Privacy and Anonymity Protection with Blind Threshold Signatures

Wen-Shenq Juang, Chin-Laung Lei, and Horng-Twu Liaw

ABSTRACT: A set of group-oriented blind (*t*, *n*) threshold signature schemes is proposed based on the discrete logarithm problem. Using these schemes, any *t* out of *n* signers in a group can represent the group in signing blind threshold signatures. A threshold signature in the proposed schemes is the same size as an individual signature, and the signature verification process is simplified by means of a group public key. The schemes are suitable for single-authority applications in privacy protection, secure voting systems, and anonymous payment systems for distributing the power of a single authority. The assistance of a mutually trusted authority is not required. In addition, individual signers can choose their own private keys, and all the members together decide on the group public key.

KEY WORDS AND PHRASES: Anonymity, anonymous payment systems, blind signatures, privacy, secure voting systems, security, threshold signatures.

The concept of blind signatures was introduced by Chaum [5]. It allows the realization of privacy protection in such applications as secure voting systems that preserve the privacy of voters [12, 13, 19] and secure electronic payment systems that protect the anonymity of customers [1, 2, 5, 11, 12, 24]. In systems of this kind, a person called the signer is responsible for producing digital signatures. The other persons, called requesters, wish to obtain blind signatures on the messages they provide to the signer. In a distributed environment, the signed blind messages can be regarded as a certain amount of electronic money in a secure electronic payment system or as ballots in secret voting systems. A blind signature scheme must have the property of "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 that will later be made public [3, 5, 12, 17, 29]. In the blind signature schemes proposed by Camenisch, Piveteau, and Stadler; Horster, Michels, and Petersen; and Pointcheval and Stern [3, 17, 29], security is based on the difficulty of computing discrete logarithms [9, 28]. In the schemes proposed by Chaum, it is based on the difficulty of factorization [5, 29, 32].

Shamir was the first to propose the concept of threshold schemes [33]. Since then, many threshold cryptosystems have been proposed [8, 27]. The scheme proposed by Gennaro, Jarecki, Krawczyk, and Rabin allows *n* cooperating participants in a group to generate a group public key and to distribute secret shadows without the assistance of a mutually trusted authority [15]. Anyone can send a secret message to the group by using the public key to encrypt the message. The group secret key can only be reconstructed by at least *t* out of

This work was supported in part by the National Science Council of the Republic of China under contract NSC-91-2213-E-128-005.

International Journal of Electronic Commerce / Winter 2002–3, Vol. 7, No. 2, pp. 143–157.

1086-4415/2003 $9.50 + 0.00.

the n group members. Threshold signatures are motivated by the organizational need to protect a group of employees who agree on a message before signing and to protect the group private key from attacks launched by internal and external adversaries [14, 16]. The latter becomes more important with the actual deployment of public key schemes in practice. The signing power of some authorities inevitably invites attackers.

Several single-authority voting systems have been proposed [12, 13, 19]. All of these systems involve voters and the authority. The voters apply the blind signature technique to get their votes from the authority and return them to the authority (the counter) via an untraceable e-mail [4, 6, 20]. The authority publishes all the valid ballots. These systems assume that all the registered voters will cast their votes and no voter will abstain. In real life, registered voters may abstain from voting after the registration phase. The authority then can impersonate any voter who abstains and add extra ballots as desired. To cope with this dilemma, a blind (t, n) threshold signature scheme can be adopted for distributing the power of a single authority. In a blind (t, n) threshold signature scheme, any honest t out of n signers can be designated by a group (an organization) to sign a signature. The underlying assumption is that at least $(n - t + 1)$ of the n signers do not conspire with the others. The blind threshold signature will work when at least t out of n signers are honest. If $t - 1$ (or fewer) of the signers are dishonest, they cannot generate a valid blind threshold signature. Secure voting systems based on blind threshold signature schemes can satisfy the needs of a real-world environment in that the issue of votes is controlled by several authorities representing the concerned organization and can be chosen by the voters or assigned by the system, on the current available authorities list, according to the Internet condition. Since voters only need to request t members from n authorities, this can increase the availability of the signing authorities and thus the degree of protection against forgery by making it harder for an adversary to learn the group secret key.

This paper proposes an efficient blind threshold signature scheme as an example and discusses some possible extension schemes. The security of the proposed schemes relies on the difficulty of computing discrete logarithms, and it is computationally not feasible 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. In the proposed schemes, a threshold signature and an individual signature are the same size, and the verification process for the threshold signature is equivalent to that for each individual signature.

The Blind Threshold Signature Scheme

The blind threshold signature scheme proposed in this paper is based on the Nyberg-Rueppel scheme with message recovery [3]. One of its main advantages is that it can be combined with ElGamal encryption in a natural manner [25]. The scheme provides a mechanism for detecting wrong partial signatures. Without this mechanism or the correction capability proposed by

Gennaro, Jarecki, Krawczyk, and Rabin [14], one would have to try up to $\binom{n}{t}$ subsets of signers in order to find a subset that generates a valid blind threshold signature. The signing process of a typical blind threshold signature scheme involves two kinds of participants, the signers and a requester. Before the requester can obtain a signature from them, the signers have to cooperate to distribute their secret shadows to other signers in advance. Then the requester can request a blind threshold signature from the signers. The proposed scheme consists of the shadow-distribution phase, the signature-generation phase, and the signature-verification phase. The signers perform the shadow-distribution phase only once and then can use their secret shadows to sign messages. After this phase, the signers generate and publish a unique group public key. In the signature-generation phase, a requester requests a blind threshold signature from the signers, and they cooperate to issue the blind threshold signature to the requester. In the signature-verification phase, anyone can use the group public key to verify whether a threshold signature is valid.

Let n' be the number of signers before the shadow-distribution phase, let $QUAL$ be the set of nondisqualified signers after the shadow-distribution phase, let n be the number of nondisqualified signers $QUAL$. Let V_i, $1 \le i \le n'$ be the identification of signer i before the shadow-distribution phase. Let U_i, $1 \le i \le n$ be the identification of nondisqualified signer i after the shadow-distribution phase. Let n be the number of signers, let t be the threshold value of the blind threshold signature scheme, so that at least $(n - t + 1)$ signers are honest. Let m be the message to be blinded, let p, q be two large strong prime numbers such that q divides $(p - 1)$, and let ρ and ζ be two generators of Z_p^* [22] and ζ be a random value generated by a generic distributed coin-flipping protocol. Let $g \equiv_p \rho^{(p-1)/q}$ and $h \equiv_p \zeta^{(p-1)/q}$. In a distributed environment, V_i can choose the secret key d_i and publish the corresponding public key e_i. Anyone can get e_i via some authentication service (e.g., the X.509 directory-authentication service [34]). Using a secure public key signature scheme [9, 32], V_i can produce signatures of messages by d_i. Anyone can verify these signatures using the corresponding e_i. To make the proposed scheme clear, it is assumed that the message transmitted in the following protocol is via an authentication scheme (e.g., the RSA signature scheme). In other words, one cannot fake any other participant's messages, and one cannot deny the messages one really transmitted.

The Shadow-Distribution Phase

Before a requester can request a threshold signature from the signers, all the signers must cooperate to distribute their shadows to other signers without the assistance of a mutually trusted authority. In this phase, signers can use the verification equations to detect any incorrect shares. In the shadow-distribution phase, all V_i, $1 \le i \le n'$, cooperate to generate their public keys and the corresponding group public key, and distribute secret shadows to one other without a trusted third party. The process in the shadow-distribution phase is similar to the one proposed by Gennaro, Jarecki, Krawcyzk, and Rabin [15]. Together with the system parameters it is presented briefly in what follows.

Let z_i be the secret key and $f_i(x) = \sum_{k=0}^{t-1} a_{i,k} x^k$, where $a_{i,0} = z_i$, is a random secret polynomial chosen by V_i. Let $A_{i,l} \equiv_p g^{a_{i,l}}$. The signers then do the same processes as Gennaro, Jarecki, Krawcyzk, and Rabin [15] to distribute their secret shadows to others. Assume the set of nondisqualified signers is $QUAL$. Finally, V_i, $i \in QUAL$, can get his shares $\delta_{i,j} \equiv_q f_i(x_j)$, where $j \neq i$, $j \in QUAL$ and x_j is a unique public number for V_j. The public shadows $P_{j,i} \equiv_p g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-1} (A_{j,l})^{x_i^l}$, where i and $j \in QUAL$, the group public key $y \equiv_p \prod_{j \in QUAL} y_j \equiv_p \prod_{j \in QUAL} A_{j,0} \equiv_p \prod_{j \in QUAL} g^{a_{j,0}} \equiv_p g^{\sum_{j \in QUAL} a_{j,0}} \equiv_p g^{\sum_{j \in QUAL} z_j}$, and the personal public key $y_i \equiv_p A_{i,0} \equiv_p g^{z_i}$ will then be published. The corresponding group secret key is $z \equiv_q \sum_{j \in QUAL} z_j$. Without loss of generality, we assume that n nondisqualified signers $QUAL$ are U_i, $1 \le i \le n$. This can be done by renaming the index of each signer V_i, $i \in QUAL$.

The Signature-Generation Phase

Without loss of generality, it is assumed that t out of n signers are U_i, $1 \le i \le t$. A requester who requests a blind threshold signature, together with the t signers, performs 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 $\hat{r}_i$, $1 \le i \le t$, the requester does the following:
   (a) Choose two random numbers $\alpha \in Z_q$ and $\beta \in Z_q^*$, compute $r \equiv_p m \prod_{i=1}^{t} r_i \equiv_p m g^{t\alpha} (\prod_{i=1}^{t} \hat{r}_i)^{\beta}$ and $\hat{m} \equiv_q \beta^{-1} r$, where $r_i \equiv_p g^{\alpha} \hat{r}_i^{\beta}$ and $1 \le i \le t$.
   (b) Check if $\hat{m} \neq 0$. If yes, send $\hat{m}$ to all U_i, $1 \le i \le t$. Otherwise, go back to Step 2a.
3. Upon receiving $\hat{m}$, each U_i computes $\hat{s}_i \equiv_q \hat{m} (z_i + \sum_{j=t+1}^{n} f_j(x_i) (\prod_{k=1, k \neq i}^{t} ((-x_k) / (x_i - x_k)))) + k_i$ and sends $\hat{s}_i$ back to the requester.
4. After receiving all $\hat{s}_i$, the requester computes $\hat{s}_i \equiv_p \hat{s}_i \beta + \alpha$, and checks if

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

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

The Signature-Verification Phase

To verify the threshold signature (r, s), one simply computes $m \equiv_p g^{-s} y^r r$ and checks whether m has any redundancy information. If m has no proper redundancy, a secure one-way hashing function 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.

Analysis

The correctness and security of the proposed scheme will now be discussed.

Gennaro et al. have shown that in their distributed key generation protocol, the view of an adversary of the protocol can be simulated [15]. In the scheme proposed here, unlike their scheme, cheating by a signer can be detected if all the signers publish the public shadows ($P_{j,i} \equiv_p g^{\delta_{j,i}} \equiv_p \prod_{l=0}^{t-l} (A_{j,l})^{x_i l}$, where i and $j \in QUAL$). The public shadows ($P_{j,i}$, where i and $j \in QUAL$) can be computed by the public values $A_{i,k} \equiv_p g^{a_{i,k}}$, $i \in QUAL$, $0 \le k \le t-1$, broadcast in the shadow-distribution phase. These public shadows will not disclose any extra information about the group secret key. The foregoing shadow-distribution phase is secure in that it satisfies the simulation argument [15, 23].

To prevent a signer from sending an invalid partial signature to the requester, a partial signature can be checked in Step 4 of the shadow-generation phase. The following lemma ensures the correctness of partial signatures.

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

Proof. By our scheme, we have

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

When the signature-generation phase is over, the threshold signature can be verified by the group public key in the signature-verification phase. Theorem 2 ensures the correctness of the scheme.

*Theorem 2 The pair (*r, s*) is a valid 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:

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

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

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

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

$$\equiv_p mg^{-\left(\hat{m}\left(\sum_{i=1}^{t}z_i+\sum_{i=t+1}^{n}z_i\right)\right)\beta} g^{\sum_{i=1}^{n}z_i r}$$

$$\equiv_p mg^{-\hat{m}\sum_{i=1}^{n}z_i\beta} g^{\sum_{i=1}^{n}z_i r}$$

$$\equiv_p mg^{-r\sum_{i=1}^{n}z_i} g^{\sum_{i=1}^{n}z_i r}$$

$$\equiv_p m.$$

To prove that the scheme is blind, it can be shown that, given any view and any valid message-signature pair $(m, (r, s))$, there exists a unique pair of blinding factors α and β. Since the requester randomly chooses the blinding factors α and β, the blindness of the signature scheme follows.

Extension Schemes and Performance Considerations

Extension Schemes

The proposed scheme uses the blind signature scheme proposed by Camenisch, Piveteau, and Stadler with message recovery [3]. It can also use their modifi-

cation of the DSA blind signature scheme. Horster, Michels, and Petersen extended the blind signature scheme proposed by Camenisch, Piveteau, and Stadler [3, 17]. As the latter mentioned, not every variant of the Meta-Message recovery signature scheme can be transformed into a blind signature scheme. For example, there is as yet no blind signature scheme for the original ElGamal signature scheme. The extensions of the secure blind signature schemes proposed by Horster et al. can be used in the scheme proposed here, except that $\tilde{B}$ contains $\tilde{s}$ in the signature-generation equation. The security considerations and performance analysis of these extended schemes are similar to those in the present proposed scheme. Pointcheval and Stern proposed two provable secure blind signature schemes [29]. 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 the present scheme, Pointcheval and Stern's secure blind signature scheme based on discrete logarithms can also be used in the modified scheme [29]. The security considerations of this modified scheme are similar to those of the scheme proposed here.

Performance Considerations

The computational cost required to compute blind threshold signatures using the proposed scheme and the extended schemes will now be analyzed. The measures will be the number of modular exponentiations and modular inverses required by a single player during the execution of the signature-generation phase. The shadow-distribution phase only needs to be executed once and can be computed on-line. Then signers can cooperate to issue blind threshold signatures. Table 1 shows a comparison between the blind threshold signature scheme and its underlying blind signature scheme. The performance analyses of the extended schemes and the proposed scheme are similar. Scheme 1 denotes the blind threshold signature scheme discussed above, and Scheme 1* denotes its corresponding underlying single-authority blind signature scheme. To reduce the computational cost for each signer, the value $-x_k/(x_i - x_k)$, $1 \le k \le n$ and $k \ne i$, in Step 3 of the signature-generation phase can be computed off-line. In this case, each signer needs to compute only one modular exponentiation in the proposed 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 to compute $\sum_{j=t+1}^{n} f_j(x_i)(\prod_{k=1,k\ne i}^{t}((-x_k)/(x_i - x_k)))$ in Step 3, which contains $n-2$ modular multiplications and $n-t$ additions. To reduce the computational cost needed by the requester, the partial signature verification in Step 4 would not be done except that the final threshold signature cannot pass the verification equation in the signature-verification phase. If a requester finds a dishonest signer via the verification equation, the system will publish the identity of the dishonest signer and the dishonest signer will be excluded. In a payment or voting system, the signers must be persons of good repute in real-world environments. The partial verification equation will rarely be used. In this approach, the requester only needs to perform two modular exponentiations and one modu-

	The requester				The signer or U_i			
	EXP	**INV**	**MUL**	**ADD**	**EXP**	**INV**	**MUL**	**ADD**
Scheme 1	2	1	$t+5$	t	1	0	$n-1$	$n-t+1$
Scheme 1*	2	1	4	1	1	0	1	1

Table 1. Cost Comparison of the Signature-Generation Phases.

EXP: number of modulo exponentiations; INV: number of modulo inversions (divisions); MUL: number of modulo multiplications; ADD: number of modulo additions.

lar inverse in Step 2 of the signature-generation phase, which is the same as the underlying blind signature scheme. Since the blind threshold verification function of the proposed scheme is the same as that of the underlying blind signature scheme, the verification cost is the same for the blind threshold signature and the underlying blind signature. Compared with the underlying blind signature scheme, the extra cost for requesting a blind threshold signature in the proposed scheme proposed in the third section is to compute $t\alpha$, $\prod_{i=1}^{t} \hat{r}_i$, $t\alpha$and $\sum_{i=1}^{t} \hat{s}_i$ in the equation $s \equiv_q \sum_{i=1}^{t} s_i \equiv_q \sum_{i=1}^{t} (\hat{s}_i\beta + \alpha) \equiv_q t\alpha + \beta \sum_{i=1}^{t} \hat{s}_i$, which contains $t + 1$ modular multiplications and $t - 1$ modular additions.

Gennaro, Jarecki, Krawczyk, and Rabin proposed three robust threshold signature protocols: DSS-Thresh-Sig-1, DSS Thresh- Sig-2, and DSS-Thresh-Sig-3 [14]. One approach to generate blind threshold signatures is to take robust threshold signature schemes and turn them into blind signature schemes [14]. 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 require $O(nt)$ modular exponentiations. When there are only a few cheaters, this approach is quite clearly inefficient as compared to the schemes proposed in this paper.

Applications in Privacy Protection

The concept of blind signatures makes it possible to protect privacy in such applications as secure voting systems that preserve voter privacy [12, 13, 19] and secure electronic payment systems that protect customer anonymity [1, 2, 5, 10, 11, 12, 24, 26]. The discussion will now explore how the proposed schemes can be used with existing single-authority voting systems or anonymous payment systems to distribute the power of a single authority.

Multi-Authority Secure Voting Systems

Fujioka, Okamoto, and Ohta and Juang and Lei have proposed several single-authority voting systems [13, 19]. These can be simplified to the three phases of registration, voting, and publication. During the registration phase, voters apply the blind signature technique to get their blind votes. In the voting phase, they generate real ballots from the blind votes received in the registration phase and send them to the authority via an untraceable e-mail [4, 6, 20]. Finally, in the publication phase, the authority publishes the valid ballots.

Since voters only need to communicate with the authority in these protocols, there is no global computation of voters. But the authority can impersonate any voter who abstains from voting after the registration phase. All of these systems assume that all the registered voters must cast their votes and no voter can abstain, but in real life, registered voters may abstain from voting after the registration phase. A simple solution is to require the voters, during the voting phase, to send their ballots to a counter rather than the authority. Thus, some

of the authority's power is distributed to the counter. If the authority and the counter do not conspire and only a very few voters abstain, the authority cannot add extra ballots to the tally. Otherwise the secret-ballot systems of Fan and Chen; Fujioka, Okamoto, and Ohta; and Juang and Lei must be modified [12, 13, 19], as shown below.

1. Instead of a unique authority, the modified systems consist of n authorities. Let $t > n/2$ be the threshold value of the threshold scheme, so that at least $(n - t + 1)$ authorities are honest; that is, at least $(n - t + 1)$ out of n authorities do not conspire with the others.
2. Each system involves voters and the n authorities, and consists of the registration, voting, and publication phases.

In the registration phase, voters send their registration certificates to t honest authorities and apply the blind threshold signature technique to get their blind votes from these authorities. In the voting phase, voters generate their real ballots from the blind votes received in the registration phase and send them to a counter (any authority can serve as the counter) via an untraceable e-mail.

In the publication phase, the counter publishes all valid votes and all registration certificates.

Any interested voter must check whether his vote has been properly counted. If his ballot is misplaced or not counted by any authority, the voter can send it to a third party to make an objection. Since at least $(n - t + 1)$ out of n authorities do not conspire with the other authorities, the total number of ballots published by the authority must be less than or equal to the number of registrations.

The above modifications distribute the power of a single authority among several authorities, and registered voters can abstain from voting after the registration phase. Since voters only need to request exactly t members from n authorities in the registration phase, it can meet the requirements of a real-world environment without a single trusted authority or with some absent or dishonest authorities.

Compared with single-authority voting systems [12, 13, 19], the extra cost for a requester to get a vote is $(t + 1)$ multiplications and $(t - 1)$ additions in Table 1 and no extra exponentiation operation. To make the application user-interface user-friendly, the client program will automatically choose t honest (available) authorities according to the Internet condition. From the voter's standpoint, the procedures of the proposed scheme are transparent, as are those of single-authority voting schemes [12, 13, 19]. In a distributed environment, to make each blind threshold signature atomistic, a voter requesting a blind threshold signature as a vote must include in the registration information the identifications of t honest (available) authorities as certificated by the voter. If a transaction fails, the transaction log must be sent to the counter and kept in its database. If a voter tries to register again, the authority can ask the counter to check whether the last transaction failed. If yes, the authority allows the voter to register. Otherwise, the voter is rejected. All of the preceding procedures can be embedded in programs and executed automatically. In real-world

environments, the candidates of authorities can be elected from major parties. As a practical implementation, the parameters $t = 3$ and $n = 5$ are suggested.

Cramer et al. proposed a multi-authority voting system, based on homomorphic encryption and proofs of knowledge, that is more suitable for large-scale elections because of the low computation and communication overhead even with a large number of voters [7]. The system's essential drawback is that if t authorities conspire, where t is the threshold value of the threshold cryptosystem generated by n authorities, the privacy of the voters is violated. Since the voters can only state their intentions as "yes" or "no," this system is not a general election protocol. When voters can make choices from among several options, computing the individual ballots and the final tally is generally more complicated.

Multi-Authority Anonymous-Payment Systems

The critical success factors in operating and implementing an electronic business are money flow, material flow, and information flow. E-commerce entrepreneurs have to provide services on the Internet that will keep existing customers and attract new ones. From the customer's point of view, security, anonymity, efficiency, and flexibility are the main criteria of electronic payment systems. From the standpoint of a bank or the government, security and implementation costs are most important [1, 30]. Secure payment systems have been investigated both practically and theoretically by many researchers [1, 2, 5, 10, 11, 12, 24, 26]. A secure payment system can be regarded as a protocol involving a customer, a shop, and a bank. Both the shop and the customer have accounts with the bank. Payment systems that verify the validity of an electronic payment transaction may be on-line or off-line. In an on-line system, all the participants—customer, shop, and bank—have to be connected on-line when the customer buys something [2, 5, 11, 12, 24]. In off-line systems, each transaction during the protocol only requires two participants [10, 26]. Off-line systems do not prevent double-spending, but they make it possible to detect frauds and identify cheaters. Banks may decide not to adopt off-line systems because of the risk of double-spending [30]. These systems are intended to produce electronic money that has the same properties as paper cash. The protocols can be simplified in on-line systems [2, 5, 11, 24]. In the withdrawal phase, to withdraw an e-coin with a fixed value, $\varkappa$ dollars, a customer applies the blind signature technique to get the blind e-coin from the bank. The bank deducts $\varkappa$ dollars from the customer's account. In the unblinding phase, the customer generates the real e-coin from the blind e-coin received in the withdrawal phase. In the spending phase, in order to spend the e-coin at a designated shop, the customer sends the e-coin to the shop. The shop can check whether the e-coin is valid. If yes, it sends the e-coin to the bank. The bank also checks whether the e-coin is valid and has not been reused by checking the used e-coins database. If the e-coin has not been double-spent, the shop and the bank accept the payment, and the shop deposits the e-coin, $\varkappa$ dollars, in the bank. The bank then stores the e-coin in the used e-coins database and increases the amount of the shop's account by $\varkappa$ dollars.

All the proposed payment systems are single-authority systems [1, 2, 5, 10, 11, 12, 24, 26]. They are all based on the assumption that the single money issuer of these systems is trustworthy. However, the money issuer may decide to issue extra e-coins. Doing so may cause great harm to the corporation or to society. This problem can be eliminated if, instead of a unique authority, every customer has to request blind (t, n) threshold signatures as e-coins from t arbitrary money issuers in the withdrawal phase. The issue of e-coins is controlled by several money 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.

Compared with single-authority payment systems [1, 2, 5, 11, 12, 24], the extra cost for a requester to get an e-coin is $(t + 1)$ multiplications and $(t - 1)$ additions in Table 1 and no extra exponentiation operation. The application interface is made user-friendly by having the client program automatically choose t honest (available) issuers depending on the Internet condition. From the customer's standpoint, all the procedures in the proposed scheme are transparent, and the same holds for single-authority payment schemes [1, 2, 5, 11, 12, 24]. In a distributed environment, to make the transaction of each blind threshold signature atomistic, a customer requesting a blind threshold signature as an e-coin must include in the registration information the identities of t honest (available) issuers and a logical time-stamp to indicate that this transaction and the registration information are certified by the customer. Any of the t issuers who receives this certificate verifies it. If it is valid, then the issuer sends it to the bank. The bank can deduct $\mathcal{X}$ dollars from the customer's account in the bank. If a transaction fails, the issuers must send the logs of the transaction to the bank. The bank can undo a transaction and keep the log in its database. All the above procedures can be embedded in programs and executed automatically. In real-world environments, issuers can select persons known to be honest or audit managers as candidates. As a practical implementation, the parameters $t = 2$ and $n = 3$ are suggested.

The critical success factors for an enterprise to provide attractive services on the Internet are money flow, material flow, and information flow. E-commerce entrepreneurs have to provide various services on the Internet in order to keep customers and attract new ones. As indicated by Rivest, anonymity will be a valued-added feature that a customer may purchase or see as an appealing new service [30]. From the customer's point of view, anonymity, security, efficiency, and flexibility are the main criteria of electronic payment systems. From the point of view of a bank or the government [30], security, selective anonymity (e.g., only for micropayments), and implementation costs are most important. A payment system that satisfies the needs for security, anonymity, efficiency, and micropayments will probably work well in the near future [30]. The concept of PayWord chains proposed by Jutla and Jung and by Rivest and Shamir can be directly applied to the proposed scheme in order to achieve the possibility of spending fractions of an e-coin [21, 31]. As indicated by Asokan, Janson, Steiner, and Waidner, several different off-line transaction schemes use tamper-resistant devices [1]. This concept can also be directly applied to the present scheme. Fan et al. proposed an efficient blind signature scheme for such applications as ownership-claimable payment systems and

fair voting schemes [12]. The additional computation of these schemes consists of just two hashing operations. Since the scheme proposed by Fan and Chen is based on a generic blind signature scheme, it can be directly applied to the present scheme without affecting its corresponding infrastructure [12].

Conclusion

A set of blind threshold signature schemes has been proposed based on the discrete logarithm problem. In these schemes, threshold signatures and individual signatures are the same size and are verified by equivalent processes. The proposed schemes can be easily applied to efficient single-authority applications in privacy protection, such as secure voting systems and anonymous payment systems for distributing the power of a single authority, without changing the underlying structure or degrading overall performance.

REFERENCES

1. Asokan, N.; Janson, P.; Steiner, M.; and Waidner, M. State of the art in electronic payment systems. *IEEE Computer, 30,* 9 (1997), 28–35.
2. Camenisch, J.; Piveteau, J.; and Stadler, M. An efficient payment system protecting privacy. In D. Gollmann (ed.), *Proceedings of ESORICS'94.* Berlin: Springer-Verlag, 1994, pp. 207–215.
3. Camenisch, J., Piveteau, J., and Stadler, M. Blind signatures based on the discrete logarithm problem. In D. Santis (ed.), *Advances in Cryptology-EuroCrypt'94.* Berlin: Springer-Verlag, 1995, pp. 428–432.
4. Chaum, D. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, 24,* 2 (1981), 84–88.
5. Chaum, D. Blind signatures for untraceable payments. In D. Chaum, L. Rivest, and T. Sherman (eds.), *Advances in Cryptology: Crypt '82.* Berlin: Springer-Verlag, 1983, pp. 199–203.
6. Chaum, D. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology, 1* (1988), 65–75.
7. Cramer, R.; Gennaro, R.; and Schoenmakers, B. A secure and optimally efficient multi-authority election system. In *Advances in Cryptology: EuroCrypt '97.* Berlin: Springer-Verlag, 1997, pp. 103–118.
8. Desmedt, Y., and Frankel, Y. Threshold cryptosystems. In G. Brassard (ed.), *Advances in Cryptology: Crypt'89.* Berlin: Springer-Verlag, 1990, pp. 307–315.
9. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithm. *IEEE Transactions on Information Theory, IT-31,* 4 (1985), 469–472.
10. Eng, T., and Okamoto, T. Single-term divisible electronic coins. In D. Santis (ed.), *Advances in Cryptology: EuroCrypt'94.* Berlin: Springer-Verlag, 1995, pp. 306–319.
11. Fan, C., and Lei, C. Low computation partially blind signatures for electronic cash. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E81-A,* 5 (1998), 818–824.

12. Fan, C., and Chen, W. An efficient blind signature scheme for information hiding. *International Journal of Electronic Commerce, 6,* 4 (summer 2002), 93–100.
13. Fujioka, A.; Okamoto., T.; and Ohta, K. A practical secret voting scheme for large scale elections. In J. Deberry and Y. Zheng (eds.), *Advances in Cryptology: AusCrypt'92.* Berlin: Springer-Verlag, 1992, pp. 244–251.
14. Gennaro, R.; Jarecki, S.; Krawczyk, H.; and Rabin, T. Robust threshold DSS signatures. In U. Maurer (ed.), *Advances in Cryptology: EuroCrypt '96.* Berlin: Springer Verlag, 1996, pp. 354–371.
15. Gennaro, R.; Jarecki, S.; Krawczyk, H.; and Rabin, T. Secure distributed key generation for discrete log-based cryptosystems. In J. Stern (ed.), *Advances in Cryptology: EuroCrypt '99.* Berlin: Springer-Verlag, 2000, pp. 295–310.
16. Harn, L. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. *IEE Proceedings on Computers and Digital Techniques, 141,* 5 (1994), 307–313.
17. Horster, P.; Michels, M.; and Petersen, H. Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications. In J. Pieprzyk and R. Safavi-Naini (eds.), *Advances in Cryptology: AisaCrypt '94.* Berlin: Springer-Verlag, 1994, pp. 224–237.
18. Juang, W., and Lei, C. Blind threshold signatures based on discrete logarithm. In J. Jaffar and H. Yap (eds.), *Proceedings of Second Asian Computing Science Conference on Programming, Concurrency and Parallelism, Networking, and Security*. Berlin: Springer-Verlag, 1996, pp. 172–181.
19. Juang, W., and Lei, C. A secure and practical electronic voting scheme for real world environments. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E80-A*, 1 (1997), 64–71.
20. Juang, W.; Lei, C.; and Chang, C. Anonymous channel and authentication in wireless communications. *Computer Communications, 22*, 15/16 (1999), 1502–1511.
21. Jutla, C., and Yung, M. PayTree: "Amortized signature" for flexible micropayments. In *Proceedings of the Second USENIX Workshop on Electronic Commerce.* Berkeley, CA: USENIX, 1996, pp. 213–221.
22. Menezes, A.; Oorschot, P.; and Vanstone, S. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.
23. Micali, S., and Rogaway, P. Secure computation. In J. Feigenbaum (ed.), *Advances in Cryptology: Crypt '91*. Springer-Verlag, 1992, pp. 392–404.
24. The NetBill Project (www.ini.cmu.edu/NETBILL/).
25. Nyberg, K., and Rueppel, R. Message recovery for signature schemes based on the discrete logarithm problem. In D. Santis (ed.), *Advances in Cryptology: EuroCrypt '94.* Berlin: Springer-Verlag, 1995, pp. 182–193.
26. Okamoto, T., and Ohta, K. Universal electronic cash. In J. Feigenbaum (ed.), *Advances in Cryptology: Crypt '91.* Berlin: Springer-Verlag, 1992, pp. 324–337.
27. Pedersen, T. A threshold cryptosystem without a trusted party. In W. Davies (ed.), *Advances in Cryptology: EuroCrypt '91.* Berlin: Springer-Verlag, 1991, pp. 522–526.

28. Pohlig, S., and Hellman, M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory, IT-24* (1978), 106–110.
29. Pointcheval, D., and Stern, J. Provably secure blind signature schemes. In K. Kim and T. Matsumoto (eds.), *Advances in Cryptology: AsiaCrypt '96.* Berlin: Springer-Verlag, 1996, pp. 252–265.
30. Rivest, R. Perspectives on financial cryptography. In B. Kaliski (ed.), *Financial Crypto '97.* Berlin: Springer-Verlag, 1997, pp. 145–150.
31. Rivest, R., and Shamir, A. PayWord and MicroMint: Two simple micropayment schemes. In M. Lomas (ed.), *Proceedings of International Workshop on Security Protocols.* New York: Springer, 1997, pp. 69–87.
32. Rivest, R.; Shamir, A.; and Adelman, L. A method for obtaining digital signatures and public key cryptosystem. *Communications of the ACM, 21,* 2 (1978), 120–126.
33. Shamir, A. How to share a secret. *Communications of the ACM, 22* (1979), 612–613.
34. Stallings, W. *Cryptography and Network Security,* 2d ed. Englewood Cliffs, NJ: Prentice Hall International, 1999.

WEN-SHENQ JUANG (wsjuang@cc.shu.edu.tw) is an assistant professor of information management at Shih Hsin University in Taipei. He received his master's degree in computer information science from National Chiao Tung University in 1993 and his Ph.D. in electrical engineering from National Taiwan University in 1998. His research interests include information security, cryptographic protocols, and electronic commerce. Dr. Juang is a member of the Chinese Cryptology and Information Security Association.

CHIN-LAUNG LEI (lei@cc.ee.ntu.edu.tw) is a professor of electrical engineering at National Taiwan University in Taipei. He received his B.S. degree in electrical engineering from National Taiwan University in 1980 and his Ph.D. in computer science from the University of Texas in 1986. From 1986 to 1988, he was an assistant professor of computer and information science at Ohio State University. His research interests include network security, cryptography, algorithm design and analysis, and operating system design. Dr. Lei is a member of the Institute of Electrical and Electronic Engineers and the Association for Computing Machinery.

HORNG-TWU LIAW (htliaw@cc.shu.edu.tw) is an associate professor of information management at Shih Hsin University in Taipei. He received his Ph.D. in electrical engineering from National Taiwan University in 1992. His research interests include electronic commerce, information security, and algorithm design and analysis.