AMC 8869
10 April 2004 Disk used
ARTICLE IN PRESS
No. of Pages 10, DTD = 4.3.1

Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®

ELSEVIER Applied Mathematics and Computation xxx (2004) xxx–xxx

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

An improvement on the Lin–Wu (t, n) threshold verifiable multi-secret sharing scheme ☆

Ting-Yi Chang [a], Min-Shiang Hwang [b,*], Wei-Pang Yang [a]

[a] *Department of Computer and Information Science, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, ROC*

[b] *Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, ROC*

Abstract

Lin and Wu [IEE Proc. Comput. Digit. Tech. 146 (1999) 264] have proposed an efficient (t, n) threshold verifiable multi-secret sharing (VMSS) scheme based on the factorization problem and the discrete logarithm modulo a large composite problem. In their scheme, the dealer can arbitrarily give any set of multiple secrets to be shared, and only one reusable secret shadow is to be kept by every participant. On the other hand, they have claimed that their scheme can provide an efficient solution to the cheating problems between the dealer and any participant. However, He and Wu [IEE Proc. Comput. Digit. Tech. 148 (2001) 139] have shown that Lin and Wu's scheme is in fact insecure against a cheating participant. In this paper, we shall try to improve the security of Lin and Wu's scheme while providing more efficient performance than other VMSS schemes in terms of computational complexity.

Keywords: Cryptosystem; Cheater identification; Threshold scheme; Verifiable secret sharing

☆ This research was partially supported by the National Science Council, Taiwan, ROC, under contract no. NSC90-2213-E-324-004.

* Corresponding author.

E-mail addresses: mshwang@nchu.edu.tw (M.-S. Hwang), wpyang@cis.nctu.edu.tw (W.-P. Yang).

0096-3003/$ - see front matter © 2004 Published by Elsevier Inc.
doi:10.1016/j.amc.2004.01.029

1. Introduction

The first (t, n) threshold secret sharing schemes, based on the Lagrange interpolating polynomial and linear project geometry, were proposed by Shamir [20] and Blakley [2], respectively. In their schemes, the dealer first splits the secret into n different pieces, called shadows, which are given to the participants over a secret channel. At least t or more participants can use their shadows to collaboratively reconstruct the secret, but only $t-1$ or fewer participants will not be enough. However, there are several common drawbacks in both secret-sharing schemes [2,20] as follows:

(1) Only one secret can be shared during one secret sharing process [11].
(2) Once the secret has been reconstructed, it is required that the dealer redistributes a fresh shadow over a secret channel to every participant [16].
(3) A dishonest dealer may distribute a fake shadow to a certain participant, and then that participant would subsequently never obtain the true secret [8].
(4) A malicious participant may provide a fake shadow to other participants, which makes the malicious participant the only one who gets to reconstruct the true secret [23].

To overcome the drawback in (1), some efficient (t, n) multi-secret sharing schemes have been proposed [7,10,11] to share multiple secrets. To deal with the drawback in (2), Jakson et al. [16] have further classified multi-secret sharing scheme into two types: one-time-use scheme and multi-use scheme. The difference between one-time-use scheme and multi-use scheme is that the shadow kept by each participant in a multi-use scheme is reusable after secret reconstruction while the shadow kept by each participant in a one-time-use scheme is not. To redistribute shadows is a very costly process with respect to both time and resources. However, both types of schemes still have the common drawbacks in (3) and (4).

To do away with the drawback in (3), Chor et al. [8] have proposed a verifiable secret sharing (VSS) scheme to detect cheating by a dishonest dealer. In Chor et al.'s VSS scheme [8], every participant can verify the validity of his/her own shadow distributed by the dealer, which allows the honest participants to ensure that the secret to be reconstructed is unique. However, the drawback in (4) still exists in their scheme. Years ago, Stadler [21] provided a solution to the problems in (3) and (4). Stadler's VSS scheme [21] is not only robust against the cheating by the dealer [9] but also against the cheating by any participant [3,4,17,22,23]. Nevertheless, both VSS schemes can only deal with one secret in one secret sharing process.

Taking all the above problems into consideration, Harn [10] has proposed a (t, n) threshold verifiable multi-secret sharing (VMSS) scheme which can detect

AMC 8869
10 April 2004 Disk used
ARTICLE IN PRESS
No. of Pages 10, DTD = 4.3.1

both the cheating by the dealer and that by any participant. In Harn's scheme [10], every participant keeps only one reusable shadow (which makes it a multi-use scheme) distributed by the dealer. When reconstructing a secret, each participant first computes a subshadow from his/her own shadow. If t or more subshadows are released, the secret can be reconstructed. The other multiple secrets can be reconstructed the same way. However, Lin and Wu [18] have pointed out that Harn's scheme still suffers from the problems as follows:

- Every participant should perform $n!/((n-t)! \cdot t!)$ module exponentiations to verify the validity of his/her own shadow against the cheating by the dealer.
- The subshadows generated by the participants are not implicitly verifiable against the cheating by a participant. In the secret reconstruction process, every participant runs an interactive verification protocol with each of the other cooperators to verify that their released subshadows are valid.
- Only predetermined or computed secrets can be shared. This restricts the dealer from dynamically adding a new secret to be shared among those n participants.

Chen et al. [6] have proposed an alternative (t, n) VSS scheme to avoid the disadvantages in Harn's scheme [10]. However, Lin and Wu [18] have also pointed out that Chen et al.'s scheme is inefficient because the dealer has to record all participants' the shadows and take $2n$ modulo exponentiations to compute an n-dimensional verification vector for each shard secret. This n-dimensional verification vector is used to prevent any cheating by the participants in the secret reconstruction process. In order to avoid the disadvantages in Harn's scheme [10] and to reduce the computational complexity in Chen et al.'s scheme [6], Lin and Wu [18] have further proposed a (t, n) threshold VMSS scheme based on the intractability of factorization and the problem of discrete logarithm module a composite [1]. However, He and Wu [12] have indicated that a malicious participant can provide a fake subshadow to cheat other honest participants. Hence, it would turn out that only the malicious participant could reconstruct the secret.

With this paper, we shall improve Lin and Wu's scheme [18] and prevent the cheating by any malicious participant. The improved VSS scheme will still maintain the advantages of Harn's [10] and Chen et al.'s schemes [6] while reducing the computational complexity. The improved scheme will have the following features [18]:

1. The dealer can arbitrarily give any set of multiple secrets for sharing, and only one shadow, which is reusable, should be kept by each participant. Furthermore, the number of public values published by the dealer for reconstructing every secret without cheating participants can be further minimized.

AMC 8869
10 April 2004 Disk used
ARTICLE IN PRESS
No. of Pages 10, DTD = 4.3.1

2. Every participant can detect any cheating by the dealer and verify his/her own shadow.
3. Every participant can detect the cheating by any other participant by using a non-interactive verification protocol and verify his/her subshadow.

The remainder of our paper is organized as follows. In Section 2, we shall propose our improved (t, n) threshold VMSS scheme, which is an improvement on Lin and Wu's scheme. In Section 3, we shall mount several possible attacks to demonstrate the security of our improved (t, n) VMSS scheme. In Section 4, we shall compare the performance of our improved (t, n) VMSS scheme with that of Chen et al.'s scheme. Finally, our conclusion will be in Section 5.

2. Improved (t, n) threshold VMSS scheme

In this section, we shall propose a new method that is an improvement on Lin and Wu's (t, n) VMSS scheme [18]. Our new scheme can withstand He and Wu's attack (see [12,18] for more details). Our improved (t, n) VMSS scheme is also comprised of four phases: (1) initialization stage, (2) shadow generation and verification stage, (3) credit ticket generation stage, and (4) subshadow verification and secret reconstruction stage. The details of four stages are as follows:

2.1. Initialization stage

The dealer (denoted as U_{D}) first creates a public notice board (NB) which is used for storing necessary public parameters. The participants can access those parameters on the NB. The contents on the board can only be modified or updated by U_{D}. The parameters are defined by U_{D} as follows: N denotes the product of two large primes p and q, where $p = 2p' + 1$ and $q = 2q' + 1$, with themselves prime; R is the product of p' and q'; g is denotes a generator with order R in Z_N; e and d separately denote the pubic and private keys in the RSA algorithm [5,14,19], where $e \cdot d = 1 \bmod \phi(n)$. After generating these parameters, U_{D} puts $\{N, g, e\}$ on the NB and keeps $\{R, d\}$ secret.

2.2. Shadow generation and verification stage

Let $G = \{U_1, U_2, \ldots, U_n\}$ be a group of n participants and $S = \{S_1, S_2, \ldots, S_m\}$ be a set of m secrets. Every U_i has her/his identity ID_i $(i = 1, 2, \ldots, n)$. U_{D} performs the following steps:

Step 1. Randomly generate a polynomial $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1} \bmod R$, where each $a_k \in Z_R$, and compute a check vector

$V = [V_0, V_1, \ldots, V_{k-1}]$ for each coefficient a_k as

$$V_k = g^{a_k} \bmod N \quad \text{for } k = 0, 1, \ldots, (t-1), \tag{1}$$

and put V on the NB.

Step 2. Compute a secret shadow x_i for every $U_i \in G$ as

$$x_i = f(\mathrm{ID}_i) \cdot p_i^{-1} \bmod R, \tag{2}$$

where

$$p_i = \prod_{U_k \in G, U_k \neq U_i} (\mathrm{ID}_i - \mathrm{ID}_k) \bmod R$$

and compute the associated $y_i = g^{x_i} \bmod N$ as this U_i's public key to be put on the NB.

Step 3. Distribute $\{y_i = g^{p_i} \bmod N, x_i\}$ to every $U_i \in G$ over a secret channel.

When every $U_i \in G$ receives the secret shadow x_i, he/she can check the following equation to verify the validity of x_i:

$$(g^{p_i})^{x_i} = \prod_{k=0}^{t-1} (V_k)^{(\mathrm{ID}_i)^k} \bmod N. \tag{3}$$

If Eq. (3) does not hold, the secret shadow x_i distributed by U_D is not valid.

2.3. Credit ticket generation stage

In this phase, U_D performs the following steps to compute m credit tickets $C_1, C_2, \ldots, C_m$ for each secret $S_1, S_2, \ldots, S_m \in S$.

Step 1. Randomly choose m distinct integers $r_1, r_2, \ldots, r_m \in Z_R$ for each secret $S_1, S_2, \ldots, S_m \in S$.

Step 2. Compute a credible ticket C_j and a value h_j as

$$C_j = g^{r_j \cdot d} \bmod N \tag{4}$$

and

$$h_j = (g^{a_0 \cdot r_j \cdot d} \bmod N) \oplus S_j \quad \text{for } j = 1, 2, \ldots, m. \tag{5}$$

Then, the 3-tuple $\{r_j, C_j, h_j\}$ is put on the NB.

In addition, if U_D wants to add a new secret S_new for sharing, he/she only needs to generate a new 3-tuple $\{r_\mathrm{new}, C_\mathrm{new}, h_\mathrm{new}\}$ for S_new and put it on the NB without interfering with the results generated in the previous phases.

AMC 8869 ARTICLE IN PRESS No. of Pages 10, DTD = 4.3.1
10 April 2004 Disk used

2.4. Subshadow verification and secret reconstruction stage

Let W ($|W| = t \leqslant n$) be any subset of t participants in G. Without loss of generality, assume that t participants $U_i \in W$ cooperate to reconstruct a secret $S_j \in S$. Every $U_i \in W$ obtains the 3-tuple $\{r_j, C_j, h_j\}$ from the NB and uses his/her secret shadow x_i to compute a subshadow A_{ij} as

$$A_{ij} = (C_j)^{x_i} \bmod N. \tag{6}$$

Then, U_i releases A_{ij} to the other cooperators in W. Any other cooperator in W obtains U_i's public key y_i form the NB to verify the validity of A_{ij} as

$$(A_{ij})^e = (y_i)^{r_j} \bmod N. \tag{7}$$

If Eq. (7) does not hold, then they can stop this phase and announce that cheating by U_i has been identified. If all A_{ij}'s released by the t participants in W are valid, every participant in W can reconstruct S_j as

$$S_j = h_j \oplus \left(\prod_{U_i \in W} (A_{ij})^{\Delta_i} \bmod N \right), \tag{8}$$

where

$$\Delta_i = \left(\prod_{U_k \in G, U_k \neq U_i} - \mathrm{ID}_k \right) \cdot \left(\prod_{U_k \in G, U_k \notin W} (\mathrm{ID}_i - \mathrm{ID}_k) \right).$$

Then, all the secrets $S_1, S_2, \ldots, S_m \in S$ can be reconstruct by performing this phase repetitively.

In the rest of this section, we shall show the correctness of verifying the secret shadow distributed by U_D in Eq. (3), verifying the subshadow released by any participant in Eq. (7), and the secret reconstruction in Eq. (8).

In the shadow generation and verification stage, any participant $U_i \in G$ can verify the secret shadow x_i distributed by U_D in Eq. (3) as follows. According to Eqs. (1) and (2), we can rewrite Eq. (3) as

$$\begin{aligned}
(g^{p_i})^{x_i} &= g^{p_i \cdot f(\mathrm{ID}_i) \cdot p_i^{-1}} \bmod N \\
&= g^{f(\mathrm{ID}_i)} \bmod N \\
&= g^{\sum_{k=0}^{t-1} a_k \cdot (\mathrm{ID}_i)^k} \bmod N \\
&= \prod_{k=0}^{t-1} (V_k)^{(\mathrm{ID}_i)^k} \bmod N.
\end{aligned}$$

In the subshadow verification and secret reconstruction stage, any cooperator can verify the subshadow released by any $U_i \in W$ in Eq. (7) as follows.

AMC 8869
10 April 2004 Disk used
ARTICLE IN PRESS
No. of Pages 10, DTD = 4.3.1

Assume that U_i is an honest participant who uses his/her shadow x_i to compute A_{ij} in Eq. (6). According to Eqs. (4) and (6), we can rewrite Eq. (7) as

$$\begin{aligned}(A_{ij})^e &= (C_j^{x_i})^e \bmod N \\ &= (g^{r_j \cdot d \cdot x_i})^e \bmod N \\ &= g^{r_j \cdot x_i} \bmod N \\ &= y_i^{r_j} \bmod N.\end{aligned}$$

In the subshadow verification and secret reconstruction stage, every participant in W can reconstruct $S_i \in S$ in Eq. (8) as follows. Assume that all the A_{ij}'s released by the t participants in W are valid. According to Eq. (5), we can rewrite Eq. (8) as

$$\begin{aligned}S_j &= h_j \oplus \left(\prod_{U_i \in W} (A_{ij})^{\Delta_i} \bmod N \right) \\ &= (g^{a_0 \cdot r_j \cdot d} \bmod N) \oplus S_j \oplus \left(\prod_{U_i \in W} (A_{ij})^{\Delta_i} \bmod N \right) \\ &= (g^{a_0 \cdot r_j \cdot d} \bmod N) \oplus S_j \oplus \left(\prod_{U_i \in W} (C_j)^{x_i \cdot \Delta_i} \bmod N \right) \\ &= (g^{a_0 \cdot r_j \cdot d} \bmod N) \oplus S_j \oplus (C_j)^{f(0)} \bmod N \\ &= S_j.\end{aligned}$$

3. Security analysis

The security of our proposed scheme is the same as that of Lin and Wu's scheme [18], which is based on factorization and discrete logarithm modulo a composite problem. In the rest of this section, some possible attacks will be raised and fought against to demonstrate the security of our scheme.

Attack 1. An adversary tries to reveal the participants' secret shadows x_i's from the known information.

(a) Known the equation $y_i = g^{x_i} \bmod N$ and U_i's public key y_i $(i = 1, 2, \ldots, n)$ and the parameters g, N: It is as difficult as breaking the discrete logarithm module a composite (DLMC) problem [1].

(b) Known the equation $A_{ij} = (C_j)^{x_i} = g^{r_j \cdot d \cdot x_i} \bmod N$ and A_{ij}, C_j $(i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m)$ and the parameter N: As with Attack 1(a), the adversary should face the difficulty of the DLMC problem.

AMC 8869
10 April 2004 Disk used
ARTICLE IN PRESS
No. of Pages 10, DTD = 4.3.1

Attack 2. A malicious participant who has obtained some previously recovered secrets tries to reveal any remaining secret in S without the assistance of the other $t-1$ cooperators.

Known the equation $h_j = (g^{a_0 \cdot r_j \cdot d} \bmod N) \oplus S_j$ and the check value $V_0 = g^{a_0} \bmod N$ and the 3-truple $\{r_j, C_j, h_j\}$ $(j = 1, 2, \ldots, m)$: Assume that the malicious participant has recovered the secrets $S_a \in S$ and $S_b \in S$ with the other $t-1$ cooperators; in other words, he/she has the knowledge of the values $g^{a_0 \cdot r_a \cdot d} \bmod N$ and $g^{a_0 \cdot r_b \cdot d} \bmod N$. In order to disclose another secret $S_c \in S$ in Eq. (5), the malicious participant has to first find out the value $g^{a_0 \cdot d} \bmod N$ and multiply the exponent r_c by it. He/she has to calculate the r_ath root of $g^{a_0 \cdot r_a \cdot d} \bmod N$ or the r_bth root of $g^{a_0 \cdot r_b \cdot d} \bmod N$ to obtain the value $g^{a_0 \cdot d} \bmod N$. However, the difficulty of extracting the r_ath root of $g^{a_0 \cdot r_a \cdot d} \bmod N$ or the r_bth root of $g^{a_0 \cdot r_b \cdot d} \bmod N$ is equivalent to that of breaking the factorization (FAC) problem [1,15] in the RSA scheme [19]. On the other hand, if the malicious participant finds $C_c = C_a \cdot C_b \bmod N$, he/she can easily derive $t-1$ verified A_{ic}'s from A_{ia}'s and A_{ib}'s as

$$\begin{aligned} A_{ic} &= A_{ia} \cdot A_{ib} \bmod N \\ &= (C_a)^{x_i} \cdot (C_b)^{x_i} \bmod N \\ &= g^{r_a \cdot d \cdot x_i} \cdot g^{r_b \cdot d \cdot x_i} \bmod N \\ &= (g^{d \cdot x_i \cdot (r_a + r_b)} \bmod N). \end{aligned}$$

However, the integers r_j's are randomly chosen by U_{D} for computing distinct C_j's. The malicious participant still cannot succeed in this attack. (For example, U_{D} chooses r_j's as 3^j.)

Attack 3. The dealer U_{D} tries to distribute a fake shadow x_i' to cheat participant U_i without being detected in Eq. (2).

The check vector $V = [V_0, V_1, \ldots, V_{k-1}]$ in Eq. (1) has been published by U_{D} on the NB, and therefore $f(x)$ is unchangeable already. For this reason, any fake shadow $x_i' \neq f(\mathrm{ID}_i) \cdot p^{i-1} \bmod R$ cannot pass the shadow verification in Eq. (3).

Attack 4. A dishonest participant U_i in W tries to release a fake subshadow A_{ij}' to cheat the other cooperators in W without being detected in Eq. (7). The dishonest participant U_i should first find out U_{D}'s private key d. Then, he/she has to modify his/her public key y_i or r_j on the NB to pass Eq. (7). However, retrieving d from $\{N, e\}$ is as difficult as breaking the RSA scheme [13,19]. Furthermore, the contents of the NB can only be modified or updated by U_{D}. Thus, the dishonest participant U_i cannot release a fake A_{ij}' subshadow to pass Eq. (7).

AMC 8869 ARTICLE IN PRESS No. of Pages 10, DTD = 4.3.1
10 April 2004 Disk used

4. Performance analysis

In Lin and Wu's paper, they have claimed that their scheme was more efficient than Harn's scheme [10] and Chen et al.'s scheme [6]. However, He and Wu [12] showed that a malicious participant in Lin and Wu's scheme could provide a fake subshadow to deceive other honest participants. In Section 3, we have demonstrated that our improved scheme can withstand such an attack. Our improved scheme is even more efficient than Harn's scheme [10] and Chen et al.'s scheme because each participant has to run an interactive verification protocol with each and every one of the other cooperators to verify their released subshadows in Harn's scheme. That is inefficient. Here, we analyze the number of modular exponentiations ($T_{\exp}$) and compare ours with that of Chen et al.'s scheme.

In Table 1, though the number of modular exponentiations employed to guard against cheating by U_i (done by U_i) in our scheme is greater than that in Chen et al.'s scheme [6], our scheme outperforms Chen et al.'s scheme in the number of modular exponentiations against cheating by U_i (done by U_D). Moreover, $2n$ modular exponentiations are required by Chen et al.'s scheme to guard against cheating by U_i (done by U_D), which increases the number of participants in the system. Generally speaking, our scheme has a more efficient overall performance than Chen et al.'s scheme. In addition, the number of public parameters published by the dealer for reconstructing a secret is only 3 in our scheme. In contrast, Chen et al.'s scheme need as many as $n+2$. For the same reason, the number of public parameters increases the number of participants in the system in Chen et al.'s scheme.

5. Conclusion

In this article, we have proposed an improved (t,n) VMSS scheme which is a modified version of Lin and Wu's scheme. Our scheme can successfully withstand He and Wu's attack, and our security is based on factorization and discrete logarithm modulo a composite problem. Though modifications have been made, the original advantages are maintained.

Table 1
Comparison between our scheme and Chen et al.'s scheme

	Chen et al.'s scheme	Our scheme
Against cheating by U_D (done by U_i)	$2t\,T_{\exp}$	$2t\,T_{\exp}$
Against cheating by U_i (done by U_i)	$(t-1)\,T_{\exp}$	$(t-1)2\,T_{\exp}$
Against cheating by U_i (done by U_D)	$2n\,T_{\exp}$	$2T_{\exp}$
Public values published by U_D for reconstructing a secret	$n+2$	3

References

[1] L. Adleman, K. McCurley, Open problems in number theoretic complexity, 2', Lecture Notes Comput. Sci. 877 (1994) 291–322.

[2] G. Blakley, Safeguarding cryptographic keys, in: Proc. AFIPS 1979 Natl. Conf., New York, 1979, pp. 313–317.

[3] M. Carpentieri, A perfect threshold secret sharing scheme to identify cheaters, Designs, Codes and Cryptography 5 (3) (1995) 183–187.

[4] C.C. Chang, R.J. Hwang, Efficient cheater identification method for threshold schemes, IEE Proc. Comput. Digit. Tech. 144 (1) (1997) 23–27.

[5] C.-C. Chang, M.-S. Hwang, Parallel computation of the generating keys for RSA cryptosystems, IEE Electron. Lett. 32 (15) (1996) 1365–1366.

[6] L. Chen, D. Gollmann, C.J. Mitchell, P. Wild, Secret sharing with reusable polynomials, in: Proceedings of ACISP '97, 1997, pp. 183–193.

[7] H.-Y. Chien, J.-K. Jan, Y.-M. Tseng, A practical (t, n) multi-secret sharing scheme, IEICE Trans. Fundamentals E83-A (12) (2000) 2762–2765.

[8] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, in: Proc. 26th IEEE Symp. FOCS, 1985, pp. 251–260.

[9] R. Gennaro, S. Micali, Verifable secret sharing as secure computation, in: Advances in Cryptology, EUROCRYPT'95, Lecture Notes in Computer Science, pp. 168–182, 1995.

[10] L. Harn, Efficient sharing (broadcasting) of multiple secret, IEE Proc. Comput. Digit. Tech. 142 (3) (1995) 237–240.

[11] J. He, E. Dawson, Multistage secret sharing based on one-way function, Electron. Lett. 30 (19) (1994) 1591–1592.

[12] W.H. He, T.S. Wu, Comment on Lin–Wu (t, n)-threshold verifiable multisecret sharing scheme, IEE Proc. Comput. Digit. Tech. 148 (3) (2001) 139.

[13] M.-S. Hwang, C.-C. Lee, Y.-C. Lai, Traceability on RSA-based partially signature with low computation, Appl. Math. Comput. (2002).

[14] M.-S. Hwang, I.-C. Lin, K.-F. Hwang, Cryptanalysis of the batch verifying multiple RSA digital signatures, Informatica 11 (1) (2000) 15–19.

[15] M.-S. Hwang, C.-C. Yang, S.-F. Tzeng, Improved digital signature scheme based on factoring and discrete logarithms, J. Discrete Math. Sci. Cryptography, in press.

[16] W.-A. Jackson, K.M. Martin, C.M. O'Keefe, On sharing many secrets, Asiacrypt'94, 1994, pp. 42–54.

[17] E.D. Karnin, J.W. Greene, M.E. Hellman, On secret sharing systems, IEEE Trans. Inform. Theory IT-29 (1) (1983) 35–41.

[18] T.Y. Lin, T.C. Wu, (t, n) threshold verifiable multisecret sharing scheme based on factorisation intractability and discrete logarithm modulo a composite problems, IEE Proc. Comput. Digit. Tech. 146 (5) (1999) 264–268.

[19] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Commun. ACM 21 (February) (1998) 120–126.

[20] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613.

[21] M. Stadler, Publicly verifiable secret sharing, in: Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Science, 1996, pp. 190–199.

[22] K.J. Tan, H.W. Zhu, S.J. Gu, Cheater identification in (t, n) threshold scheme, Comput. Commun. 22 (8) (1999) 762–765.

[23] M. Tompa, H. Woll, How to share a secret with cheaters, J. Cryptol. 1 (1988) 133–138.