JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 15, 669-678 (1999)

(t, n) Threshold Digital Signature With Traceability Property

WEI-BIN LEE AND CHIN-CHEN CHANG+
Department of Information Engineering
Feng Chia University
Taichung, Taiwan 407, R.O.C.
+Institute of Computer Science and Information Engineering
National Chung Cheng University
Chiayi, Taiwan 621, R.O.C.
E-mail: ccc@cs.ccu.edu.tw

Group oriented (t, n) threshold digital signature schemes have a problem in that the underlying signature schemes will be broken if any t or more shadowholders conspire together with each other. This weakness was noted by Li et al. at Crypt'93, and later in 1994, they proposed a solution to this problem. However, their solution is impractical from the verifier's point of view. In fact, many people think that the verification period should be processed as quickly as possible since the message is signed just once but is verified many times. Besides the inefficiency of verification in Li et al.'s scheme, Michels and Horster have also shown that the signer cannot be sure who his co-signers are in this scheme. Hence, impersonation in their solution is possible. To enhance security and promote the efficiency, we propose a new (t, n) threshold signature scheme.

Keywords: secret sharing scheme, digital signature, Lagrang interpolating polynomial, discrete logarithm problem, factoring problem, Chinese remainder theorem

1. INTRODUCTION

Digital signatures play an important role in our modern electronic society because they have the properties of integrity and authentication. The integrity property ensures that the received message is not modified, and the authentication property ensures that the sender is not impersonated. In well known conventional digital signatures, such as RSA [1] and DSA [2], a single signer is sufficient to produce a valid signature, and anyone can verify the validity of any given signature. However, on many occasions, we need to share the responsibility of the signing message with a set of signers. Issuing checks for a company is an example for this. For the sake of security, it may be a policy of a company that checks must be signed by a group of individuals rather than one person [3]. Threshold signature schemes [3-5] and multisignature schemes [3, 6, 7] are designed to solve such problems. There are two major differences between multisignature and threshold signature schemes. Firstly, it is not necessary to restrict the number of signers to generate a valid signature in a multisignature scheme. In contrast with a multisignature scheme, a threshold value t must be predetermined to guarantee the security of the system in a threshold signature scheme. Secondly, a threshold signature represents the signature signed by the group while a

Received March 12, 1997; accepted May 12, 1998.
Communicated by Jean-Lien C. Wu.

multisignature is a signature which represents a set of individuals who sign the message. Consequently, a threshold signature is suitable for the case where the members of a group are allowed to sign on behalf of the group.

The concept of the (t, n) threshold cryptosystem was introduced by Desmedt and Frankel [4] in 1991; its digital signature version permits a valid signature to be produced among participants in such a way that:

1. only t or more participants can sign the message;
2. any t-1 or fewer participants cannot forge the signature.

However, Li et al. have pointed out that if t or more participants act in collusion, then they can impersonate any other set of members to forge the signature [8]. This case implies that a malicious subgroup of members can forge signatures without taking any responsibility. We believe that a signer should take responsibility for the signature he has signed. Obviously, Li et al.'s observation has shown that t or more participants acting in collusion can violate this responsibility concept. In fact, all the (t, n) threshold digital signature schemes proposed so far cannot solve this problem. Basically, a (t, n) threshold digital signature scheme is a combination of a conventional digital signature scheme and a secret sharing scheme. Thus, it is no surprise that if t or more participants act in collusion, then they can impersonate any other set of members to forge a signature. The major reason is that the secret key used to sign the message in a (t, n) threshold digital signature scheme is the shadow in the secret sharing scheme. In a secret sharing scheme [9], by definition, any t or more members can easily obtain the shared secret key. It is readily seen that a certain malicious subgroup of t or more members can derive other members' secret keys. To solve this problem, Li et al. added a random number to the shadow to form a secret key held by each member. Thus, the security of the scheme is guaranteed by the additional random number. The additional random number gives the (t, n) threshold digital signature scheme the property of traceability, which means that we can trace adversarial signers if forgery is suspected.

Multisignature schemes, on the other hand, can generate a signatures by multiple signers with knowledge of multiple secrets [3]. There are two major differences between multisignature and threshold signature schemes. Firstly, it is not necessary to restrict the number of signers in order to generate a valid signature in a multisignature scheme. In contrast with a multisignature scheme, a threshold value t must be predetermined to guarantee the security of the system in a threshold signature scheme. Secondly, a threshold signature represents the signature signed by the group while a multisignature is a signature which represents a set of individuals who sign the message. Thus, a multisignature has to be verified using with the public keys of the signers to it.

In this study, we have designed a new (t, n) threshold signature scheme by employing both the idea of a (t, n) threshold signature to represent the signature signed by the group and the idea of a multisignature to guarantee the property of traceability. In terms of performance, our scheme is more efficient than Li et al.'s scheme in both storage and computation costs. In the next section, we shall review Li et al.'s scheme and make some comments on it. The new scheme will be proposed in section 3. In section 4, we shall discuss the performance and the security of our scheme. Finally, our conclusions will be stated in section 5.

2. REVIEW LI ET AL.'S SCHEME

In this section, we shall review the first scheme proposed by Li, Hwang and Lee [5]. In their scheme, a trusted dealer is assumed to take the responsibility of picking the parameters. This dealer selects two large primes p and q so that $q \mid (p - 1)$, a generator g with order q over $GF(p)$ and a polynomial $f(x) = \sum_{i=0}^{t-1} a_i x_i \bmod q$. Then, the dealer computes the system secret key $x = f(0) \bmod q$ and computes the public group key $y = g^x \bmod p$. For each member U_i in the group with identity ID_i, the dealer computes the secret key $x_i = t_i + f(ID_i) \bmod q$ for him, where t_i is a random number. Thus, in the scheme, each member must carry two public keys, $y_i = g^{x_i} \bmod p$ and $z_i = g^{t_i} \bmod p$.

To sign the message m, each member in B picks a random number k_i and computes $r_i = g^{k_i} \bmod p$, where B is a subset in the group. The public value r_i is sent to the clerk. If all r_i's are available, then each signer generates his partial signature s_i using the equation below:

$$s_i = x_i\Big(\prod_{\substack{j\in B\\ j\neq i}} \frac{0 - ID_j}{ID_i - ID_j}\Big) + k_i E \bmod q, \text{ where } E = h(m, R) \bmod q \text{ and } R = \prod_{i\in B} r_i \bmod p.$$

The individual signature s_i can be verified as

$$g^{s_i} = y_i^{\left(\prod_{\substack{j\in B\\ j\neq i}} \frac{0-ID_j}{ID_i - ID_j}\right)} r_i^E \bmod p.$$

The clerk combines the individual signatures into a group oriented (t, n) threshold signature if all the partial signatures are correct. The clerk computes

$$S = \sum_{i\in B} s_i \bmod q.$$

Then (m, B, R, S) is the group signature of message m signed by the members in B. This signature can be verified by computing

$$T = \prod_{i\in B} z_i^{\left(\prod_{j\in B, j\neq i} \frac{0-ID_j}{ID_i - ID_j}\right)} \bmod p \tag{1}$$

and

$$E = h(m, R) \bmod q,$$

and by checking whether the following relation holds:

$$g^S \equiv YTR^E \bmod p.$$

We will discuss this scheme from the viewpoint of computation cost, storage cost, and security. Because there are t participants in the subgroup B, the verifier needs t multiplications and t exponentiation computations to derive the verification value T. Computing Eq. (1) is a very time-consuming operation for the verifier. On the other hand, each member in the group must carry two public keys and one secret key with him. The storage cost of these keys is $O(2p + q)$. According to the assumptions made in [5], we need about 1184 bits to keep the keys.

Recently, Michels and Horster showed that the signer cannot be sure who his co-signers are in Li et al.'s scheme[5]. Unfortunately, this weakness violates the traceability property.

The major concern in this study was to design a new threshold signature scheme which is better than Li et al.'s scheme in terms of computation cost, storage cost and security.

3. NEW PROPOSED THRESHOLD DIGITAL SIGNATURE SCHEME

We assume that there is a trusted dealer *TD* to determine the group secret key and to deliver the secret shadows to all the members in the group. Let A be the set of all the group members of size N, and let B be any subset in A of size t. The word "trusted" implies that the dealer must ensure that the secret information is not disclosed or revealed to unauthorized people and prevent unauthorized alternation or destruction of data. It is expected that if the dealer is compromised, the security of the whole system will be lost.

Let us divide our scheme into three phases: the initialization phase, the signature generation phase and the signature verification phase. The new scheme can thus be stated as follows.

3.1 Initialization Phase

Firstly, the trusted *TD* selects the following parameters:

1. a huge prime p, where $2^{511} < p < 2^{512}$;
2. a number $n = qw$, where q and w are two large primes and $n \mid (p-1)$; here, we let $2^{160} < q$, $w < 2^{161}$;
3. a generator g of order n in $GF(p)$;
4. a collision free hash function h;
5. a polynomial $f(x)$ of degree t-1 over $GF(q)$, where $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \dots + a_1x + a_0 \bmod q$.

For the sake of convenience, we can further prepare two parameters c_q and c_w, where

$$\begin{aligned} c_q &= 1 \bmod q \\ &= 0 \bmod w, \text{ and} \\ c_w &= 0 \bmod q \\ &= 1 \bmod w. \end{aligned}$$

Using these two parameters, we can compute $k \equiv k_qc_q + k_wc_w \pmod n$, which satisfies

$$\begin{aligned} k &= k_q \bmod q \\ &= k_w \bmod w. \end{aligned}$$

Thus, the trusted *TD* publishes $\{p, n, c_q, c_w, g, h\}$ as the group public parameters and keeps polynomial $f(x)$ from being revealed.

Then, the *TD* determines $x = f(0) \bmod q$ as the group secret key and computes $y = g^x \bmod p$ as the group public key.

For each member U_i in the group, the *TD* computes $x_i = f(ID_i) \bmod q$ for him, where ID_i is a public value associated with each user U_i.

Each member U_i in the group should choose a secret key $t_i \in [1, w-1]$ by himself and publish $y_i = g^{t_i} \bmod p$ as his individual public key.

Hence, each member U_i in the group should have two secret keys, x_i and t_i, and one public key y_i.

3.2 Signature Generation Phase

To produce a group oriented signature for message m, each member U_i in B should randomly choose two secret numbers $k_{iq} \in [1, q-1]$ and $k_{iw} \in [1, w-1]$ and compute a public value $r_i = g^{k_i} \bmod p$, where $k_i = k_{iq}c_q + k_{iw}c_w \bmod n$.

Upon receiving all the public values r_i's sent from the participants in B, each member $U_i \in B$ computes

$$R = \prod_{i \in B} r_i \bmod p, \text{ and}$$
$$E = h(m, R, B). \tag{2}$$

There are two ways to distribute r_i's to each member:

1. Each member U_i sends his own r_i to a predefined public bulletin board.
2. The clerk takes responsibility for doing this just as in [5].

According to R and E, each member U_i in B can generate the partial signature s_i by using his two secret keys:

$$\begin{aligned} s_i &= x_i\delta_i + k_{iq}E \bmod q \\ &= t_i + k_{iw}E \bmod w, \end{aligned} \tag{3}$$
where $\delta_i = \left(\prod_{\substack{j \in B \\ j \neq i}} \frac{0 - ID_j}{ID_i - ID_j}\right) \bmod q.$

Each member U_i in B sends his partial signature s_i to the clerk, who takes responsibility for collecting the partial signatures and for producing a valid group oriented signature.

Once these t partial signatures are collected, the clerk can compute S as

$$S = \sum_{i \in B} s_i \bmod n.$$

Thus, (m, R, S, B) is a group oriented signature formed for m.

3.3 Signature Verification Phase

For the sake of efficiency, we may skip the verification of individual signatures. Instead, (m, R, S, B) can be computed and verified directly by the clerk. Only when this verification procedure fails does the clerk have to perform verification of each partial signature to detect cheaters and to recompute the group oriented signature. Here, we shall show how to verify the signature (m, R, S, B).

First of all, the verifier (or the clerk) needs to compute the verification public key Y as

$$Y = y^{c_q}(\prod_{i \in B} y_i)^{c_w} \bmod p$$

to verify the signature.

Then, the verifier uses Y to check whether the equation below holds:

$$g^S \equiv YR^E \ (\bmod p) \tag{4}$$

If this relation holds, then the group oriented signature is valid; otherwise, it is a false signature.

Theorem 1 : If $g^S \equiv YR^E$ (mod p), then (m, R, S, B) is the group oriented signature of m.

Proof: Because $S = \sum_{i \in B} s_i$ mod n, we have

$$\begin{aligned} S &= \sum_{i \in B} s_i \bmod q \\ &= \sum_{i \in B} s_i \bmod w. \end{aligned} \tag{5}$$

According to this relation, we can rewrite Eq. (3) as

$$\begin{aligned} S &= \sum_{i \in B}(x_i\delta_i + k_{iq}E) \bmod q \\ &= \sum_{i \in B}(x_i\delta_i) + \sum_{i \in B}(k_{iq}E) \bmod q \\ &= \sum_{i \in B}(x_i\delta_i) + E\sum_{i \in B} k_{iq} \bmod q, \end{aligned} \tag{6}$$

and

$$= \sum_{i \in B} t_i + E\sum_{i \in B} k_{iw} \bmod w. \tag{7}$$

With the knowledge of (ID_i, x_i), the unique polynomial $f(x)$ can be reconstructed as

$$f(x) = \sum_{i \in B}(x_i \prod_{\substack{j \in B \\ j \neq i}} \frac{x - ID_j}{ID_i - ID_j}) \bmod q.$$

Thus, $f(0) = \sum_{i \in B}(x_i \prod_{\substack{j \in B \\ j \neq i}} \frac{0 - ID_j}{ID_i - ID_j}) \bmod q = \sum_{i \in B}(x_i\delta_i) \bmod q = x.$

Hence, Eq. (5) and (6) can be rewritten as

$$S = x + E\sum_{i\in B} k_{iq} \bmod q, \tag{8}$$

and

$$= \sum_{i\in B} t_i + E\sum_{i\in B} k_{iw} \bmod w. \tag{9}$$

Using c_q and c_w, we can obtain

$$\begin{aligned} S &= (x + E\sum_{i\in B} k_{iq})c_q + (\sum_{i\in B} t_i + E\sum_{i\in B} k_{iw})c_w \bmod n \\ &= xc_q + (\sum_{i\in B} t_i)c_w + E\sum_{i\in B}(k_{iq}c_q + k_{iw}c_w) \bmod n \\ &= xc_q + (\sum_{i\in B} t_i)c_w + E(\sum_{i\in B} k_i) \bmod n. \end{aligned}$$

It is obvious that S, Y, E and R satisfy the equation

$$\begin{aligned} g^S &\equiv g^{xc_q + \sum_{i\in B} t_i c_w + E(\sum_{i\in B} k_i) \bmod n} \pmod p \\ &\equiv y^{c_q}(g^{\sum_{i\in B} t_i})^{c_w} g^{E(\sum_{i\in B} k_i)} \pmod p \\ &\equiv y^{c_q}(\prod_{i\in B} y_i)^{c_w} g^{E(\sum_{i\in B} k_i)} \pmod p \\ &\equiv Y(g^{\sum_{i\in B} k_i})^E \pmod p \\ &\equiv Y(\prod_{i\in B} r_i)^E \pmod p \\ &\equiv YR^E \pmod p. \end{aligned}$$

Therefore, the group oriented signature (m, R, S, B) can be verified. □

To achieve traceability, our newly proposed signature scheme should not be forged. Furthermore, the incorrect partial signatures should be detected and identified if the signature is suspected forgery.

To verify the partial signature s_i, each user U_i must publish another public key $y_i' = g^{x_i} \bmod p$.

If the following congruence relation does not hold, then the false partial signature is detected:

$$g^{s_i} \equiv (y_i')^{c_q\delta_i}(y_i)^{c_w}(r_i)^E \pmod p.$$

The relation can be verified easily.

Because $s_i = x_i\delta_i c_q + t_i c_w + k_i E \bmod n$, we have

$$\begin{aligned} g^{s_i} &\equiv (g^{x_i c_q \delta_i})(g^{t_i c_w})(g^{k_i E}) \pmod p \\ &\equiv (y_i')^{c_q\delta_i}(y_i)^{c_w}(r_i)^E \pmod p. \end{aligned}$$

To reduce the storage cost of the public key y_i', we can integrate two public keys y_i and y_i' into a single public key Y_i using the Chinese Remainder Theorem.

Hence, $Y_i \equiv g^{x_i c_q} g^{t_i c_w}$ (mod p). This implies that

$$y'_i = g^{x_i} \equiv Y_i^w \ (\bmod p), \text{ and}$$
$$y_i = g^{t_i} \equiv Y_i^q \ (\bmod p).$$

This method reduces the storage cost by half. However, there is a potential drawback, which may increase the computational cost. To derive y_i and y_i' from Y_i, we need some extra computation. Fortunately, this case does not occur often. Furthermore, for an outsider, it is not necessary to publish y'_i.

4. PERFORMANCE ANALYSES AND SECURITY DISCUSSIONS

Let Te be the time complexity for computing 160 bits of exponentiation, and Tm be that for multiplication. Because all the exponents except S in our scheme never exceed 160 bits and we assume that the prime factor q is also 160 bits in Li's scheme, we may further compare the performance between these two schemes. Considering the computational cost, we need $2Te + tTm$ and $2Te$(for computing g^S) $+ Te + Tm = 3Te + Tm$ time complexity to compute Y and Eq. (3), respectively. In Li et al.'s scheme, we need $t(Te + Tm)$ and $2(Te + Tm)$ to compute the public verification value T and to verify the signature, respectively. In advance, we optimize the signature generation process by omitting the cost of verification of the individual signatures. This optimization, unfortunately, cannot be used on Li et al.'s scheme. According to the result in [10], a malicious signer can cooperate with a clerk to create a valid group oriented signature, but he can not succeed in creating a valid individual signature. Therefore, it is important to check each individual signature in Li et al.'s scheme.

Considering the storage cost, we need $O(q + w + p)$ to store both the public and the secret keys while in Li et al.'s scheme, $O(2p + q)$ is needed. According to the assumption, we need 834 bits to store the keys while Li et al.'s scheme needs 1184 bits.

According to Theorem 1, any subset B of size t can produce a valid signature for set A, and subsets with less than t participants cannot. Verification is easy for anyone who can obtain the corresponding public key.

Because we implement two types of signature in two channels, the q channel and the w channel, malicious users can forge the signature only if the signatures in both the q channel and the w channel can be forged.

The attack described in [10] may succeed in forging the q channel signatures. However, the w channel signature can avoid this attack since we apply a hash function to the signed messages m and r. This countermeasure can avoid the attack in [10]. In fact, we directly adopt the signature scheme proposed in [10] as our w channel signature; thus, our scheme can withstand the attack presented by Michels and Horster.

Furthermore, we can check the security of our scheme by replying to the questions given in [5]. We omit the detail analysis here because it is very similar to that in [5]. The reader may refer to [5] for more detailed information.

Now let us consider the case where two members U_i and U_i' conspire with each other to change the group signature (m, R, S, B) into (m, R', S', B'), where $U_i \in B$, $U_i' \notin A$, $A \subset B$,

$$R' = R,$$
$$S' = S - t_i c_w + t_i' c_w, \text{ and}$$
$$B' = B - U_i + U_i'.$$

In this case, the verifier will reject (B')'s legality without verification of each signer's partial signature.

The reason is that $E = h(m, R, B)$ includes the information about the signer group B. For signers, the signed message is $E = h(m, R, B)$. On the other hand, for the verifier, he will compute $E' = h(m, R', B')$ first and then compute $Y'R^{E'}$. Since $E \neq E'$, it is impossible that $g^{S'} \equiv Y'R^{E'} \pmod p$. Consequently, we can save the cost of partial signature verification.

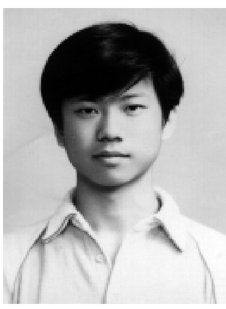
5. CONCLUSIONS

By choosing the system parameters carefully, we can build a signature system so that the order of the generator g is a composite number. Hence, we can combine the idea of traditional (t, n) threshold signature schemes with that of multisignature schemes by applying Chinese Remainder Theorem. Thus, our solution enjoys the advantages of both group orientation in a threshold digital signature scheme and of traceability in a multisignature scheme. The new scheme we have proposed is more secure and efficient than Li et al.'s scheme.

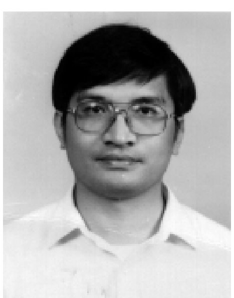
REFERENCES

1. R. L. Rivest, A. Shamir and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.
2. National Institute of Standards and Technology (NIST), "The digital signature standard, proposal and discussion," *Communications of the ACM*, Vol. 35, No. 7, 1992, pp. 36-34.
3. L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," in *IEE Proceedings of Computer and Digital Techniques*, Vol. 141, No. 5, 1994, pp. 307-313.
4. Y. Desmedt and Y. Frankel, "Shared generation of authentication and signatures," *Advances in Cryptology – CRYPTO '91*, 1991, pp. 457-469.
5. C. Li, T. Hwang and N. Lee, "Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders,"*Advances in Cryptology–Proceedings of EUROCRYPT'94*, 1994, pp.413- 419.
6. T. Hardjono and Y. Zheng, "A practical digital multisignature scheme based on discrete logarithm," *Advances in Cryptology–Proceedings of Asiacrypto '92*, 1993, pp. 16- 21.
7. L. Harn and T. Kiesler, "New scheme for digital multisignatures," *Electronics Letters*, Vol. 25, No. 15, 1989, pp. 1002-1003.
8. C. Li, T. Hwang and N. Lee, "Remark on the threshold RSA signature scheme," *Advances in Cryptology–CRYPTO'93, Lecture Notes in Computer Science*, Vol. 773, 1994,

pp. 413-420.
9. A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, No. 11, 1979, pp. 612-613.
10. M. Michels and P. Horster, "On the risk of disruption in several multiparty signature schemes," *Advances in Cryptology–Proceedings of Asiacrypto'96*, 1996, pp. 334 - 345.



Wei-Bin Lee (李維斌) received his B.S. degree from the Department of Information and Computer Engineering, Chung-Yuan Christian University, Chungli, Taiwan, in 1991 and his M.S. degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan in 1993. He completed his Ph.D. degree in May, 1997, at National Chung Cheng University. Now, he is an assistant professor in the Department of Information Engineering at Feng Chia University. His research interests currently include cryptography, computer communication and data security.



Chin-Chen Chang (張真誠) was born in Taichung, Taiwan, Republic of China, on November 12, 1954. He received his B.S. degree in applied mathematics in 1977 and his M.S. degree in computer and decision sciences in 1979 from National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. degree in computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. During the academic years 1980-83, he was on the faculty of the Department of Computer Engineering at National Chiao Tung University.

From 1983 to 1989, he was on the faculty of the Institue of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of and a professor in the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the Dean of the College of Engineering at National Chung Cheng University. Since August 1995, he has been the Dean of Academic Affairs at National Chung Cheng University.

In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, coding theory, and data structures.

Dr. Chang is a senior member of IEEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China.