Schemes for Digital Gift Certificates with Low Computation Complexity

Ya-Fen CHANG[2], Chin-Chen CHANG[1,2]

[1]*Department of Information Engineering and Computer Science, Feng Chia University*
Taichung, Taiwan, 40724, R.O.C.
[2]*Department of Computer Science and Information Engineering*
National Chung Cheng University
Chiayi, Taiwan, 621, R.O.C.
e-mail: cyf@cs.ccu.edu.tw, ccc@cs.ccu.edu.tw

Received: November 2003

Abstract. Recently, e-commerce becomes widespread; hence electronic department stores come into being. As a result, Chan and Chang proposed a scheme for digital gift certificates in 2002. Because it is hard to estimate the number of the clients of the electronic department stores, reducing the computation complexity of the electronic department stores becomes an important issue. Due to the need, we propose two schemes for digital gift certificates. Our proposed schemes are very practical since the computation load is light. So the schemes can be applied to the terminals with low computation power.

Key words: digital gift certificate, e-commerce.

1. Introduction

In the real world, gift certificates are sold in the department stores for being used as currency in the gift-certificate-issuing department stores. A gift certificate contains a limited amount of money of the gift certificate holder. The holder can give the gift certificate to somebody as a present or sell it to anyone as the goods. When the holder wants to buy some goods, the amount of the spent digital certificate is usually less than the price of the goods. If the amount of the spent digital certificate is more than the value of the goods, no change will be given.

Nowadays, e-commerce becomes more and more popular. Lots of people purchase any desired goods over the Internet. The electronic department stores come into being because of the demand for convenience. As a result, Chan and Chang proposed the notion of digital gift certificates in 2002. In Chan and Chang's proposed scheme, the digital gift certificate holder can spend the digital certificate with the equivalent amount of the goods. In other words, the holder can be given change in Chan and Chang's scheme. This approach can provide the convenience of the clients since they do not need to make the different pay by other ways – credit cards for example. Before being spent, the digital gift certificate needs to be verified and checked whether it has been spent. If the digital gift certificate is ensured to be valid and not be spent before, the holder can spend it to buy the goods in the digital-gift-certificate-issuing electronic department stores. According to the above approaches, Chan and Chang also claimed that the digital gift certificate has a lower security condition than the digital cash. On one hand, unlike (Goh and Yip, 2000; Wang and Zhang, 2001; Bellare *et al.*, 2000; Ming *et al.*, 2000), the ownership of the digital gift certificate can be transferred easily in Chan and Chang's proposed scheme; what is more, no extra incentive is needed while the digital gift certificate is spent since no bank is involved in the scheme involving digital gift certificates. On the other hand, digital gift certificates provide the transference of the ownership, which is not provided by the traditional gift certificates.

The notion of digital gift certificates is meaningful and practical in the real world owing to the popularity of e-commerce. Since the clients of the electronic department stores purchase the goods over the Internet, it is hard to estimate the number of the clients. Hence the computation ability of the electronic department stores becomes the bottleneck if there are many clients want to purchase goods or buy the digital gift certificates. In other words, the computation complexity of the electronic department stores should be as low as possible. In order to reduce the overhead of the electronic department stores, we propose two schemes in this paper. One scheme owns the same characteristics of Chan and Chang's scheme, and the other provides another option of spending of the digital certificates with fixed quotas and makes the management of the digital certificates easier since the department store can control the frequency of spending.

This paper is organized as follows. In Section 2, we review Chan and Chang's proposed scheme. Then, our proposed schemes are presented in Section 3, followed by the security analyses in Section 4. In Section 5, we make more discussions over our proposed schemes. Finally, the conclusions will be given in Section 6.

2. The Previous Work

We review Chan and Chang's scheme for digital gift certificates (CC-DGC) (Chan and Chang, 2002) in this section. First, we list the requirements of the digital gift certificates in Subsection 2.1. In Subsection 2.2, we review CC-DGC.

2.1. *Requirements of Digital Gift Certificates*

In (Chan and Chang, 2002), authors claimed that the digital gift certificate is similar to the existing gift certificates found in the department stores. Each digital gift certificate contains some secret information from both of the electronic department store and the digital gift certificate buyer. The digital gift certificate can be verified and be prevented from being doubly spent. Moreover, even though there are duplicates of the digital certificate, only the valid digital certificate holder can spend the digital gift certificate. The ownership of the digital gift certificate can be transferred if the digital gift certificate is sold to another person or is given to somebody as a present.

The requirements of the digital certificates (Chan and Chang, 2002) are presented as follows:

Requirement 1. The digital gift certificate contains a unique serial number for the prevention of double spending of the digital gift certificate.

Requirement 2. The digital gift certificate is only generated by both of the electronics department store and the digital gift certificate buyer.

Requirement 3. The digital gift certificate preserves a unique ownership.

Requirement 4. The ownership of the digital certificate can be transferred.

2.2. *A Review of the Previous Work*

CC-DGC consists of three phases, which are setup phase, ownership transfer phase, and digital gift certificate spending phase, described in Subsections 2.2.1, 2.2.2, and 2.2.3, respectively.

2.2.1. *Setup Phase*

p is a public prime number, and g is a public primitive element of Z_p, where $g \in Z^*_{p-1}$. The department store D randomly chooses $x_D \in Z_p$ as the secret key and gets the public key y_D, where $y_D = g^{x_D} \bmod p$. The customer A has a secret key x_A and the public key y_A, where $y_A = g^{x_A} \bmod p$, as D. Suppose that A wants to purchase a digital gift certificate from D. A and D perform as follows:

Step 1. A chooses a random number t_A, where $t_A \in Z^*_{p-1}$, and computes

$$r_A = g^{t_A} \bmod p, \quad \text{and} \quad s_A = x_A + t_A r_A \bmod (p-1).$$

Step 2. A sends $\{A, D, s_A, r_A, M\}$ to D, where M denotes the relative information of the digital gift certificate – the amount of money contained in the digital gift certificate for example.

Step 3. D first checks whether $g^{s_A} = y_A r_A^{r_A} \bmod p$ holds or not to authenticate A. If it does not hold, D rejects the purchase request from A; otherwise, the phase is straightforward.

Step 4. D chooses a random number t_D, where $t_D \in Z^*_{p-1}$, and computes

$$\begin{aligned}
&r_D = g^{t_D} \bmod p,\\
&K_{D,A} = r_D \bmod p,\\
&r'_A = r_A \bmod p,\\
&s_D = h(M)(x_D + s_A) + t_D r_D \bmod (p-1), \quad \text{and}\\
&s_{D,A} = M^{sn \cdot r'_A{}^{t_D}} \bmod p,
\end{aligned}$$

where $h(m)$ is a public hash function with m as the input and sn represents the unique serial number, which is relatively prime to $(p-1)$, of the digital gift certificate. Thereupon, D generates the digital gift certificate $G_A = \{D, A, sn, M, r_A, r_D, s_D\}$ and the ownership $O_A = \{D, A, sn, s_{D,A}, r'_A, K_{D,A}\}$. Then, D sends G_A and O_A to A.

Step 5. After receiving G_A and O_A, A checks whether $g^{s_D} \equiv (y_D y_A r_A^{r_A})^{h(M)} r_D^{r_D} (\bmod\, p)$ and $M^{sn} \equiv s_{D,A}^{(K_{D,A}^{t_A})^{-1}} (\bmod\, p)$, where $K_{D,A}^{t_A} \times (K_{D,A}^{t_A})^{-1} \equiv 1(\bmod\, (p-1))$. If they do hold, A is convinced that G_A and O_A are valid.

2.2.2. *Ownership Transfer Phase*

Suppose the scenario that A wants to sell the owned digital gift certificate to B or gives B the digital gift certificate as a present. The procedures of the ownership transfer phase are presented as follows:

Step 1. A sends r'_A to B over the secure channel.

Step 2. B chooses a random number t_B, where $t_B \in Z_{p-1}^*$, and computes

$$r'_B = {r'_A}^{t_B} \bmod p.$$

Then, B sends r'_B to A over the secure channel.

Step 3. Upon receiving r'_B, A computes

$$\begin{aligned} sn' &\equiv h(sn)^{K_{D,A}^{t_A}} (\bmod\, p), \\ \beta_{A,B} &\equiv x_A + t_A r'_B (\bmod\, p), \quad \text{and} \\ \bar{\beta}_{A,B} &\equiv \beta_{A,B}^{K_{D,A}^{t_A}} (\bmod\, p), \end{aligned}$$

and then sends $\{D, A, sn, sn', \bar{\beta}_{A,B}, r'_B\}$ to D for transferring the ownership of the digital gift certificate.

Step 4. D first computes $\beta'_{A,B} \equiv \bar{\beta}_{A,B}^{({r'_A}^{t_D})^{-1}} (\bmod p)$, where ${r'_A}^{t_D} \times ({r'_A}^{t_D})^{-1} \equiv 1(\bmod\, (p-1))$. Then, D checks whether $g^{\beta'_{A,B}} \equiv y_A {r'_A}^{r'_B} (\bmod\, p)$, and $sn' \equiv h(sn)^{{r'_A}^{t_D}} (\bmod\, p)$. If they hold, D believes that A wants to transfer the ownership to B and computes

$$\begin{aligned} s_{A,B} &= M^{sn \cdot {r'_B}^{t_D}} \bmod p, \quad \text{and} \\ K_{D,B} &= K_{D,A}^{t_D} \bmod p. \end{aligned}$$

Then, D updates the ownership O_A to O_B of the digital gift certificate with the serial number sn and sends O_B to A, where $O_B = \{D, A, sn, s_{A,B}, r'_B, K_{D,B}\}$.

Step 5. A sends G_A and O_B to B.

Step 6. B verifies the received digital gift certificate and the ownership by checking whether $g^{s_D} \equiv (y_D y_A r_A^{r_A})^{h(M)} r_D^{r_D} (\bmod p)$ and $M^{sn} \equiv s_{A,B}^{(K_{D,B}^{t_B})^{-1}} (\bmod p)$, where $K_{D,B}^{t_B} \times (K_{D,B}^{t_B})^{-1} \equiv 1(\bmod\, (p-1))$.

After the above steps, B gets the valid digital gift certificate G_A with the ownership O_B.

2.2.3. *Digital Gift Certificate Spending Phase*

Suppose A wants to purchase the goods at the electronics department store over the Internet with the digital gift certificate G_A. He/she performs as follows:

Step 1. A computes $S_1 = (sn + M)^{K_{D,A}^{t_A}} \bmod\ p$ and sends sn with S_1 to D.

Step 2. D retrieves the relative information of the digital gift certificate numbered sn and computes $M' \equiv S_1^{({r'_A}^{t_D})^{-1}} - sn \pmod p$, where $({r'_A}^{t_D}) \times ({r'_A}^{t_D})^{-1} \equiv 1(\mathrm{mod}\ (p-1))$. If $M' = M$ and G_A is not sent previously, D agrees the one who knows the common shared value ${r'_A}^{t_D} \bmod\ p$ to spend G_A. If A does not use the total amount of M, D needs to update the values of M, s_D, $s_{D,A}$.

3. The Proposed Schemes for Digital Gift Certificates

In this section, we are going to introduce our proposed schemes for digital gift certificates. In Subsection 3.1, the preliminaries and notations used in our proposed schemes are listed. Then, the proposed schemes will be shown in Subsections 3.2 and 3.3, respectively.

3.1. *Preliminaries and Notations*

First, the preliminaries will be shown in Subsection 3.1.1. Then, the notations used in the proposed schemes are listed in Subsection 3.1.2.

3.1.1. *Preliminaries*

In this subsection, the preliminaries are shown as follows. Public keys are needed in some approaches in the proposed schemes. With Public Key Infrastructure (PKI), each of the digital certificate holders and the electronic department stores owns a public key and a corresponding private key. In other words, any approach involving the public key cannot be executed before the used public keys are verified.

3.1.2. *Notations*

In the following, we list the notations used in our proposed schemes:

A, B – the customers,

S – the electronic department store,

$ID_A/ID_B/ID_S$ – the identity of $A/B/S$,

$PK_A/PK_B/PK_S$ – $A/B/S$'s public key,

$SK_A/SK_B/SK_S$ – $A/B/S$'s private key,

E_{PK}/D_{SK} – an asymmetric encryption/decryption scheme with a public key PK/a private key SK,

$F(\,)$, $H(\,)$ – one-way hash functions,

$||$ – the concatenation symbol,

$\oplus$ – the XOR operation,

$H^i(P)$ – hashing P i times,

K_A/K_B – A/B's secret computed by inputting a "pass-phrase" chosen by A/B himself/herself.

3.2. *Digital Gift Certificates with Unconstrained Spending* (*DGC-US*)

In this subsection, we will present the first scheme, in which the user can use the equivalent amount of money of the digital certificates to pay the bill. The scheme is comprised of three phases: the application phase, the ownership-transference phase, and the payment phase. In the following, these phases are demonstrated in Subsections 3.2.1, 3.2.2 and 3.2.3, respectively.

3.2.1. *The Application Phase*

Suppose the scenario that A wants to purchase a digital certificate, which contains the sum of money M, from S. A and S perform as follows:

Step 1. A sends $E_{PK_S}(M||ID_A||D_{SK_A}(M))$ to S.

Step 2. After getting the transmitted data in Step 1, S computes $D_{SK_S}(E_{PK_S}(M|| ID_A||D_{SK_A}(M)))$ to retrieve $(M||ID_A||D_{SK_A}(M))$. Then, S checks whether M and $E_{PK_A}(D_{SK_A}(M))$ are equal. If it holds, S generates a unique serial number sn. S randomly generates two large numbers $SEED_A$ and R_{A0}. S computes and sends $E_{PK_A}(M||ID_A||sn||SEED_A||D_{SK_S}(H(M||ID_A||sn|| SEED_A)))$, $SEED_A \oplus R_{A0}$, and $H(R_{A0})$ to A.

Step 3. Upon receiving the data sent from S, A computes $D_{SK_A}(E_{PK_A}(M||ID_A||sn|| SEED_A||D_{SK_S}(H(M||ID_A||sn||SEED_A))))$ to retrieve $(M||ID_A||sn|| SEED_A||D_{SK_S}(H(M||ID_A||sn||SEED_A)))$. Then, A checks whether $H(M|| ID_A||sn||SEED_A)$ and $E_{PK_S}(D_{SK_S}(H(M||ID_A||sn||SEED_A)))$ are equal. If it holds, A stores $(M, sn, ID_A, SEED_A)$ as the issued digital certificate, calculates $SEED_A \oplus (SEED_A \oplus R_{A0})$ and checks whether $H(SEED_A \oplus (SEED_A \oplus R_{A0}))$ is equal to $H(R_{A0})$; otherwise, it denotes that the data received is not sent from S. If $H(SEED_A \oplus (SEED_A \oplus R_{A0}))$ and $H(R_{A0})$ are equivalent, A computes $H^3(P_{A0}) \oplus H(R_{A0} + 1)$ and $H^2(P_{A0}) \oplus H(R_{A0} + 1)$, where $P_{A0} = H^{F(R_{A0})}(K_A \oplus SEED_A)$, and sends the computation results to S; otherwise, A may inform S to retransmit some necessary information.

Step 4. After getting the transmitted data, S checks whether $H(R_{A0}+1) \oplus (H^3(P_{A0}) \oplus H(R_{A0} + 1))$ and $H(H(R_{A0} + 1) \oplus (H^2(P_{A0}) \oplus H(R_{A0} + 1)))$ are equal to each other. If it holds, S records $(M, sn, ID_A, SEED_A, F(R_{A0}), H^3(P_{A0}))$ in the maintained database; otherwise, S will inform A to retransmit some necessary information for the verification of the digital certificate ownership.

3.2.2. *The Ownership-transference Phase*

In the previous subsection, we have shown how A buys a digital certificate from S. A may want to sell the digital certificate to B or sends it to B as a gift. In the following, the approaches to transfer the ownership are shown.

Step 1. A sends $E_{PK_B}(M||ID_A||sn||SEED_A||ID_B||D_{SK_A}(H(M||ID_A||sn|| SEED_A||ID_B)))$ to B.

Step 2. B verifies the received data as mentioned in Step 3 of the application phase. If the data sent in Step 1 is valid, B sends $E_{PK_S}(M||ID_A||sn||SEED_A||ID_B||$

$D_{SK_A}(H(M||ID_A||sn||SEED_A||ID_B)))$ to S; otherwise, B may ignore the deals or ask A to retransmit the necessary information.

Step 3. S verifies the received data as mentioned in Step 3 of the application phase. If the received data sent from B is valid, S is convinced that A indeed wants to transfer the ownership of the digital certificate to B. Then, S randomly generates two large numbers $SEED_B$ and R_{B0}. S computes and sends $E_{PK_B}(M||ID_B||sn||SEED_B||D_{SK_S}(H(M||ID_B||sn||SEED_B)))$, $SEED_B \oplus R_{B0}$, and $H(R_{B0})$ to B.

Step 4. After getting the transmitted data, B computes $D_{SK_B}(E_{PK_B}(M||ID_B||sn|| SEED_B||D_{SK_S}(H(M||ID_B||sn||SEED_B))))$ and then retrieves $(M||ID_B|| sn||SEED_B||D_{SK_S}(H(M||ID_B||sn||SEED_B)))$. If $H(M||ID_B||sn|| SEED_B)$ and $E_{PK_S}(D_{SK_S}(H(M||ID_B||sn||SEED_B)))$ are equal, B stores $(M, sn, ID_B, SEED_B)$ as the issued digital certificate, calculates $SEED_B \oplus (SEED_B \oplus R_{B0})$ and checks whether $H(SEED_B \oplus (SEED_B \oplus R_{B0}))$ and $H(R_{B0})$ are equivalent; otherwise, it denotes that the data received is not sent from S. If $H(SEED_B \oplus (SEED_B \oplus R_{B0}))$ and $H(R_{B0})$ are equal, B computes $H^3(P_{B0}) \oplus H(R_{B0}+1)$ and $H^2(P_{B0}) \oplus H(R_{B0}+1)$, where $P_{B0} = H^{F(R_{B0})}(K_B \oplus SEED_B)$, and sends them to S; otherwise, B may inform S to retransmit some necessary information.

Step 5. After getting the data sent from B, S checks whether $H(R_{B0}+1) \oplus (H^3(P_{B0}) \oplus H(R_{B0}+1))$ and $H(H(R_{B0}+1) \oplus (H^2(P_{B0}) \oplus H(R_{B0}+1)))$ are equal to each other. If it holds, S records $(M, sn, ID_B, SEED_B, F(R_{B0}), H^3(P_{B0}))$ in the maintained database; otherwise, S will inform B to retransmit some necessary information for authentication.

3.2.3. *The Payment Phase*

For A's tth usage of the issued digital certificate, A and S perform as follows:

Step 1. A sends AS and sn to S, where AS denotes the amount of spending and $AS \leqslant M$.

Step 2. After getting the data sent in Step 1, S checks whether $AS \leqslant M$. If it holds, S randomly generates a large number $R_{A,t}$ and sends $(F(R_{A,t-1}), SEED_A \oplus R_{A,t}, H(R_{A,t}+1) \oplus H^3(P_{A,t-1}))$, where $P_{A,t-1} = H^{F(R_{A,t-1})}(K_A \oplus SEED_A)$ to A.

Step 3. After receiving the transmitted data, A computes $H(SEED_A \oplus (SEED_A \oplus R_{A,t})+1) \oplus H^3(H^{F(R_{A,t-1})}(K_A \oplus SEED_A))$. Then, A checks whether the computation result is equal to $H(R_{A,t}+1) \oplus H^3(P_{A,t-1})$. If it holds, A can make sure that S is the valid electronic department store and computes $H(P_{A,t-1}) \oplus H(R_{A,t}+1), H^3(P_{A,t}) \oplus H(R_{A,t}+1)$, and $H^2(P_{A,t}) \oplus H(R_{A,t}+1)$, where $P_{A,t} = H^{F(R_{A,t})}(K_A \oplus SEED_A)$. Then, A sends $(H(P_{A,t-1}) \oplus H(R_{A,t}+1), H^3(P_{A,t}) \oplus H(R_{A,t}+1), H^2(P_{A,t}) \oplus H(R_{A,t}+1))$ to S and updates M to $(M - AS)$.

Step 4. After getting the transmitted data, S first authenticates A by checking whether $H^2(H(R_{A,t}+1) \oplus (H(P_{A,t-1}) \oplus H(R_{A,t}+1)))$ and $H^3(P_{A,t-1})$ are equivalent. If it does not hold, S will reject the purchase request from A; otherwise, S checks whether $H(R_{A,t}+1) \oplus (H^3(P_{At}) \oplus H(R_{A,t}+1))$ and $H(H(R_{A,t}+1) \oplus (H^2(P_{A0}) \oplus H(R_{A,t}+1)))$ are equal to each other. If it holds, S updates $(M, sn, ID_A, SEED_A, F(R_{A,t-1}), H^3(P_{A,t-1}))$ to $((M - AS), sn, ID_A, SEED_A, F(R_{A,t}), H^3(P_{A,t}))$ in the maintained database; otherwise, S will inform A to retransmit some necessary information for authentication.

3.3. *Digital Gift Certificates with Fixed-quota Spending (DGC-FS)*

In this subsection, we are going to demonstrate the other proposed scheme, which is different from the scheme mentioned in the above subsection. DGC-FS provides another option of spending of the digital certificates with fixed quotas. This approach can make the management of the digital certificates be easier since S can control the frequency of spending. In DGS-US, the customer pays $m * n$ dollars to buy the digital certificate, where m is the number of the quotas and n is the face value of the quota. Suppose the customer wants to buy the digital certificate containing one thousand dollars with the quota, of which the face value is one hundred. In the above scenario, m is 10 and n is 100. Whenever the customer purchases goods, of which the value is v, the customer uses m' quotas to pay the bill, where $m' * n \leqslant v$, and he/she only needs to make a deferred payment. If $m' * n > v$, the customer will not be given change. The characteristics, mentioned above, of DGS-US are the same as those of the existing gift certificates sold in the department stores. This scheme is comprised of three phases: the application phase, the ownership-transference phase, and the payment phase. In the following, these phases are demonstrated in Subsections 3.3.1, 3.3.2 and 3.3.3, respectively.

3.3.1. *The Application Phase*

Suppose the scenario that A wants to purchase a digital certificate, which contains the sum of money $M = m * n$, where m is the number of the quotas and n is the face value of the quota, from S. A and S perform as follows:

Steps 1 to 3 are almost the same as those in Subsection 3.2.1 except the followings: (1) M is replaced by m. (2) In Step 3, after ensuring that $H(SEED_A \oplus (SEED_A \oplus R_{A0}))$ and $H(R_{A0})$ are equivalent, A computes $P_{A0} = H^m(K_A \oplus SEED_A)$, $P_{A0} \oplus H(R_{A0}+1)$ and $H(P_{A0}) \oplus H(R_{A0}+1))$ instead of $P_{A0} = H^{F(R_{A0})}(K_A \oplus SEED_A)$, $H^3(P_{A0}) \oplus H(R_{A0}+1)$ and $H^2(P_{A0}) \oplus H(R_{A0}+1)$, and then A sends $P_{A0} \oplus H(R_{A0}+1)$ and $H(P_{A0}) \oplus H(R_{A0}+1))$ to S.

Step 4. After getting the transmitted data, S checks whether $H(H(R_{A0}+1) \oplus (P_{A0} \oplus H(R_{A0}+1)))$ and $H(R_{A0}+1) \oplus (H(P_{A0}) \oplus H(R_{A0}+1))$ are equal to each other. If it holds, S records $(m, sn, ID_A, SEED_A, P_{A0})$ in the maintained database; otherwise, S will inform A to retransmit some necessary information for the verification of the digital certificate ownership.

3.3.2. *The Ownership-transference Phase*

In the previous subsection, we have shown how A buys a digital certificate from S. A may want to sell the digital certificate to B or sends it to B as a gift. In the following, the approaches to transfer the ownership are shown.

Steps 1 to 4 are almost the same as those in Subsection 3.2.2 except the followings: (1) M is replaced by m. (2) In Step 4, after ensuring that $H(SEED_B \oplus (SEED_B \oplus R_{B0}))$ and $H(R_{B0})$ are equal, B computes $P_{B0} = H^m(K_B \oplus SEED_B)$, $P_{B0} \oplus H(R_{B0}+1)$ and $H(P_{B0}) \oplus H(R_{B0}+1)$ instead of $P_{B0} = H^{F(R_{B0})}(K_B \oplus SEED_B)$, $H^3(P_{B0}) \oplus H(R_{B0}+1)$ and $H^2(P_{B0}) \oplus H(R_{B0}+1)$, and B sends $P_{B0} \oplus H(R_{B0}+1)$ and $H(P_{B0}) \oplus H(R_{B0}+1)$ to S.

Step 5. After getting the data sent from B, S checks whether $H(R_{B0}+1) \oplus (H(P_{B0}) \oplus H(R_{B0}+1))$ and $H(H(R_{B0}+1) \oplus (P_{B0} \oplus H(R_{B0}+1)))$ are equal to each other. If it holds, S records $(m, sn, ID_B, SEED_B, P_{B0})$ in the maintained database; otherwise, S will inform B to retransmit some necessary information for authentication.

3.3.3. *The Payment Phase*

For generalization, it is supposed that A has used $(t-1)$ quotas of the digital certificate. S records $(m'', sn, ID_A, SEED_A, P_{A,t-1})$, where $m'' = (m-(t-1))$ and $P_{A,t-1} = H^{m''}(K_A \oplus SEED_A)$, in the database, and A stores $(m'', sn, ID_A, SEED_A)$ as the issued digital certificate. When A wants to purchase goods, of which the value is v, A uses m' quotas to pay the bill. There are two possible cases: (1) $m' * n \leqslant v$, and (2) $v < m' * n$. In the first case, A only needs to make a deferred payment by other approaches – credit card for example. In the second case, A will not be given change.

In the payment phase, A and S perform as follows:

Step 1. A sends (m', v, sn) to S.

Step 2. Upon getting (m', v, sn), S first checks whether $m' \leqslant m''$. If it holds, S randomly generates a large number $R_{A,t}$ and sends $(C, SEED_A \oplus R_{A,t}, H(R_{A,t}+1) \oplus P_{A,t-1})$ to A, where $C = m'' - m'$.

Step 3. After receiving the transmitted data, A computes $H(SEED_A \oplus (SEED_A \oplus R_{A,t})+1) \oplus H^{m''}(K_A \oplus SEED_A)$. Then, A checks whether the computation result is equal to $H(R_{A,t}+1) \oplus P_{A,t-1}$. If it holds, A can make sure that S is the valid electronic department store and sends $P_{A,t+m'-1} \oplus H(R_{A,t}+1)$ to S, where $P_{A,t+m'-1} = H^C(K_A \oplus SEED_A)$.

Step 4. After getting the transmitted data, S authenticates A by checking whether $H^{m'}(H(R_{A,t}+1) \oplus (P_{A,t+m'-1} \oplus H(R_{A,t}+1)))$ and $P_{A,t-1}$ are equivalent. If it does not hold, S will not grant the purchase; otherwise, S updates $(m'', sn, ID_A, SEED_A, P_{A,t-1})$ to $((m''-m'), sn, ID_A, SEED_A, P_{A,t+m'-1})$ in the maintained database.

4. Security Analyses

Here, we are going to demonstrate that our proposed schemes are secure. In the following, we show the possible attack scenarios.

4.1. *Attack Scenario* 1

An imposter Eve impersonates the user A to spend the digital gift certificate.

In both DGC-US and DGC-FS, the digital gift certificate holder A pre-shares a secret $SEED_A$ with S. $SEED_A$ is never transmitted without being encrypted in the application phase or the ownership-transference phase. In other words, only S and A know $SEED_A$. In the payment phase, for the tth usage of the digital gift certificate, $SEED_A$ is used to protect the secret number $R_{A,t}$, which is treated as the session key to keep the updated password and the authentication pattern of the password secret. Besides, K_A is only known by A himself/herself. As mentioned above, it is obvious that Eve cannot spend A's digital gift certificate since Eve does not know $SEED_A$ to retrieve $R_{A,t}$ from the data, sent from S, and K_A to compute the correct authentication pattern of the password for the tth usage of the digital gift certificate.

4.2. *Attack Scenario* 2

An imposter Eve impersonates the digital gift certificate holder A to transfer the ownership of the digital gift certificate.

It is impossible for Eve to have the ownership of the digital gift certificate transferred since A must sign the transmitted data with A's secret key in Step 1 of the ownership-transference phase to prove the agreement of transference of the ownership of the digital gift certificate to another person. Hence, this attack will not succeed.

4.3. *Attack Scenario* 3

A, who is the valid digital gift certificate holder, wants to cheat B, who wants to purchase A's digital gift certificate, that the ownership is indeed transferred by impersonating S.

B can easily check whether A is cheating in the ownership-transference phase because S needs to sign the transmitted data with his/her own private key in Step 3, and B will check the validity of the digital gift certificate in Step 4. Since A does not know S's private key, A cannot successfully cheat B that the ownership is transferred.

4.4. *Attack Scenario* 4

An imposter Eve impersonates S to get the important information of the digital gift certificate such that Eve can spend it.

As mentioned previously, the valid digital gift certificate holder A pre-shares a secret $SEED_A$ with S. $SEED_A$ is only known by S and A. Even though Eve impersonates S, he/she cannot cheat A since A will authenticate S in Step 3 of the payment phase. If A finds out that someone pretends to be S, he/she will not send any meaningful information to the imposter. Obviously, the attack will not work in our proposed schemes.

4.5. *Attack Scenario* 5

An attacker Eve wants to get the secret information from the transmitted data.

As mentioned in Subsection 4.1, Eve cannot get the secret information from the transmitted data. There are three powerful reasons: (1) the pre-shared secret $SEED_A$ is only known by S and A; (2) the updated password and the authentication pattern of the password secret are kept secret by the session key $R_{A,t}$ for the tth usage of the digital gift certificate; (3) K_A is only known by A himself/herself. Even if Eve eavesdrops the transmitted data between A and S, Eve still cannot get any meaningful information about the valid digital gift certificate.

4.6. *Replay Attack*

First, the session key $R_{A,t}$ for the tth usage of the digital gift certificate, is changed while t is different. Second, the password for authentication is also updated each time for spending the digital gift certificate. That is, such a kind of attacks will not be workable in our proposed schemes.

5. Discussions

In this section, we are going to make discussion on our proposed schemes. First, we prove that the proposed schemes achieve the requirements listed in Subsection 2.1. Second, we compare our proposed schemes with Chan and Chang's to show that our proposed schemes are both secure and efficient. At last, we present possible modifications of the proposed schemes.

5.1. *The Achieved Requirements*

In both DGC-US and DGS-FS, S generates a unique serial number sn for the sold digital gift certificate in Step 2 of the application phase. Second, $SEED_A$ is only known the valid digital gift certificate holder A. In the payment phase, S authenticates A with $SEED_A$ and checks whether the digital gift certificate is spent before. Hence, it is sure that our proposed schemes satisfy Requirement 1 such that the digital gift certificate contains a unique serial number for the prevention of double spending of the digital gift certificate.

As shown in Subsections 3.2.1 and 3.3.1, S shares a secret $SEED_A$ with the buyer A and stores $SEED_A$ and the corresponding authentication pattern combining $SEED_A$ with K_A, where K_A is only known by A. As described in Subsections 3.2.2 and 3.3.2, S updates the issuing digital gift certificate with the new digital gift certificate holder B with the pre-shared $SEED_B$ and the corresponding authentication pattern combining $SEED_B$ with K_B, where K_B is only known by B. The above approaches ensure that the issued digital gift certificate is only generated by both of the electronics department store and the digital gift certificate buyer. In other words, Requirement 2 is indeed achieved.

As mentioned previously, S still can determine the valid holder even if the ownership of the digital certificate has been transferred or there are copies of the digital gift certificates. In a word, it is obvious that the digital gift certificate preserves a unique ownership. That is, our proposed schemes satisfy Requirement 3. At last, it is sure that the ownership of the digital certificate can be transferred as shown in Subsections 3.2.2 and 3.3.2.

According to the above descriptions, it is confirmed that our proposed schemes achieve the requirements listed in Subsection 2.1.

5.2. *Comparison between our Proposed Schemes and Chan and Chang's Scheme*

Here, we compare our proposed schemes with Chan and Chang's scheme. First, we use Table 1 to show the performance analyses of the setup phase of CC-DGC and the application phases of DGC-US and DGC-FS, where A and S denote the digital gift certificate buyer and the electronic department store, respectively. We eliminate the number of fragmentary hash function operations to simplify the analyses. For example, A may hash the data two times to keep the data secret, and the number of the needed hash function operations is still recorded as 0. In DGC-US, there are a sequence of hash function operations needed. The size of this sequence is relative to $F(\,)$. As a result, we use F to represent the needed number of hash function operations. And, m denotes the number of the quotas.

Second, we use Table 2 to show the performance analyses of the ownership transfer phase of CC-DGC and the ownership-transference phases of DGC-US and DGC-FS. In

Table 1

Performance comparison of the setup phase of CC-DGC and the application phases of DGC-US and DGC-FS

Operations	Participants					
	CC-DGC		DGC-US		DGC-FS	
	A	D	A	S	A	S
Modular exponential	8	5	0	0	0	0
Public key en/decryption	0	0	2/2	2/2	2/2	2/2
Hash function operation	1	1	$6+F$	4	$4+m$	3
Total needed steps	5		4		4	

Table 2

Performance comparison of the ownership transfer phase of CC-DGC and the ownership-transference phases DGC-US and DGC-FS

Operations	Participants								
	CC-DGC			DGC-US			DGC-FS		
	A	B	D	A	B	S	A	B	S
Modular exponential	3	8	8	0	0	0	0	0	0
Public key en/decryption	0	0	0	1/1	3/2	2/2	1/1	3/3	2/2
Hash function operation	1	1	1	1	$7+F$	5	1	$5+m$	5
Total needed steps	6			5			5		

Table 2, A denotes the valid digital gift certificate holder, and A wants to transfer the ownership of the digital gift certificate to B, where S is the electronic department store.

At last, Table 3 is used to show the performance analyses of the spending phase of CC-DGC and the payment phases of DGC-US and DGC-FS, where m'' denotes the remained quotas and m' is the number of quotas to pay the bill. If the previous computation results are stored, the needed number of hash function operations can decrease. For a(b) in Table 3, a denote the number of hash function operations with maintaining the previous computation results, and b denotes that without maintaining the previous computation results. In CC-DGC, DGC-US, and DGC-FS, public keys are needed. As a result, certificates are needed to prove the validity of the public keys. Since public keys are involved in all CC-DGC, DGC-US, and DGC-FS, the computation for verifying public keys are eliminated.

The bit length of the product of $F(\,)$ does not need to be very long. Thus, simple hash functions (Chang, 1984a; Chang *et al.*, 1982; Chang, 1984b; Chang *et al.*, 1991) can be employed as $F(\,)$. On the other hand, the security of $H(\,)$ is demanded, so the secure hash function is required to be $H(\,) - SHA - 1$ (FIPS PUB 180-1) and $MD5$ (RFC 1321) for example. Any public key cryptosystem can be employed to encrypt or decrypt the messages – RSA (Rivest *et al.*, 1978) and ECC (Koblitz, 1987) for example.

From Tables 1, 2, and 3, we observe that the computation overhead of the participants in DGC-US and DGC-FS is smaller than that in CC-DGC. For example, RSA is a well-known public key cryptology, which also applies modular exponential operations. If we employ RSA in DGC-US and DGC-FS, it is obvious that the result is the same as the observation mentioned above. What is more, the needed steps in the application phase and the ownership-transference phase are fewer than those in CC-DGC. Although the steps in the payment phase of our proposed schemes are more than those in the spending phase of CC-DGC by two, the computation overhead of the electronic store S is reduced greatly such that S has the ability to allow multiple digital gift certificate holders to purchase the goods at the same time.

In our proposed schemes, according to the above observation, it is sure that the computation complexity of the electronic department stores is actually reduced; moreover, the

Table 3
Performance comparison of the spending phase of CC-DGC and the payment phases of DGC-US and DGC-FS

Operations	Participants					
	CC-DGC		DGC-US		DGC-FS	
	A	D	A	S	A	S
Modular exponential	2	2	0	0	0	0
Public key en/decryption	0	0	0/0	0/0	0/0	0/0
Hash function operation	0	0	$5+F$ $(8+2F)$	0	1 $(1+m'')$	$1+m'$
Total needed steps	2		4		4	

computation overhead of all the participants is also reduced. This is helpful for terminals with limited computation ability. We can sum up that our proposed schemes are really practical.

5.3. *Possible Modifications*

In this subsection, we are going to present the possible modifications of our proposed schemes.

5.3.1. *Adding Values of the Digital Gift Certificates*

DGC-US provides the same characteristics of Chan and Chang's proposed scheme; in addition, the number of spending the digital gift certificate is not limited due to the properties of DGC-US. For the digital gift certificate holder, having the will of adding the value of the held digital gift certificate is a strong probability. As a result, S can provide such service in DGC-US.

5.3.2. *Simplifying DGC-US*

We may reduce the number of hash operations in DGC-US. If the digital gift certificate holder does not have the will to add the value of the held digital gift certificate, S may just apply DGC-FS to DGC-US by setting m to be M, where m and M denote the number of quotas and the amount contained in the digital gift certificate, respectively. In one hand, this approach can reduce the needed number of hash operations in DGC-US; in the other hand, this approach will limit the service provided by S as mentioned in Subsection 5.3.1 and will not gain benefit if M is very large.

5.3.3. *Operating without Public Keys*

In fact, key derivation services without public keys are quite often superior in practice to PKI's or are at least widely deployed. However, applying public keys burdens the users since users need to verify the involved public keys before using them for computation. If public keys are not used, the trusted third party must involve in the interaction between all the participants. The overhead of the trusted third party, which is the bottleneck, will become an important issue.

6. Conclusions

As e-commerce becomes more and more popular nowadays, electronic department stores come into being. Hence, Chan and Chang proposed a scheme for digital gift certificates recently. Because it is hard to estimate the number of the clients of the electronic department stores, reducing the computation complexity of the electronic department stores becomes an important issue. Because of the need, we propose two schemes for digital gift certificates. According to Sections 4 and 5, it is obvious that our proposed schemes are not only secure but also practical since the computation complexity is reduced such that the terminals with low computation ability can easily handle the computation needed in the interactions between the participants. In a word, our proposed schemes are suitable for being used in the real world because of the security and the efficiency provided by them.

References

Bellare, M., J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. Van Herreweghen and M. Waidner (2000). Design, implementation, and deployment of the ikp secure electronic payment system. *IEEE Journal on Selected Area in Communications*, **18**(4), 611–627.

Chan, C.W., and C.C. Chang (2002). A scheme for digital gift certificates. In *Proceedings of the 2nd International Workshop for Asian Public Key Infrastructures* (*IWAP 2002*). Taipei, Taiwan, October 2002. pp. 136–141.

Chang, C.C. (1984a). The study of an ordered minimal perfect hashing scheme. *Communications of the Association for Computing Machinery*, **27**(4), 384–387.

Chang, C.C. (1984b). An ordered minimal perfect hashing scheme based upon Euler's theorem. *Information Sciences*, **32**(3), 165–172.

Chang, C.C., R.C.T. Lee and M.W. Du (1982). Symbolic gray code as a perfect multi-attribute hashing scheme for partial match queries. *IEEE Transactions on Software Engineering*, **SE-8**(3), 235–249.

Chang, C.C., C.Y. Chen and J.K. Jan (1991). On the design of a machine-independent perfect hashing scheme. *The Computer Journal*, **34**(5), 469–474.

FIPS PUB 180-1.

Goh, A., and W.K. Yip (2000). A divisible extension of the brands digital cash protocol: k-term coins implemented via secret sharing. In *Proceedings of TENCON 2000*, Vol. 3. Kuala Lumpur, Malaysia. pp. 452–457.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, **48**, 203–209.

Ming, Z., F. Yunbo and Y. Yixian (2000). Single-term divisible electronic cash based on bit commitment. In *Proceedings of 5th IEEE Symposium on Computers and Communications* (*ISCC 2000*). Antibes, France, pp. 280–285.

RFC 1321 – The MD5 Message-Digest Algorithm.

Rivest, R.L., A. Shamir and L. Adelman (1978). A method for obtaining digital signature and public key cryptosystem. *Communications of the ACM*, **21**(2), 120–126.

Wang, H., and Y. Zhang (2001). Untraceable off-line electronic cash flow in e-commerce. In *Proceedings of the 24th Australasian Computer Science Conference* (*ACSC 2001*). Australasian. pp. 191–198.

Y.-F. Chang received the BS degree in computer science and information engineering from National Chiao Tung University, Hsinchu, Taiwan in 2000. She is currently pursuing her PhD degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan. Her current research interests include electronic commerce, information security, cryptography, and mobile communications.

C.-C. Chang received the BS degree in applied mathematics in 1977 and the MS degree in computer and decision sciences in 1979, both from National Tsing Hua University, Hsinchu, Taiwan. He received his PhD in computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980–1983, he was on the faculty of the Department of Computer Engineering at National Chiao Tung University. From 1983 to 1989, he was among the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he has worked as a professor of the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2002, he has been a chair professor of National Chung Cheng University. His current research interests include database design, computer cryptography, image compression and data structure. Dr. Chang is a fellow of the IEEE, a fellow of the IEE, a research fellow of National Science Council of ROC, and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, the International Association for Crypto-logic Research, the Computer Society of the Republic of China, and the Phi Tau Phi Honorary Society of the Republic of China. Dr. Chang was the chair and is the honorary chair of the executive committee of the Chinese Cryptography and Information Security Association of the Republic of China.

Nedidelio skaičiavimų sudėtingumo schemos skaitmeniniams dovanų sertifikatams

Ya-Fen CHANG, Chin-Chen CHANG

Neseniai elektroninė komercija plačiai paplito; taigi atsirado elektroninės parduotuvės. To rezultate 2002 metais Chan ir Chang pasiūlė skaitmeninių dovanų sertifikatų schemą. Kadangi sunku įvertinti elektroninių parduotuvių klientų skaičių, tampa svarbu sumažinti elektroninių parduotuvių skaičiavimo sudėtingumą. Dėl šio poreikio mes siūlome dvi skaitmeninių dovanų sertifikatų schemas. Mūsų pasiūlytos schemos yra labai praktiškos del nedidelio skaičiavimo apkrovimo. Taigi šios schemos gali būti panaudojamos terminaluose su mažu skaičiavimų pajėgumu.