A Multiple Secret Sharing Scheme based on Matrix Projection

Kai Wang, Xukai Zou and Yan Sui
Department of Computer and Information Science
Indiana University Purdue University
Indianapolis, IN 46202, USA
{*wangk,xkzou,ysui*}*@cs.iupui.edu*

***Abstract*—In [3], Bai et al. have proposed a multiple secret sharing scheme based on matrix projection. It is an elegant scheme with several advantages such as small share size and dynamic to secret changes. However, one of its disadvantages is that the secrets are organized in a square matrix and hence the number of secrets must be a square. So there is often a necessity to stuff dummy secrets into the secret matrix if the number of secrets is not a square. We present a new scheme based on matrix projection method that can share any number of secrets and make full use of every element of the secret matrix. The proposed scheme is as secure as Bai's scheme. Besides, the proposed scheme can also take advantage of the proactive characteristic of the Matrix Projection Method to update shares periodically to improve security. Our scheme increases the potential range of the threshold. The increment of the threshold range is even more when we are using the proactive feature of the scheme. It also further reduces the share size to a constant (equal to that of a single secret). As with Bai's scheme, our scheme is partially verifiable based on the properties of the projection matrix. The paper also summarizes and classifies typical existing secret sharing schemes.**

***Keywords*-secret sharing; matrix projection;**

I. Introduction

Secret sharing schemes have many interesting applications in the real world. In 1979, Shamir [27] and Blakley [4] independently devised secret sharing schemes for the application of key distribution. Informally, a secret sharing scheme allows a dealer to protect a secret among a set of w participants with each participant holding one share. The *access structure* of the scheme is the set of subsets of the participants that are authorized to reconstruct the secret using their shares. A special case called (t, w)-threshold access structure consists of subsets containing at least t participants. In this case, any t out of w participants can recover the secret.

A secret sharing scheme is called *perfect* if any subset in the access structure can recover the secret while any unauthorized subset cannot gain any information (in the information theoretic sense) about the secret. Shamir's (t, w)-threshold scheme is a perfect secret sharing scheme based on Lagrange interpolating polynomial. Blakley's (t, w)-threshold scheme is not perfect because each participant knows the secret lies on the hyperplane determined by his/her share.

There are situations in which many secrets need to be shared, possibly each with respect to a different access structure. As an example, consider the following situation, proposed in [28]. There is a missile battery and not all of the missiles have the same launch code. The problem is to devise a scheme which will allow any one, or any selected subset, of the launch enable codes to be activated in this scheme. The scheme needs an algorithm such that the same pieces of private information could be used to recover different secrets. This problem could be trivially solved by realizing different secret sharing schemes, one for each of the launch enable codes. This solution is inefficient since each participant should hold multiple shares.

Another scenario in which the sharing of multiple secrets is important was considered by Franklin and Yung [10]. They investigated the communication complexity of unconditionally secure multi-party computation, and its relations with various fault-tolerant models. They presented a general technique for parallelizing non-cryptographic computation protocols at a small cost in fault-tolerance. Their technique replaces polynomial based (single) secret sharing with a technique allowing multiple secrets to be hidden in a single polynomial. The technique applies to all of the protocols for secure computation which use polynomial based threshold schemes and applies to all fault-tolerant models.

Considering the potential application of multiple secret sharing, Bai [3] introduced a multiple secret sharing scheme based on matrix projection method for sharing a secret square matrix. The scheme is a threshold scheme with the threshold range related to the number of secrets. So either all the secrets can be recovered when given an authorized subset of shares or no secret can be recovered when only given an unauthorized subset of shares. One of the characteristics of the scheme is that the number of secrets is a square since the secrets are organized into a square matrix. The natural question to ask is how to implement secret sharing of arbitrary number of secrets systematically. We can obviously use Bai's scheme and stuff dummy secrets into the secret matrix if necessary. However, the participants have to keep track of what elements of the secret matrix are target secrets to share. This is an additional burden.

In this paper, we propose a scheme to share arbitrary number of secrets based on matrix projection method. The

0730-3157/09 $25.00 © 2009 IEEE
DOI 10.1109/COMPSAC.2009.60

Table I
PERFECT AND NON-PERFECT SECRET SHARING SCHEMES

Perfect	Non-perfect
Shamir; Benaloh; Feldman; Pedersen; Herzberg; He	Brickell; Ghodosi; Mignotte; Asmuth-Bloom; Blakley(ramp); Pang(ramp); Iftene; Bai(ramp); Franklin(ramp); Ours(MP,ramp)

Table II
THRESHOLD AND NON-THRESHOLD SECRET SHARING SCHEMES

Threshold	Non-threshold
Shamir; Blakley; Mignotte; Martin; Feldman; Pedersen; Ingemarsson; Steinfelda; Herzberg; Pang; He; Asmuth-Bloom; Bai; Ours(MP)	Brickell; Benaloh; Ghodosi; Iftene; Jackson

scheme has the desirable properties that we do not have to stuff dummy entries into the secret matrix and the search space for each secret is not reduced compared to Bai's scheme so it is as secure. The scheme can also take advantage of the proactive characteristic of the Matrix Projection Method to periodically update shares without modifying the secret. Our scheme also increases the potential range of the threshold and reduces the share size. So it has more application areas and performance advantages.

II. CLASSIFICATIONS AND PROPERTIES OF SECRET SHARING SCHEMES

The literature has seen many secret sharing schemes since Shamir [27] and Blakley [4] proposed their secret sharing primitives independently in 1979. Here we list some representative schemes such as Feldman [9], Pedersen [26], Herzberg [16], He [14], Mignotte [24], Asmuth-Bloom [1], Brickell [6], Ghodosi [11], Pang [25], Iftene [17], Ingemarsson [18], Martin [23], Steinfelda [29], [30].

Secret sharing schemes can be categorized according to whether they are perfect. Table I categorizes the secret sharing schemes into two classes according to this criterion.

Secret sharing schemes can be classified according to the access structures they could be used for. Table II categorizes the schemes we have listed based on whether they are threshold or non-threshold schemes.

Secret sharing schemes can be classified according to whether they can share only one secret or can share multiple secrets, as shown in Table III.

We also categorize the secret sharing schemes based on the techniques they use, as shown in Table IV.

Secret sharing schemes can have many properties. It is important to discuss their dynamics such as whether it is easy to change the secret(s), whether it is easy to change the access structure. Even if we don't need to change the secret(s) or the access structure, we may need to periodically change the shares at different time rounds so that the shares from different time rounds cannot be pooled together to recover the secrets. This is called the proactive feature of a secret sharing scheme and it can improve the overall security of a secret sharing scheme. Another property is the verifiable feature. We can verify whether the dealer or the participants have followed the sharing protocols honestly when the secret sharing scheme is verifiable.

Table III
SINGLE AND MULTI-SECRET SHARING SCHEMES

Single secret sharing	Multi-secret sharing
Shamir; Blakley; Mignotte; Asmuth-Bloom; Brickell; Ghodosi; Iftene; Benaloh; Feldman; Pedersen; Ingemarsson; Jackson; Martin; Steinfelda; Herzberg	Chien; Yang; Shao; Franklin; Pang; He; Bai; Ours(MP)

Table IV
UNDERLYING TECHNIQUES OF SECRET SHARING SCHEMES

Polynomial based	Shamir; Ghodosi; Feldman; Pedersen; Herzberg; Yang; Pang; Franklin; He
Systematic block codes based	Chien
Vector space based	Blakley
CRT based	Mignotte; Asmuth-Bloom; Iftene
Matrix projection based	Bai; Ours(MP)
Circuit based	Benaloh

We summarize the dynamics and verifiability of secret sharing schemes, as shown in Table V. Regarding the accommodation of changing access structures, some schemes are "easy to add user". This means that the dealer can easily compute a new share and securely give it to the new user without affecting existing users' shares. Most of these kind of schemes are polynomial based since a new share is just a new point evaluated on the polynomial.

III. REVIEW OF TYPICAL MULTIPLE SECRET SHARING SCHEMES AND BAI'S SCHEME

Blundo [5] laid foundations for a general theory of multi-secret sharing schemes by using the entropy approach. They considered the case in which m secrets are shared among a group of participants on a single access structure in such a way that 1) any qualified subset of participants can reconstruct all the secrets, 2) any non-qualified subset has absolutely no information on any secret, and 3) any non-qualified subset knowing the values of a number of secrets might determine some (possibly no) information on other secrets. They proved lower bounds on the size of information held by each participant in any multi-secret sharing scheme and provided an optimal protocol for multi-secret sharing schemes on a particular access structure.

Jackson, Martin, and O'Keefe [20] considered the problem where participants can reconstruct more than one secret using the information they hold. In particular, they considered the situation in which there is a secret associated with each set $K \in \mathcal{P}$, where $|K| = k$. This secret can

Table V
DYNAMICS ACCOMMODATION CAPABILITY AND VERIFIABILITY

Schemes	Change Secrets?	Change Access Structure?	Proac-?tive?	Verifiable?
Shamir	rerun	easy to add user	No	No
Blakley	rerun	easy to add user	No	No
Mignotte	rerun	rerun	No	No
Asmuth-Bloom	rerun	rerun	No	No
Brickell	rerun	rerun	No	No
Ghodosi	rerun	rerun	No	No
Iftene (compartment)	rerun	rerun	No	No
Iftene (weighted)	rerun	rerun	No	No
Benaloh	rerun	rerun	No	No
Feldman	rerun	easy to add user	No	Yes
Pedersen	rerun	easy to add user	No	Yes
Ingemarsson	easy	easy	No	No
Jackson	rerun	rerun	No	No
Martin	rerun	easy	No	No
Steinfelda	rerun	easy	No	No
Herzberg	rerun	easy to add user	Yes	No
Pang	easy	rerun	Yes	Yes
Franklin	rerun	rerun	No	No
He(multi-stage)	rerun	easy to add user	Yes	No
He(multi-secret)	rerun	easy to add user	Yes	No
Bai	easy	easy to add user	Yes	Partial
Ours(MP)	easy	easy to add user	Yes	Partial

be reconstructed by any $t(t \leq k)$ participants of K. They proved bounds on the size of information that participants must hold in order to ensure that up to w participants ($0 \leq w \leq n-k+t-1$) cannot obtain any information about a secret they are not associated with. In [21] the authors provided an optimal scheme, with respect to the information given to each participant, for some values of the parameters t and w.

In [14], He and Dawson pointed out one drawback of the one-time-use secret sharing scheme, that is, the secret share of each participant can be used in only one sharing session. Once a qualified group of participants reconstructs the secret by pooling their shares, both the secret and the associated shares become known to everyone in the group. Several multi-secret sharing schemes were proposed [14], [12], [13], [15]. In such schemes, each participant only needs to keep one share that can be used in several sharing sessions without being refreshed. The reconstruction of a secret will not compromise the secrecy of the remaining sharing sessions. However, these schemes can share only one secret in one sharing session.

In [7], Chien et al. proposed a multiple secret sharing scheme based on systematic block codes in which multiple secrets can be shared in each sharing session. In [8], [22], Yang et al. proposed two different implementations of the scheme [7] based on Shamir's secret sharing scheme. These schemes are not verifiable, that is, the schemes do not provide a way to check whether the dealer or every participant is honest. In [19], Shao et al. proposed a verifiable multi-secret sharing scheme in which the participants' shares can be negotiated over a public channel but cannot be reused. In [25], Pang et al. proposed a verifiable (t, n) multiple secret sharing scheme in which the shares can be reused, multiple secrets can be shared in each sharing session, the shares can be negotiated over a public channel and it is easy to check the dealer and every participant's honesty.

A. *Review of Bai's Scheme*

We briefly describe Bai's multiple secret sharing scheme based Matrix Projection Method [3].

Assume all matrix elements and operations are in the finite field Z_p where p is a large prime. Let A be an $m \times k$ matrix of rank k ($m \geq k > 0$), and

$$\mathbb{S} = A(A'A)^{-1}A',$$

where $(\bullet)'$ is the transpose of a matrix. The $m \times m$ matrix $\mathbb{S}$ is called the projection matrix of matrix A.

Suppose we have k linearly independent $k \times 1$ vectors x_i and compute

$$v_i = Ax_i,$$

where $1 \leq i \leq k$. These $m \times 1$ vectors v_i can be used to construct an $m \times k$ matrix

$$B = \left[\begin{array}{cccc} v_1 & v_2 & \ldots & v_k \end{array} \right].$$

According to Invariance Theorem [3], the projection matrix of B is the same as that of A:

$$A(A'A)^{-1}A' = B(B'B)^{-1}B'$$

Now suppose the dealer wants to share a secret $m \times m$ matrix S. Then a (k, n)-threshold secret sharing scheme based on Matrix Projection Method can be constructed in the following two phases.

- Phase One: Construction of Shares from the Secret Matrix S
  1) Construct a random $m \times k$ matrix A of rank k where $m > 2k - 3$;
  2) Choose n random $k \times 1$ vectors x_i any k of which are linearly independent;
  3) Calculate n shares $v_i = Ax_i \bmod p$ for $1 \leq i \leq n$;
  4) Compute a projection matrix $\mathbb{S} = (A(A'A)^{-1}A') \bmod p$;
  5) Calculate a remainder matrix $R = (S - \mathbb{S}) \bmod p$;
  6) Destroy the matrix A, the vector x_is, the projection matrix $\mathbb{S}$, the secret matrix S;
  7) Distribute n shares v_i to n participants and make the remainder matrix R publicly known.
- Phase Two: Secret Reconstruction
  1) Collect k shares $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ from the participants;
  2) Construct an $m \times k$ matrix
  $$B = \left[\begin{array}{cccc} v_{i_1} & v_{i_2} & \ldots & v_{i_k} \end{array} \right];$$
  3) Calculate the projection matrix $\mathbb{S} = (B(B'B)^{-1}B') \bmod p$;

4) Compute the secret $S = \mathbb{S} + R \bmod p$.

Note that in step 1 of Phase One, the requirement that $m > 2k - 3$ comes from a condition to correctly apply Matrix Projection Method to multiple secret sharing (See [2]). In steps 2 and 3 of Phase Two, when the group of participants have computed B and $\mathbb{S}$, they can check if B has a rank k and if the projection matrix of B satisfies the previously mentioned five properties. If any of these checks fails, they know that there must have been some accidental errors or dishonest behavior. In this sense, the scheme is also partially verifiable.

IV. Our Multiple Secret Sharing Scheme based on Matrix Projection Method

One of the characteristics of Bai's scheme is that the number of secrets is a square m^2 since the secrets are organized into an $m \times m$ square matrix S that is being processed to produce the shares v_i and the public matrix R. The natural question to ask is how to implement secret sharing of arbitrary number of secrets systematically. We can obviously use Bai's scheme and stuff dummy secrets into the secret matrix S if necessary. However, the participants have to keep track of what elements of the secret matrix are target secrets to share. This is an additional burden. Besides, the threshold k is bounded linearly by m, which is the square root of the number of secrets. So the possible range of the threshold k is limited at the scale of the square root of the number of secrets, while in our scheme the range of k is limited at the scale of the number of secrets (see below).

We next propose a scheme to share arbitrary number of secrets based on the matrix projection method. The scheme has the desirable properties that we do not have to stuff dummy entries into the secret matrix and the search space for each secret is not reduced compared to Bai's scheme so it is as secure. The performance of the scheme is also good and the scheme can also take advantage of the proactive characteristic of the Matrix Projection Method to periodically update shares without modifying the secret matrix.

A. Principle

Suppose $m (m \geq 2)$ is an integer and we have m secret numbers to share: $s_1, s_2, \cdots, s_m$. Each number has a binary representation of N bits. That is, $0 \leq s_i < 2^N$, for $i = 1, \cdots, m$.

Now we choose the smallest prime p such that $p^m \geq 2^N$. (Note that it does not matter if we choose a prime larger than this smallest one.) It's plain that $p \geq 2^{N/m}$. Since $0 \leq s_i < p^m$, we can represent s_i based on radix p with m "digits". That is, for each $i = 1, \cdots, m$, we have

$$s_i = s_{i,m-1}p^{m-1} + s_{i,m-2}p^{m-2} + \cdots + s_{i,1}p + s_{i,0},$$

$$0 \leq s_{i,j} \leq p - 1, j = 0, \ldots, m - 1$$

Furthermore, this representation is unique. Then we can construct an $m \times m$ matrix S using the representations of s_i's based on radix p as follows:

$$S = \begin{pmatrix} s_{1,0} & s_{1,1} & \cdots & s_{1,m-1} \\ s_{2,0} & s_{2,1} & \cdots & s_{2,m-1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{m,0} & s_{m,1} & \cdots & s_{m,m-1} \end{pmatrix}$$

Note that we have chosen each row of S to be the p-radix representation of an original secret. It is equally reasonable to choose the columns of S. Treating S as a new secret matrix, we can construct a (k, n) threshold secret sharing scheme using Matrix Projection Method which performs matrix operations in Z_p where p is the above chosen prime. When we recover S from any k out of n shares, we can compute the original m secret numbers using the above formula. Here we can see that no matter what value m takes we are always sharing a square secret matrix of which every element is utilized. So there is no need to stuff dummy secrets into the matrix. This releases the burden of the participants to keep track of how many secrets are actually shared in the matrix and what positions they occupy in the matrix. In fact, we also get a hidden advantage. When we are trying to share m secrets, the dimension of the secret matrix increases from $\Omega(m^{1/2})$ to m in our scheme comparing to Bai's scheme. Since we have a threshold constraint $m > 2k - 3$, i.e. $k < (m + 3)/2$, we also increase the potential range of the threshold k. Consequently more access structures can be realized by our scheme than Bai's scheme in which the range of k is at the scale of the square root of the number secrets.

B. Dynamics and Proactivity of Our Proposed Scheme

Like He's multi-stage secret sharing scheme [14] and He's multi-secret sharing scheme [15], our multiple secret sharing scheme based on the matrix projection method can change the secrets without changing the shares of the participants as long as the new set of shared secrets are within the same range as the old set of shared secrets. When a new set of m secrets are to be shared, only the $m \times m$ public remainder matrix R needs to be updated. This is very efficient because secure channels between the dealer and the participants are not required when sharing these new secrets.

The proactive feature of the secret sharing scheme based on the matrix projection method is achieved through Pythagorean triples. We first introduce Pythagorean triples [32]. The Pythagorean triples are three integers $\{Z_1, Z_2, Z_3\}$ that satisfy the following equation:

$$Z_1^2 + Z_2^2 = Z_3^2.$$

The general form of a Pythagorean triples is

$$Z_1 = a^2 - b^2, Z_2 = 2ab, Z_3 = a^2 + b^2$$

where $a > b$ are both positive integers. Suppose $k \geq 2$ is an integer and g, h are two random integers that satisfy $1 \leq g, h \leq k, g \neq h$. We can use the Pythagorean triples $\{Z_1, Z_2, Z_3\}$ to construct a $k \times k$ matrix $L = (l_{ij})_{k \times k}$ with its elements defined as follows:

$$l_{ij} = \begin{cases} \frac{Z_1}{Z_3} (\text{mod } p) & \text{if } i = j = g, \\ \frac{Z_1}{Z_3} (\text{mod } p) & \text{if } i = j = h, \\ \frac{Z_2}{Z_3} (\text{mod } p) & \text{if } i = g, j = h, \\ -\frac{Z_2}{Z_3} (\text{mod } p) & \text{if } i = h, j = g, \\ 1 & \text{if } i = j, i \neq g, i \neq h, \\ 0 & \text{otherwise.} \end{cases}$$

The matrix L is orthogonal since $LL' = I_{k \times k}$ (the identity matrix). Given this orthogonal matrix L, we can also construct the following $(m+k) \times (m+k)$ orthogonal matrix T:

$$T = \begin{bmatrix} I_m & 0_{m \times k} \\ 0_{k \times m} & L_{k \times k} \end{bmatrix}.$$

The proactivity of the secret sharing scheme based on the matrix projection method can be achieved as follows. Suppose we have m secrets $s_1, \ldots, s_m$ to share among a group of n participants. First we can still choose a prime p and construct an $m \times m$ secret matrix each row of which consists of a p-radix representation of an original secret number. Suppose we are sharing these secrets with respect to a (k, n)-threshold access structure. The actually shared secret matrix will be an $(m+k) \times (m+k)$ matrix with its upper left $m \times m$ submatrix equal to the desired matrix. At the end of each time round $t = 0, 1, \ldots$, the dealer chooses random numbers $1 \leq g_t, h_t \leq k, g_t \neq h_t$ and $0 < b_t < a_t < p$ and computes the Pythagorean triples $Z_{1t} = a_t^2 - b_t^2 \bmod p$, $Z_{2t} = 2a_t b_t \bmod p$, $Z_{3t} = a_t^2 + b_t^2 \bmod p$. The dealer then computes the $k \times k$ orthogonal matrix L_t and $(m+k) \times (m+k)$ orthogonal matrix T_t and securely distributes the matrix T_t to each of the participants. Upon receiving this matrix at the end of each time round t, each participant can update his share as $v_{i,t} = T_t v_{i,t-1}$ with $v_{i,0}$ being the first round share. With the shares updated in this manner, shares from the same round can recover the secret matrix as normal while shares from different time rounds cannot be pooled together to recover the secret matrix. Thus, the proposed scheme easily achieves proactivity.

To achieve the proactive feature, we have to incur the disadvantage of stuffing dummy secrets into the secret matrix. The number of dummy secrets will be $(m+k)^2 - m^2 = 2mk + k^2$. However, this time the threshold k must satisfy the new requirement $m + k > 2k - 3$, that is, $k < m + 3$. So the range of threshold actually increases furthermore comparing to the original range $k < (m+3)/2$. This is the further advantage of using the proactive feature of the scheme.

C. Security and Performance Analysis of our Proposed Scheme

1) Security Analysis: As we have assumed we are sharing m secrets and each secret has a binary representation of N bits. In Bai's scheme, the search space of each entry of the secret matrix will be 2^N. In our scheme, the search space of each entry of the secret matrix will be roughly $2^{N/m}$. (The actual search space should be as large as the prime p we have chosen to be larger than $2^{N/m}$). However, an adversary has to simultaneously collect m entries of the secret matrix to correctly recover one secret. The combined search space for each secret number is roughly $(2^{N/m})^m = 2^N$ and is not reduced. We conclude that our scheme is at least as secure as Bai's scheme.

2) Performance Analysis: In Bai's scheme, when we need to share m secret numbers, we must construct a secret matrix with at least m entries. The number of rows or columns of the secret matrix is $\Omega(m^{1/2})$. Each entry of the matrix occupies N bits. Thus each share, which is a vector of length $\Omega(m^{1/2})$, occupies $N \cdot \Omega(m^{1/2}) = \Omega(Nm^{1/2})$ bits. In addition, we need to broadcast the public remainder matrix R which is $\Omega(m^{1/2}) \cdot \Omega(m^{1/2}) \cdot N = \Omega(Nm)$ bits.

In our scheme, when we need to share m secret numbers, we must construct a secret matrix with m^2 entries. Each entry of the secret matrix occupies roughly $\Omega(N/m)$ bits. Each share occupies roughly $\Omega(N/m) * m = \Omega(N)$ bits. The broadcast public matrix R is roughly $\Omega(N/m) * m^2 = \Omega(Nm)$ bits. We can see that although the matrix R is about the same size in the two schemes, each share can be much smaller in length than that in Bai's scheme and is constant size (the same as that of a single secret). We conclude that our scheme is space efficient.

In terms of computation complexity, we point out that although our scheme needs to first convert the secret numbers into a square matrix and later back, all the other matrix arithmetics are done reducing a smaller modulus (roughly the m-th square root of the original modulus). These matrix operations are faster when done reducing a smaller modulus [31]. So the total computation time on both the dealer's part and the participants' part should be no more than those in Bai's scheme.

V. Conclusion

We proposed a multiple secret sharing scheme based on matrix projection method. It is secure in most applications. The scheme has the advantage that we can share any number of secrets and do not need to stuff dummy elements into the secret matrix. It also increases the potential range of the threshold parameter thus increasing the range of threshold access structures that can be realized. The scheme also reduces the share size comparing to Bai's scheme. Particularly, it achieves constant share size-that of a single secret. We can also take advantage of the proactive characteristic of the matrix projection method to update shares periodically without changing the secrets to increase the scheme's overall security. When we are using the proactive feature of the scheme, the threshold range can be further increased. The scheme is partially verifiable based on the properties of the projection matrix. And the scheme is dynamic to secret change-it only needs to change the public remainder matrix to share a new set of secrets.

REFERENCES

[1] C. A. Asmuth and J. Bloom. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 29:208–210, 1983.

[2] Li Bai. A strong ramp secret sharing scheme using matrix projection. *Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 652–656, 2006.

[3] Li Bai and Xukai Zou. A proactive secret sharing scheme in matrix projection method. *International Journal of Security and Networks*, 4:In Press, 2009.

[4] G. R. Blakley. Safeguarding cryptographic keys. *American Federation of Information Processing Societies Proceedings*, 48:313–317, 1979.

[5] Carlo Blundo, Alfredo De Santis, and Ugo Vaccaro. Efficient sharing of many secrets. *LNCS*, 665:692–703, 1993.

[6] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 6:105–113, 1989.

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

[8] Yang Chou-Chen, Chang Ting-Yi, and Hwang Min-Shiang. A (t,n) multi-secret sharing scheme. *Applied Mathematics and Computation*, 151:483–490, 2004.

[9] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. *Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science*, pages 427–437, 1987.

[10] M. Franklin and M. Yung. Communication complexity of secure computation. *STOC*, pages 699–710, 1992.

[11] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini. Secret sharing in multilevel and compartmented groups. *Lecture Notes in Computer Science*, 1438:367–378, 1998.

[12] L. Harn. Comment: Multistage secret sharing based on one-way function. *Electronics Letters*, 31:262, 1995.

[13] L. Harn. Efficient sharing (broadcasting) of multiple secret. *IEE Proceedings-Computers and Digital Techniques*, 142:237–240, 1995.

[14] J. He and E. Dawson. Multistage secret sharing based on one-way function. *Electronics Letters*, 30:1591–1592, 1994.

[15] J. He and E. Dawson. Multisecret-sharing scheme based on one-way function. *Electronics Letters*, 31:93–95, 1995.

[16] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. *Lecture Notes in Computer Science*, 963:339–352, 1995.

[17] S. Iftene. General secret sharing based on the chinese remainder theorem with applications in e-voting. *Electronic Notes in Theoretical Computer Science*, 186:67–84, 2007.

[18] I. Ingemarsson and G. J. Simmons. A protocol to set up shared secret schemes without the assistance of mutually trusted party. *LNCS*, 473:266–282, 1991.

[19] SHAO J and CAO Z.-F. A new efficient (t, n) verifiable multi-secret sharing (vmss) based on ych scheme. *Applied Mathematics and Computation*, 168:135–140, 2005.

[20] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe. Multisecret threshold schemes. *Proceedings of the 13th annual international cryptology conference on Advances in cryptology*, pages 126–135, 1994.

[21] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe. A construction for multisecret threshold schemes. *Designs, Codes and Cryptography*, 9:287–303, 1996.

[22] PANG L.-J and WANG Y.-M. A new (t, n) multi-secret sharing scheme based on shamir's secret sharing. *Applied Mathematics and Computation*, 167:840–848, 2005.

[23] K. M. Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang. Changing thresholds in the absence of secure channels. *Lecture Notes in Computer Science*, 1587:177–191, 1999.

[24] M. Mignotte. How to share a secret. *Lecture Notes in Computer Science*, 149:371–375, 1983.

[25] Liaojun Pang, Huixian Li, Ye Yao, and Yumin Wang. A verifiable (t, n) multiple secret sharing scheme and its analyses. *2008 International Symposium on Electronic Commerce and Security*, pages 22–26, 2008.

[26] T. P. Pedersen. non-interactive and information theoretic secure verifiable secret sharing. *Lecture Notes in Computer Science*, 576:129–140, 1992.

[27] A. Shamir. How to share a secret. *Communication of ACM*, 22:612–613, November 1979.

[28] G. J. Simmons. An introduction to shared secret and/or shared control schemes and their application. *Contemporary Cryptology*, pages 441–497, 1991.

[29] Ron Steinfelda, Josef Pieprzyka, and Huaxiong Wang. Lattice-based threshold-changeability for standard crt secret-sharing schemes. *Finite Fields and Their Applications*, 12:653–680, 2006.

[30] Ron Steinfelda, Josef Pieprzyka, and Huaxiong Wang. Lattice-based threshold changeability for standard shamir secret-sharing schemes. *IEEE Transactions on Information Theory*, 53:2542–2559, 2007.

[31] D. R. Stinson. *Cryptography: Theory and Practice, 3rd.* CRC Press, Boca Raton, FL, 2005.

[32] Eric W. Weisstein. Pythagorean triple - from mathworld. 2003.