Eigenvalue-Based Special Threshold Secret Sharing Scheme in the Black-Box Sense: Postprint

Authors: Zhang Yanshuo, Li Wenjing, Shi Guozhen, Jiang Hua, Chen Lei, Yang Tao

Date: 2018-05-24T00:00:00+00:00

Abstract

Based on Shamir' s (n,t) secret sharing scheme, we propose a novel threshold secret sharing scheme. By exploiting the property that the characteristic equation of an n×n matrix possesses repeated roots, we realize secret sharing among participants from different sets. The sub-master keys corresponding to the same participant set are identical—that is, the eigenvalues are identical—and different eigenvectors corresponding to the same eigenvalue are employed as sub-keys and distributed to participating members within the same set. Moreover, by utilizing a black box, members within the same set can verify the authenticity of their sub-keys, thereby achieving fraud prevention. Analysis results demonstrate that this scheme is a secure ideal secret sharing scheme.

Full Text

Preamble

A Special Threshold Secret Sharing Scheme in the Black-Box Sense Based on Eigenvalues

Zhang Yanshuo[1,2], Li Wenjing[1,2], Shi Guozhen[1], Jiang Hua[1], Chen Lei[1], Yang Tao[2]

[1]Beijing Electronic Science & Technology Institute, Beijing 100070, China
[2]The Third Research Institute of Ministry of Public Security, Shanghai 201204, China

Abstract: Based on the Shamir (n, t) secret sharing scheme, this paper proposes a novel threshold secret sharing scheme. By leveraging the property that the characteristic equation of an n-th order matrix has multiple roots, the scheme enables secret sharing among participants from different sets. The secondary master key corresponding to the same participation set is identical—

that is, the eigenvalues are the same—and the different eigenvectors corresponding to the same eigenvalue are used as sub-keys distributed to members of the same participation set. Moreover, using the black box, members within the same set can verify the authenticity of their sub-keys, thereby achieving fraud prevention. Analysis results demonstrate that this scheme is a secure and ideal secret sharing scheme.

Keywords: Shamir (n, t) secret sharing; symmetric matrix; eigenvalues; eigenvector; black box

0 Introduction

Since Shamir[1] and Blakley[2] first proposed threshold secret sharing schemes in 1979, research on secret sharing mechanisms has attracted extensive attention and yielded fruitful results. Ito et al.[3] described general methods for secret sharing and presented techniques for implementing secret sharing schemes with arbitrary monotone access structures. Laih et al. introduced the concept of dynamic secret sharing, where the master secret can be updated arbitrarily while participants' sub-secret values remain unchanged. Traverso et al. proposed the first dynamic and verifiable hierarchical secret sharing scheme based on Birkhoff interpolation. Zarepour-Ahmadabadi et al. presented a novel and efficient algorithm to address the high communication cost of dynamic keys. Yang et al. proposed a weighted hyperelliptic secret sharing scheme. Binu et al. introduced a secret sharing scheme with monotone generalized access structures that provides a new approach to solving information security and key management problems, utilizing Shamir' s scheme and elliptic curve pairing methods to achieve verifiability. Jarecki et al. proposed a round-optimal PPSS scheme. Pilaram et al.[1] constructed a lattice-based threshold multi-stage secret sharing (MSSS) scheme based on Ajtai' s one-way function. Sarkar and Wang et al.[11],[12] proposed secret sharing schemes based on bilinear pairing (BLP) mappings.

Building upon Shamir' s threshold scheme, this paper proposes a new design method for threshold secret sharing based on eigenvalues, exploiting the property that the characteristic equation of an n-order symmetric matrix has multiple roots. Simultaneously, the scheme designs a "black box" and utilizes it to implement sub-secret generation and master key recovery functions. Through analysis and proof, the scheme is shown to be perfectly ideal and theoretically unbreakable.

1 Preliminary Knowledge

For convenience of scheme description, we first introduce the foundational knowledge employed.

1.1 Eigenvalues and Eigenvectors of Square Matrices

Definition 1[13]: Let A be an n-order matrix. If a scalar and an n-dimensional non-zero column vector p satisfy the relation:

$$Ap = \lambda p \quad (1)$$

then is called an eigenvalue of matrix A, and the non-zero vector p is called an eigenvector of A corresponding to eigenvalue . Equation (1) can also be written as:

$$(A - \lambda E)p = 0$$

This is a homogeneous linear system with n unknowns and n equations.

1.2 Properties of Symmetric Matrices

Theorem 1: Let A be an n-order symmetric matrix. Then there must exist an orthogonal matrix P such that:

$$P^{-1}AP = \Lambda$$

where Λ is a diagonal matrix with the n eigenvalues (i = 1, 2, ···, n) of A as its diagonal elements.

Corollary 1: Let A be an n-order symmetric matrix. If is a k-fold root of the characteristic equation of A, then there are exactly k linearly independent eigenvectors corresponding to eigenvalue .

1.3 Black Box

1.3.1 Definition of Black Box The so-called "black box" refers to a device or product whose internal structure and principles are unknown to users, who only care about its functions and how to use them[1] . Based on this definition, we provide the definition used in this scheme:

Definition 2: The internal structure of the black box is known only to its designer and no one else. During the sub-secret generation phase, the distributor inputs the master key K, participants input the number of sets t and the number of participants in each set n , and the black box generates t × n eigenvectors p , distributing these eigenvectors as sub-secrets to participants in each set. During the master key recovery phase, participants input their sub-keys p . If the input sub-secrets are authentic, the corresponding eigenvalues are obtained, thereby recovering the master key K; otherwise, the master key cannot be recovered.

1.3.2 Principle of Black Box

a) **Sub-secret generation phase** is designed according to Equation (3), i.e.:

$$A = P^{-1}\Lambda P \quad (3)$$

where: A is a randomly generated symmetric matrix; Λ is a diagonal matrix with eigenvalue as diagonal elements; the required sub-secret p is the eigenvector of matrix A.

b) **Master key recovery phase** is designed according to Equation (1), i.e.:

$$Ap = \lambda p$$

where: matrix A is the matrix generated during the sub-secret generation phase and stored in the black box. When participants input the correct sub-secret p, the black box outputs the corresponding eigenvalue . If an incorrect sub-secret is input, the eigenvalue cannot be obtained.

1.4 Cryptographic Knowledge

Definition 3: Secret Distributor. Refers to the person or device that distributes sub-secrets to n sharing participants. Their task also includes publishing corresponding auxiliary information on the bulletin board.

Definition 4: Secret Participant. Refers to a person or device who possesses a sub-secret and can obtain the shared secret through cooperation with a sufficient number of other participants.

Definition 5: Bulletin Board. A medium where the secret distributor publishes auxiliary information, such as a website. The bulletin board is writable only by the secret distributor and readable only by participants.

---

2 Shamir Threshold Scheme

In 1979, Shamir[1] proposed a (t, n) threshold scheme based on polynomial Lagrange interpolation, known as the Shamir threshold scheme or Lagrange interpolation method. The scheme is described in detail as follows:

a) Parameter Selection: Let the shared secret be K Z , select a prime p (p > n), with n participants, requiring at least t people to reconstruct the shared secret K.

b) Secret Distribution: First, randomly select t-1 distinct numbers, denoted as a , a , ···, a Z , to obtain the polynomial:

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{p}$$

This polynomial satisfies f(0) K (mod p). Second, select n different integers x (e.g., choose 1, 2, ···, n), and for each integer compute the pair (x , y), where y f(x) (mod p). Finally, the n pairs (x , y), i = 1, 2, ···, n are secretly transmitted to the n members, while the polynomial f(x) is kept confidential and can be destroyed.

c) Secret Recovery: Suppose t people jointly prepare to recover secret K, let their pairs be (x , y), (x , y), ···, (x , y). First, the t people compute the polynomial:

$$f(x) = \sum_{j=1}^{t} y_j \prod_{\substack{k=1 \\ k \neq j}}^{t} \frac{x - x_k}{x_j - x_k} \pmod{p}$$

Second, take the polynomial f(x), the desired secret is K = f(0).

---

3 Special Threshold Secret Sharing in the Black-Box Sense Based on Eigenvalues

Before presenting this threshold scheme, we provide an example. Three banks B , B , and B jointly manage a fund. The fund can only be used with the approval of executive directors from all three banks. Bank B has 3 executive directors, bank B has 4 executive directors, and bank B has 3 executive directors. In this example, each bank only needs to send any one executive director to decide on the use of the fund, resulting in $3 \times 4 \times 3 = 36$ decision-making combinations. From this, we define a new (t, n + n + ···+ n) threshold scheme.

Definition 6: Let B , B , ···, B be t sets of participants, where B B = (i j), |B | = n , |B | = n , ···, |B | = n , and n + n + ···+ n = n. Each participant in set B receives a secret pair (x , p) (1 j n), each participant in set B receives a secret pair (x , p) (1 j n), ···, and each participant in set B receives a secret pair (x , p) (1 j n). Each set must contribute at least one person to calculate the key K. Without the secret participants from any one set, the key K cannot be calculated.

3.2 Scheme Implementation

The proposed scheme consists of three parts: parameter assumptions, secret distribution, and secret recovery, described in detail as follows.

3.2.1 Parameter Assumptions Let there be a total of n secret participants (participant sets B , B , ···, B , with n , n , ···, n participants respectively), and let p (p > n) be a prime number. The secret distributor randomly selects t-1 numbers, denoted as a , a , ···, a Z , to obtain the polynomial:

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{p}$$

where the shared secret master key is K = f(0).

3.2.2 Secret Distribution First, the secret distributor selects t non-zero, distinct elements x Z and computes = f(x) (i = 1, 2, ···, t), obtaining t pairs (x ,). Since is the characteristic root corresponding to characteristic equation (1), there are n of , n of , ···, n of .

Second, the secret distributor randomly generates a sufficiently large n-order symmetric matrix A, thereby obtaining matrix Λ:

$$\Lambda = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_1 & & & \\ & & & \lambda_2 & & \\ & & & & \ddots & \\ & & & & & \lambda_t \end{pmatrix}$$

From linear algebra knowledge, matrices A and Λ have the same eigenvalues. By Corollary 1, each eigenvalue root corresponds to n linearly independent eigenvectors. Here, is used as the secondary master key. Where corresponds to eigenvectors p , p , ···, p , corresponds to eigenvectors p , p , ···, p , ···, corresponds to eigenvectors p , p , ···, p . The secret distributor distributes (x , p) as sub-keys to participants in different participation sets, where x is public and p is the private sub-key belonging to B .

3.2.3 Secret Recovery Due to the special nature of the threshold, the number of participants required to recover the secret must meet the requirement, i.e., not less than the threshold value t, meaning each participant set must contribute at least one person. Without loss of generality, assume one participant from B with sub-key (x , p), one from B with sub-key (x , p), ···, and one from B with sub-key (x , p) are recovering the secret.

First, each participant inputs their sub-secret p into the black box to obtain .

Second, substitute (x ,), (x ,), ···, (x ,) into f(x). Since f(x) is a t-1 degree curve, if t points are known, the curve can be expressed using the Lagrange interpolation formula:

$$f(x) = \sum_{k=1}^{t} \lambda_k l_k(x)$$

where:

$$l_k(x) = \begin{cases} 1 & \text{when } k = j \\ 0 & \text{when } k \neq j \end{cases}$$

The value at point 0 is the shared key:

$$K = f(0) = \sum_{k=1}^{t} \lambda_k \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{-x_j}{x_k - x_j} \pmod{p}$$

3.3 Black Box Implementation

3.3.1 Function Introduction The black box is the core of this scheme. To better understand the scheme, we detail the functions of the black box, whose functional structure is shown in Figure 1.

[Figure 1: see original paper]

The black box includes a sub-key generation unit and a master key recovery unit. The sub-key generation unit comprises modules for random numbers, random large primes, random symmetric matrix generation, polynomial generation, eigenvalue generation, n-order diagonal matrix Λ generation, and sub-secret generation. The master key recovery unit is relatively simple, consisting only of a key recovery module. Specific functions are as follows:

a) **Module 1—Random Numbers, Random Large Prime, Random Symmetric Matrix Generation Module.** Generates random numbers, random large primes, and random symmetric matrices according to instructions.

b) **Module 2—Polynomial Generation Module.** Generates polynomials based on generated random numbers, large primes, and the master key.

c) **Module 3—Eigenvalue Generation Module.** Generates eigenvalues corresponding to the generated random numbers x .

d) **Module 4—n-order Diagonal Matrix Λ Generation Module.** Generates n-order real symmetric matrices based on the number of sets t, the number of participants in each set n , and the corresponding eigenvalues .

e) **Module 5—Sub-secret Generation Module.** Using the symmetric matrix A generated by Module 1 and the diagonal matrix Λ generated by

Module 4, obtains matrix A = P ^{1}ΛP, thereby obtaining n eigenvectors p as sub-keys distributed to participants in each set.

f) **Module 6–Key K Recovery Module.** Participants from each set input their obtained sub-keys into the black box. If all participants input correct sub-keys, the secondary master key (i.e., eigenvalue) is obtained, thereby recovering the master key; otherwise, the master key cannot be recovered.

3.3.2 Function Implementation 1) Sub-key Distribution Process

a) **Generate Polynomial:** Based on the number of participant sets t, total number of participants n, Module 1 generates a random large prime p, t-1 random numbers a (i = 1, 2, ···, t-1), and sends them to Module 2. Simultaneously, the distributor inputs the master key K into Module 2, which together with the above data generates polynomial f(x) and sends it to Module 3.

b) **Generate Eigenvalues :** Module 1 generates t random numbers x (i = 1, 2, ···, t) and sends them to Module 3, obtaining t eigenvalues .

c) **Generate Diagonal Matrix Λ:** Module 4 generates an n-order diagonal matrix Λ based on the input number of sets t, the number of participants in each set n , and the corresponding eigenvalues .

d) **Generate Sub-secrets:** Module 5 uses the symmetric matrix A generated by Module 1 and the diagonal matrix Λ generated by Module 4 to obtain matrix A = P ^{1}ΛP, thereby obtaining n eigenvectors p as sub-keys distributed to participants.

2) Master Key Recovery Process: Participants from each set input their obtained sub-keys p into the black box. If all participants input correct sub-keys, the secondary master key is obtained, thereby recovering the master key; otherwise, the master key cannot be recovered.

3.3.3 Main Functional Program of Black Box

This black box is designed in the MATLAB language environment. The main functional programs are:

a) **Generate Large Prime p:**

```
psl = [10, 20];
asl = primes(psl(1));
bsl = primes(psl(2));
csl = setxor(asl, bsl);
msl = round(1 + (numel(csl) - 1) * rand());
p = csl(msl);
```

b) **Generate Random Numbers:**

```
function d = randnorepeat(m, n)
    p = randperm(n);
```

```
    d = p(1:m);
```

c) **Generate Random Symmetric Matrix:**

```
m = diag(Ei);
a = rand(n, n);
b = tril(a, -1) + triu(a', 0);
```

d) **Generate Polynomial:**

```
Ei = [];
for j = 1:t
    fx = K;
    fxy = K;
    xi = xii(1, j);
    fprintf('%d', xi)
    ni = input('Number of participants in corresponding set:');
    for i = 1:t-1
        fx = fx + a(1, i) * (x^(i));
        fxy = fxy + a(1, i) * (xi^(i));
    end
    for k = 1:ni
        Ei = [Ei, mod(fxy, p)];
    end
```

e) **Generate Matrix A:**

```
dm = b^-1 * m * b;
```

f) **Generate Sub-secrets:**

```
[V, D] = eig(dm);
for l = 1:n
    fprintf('Sub-secret obtained')
    V(:, l)
```

g) **Recover Master Key:**

```
fprintf('Please input obtained sub-secret')
pz = input('Number pz to input:')
la = pz^-1 * m * pz
```

---

4 Security Analysis

4.1 Correctness[1]

The correctness of this scheme is proven in two steps:

a) Proof that the polynomial constructed by t sets satisfies f(x) = .

Since the Lagrange interpolation polynomial:

$$l_k(x) = \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{x - x_j}{x_k - x_j}$$

contains a zero factor when k j, and equals 1 when k = j. The Lagrange interpolation polynomial:

$$f(x) = \sum_{k=1}^{t} \lambda_k l_k(x)$$

passes through points (x ,), (x ,), ···, (x ,). This means we know t linear equations f(x) = (i = 1, 2, ···, t) where (x ,) are known and the polynomial coefficients are unknown. This can be rewritten as:

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_t \end{pmatrix} \pmod{p}$$

The left matrix is a Vandermonde matrix whose determinant:

$$D = \prod_{1 \leq m < s \leq t} (x_s - x_m) \neq 0$$

Since x are distinct, D 0. By Cramer' s rule, the system has a unique solution. As we have already proven that polynomial f(x) is a solution, it follows that f(x) = . QED.

The correctness of this scheme is essentially built upon the correctness of Shamir' s threshold scheme.

b) Reconstructing the (t-1)-degree polynomial through points (x ,), (x ,), ···, (x ,). This means we know t linear equations where (x ,) are known and the coefficients are unknown. The proof above demonstrates that this scheme is a perfect ideal secret sharing scheme.

4.2 Attack Resistance

We analyze the security of the scheme in combination with possible attacks:

a) Attackers attempt to obtain (x ,) from (x , p) to recover secret K.

Analysis: Assuming the black box data cannot be cracked. If attackers only obtain (x , p) but cannot decrypt the black box, they only get sub-keys but

not eigenvalues , cannot obtain t equations, and cannot solve for K. Therefore, obtaining only (x , p) cannot crack key K.

b) Attackers forge and distribute incorrect sub-keys to participants.

Analysis: Sub-keys distributed to participants in the same set correspond to the same eigenvalue. Participants in the same set can verify their sub-keys in the black box. If the obtained eigenvalues are not identical, the system is under attack and accountability can be pursued; otherwise, the system is secure. Moreover, the application of the black box is an innovation of this scheme.

4.3 Perfection Proof

1) t-1 participants cannot recover key K.

Proof: Participants must solve for t unknowns through t-1 equations, with at least one free variable. The probability of obtaining the correct secret is at most 1/q, equivalent to brute force, so they cannot recover the secret. This proves the scheme is a perfect threshold secret sharing scheme.

2) Information Rate

Since a , a , ···, a , K are all randomly selected values from Z , the probability distributions of set B and sub-keys are uniform. Therefore, the information rate of the secret sharing scheme constructed by this method is:

$$\rho = \frac{H(K)}{\max_{i=1,\ldots,n} H(k_i)} = \frac{\log q}{\log q} = 1$$

5 Concrete Application of the Scheme

To illustrate the operability of the scheme, we provide the following example.

Example: Suppose there are 3 sets B , B , and B with 2, 3, and 2 secret participants respectively. Distribute keys to these 7 users and analyze the key reconstruction process.

1) Parameter Selection: The secret distributor randomly selects a 2-degree polynomial (t = 3):

$$f(x) = 3 + 2x + x^2 \pmod{17}$$

2) Secret Distribution: The secret distributor generates a random symmetric matrix A:

$$A = \begin{pmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 11 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 11 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 10 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 10 \end{pmatrix}$$

The generated matrix P:

$$P = \begin{pmatrix} 31469 & 28963 & 41119 & 80566 & 19616 & 17611 & 77466 \\ 47277 & 70287 & 82919 & 30016 & 53948 & 80280 & 53953 \\ 61415 & 89511 & 36717 & 85287 & 87421 & 21034 & 93478 \\ 53167 & 66136 & 14033 & 94625 & 16431 & 71292 & 91210 \\ 27241 & 18431 & 14910 & 01321 & 41647 & 55471 & 24822 \\ 84228 & 44227 & 11754 & 16895 & 93256 & 63184 & 11491 \end{pmatrix}$$

Matrix Λ:

$$\Lambda = P^{-1}AP = \begin{pmatrix} 36370 & 91168 & 11382 & 47126 & 48283 & 24813 & 37172 \\ 72987 & -47338 & 93191 & 32741 & 95329 & 23973 & 91433 \\ 46574 & 27125 & 34373 & -71063 & 86723 & 54824 & 65571 \\ 52513 & 09163 & 57932 & 46547 & 03229 & -35442 & 29491 \\ 60065 & 27833 & 36 & & & & \end{pmatrix}$$

The eigenvector corresponding to is:

$p_{11} = (12598, 17777, 04280, 11951, 02336, 51, -44993, 13951, 71315, 14454, 10813, 32578, 14259, 47832, 20769, 474$

The eigenvector corresponding to is:

$p_{21} = (-39928, 93685, 73011, 03349, 73431, 66471, 78517, 12346, 96289, 63411, 19805, 66196, 16177, 46647, 27702,$

The eigenvector corresponding to is:

$p_{31} = (21194, 49410, 16323, 15725, 85062, 22913, 15919, 45206, 62715, 32525, 93)$

The secret distributor distributes these 7 eigenvectors as sub-keys, obtaining 3 groups:

- **Group 1:** k = (1, p), k = (1, p)
- **Group 2:** k = (2, p), k = (2, p), k = (2, p)
- **Group 3:** k = (4, p), k = (4, p)

These three groups of sub-keys are distributed to secret participants in B , B , and B respectively.

3) Secret Recovery: Suppose one participant each from B , B , and B holding sub-keys k , k , and k want to recover the key. They first input their sub-keys into the black box to obtain:

$$\lambda_1 = f(1) = 6, \quad \lambda_2 = f(2) = 11, \quad \lambda_3 = f(4) = 10$$

Since there are 3 participants present, f(x) can be reconstructed:

$$f(x) = 6\frac{(x-2)(x-4)}{(1-2)(1-4)} + 11\frac{(x-1)(x-4)}{(2-1)(2-4)} + 10\frac{(x-1)(x-2)}{(4-1)(4-2)} \pmod{17}$$

Simplifying:

$$f(x) = 2(x-2)(x-4) - \frac{11}{2}(x-1)(x-4) + \frac{5}{3}(x-1)(x-2) \pmod{17}$$

After calculation:

$$f(x) = 3 + 2x + x^2 \pmod{17}$$

Thus, the shared key is obtained: K = f(0) = 3.

---

6 Conclusion

This paper proposes for the first time a new secret sharing scheme based on eigenvalues of special symmetric matrices. Multiple participants in one set correspond to the same eigenvalue. One secret is shared among t participants from t sets, and only when participants from all sets participate in key recovery can the key be recovered. Simultaneously, this scheme utilizes a black box to implement sub-secret generation and master key recovery, providing reference value for both theoretical and engineering applications.

References

[1] Shamir A. How to share a secret [J]. Comm ACM, 1979, 22(11): 612-613.
[2] Blakley G R. Safeguarding cryptographic keys [C]// Proc of IEEE Computer Society, 1979: 313-317.
[3] Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure [J]. Electronics & Communications in Japan, 1989, 72(9): 56-64.
[4] Laih C S, Harn L, Lee J Y, et al. Dynamic threshold scheme based on the definition of cross-product in an N-dimensional linear space [C]// Advances in Cryptology. New York: Springer-Verlag, 1989: 286-298.
[5] Traverso G, Demirel D, Buchmann J. Dynamic and verifiable hierarchical secret sharing [C]// Proc of International Conference on Information Theoretic Security. Springer, 2016: 24-43.
[6] Zarepour-Ahmadabadi J, Shiri-Ahmadabadi M E, Miri A, et al. A new gradual secret sharing scheme with diverse access structure [J]. Wireless Personal Communications, 2018(2): 1-16.
[7] Yang S, Wu H, Li J. Access structures of hyperelliptic secret sharing schemes [J]. Finite Fields & Their Applications, 2016, 37: 46-53.
[8] Binu V P, Sreekumar A. Secure and efficient secret sharing scheme with general access structures based on elliptic curve and pairing [J]. Wireless Personal Communications, 2017, 92(4): 1531-1543.
[9] Jarecki S, Kiayias A, Krawczyk H. Round-optimal password-protected secret sharing and T-PAKE in the password-only model [C]// Advances in Cryptology -ASIACRYPT 2014. Berlin: Springer, 2014: 233-253.
[10] Pilaram H, Eghlidos T. An efficient lattice based multi-stage secret sharing scheme [J]. IEEE Trans on Dependable & Secure Computing, 2017, 14(1):
[11] Sarkar P, Nandi S, Chowdhury M U. Publicly verifiable secret sharing scheme in hierarchical settings using CLSC over IBC [C]// Proc of International Conference on Applications and Techniques in Cyber Security and Intelligence. 2017: 194-205.
[12] Wang N, Fu J, Zeng J. Verifiable secret sharing scheme without dealer based on vector space access structures over bilinear groups [J]. Electronics Letters, 2018, 54(2): 77-79.
[13] 同济大学数学系编. 工程数学线性代数 [M]. 北京: 高等教育出版社, 2014: 124-128. (School of Mathematic Sciences, Tongji University. Engineering mathematics, linear algebra [M]. Beijing: Higher Education Press, 2014: 124-128.)
[14] 曹尔强, 张沂, 曹晔, 潘继宏. “软件黑盒子”文件加锁和加密的一个方法 [J]. 长春邮电学院学报, 1991(3): 11-14. (Cao Erqiang, Zhang Yi, Cao Ye, et al. A technique of locking a disk and secreting a whole disk [J]. Journal of Changchun Post & Telecommunication Institute, 1991(3): 11-14.)
[15] 谷利泽, 郑世慧, 杨义先, 等. 现代密码学教程 [M]. 北京: 北京邮电大学出版社, 2009: 338-341. (Gu Lize, Zheng Shihui, Yang Yixian, et al. Modern cryptography course [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2009: 338-341.)

Note: Figure translations are in progress. See original paper for figures.