A Practical Anonymous Off-line Multi-authorities Payment Scheme for Electronic Commerce

Wen-Shenq Juang, Horng-Twu Liaw and Yenmun Huang

Department of Information Management
Shih Hsin University
Taipei, Taiwan, 116, R.O.C.
Email: [wsjuang, htliaw]@cc.shu.edu.tw

Abstract

We propose a practical anonymous off-line multi-authorities payment scheme. By means of our proposed scheme, the size of a bank's database is dramatically reduced and distributed to shops. Also, the issue of e-coins is controlled by several issuers, who represent a bank and can be chosen by the customer or assigned by the system, on the current available issuers list according to the Internet condition.

Keywords: *Multi-authorities Schemes, Off-line Payment Schemes, Privacy and Security, Tamper-proof Devices, Electronic Commerce.*

1 Introduction

Due to the fast progress of the Internet and wireless communications, many conventional services such as payments, auctions, voting and shopping, etc. can be conducted over it. However, these Internet services are still inhibited because of the concern of the lack of security. The critical success factors for an enterprise to implement and operate an e-business are money flow, material flow and information flow. Entrepreneurs have to provide various services on the Internet for keeping customers and attracting new ones for electronic commerce. From a customer's point of view, security, anonymity, efficiency, and flexibility are the main criteria of electronic payment schemes. Also, from the point of view of a bank or the government [2, 33], security, selective anonymity, e.g., anonymity is just for small payments, and implementation costs are most important.

So far, secure payment schemes have been investigated by many researchers from practical and theoretical points of view [1, 2, 3, 4, 5, 7, 9, 11, 12, 13, 14, 15, 24, 26, 32]. A typical secure payment scheme can be regarded as a protocol involving a customer, a shop and a bank. Both the customer and the shop have their accounts with the bank. There are two types of payment schemes for verifying the validity of an electronic payment transaction: off-line schemes and on-line schemes. In off-line schemes [1, 3, 4, 9, 11, 12, 13, 15, 26], each transaction during the protocol requires two participants (a customer and a shop) only. For preventing double-spending in advance and not just only allowing the detection of frauds and identification of cheaters after the fact, some off-line schemes use tamper-proof devices in the wallet [1, 3, 4, 12]. Off-line schemes without using the tamper-proof devices may not be adapted by a bank since she/he will get extra risk for double-spending [33]. In an on-line scheme [5, 7, 14, 24, 32], all participants, a customer, a shop and a bank, have to connected on-line when the customer buys some goods. In [22, 23]. Juang et. al. proposed on-line multi-authorities payment schemes. In [23], Juang et. al. used the concept of anonymous accounts to reduce the size of the bank's database. All proposed off-line payment schemes [1, 3, 4, 9, 11, 12, 13, 15, 26] are single authority schemes. The basic assumption of these schemes is that the single money issuer of these schemes is trustworthy. However, the money issuer may issue extra e-coins as she/he wishes. If the money issuer does that, it may cause great danger or hurt for the corporation or society.

In [10], Chaum et. al. proposed the concept of wallet with observers. It uses tamper-proof devices, such as Java cards, that the person

cannot modify or probe, to keep correct and secret databases. In this concept, a customer can use two modules to handle ordinary consumer transactions: (1) the tamper-proof module, called an observer, whose inner working is programmed by a trusted third party; and (2) the personal workstation whose inner working is totally under control of the customer. By this combined device, called a wallet, the two modules owned by a customer can keep his personal secret database and ensure the correctness of this database. Several single authority off-line payment schemes [1, 3, 4, 12] are based on the concept proposed in [10].

To remedy all the above problems, we propose a practical anonymous off-line multi-authorities payment scheme that satisfies security, anonymity, efficiency, and micropayment properties. In our proposed scheme, the bank's database is dramatically reduced and distributed to shops, and the issue of e-coins is controlled by several issuers. The bank will choose some reliable persons as the money issuers, and she/he can be regarded as a manager and can not issue any e-coin without the help of these reliable money issuers. The proposed scheme can not only satisfy real world environments without a single trusted authority or with some absent/dishonest authorities, but also can increase availability of the issuers, and increase protection against forgery by making it harder for the adversary to learn the group secret key.

2 Off-line multi-authorities payment scheme

In this section, we propose a practical anonymous off-line multi-authorities payment scheme. To reduce the bank's (the account manager's) database, the bank's database is distributed to shops. In our scheme, blind threshold signatures [19, 20] are used to distribute the power of a single trusted money issuer. The scheme involves a customer, shops, n e-coin issuers and a bank. The scheme consists of four phases: the preparation phase, the initialization phase**,** the withdrawing phase, and the paying phase. During the preparation phase, the bank first publishes all public parameters, and then all money issuers cooperate to generate their threshold verifiable public keys and distribute shares to each other without a trusted third party. In the initialization phase, the customer requests one pseudonym from the bank. In the withdrawing phase, a customer applies the uniquely blind threshold signature technique [18, 19, 20] to get a blind encrypted e-coin from t issuers and extracts the real e-coin from the encrypted e-coin. In the paying phase, if a customer decides to pay a shop some dollars, then she/he sends a PayWord [32] to the shop. The shop can check if the PayWord is valid and does not exceed the amount of the e-coin. If yes, she/he stores the PayWord in the database.

2.1 Basic assumptions

The underlying assumptions of this scheme are: (a) There are at least $(n-t+1)$ honest money issuers, where n is total number of money issuers and $t > n/2$ is the threshold value of the blind threshold signature scheme; (b) Every eligible customer can communicate with at least t out of n issuers, the shop and the bank; (c) There exist a secure blind signature scheme [7, 17, 29], a secure blind threshold signature scheme [19, 20], a secure secret key cryptosystem [34], a secure one-way permutation function [18, 28], and a secure and efficient one-way hashing function [31]; (d) There exist a secure public key signature scheme and a public key cryptosystem [30]; (e) There exists a secure anonymous channel [6, 8, 21]; (f) There exists a secure tamper-proof device [1, 3, 4, 12].

The concept of blind threshold signatures [19, 20] and one-way permutation functions combined with users' identifications [18] are used to realize a uniquely blind threshold signature scheme in our proposed scheme.

In [6, 8, 21], several anonymous channels have been proposed. The anonymous channels proposed in [6, 21] can be directly used in our scheme.

In [1, 3, 4, 12], several payment schemes based on the tamper-proof devices are proposed.

For simplicity, the message authentication in our protocol is achieved by a secure signature scheme [30] in which the signed message m is attached with its signature $Cert_d(\mathcal{H}(m))$, where $\mathcal{H}$ is a secure one-way hash function and d is the corresponding secret key of the signer. The verification of the signature can be achieved by the comparison method [25].

2.2 Notations

Let ξ be a public one-way permutation function [28, 18], let $\mathcal{H}$ be a public one-way hash function [31]. Let $n^{'}$ be the number of money issuers before the preparation phase, $QUAL$ be the set of non-disqualified money issuers after the preparation phase, let n be the number of non-disqualified money issuers $QUAL$. Let $\mathcal{I}_i, 1 \leq i \leq n^{'}$, denote the identification of money issuer i before the preparation phase. Let $I_i, 1 \leq i \leq n$, denote the identification of non-disqualified money issuer i after the preparation phase. Let C be the computer controlled by the customer, T be the tamper-proof device issued by the bank (or some trusted authority) for the customer, let d_b be the secret key chosen by the bank and let $d_{\mathcal{I}_i}$ be the secret key chosen by $\mathcal{I}_i$. Let d_T be the secret key stored in T when T is born and e_T be the corresponding public key. In a distributed environment, the bank and $\mathcal{I}_i$ can publish their corresponding public keys e_b and $e_{\mathcal{I}_i}$. Anyone can get e_b, and $e_{\mathcal{I}_i}$ via some authentication service (e.g., the X.509 directory authentication service [34]). Using secure public key signature schemes [30], $\mathcal{I}_i$ and the bank can produce signatures of messages using their own secret keys $d_{\mathcal{I}_i}$ and d_b. Anyone can verify these signatures using the corresponding public keys $e_{\mathcal{I}_i}$ and e_b. Let p and q be two large strong prime numbers such that q divides $(p-1)$, and let ρ and ζ be two generators of Z_p^* (*i.e.*, $\gcd(\rho, p) = 1, \gcd(\zeta, p) = 1$, $\rho \neq 1, \zeta \neq 1$) and ζ be a random value generated by a generic distributed coin flipping protocol. Let $g \equiv_p \rho^{(p-1)/q}$ and $h \equiv_p \zeta^{(p-1)/q}$. Let " $\cdot$ " denote the ordinal string concatenation operator, and let $x \equiv_p y$ denote $x = y \bmod p$. For making our scheme clear, we assume that the message transmitted in the following protocol is via an authentication scheme (e.g. the RSA signature scheme); that is, no one can fake any other's messages and no one can deny the messages she/he really transmitted.

2.3 The proposed scheme

Our proposed scheme is described in the following.

Phase 1 (the preparation phase)

The bank first publishes all public parameters n, t, p, q, g, h, all identifications $\mathcal{I}_i$, $1 \leq i \leq n'$, of possible e-coins issuers and the public one-way permutation ξ and the public one-way hash function $\mathcal{H}$. Then, all $\mathcal{I}_i$, $1 \leq i \leq n'$, must cooperate to distribute their secret shadows to each other. Each $\mathcal{I}_i, 1 \leq i \leq n'$, carries out the following steps:

1. $\mathcal{I}_i$ chooses a secret key $z_i \in Z_q$ and two secret polynomials $f_i(x) = \sum_{k=0}^{t-1} a_{i,k} x^k$ and $f_i^{'}(x) = \sum_{k=0}^{t-1} a_{i,k}^{'} x^k$ such that $a_{i,0} = z_i$, it computes $G_{i,k} \equiv_p g^{a_{i,k}} h^{a_{i,k}^{'}}$, $0 \leq k \leq t-1$, and it sends $(G_{i,k}, 0 \leq k \leq t-1))$ to $\mathcal{I}_j$, $1 \leq j \leq n'$, $j \neq i$.

2. Upon receiving $(G_{j,k}, 1 \leq j \leq n', j \neq i, 0 \leq k \leq t-1)$ from all other issuers, $\mathcal{I}_i$ sends $\delta_{i,j} \equiv_q f_i(x_j)$ and $\delta_{i,j}^{'} \equiv_q f_i^{'}(x_j)$, where x_j is a unique public number for $\mathcal{I}_j$, secretly to every $\mathcal{I}_j$, $1 \leq j \leq n'$, $j \neq i$.

3. When $\mathcal{I}_i$ receives all $\delta_{j,i}$ and $\delta_{j,i}^{'}$, $1 \leq j \leq n'$, $j \neq i$, from other issuers, she/he verifies if the shares $\delta_{j,i}$ and $\delta_{j,i}^{'}$received from $\mathcal{I}_j$ is consistent with the certified values $G_{j,l}$, $0 \leq l \leq t-1$, by checking whether $g^{\delta_{j,i}} h^{\delta_{j,i}^{'}} \equiv_p \prod_{l=0}^{t-1} (G_{j,l})^{{x_i}^l}$. If it fails, $\mathcal{I}_i$ broadcasts that an error has been found, publishes $\delta_{j,i}$ and $\delta_{j,i}^{'}$, the authentication information of $\delta_{j,i}, \delta_{j,i}^{'}$ and $\mathcal{I}_j$. Each issuer except the dishonest issuer $\mathcal{I}_j$ then marks $\mathcal{I}_j$ as a disqualified issuer and builds the set of non-disqualified issuers $QUAL$.

4. Every issuer $\mathcal{I}_i, i \in QUAL$, broadcasts $A_{i,k} \equiv_p g^{a_{i,k}}$, $0 \leq l \leq t-1$.

5. When $\mathcal{I}_i$, $i \in QUAL$, receives all $A_{i,k}$, $1 \leq j \leq n$, $j \neq i$, from other issuers in $QUAL$, she/he verifies whether $g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1} (A_{j,l})^{{x_i}^l}$. If this check fails for an index i, $\mathcal{I}_i$ broadcasts that an error has been found, publishes $\delta_{j,i}$, the authentication information of $\delta_{j,i}$ and $\mathcal{I}_j$. Any t issuers in $QUAL$ can compute $z_j, f_j(x), A_{j,k}, 0 \leq k \leq t-1$. Anyone then can compute the public shadows $\mathcal{V}_{j,i} \equiv_p g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1} (A_{j,l})^{{x_i}^l}$, where i and $j \in QUAL$, and the group public key $y \equiv_p \prod_{j \in QUAL} y_j \equiv_p \prod_{j \in QUAL} A_{j,0}$. The group public key y and all public shadows $\mathcal{V}_{j,i}$, where i and $j \in QUAL$, the personal public key $y_i \equiv_p A_{i,0} \equiv_p g^{z_i}$ can then be published by each issuer $\mathcal{I}_i$. Without loss of generality, we assume that n non-disqualified issuers $QUAL$ are I_i, $1 \leq i \leq n$. It can be done by renaming the index of each issuer $\mathcal{I}_i, i \in QUAL$.

(Phase 2) The initialization phase

Before a customer can request a blind threshold signature from the issuers, she/he must acquire one pseudonym from the bank. The public key of the pseudonym is signed by the bank by a secure blind signature scheme [7, 17, 29] and the corresponding secret key is stored in the temper-proof device T issued by some organization (e.g. the bank) and known only by this device T. The customer and the bank then carry out the following steps:

1. T sends a request information including the certificate $Cert_{d_T}(\mathcal{H}(RD))$, where RD contains some redundancy information indicating the registration, for a pseudonym to the bank.

2. The bank first verifies $T's$ identification by the certificate $Cert_{d_T}(\mathcal{H}(RD))$ using his corresponding public key e_T, and then use any secure blind signature scheme to issue a pseudonym for T. Let d_z be the secret key chosen by T and e_z be the corresponding public key. After the blind signature generation process, the secret key d_Z and the certificate of the corresponding public key $Cert_J(\mathcal{H}(e_z))$ is stored in T.

Phase 3 (the withdrawing phase)

Let ID_c be the identification of some customer. Without loss of generality, we assume that t out of the n issuers are I_j, $1 \leq j \leq t$. In this phase, ID_c (C and T) applies the uniquely blind threshold signature technique to get a blind e-coin from t honest issuers. ID_c, the bank, and $I_j, 1 \leq j \leq t$, then perform the following protocol.

1. Each I_j randomly chooses a number $k_j \in Z_q$, computes $\widehat{r_j} \equiv_p g^{k_j}$ and sends $\widehat{r_j}$ to ID_c.

2. After receiving all $\widehat{r_j}$, T computes $\mathcal{H}_x(\sigma)$, where σ is a random number and $\mathcal{H}_0(\sigma) = \sigma$, $\mathcal{H}_i(\sigma) = \mathcal{H}(\mathcal{H}_{i-1}(\sigma)), 1 \leq i \leq x$, and sends $\mathcal{H}_x(\sigma)$ to C. C then does the following.

   (a) Compute the value $m = H_{ID} \cdot RD \cdot \mathcal{H}_x(\sigma)$, where RD is the redundancy information for verification, $H_{ID} = \xi(ID_c \cdot \lambda)$ is a unique header, and λ is a random number used to avoid the attack by an exhaustive search.

   (b) Choose two random numbers $\alpha \in Z_q$ and $\beta \in Z_q^*$, and compute $r_j \equiv_p g^{\alpha}\widehat{r_j}^{\beta}$, $r \equiv_p m\prod_{k=1}^{t} r_k$ and $\widehat{m} \equiv_q \beta^{-1}r$.

   (c) Check if $\widehat{m} \neq 0$. If yes, sends $\widehat{m}$ to all $I_j, 1 \leq j \leq t$. Otherwise, go back to step (b).

3. Upon receiving message $\widehat{m}$, $I_j, 1 \leq j \leq t$, checks if ID_c has enough money in the bank. If not, I_j rejects the money withdrawing of ID_c. If yes, she/he informs the bank to deduct x dollars from ID_c's account and computes $\widehat{s_j} \equiv_q \widehat{m}(z_j + \sum_{l=t+1}^{n}(f_l(x_j)(\prod_{k=1,k\neq j}^{t}(\frac{-x_k}{x_j - x_k})))) + k_j$ and sends $\widehat{s_j}$ back to ID_c.

4. After receiving all $\widehat{s_j}$, $1 \leq j \leq t$, C computes $s_j \equiv_q \widehat{s_j}\beta_i + \alpha_i$, and checks if $g^{-s_j}y_j^r r_j \equiv_p (\prod_{l=t+1}^{n}(\mathcal{V}_{l,j}))^{(\prod_{k=1,k\neq j}^{t}(\frac{-x_k}{x_j - x_k}))(-r)}$, $1 \leq j \leq t$. If $\widehat{s_j}$ is not valid, it has to ask the corresponding issuer to send it again. Otherwise, C computes $s \equiv_q \sum_{j=1}^{t} s_j$ and sends $(r, s, m, 0, \mathcal{H}_x(\sigma))$ to T. T first computes $g^{-s}y^r r \equiv_p m = H_{ID} \cdot RD \cdot \mathcal{H}_x(\sigma)$ and checks if $\mathcal{H}_x(\sigma)$ is issued by himself. If yes, it then stores $(r, s, m, 0, \mathcal{H}_x(\sigma), \sigma)$ in its database.

5. After exact t issuers inform the bank to deduct x dollars from ID_c's account, the bank submits the deduction operation.

Phase 4 (the paying phase)

Let a customer has spent τ dollars in some shops for an e-coin $(r, s, m, \tau, \mathcal{H}_{x-\tau}(\sigma))$, where $\tau \leq x$. Let ID_s be the identification of a shop. If the customer decides to pay ID_s ϵ dollars, then she/he (C and T) and the shop do the following.

1. C sends $(r, s, m, \tau, \epsilon, \mathcal{H}_{x-\tau}(\sigma), ID_s)$ to T.

2. T checks that $(r, s, m, \tau, \mathcal{H}_{x-\tau}(\sigma))$ is in his database and $\tau + \epsilon \leq x$. If yes, it computes $Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s))$, stores $(r, s, m, \tau + \epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), \sigma)$ in his database and sends $Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s))$ and $\mathcal{H}_{x-\tau-\epsilon}(\sigma)$ back to C.

3. C then sends the e-coin $(r, s, m, \tau, \epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s)))$ representing ϵ dollars secretly to ID_s.

4. ID_s checks if $(r, s, m, \tau, \epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s)))$ is already in his database for double-spent checking. If not, she/he verifies if $g^{-s}y^r r \equiv_p m = H_{ID} \cdot RD \cdot \mathcal{H}_x(\sigma)$, where RD is the redundancy information for verification, $\tau + \varepsilon \leq x$, $\mathcal{H}_x(\sigma) = \mathcal{H}_{(\tau+\varepsilon)}(\mathcal{H}_{x-(\tau+\varepsilon)}(\sigma))$ and $Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s))$ is valid. If it is valid, ID_s records the e-coin $(r, s, m, \tau, \epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s)))$ representing ϵ dollars in his database. After some period of time, ID_s can send all e-coins secretly to the bank for exchanging the real money.

3 Discussions

3.1 Correctness

In our scheme, customers will first initial his tamper-proof device, withdraw blind e-coins, and extract real e-coins from the blind e-coins. When customers withdraw blind e-coins, to prevent an issuer from sending an invalid partial signature to a customer, a partial signature can be checked in step 4 of the withdrawing phase. The following lemma ensures the correctness of partial signatures.

Lemma 1 *The customer's partial signature (r_i, s_i) is valid if I_i is honest.*

Proof. By means of our scheme, we have

$$\begin{aligned}
& g^{-s_i} y_i^r r_i \\
\equiv_p\ & g^{-(\widehat{s_i}\beta+\alpha)} g^{z_i r}\ g^{\alpha} \widehat{r_i}^{\beta} \\
\equiv_p\ & g^{-(\widehat{m}(z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k})))+k_i)\beta} \\
& g^{z_i r} g^{k_i \beta} \\
\equiv_p\ & g^{-\widehat{m}(z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k})))\beta} g^{z_i r} \\
\equiv_p\ & g^{-\widehat{m} z_i \beta - \widehat{m} \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))\beta} g^{z_i r} \\
\equiv_p\ & g^{\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))(-\widehat{m}\beta)} \\
\equiv_p\ & (\prod_{j=t+1}^{n}(\mathcal{V}_{j,i}))^{(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))(-r)}
\end{aligned}$$

□

After the withdrawing phase, the threshold e-coin will be verified using the group public key in step 4 of the withdrawing phase. Lemma 2 ensures the correctness of the threshold e-coin.

Lemma 2 *The signature (r, s) generated in the withdrawing phase is a valid blind threshold signature on message m for the Nyberg-Rueppel signature scheme.*

Proof. The validity of the signature (r, s) can easily be established as follows.

$$\begin{aligned}
& g^{-s} y^r r \\
\equiv_p\ & g^{-(\sum_{i=1}^{t}(\widehat{s_i}\beta+\alpha))} g^{\sum_{i=1}^{n} z_i r} m(\prod_{i=1}^{t} r_i) \\
\equiv_p\ & m g^{-(\widehat{m}(\sum_{i=1}^{t} z_i + \sum_{i=1}^{t}(\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))))+\sum_{i=1}^{t} k_i)\beta - t\alpha} g^{\sum_{i=1}^{n} z_i r}(\prod_{i=1}^{t} g^{\alpha}\widehat{r_i}^{\beta}) \\
\equiv_p\ & m g^{-(\widehat{m}(\sum_{i=1}^{t} z_i + \sum_{j=t+1}^{n}(\sum_{i=1}^{t} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))))+\sum_{i=1}^{t} k_i)\beta} g^{\sum_{i=1}^{n} z_i r}(\prod_{i=1}^{t} g^{k_i\beta}) \\
\equiv_p\ & m g^{-(\widehat{m}(\sum_{i=1}^{t} z_i + \sum_{i=t+1}^{n} z_i))\beta} g^{\sum_{i=1}^{n} z_i r} \\
\equiv_p\ & m g^{-\widehat{m}\sum_{i=1}^{n} z_i \beta} g^{\sum_{i=1}^{n} z_i r} \\
\equiv_p\ & m g^{-r\sum_{i=1}^{n} z_i} g^{\sum_{i=1}^{n} z_i r} \\
\equiv_p\ & m.
\end{aligned}$$

□

For achieving the possibility of spending fractions of an e-coin in our scheme, we use the concept of PayWord chains proposed in [32] in our proposed scheme. In the paying phase, for paying ID_s ϵ dollars, a customer sends $(r, s, m, \tau, \epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s)))$ to the shop. The shop first checks if $(r, s, m, \tau, \epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s)))$ is already in his database for double-spent checking and then verifies the certificates $Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma)))$ for ensuring this e-coin is signed by a tamper-proof device issued by the bank and verifies whether the following equations holds.

$$\begin{aligned}
& \mathcal{H}_{(\tau+\varepsilon)}(\mathcal{H}_{x-(\tau+\varepsilon)}(\sigma)) \\
= \ & \mathcal{H}_x(\sigma).
\end{aligned}$$

In our scheme, we use the uniquely blind threshold signature technique [18, 19] to make our e-coins collision free; that is, all e-coins requested by honest customers are unique. We give the definition of a uniquely blind threshold signature scheme as following.

Definition 1 *A uniquely blind threshold signature scheme is a blind threshold signature scheme such that the signing function is injective and all the signatures requested by the honest customers are distinct.*

It is clear that the signature scheme used in the withdrawing phase is a uniquely blind threshold signature scheme since this scheme is a blind threshold signature scheme whose signing function is bijective (providing the message recovery capability) [19, 20] and the signed message $m = H_{ID} \cdot RD \cdot \mathcal{H}_x(\sigma) = \xi(ID_c \cdot \lambda) \cdot RD \cdot \mathcal{H}_x(\sigma)$ is unique [18].

3.2 Security analysis

In [16], Gennaro et. al. proposed an improved distributed key generation scheme based on discrete logarithm. They use the information-theoretic verifiable secret sharing protocol [27] to guarantee that no bias for a bit in the output group public key of the protocol is possible in their scheme. The shadow distribution phase of our scheme is based on the distributed key generation scheme in [16]. Different from the scheme in [16], in order to do cheater detecting when some issuer cheats, the public shadows ($\mathcal{V}_{j,i} \equiv_p g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1}(A_{j,l})^{x_i{}^l}$,where i and $j \in QUAL$) will be published by all issuers. All the public shadows ($\mathcal{V}_{j,i}$, where j and $i \in QUAL$) can be computed by the public values $A_{j,l} \equiv_p g^{a_{j,l}}, j \in QUAL, 0 \leq l \leq t-1$, broadcasted in Step 4 of the preparation phase. This public shadows will not disclose any extra information of the group secret key.

Keeping the privacy of customers from all the issuers and the bank is the most important property of our proposed scheme. Also, the amount of an e-coin spent by a customer must be less or equal to x dollars withdrawn from the issuers and the bank. Our proposed scheme preserves customers' anonymity, but not untraceability if the same e-coin is used for several transactions. Complete untraceability is preserved if each e-coin is used only once. We now show that our proposed scheme possesses the above two properties.

In our protocol, a malicious bank may try to derive the identification of the customer in the following possible ways: (1) Derive the identification of a customer who gets an pseudonym in the initialization phase. (2) Derive the link between the authentication message which is sent to the issuers in the withdrawing phase and the e-coin which is used in paying phase. (3) Derive ID_c from the e-coin (r, s, m).

To derive the identification of the pseudonym of a tamper-proof device owned by the customer in the initialization phase is computational infeasible since it clearly contradicts to the assumption that there exists a secure blind signature scheme.

To derive the link between the authentication message which is sent to the issuers in the withdrawing phase and the e-coin which is used in the paying phase is computational infeasible since it clearly contradicts to the assumption that there exists a secure blind threshold signature scheme.

To derive ID_c from the e-coin (r, s, m) is computational infeasible since it clearly contradicts with the assumption that ξ is a one-way permutation function.

From the above, the privacy of customers is preserved in our protocol.

In our protocol, when some customer spends some e-coin $(r, s, m, \tau, \epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\tau-\epsilon}(\sigma), ID_s)))$, the shop will check if this coin signed by the tamper-proof device T is in his database for preventing double-spending. So all withdrawn e-coins can be used only once. Also, an malicious customer Alice may try to spend extra e-coins in the following possible ways.

In our scheme, all issuers cooperate to generate threshold verifiable public keys. An eligible customer needs to withdraw an e-coin from t issuers. If Alice can generate an extra e-coin himself, then she can forge blind threshold signatures made by the issuers. It clearly contradicts to the assumption that the blind threshold signature scheme is secure.

Second, if Alice can make a counterfeit signature and pass the user authentication check performed by $I_j, 1 \leq j \leq t$, in the withdrawing phase, then she can get an extra e-coin. It clearly contradicts to the assumption that the RSA signature scheme is secure.

Third, given a used e-coin $(r, s, m, \tau, \mathcal{H}_{x-\tau}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\tau, \mathcal{H}_{x-\tau}(\sigma), ID_s)))$, which represents $\tau \leq x$ dollars and was spent by a customer, stored in the shop's database, if Alice can deriving another e-coin $(r, s, m, \epsilon, \mathcal{H}_{x-\epsilon}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\epsilon, \mathcal{H}_{x-\epsilon}(\sigma), ID_s)))$, which represents ϵ dollars, where $\tau < \varepsilon$, then she can spend extra money. The difficulty for the above operation relies on the strength of the one-way hash function $\mathcal{H}$ [31, 32] and the public key signature scheme [30].

Fourth, given a used e-coin $(r, s, m, \tau, \mathcal{H}_{x-\tau}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\tau, \mathcal{H}_{x-\tau}(\sigma), ID_s)))$, which represents $\tau \leq x$ dollars and was spent by a customer, stored in a shop's database, if Alice can deriving another e-coin $(r, s, m, \tau, \mathcal{H}_{x-\tau}(\sigma), Cert_{d_b}(\mathcal{H}(e_z)), e_z, Cert_{d_Z}(\mathcal{H}(\tau, \mathcal{H}_{x-\tau}(\sigma), ID_{s'})))$, which also represents τ dollars but will spent in another shop $ID_{s'}$, then she can spend extra money. It clearly contradicts to the assumption that the RSA signature scheme is secure.

From the above, no customer can spend the mount of an e-coin more than x dollars with-

drawn from the issuers and the bank in our protocol.

3.3 Performance considerations

In our scheme, the preparation phase only has to be executed once and can be done off-line. The initialization also only has to be executed once. The tamper-proof device can be used until the lifetime of this device expires. In the withdrawing phase, every customer will request a blind threshold signature as an e-coin. The size of a blind threshold signature is the same as the size of an individual signature and the verification process of a blind threshold signature is equivalent to that of an individual signature [19, 20]. In addition to verifying the validation of the e-coin, the extra computation required for spending fractions of an e-coin is just hashing [32]. The value $-x_k/(x_i - x_k)$, $1 \leq k \leq n$ and $k \neq i$, in Step 3 of the withdrawing phase can be computed off-line. So each issuer needs to compute only 1 modular exponentiation in our scheme, which is the same as in the underlying blind signature scheme. Compared with the underlying blind signature scheme, the extra cost for signing a blind threshold signature is $\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t} (\frac{-x_k}{x_i - x_k}))$ in Step 3 of the withdrawing phase, which contains $n-2$ modular multiplications and $n-t$ additions. To reduce the computational cost due to the customer, the partial signature verification in step 4 of the withdrawing phase is not done except when the final e-coin can not satisfy the verification equation done by T in step 4 of the withdrawing phase. The customer does not need to know the public shadows $\mathcal{V}_{l,j}$,where l and $j \in QUAL$, in advance except there exists some dishonest issuers in the withdrawing phase. In this approach, the customer only needs to compute 2 modular exponentiations and 1 modular inverse in step 2 of the withdrawing phase, which is the same as in the underlying blind signature scheme.

4 Conclusion

We have proposed a practical anonymous off-line multi-authorities payment scheme. By means of our scheme, the bank's database is dramatically reduced and distributed to shops. A customer can request an e-coin from several issuers, who represent a bank, on the current available issuers list according to the Internet condition.

Acknowledgment

This work was supported in part by the National Science Council of the Republic of China under contract NSC-90-2213-E-128-004.

References

[1] M. Anderson, The electronic check architecture, Technical Report Version 1.0.2, Financial Services Technology Consortium, September 1998.

[2] N. Asokan, P. Janson, M. Steiner and M. Waidner, "State of the art in electronic payment systems," *IEEE Computer*, Vol. 30, No. 9, pp. 28-35, 1997.

[3] J. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjolsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. de Rooij, B. Schoenmakers, M. Schunter, L. Vallee and M. Waidner, "The ESPRIT project CAFE-high security digital payment systems," Proc. of ESORICS'94, LNCS 875, Springer-Verlag, 1994.

[4] S. Brands, "Untraceable off-line cash in wallets with observers," Advances in Cryptology: Proc. of Crypt'93, LNCS 773, Springer-Verlag, pp. 302-318, 1993.

[5] J. Camenisch, J. Piveteau, and M. Stadler, "An efficient payment system protecting privacy," Proc. of ESORICS'94, LNCS 875, Springer-Verlag, pp. 207-215, 1994.

[6] D. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms," *Comm. of ACM*, Vol. 24, No. 2, pp.84-88, 1981.

[7] D. Chaum, "Blind signatures for untraceable payments," Advances in Cryptology: Proc. of Crypt'82, Plenum, NY, pp. 199-203, 1983.

[8] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," *Journal of Cryptology*, Vol. 1, pp. 65-75, 1988.

[9] D. Chaum, A. Fiat and M. Naor, "Untraceable electronic cash," Advances in Cryptology: Proc. of Crypt'88, LNCS 403, Springer-Verlag, pp. 319-327, 1990.

[10] D. Chaum and T. Pedersen, "Wallet databases with observers," Advances in Cryptology: Proc. of Crypt'92, LNCS 740, Springer-Verlag, pp. 89-105, 1993.

[11] D. Chaum and T. Pedersen, "Transferred cash grows in size," Advances in Cryptology: Proc. of EuroCrypt'92, LNCS 658, Springer-Verlag, pp. 390-407, 1993.

[12] Common Electronic Purse Specification, http://www.europay.com/SmartCard/html/Index_ceps.html.

[13] T. Eng and T. Okamoto, "Single-term divisible electronic coins," Advances in Cryptology: Proc. Of EuroCrypt'94, LNCS 950, Springer-Verlag, pp. 306-319, 1995.

[14] C. Fan and C. Lei, "Low computation partially blind signatures for electronic cash," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E81-A, No. 5, pp. 818-824, 1998.

[15] N. Ferguson, "Single term off-line coins," Advances in Cryptology: Proc. of EuroCrypt'93," LNCS 765, Springer-Verlag, pp. 318-328, 1993.

[16] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," Advances in Cryptology: Proc. of EuroCrypt'99, LNCS 1592, Springer-Verlag, pp. 295-310, 2000.

[17] P. Horster, M. Michels and H. Petersen, "Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications," Advances in Cryptology: Proc. of AisaCrypt'94, LNCS 917, Springer-Verlag, pp. 224-237, 1994.

[18] W. Juang and C. Lei, "A collision free secret ballot protocol for computerized general elections," *Computers & Security*, Vol. 15, No. 4, pp. 339-348, 1996.

[19] W. Juang and C. Lei, "Blind threshold signatures based on discrete logarithm," Proc. of Second Asian Computing Science Conference on Programming, Concurrency and Parallelism, Networking and Security, LNCS 1179, Springer-Verlag, pp. 172 -181, 1996.

[20] W. Juang and C. Lei, "Partially blind threshold signatures based on discrete logarithm," *Computer Communications*, Vol. 22, No. 1, pp. 73-86, 1999.

[21] W. Juang, C. Lei and C. Chang, "Anonymous channel and authentication in wireless communications," *Computer Communications*, Vol. 22, No. 15-16, pp. 1502-1511, 1999.

[22] W. Juang, H. Liaw, C. Lei and P. Yu, "A secure and anonymous multi-authorities e-cash scheme for electronic commerce," National Information Security Conference, pp. 281-288, Tainan, Taiwan, May 2001.

[23] W. Juang, H. Liaw and C. Lei, "A practical anonymous payment scheme for electronic commerce," The Seventh International Conference on Distributed Multimedia Systems, pp. 305-311, Taipei, Taiwan, September 2001.

[24] The NetBill Project. http://www.ini.cmu.edu /NETBILL/.

[25] T. Okamoto, "A digital multisignature scheme using bijective public key cryptosystem," *ACM Trans. on Computer Sciences*, Vol. 6, No. 8, pp. 32-441, 1988.

[26] T. Okamoto and K. Ohta, "Universal electronic cash," Advances in Cryptology: Proc. of Crypt'91, LNCS 576, Springer-Verlag, pp. 324-337, 1992.

[27] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," Advances in Cryptology: Proc. of Crypt'91, LNCS 576, Springer-Verlag, pp. 129-140, 1991.

[28] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Trans. on Inform. Theory*, Vol. IT-24, pp. 106-110, 1978.

[29] D. Pointcheval and J. Stern, "Provably secure blind signature schemes," Advances in Cryptology: Proc. of AisaCrypt'96, LNCS 1163, Springer-Verlag, pp. 252-265, 1996.

[30] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Comm. of ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[31] R. Rivest, "The MD5 message-digest algorithm," RFC 1321, Internet Activities Board, Internet Privacy Task Force, 1992.

[32] R. Rivest and A. Shamir, "PayWord and MicroMint–two simple micropayment schemes," Proc. of International Workshop on Security Protocols, LNCS 1189, Springer-Verlag, pp. 69–87, 1997.

[33] R. Rivest, "Perspectives on financial cryptography," the rump session at Financial Crypto'97, 1997.

[34] W. Stallings, *Cryptography and network security*, 2nd Edition, Prentice Hall International, 1999.