Available online at www.sciencedirect.com

SCIENCE DIRECT®

The Journal of Systems and Software 72 (2004) 25–31

The Journal of Systems and Software

www.elsevier.com/locate/jss

Fair blind threshold signatures in wallet with observers

Wen-Shenq Juang *, Horng-Twu Liaw [1]

Department of Information Management, Shih Hsin University, No. 1, Lane 17, Sec. 1, Muja Rd., Wenshan Chiu, Taipei 116, Taiwan, ROC

Received 21 July 2002; received in revised form 11 January 2003; accepted 11 January 2003

Abstract

In this paper, we propose efficient fair blind (t, n) threshold signature schemes in wallet with observers. By these schemes, 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 schemes allow the judge (or the judges) to deliver information allowing anyone of the t signers to link his view of the protocol and the message–signature pair.

Keywords: Fair blind signatures; Threshold signatures; Wallet with observers; Discrete logarithm; Privacy and security; Secure e-cash systems

1. Introduction

The concept of blind signature was introduced by Chaum (1982). It allows a requester to obtain signatures on the messages he provides to the signer without revealing these messages. The blind signatures can realize secure electronic payment schemes (Chaum, 1982; Ferguson, 1993; Okamoto and Ohta, 1991) protecting customers' anonymity. In a distributed environment, the signed blind messages can be regarded as a fixed amount of electronic money in secure electronic payment 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 he wishes. If the money issuer does that, it may cause great danger or hurt for the corporation or society. For distributing the power of a single authority, the concept of threshold schemes was proposed by Shamir (1979). Threshold signatures (Gennaro et al., 1996; Harn, 1994; Hsu et al., 2001; Wu and Hsu, in press) are motivated by the need that arises in organizations to have a group of employees who agree on a message before signing and by the need to protect the group private key from attacks launched by internal and external adversaries. The later becomes more important with the actual deployment of public key schemes in practice. The signing power of some authorities inevitably invites attackers to try to steal this power. For distributing the power of a single money issuer, instead of a single signer, blind threshold signature schemes and their variations (Juang and Lei, 1996, 1999) have been proposed in a distributed environment, where several signers work together to sign a blind threshold signature. These schemes allows t out of n participants in a group cooperating to sign a blind threshold signature without the assistance of a single trusted authority.

Since blind signature schemes provide perfect unlinkability, such e-cash schemes can be misused by criminals, e.g. to safely obtain a ransom or to launder money (Solms and Naccache, 1992). To cope with this dilemma, the concept of fair blind signatures was introduced to prevent the misuse of the unlinkability property (Stadler et al., 1995). With the help of the judge, the signer can link a signature to the corresponding signing process. Juang et al. proposed a fair blind threshold signature scheme (Juang et al., 2001) based on the blind threshold signature scheme (Juang and Lei, 1996) and the registration method (Stadler et al., 1995). This scheme allows the judge to deliver information allowing anyone of the t signers to link his

* Corresponding author. Tel.: +886-2-2236-8225x3352; fax: +886-2-22367114.

E-mail addresses: wsjuang@cc.shu.edu.tw (W.-S. Juang), htliaw@cc.shu.edu.tw (H.-T. Liaw).

[1] Tel.: +886-2-2236-8225-3341; fax: +886-2-22367114.

0164-1212/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/S0164-1212(03)00017-7

view of the protocol and the message–signature pair. But this scheme (Juang et al., 2001) needs more exponential operations than the blind threshold signature scheme (Juang and Lei, 1996).

The concept of wallet databases with observers was introduced by Chaum and Pedersen (1992). It uses the tamper-proof devices, such as Java cards, that the person cannot modify or probe, to keep some correct and secret database. In this concept, a person (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 authority; and (2) the personal workstation whose inner working is totally under control of the person. By this combined device, called a wallet, the two modules owned by a person can keep his personal secret database and ensure the correctness of these databases. Also, Brands also use this concept and the representation problem to design an off-line cash system (Brands, 1994).

In this paper, we propose an efficient fair blind threshold signature scheme based on the blind threshold signature scheme (Juang and Lei, 1996) and the concept of wallet with observers (Chaum and Pedersen, 1992). In our scheme, the size of a fair threshold signature and the signature verification process are all the same as that of an individual signature. The security of our schemes relies on the difficulty of computing discrete logarithm and the tamper-proof devices 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 judges) or the requester.

2. The proposed scheme

In this section, we propose fair blind threshold signature schemes in wallet with observers. For simplicity, the fair blind threshold signature scheme is based on the Nyberg–Rueppel blind signature scheme (Camenisch et al., 1994) with message recovery. All secure Meta–ElGamal blind signature schemes (Camenisch et al., 1994; Horster et al., 1994) can be used in our scheme. 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 installs his temper-proof device with the judge and uses the wallet to request a fair blind threshold signature from the signers. The proposed scheme consists of four phases: (1) the shadow distribution phase, (2) the initialization 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 initialization phase, the requester requests one pseudonym from the judge. The public key of the pseudonym is signed by the judge by a secure blind signature scheme and the corresponding secret key is stored in the tamper-proof device and known only by this device. These process is performed only once and this tamper-proof device can be used until it expires. In the signature generation phase, a requester requests a fair blind threshold signature from the signers. Before the requester can generate the real threshold signature from signers, he must send the unblinding information encrypted by the judge's public key to the judge. This information is also stored in the wallet databases and it contains necessary information to link message–signature pair. Thus, the judge, who knows the corresponding secret key, can link the message–signature pair with the corresponding signer's view when necessary. In the signature verification phase, anyone can use the group public key to verify if a threshold signature is valid.

Let n' be the number of signers before the shadow distribution phase, QUAL be the set of non-disqualified signers after the shadow distribution phase, let n be the number of non-disqualified signers QUAL. Let $\mathcal{U}_i$, $1 \leqslant i \leqslant n'$, be the identification of signer i before the shadow distribution phase. Let U_i, $1 \leqslant i \leqslant n$, be the identification of non-disqualified signer i after the shadow distribution phase. Let C be the computer controlled by the requester, T be the tamper-proof device issued by the judge (or some trusted authority) for the requester, n be the number of signers, t be the threshold value of the fair blind threshold signature scheme, so that at least $(n - t + 1)$ signers are honest. Let d_T be the secret key stored in T when T is born and e_T be the corresponding public key. Let m be the blind message to be signed, $\mathcal{H}$ be a secure one-way hashing function (Stallings, 1999). 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^* (Menezes et al., 1997) 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 "$\|$" denote the ordinal string concatenation. Let d_i be the secret key chosen by $\mathcal{U}_i$ and d_J be the secret key chosen by the judge. In a distributed environment, $\mathcal{U}_i$ and the judge can publish their corresponding public keys e_i and e_J. Anyone can get e_T, e_i and e_J via some authentication service (e.g. the X.509 directory authentication service (Stallings, 1999)). Using a secure public key signature scheme (ElGamal, 1985; Rivest et al., 1978), T, $\mathcal{U}_i$ and the judge can produce signatures of messages by their own secret keys d_T, d_i and d_J. Anyone can verify these signatures by the corresponding public keys e_T, e_i and e_J. Let $\mathrm{Cert}_{d_T}(m)$ be the signature on the message m produced by T, $\text{Cert}_{d_z}(m)$ be the signature on the message m produced by T with the secret key d_z of its pseudonym requested in the initialization phase, and $\text{Cert}_J(m)$ be the signature on the message m produced by the judge. 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 he really transmitted.

2.1. The shadow distribution phase

Before a requester can request a fair blind threshold signature from the signers, all the signers must cooperate to distribute their secret shadows to other signers without the assistance of a mutually trusted authority. In this phase, signers can detect the incorrect shares by the verification equations. In the shadow distribution phase, each $\mathscr{U}_i$, $1 \leqslant i \leqslant n'$, carries out the following steps:

1. $\mathscr{U}_i$ 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 $G_{i,k} \equiv_p g^{a_{i,k}}h^{a'_{i,k}}$, $0 \leqslant k \leqslant t-1$, and it sends $(G_{i,k},\ 0 \leqslant k \leqslant t-1)$ to $\mathscr{U}_j$, $1 \leqslant j \leqslant n'$, $j \neq i$.
2. Upon receiving $(G_{j,k},\ 1 \leqslant j \leqslant n',\ j \neq i,\ 0 \leqslant k \leqslant t-1)$ from all other signers, $\mathscr{U}_i$ 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 $\mathscr{U}_j$, secretly to every $\mathscr{U}_j$, $1 \leqslant j \leqslant n'$, $j \neq i$.
3. When $\mathscr{U}_i$ receives all $\delta_{j,i}$ and $\delta'_{j,i}$, $1 \leqslant j \leqslant n'$, $j \neq i$, from other signers, he verifies if the shares $\delta_{j,i}$ and $\delta'_{j,i}$ received from $\mathscr{U}_j$ is consistent with the certified values $G_{j,l}$, $0 \leqslant l \leqslant t-1$, 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, $\mathscr{U}_i$ 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 $\mathscr{U}_j$. Each signer except the dishonest signer $\mathscr{U}_j$ then marks $\mathscr{U}_j$ as a disqualified signer and builds the set of non-disqualified signers QUAL.
4. Every signer $\mathscr{U}_i$, $i \in \text{QUAL}$, broadcasts $A_{i,l} \equiv_p g^{a_{i,l}}$, $0 \leqslant l \leqslant t-1$.
5. When $\mathscr{U}_i$, $i \in \text{QUAL}$, receives all $A_{j,l}$, $j \in \text{QUAL}$, $j \neq i$, $0 \leqslant l \leqslant t-1$, from other signers in QUAL, 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 j, $\mathscr{U}_i$ broadcasts that an error has been found, publishes $\delta_{j,i}$, the authentication information of $\delta_{j,i}$ and $\mathscr{U}_j$. Any t signers in QUAL can compute z_j, $f_j(x)$, $A_{j,k}$, $0 \leqslant k \leqslant t-1$. Anyone then computes the public shadows $\mathscr{P}_{j,i} \equiv_p g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1}(A_{j,l})^{x_i^l}$, where i and $j \in \text{QUAL}$, and the group public key $y \equiv_p \prod_{j\in\text{QUAL}} y_j \equiv_p \prod_{j\in\text{QUAL}} A_{j,0}$. The group public key y and all public shadows $\mathscr{P}_{j,i}$, where i and $j \in \text{QUAL}$, the personal public key $y_i \equiv_p A_{i,0} \equiv_p g^{z_i}$ can then be published by each signer $\mathscr{U}_i$. Without loss of generality, we assume that n non-disqualified signers QUAL are U_i, $1 \leqslant i \leqslant n$. It can be done by renaming the index of each signer $\mathscr{U}_i$, $i \in \text{QUAL}$.

2.2. The initialization phase

Before a requester can request a fair blind threshold signature from the signers, he must acquire one pseudonym from the judge. The public key of the pseudonym is signed by the judge by a secure blind signature scheme (Camenisch et al., 1994; Chaum, 1982; Horster et al., 1994) and the corresponding secret key is stored in the temper-proof device T issued by some organization (e.g. the judge) and known only by this device T. The requester and the judge then carry out the following steps:

1. T sends a request information including the certificate $\text{Cert}_{d_T}(\mathscr{H}(\text{RD}))$, where RD contains some redundancy information indicating the registration, for a pseudonym to the judge.
2. The judge first verifies T's identification by the certificate $\text{Cert}_{d_T}(\mathscr{H}(\text{RD}))$ 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 $\text{Cert}_J(\mathscr{H}(e_z))$ of the corresponding public key e_z is stored in T.

2.3. The signature generation phase

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

1. Each U_i randomly chooses a number $k_i \in Z_q$, computes $\hat{r}_i \equiv_p g^{k_i}$ and sends $\hat{r}_i$ to the requester.
2. After receiving all $\hat{r}_i$, $1 \leqslant i \leqslant t$, C does the following:
   (a) Choose two random numbers $\alpha \in Z_q$ and $\beta \in Z_q^*$, compute $r \equiv_p m\prod_{i=1}^{t} r_i \equiv_p mg^{t\alpha}(\prod_{i=1}^{t}\hat{r}_i)^{\beta}$ and $\hat{m} \equiv_q \beta^{-1}r$, where $r_i \equiv_p g^{\alpha}\hat{r}_i^{\beta}$ and $1 \leqslant i \leqslant t$.
   (b) Check if $\hat{m} \neq 0$. If yes, sends $(\alpha, \beta, \hat{r}_i, 1 \leqslant i \leqslant t, m)$ to T. Otherwise, go back to step (a).
   (c) T also computes $r \equiv_p m\prod_{i=1}^{t} r_i \equiv_p mg^{t\alpha}(\prod_{i=1}^{t}\hat{r}_i)^{\beta}$, $\hat{m} \equiv_q \beta^{-1}r$, where $r_i \equiv_p g^{\alpha}\hat{r}_i^{\beta}$ and $1 \leqslant i \leqslant t$, $\text{Cert}_{d_Z}(\mathscr{H}(\hat{m}))$, and sends $E_{e_J}(\alpha\|\beta\|\hat{r}_1\|\cdots\|\hat{r}_t\|m)$ to C. C then forwards $E_{e_J}(\alpha\|\beta\|\hat{r}_1\|\cdots\|\hat{r}_t\|m)$ to the judge.
   (d) After receiving the receipt from the judge, C forwards the receipt to T. If the receipt is valid, T then sends $\text{Cert}_{d_Z}(\mathscr{H}(\hat{m}))$ back to C.
   (e) C then sends $\text{Cert}_J(\mathscr{H}(e_z))$, e_z, $\text{Cert}_{d_Z}(\mathscr{H}(\hat{m}))$, $\hat{m}$ to all U_i, $1 \leqslant i \leqslant t$.

3. Upon receiving $\hat{m}$, each U_i verifies if $\mathrm{Cert}_{d_Z}(\mathscr{H}(\hat{m}))$ is valid. If yes, he computes

$$\hat{s}_i \equiv_q \hat{m}\left(z_i + \sum_{j=t+1}^{n} f_j(x_i)\left(\frac{-x_k}{x_i - x_k}\right)\right) + k_i$$

   and sends $\hat{s}_i$ back to the requester.
4. After receiving all $\hat{s}_i$, C computes $s_i \equiv_q \hat{s}_i\beta + \alpha$, and checks if

$$g^{-s_i} y_i^r r_i \equiv_p \left(\prod_{j=t+1}^{n} (\mathscr{P}_{j,i})\right)^{\left(\prod_{k=1,k\neq i}^{t}\left(\frac{-x_k}{x_i-x_k}\right)\right)(-r)},$$

$$1 \leqslant i \leqslant t.$$

If any of the $\hat{s}_i$ is not valid, it has to ask the corresponding signer to send it again. Otherwise, it computes $s \equiv_q \sum_{i=1}^{t} s_i$. The threshold signature of m is (r, s).

2.4. The signature verification phase

To verify the threshold signature (r, s), one simply computes $m \equiv_p g^{-s} y^r r$ and checks if m has some redundancy information. If m has no proper redundancy, a secure one-way hashing function $\mathscr{H}$ can be applied to m. But this approach cannot provide the message recovery capability. To verify the threshold signature (r, s) on m without redundancy, one must send m along with (r, s) to the verifier.

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

By means of our scheme, we have

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

$$\begin{aligned}
g^{k_i\beta} &\equiv_p g^{-\hat{m}\left(z_i+\sum_{j=t+1}^{n} f_j(x_i)\left(\prod_{k=1,k\neq i}^{t}\left(\frac{-x_k}{x_i-x_k}\right)\right)\right)\beta} g^{z_i r} \\
&\equiv_p g^{-\hat{m}z_i\beta-\hat{m}\sum_{j=t+1}^{n} f_j(x_i)\left(\prod_{k=1,k\neq i}^{t}\left(\frac{-x_k}{x_i-x_k}\right)\right)\beta} g^{z_i r} \\
&\equiv_p g^{\sum_{j=t+1}^{n} f_j(x_i)\left(\prod_{k=1,k\neq i}^{t}\left(\frac{-x_k}{x_i-x_k}\right)\right)(-\hat{m}\beta)} \\
&\equiv_p \left(\prod_{j=t+1}^{n} (\mathscr{P}_{j,i})\right)^{\left(\prod_{k=1,k\neq i}^{t}\left(\frac{-x_k}{x_i-x_k}\right)\right)(-r)}
\end{aligned}$$

After the signature generation phase, the blind threshold signature can be verified by the group public key in the signature verification phase. Lemma 2 ensures the correctness of the scheme.

Lemma 2. *The signature (r, s) generated in the signature generation 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:

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

3. Analysis

We examine 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 4 of the signature generation phase. The following lemma ensures the correctness of partial signatures.

To prove the blindness of the scheme, we can show that given any view v and any valid message–signature pair $(m, (r, s))$, there exists a unique pair of blinding factors α and β. Since the requester chooses the blinding factors α and β randomly, the blindness of the signature scheme follows.

3.2. Security considerations

The shadow distribution phase of Section 2.1 is the same as the distributed key generation protocol (Gennaro et al., 1999) except that it publishes the public shadows ($\mathscr{P}_{j,i}$, where i and $j \in \mathrm{QUAL}$) for cheater detection. In this scheme, they use the information-theoretic verifiable secret sharing protocol (Pedersen, 1991) to guarantee that no bias for a bit in the output group public key of the protocol is possible. Lemma 3 ensures the security of the shadow distribution phase in Section 2.1.

Lemma 3. *The shadow distribution phase in Section* 2.1 *is a secure protocol for distributed key generation in discrete-log based cryptosystems.*

Proof. The distribution phase of Section 2.1 is based on the distributed key generation protocol (Gennaro et al., 1999). Gennaro et al. have showed that in their proposed distributed key generation protocol, the view of an adversary of the protocol is simulatable (Gennaro et al., 1999). Different from this scheme (Gennaro et al., 1999), in order to do cheater detection when some signer cheats, the public shadows ($\mathscr{P}_{j,i} \equiv_p g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1}(A_{j,l})^{x_i^l}$), where i and $j \in$ QUAL, will be published by all signers in our proposed scheme. All the public shadows ($\mathscr{P}_{j,i}$), where i and $j \in$ QUAL, can be computed by the public values ($A_{i,k} \equiv_p g^{a_{i,k}}, \ \ i \in \text{QUAL}, \ \ 0 \leqslant k \leqslant t-1$) broadcasted in Step 4 of the shadow distribution phase. This public shadows will not disclose any extra information of the group secret key. The shadow distribution phase of Section 2.1 satisfies the simulation argument, that is, it is a secure distributed key generation protocol (Gennaro et al., 1999). □

Since blind threshold signature schemes without the fairness property provide perfect unlinkability, such e-cash schemes can be misused by criminals, e.g. to safely obtain a ransom or to launder money. For example, a criminal can safely obtain a ransom by joining a blind threshold signature scheme where the request is via an untraceable mail (e.g. an ordinary mail or an untraceable e-mail (Chaum, 1981; Juang et al., 1999)) and the signers put the blind threshold signature on a public board. Then the criminal can easily obtain the blind threshold signature from the public board and derive the corresponding e-coins. To cope with this dilemma, in our proposed scheme, anyone of the t signers U_i can first send the messages $(\hat{r}_i, \hat{m})$ requested by the criminal to the judge and then the judge sends all the corresponding view $(\alpha\|\beta\|\hat{r}_1\|\cdots\|\hat{r}_t\|m)$ back to the signer. The signer can verify validity of the corresponding view by computing $r \equiv_p m\prod_{i=1}^{t} r_i \equiv_p mg^{t\alpha}(\prod_{i=1}^{t}\hat{r}_i)^{\beta}$, $\hat{m} \equiv_q \beta^{-1}r$. When the criminal withdraws these e-coins from the signer, the signer can easily identify the criminal by linking the message–signature pair (m, r, s) with the corresponding signer's view k_i, $\hat{r}_i \equiv_p g^{k_i}$, and $\hat{m}$. 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. Discussions

4.1. Extension schemes

The blind signature scheme with message recovery (Camenisch et al., 1994) is used in our proposed scheme. The modification of DSA-type blind signature scheme (Camenisch et al., 1994) can also be used in our scheme. Some extensions of Camenisch et al.'s blind signature schemes of were introduced (Horster et al., 1994). Not all variants of Meta-Message recovery signature schemes can be transformed to blind signature schemes (Horster et al., 1994). For example, there is no blind signature scheme for the original ElGamal signature scheme yet. All extensions of secure blind signature schemes (Horster et al., 1994), except that $\widetilde{B}$ contains $\tilde{s}$ in the signature generation equation, can be used in our scheme. The security considerations and performance analysis of these extended schemes are similar to those of our proposed scheme. Pointcheval et al. proposed two provably secure blind signature schemes (Pointcheval and Stern, 1996). One has been proved to be equivalent to the discrete logarithm problem in a subgroup. The other has been proved to be equivalent to the RSA problem. By suitable modifications for our scheme, the secure blind signature scheme based on discrete logarithm (Pointcheval and Stern, 1996) can also be used in the modified scheme (Lei et al., 2002). Since the security of the underlying blind signature scheme has been proven to be equivalent to the discrete logarithm problem in the random oracle model, the security of this modified scheme (Lei et al., 2002) is also equivalent to the discrete logarithm problem in the random oracle model.

4.2. Distributing the power of a single judge to multi-judges

In our scheme, the duty of the judge is to issue pseudonyms to requesters and keep the unblinding information sent from the requesters. In some situations, it is hard to find a trusted judge. We can modify the scheme in Section 2 as follows: (1) Instead of a unique judge, the modified system consists of κ judges and at least $\lceil\kappa/2\rceil$ judges are honest. (2) These κ judges execute a distributed key generation protocol similar to the shadow distribution phase in Section 2 to generate a group public key e_{Js} and the corresponding group secret key d_{Js}. (3) During the initialization phase, a requester must acquire one threshold pseudonym from $\lceil\kappa/2\rceil$ judges. The public key of the threshold pseudonym is signed by these judges by a blind threshold signature scheme and the corresponding secret key is stored in the temper-proof device T and known only by this device. (4) In the signature generation phase, any requester must send the unblinding information $E_{e_{Js}}(\alpha\|\beta\|\hat{r}_1\|\cdots\|\hat{r}_t\|m)$ to any honest judge (just as a database manager). By the above modifications, the power of a single judge is distributed to several judges. When anyone of the t signers U_i sends the messages $(\hat{r}_i, \hat{m})$ requested by the criminal to the judge (as a database manager) and then $\lceil \kappa/2 \rceil$ judges can first decrypt the unblinding information $E_{e_{Js}}(\alpha\|\beta\|\hat{r}_1\| \cdots \|\hat{r}_t\|m)$ received soon, find $(\alpha\|\beta\|\hat{r}_1\| \cdots \|\hat{r}_t\|m)$ and send all the corresponding view $(\alpha\|\beta\|\hat{r}_1\| \cdots \|\hat{r}_t\|m)$ back to the signer. By this approach, the power of a single judge is distributed to several judges. The fair blind threshold signature scheme (Juang et al., 2001) is just a single judge. It is still an open problem that whether there exists an efficiently multi-judges fair blind threshold signature scheme without the assistance of a tamper-proof device like this scheme (Juang et al., 2001).

4.3. Performance considerations

In this subsection we give an analysis of the computational effort required to compute fair blind threshold signatures in our scheme. Table 1 illustrates the comparison of our proposed scheme and Juang et al.'s scheme without the assistance of a tamper-proof device (Juang et al., 2001). For reducing the computational cost needed by the requester, the partial signature verification in Step 4 would not be done except the final threshold signature cannot pass the verification equation in the signature verification phase. The requester does not need to know the public shadows $\mathscr{P}_{l,j}$, where l and $j \in$ QUAL, in advance except there exists some dishonest signer in the signature generation phase. In this approach, the requester only needs to compute 2 modular exponentiations and 1 modular inverse in step 2 of the signature generation phase. Since the blind threshold verification functions of our schemes all are the same as those of the underlying blind signature schemes, the verification cost of our blind threshold signature is the same as that of the underlying blind signature. Comparative to the scheme without the assistance of a tamper-proof device (Juang et al., 2001), the extra cost for requesting a fair blind threshold signature in our scheme is to compute $E_{e_J}(\alpha\|\beta\|\hat{r}_1\| \cdots \|\hat{r}_t\|m)$ which contains one public key encryption. For reducing the computation cost, T can first negotiate a session key with the judge and then send the unblinding information to the judge by a secret key cryptosystem. This approach will greatly reduce the computation cost when the number of signers t is large. But if we want to change our scheme to multi-judges environments, instead of the above approach, T must send the unblinding information $E_{e_{Js}}(\alpha\|\beta\|\hat{r}_1\| \cdots \|\hat{r}_t\|m)$ to a judge (as a database manager) by the judges' group public key e_{Js} for distributing the power of a single judge.

Let the fair blind threshold signature of m in Juang et al.'s scheme without the assistance of a tamper-proof device (Juang et al., 2001) be $(\Omega_1, \mathrm{Cert}_J(h(\Omega_1)), v_1, v_2, s, u)$. Let the prime p be 1024-bits long and the prime q be 160-bits long. Totally, the fair threshold signature in Juang et al.'s scheme without the assistance of a tamper-proof device (Juang et al., 2001) and our proposed scheme in Section 2 are $1024 + 1024 + 1024 + 1024 + 160 + 1024 = 5280$ bits and $160 + 1024 = 1184$ bits, respectively. Hence, our proposed scheme reduces the length of the fair blind threshold signature by $(5280 - 1184)/5280 = 78\%$. Three robust threshold signature protocols, namely, DSS-Thresh-Sig-1, DSS-Thresh-Sig-2 and DSS-Thresh-Sig-3, are proposed by Gennaro et al. (1996). One approach to generate blind threshold signatures is to take robust threshold signature schemes (Gennaro et al., 1996) and turn them into fair blind signature schemes. The advantage of this approach is that it is quite robust and can deal with the situation where there are many cheaters. However, in DSS-Thresh-Sig-1, $2t + 3$ modular exponentiations are required for each signer to generate a threshold signature and it is even worse for DSS-Thresh-Sig-2 and DSS-Thresh-Sig-3 which requires $O(nt)$ modular exponentiations. It is clear that this approach is quite inefficient compared to our proposed schemes.

Table 1
Cost of the signature generation phase and the signature verification phase in our proposed scheme and that in Juang et al.'s scheme without the assistance of a tamper-proof device (Juang et al., 2001)

	The requester (verifier)				
	EXP	INV	ENC	MUL	ADD
Cost of the signature generation phase					
Our proposed scheme	2	1	1	$t+5$	t
Juang et al. (2001)	5	1	0	$3t+6$	t
Cost of the verification phase					
Our proposed scheme	2	1	0	2	0
Juang et al. (2001)	4	1	0	3	0

EXP = the number of modulo exponentiations; INV = the number of modulo inversions; ENC = the number of message encryption; MUL = the number of modulo multiplications; ADD = the number of modulo additions.

5. Conclusion

We have proposed efficient fair blind threshold signature schemes in wallet with observers. In our schemes, the size of a fair threshold signature and the signature verification process are all the same as that of an individual signature. The security of our schemes relies on the difficulty of computing discrete logarithm and the tamper-proof devices 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 judges) or the requester. Our proposed schemes can be easily applied to current efficient single-authority e-cash schemes for distributing the power of a single authority without changing the underlying structure and degrading the overall performance.

Acknowledgements

This work was supported in part by the National Science Council of the Republic of China under contract NSC-91-2213-E-128-005. The authors would like to thank Professor Chin-Laung Lei for several very helpful comments and suggestions.

References

Brands, S., 1994. Untraceable off-line cash in wallet with observers. In: Santis, A. (Ed.), Advances in Cryptology: Proceedings of EuroCrypt'94, LNCS 950. Springer-Verlag, pp. 428–432.

Camenisch, J., Pivereau, J., Stadler, M., 1994. Blind signatures based on the discrete logarithm problem. In: Santis, A. (Ed.), Advances in Cryptology: Proceedings of EuroCrypt'94, LNCS950. Springer-Verlag, pp. 428–432.

Chaum, D., 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24, 84–88.

Chaum, D., 1982. Blind signatures for untraceable payments. In: Chaum, D., Rivest, L., Sherman, T. (Eds.), Advances in Cryptology: Proceedings of Crypt'82. Plenum, NY, pp. 199–203.

Chaum, D., Pedersen, T., 1992. Wallet databases with observers. In: Brickell, F. (Ed.), Advances in Cryptology: Proceedings of Crypt'92, LNCS 740. Springer-Verlag, pp. 89–105.

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithm. IEEE Transactions on Information Theory IT-31, 469–472.

Ferguson, N., 1993. Single term off-line coins. In: Helleseth, T. (Ed.), Advances in Cryptology: Proceedings of EuroCrypt'93, LNCS 765. Springer-Verlag, pp. 318–328.

Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T., 1996. Robust threshold DSS signatures. In: Maurer, U. (Ed.), Advances in Cryptology: Proceedings of EuroCrypt '96, LNCS 1070. Springer-Verlag, pp. 354–371.

Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T., 1999. Secure distributed key generation for discrete-log based cryptosystems. In: Stern, J. (Ed.), Advances in Cryptology: Proceedings of EuroCrypt'99, LNCS 1592. Springer-Verlag, pp. 295–310.

Harn, L., 1994. Group-oriented (t,n) threshold digital signature scheme and digital multisignature. IEE Proceedings on Computers and Digital Techniques 141, 307–313.

Horster, P., Michels, M., Petersen, H., 1994. Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications. In: Pieprzyk, J., Safavi-Naini, R. (Eds.), Advances in Cryptology: Proceedings of AisaCrypt'94, LNCS 917. Springer-Verlag, pp. 224–237.

Hsu, C.L., Wu, T.S., Wu, T.C., 2001. New nonrepudiable threshold proxy signature scheme with known signers. The Journal of Systems and Software 148, 119–124.

Juang, W., Lei, C., 1996. Blind threshold signatures based on discrete logarithm. In: Jaffar, J., Yap, H. (Eds.), Proceedings of Second Asian Computing Science Conference on Programming, Concurrency and Parallelism, Networking and Security, LNCS 1179. Springer-Verlag, pp. 172–181.

Juang, W., Lei, C., 1999. Partially blind threshold signatures based on discrete logarithm. Computer Communications 22, 73–86.

Juang, W., Lei, C., Chang, C., 1999. Anonymous channel and authentication in wireless communications. Computer Communications 22, 1502–1511.

Juang, W., Lei, C., Liaw, H., 2001. Fair blind threshold signatures based on discrete logarithm. International Journal of Computer Systems Sciences & Engineering 16, 371–379.

Lei, C., Juang, W., Yu, P., 2002. Provably secure blind threshold signatures based on discrete logarithm. Journal of Information Science and Engineering 18, 23–39.

Menezes, A., Oorschot, P., Vanstone, S., 1997. Handbook of Applied Cryptography. CRC Press, New York.

Okamoto, T., Ohta, K., 1991. Universal electronic cash. In: Feigenbaum, J. (Ed.), Advances in Cryptology: Proceedings of Crypt'91, LNCS 576. Springer-Verlag, pp. 324–337.

Pedersen, T., 1991. Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (Ed.), Advances in Cryptology: Proceedings of Crypt'91, LNCS 576. Springer-Verlag, pp. 129–140.

Pointcheval, D., Stern, J., 1996. Provably secure blind signature schemes. In: Kim, K., Matsumoto, T. (Eds.), Advances in Cryptology: Proceedings of AisaCrypt'96, LNCS 1163. Springer-Verlag, pp. 252–265.

Rivest, R., Shamir, A., Adelman, L., 1978. A method for obtaining digital signatures and public key cryptosystem. Communications of ACM 21, 120–126.

Shamir, A., 1979. How to share a secret. Communications of ACM 22, 612–613.

Solms, S., Naccache, D., 1992. On blind signatures and perfect crime. Computers & Security 11, 581–583.

Stadler, M., Piveteau, J., Camenisch, J., 1995. Fair blind signatures. In: Guillou, C., Quisquater, J. (Eds.), Advances in Cryptology—EuroCrypt'95, LNCS 921. Springer-Verlag, pp. 209–219.

Stallings, W., 1999. Cryptography and Network Security, second ed. Prentice Hall International.

Wu, T.S., Hsu, C.L., in press. Threshold signature scheme using self-certified public keys. The Journal of Systems and Software.

Wen-Shenq Juang is an assistant professor at the department of Information Management, Shih Hsin University, Taipei, Taiwan. He received his master degree in Computer Information Science from National Chiao Tung University in 1993, and his Ph.D. degree in electrical engineering from National Taiwan University in 1998. His current research interests include information security, cryptographic protocols, and electronic commerce. Dr. Juang is a member of Chinese Cryptology and Information Security Association.

Horng-Twu Liaw is an associate professor at the department of Information Management, Shih Hsin University, Taipei, Taiwan. He received his Ph.D. degree in electrical engineering from National Taiwan University in 1992. His current research interests include electronic commerce, information security, and design and analysis of algorithm.