基於離散對數之公平盲目門檻式簽章
Fair Blind Threshold Signatures Based on Discrete Logarithm

莊文勝
Wen-Shenq Juang

台灣大學電機工程學系
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.
vimal@fractal.ee.ntu.edu.tw

雷欽隆
Chin-Laung Lei

台灣大學電機工程學系
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.
lei@cc.ee.ntu.edu.tw

摘要

在本篇論文中，我們提出一基於離散對數問題的群體導向公平盲目 (t, n) 門檻式簽章方案。藉由此方案，一包含 n 位簽章者的群體中，任何 t 位簽章者能代表此群體簽署一可用於匿名電子貨幣系統之公平盲目門檻式簽章。因爲盲目簽章方案提供完美的不可連結性，此匿名電子貨幣系統可能被犯罪者所濫用，諸如：取得贖款或洗錢。我們的方案允許法官(或主政者)送出可讓任何一位實際參予簽章的簽章者將其簽章時所見的過程與訊息簽章對相連結的資訊。在我們的方案中，一公平盲目門檻式簽章的大小與個別的公平盲目簽章一樣且簽章的驗證程序藉由一群體公開金匙簡化。我們的方案的安全性是基於計算離散對數的困難度上。

關鍵字：公平盲目簽章，門檻式簽章，離散對數，安全的電子貨幣系統。

Abstract

In this paper, we propose a group-oriented fair blind (t, n) threshold signature scheme based on the discrete logarithm problem. By the scheme, any t out of n signers in a group can represent the group to sign fair blind threshold signatures, which can be used in anonymous e-cash systems. Since blind signature schemes provide perfect unlinkability, such e-cash systems can be misused by criminals, e.g. to safely obtain a ransom or to launder money. Our scheme allows the judge (or the government) to deliver information allowing anyone of the t signers to link his view of the protocol and the message-signature pair. In our scheme, the size of a fair blind threshold signature is the same as that of an individual fair blind signature and the signature verification process is simplified by means of a group public key. The security of our scheme relies on the difficulty of computing discrete logarithm.

Keywords: Fair Blind Signatures, Threshold Signatures, Discrete Logarithm, Privacy and Security, Secure E-cash Systems.

1 Introduction

The concept of blind signature was introduced by Chaum [3]. It allows a requester to obtain signatures on the messages he provides to the signer without revealing these messages. A distinguishing property required by a typical blind signature scheme [1, 3, 8] is so-called the "unlinkability", which ensures that requesters can prevent the signer from deriving the exact correspondence between the actual signing process performed by the signer and the signature which later made public. The blind signatures can realize the secure electronic payment systems [3, 4, 7] protecting customers' anonymity, and the secure voting schemes [9, 10] preserving voters' privacy. In a distributed environment, the signed blind messages can be thought as fixed amount of electronic money in secure electronic payment systems, or as tickets in applications such as secret voting schemes. The security of the blind signature schemes proposed in [3] is based on the hardness of factorization [14] and the schemes proposed in [1, 8] is based on the hardness of computing discrete logarithm [6].

Instead of a single signer, two blind threshold signature schemes [11] have been proposed in a distributed environment, where several signers work together to sign a blind threshold signature. The schemes proposed in [11] allows t out of n participants in a group cooperating to sign a blind threshold signature without the assistance of a single trusted authority. In these schemes, the size of a threshold signature is the same as that of an individual signature and the signature verification process is equivalent to that of an individual signature. Therefore, these schemes are optimal with respect to the threshold signature size and the verification process.

Up to date, the on-line e-cash systems proposed by Chaum [3, 4] are more efficient and practical. The aim of these systems was to produce an electronic version of money which retains the same properties as paper cash. These systems involve customers, the bank and the shop. In real world environments, it is very hard to find any single authority as the bank. To cope with this dilemma, instead of a unique administrator, every customer needs to request blind threshold signatures as e-cashes from t administrators. The underlying assumption can be relaxed as follows: at least $(n - t + 1)$ of the n administrators do not conspire with the others. The blind threshold signature schemes can be directly applied to these secure e-cash systems for distributing the power of

a single authority. By these schemes, secure e-cash systems can meet the real world environments, such that, the issue of e-cashes is controlled by several authorities.

Since blind signature schemes provide perfect unlinkability, such e-cash systems can be misused by criminals, e.g. to safely obtain a ransom or to launder money [16]. To cope with the dilemma, the concept of fair blind signatures is introduced in [17]. In [17], three fair blind signature schemes are introduced to prevent the misuse of the unlinkability property. With the help of the judge, the signer can link a signature to the corresponding signing process. Since the fairness property is very important for preventing criminals from misusing the unlinkability property in e-cash systems, we propose a fair blind threshold signature scheme based on the blind threshold signature scheme proposed in [11] and the registration method proposed in [17]. Our scheme allows the judge to deliver information allowing anyone of the t signers to link his view of the protocol and the message-signature pair. In our scheme, the size of a fair threshold signature is the same as that of an individual fair signature and the signature verification process is simplified by means of a group public key. The proposed scheme provides the message recovery capability [13]. The security of our schemes relies on the difficulty of computing discrete logarithm and it is computationally infeasible for signers to derive the exact correspondence between the message they actually sign and all signers' complete views of the execution of the signing process without the assistance of the judge or the requester.

The paper is organized as follows. In Section 2, we present an efficient fair blind threshold signature scheme. Then we discuss its correctness, security and linkage recovery in Section 3. In Section 4, we describe some applications of the scheme. Finally, a concluding remark is given in Section 5.

2 The proposed scheme

In this section, we propose a fair blind threshold signature scheme with message recovery. In a typical signing process of a fair blind threshold signature scheme, there are three kinds of participants, the signers, the judge and a requester. Before the requester can obtain a signature from the signers, all the signers have to cooperate to distribute their secret shadows to other signers in advance. Then the requester acquires two pseudonyms from the judge and uses one of the pseudonyms to request a fair blind threshold signature from the signers. The proposed scheme consists of four phases: (1) the shadow distribution phase, (2) the registration phase, (3) the signature generation phase and (4) the signature verification phase. The shadow distribution phase is performed only once among the signers and then they can use their secret shadows to sign messages. In the registration phase, the requester requests two pseudonyms from the judge. One of the pseudonyms is used in the signature generation phase, whereas the other one is part of the signature. Thus, the judge, who knows the two corresponding pseudonyms, can link the message-signature pair with the corresponding signer's view. In the signature generation phase, a requester requests a blind signature from the signers by sending the pseudonym to the signers and the signers cooperate to issue the fair blind threshold signature to the requester. In the signature verification phase, anyone can use the group public key to verify if a fair threshold signature is valid.

Let U_i be the identification of signer i, n be the number of signers, t be the threshold value of the fair blind threshold signature scheme, m be the blind message to be signed, h be a secure one-way hashing function [15], p and q be two large strong prime numbers such that q divides $(p-1)$, and ρ be a generator of Z_p^* ($i.e.$, $\gcd(\rho, p) = 1$, $\rho \neq 1$). Let $g \equiv_p \rho^{(p-1)/q}$ and "$\cdot$" denote the ordinal string concatenation. Let d_i be the secret key chosen by U_i and d_J be the secret key chosen by the judge. In a distributed environment, U_i and the judge can publish their corresponding public keys e_i and e_J. Anyone can get e_i and e_J via some authentication service (e.g. the X.509 directory authentication service [18]). Using a secure public key signature scheme [6, 14], U_i and the judge can produce signatures (certificates) of messages by their own secret keys d_i and d_J. Anyone can verify these signatures by the corresponding public keys e_i and e_J. Let $Cert_{U_i}(w)$ be the signature (certificate) on message w produced by U_i and $Cert_J(w)$ be the signature on message w produced by the judge.

2.1 The shadow distribution phase

Before a requester can request a threshold signature from the signers, all signers must cooperate to distribute their shadows to other signers. In the shadow distribution phase, each U_i, $1 \leq i \leq n$, carries out the following steps:

1. U_i chooses a secret key $z_i \in Z_q$ and a secret polynomial $f_i(x) = \sum_{k=0}^{t-1} a_{i,k} x^k$ such that $a_{i,0} = z_i$, computes $\Psi_{i,k} \equiv_p g^{a_{i,k}}$ and the signatures $Cert_{U_i}(h(\Psi_{i,k}))$ on $\Psi_{i,k}$ for $0 \leq k \leq t-1$ and sends $((\Psi_{i,k}, Cert_{U_i}(h(\Psi_{i,k})), 0 \leq k \leq t-1)$ to U_j, $1 \leq j \leq n$, $j \neq i$.

2. Upon receiving $((\Psi_{j,k}, Cert_{U_j}(h(\Psi_{j,k}))), 1 \leq j \leq n, j \neq i, 0 \leq k \leq t-1)$ from all other signers, U_i verifies if all $Cert_{U_j}(h(\Psi_{j,k}))$ are valid. If yes, he sends $\delta_{i,j} \equiv_q f_i(x_j)$, where x_j is a unique public number for U_j, and a signature $Cert_{U_i}(h(\delta_{i,j}))$ on $\delta_{i,j}$ secretly to every U_j, $1 \leq j \leq n$, $j \neq i$. Otherwise, he publishes the invalid signatures and stops.

3. When U_i receives all $\delta_{j,i}$, $Cert_{U_j}(h(\delta_{j,i}))$, $1 \leq j \leq n$, $j \neq i$, from other signers, he verifies if the share $\delta_{j,i}$ received from U_j is consistent with the certified values $\Psi_{j,l}$, $0 \leq l \leq t-1$, by checking whether $g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1} (\Psi_{j,l})^{x_i{}^l}$. If it fails, U_i broadcasts that an error has been found, publishes $\delta_{j,i}$, $Cert_{U_j}(h(\delta_{j,i}))$ and the identification of U_j, and then stops. Otherwise, U_i computes the signature $Cert_{U_i}(h(y))$ on the group public key $y \equiv_p \prod_{l=1}^{n} y_l \equiv_p \prod_{l=1}^{n} \Psi_{l,0}$ and the signature $Cert_{U_i}(h(\Phi_{j,i}))$ on $\Phi_{j,i} \equiv_p g^{\delta_{j,i}}$, $1 \leq j \leq n$. He then sends $(Cert_{U_i}(h(y)), (\Phi_{j,i}, Cert_{U_i}(h(\Phi_{j,i})), 1 \leq j \leq n))$ to all other signers.

4. Upon receiving all $((Cert_{U_j}(h(y)), 1 \le j \le n, j \ne i), (\Phi_{l,j}, Cert_{U_j}(h(\Phi_{l,j})), 1 \le l \le n, 1 \le j \le n, j \ne i))$, U_i verifies if all $((Cert_{U_j}(h(y)), 1 \le j \le n, j \ne i), (Cert_{U_j}(h(\Phi_{l,j})), 1 \le l \le n, 1 \le j \le n, j \ne i))$ are valid. If yes, the shadow keys corresponding to the group secret key $z \equiv_q \sum_{j=1}^{n} z_j$ have been securely and correctly distributed. The group public key $y \equiv_p \prod_{j=1}^{n} y_j \equiv_p g^{\sum_{j=1}^{n} z_j}$, all signers' public keys y_j, $1 \le j \le n$, and all public shadows $\Phi_{l,j} \equiv_p g^{\delta_{l,j}}$, $1 \le l, j \le n$, can then be published by each signer. Otherwise, U_i publishes the invalid signatures and stops.

2.2 The registration phase

Before a requester requests a fair blind threshold signature from the signers, he must acquire two pseudonyms from the judge by performing the following steps.

1. The requester sends a request for pseudonyms to the judge.
2. The judge randomly chooses η and $\gamma \in Z_q$, computes $\Omega_0 \equiv_p g^{\eta}$ and $\Omega_1 \equiv_p \Omega_0^{\gamma}$, stores $(\gamma, \Omega_0, \Omega_1)$ and then sends the pseudonyms $(\eta, \gamma, \Omega_0, \Omega_1, Cert_J(h(\Omega_0)), Cert_J(h(\Omega_1)), Cert_J(h(\eta \cdot \gamma \cdot \Omega_0 \cdot \Omega_1)))$ back to the requester.
3. Upon receiving the pseudonyms $(\eta, \gamma, \Omega_0, \Omega_1, Cert_J(h(\Omega_0)), Cert_J(h(\Omega_1)), Cert_J(h(\eta \cdot \gamma \cdot \Omega_0 \cdot \Omega_1)))$, the requester verifies if $\Omega_0 \equiv_p g^{\eta}$, $\Omega_1 \equiv_p \Omega_0^{\gamma}$ and the certificates of pseudonyms are valid. If not, the requester has to ask the judge to retransmit a valid pair of pseudonyms.

2.3 The signature generation phase

Without loss of generality, we assume that t out of the n signers are U_i, $1 \le i \le t$. When a requester requests a fair blind threshold signature, he and the t signers perform the following steps during the signature generation phase.

1. The requester sends $\Omega_0, Cert_J(h(\Omega_0))$ to all $U_i, 1 \le i \le t$.
2. Upon receiving $\Omega_0, Cert_J(h(\Omega_0))$, each U_i verifies if $Cert_J(h(\Omega_0))$ is valid. If yes, each U_i randomly chooses a number $k_i \in Z_q$, computes $\hat{r}_i \equiv_p g^{k_i}$, $\Gamma_i \equiv_p \Omega_0^{k_i}$ and sends $\hat{r}_i$, Γ_i to the requester. Otherwise, he rejects it and stops.
3. After receiving all $\hat{r}_i$ and $\Gamma_i, 1 \le i \le t$, the requester does the following.
   (a) Choose two random numbers $\alpha \in Z_q$ and $\beta \in Z_q^*$, compute $\Gamma \equiv_p \prod_{i=1}^{t} \Gamma_i$, $r_i \equiv_p g^{\alpha} \hat{r}_i^{\beta}$, $v_1 \equiv_p m \prod_{i=1}^{t} r_i, v_2 \equiv_p (\Omega_1)^{(t\alpha)} \Gamma^{\gamma\beta}$ and $\hat{m} \equiv_q \beta^{-1} v_1$.
   (b) Check if $\hat{m} \ne 0$. If yes, send $\hat{m}$ to all $U_i, 1 \le i \le t$. Otherwise, go back to step (a).
4. Upon receiving $\hat{m}$, each U_i computes
$$u_i \equiv_p \Omega_0^{z_i + \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\ne i}^{t}(\frac{-x_k}{x_i - x_k}))} \quad (1)$$
and
$$\hat{s}_i \equiv_q \hat{m}(z_i + \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\ne i}^{t}(\frac{-x_k}{x_i - x_k}))) - k_i \quad (2)$$
and sends $\hat{s}_i$ and u_i back to the requester.
5. After receiving all $\hat{s}_i$ and $u_i, 1 \le i \le t$, the requester computes $s_i \equiv_q \hat{s}_i \beta + \alpha, 1 \le i \le t$, and checks if
$$g^{-s_i} y_i^{v_1} r_i \equiv_p (\prod_{j=t+1}^{n} (\Phi_{j,i}))^{(\prod_{k=1,k\ne i}^{t}(\frac{-x_k}{x_i - x_k}))(-v_1)}$$
and (3)
$$u_i \equiv_p (\Psi_{i,0}(\prod_{j=t+1}^{n} \Phi_{j,i})^{\prod_{k=1,k\ne i}^{t}(\frac{-x_k}{x_i - x_k})})^{\eta}, \quad (4)$$
$$1 \le i \le t.$$

If either $\hat{s}_i$ or $u_i, 1 \le i \le t$, is not valid, he has to ask the corresponding signer to send it again. Otherwise, he computes $u \equiv_p (\prod_{i=1}^{t} u_i)^{\gamma}$, $s \equiv_q \sum_{i=1}^{t} s_i$. The fair threshold signature of m is $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$.

2.4 The signature verification phase

To verify the fair threshold signature $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$, one simply checks if $\Omega_1^s \equiv_p v_2 u^{v_1}$, computes $m \equiv_p g^{-s} y^{v_1} v_1$ and checks if m has some redundancy information. If m has no proper redundancy, a secure one-way hashing function h [15] can be applied to m. But this approach can not provide the message recovery capability. To verify the threshold signature $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$ on m without redundancy, one must send m along with $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$ to the verifier.

3 Discussion

We discuss the correctness and security of our scheme in this section. We also show how to link a given signature to its corresponding signing process under the assistance of the judge.

3.1 Correctness

To prevent a signer from sending an invalid partial signature to the requester, the partial signature must be checked in step 5 of the signature generation phase. The following lemma ensures the correctness of partial signatures.

Lemma 1. *The partial signature (r_i, s_i, u_i) is valid if signer U_i is honest.*

Proof. By our scheme, we have
$$g^{-s_i} y_i^{v_1} r_i$$
$$\equiv_p g^{-(\hat{s}_i \beta + \alpha)} g^{z_i v_1} g^{\alpha} \hat{r}_i^{\beta}$$

$\equiv_p g^{-\widehat{m}(z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k})))\beta} g^{z_i v_1}$

$\equiv_p g^{-\widehat{m} z_i \beta - \widehat{m}\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))\beta} g^{z_i v_1}$

$\equiv_o g^{\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))(-\widehat{m}\beta)}$

$\equiv_p (\prod_{j=t+1}^{n}(\Phi_{j,i}))^{(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))(-v_1)}$

and

$u_i \equiv_p \Omega_0^{z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))}$

$\equiv_p (g^{\eta})^{z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))}$

$\equiv_p g^{(z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k})))\eta}$

$\equiv_p (g^{z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))})\eta$

$\equiv_p (\Psi_{i,0}(\prod_{j=t+1}^{n}\Phi_{j,i})^{\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k})})\eta$. □

After the signature generation phase, the blind signature can be verified by the group public key in the signature verification phase. Let ν denote the signers' complete views of an execution in the signature generation phase and let $(m, (\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$ denote the message-signature pair generated in that execution. Theorem 2 ensures the correctness of the scheme.

Theorem 2. *If the threshold signature* $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$ *on message* m *is valid, it can be verified and there exists a unique triple of blind factors* α, β *and* γ *for the link between the signers' views* ν *and the signature* $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$.

Proof. The validity of the signature $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$ on message m can easily be established as follows.

$g^{-s} y^{v_1} v_1$

$\equiv_p g^{-(\sum_{i=1}^{t}(\widehat{s}_i\beta+\alpha))} g^{\sum_{i=1}^{n} z_i v_1} m(\prod_{i=1}^{t} r_i)$

$\equiv_p m g^{-(\widehat{m}(\sum_{i=1}^{t} z_i + \sum_{i=t+1}^{n} z_i))\beta} g^{\sum_{i=1}^{n} z_i v_1}$

$\equiv_p m g^{-\widehat{m}\sum_{i=1}^{n} z_i \beta} g^{\sum_{i=1}^{n} z_i v_1}$

$\equiv_p m g^{-v_1 \sum_{i=1}^{n} z_i} g^{\sum_{i=1}^{n} z_i v_1}$

$\equiv_p m$

and

$\Omega_1^s \equiv_p \Omega_0^{\gamma(\sum_{i=1}^{t} s_i)}$

$\equiv_p \Omega_0^{\gamma(\sum_{i=1}^{t}(\widehat{s}_i\beta+\alpha))}$

$\equiv_p \Omega_0^{\gamma t\alpha + \gamma\beta\sum_{i=1}^{t}\widehat{s}_i}$

$\equiv_p \Omega_0^{\gamma t\alpha + \gamma\beta\sum_{i=1}^{t} k_i + \gamma v_1 \sum_{i=1}^{n} z_i}$

$\equiv_p (\Omega_1)^{(t\alpha)} (\Omega_1)^{(\beta\sum_{i=1}^{t} k_i)} (\Omega_1)^{(v_1\sum_{i=1}^{n} z_i)}$

$\equiv_p (\Omega_1)^{(t\alpha)} (\Omega_1)^{(\beta\sum_{i=1}^{t} k_i)} (u)^{v_1}$

$\equiv_p (\Omega_1)^{(t\alpha)} \Gamma^{\gamma\beta} u^{v_1}$

$\equiv_p v_2 u^{v_1}$.

Then we show that given views of all the signers in the signing process and the corresponding valid signature pair $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$, there exists a unique triple of blind factors α, β and γ.

Without loss of generality, assume that the signature $(\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$ has been generated by t signers U_i, $1 \le i \le t$, with the view consisting of Ω_0, k_i, $\widehat{r}_i \equiv_p g^{k_i}, \Gamma_i \equiv_p \Omega_0^{k_i}$, $\widehat{s}_i \equiv_q \widehat{m}(z_i + \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))) + k_i$, $u_i \equiv_p \Omega_0^{z_i+\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))}$, $1 \le i \le t$ and $\widehat{m}$, then the following equations must hold for α and β.

$$v_1 \equiv_p m\prod_{i=1}^{t} r_i \equiv_p m\prod_{i=1}^{t} g^{\alpha}\widehat{r}_i^{\beta} \quad (5)$$

$$\widehat{m} \equiv_q v_1 \mathcal{B}^{-1} \quad (6)$$

$$s \equiv_q \sum_{i=1}^{t} s_i \equiv_q \sum_{i=1}^{t}(\widehat{s}_i\beta + \alpha) \quad (7)$$

Note that if $t < q$, then $\gcd(t, q) = 1$. Since $\widehat{m} \in Z_q$ and $\widehat{m} \neq 0$, by equations (6) and (7), the unique solution for α and β is:

$$\mathcal{B} \equiv_q \widehat{m}^{-1} v_1 \quad (8)$$

$$\alpha \equiv_q (s - \sum_{i=1}^{t}\widehat{s}_i\beta)t^{-1} \quad (9)$$

In the following, we show that the solutions of α and β in equations (8) and (9) also satisfies equation (5).

$m\prod_{i=1}^{t} g^{\alpha}\widehat{r}_i^{\beta}$

$\equiv_p g^{-s} y^{v_1} v_1 g^{t\alpha}\prod_{i=1}^{t} g^{k_i\beta}$

$\equiv_p v_1 g^{-\sum_{i=1}^{t}(\widehat{s}_i\beta+\alpha)} g^{v_1\sum_{i=1}^{n} z_i} g^{t\alpha} g^{\beta\sum_{i=1}^{t} k_i}$

$\equiv_p v_1 g^{-((\widehat{m}\sum_{i=1}^{n} z_i + \sum_{i=1}^{t} k_i)\beta)} g^{v_1\sum_{i=1}^{n} z_i} g^{\beta\sum_{i=1}^{t} k_i}$

$\equiv_p v_1 g^{-\sum_{i=1}^{n}\widehat{m} z_i\beta} g^{v_1\sum_{i=1}^{n} z_i}$

$\equiv_p v_1$.

In additional to the equations (5), (6) and (7), the following equations must hold for γ.

$$\Omega_1 \equiv_p \Omega_0^{\gamma} \quad (10)$$

$$u \equiv_p (\prod_{i=1}^{t} u_i)^{\gamma} \quad (11)$$

$$v_2 \equiv_p (\Omega_0^{\gamma})^{(t\alpha)} \Gamma^{\gamma\beta} \quad (12)$$

Since $g \equiv_p s^{(p-1)/q}$ and s is a generator of Z_p^*, g generates a cyclic subgroup S_g of Z_p^* with $|S_g| = q$ and $\Omega_0, \Omega_1 \in S_g$, we can only find a unique solution for γ satisfying equation (10). This unique solution γ also satisfies equation (11) and (12). □

3.2 Security analysis

Given the secret information of a group of $l < t$ members, Lemma 3 ensures that the threshold cryptosystem constructed in the shadow distribution phase will not discloses any extra information about the group secret key $\sum_{i=1}^{n} z_i$.

Lemma 3. *Given a group of* $\sigma < t$ *members* $G = \{p_i | p_i \in [1, n], 1 \le i \le \sigma\}$ *and the set of shares* $\{\delta_{j,i} | 1 \le j \le n, i \in G\}$. *For any fixed* j, $1 \le j \le n$, *it takes polynomial time on* $|p|$ *to generate a random set* $\{\widehat{g^{a_{j,k}}} | 1 \le k \le t-1\}$ *satisfying* $g^{\delta_{j,i}} \equiv_p \prod_{k=0}^{t-1}(\widehat{g^{a_{j,k}}})^{x_i{}^k}$ *for* $i \in G$.

Proof. In step 3 of the shadow distribution phase, after U_i has received all $\delta_{j,i}$, he verifies if the share $\delta_{j,i}$ received from U_j is consistent with the certified

values $\Psi_{j,l}$, $1 \le l \le t-1$, by checking if $g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1}(\Psi_{j,l})^{{x_i}^l}$. Therefore

$$g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1}(g^{a_{j,l}})^{{x_i}^l} \equiv_p g^{\sum_{l=0}^{t-1} a_{j,l} * {x_i}^l}. \quad (13)$$

Since $g \equiv_p s^{(p-1)/q}$ and s is a generator of Z_p^*, g generates a cyclic subgroup S_g of Z_p^* with $|S_g| = q$. From (13), we have

$$\delta_{j,i} \equiv_q \sum_{l=0}^{t-1} a_{j,l} * {x_i}^l \quad (14)$$

From (14), we know that given a fixed index j, the shares $\delta_{j,i}$, $i \in G$, will use the same variables $\widehat{a_{j,k}}$, $0 \le k \le t-1$, as follows:

$$\delta_{j,i} \equiv_q \sum_{k=0}^{t-1} \widehat{a_{j,k}} * {x_i}^k. \quad (15)$$

Given a fixed index j, we can get at most σ linear equations with t variables as follows:

$$\delta_{j,i} \equiv_q \sum_{k=0}^{t-1} \widehat{a_{j,k}} * {x_i}^k (i \in G). \quad (16)$$

Since the linear equations have at least one solution $\widehat{a_{j,k}} = a_{j,k}$, $0 \le k \le t-1$, we can solve the linear equations (16) and get a random solution $\widehat{a_{j,k}}$, $1 \le k \le t-1$, by assigning random values to all free variables. From (16), it is clear that $g^{\delta_{j,i}} \equiv_p g^{\sum_{k=0}^{t-1} \widehat{a_{j,k}} * {x_i}^k} \equiv_p \prod_{k=0}^{t-1}(g^{\widehat{a_{j,k}}})^{{x_i}^k}$. □

In our fair blind threshold signature scheme, the partial signature (s_i, r_i, u_i) must satisfy the equation $g^{-s_i} y_i^{v_1} r_i \equiv_p g^{-s_i} g^{z_i v_1} r_i \equiv_p (\prod_{j=t+1}^{n}(\Phi_{j,i}))(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i - x_k}))(-v_1)$ and $g^{u_i} \equiv_p (\Psi_{i,0}(\prod_{j=t+1}^{n}\Phi_{j,i}) \prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k})^{\Omega_0}$. Since v_1, $\Phi_{j,i}$, x_k, r_i, y_i and s_i are all public, an attacker has to solve the discrete logarithm problem in order to get the secret value z_i.

With the information of all partial signatures and the corresponding threshold signature, an attacker is not capable of deriving the secret keys since it has to solve the equation $v_1 g^{-s} y^{v_1} \equiv_p m(\prod_{i=1}^{n} r_i) g^{-(\sum_{i=1}^{n} s_i)}(\prod_{i=1}^{n} g^{z_i})^{v_1}$. To solve this equation is equivalent to solve the discrete logarithm problem.

Since γ, α and β are kept secret by the requester and all signatures are equally likely from the signer's point of view, it is computationally infeasible for the signer to derive the link between the view consisting of $\Omega_0, k_i, \widehat{r_i} \equiv_p g^{k_i}, \Gamma_i \equiv_p \Omega_0^{k_i}$, $\widehat{s_i} \equiv_q \widehat{m}(z_i + \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))) + k_i$, $u_i \equiv_p \Omega_0^{z_i + \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))}$, $1 \le i \le t$, $\widehat{m}$ and the signature $(\Omega_1 \equiv_p \Omega_0^{\gamma}, Cert_J(h(\Omega_1)), v_1, v_2, s, u)$ submitted by a requester for verification later.

3.3 Linkage recovery

Since blind threshold signature schemes without fairness property provide perfect unlinkability, such e-cash systems can be misused by criminals, e.g. to safely obtain a ransom or to launder money. To cope with this dilemma, in our proposed scheme, anyone of the t signers can first send all pseudonyms $(\Omega_0, Cert_J(h(\Omega_0)))_s$ requested by the criminal to the judge and then the judge sends all the corresponding pseudonyms $(\gamma, \Omega_0, \Omega_1, Cert_J(h(\Omega_0)), Cert_J(h(\Omega_1)))_s$ back to the signer. The signer can verify validity of the corresponding pseudonyms by checking if $\Omega_0^{\gamma} \equiv_p \Omega_1$ and both $Cert_J(h(\Omega_0))$ and $Cert_J(h(\Omega_1))$ are valid. When the criminal withdraws these e-cashes from the signer, the signer can easily identify the criminal by linking the message-signature pair $(m, (\Omega_1, Cert_J(h(\Omega_1)), v_1, v_2, s, u))$ with the corresponding signer's view $\Omega_0, k_i, \widehat{r_i} \equiv_p g^{k_i}, \Gamma_i \equiv_p \Omega_0^{k_i}$, $\widehat{s_i} \equiv_q \widehat{m}(z_i + \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))) + k_i$, $u_i \equiv_p \Omega_0^{z_i + \sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\neq i}^{t}(\frac{-x_k}{x_i-x_k}))}$ and $\widehat{m}$. If the judge is honest, all crimes by misusing the unlinkability property of blind threshold signatures will be prevented and the anonymity of honest customers will also be preserved.

4 Applications

Up to date, the on-line e-cash systems proposed by Chaum [3, 4] are more efficient and practical. The aim of these systems was to produce an electronic version of money which retains the same properties as paper cash. These systems involve customers, the bank and the shop. In these systems, the protocols can be simplified as the following phases: the withdrawal phase, the spending phase and the deposit phase. During the withdrawal phase, customers apply the blind signature technique to get their blind e-cashes. In the spending phase, customers first generate their real e-cashes from the blind e-cashes received in the withdrawal phase and then spend them at designated shops. Finally, in the deposit phase, the shops deposit the e-cashes at the bank. The bank will check if the e-cash has been reused by copying a coin. In real world environments, it is very hard to find any single authority as the bank. To deal with the dilemma, some modifications of schemes in [3, 4] must be made.

The modifications are described below: (1) Instead of a unique administrator, the modified systems consist of n administrators and at least $(n - t + 1)$ out of n administrators do not conspire with the others. (2) Each scheme involves voters and the n administrators and consists of the following phases: the withdrawal phase, the spending phase and the deposit phase. (3) In the registration phase, customers apply the fair blind threshold signature technique to get their fair blind e-cashes from t honest administrators. (4) In the spending phase, customers generate their real e-cashes from the fair blind e-cashes received in the withdrawal phase and send them to the shop. (5) In the deposit phase, the shops deposit the e-cashes at the bank. The bank will check if the e-cash has been reused by copying

a coin.

By the above modifications, the power of a single administrator is distributed among several administrators and the issue of e-cashes is controlled by several authorities. The fair threshold blind signature will work when at least t out of n administrator are honest. Since in the withdrawal phase, customers only need to request exact t members from n administrators, it can meet the real world environments without a single trusted administrator or with some absent/dishonest administrators.

Since blind signature schemes without fairness property provide perfect unlinkability, such e-cash systems can be misused by criminals, e.g. to safely obtain a ransom or to launder money. For example, a criminal can safely obtains a ransom by joining a blind signature scheme where the request is via an untraceable mail (e.g. an ordinary mail or an untraceable e-mail [2, 12]) and the signer puts blind signature on a public board. Then the criminal can easily obtain the blind signature from the public board and derive the corresponding e-cashes. To cope with this dilemma, in our proposed scheme, any one of the t signers can first send all $(\Omega_0, Cert_J(h(\Omega_0)))_s$ requested by the criminal to the judge and then the judge sends all pseudonyms $(\gamma, \Omega_0, \Omega_1, Cert_J(h(\Omega_0)), Cert_J(h(\Omega_1)))_s$ back to the signer. When the criminal withdraws these e-cashes from the signer (or called the bank), the signer can easily identify the criminal. If the judge (the government) is honest, all crimes by misusing the unlinkability property of blind signatures will be prevented and the anonymity of honest customers will also be preserved.

5 Conclusion

We have proposed an efficient fair blind threshold signature scheme based on discrete logarithm. In our scheme, the size of a fair threshold signature is the same as that of an individual fair signature and the signature verification process is simplified by means of a group public key. The security of our schemes relies on the hardness of computing discrete logarithm and it is computationally infeasible for the signers to derive the exact correspondence between the message they actually sign and all signers' complete views of the execution of the signing process without the assistance of the judge or the requester. Our proposed scheme can be easily applied to current efficient single-authority e-cash systems for distributing the power of a single authority without changing the underlying structure and degrading the overall performance.

References

[1] J. L. Camenisch, J. M. Pivereau and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," *Advances in Cryptology: Proc. of EuroCrypt'94*, LNCS 950, pp. 428-432, Springer-Verlag, 1995.

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

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

[4] D. Chaum, "Privacy protected payments: unconditional payer and/or payee untraceability," *In Smartcard 2000*, North Holland, 1988.

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

[6] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithm," *IEEE Trans. on Information Theory*, Vol. IT-31, No. 4, pp. 469-472, 1985.

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

[8] 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-AisaCrypt'94*, LNCS 917, pp. 224-237, Springer-Verlag, 1994.

[9] 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.

[10] W. Juang and C. Lei, "A secure and practical electronic voting scheme for real world environments," *IEICE Trans. on Fundamentals*, Vol. E80-A, No. 1, pp. 64-71, January, 1997.

[11] 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, pp. 172 -181, Springer-Verlag, 1996.

[12] W. Juang, C. Lei and C. Fan, "Anonymous Channel and Authentication in Wireless Communications," *Proceedings of International Conference on Networking and Multimedia*, pp. 227 -234, Kaohsiung, Taiwan, R.O.C, December 1996.

[13] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," *Advances in Cryptology: Proc. of EuroCrypt'94*, LNCS 950, pp. 182-193, Springer-Verlag, 1995.

[14] R. L. Rivest, A. Shamir and L. Adelman, "A method for obtaining digital signatures and public key cryptosystem," *Commun. ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

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

[16] S. von Solms and D. Naccache, "On blind signatures and perfect crime," Computer & Security, Vol. 11, 1992, pp. 581-583.

[17] M. Stadler, J. Piveteau and J. Camenisch, "Fair blind signatures," *Advances in Cryptology-EuroCrypt'95*, LNCS 921, pp. 209-219, Springer-Verlag, 1995.

[18] W. Stallings, "Network and internetwork security," Prentice Hall International, pp. 333-340, 1995.