implementation (Okamoto 1995). As an example, to achieve value-divisibility and double-spending detection, a cash scheme should either employ on-line authorities that records transactions and provides 'cash pools' for credit/debit or use special devices which can communicate only through private or dedicated lines. Double-spending is also a challenge in designing a transferable scheme where, for practical purposes, there is usually a limitation on the number of allowed transfers so that the cost of fraudulent transactions discovered after the fact, would not be huge. Thus, transferable schemes need some traceability mechanisms to identify malicious users, and as such cannot ensure at the same time full anonymity and security (Tewari et al. 1998).

In this paper, we propose an untraceable off-line blind-signature-based electronic cash scheme. Our proposed scheme attaches expiration date to each coin so that old coins can be exchanged for new ones by using a protocol called the *exchange protocol* (see Varadharajan et al. (1999), Wang et al. (2007), Fan (2006) for examples of schemes without this feature). This feature can greatly reduce the size of the databases the bank has to manage. The fraud control procedure for the proposed scheme proves that the scheme is highly secure against a variety of possible frauds. In order to achieve double spender detection, we employ a special signature scheme, the ElGamal signature scheme so that (as explained in Section 5.3) if the coin is spent twice, Spender's identity is revealed efficiently. The security of the scheme comes from the difficulty of the discrete logarithm problem and factoring of integers for large enough primes. We also prove anonymity in the standard model.

The rest of the paper is organized as follows. In Section 2, existing approaches on e-cash are reviewed. Section 3 briefly reviews techniques used throughout the paper. The proposed scheme is outlined in Section 4. Security analysis is covered in Section 5 and the fraud control procedure is described in Section 6. Comparisons are made in Section 7 and final conclusions are given in Section 8.

2. Existing approaches

The most widely used model for electronic payment schemes involves three different parties, namely a bank, spenders and merchants. The life cycle of a generic electronic coin involves all the parties. First, a spender withdraws the coin from the bank. The spender then sends the coin to a merchant in exchange for some goods and services. Finally, the merchant completes the cycle when he/she deposits the coin at the bank. There are three distinct phases in this cycle, the withdrawal phase, the payment phase, and the deposit phase. Prior to these, we have the initialization phase where necessary information such as public keys are generated, and the account opening phase where a user's account is registered with the bank. There are two types of electronic cash schemes namely on-line and off-line. In general off-line schemes are more efficient than on-line ones. In an on-line electronic cash, the payment and deposit phases occur in the same transaction. In other words, every coin is verified by the bank at the time of payment and this requires the bank to be on-line for every coin exchanged between the spenders and the merchants. In off-line electronic cash schemes, the coins are verified after the transaction at some convenient time for both merchants and the bank so that the bank does not have to be involved in every payment transaction. However, as the coins are not verified at the time of payment, there is a potential for dishonest spenders to double spend their coins. This is because digital cash, which is essentially a set of numbers, is easy to copy. Another requirement that can arise in electronic coins is the need for anonymity, that is, the privacy of the spenders may need to be protected. Hence, we would like to stress once again that anonymity and double-spending requirements make the design of secure efficient electronic payment schemes a challenging task.

Cut-and-choose technology was employed in Chaum (1983) as a way of addressing the double-spending problem in off-line anonymous electronic cash. Informally, each coin is constructed as k sets of two-element sets of numbers. Given any two numbers in the same set, anyone can compute the identity of the coin owner (the spender); if only one number in each set is known, regardless of the number of sets involved, it is computationally infeasible to identify the spender. When the spender wishes to spend the coin to a merchant, the spender has to reveal k different numbers, one from each set. The set of these numbers is normally referred to as the response, which is chosen blindly and randomly by the merchant. If the spender double spends any coin, the bank can eventually obtain two different numbers in the same set for the double-spent coin. This reveals the identity of the spender. However, this technique is highly inefficient in terms of the data exchanged between the spenders and the merchants during each payment as each coin contains $2k$ different numbers of reasonably large size. Subsequent to the original proposal, several improvements and new constructions have been proposed; see for instance (Ferguson 1994, Okamoto and Ohta 1991, Brands 1993, Camenisch et al. 1996, Ferguson 1994, Frankel et al. 1996, Yacobi 1995). Notably, the works of Brands (1993) and Ferguson (1994) achieve both double-spending detection and spender anonymity without using the cut-and-choose method.

Blind signatures, introduced by Chaum (1983) were initially used to design e-cash protocols. Subsequently, numerous untraceable electronic cash protocols were proposed based on these constructs (Chaum 1983, Fan and Lei 1998, Ferguson 1994, Pointcheval and Stern 1997, Camenisch et al. 1995, Pointchval and Stern 1996). In these schemes, the signature of the bank is used to generate a coin such that no link can be driven between the withdrawal and the deposit phase, i.e. the bank cannot link an e-cash to the blinded form of the coin without the blinding factor, which is kept secret by the spender.

Among the existing approaches one can name NetCash (Medvinsky and Neuman 1993) which satisfies many practical requirements but lacks anonymity, Mondex and Visa Cash which are card-based purses, and their on-line equivalents such as Ecash and Cybercoin (Mavridis et al. 1993, Mondex 1999). Here, we propose an e-cash scheme which satisfies important baseline requirements such as anonymity, unreusability, portability, and unforgeability and has therefore comparative advantage over most existing solutions.

3. Preliminaries

In this section, we briefly cover related techniques employed throughout the paper. We make use of the following lemma which is proved in Trappe and Washington (2006).

Lemma 1. *Let α be a primitive root for the prime p. For integers i and j, $g^i \equiv g^j \pmod p$ if and only if $i \equiv j \pmod{(p-1)}$.*

3.1. RSA encryption/decryption

Let $(p_X, q_X, n_X, e_X, d_X)$ be a set of RSA parameters for X, where p_X and q_X are two large primes, $n_X = p_X q_X$ and $e_X d_X \equiv 1 \pmod$

$(p_X - 1)(q_X - 1)$). (p_X, q_X, d_X) are private while (n_X, e_X) are public. RSA's public operation (encrypting/verifying) is applied over the message m using X's public key e_X, i.e. m is encrypted (verified) as $m^{e_X} \pmod{n_X}$. RSA's private operation (decrypting/signing) will be carried out using entity X's private key d_X so that m is decrypted/signed as $m^{d_X} \pmod{n_X}$. Clearly we have: $m^{d_X e_X} = m^{e_X d_X} = m \pmod{n_X}$.

3.2. Blind signatures

Blind signatures, introduced by Chaum (1983) were initially used to design e-cash protocols. Later Fujioka et al. (1993) utilized them in e-voting schemes. Blind signatures are used in cases where we need the signature of X on m and at the same time we do not wish to disclose the content of m to X. To get X's RSA-blind signature on a document m, choose a random number b as a blinding factor and give X the message $b^{e_X} m$ (i.e. a random multiple of m) to sign. X performs signing as $(b^{e_X} m)^{d_X} \pmod{n_X}$ which results in $bm^{d_X} \pmod{n_X}$. By removing the blinding factor from the signed message, (i.e. multiplying the signature by b^{-1}), we easily obtain the desired signature for m (i.e. m^{d_X}). Note that in order for $b^{-1} \pmod{n_X}$ to exist, we must have $gcd(b, n_X) = 1$.

3.3. The discrete logarithm problem

Let G be a cyclic group of order q with a generator g so that $G = \{g^0, g^1, \ldots, g^{q-1}\}$. Equivalently, for every $h \in G$, there is a unique $x \in Z_q$ such that $g^x = h$ and x is called the discrete logarithm of h with respect to g. The discrete logarithm assumption states that there exists a group G such that computing the discrete logarithm is hard and hence we have the discrete logarithm problem (DLP for short).

3.4. The ElGamal signature scheme

This signature is used in our scheme as a means for revealing identity of malicious coin owners who spend their coins more than once (see Section 5.3. The ElGamal signature was described in 1985. A modification of this scheme has been adapted as the Digital Signature Algorithm (DSA). This algorithm is non-deterministic which means that there are many valid signatures for any given message, and the verification algorithm must be able to accept any of these valid signatures as authentic. A complete treatment of the scheme can be found in Stinson (2005). Let p be a prime such that the discrete log problem in Z_p is intractable, and let $\alpha \in Z_p^*$ be a primitive element. Define $\kappa = \{(p, \alpha, w, g): g \equiv \alpha^w \pmod{p}\}$ as the set of all possible keys. The values p, α and g are the public key, and w is the private key. For $d \in Z_p^*, K = (p, \alpha, w, g) \in \kappa$, and a (secret) random number $y \in Z_{p-1}^*$, define

$$sig_K(d, y) = (u, \gamma)$$

where

$$u = \alpha^y \pmod{p},$$

and

$$\gamma = (d - wu)y^{-1} \pmod{(p-1)}.$$

To verify the signature (u, γ) on d, we observe that

$$ver(d, (u, \gamma)) = true \iff g^u u^\gamma \equiv \alpha^d \pmod{p}.$$

4. The proposed scheme

There are four participants in the scheme: a Central Authority (CA), the Bank (B), the Spender (S) and the Merchant (M).

Since the coins in the proposed scheme can be used over open (untrusted) channels such as the Internet, appropriate security concerns, namely privacy and authenticity must be considered. Privacy pertains to protecting against unauthorized disclosure of personal information (Law et al. 1996, Simplot-Ryl et al. 2009). Hence, a scheme should be designed such that the identity of honest coin owner is not revealed and at the same time a coin can not be traced back to its owner. Authenticity can be achieved by implementing infrastructures to ensure key management, user identification, and message integrity. Therefore, the authentication infrastructure is an entity separate from the bank which we call a central authority (CA) that considers identity and related proofs for the participants involved in payment transactions and binds public keys to an entity.

There are also five distinct phases: (1) the initialization phase where necessary information such as (certified) public keys are generated, (2) the withdrawal phase in which for each coin a 6-tuple integer with certain properties is generated, (3) the payment phase where necessary steps are taken to ensure that dishonest clients can not re-spent the coins, (4) the deposit phase in which the merchant deposits the accepted e-coin in the bank and a fraud control procedure is carried out to detect possible cheating, (5) the exchange phase where outdated coins (which are not already deposited or exchanged) can be exchanged with new valid ones.

The Bank maintains two tables: the *DepositTable* and the *ExchangeTable*. These tables are used in deposit and the exchange phase as well as the fraud control procedure.

Note that we use the notation $A \mapsto B(m)$ to denote that the message m is sent from entity A to entity B.

4.1. Initialization

In this phase is done by CA, first some parameters are fixed. It is assumed that the public keys corresponding to the Bank, Spender and Merchant are certified by (CA), i,e, each authenticated participant should be able to provide its digital certificate if asked.

Step 1. The central authority CA:
- 1.1 Selects a large prime p such that $q = (p-1)/2$ is also prime.
- 1.2 Selects α as square of a primitive root mod p.
- 1.3 Selects three public hash functions H, H_0 and H_1. The output of H and H_0 is an integer mod q. H takes a 3-tuple of integers as input while H_0 inputs 5-tuple integers.
- 1.4 Publishes p, α, H, H_0, H_1.

Note that Lemma 1 implies that for p, q and α we have $\alpha^{k_1} \equiv \alpha^{k_2} \pmod{p} \leftrightarrow k_1 \equiv k_2 \pmod{q}$.

Step 2. The Bank B:
- 2.1 Selects its RSA parameters as $(p_B, q_B, n_B, e_B, d_B)$ such that $(n_B > p)$.
- 2.2 Chooses a secret identity number x and computes $z \equiv \alpha^x \pmod{p}$.
- 2.3 Publishes z.

Step 3. The Spender S:
- 3.1 Selects its RSA parameters as $(p_S, q_S, n_S, e_S, d_S)$, where $n_S > p$.
- 3.2 Chooses an identity number m and random number r_m and computes $I \equiv (H_1(m \| \alpha^{r_m}), m)^{e_B} \pmod{n_B}$.
- 3.3 $S \mapsto B(I, \alpha^{r_m} \pmod{p})$.

Step 4. The Bank B:
- 4.1 Computes $I^{d_B} \pmod{n_B}$ to obtain m and stores m and $\alpha^{r_m} \pmod{p}$ along with identity information of the Spender (e.g., name, address, etc.) in its database.

4.2 Chooses a random number k and calculates the numbers
- $s = (m||k) \pmod p$,
- $v \equiv \alpha^s \pmod p$,
- $R \equiv v^x \pmod p$,

4.3 Stores s, k, v, R in its database.
4.4 $B \mapsto S(v^{e_S}, R^{e_S})$.

Step 5. The Merchant M chooses an identification number ID_M and registers it with the Bank.

The conditions on n_B and n_S are imposed to prevent the so-called re-blocking problem (see Menezes et al. 1996). Note that from the Bank's viewpoint, the Spender's identity is composed of m and α^{r_m}, where r_m is known only to the Spender. Therefore, I is computed as a function of both of these values. The value of r_m will be used later in exchange protocol to validate client's identity by a zero-knowledge technique. This value is also used in fraud control procedure (item 7) to prevent attackers from impersonating the Spender.

4.2. Withdrawal

The Spender contacts the Bank, asking for a coin. The Bank requires proof of identity (i.e. the digital certificate issued by *CA*), just as when someone is withdrawing classical cash from an account. All coins in the present scheme have the same value. A coin will be represented by a 6-tuple (u,g,A,r,A'',t) of numbers that are generated through the following steps (Fig. 1).

Step 1. The Spender S:
1.1 Decrypts v^{e_S}, R^{e_S} with his private key d_S and obtains the numbers v and R, i.e. S computes $v = (v^{e_S})^{d_S} \pmod{n_S}$ and $R = (R^{e_S})^{d_S} \pmod{n_S}$.
1.2 Chooses random numbers e, l, β_1, β_2 and y such that $gcd(y, p-1) = 1$, $gcd(l, n_B) = 1$, and $gcd(\beta_1, q) = 1$.
1.3 Computes
- $u \equiv \alpha^y \pmod p$,
- $w = (R||e)$,
- $g \equiv \alpha^w \pmod p$,
- $A \equiv v^{\beta_1}\alpha^{\beta_2} \pmod p$,
- $c \equiv \beta_1^{-1} H(u,g,A) \pmod q$,
- $a \equiv Al^{e_B} \pmod{n_B}$

1.4 $S \mapsto B(a,c)$.

Step 2. The Bank B:
2.1 Selects $t = (Date \parallel Time)$ as the expiration date of the coin.
2.2 Computes
- $c' \equiv cx + s \pmod q$,
- $A' \equiv (aH_1(t))^{d_B} \pmod{n_B} \equiv l(AH_1(t))^{d_B} \pmod{n_B}$.

2.3 $B \mapsto S(A', c', t)$.

Step 3. The Spender S:
- $r \equiv \beta_1 c' + \beta_2 \pmod q$,
- $A'' \equiv l^{-1}A' \pmod{n_B}$.

The coin (u,g,A,r,A'',t) is now complete.

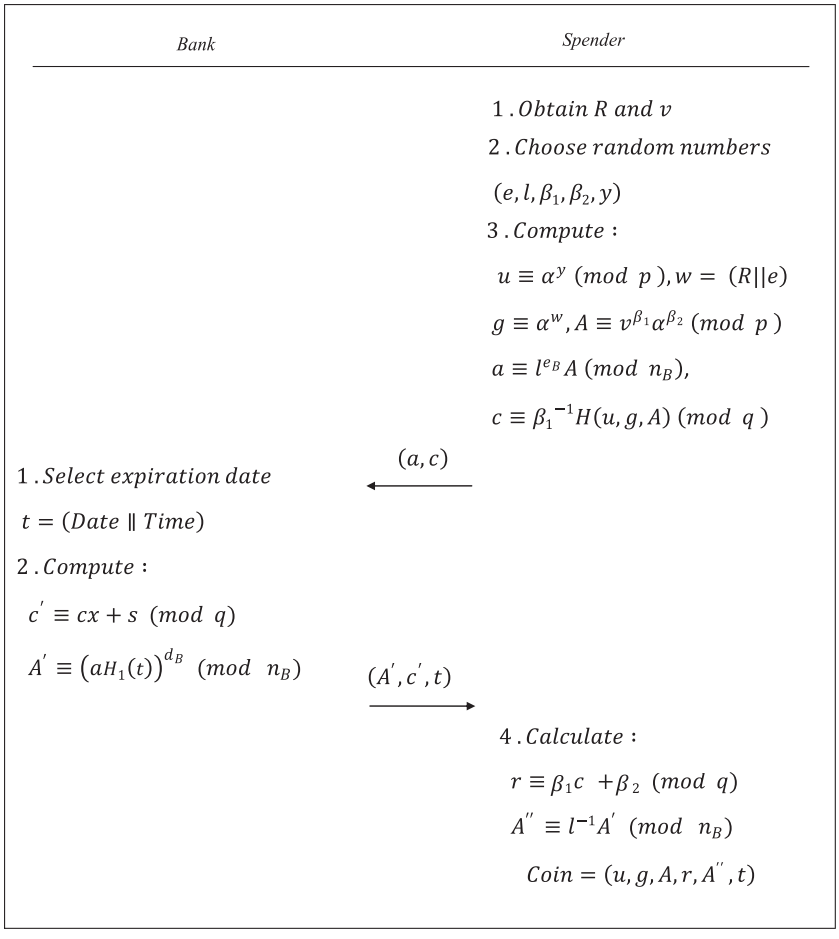

Fig. 1. Withdraw protocol.

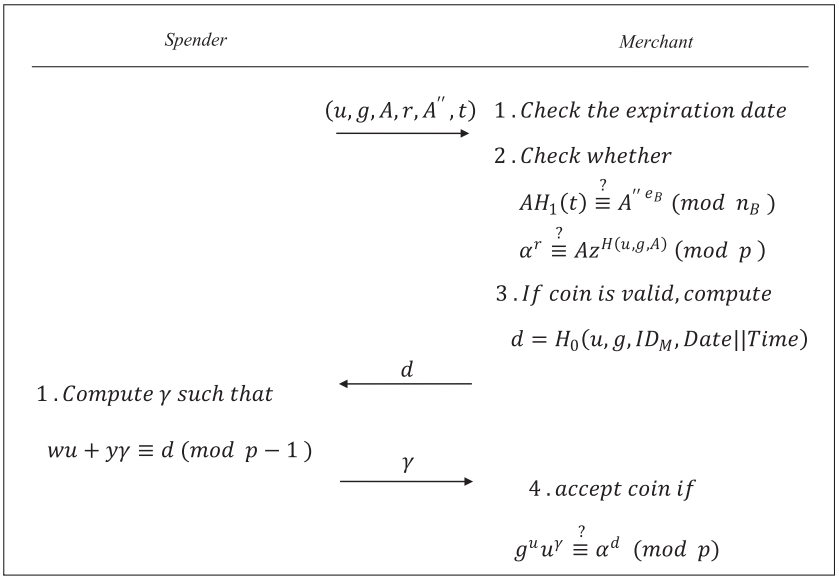

Fig. 2. Payment protocol.

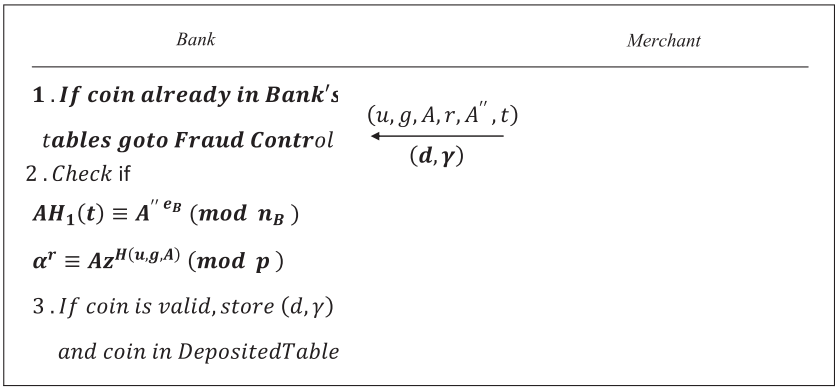

Fig. 3. Deposit protocol.

Lemma 2. *The coin (u,g,A,r,A'',t) constructed during withdrawal satisfies:*

(1) $AH_1(t) \equiv A''^{e_B} \pmod{n_B}$,
(2) $\alpha^r \equiv Az^{H(u,g,A)} \pmod{p}$,

Proof 3. Since A'' equals $(AH_1(t))^{d_B} \pmod{n_B}$, (1) is obvious. To prove (2), we first note that

$Az^{H(u,g,A)} \pmod{p} \equiv \alpha^{s\beta_1+\beta_2+xH(u,g,A)} \pmod{p}$,

We also have

$s\beta_1 + \beta_2 + xH(u,g,A) \pmod{q} \equiv \beta_1 c' + \beta_2 \pmod{q} \equiv r$,

By Lemma 1, the proof is complete. □

4.3. Payment

The details of this phase are also depicted in Fig. 2.

Step 1. $S \mapsto M(u,g,A,r,A'',t)$.
Step 2. The Merchant M:
- 2.1 Checks the expiration date of the coin.
- 2.2 Checks whether

$$\alpha^r \equiv Az^{H(u,g,A)} \pmod{p}, AH_1(t) \equiv A''^{e_B} \pmod{n_B},$$

If this is the case, the Merchant knows by Lemma 2 that the coin is valid. However, more steps are required to prevent double spending.
- 2.3 Computes $d = H_0(u,g,ID_M,Date \parallel Time)$, where H_0 is the hash function in the initialization phase and *Date* and *Time* represent the date and time of the transaction.
- 2.4 $M \mapsto S(d)$.

Step 3. The Spender S:
- 3.1 Utilizes ElGamel's scheme to compute γ such that $wu + y\gamma \equiv d \pmod{p-1}$
- 3.2 $S \mapsto M(\gamma)$.

Step 4. The Merchant M accepts the coin if $g^u u^\gamma \equiv \alpha^d \pmod{p}$.

4.4. Deposit

The details of this phase are also depicted in Fig. 3.

Step 1. $M \mapsto B((u,g,A,r,A'',t),d,\gamma)$.
Step 2. The Bank B:
- 2.1 If the coin (u,g,A,r,A'',t) exits in either of the *DepositTable* or the *ExchangeTable*, skips to Fraud Control procedure.
- 2.2 If not, checks if

Table 1
The content of *DepositTable*.

CoinInformation	*Deposited by*	*Date*
$(u_1,g_1,A_1,r_1,A_1'',t_1,\gamma_1,d_1)$	*ID*1	*date*1
$(u_2,g_2,A_2,r_2,A_2'',t_2,\gamma_2,d_2)$	*ID*2	*date*2
.	.	.
.	.	.
.	.	.
$(u_n,g_n,A_n,r_n,A_n'',t_n,\gamma_n,d_n)$	*IDn*	*daten*

Table 2
The content of *ExchangeTable*.

CoinInformation	*Exchanged by*	*Date*
$(u_1,g_1,A_1,r_1,A_1'',t_1)$	*ID*1	*date*1
$(u_2,g_2,A_2,r_2,A_2'',t_2)$	*ID*2	*date*2
.	.	.
.	.	.
.	.	.
$(u_n,g_n,A_n,r_n,A_n'',t_n)$	*IDn*	*daten*

$$\alpha^r \equiv Az^{H(u,g,A)} \pmod p, AH_1(t) \equiv A''^{e_B} \pmod{n_B},$$

if so, the coin is valid by Lemma 2 and the Bank stores $((u,g,A,r,A'',t),d,\gamma)$ into *DepositTable* and transfers money to the Merchant's account.

The content of *DepositTable* may look like Table 1.

4.5. Exchange

In this phase, the Bank exchanges only outdated coins which are not in the *DepositTable* or the *ExchangeTable*. The owner of such coins, denoted by *Ow*, can present the coin to the Bank and receive a new coin with updated expiration date. The details are as follows.

Step 1. *Ow* presents his/her outdated coin together with *I* to the Bank which checks (using a zero-knowledge technique) if *Ow* knows the corresponding r_m and if the coin is valid according to Lemma 2. Now, a new coin can be generated.

Step 2. *Ow* Chooses random numbers $e', I', \beta_1', \beta_2'$ and y' such that $gcd\ (y', p-1) = 1$, $gcd\ (I', n_B) = 1$, and $gcd\ (\beta_1', q) = 1$. Then computes u', w', g', A_1, c', a' as in step *1.3* of Withdrawal protocol and sends a', c' to the Bank.

Step 3. The Bank computes c_1', A_1' as in steps 2.1 and 2.2 of Withdrawal protocol and sends these numbers along with t' to *Ow*.

Step 4. *Ow* computes r', A_1'' as in step 3 of Withdrawal protocol.

The new coin $(u', g', A_1, r', A_1'', t')$ is now complete. The Bank then updates *ExchangeTable*. The content of *ExchangeTable* may look like Table 2. Note that when a coin enters this table, then it is considered invalid and no further transaction on it can be performed. We elaborate more on this in the deposit phase and fraud control procedures.

5. Security analysis

According to the related researches (Chaum 1983, Cao et al. 2005), anonymity, unforgeability and double-spending detection are the most important security issues pertaining to electronic cash. In this section, we first prove that the proposed scheme achieves anonymity in the standard model. We then consider unforgeability and double-spending. Other fraud control procedures are discussed in the next section.

5.1. Anonymity

A payment protocol is anonymous if and only if the spender's identity is not revealed after the withdrawal phase. In order to prove that our scheme, denoted here by Π, achieves anonymity, we define an experiment $Exprt^{eav}_{\mathscr{A},\Pi}$ for a probabilistic polynomial-time eavesdropping adversary $\mathscr{A}$. The experiment is essentially a game played between the adversary $\mathscr{A}$ and an imaginary challenger who wants to test if $\mathscr{A}$ succeeds in revealing the identity of the coin owner. We show that even if $\mathscr{A}$ knows all the identity information of a particular spender *S*, it will be unable to distinguish the coins generated by *S* from a completely random coin, and hence the coins produced by the scheme are not linkable to their owners. In the following, we use the same notations as in Section 4.$Exprt^{eav}_{\mathscr{A},\Pi}$:

1. The withdrawal protocol of is executed for a spender *S* with identity *I*. The execution results in a transcript *Trans* containing all the messages exchanged between *S* and the Bank *B*, i.e. $Trans = \{(c', A', t), (c, a)\}$, and a coin $Coin_1 = (u_1, g_1, A_1, r_1, A_1'', t)$.
2. A random bit b is chosen. If $b = 0$ then a random valid coin $Coin_0 = (u_0, g_0, A_0, r_0, A_0'', t)$ is created.
3. $\mathscr{A}$ is given $Coin_b = (\hat{u}, \hat{g}, \widehat{A}, \hat{r}, \widehat{A}'', t), Trans$, plus all identity information of *S* that the Bank has (Id_S).
4. $\mathscr{A}$ then outputs a bit b'.
5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. In case that $Exprt^{eav}_{\mathscr{A},\Pi} = 1$, we say that $\mathscr{A}$ succeeds.

The fact that $\mathscr{A}$ is given the transcript *Trans* reflects that $\mathscr{A}$ eavesdrops on the entire execution of coin generation and sees all the exchanged messages. $\mathscr{A}$ is further given all the identity information of the Spender. Now, in the experiment, when a coin is produced by *S*, $\mathscr{A}$ is also given $Coin_b = (\hat{u}, \hat{g}, \widehat{A}, \hat{r}, \widehat{A}'', t)$ which is either the real coin $(u_1, g_1, A_1, r_1, A_1'', t)$ or a random valid coin $(u_0, g_0, A_0, r_0, A_0'', t)$. This is to define what it means for $\mathscr{A}$ to violate anonymity, i.e. the adversary succeeds to "break" anonymity of Π if it can correctly determine whether $Coin_b$ it was given, corresponds to the given execution of the protocol by *S*, or if $Coin_b$ is a completely random coin which is independent of the transcript. We say that Π achieves anonymity if the adversary succeeds with probability that is at most negligibly greater that 1/2.

To prove this, we first note that $Pr[b = 0] = Pr[b = 1] = \frac{1}{2}$. Now, the adversary receives $(Trans, Id_S, Coin_b)$, where $Coin_b$ is either the actual coin (if $b = 1$) or a random coin (if $b = 0$). Distinguishing between these two cases is equivalent to linking a coin to the Spender and violating anonymity. We have:

$$\begin{aligned}
Pr[Exprt^{eav}_{\mathscr{A},\Pi} = 1] &= \frac{1}{2} \cdot Pr[Exprt^{eav}_{\mathscr{A},\Pi} = 1 | b = 1] \\
&\quad + \frac{1}{2} \cdot Pr[Exprt^{eav}_{\mathscr{A},\Pi} = 1 | b = 0] \\
&= \frac{1}{2} \cdot Pr[\mathscr{A}(Trans, Id_S, Coin_1) = 1] \\
&\quad + \frac{1}{2} \cdot Pr[\mathscr{A}(Trans, Id_S, Coin_0) = 0] \\
&= \frac{1}{2} \cdot Pr[\mathscr{A}(Trans, Id_S, Coin_1) = 1] \\
&\quad + \frac{1}{2} \cdot (1 - Pr[\mathscr{A}(Trans, Id_S, Coin_0) = 1] \\
&\leqslant \frac{1}{2} + \frac{1}{2} \cdot |Pr[\mathscr{A}(Trans, Id_S, Coin_1) = 1] \\
&\quad - Pr[\mathscr{A}(Trans, Id_S, Coin_0) = 1],
\end{aligned}$$

The elements $\hat{u}$, $\hat{g}$ and $\widehat{A}$ in $Coin_b$ are random numbers from the viewpoint of every one except the Spender. The other elements of the coin are $\hat{r} = \beta_1 c + \beta_2 \ (mod\ q)$ and $\widehat{A}'' = l^{-1}\widehat{A}'$, where β_1, β_2 and l are randomly selected by S. Moreover,

$$c = \beta_1^{-1} H(\hat{u}, \hat{g}, \widehat{A}) \ (mod\ q),$$
$$a = l^{e_B}\widehat{A} \ (mod\ n_B)),$$

Therefore, from (a,c) in $Trans$, and $\hat{u}, \hat{g}$ and $\widehat{A}$ in $(u_1, g_1, A_1, r_1, A_1'', t)$ or $(u_0, g_0, A_0, r_0, A_0'', t)$, $\mathscr{A}$ would obtain a different value for β_1 and l. Hence, all values of β_1 and l occur with the same probability and this means that $|Pr[\mathscr{A}(Trans, Id_S, Coin_1) = 1] - Pr[\mathscr{A}(Trans, Id_S, Coin_0) = 1] \leqslant \varepsilon$ where ε is negligible and therefore:

$$Pr[Exprt^{eavesdrop}_{\mathscr{A},\Pi} = 1] \leqslant \frac{1}{2} + \varepsilon.$$

Note that the numbers β_1 and β_2 are very important, since using the coin once does not allow identification of the Spender, but using it twice does.

To see the effect of β_1, β_2, suppose β_1 is essentially removed from the process by taking $\beta_1 = 1$. Then the Bank could keep a list of values of c, along with the person corresponding to each c. When a coin is deposited, the value of H would then be computed and compared with the list. Probably there would be only one person for a given c, so the Bank could identify the Spender.

5.2. Unforgeability

A payment protocol is unforgeable if and only if the e-coins can only be generated by the bank. Trying to make an unauthorized coin requires finding (u,g,A,r,A'',t) such that $\alpha^r \equiv Az^{H(u,g,A)}$ and $AH_1(t) \equiv A''^{e_B}$. Since A'' is the Bank's blind signature on A, assuming unforgeability of the signature, A'' can not be generated. Finding r that satisfies the other equation is equivalent to solving an instance of the discrete logarithm problem which is assumed to be hard in Z_p.

5.3. Double-spending detection

A payment protocol detects double-spending if and only if the e-coin can only be used once. Suppose that in the proposed protocol the Spender spends the coin twice, once with M, and once with V. Suppose that M is the first to deposit his coin along with (d,γ). Now, when V wants to deposit his coin with (d',γ'), the Bank finds out that the coin already exists in its tables. In this section, we show how the Bank can use properties of the ElGamal signature to identify the Spender who has done this. An easy calculation shows that

$$y(\gamma - \gamma') \equiv (d - d') \ (mod\ (p-1)),$$

hence, the Bank computes y. Now, From the equation in step 3.1 of the payment phase, we have

$$wu + y\gamma \equiv d \ (mod\ (p-1))$$

the Bank can obtain w and identify the Spender.

6. Fraud control in the proposed scheme

In this section, we consider various possible ways to cheat and how they are dealt with in the proposed scheme. It turns out the scheme has strong fraud control capabilities.

1. The Merchant tries submitting the coin twice, once with the legitimate pair (d,γ) and once with a forged pair (d',γ'). This is essentially impossible for the merchant to do, since by the infeasibility of the discrete logarithm problem, it is very difficult for the Merchant to produce numbers such that
$$g^u u^{\gamma'} \equiv \alpha^{d'} \ (mod\ p).$$
2. The malicious merchant MM receives a coin from the Spender and deposits it in the Bank, but also tries to spend the coin with the Merchant. MM gives the coin to the Merchant, who computes d', which very likely is not equal to d. MM does not knows w,y, but she must choose γ' such that $g^u u^{\gamma'} \equiv \alpha^{d'} \ (mod\ p)$. This again is a type of discrete logarithm problem. Since $d \neq d'$, the Merchant would find that $g^u u^{\gamma} \not\equiv \alpha^{d'}$. Hence, MM cannot simply use the γ that he/she already knows.
3. Someone working in the Bank tries to forge a coin. This person knows the numbers s, v, R, d_B. Therefore, it is possible to make a coin that satisfies $\alpha^r \equiv Az^{H(u,g,A)}, AH_1(t) \equiv A''^{e_B} \ (mod\ n_B)$. However, since the Spender has kept w, y secret, the person in the Bank will not be able to produce a suitable γ. Therefor he/she cannot spend the coin.
4. Someone steals the coin from the Spender and tries to spend it. The verification equations are satisfied, but the thief does not know w and y. Therefore, by intractability of the discrete logarithm problem, he/she will not be able to produce a suitable γ such that $g^u u^{\gamma} \equiv \alpha^d \ (mod\ p)$.
5. The malicious merchant MM, steals the coin and (d,γ) from the Merchant before they are submitted to the Bank. Unless the Bank requires merchants to keep records of the time and date of each transaction, and therefore be able to reproduce the inputs that produced d, MM's theft will be successful. This of course is a flaw of ordinary cash, too.
   In items 6 and 7 we denote the coin before and after exchange by $Coin$ and $ExchangedCoin$, respectively.
6. The malicious spender MS spends the $Coin$ in the last day of it's expiration date with merchant M_1, then exchanges the $Coin$ and spends the $ExchangedCoin$ with merchant M_2. There are two possibilities:
   - 6.1 M_1 deposits the $Coin$ first. Since $Coin$ exists in the $ExchangeTable$, it is considered invalid and the client who has exchanged it (MS) is found from $ExchangeTable$. However, since $ExchangedCoin$ does not exist in any of tables, then M_2 can safely deposit it.
   - 6.2 M_2 deposits $ExchangedCoin$ first. Since $ExchangedCoin$ does not exist in any of tables, then M_2 can safely deposit it. However, when M_1 deposits $Coin$ since it exists in the $ExchangeTable$, it is considered invalid and the client who has exchanged it (MS) is found.
7. Someone (E) steals $Coin$ from the Spender and tries to exchange it. According to exchange protocol, this is possible only if $Coin$ is not already in $DepositTable$ or $ExchangeTable$. Moreover, in order for E to be able to spend the coin, he/she must provide his/her own identification (i.e his/her I and r_m). Suppose that E can successfully exchange it for $ExchangedCoin$. This new coin can be spent and deposited, however, since the identity of E is saved in the entry of $ExchangeTable$ corresponding to $Coin$, then legitimate transactions on $Coin$ (such as deposit or exchange) will cause E to be found guilty.

7. Performance comparison

We summarize the computation and communication complexity of related e-cash schemes in Table 3. To make the discrete logarithm problem and the factoring problem intractable, we assume (Lenstra et al. 2003; FIPS, 2001) as in that p is 1024 bits, q is 160 bits and n is 1024 bits. Assume that the output size of secure one-way hash functions (FIPS, 2004) is 160 bits. Assume that H is the computation time of one hashing operation, M is the computation time of one modular multiplication in a 1024-bit modulo, and E is the computation time of one modular exponential operation in a 1024-bit modulo (Bertoni et al. 2008, Hankerson et al. 2008,

Table 3
Performance comparisons.

	Change and Lai	*Juang*	*Liu et al.*	*Our scheme*
C_1	$2E + 6M + 2H$	$3E + 6M$	$16E + 15M + 2H$	$5E + 9M + 1H$
C_2	$4E + 2H$	$1E + 2M$	$2E + 2M$	$1E + 2M + 1H$
C_3	$2E + 2H$	$2E + 2M$	$7E + 4M + 2H$	$6E + 3M + 2H$
C_4	4096	2528	2368	2368
C_5	Yes	No	No	No
C_6	No	Yes	Yes	No
C_7	Online	Off-line	Off-line	Off-line
C_8	Factoring	DLP	Factoring	DLP, factoring

C_1: Computation cost of the withdrawing and spending for Spender, C_2: Computation cost of the withdrawing for the Bank, C_3: Computation cost of the verifying e-coin for Merchant, C_4: Communication cost of withdrawing an e-coin (bits), C_5: Need for an untraceable e-mail system, C_6: Need for smart card, C_7: Transaction mode and C_8: The fundamental hard problem of the secure e-cash scheme.

Hohenberger 2006, Ramachandran et al. 2007, Schneier 1996, Takashima 2007).

We conduct a comparison among our scheme, the method of Chang and Lai (2003), Juang (2005), and Liu et al. (2005). The properties we consider are computation cost of the withdrawing and spending for Spender C_1, computation cost of the withdrawing for the Bank C_2, computation cost of the verifying e-coin for Merchant C_3, communication cost of withdrawing an e-coin in bits C_4, the need for an untraceable e-mail system C_5, the need for smart card C_6, transaction mode C_7, the hard problem of the security of e-cash scheme C_8.

8. Conclusions

In this paper, we propose a new off-line untraceable electronic cash system which not only can maintain anonymity but also can find double spender of the coin by using the ElGamal signature scheme. The security of the system is based on discrete logarithm problem and factoring problem. The electronic cash in our proposed scheme has an expiration date which enables the banking system to manage their database in a simple and affordable manner. The coins produced by the scheme can be transferred through computer networks into storage devices and vice versa which assures portability.

References

Abe, M., and Fujisaki, E. How to date blind signatures. In K. Kwangjo and M. Tsutomu (eds.), *Advances in Cryptology – ASIACRYPT'96 (LNCS 1163)*, Springer-Verlag, Berlin, 1996, 244–251.

Bertoni, G., Breveglieri, L., Chen, L., Fragneto, P., Harrison, K., and Pelosi, G. Pairing implementation for smart-cards. *Journal of Systems and Software*, 81, 7, 2008, 1240–1247.

Brands, S. Untraceable off-line cash in wallets with observers. In *Advances in Cryptology – Crypt'93 Proceedings. Lecture Notes in Computer Science*, Vol. 773, Springer, Berlin, 1993, 302–318.

Camenisch, J., Piveteau, J., and Stadler, M. An efficient fair payment system protecting privacy. In D. Gollmann (ed.), *ESORICS'94 (LNCS 875)*, Springer-Verlag, Berlin, 1994, 207–215.

Camenisch, J., Piveteau, J., and Stadler, M. Blind signatures based on the discrete logarithm problem. In A. D. Santis (ed.), *Advances in Cryptology – EUROCRYPT'94 (LNCS 950)*, Springer-Verlag, Berlin, 1995, 28–432.

Camenisch, J., Maurer, U., and Stadler, M. Digital payment systems with passive anonymity-revoking trustees. In *Computer Security – ESORICS'96 Proceedings. Lecture Notes in Computer Science*, Vol. 1146, Springer, Berlin, 1996, 31–43.

Cao, T., Lin, D., and Xue, R. A randomized RSA-based partially blind signature scheme for electronic cash. *Computers And Security*, 2005, 44–49.

Chang, C., and Lai, Y. A flexible date-attachment scheme on e-cash. *Computers and Security*, 2003, 160–166.

Chaum, D. Blind signatures for untraceable payments. In *Crypto 82*, Plenum Press, New York, 1983, 199–203.

Chaum, D., Fiat, A., and Naor, M. *Untraceable Electronic Cash*. Springer-Verlag, 1988. 319–327.

Fan, C. Ownership-attached unblinding of blind signatures for untraceable electronic cash. *Information Sciences*, 176, 2006, 263–284.

Fan, C., and Lei, C. User efficient blind signatures. *Electronics Letters*, 34, 6, 1998, 544–546.

Fan, C., Chen, W., and Yeh, Y. Blind signatures with double-hashed messages for fair electronic elections and ownership claimable digital cash. In J. Filipe (ed.), *Enterprise Information Systems*, Kluwer Academic, Dordrecht, 1999, 191–197.

Ferguson, N. Extensions to single term off-line coins. In *Advances in Cryptology – CRYPTO'93 Proceedings*, Springer, 1994, 292–301.

Ferguson, N. Single term off-line coins. In T. Helleseth (ed.), *Advances in Cryptology – EUROCRYP'93 (LNCS 765)765)*, Springer-Verlag, Berlin, 1994, 318–328.

FIPS PUB 186-2, 2001. Digital Signature Standard, National Institute of Standards and Technology, US Department of Commerce.

FIPS PUB 180-2, 2004. Secure Hash Standard, National Institute of Standards and Technology, US Department of Commerce.

Frankel, Y., Tsiounis, Y., and Yung, M. Indirect discourse proofs: achieving fair off-line e-cash. In *Advances in Cryptology – Asiacrypt'96 Proceedings. Lecture Notes in Computer Science*, Vol. 1163, Springer, Berlin, 1996, 286–300.

Fujioka, A., Okamoto, T., and Ohta, K. A practical secret voting scheme for large scale elections. In *Advances in Cryptology – AUCRYPT 92 Proceedings*, Springer, 1993, 15–19.

Hankerson, D., Menezes, A., and Scott, M. Software implementation of pairings. In M. Joye and G. Neven (eds.), *Identity-Based Cryptography. Cryptology and Information Security Series*, Vol. 2, 2008.

Hohenberger, S. Advances in signatures, encryption, and e-cash from bilinear groups. Ph.D. Dissertation, Massachusetts Institute of Technology, 2006.

Juang, W. A practical anonymous off-line multi-authority payment scheme. *Electronic Commerce Research and Applications*, 2005, 240–249.

Law, L., Sabett, S., and Solinas, J. How to make a mint: the cryptography of anonymous electronic cash. Technical Report, National Security Agency, Office of Information Security Research and Technology, Cryptology Division, 1996.

Lenstra, A., Tromer, E., Shamir, A., Kortsmit, W., Dodson, B., Hughes, J., and Leyland, P. Factoring estimates for a 1024-bit rsa modulus. In C. Laih (ed.), *Advances in Cryptology – AsiaCrypt'03. Lecture Notes in Computer Science*, Vol. 2894, 2003, 55–74.

Liu, K., Tsang, P., and Wong, S. Recoverable and untraceable e-cash. In *Second European PKI Workshop: Research and Applications, LNCS 3545*, Springer, New York, 2005, 206–214.

Mavridis, I., Pangalos, G., Koukouvinos, T., and Muftic, S. A secure payment system for electronic commerce. In *Proceedings of DEXA'99 Workshop*, IEEE Computer Society, Florence, Italy, 1993, 832–836.

Medvinsky, G., and Neuman, B. C. Netcash: a design for practical electronic currency on the internet. In *Proceedings of the 1st Annual ACM Conference on Computer and Communications Security*, ACM, 1993, 102–106.

Menezes, A., Van Oorschot, P., and Wanstone, S. *Chapter 11 in Handbook of Applied Cryptography*. CRC Press, 1996.

Mondex International. Introduction to mondex and electronic cash, document reference: tec-gui-760 v.2-0, 1999.

Okamoto, T. An efficient divisible electronic cash scheme proc.crypto95. In *Advances in Cryptology. Lecture Notes in Computer Science*, Springer, Berlin, 1995, 438–451.

Okamoto, T., and Ohta, K. Universal electronic cash. In *Advances in Cryptology – CRYPTO'91*, Springer-Verlag, 1991, 324–337.

Pfitzmann, B., and Waidner, M. Strong loss tolerance of electronic coin systems. *ACM Transactions on Computer Systems*, 15, 2, 1997, 194–213.

Pointcheval, D., and Stern, J. New blind signatures equivalent to factorization. In *Proceedings of the 4th ACM conference on Computer and Communication Security*, 1997, 92–99.

Pointchval, D., and Stern, J. Provably secure blind signature schemes. In K. Kwangjo and M. Tsutomu (eds.), *Advances in Cryptology – ASIACRYPT'96 (LNCS 1163)*, Springer-Verlag, Berlin, 1996, 252–265.

Ramachandran, A., Zhou, Z., and Huang, D. Computing cryptographic algorithms in portable and embedded devices. In *IEEE International Conference on Portable Information Devices*, 2007, 1–7.

Schneier, B. *Applied Cryptography*, second ed.. John Wiley and Sons Inc., 1996.

Simplot-Ryl, I., Traore, I., and Everaere, P. Distributed architectures for electronic cash schemes: a survey. *International Journal of Parallel, Emergent and Distributed Systems*, 24, 3, 2009, 243–271.

Stinson, D. R. *Cryptography Theory and Practice*, 3rd edition. CRC Press, Inc., 2005.

Takashima, K. Caling security of elliptic curves with fast pairing using efficient endomorphisms. *IEICE Transactions on Fundamentals*, E90-A, 1, 2007, 152–159.

Tewari, H., OMahony, D., and Peirce, M. Reusable off-line electronic cash using secret splitting. Technical Report, TCD-CS-1998-27, Computer Science Department, Trinity College Dublin, 1998.

Trappe, W. L., and Washington, C. *Introduction to Cryptography with Coding Theory*, 2nd ed.. Pearson Prentice Hall, 2006.

Varadharajan, v., Nguyen, K. Q., and Mu, Y. On the design of efficient rsa-based off-line electronic cash schemes. *Theoretical Computer Science*, 226, 1999, 173184.

Wang, C., Tang, Y., and Li, Q. Id-based fair offline electronic cash system with multiple banks. *Journal of Computer Science and Technology*, 22, 2007, 487–493.

Westland, J. C., Kwok, M., Shu, J., Kwok, T., and Ho, H. Electronic cash in Hong Kong. *Electronic Markets*, 7, 2, 1997, 3–6.

Yacobi, Y. Efficient electronic money. In *Proceedings of ASIACRYPT'94*, 1995, 153–163.