Journal of Information Hiding and Multimedia Signal Processing ©2013 ISSN 2073-4212
Ubiquitous International Volume **4**, Number **1**, January **2013**

A Construction for Secret Sharing Scheme with General Access Structure

Cheng Guo[1], and Chin-Chen Chang[2,3]

[1]School of Software,
Dalian University of Technology, Dalian 116620, China
guo8016@gmail.com

[2]Department of Information Engineering and Computer Science,
Feng Chia University, Taichung 40724, Taiwan
alan3c@gmail.com

[3]Department of Computer Science and Information Engineering,
Asia University, Taichung 41354, Taiwan
alan3c@gmail.com

Received July 2012; revised October 2012

Abstract. *Many efficient secret sharing schemes for general access structures have been developed in efforts to deal with the problems of multi-party computations (MPC), threshold cryptography, and access control. In this paper, we have proposed a novel secret sharing scheme with general access structures that is based on the key-lock-pair mechanism. In our scheme, the dealer can assess a real situation and design the corresponding access structures,* $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$*. The different qualified subset of participants in* $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ *can cooperate to reconstruct the shared secret, and no unqualified participants can reconstruct the corresponding shared secret.*

Keywords: Secret sharing, general access structure, threshold scheme, key-lock-pair

1. Introduction.

Secret sharing was developed in 1979 by Shamir [1] and Blakley [2], who presented two different methods to construct a threshold scheme, the first of which was based on the Lagrange interpolating polynomial and the second of which was based on linear projective geometry. In a secret sharing scheme, a dealer is responsible for creating some pieces of information related to the secret data, known as shadows of the secret data, and distributing these shadows to the participants. By using a secret sharing scheme, secret data can be protected among a finite set of participants in such a way that only pre-determined, qualified subsets of participants can cooperate to reconstruct the secret data, and no unqualified subset of participants can get any information about the secret data.

Let $P = \{p_1, p_2, \ldots, p_n\}$ be the set of participants. An access structure, denoted by Γ, is a collection of qualified subsets of p. The access structure of a secret sharing scheme satisfies the monotone ascending property, i.e., for any $A \in \Gamma$, $B \subseteq A$ implies $B \in \Gamma$. The traditional (t, n) threshold secret sharing [3 - 9] is a special case of general secret sharing. Their qualified subsets are those that have at least a certain, pre-determined number of participants. Researchers have investigated (t, n) threshold secret sharing extensively, and it has been performed for a wide range of applications, including key-management problems [10] and key-distribution problems [11, 12]. In 2010, Harn and Lin [13] extended the basic idea of a $(t,\ n)$ secret sharing scheme and proposed a strong $(n,\ t,\ n)$ verifiable secret sharing (VSS) scheme. In their scheme, each participant also can act as a dealer. In 2012, Liu, Harn, Yang, and Zhang [14] proposed an efficient strong $(n,\ t,\ n)$ VSS that was more efficient than Harn and Lins scheme [13]. In addition, they proposed an $(n,\ t,\ n)$ multi-secret sharing (MSS) scheme to allow participants to share $n-t+1$ secrets.

However, $(t,\ n)$ threshold mechanisms have a serious limitation in some applications, and there are still many challenges to be overcome. One of the major problems is the determination of how different approaches can be utilized to construct secret sharing schemes with special access structures, such as multi-level access structures, weighted-threshold access structures, hierarchical access structures, and generalized-threshold access structures. Also, it is worthwhile to identify families of access structures that have other useful properties for secret sharing applications.

Shamir [1], in his seminal work on secret sharing, attempted to construct a weighted-threshold secret sharing scheme in which the participants did not have the same status. Shamir discussed the case of sharing a secret among the shareholders of a company in which each shareholder held a different amount of shadows. In 2007, Iftene [15] also presented a weighted-threshold secret sharing scheme based on the Chinese Remainder Theorem (CRT). Iftenes scheme extended the threshold Mignotte scheme [3] in order to address the weighted-threshold access structure in which each participant is associated with one positive weight, and the secret can be reconstructed when the weights of the cooperating participants are equal to or greater than a fixed threshold. In 2002, Sun and Chen [16] also proposed a weighted-decomposition construction for perfect secret sharing schemes with general access structures.

In 2007, Tassa [17] utilized the Birkhoff interpolation to propose a novel, hierarchical-threshold secret sharing scheme. In his scheme, the secret is shared among a group of participants that is partitioned into some levels, and the corresponding access structure is determined by a sequence of threshold requirements. In 2012, Zhao, Peng, Wang, and Yang [18] proposed a secret sharing scheme based on the properties of the Jordan matrix that can achieve the $(t,\ n)$ threshold and the adversary access structure. That is, there are some subsets that contain at least t participants that cannot reconstruct the shared secret.

In 1996, Jackson, Martin, and O'Keefe [19] considered a secret sharing scheme in which a number of different secrets can be shared among a group of participants with each secret being associated with a (potentially different) access structure. In 2007, Farràs, Farré, and Padró [20] presented a characterization of multipartite access structures in terms of discrete polymatroids. Also, they proposed an ideal multipartite secret sharing scheme based on the matroid. In 2011, based on monotone span programs (MSP), Hsu, Cheng, Tang, and Zeng [21] proposed an ideal, multi-threshold, secret sharing scheme for general access structures. In their scheme, each different subset of the set of participants may have different associated secrets depending on the access structures. The $(t,\ n)$-threshold secret sharing schemes also have been utilized to design a steganographic technique [22, 23, 24] for important confidential images.

Due to the difficulty of finding efficient secret sharing schemes with general access structures, more and more researchers are investigating this problem. In this paper, we proposed a novel, secret sharing scheme with general access structures that is based on the key-lock-pair mechanism. In our scheme, the dealer can design the corresponding access structure $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ according to the real situation. The subset of participants in $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ can cooperate to reconstruct the shared secret, and no unqualified participants can obtain any information about the shared secret.

The structure of this paper is organized as follows. In Section 2, the key-lock-pair mechanism is reviewed briefly. In Section 3, we describe the proposed secret sharing scheme with general access structure that is based on the key-lock-pair mechanism. Section 4 addresses the correctness and security analysis of the proposed scheme, and our conclusions are presented in Section 5.

2. **Preliminary.** In 1984, Wu and Hwang [25] proposed a revised version of the key-lock-pair (KLP) mechanism [26] that fulfills the requirement of the single-key-lock (SKL) system, in which each user keeps only one key and each resource is associated with a single lock. By an operation on the key of the i^{th} user and the lock of the j^{th} resource, we can obtain the access right of user i for resource j.

In this section, we briefly introduce this key-lock-pair mechanism [26], which is the major building block of our scheme.

We can establish an arbitrary $m \times n$ matrix A with entries a_{ij} represented by positive integer numbers in Galois Field GF(p), where p is a prime number and $1 \leq i \leq m$, $1 \leq j \leq n$. Many vector pairs exist, i.e., $\{K_i, L_j\}$, $1 \leq i \leq m$, $1 \leq j \leq n$, with dimensions $1 \times m$ and $m \times 1$, respectively, and

$$K_i * L_j = a_{ij} \tag{1}$$

where $*$ denotes the operation of inner product over Galois Field GF(p).

Therefore, we can assign K_i to user i and L_j to the file j as their single key and lock, respectively.

We will give an example that was described in reference [25].

We can establish an arbitrary, non-singular matrix K ($|K| \neq 0$) in Galois Field GF(7) of size 5 for five users:

$$K = \begin{bmatrix} 3 & 1 & 5 & 6 & 5 \\ 1 & 2 & 3 & 5 & 3 \\ 4 & 1 & 1 & 4 & 1 \\ 2 & 6 & 1 & 1 & 2 \\ 5 & 5 & 6 & 5 & 4 \end{bmatrix}$$

Given a column vector $C = (4, 3, 1, 1, 1, 0)$ with dimension 1×5 in Galois Field GF(7), we can find a coordinate vector $X = (x_1, x_2, x_3, x_4, x_5)$, which is obtained by solving the set of five linear equations in GF(7). The corresponding X for the above C is (1, 3, 0, 1, 4).

This example shows that, when the vector X is solved, the i^{th} element in vector C becomes the result of $K_i * X$, where $*$ denotes the operation of inner product over Galois Field GF(p), and K_i is the i^{th} row of matrix K.

3. **The secret sharing scheme with general access structures.** In this section, first, we give a definition of secret sharing with general access structures with respect to the proposed scheme. Then, we propose a novel, secret sharing scheme with general access structure.

3.1. **Definition of general secret sharing.** Let $P = \{p_1, p_2, \ldots, p_n\}$ be the set of participants, and let $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ be an m-tuple of access structures on the set of P, where $m \leq 2^{|P|-1}$. The secret data can be shared among these n participants, and each participant holds one piece of information relating to the secret data. Each qualified subset Γ_i, $1 \leq i \leq m$ of P, pre-determined according to the access structures $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$, can cooperate to reconstruct the shared secret data.

Example 1. Let $P = \{p_1, p_2, p_3, p_4\}$ and $\Gamma = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3\}, \{p_2, p_4\}\}$. Then, the secret data S can be shared in such a quadruple $\Gamma = (\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4)$. Since the access structures satisfy the monotone ascending property, the access structures can be described as follows:

$$(\Gamma_1)_{\min} = \{\{p_1, p_2\}\},\ (\Gamma_2)_{\min} = \{\{p_1, p_3, p_4\}\},$$
$$(\Gamma_3)_{\min} = \{\{p_2, p_3\}\},\ \textit{and}\ (\Gamma_4)_{\min} = \{\{p_2, p_4\}\}.$$

3.2. **Shadow generation and distribution.** In this subsection, we present a secret sharing scheme with general access structures. In the proposed scheme, the dealer (a trusted third party) is responsible for generating the shadows and distributing them to each participant. This scheme consists of the following steps:

Step 1. The dealer builds the corresponding access structures $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ according to the real situation.

Step 2. The dealer can establish an arbitrary, non-singular matrix K of size n ($|K| \neq 0$) in Galois Field GF(p) for n users, where p is a large prime number.

$$\text{Let } K = \begin{bmatrix} k_{11} & k_{12} & \ldots & k_{1n} \\ k_{21} & k_{22} & \ldots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \ldots & k_{nn} \end{bmatrix}$$

We can obtain n row vectors,

$$\begin{aligned} K_1 &= (k_{11}, k_{12}, \ldots k_{1n})^T, \\ K_2 &= (k_{21}, k_{22}, \ldots k_{2n})^T, \\ &\vdots \\ K_n &= (k_{n1}, k_{n2}, \ldots k_{nn})^T. \end{aligned} \tag{2}$$

Step 3. Assume that the shared secret data are S. According to the shared secret data and the corresponding access structures, the dealer can construct a matrix A of size n.

$$A = \begin{array}{c|cccc} & p_1 & p_2 & \ldots & p_n \\ \hline p_1 & a_{11} & a_{12} & \ldots & a_{1n} \\ p_2 & a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_n & a_{n1} & a_{n2} & \ldots & a_{nn} \end{array}$$

Then, we give some rules to describe how to compute the elements of matrix A. There are some access structures $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$. Given an access structure $\Gamma_i = (p_j, p_k, p_r, p_l)$, $1 \leq i \leq m$, $1 \leq j, k, r, l \leq n$, we locate three elements of matrix A, a_{kj}(the k^{th} column and j^{th} row of matrix A), a_{rj}(the r^{th} column and j^{th} row of matrix A), and a_{lj}(the l^{th} column and j^{th} row of matrix A). We randomly select three positive integers $\{a_{kj}, a_{rj}, a_{lj}\}$ in Galois Field GF(p) that satisfy $S = a_{kj} + a_{rj} + a_{lj}$. Using the same method, the dealer can compute the other corresponding elements of matrix A. The remaining elements of matrix A are set to "0". Then, we can obtain matrix A. In the following, we will give an example to describe how to construct matrix A.

Example 2. Continuing Example 1 above, $P = \{p_1, p_2, p_3, p_4\}$ and $\Gamma = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3\}, \{p_2, p_4\}\}$. Assume that the shared secret data are $S = 9$, and $p = 11$.

Since there are four participants, we define a 4×4 matrix A. The size of the matrix is equal to the number of participants. In the following, we utilize matrix A to describe the shared secret data and the corresponding access structures.

$$\text{Let } A = \begin{array}{c|cccc|} & p_1 & p_2 & p_3 & p_4 \\ p_1 & a_{11} & a_{12} & a_{13} & a_{14} \\ p_2 & a_{21} & a_{22} & a_{23} & a_{24} \\ p_3 & a_{31} & a_{32} & a_{33} & a_{34} \\ p_4 & a_{41} & a_{42} & a_{43} & a_{44} \end{array}$$

Concerning access structure $\Gamma_1 = \{\{p_1, p_2\}\}$, we find the corresponding element a_{21} located in the second column and the first row of matrix A and set $a_{21} = 9$. In the same way, concerning $\Gamma_2 = \{p_1, p_3, p_4\}$, we set $a_{31} = 2$ and $a_{41} = 7$, satisfying $S = a_{31} + a_{41}$. Concerning $\Gamma_3 = \{p_2, p_3\}$ and $\Gamma_4 = \{p_2, p_4\}$, we set $a_{32} = 9$ and $a_{42} = 9$, respectively. Then, the dealer can construct the corresponding matrix A according to the secret data S and the access structures,

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 9 & 0 & 0 & 0 \\ 2 & 9 & 0 & 0 \\ 7 & 9 & 0 & 0 \end{bmatrix}.$$

Step 4. Given the corresponding matrix A, $A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$, the dealer can compute n column vectors $(L_1, L_2, \dots, L_n)$,

$$\begin{aligned} L_1 &= (l_{11}, l_{12}, \dots, l_{1n}), \\ L_2 &= (l_{21}, l_{22}, \dots, l_{2n}), \\ &\vdots \\ L_n &= (l_{n1}, l_{n2}, \dots, l_{nn}). \end{aligned} \tag{3}$$

that satisfy $a_{ij} = L_i * K_j$, where $*$ denotes the operation of inner product over Galois Field GF(p). Since the matrix K is an arbitrary, non-singular matrix over GF(p), that is $|K| \neq 0$, the n columns of K are linearly independent over GF(p). Therefore, a unique value of L_i exists, such that $a_{ij} = L_i * K_j$.

Example 3. (Following Example 2). The dealer establishes an arbitrary, non-singular matrix K of size 4 ($|K| \neq 0$) in Galois Field GF(11).

$$\text{Let } K = \begin{bmatrix} 3 & 5 & 6 & 5 \\ 1 & 3 & 5 & 3 \\ 2 & 1 & 1 & 2 \\ 5 & 6 & 5 & 4 \end{bmatrix}$$

Therefore, we have $K_1 = (3, 5, 6, 5)^T$, $K_2 = (1, 3, 5, 3)^T$, $K_3 = (2, 1, 1, 2)^T$, and $K_4 = (5, 6, 6, 5, 4)^T$.

According to matrix A and matrix K, we can compute four column vectors (L_1, L_2, L_3, L_4) that satisfy $a_{ij} = L_i * K_j$ in Galois Field GF(11).

Concerning the vector $L_1 = (l_{11}, l_{12}, l_{13}, l_{14})$, we can compute:

$$\begin{cases} k_{11}l_{11} + k_{12}l_{12} + k_{13}l_{13} + k_{14}l_{14} = a_{11} \\ k_{21}l_{11} + k_{22}l_{12} + k_{23}l_{13} + k_{24}l_{14} = a_{12} \\ k_{31}l_{11} + k_{32}l_{12} + k_{33}l_{13} + k_{34}l_{14} = a_{13} \\ k_{41}l_{11} + k_{42}l_{12} + k_{43}l_{13} + k_{44}l_{14} = a_{14} \end{cases}$$

$$\begin{cases} 3l_{11} + 5l_{12} + 6l_{13} + 5l_{14} = 0 \\ l_{11} + 3l_{12} + 5l_{13} + 3l_{14} = 0 \\ 2l_{11} + l_{12} + l_{13} + 2l_{14} = 0 \\ 5l_{11} + 6l_{12} + 5l_{13} + 4l_{14} = 0 \end{cases}$$

Then, we can obtain the vector $L_1 = (l_{11}, l_{12}, l_{13}, l_{14}) = (0, 0, 0, 0)$. Using the same method, we can compute $L_2 = (2, 9, 2, 9)$, $L_3 = (3, 4, 1, 0)$, and $L_4 = (9, 9, 7, 5)$. Furthermore, the dealer can compute four corresponding shadows (L_1, K_1), (L_2, K_2), (L_3, K_3), and (L_4, K_4) for each participant.

Step 5. The dealer can compute n pairs of vectors (L_j, K_j), $1 \le i \le n$, and distribute (L_j, K_j) to each corresponding participant as her/his shadow over a secure channel.

3.3. **Secret reconstruction.** In traditional secret sharing, there are two kinds of modes for secret reconstruction. One mode is that all active participants send their shadows to a designated party that is responsible for reconstructing the secret data. In the other mode, if one participant wants to obtain the shared secret data, he/she must initiate a call to all participants. When this message is received, each active participant broadcasts her/his shadow. If a sufficient number of shadows are obtained, the shared secret data can be reconstructed. In the proposed scheme, we utilized the second reconstruction mode.

If one participant p_j wants to reconstruct the shared secret data, he/she will broadcast her/his shadow K_j to the group of participants. If some active participants, e.g., p_k, p_r and p_l, also want to reconstruct the shared secret data, they must broadcast their shadows, i.e., L_k, L_r and L_l. If the subset $\Omega = (p_j, p_k, p_r, p_l) \subseteq \Gamma$, they can cooperate to compute the shared data S in Galois Field GF(p) by

$$S = K_j * L_k^T + K_j * L_r^T + K_j * L_l^T \tag{4}$$

where $*$ denotes the operation of inner product over Galois Field GF(p). If the subset $\Omega = (p_j, p_k, p_r, p_l) \nsubseteq \Gamma$, these participants cannot compute the shared secret data.

Example 4. (Following Example 3). Suppose that p_1 wants to reconstruct the shared secret data, he/she must initiate a call and broadcast her/his $K_1 = (3, 5, 6, 5)^T$. Then, if both p_3 and p_4 also want to reconstruct the secret data, they must broadcast their shadows $L_3 = (4, 4, 5, 2)$ and $L_4 = (3, 5, 4, 3)$. Then, they can compute the shared secret data in Galois Field GF(11) as follows:

$$S = (4, 4, 5, 2) * (3, 5, 6, 5)^T + (3, 5, 4, 3) * (3, 5, 6, 5)^T = 5,$$

where $*$ denotes the operation of inner product over Galois Field GF(11).

4. **Analysis of correctness and security.** In this section, we discuss the correctness and security of the proposed scheme.

Proposition 1. According to the access structures, the qualified subset of participants in $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ can cooperate to reconstruct the corresponding shared secret S.

Proof. As the above description in Subsection 3.2 indicated, matrix A can be constructed according to the shared secret S and the corresponding access structures. Given any access structure $\Gamma_i = (p_j, p_k, p_r, \ldots, p_l)$, $1 \le i \le m$, $1 \le j, k, r, \ldots, l \le n$, we can set $S = a_{jk} + a_{jr} + \ldots + a_{jl}$. From [25], we will know that for an $m \times n$ access matrix A with entries a_{ij} represented by positive integer numbers, choose a prime number p such that $p \geq \max\{a_{ij}\}$, $1 \leq i \leq m$, $1 \leq j \leq n$.

Then, in [25] they can conclude the following theorem.

Theorem 1 [25]. There exist many sets of $\{K_i, L_j\}$, $1 \leq i \leq m$, $1 \leq j \leq n$, K_i, L_j having dimensions $1 \times m$ and $m \times 1$, respectively, and:

$$K_i * L_j = a_{ij}$$

where $*$ denotes the operation of inner product over Galois Field GF(p).

A detailed description of theorem 1 is provided in reference [25].

Then, we can obtain n arbitrary row vectors $(K_1, K_2, \ldots, K_n)$ that are linearly independent over GF(p) and compute n column vectors $(L_1, L_2, \ldots, L_n)$ that satisfy $a_{ij} = L_i * K_j$, where $*$ denotes the operation of inner product over Galois Field GF(p). Therefore, if a qualified subset $\{p_j, p_k, p_r, \ldots, p_l\}$ of participants in $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ wants to reconstruct the shared secret, we can compute $S = a_{jk} + a_{jr} + \ldots + a_{jl}$.

Proposition 2. No unqualified participants can reconstruct the corresponding shared secret.

Proof. According to Proposition 1, we can conclude that the shared secret can be reconstructed by any qualified subset of participants by computing $S = a_{jk} + a_{jr} + \ldots + a_{jl}$. Since these n row vectors $(K_1, K_2, \ldots, K_n)$ are arbitrary and linearly independent over GF(p), unique column vectors $(L_1, L_2, \ldots, L_n)$ exist that satisfy $a_{ij} = L_i * K_j$, where $*$ denotes the operation of inner product over Galois Field GF(p). So, any unqualified participants without the expected column vectors $\{L_k, L_r, \ldots, L_l\}$ cannot compute the corresponding corrected $\{a_{jk}, a_{jr}, \ldots, a_{jl}\}$. Consequently, they cannot compute the corrected shared secret S.

Since the entries a_{ij} of matrix A are selected randomly just satisfying $S = \sum_{j=1}^{n} a_{ij}$, $1 \leq i \leq n$, unqualified participants also cannot guess the corrected a_{ij} that satisfies $S = \sum_{j=1}^{n} a_{ij}$, $1 \leq i \leq n$.

5. **Conclusions.** In this paper, we proposed a novel, secret sharing scheme for general access structures based on the key-lock-pair mechanism. In a set of participants $P = \{p_1, p_2, \ldots, p_n\}$, the dealer can design the corresponding access structures $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ in terms of the real situation. Each qualified subset of $P = \{p_1, p_2, \ldots, p_n\}$ in these access structures $\Gamma = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ can reconstruct the shared secret. The correctness and security analysis showed that the shared secret only can be reconstructed by the corresponding qualified subset of participants and that no unqualified participants can reconstruct the corresponding shared secret.

REFERENCES

[1] A. Shamir, How to share a secret, *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. Blakley, Safeguarding cryptographic keys, *Proc. of the National Computer Conference*, pp. 313-317, 1979.

[3] M. Mignotte, How to share a secret, *Proc. of the conference on Cryptography*, pp. 371-375, 1982.

[4] L. Harn, Efficient sharing (broadcasting) of multiple secrets, *IEE Proceedings of Computers and Digital Techniques*, vol. 142, no. 3, pp. 237-240, 1995.

[5] R. J. Hwang, and C. C. Chang, An on-line secret sharing scheme for multi secrets, *Journal of Computer Communications*, vol. 21, no. 13, pp. 1170-1176, 1998.

[6] H. Y. Chien, J. K. Jan, and Y.M. Tseng, A practical (t, n) multi-secret sharing scheme, *IEICE trans. fundamentals of electronics, communications and computer*, pp. 2762-2765, 2000.

[7] C. C. Yang, T. Y. Chang, and M. S. Hwang, A (t, n) multi-secret sharing scheme, *Journal of Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483-490, 2004.

[8] R. J. Hwang, W. B. Lee, and C. C. Chang, A concept of designing cheater identification methods for secret sharing, *Journal of Systems and Software*, vol. 46, no. 1, pp. 7-11, 1999.

[9] L. J. Pang, and Y. M. Wang, A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing, *Journal of Applied Mathematics and Computation*, vol. 167, no. 2, pp. 840-848, 2005.

[10] R. D'Souza, D. Jao, I Mironov, and O. Pandey, Publicly verifiable secret sharing for cloud-based key management, *Proc. of the 12th international conference on Cryptology in India*, pp. 290-309, 2011.

[11] L. Harn, and C. L. Lin, Authenticated group key transfer protocol based on secret sharing, *IEEE Trans. Computers*, vol. 59, no. 6, pp. 842-846, 2010.

[12] C. Y. Lee, Z. H. Wang, L. Harn, and C. C. Chang, Secure key transfer protocol based on secret sharing for group communications, *IEICE Trans. Information and Systems*, no.11, pp. 2069-2076, 2011.

[13] L. Harn, and C. L. Lin, Strong (n, t, n) verifiable secret sharing scheme, *Journal of Information Sciences*, vol. 180, no. 16, pp. 3059-3064, 2010.

[14] Y. X. Liu, L. Harn, C. N. Yang, and Y. Q. Zhang, Efficient (n, t, n) secret sharing schemes, *Journal of Systems and Software*, vol. 85, no. 6, pp. 1325-1332, 2012.

[15] S. Iftene, General secret sharing based on the Chinese remainder theorem with applications in e-voting, *Journal of Electronic Notes in Theoretical Computer Science*, vol. 184, no. 14, pp. 67-84, 2007.

[16] H. M. Sun, and B. L. Chen, Weighted decomposition construction for perfect secret sharing schemes, *Journal of Computers & Mathematics with Applications*, vol. 43, pp. 877-887, 2002.

[17] T. Tassa, Hierarchical threshold secret sharing, *Journal of Cryptology*, vol. 20, no. 2, pp. 237-264, 2007.

[18] D. W. Zhao, H. P. Peng, C. Wang, and Y. X. Yang, A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure, *Journal of Computers & Mathematics with Applications*, vol. 64, pp. 611-615, 2012.

[19] W. A. Jackson, K. M. Martin, and C. M. O'Keefe, Ideal secret sharing schemes with multiple secrets, *Journal of Cryptology*, vol. 9, no. 4, pp. 233-250, 1996.

[20] O. Farràs, J.M. Farré, and C. Padró, Ideal multipartite secret sharing schemes, *Proc. of 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 448-465, 2007.

[21] C. F. Hsu, Q. Cheng, X. M. Tang, and B. Zeng, An ideal multi-secret sharing scheme based on MSP, *Journal of Information Sciences*, vol. 181, no. 7, pp. 1403-1409, 2011.

[22] C. S. Chan, C. C. Chang, and H. P. Vo, A User-Friendly Image Sharing Scheme Using JPEG-LS Median Edge Predictor, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 4, pp. 340-350, 2012.

[23] Z. H. Wang, C. C. Chang, H. N. Tu, and M. C. Li, Sharing a Secret Image in Binary Images with Verification, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 1, pp. 78-90, 2011.

[24] B. Li, J. H. He, J. W. Huang, and Y.Q. Shi, A Survey on Image Steganography and Steganalysis, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142-172, 2011.

[25] M. L. Wu, and T. Y. Hwang, Access control with single-key-lock, *IEEE Trans. Software Engineering*, no. 2, pp. 185-191, 1984.

[26] G. S. Graham, and P. J. Denning, Protection-Principles and practice, *Proc. of American Federation of Information Processing Societies*, vol. 40, pp. 417-429, 1972.