Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/88/20241746

A review of research on secret sharing

Ruoying Chen

Southwest University, Chongqing, 400715, China

swucry@126.com

Abstract. This article explores the importance and challenges of secret sharing technology in the context of rapid advancements in information technology. With increasing attention on data security and privacy protection, secret sharing serves as a key cryptographic technique that ensures secure data transmission, storage, and multi-party computation by dividing secrets into multiple shares. However, existing solutions encounter performance bottlenecks when dealing with large-scale datasets, managing share updates in dynamic environments, and facing quantum computing threats. This article systematically summarizes the basic concepts, theories, classifications, and characteristics of secret sharing while analyzing its applications in financial security, medical privacy, and other fields. Furthermore, it presents recent research progress on dynamic secret sharing and anti-quantum secret sharing. The findings indicate that dynamic secret sharing schemes improve long-term key storage security, while anti-quantum secret sharing provides a solution to counteract quantum computing threats. This study not only deepens understanding of secret sharing technology but also offers insights for future research directions, significantly contributing to enhancing data protection levels.

Keywords: Secret sharing, classification, application, latest progress.

1. Introduction

With the rapid development of information technology, data security and privacy protection have become the focus of attention in today's society. Secret sharing is a key technology in the field of cryptography, allowing a secret to be divided into multiple shares. These shares individually do not contain any information about the original secret, and only when enough shares are combined can the original secret be recovered. This technology plays an important role in ensuring the security of data transmission, promoting the reliability of distributed storage systems, and enhancing the privacy of multiparty computation [1]. Although the secret sharing technology has made significant progress over the past few decades, such as Shamir's threshold scheme and the secret sharing system of Blakley, there are still some research gaps in this field. For example, the existing scheme may encounter performance bottlenecks when dealing with large-scale datasets, and there are still challenges in updating and managing shares in the dynamic environment. In addition, with the rise of quantum computing, the security of the existing secret sharing scheme has also attracted people's attention when facing quantum attacks. This paper will systematically sort out and evaluate the existing literature through the method of literature review, mainly focusing on its basic concepts and theories, classifications and characteristics, applications in various fields, and recent new developments and research directions, aiming to provide predictions for the future development direction of secret

DOI: 10.54254/2755-2721/88/20241746

sharing technology through in-depth analysis of existing technologies and discussion of potential problems, and to provide reference for researchers and practitioners in related fields.

2. Basic concepts and theories of secret sharing

2.1. Origin and development

Shamir proposed the concept of secret sharing based on the Lagrange interpolation polynomial in 1979 and constructed the threshold secret sharing scheme [2-3]. The core principle is to cut the input data of each participant into multiple shards, and then these shards are assigned to all participants for proper preservation.Secret sharing is an important technique in secure multiparty computation. Such a design ensures that only when these entities that have been grasped by the segment can successfully restore the original keys. This technology is important in security and the application of key management.

With the development of technology, there are many different schemes in the field of secret sharing, including the Blakley solution and the Brickell solution based on hyperplane geometry, the secret sharing scheme based on the Chinese Remainder Theorem (CRT-BASED), and so on [4-6]. These schemes have their own characteristics in terms of secret distribution and reconstruction. For example, Blakley constructs a threshold secret sharing mechanism through multidimensional Euclidean space and uses hyperplane geometry principles to achieve secret segmentation and reconstruction. The Brickell scheme is similar to the Blakley scheme but uses vectorial methods to improve information rate through matrix operations, making secret sharing more efficient.

2.2. Theoretical basis

2.2.1. Polynomial theorem. The polynomial theorem is also known as the polynomial coefficient formula, which was first discovered by German mathematician Leibniz.In secret sharing, the polynomial theorem is used to construct and share secrets. Each participant obtains a polynomial coefficient. By collecting enough information shared by participants, the original secret can be reconstructed. The content of the theorem is as follows:

If n is a positive integer, the formula contained t real numbers $x_1, x_2, \ldots \ldots x_t$ is shown in Eq. (1) [7]:

$$(x_1 + x_2 + \cdots x_t)^n = \sum_{n_i \geq 0, n_1+n_2+\cdots+n_t=n} \binom{n}{n_1, n_2, \cdots, n_t} \prod_{1 \leq i \leq t} x_i^{n_i} \tag{1}$$

where $\binom{n}{n_1, n_2, \cdots, n_t} = \frac{n!}{n_1! n_2! \cdots n_{t!}}$

In the Shamir secret sharing scheme, polynomial theory is used to construct a mathematical model that encodes secret information into a polynomial f (x), where the constant term S of the polynomial is the secret that needs to be shared.

2.2.2. Lagrange interpolation. The basic idea of Lagrange interpolation is to give a polynomial that exactly passes through several known points on a two-dimensional plane and use the polynomial with the minimum degree to construct a smooth curve that passes through all known points. For n known points in a plane (any two points are not on a straight line), an n-1 degree polynomial can be found in Eq.(2):

$$f(x) = a_0 + a_1 x + a_2 x^2 \cdots a_{n-1} x^{n-1} \tag{2}$$

This polynomial curve passes through all points and is called the Lagrange polynomial. By substituting the coordinates of these n points into the polynomial, the Lagrange interpolation polynomial is solved and shown in Eq.(3) [8]:

$$L(x) = \sum_{i=0}^{n} y_i \prod_{j=0, j \neq i}^{n} \frac{x - x_j}{x_i - x_j} \tag{3}$$

DOI: 10.54254/2755-2721/88/20241746

The role of Lagrange interpolation in secret sharing is to achieve distributed storage and threshold recovery of secrets through a mathematically rigorous method, ensuring that the original secret can only be reconstructed when a sufficient number of participants cooperate.

3. Classification and characteristics of secret sharing schemes

3.1. Multi-threshold secret sharing scheme

Although the Shamir threshold scheme can effectively share secrets, it still has the following drawbacks: Running the scheme once can only share one secret. Once the secret is reconstructed or updated, the secret distributor must redistribute the secret share [9]. In addition, if a malicious member provides forged secret shares to other members, only he can reconstruct the true secret. To address the above issues, Liu proposed a new dynamic (t, n) threshold multi-secret sharing scheme based on one-way functions and large integer factorization problems [10]. This section will provide a brief introduction to the scheme.

3.1.1. System initialization. The secret distributor (dealer, D) first creates a bulletin board to provide necessary public parameters to system members. Each member can access the parameters in the bulletin board, but only D can change or refresh the content in the bulletin board. Afterwards, D defines the following parameters according to the RSA algorithm: $p = 2p' + 1, q = 2q' + 1$,and $n = pq$. p,q,p′,q′ are all prime numbers [11]. e,d is the public key and private key, respectively, with $ed = 1 \bmod \varphi_{(n)}$. H is a secure one-way function on $Z^*_{\varphi_{(n)}}$. Finally, Make (e, n) public and keep the rest confidential.

3.1.2. Generation of secret shares. Assuming $U = \{U_1, U_2, \cdots U_n\}$ is a set of n participants, $S = \{S_1, S_2, \cdots S_m\}$ is a set of m secrets to be shared, and ID_i is the identity of $U_i (i = 1,2, \cdots n)$. The generation algorithm is as follows:

D randomly selects a t-1 power polynomial as Eq.(4):

$$f(x) = a_0 + a_1 x + a_2 x^2 \cdots a_{t-1} x^{t-1} \bmod \varphi_{(n)} \tag{4}$$

where $a_k \in Z^*_{\varphi_{(n)}} (k = 0,1, \cdots t\text{-}1)$.

Then, calculate the secret share of U_i using Eq.(5):

$$x_i = f(ID_i) dp_i^{-1} \bmod \varphi_{(n)} \tag{5}$$

where $p_i = \prod_{U_k \in U, U_k \neq U_i} (ID_i - ID_k) \bmod \varphi_{(n)}$.

3.1.3. Generation of secret promise. D needs to calculate the commitment value $h_1, h_2, \cdots h_m$ for each secret $S_1, S_2, \cdots S_m \in S$ to be shared: randomly select r different integers $r_1, r_2, \cdots r_m \in Z^*_{\varphi_{(n)}}$, calculate $C_j = dr_j \bmod \varphi_{(n)}$, and $h_j = S_j \oplus H(a_0 C_j \bmod \varphi_{(n)})$, where $j = 1,2, \cdots, m$, and publish $\{r_j, C_j, h_j\}$ on the bulletin board.

3.1.4. Secret recovery. Let *Y* be an access structure for participants in *U*, where ($|Y| = t \leq n$) [12]. That means when t participants aggregate together to cooperate, the secret $S_j \in S$ can be reconstructed. Participant U_i obtains $\{r_j, C_j, h_j\}$ of S_j from the bulletin board, calculates and publishes $A_{ij} \equiv x_i C_j \bmod \varphi_{(n)}$ using the secret share x_i.Any member in the access structure *Y* can recover the secret using Eq.(6):

$$S_j = h_j \oplus H(e \sum_{i=1}^{t-1} (A_{ij} \Delta_i \bmod \varphi_{(n)})) \tag{6}$$

where $\Delta_i = \left[\prod_{U_k \in U, U_k \neq U_i} (-ID_k)\right]\left[\prod_{U_k \in U, U_k \notin Y} (ID_i - ID_k)\right]$.

DOI: 10.54254/2755-2721/88/20241746

In this scheme, each member only needs to hold one reusable secret share to participate in the sharing and recovery of multiple secrets, significantly reducing computing and storage requirements. In addition, the solution also includes an effective fraud detection mechanism to ensure the integrity and reliability of the system, suitable for various high security application scenarios.

3.2. Verifiable secret sharing scheme without trusted center

A known secret sharing scheme typically consists of a secret distributor, also known as a trusted center D, a key set S, a set of key share owners n, an access structure Y that meets decryption requirements, a key allocation algorithm, and a share synthesis algorithm. For the traditional Shamir (t, n) threshold secret sharing scheme, if the secret distributor is artificially involved in distributing secret shares and engages in cheating behavior, causing the trusted center to lose credibility, it will endanger the security of the entire scheme and be unverifiable. Huang proposed a verifiable (t, n) threshold secret sharing scheme without a trusted center based on discrete logarithms using binary polynomials [13]. This section provides a brief introduction to this scheme.

3.2.1. Parameter generation. This scheme exists on a finite field $GF(p)$, and the large prime number p should satisfy the setting in discrete logarithms. Assuming there are n users $U_1, U_2, \cdots U_n$, then select the generator $a \in GF(p)$, and each user $U_i (i = 1,2, \cdots n)$ performs the following operations:

Secretly select and save a binary polynomial shown in Eq.(7):

$$f_i(x,y) = a^i_{00} + a^i_{10}x + a^i_{20}x^2 + \cdots + a^i_{(t-1)0}x^{t-1} + a^i_{01}y + a^i_{11}xy + a^i_{21}x^2y + \cdots + a^i_{(t-1)1}x^{t-1}y + \cdots + a^i_{(t-1)t}y^{(t-1)} + a^i_{1(t-1)}xy^{(t-1)} + \cdots + a^i_{(t-1)(t-1)}x^{(t-1)}y^{(t-1)} \quad (7)$$

Select and publish a one-way trapdoor function $h_i(x)$

Publicize self-identity $ID_i \in GF(p)$ to the public.

Calculate and publicly publicize the Eq.(8):

$$A_i = a^{a^i_{00}} (\mathrm{mod}\ p) \quad (8)$$

3.2.2. Key share generation. Each user $U_i (i = 1,2, \cdots n)$ continues with the following actions:

Calculate $f_i(ID_j, 0)$ using a binary polynomial for the j-th user U_j,where $j \in \{1,2, \cdots, n\}, j \neq i$.

For the j-th user U_j, use a one-way trapdoor function to calculate $h_i(f_i(ID_j, 0))$ and send it to other users, where $j \in \{1,2, \cdots, n\}, j \neq i$.

Generate user's own share and save it using Eq.(9):

$$S_i = \sum_{j=1}^{n} f_j(ID_i, 0) \bmod p \quad (9)$$

3.2.3. Key synthesis. Assuming that among n users, any t users can collaborate to synthesize a secret key. They can use (ID_{i_m}, S_{i_m}) stored in their hands, where $m = 1,2, \cdots, t$, to synthesize the polynomial Eq.(10):

$$G(x) = \sum_{m=1}^{t} S_{i_m} \prod_{r=1, r\neq m}^{t} \left(\frac{x - ID_{i_r}}{ID_{i_m} - ID_{i_r}}\right) \bmod p \quad (10)$$

According to this formula, the key S can be calculated. Compared with existing schemes, this scheme completely eliminates the dependence on trusted centers, achieves user-generated key shares, and effectively avoids the potential fraud risks of trusted centers. Meanwhile, after key synthesis, efficient cheating verification can be carried out to ensure the integrity and credibility of the data.

4. The application of secret sharing in various fields

In the process of financial transactions, multi-factor authentication is an important means to ensure transaction security. Secret sharing can be combined with multi-factor authentication, where different authentication factors (such as passwords, phone verification codes, biometric features, etc.) can be

DOI: 10.54254/2755-2721/88/20241746

considered as secret shares, and authentication and transactions can only be completed when all factors are met. And during remote authentication, users can prove their identity by providing multiple authentication factors, thereby enhancing the security of remote access. In real life, banks are financial institutions that frequently use this authentication, and users often need to enter passwords and perform facial recognition when logging into online app interfaces.

The secret sharing scheme plays a crucial role in cross-border payments and settlements. By segmenting and storing sensitive data in multiple financial institutions, combined with strict access control and identity verification mechanisms, it effectively prevents data leakage and fraudulent behavior, reduces transaction costs and risks, and improves the efficiency and reliability of cross-border financial transactions.

Besides, when conducting joint statistical analysis, medical institutions do not need to directly exchange raw data. They only need to calculate based on their respective holdings and share the calculation results (such as model parameters, etc.). These statistical values can be used to construct an overall analysis model without exposing individual data. For example, by sending the modulus of polynomial coefficients as a promise, the other party can verify it by sharing the value and promise. Thus, all parties can confirm the correctness of the calculation results without exposing specific input data.

5. The latest research progress

The dynamic secret sharing scheme aims to solve the security issue of long-term storage of secret sharing schemes without changing the secret [14]. It periodically replaces key shards, so that after each key shard replacement, the information obtained by the attacker in the previous cycle is completely invalidated [15]. Therefore, the length of the sub-secret replacement cycle can be determined according to the degree of possible attack on the key. In addition, dynamic secret sharing must meet the requirement that the information contained in expired subsecrets will not have an unsafe impact on the construction (or recovery) of future secrets.

Amir Herzberg first proposed the Amir Herzberg scheme in 1995, which added a key shard update protocol based on the Shamir scheme, that is, sub-secret updates must be performed at the beginning of each time period. After entering the k-th time period, the sub-secrets held by the user U_i need to be updated from $S_i^{k-1} = f^{k-1}(i)$ to $s_j^k(x) = s_j^{k-1}(x) + \sum_{i=0}^{n} \delta_{ij}$ as new key shards, where $\delta_{ij}^k = h_i^k(j) \bmod q$ and $h_i^k(j)$ are derived from the constructed polynomial $h_i^k(x)$.

The dynamic secret sharing scheme can effectively improve the security of long-period keys.

Anti-quantum secret sharing is a novel encryption method based on post-quantum cryptography aimed at addressing the threat posed by quantum computing to traditional encryption algorithms. In the current context of quantum computing development, traditional discrete logarithm and large integer factorization problems may be quickly solved by quantum algorithms such as Shor's algorithm, making traditional public key encryption algorithms insecure (such as RSA). To address this challenge, researchers have proposed various anti quantum secret sharing schemes. One important method is the verifiable secret sharing scheme based on lattices. Compared with traditional solutions based on discrete logarithm problems, lattice-based solutions have higher computational efficiency and resistance to quantum attacks [16]. In addition, the lattice-based verifiable secret sharing scheme also has the feature of unconditional security, even if the lattice problem is solved, the process of verifying sub-shares will not explore any secret information.

6. Conclusion

This article delves into the key role of secret sharing technology in password security and privacy protection, systematically reviewing the basic concepts, classifications, characteristics, and applications of secret sharing in fields such as financial security and medical privacy. Through the literature review, this article briefly explains the principles of two advanced secret sharing schemes based on the Shamir threshold scheme and emphasizes the importance of secret sharing in the fields of finance and healthcare. However, this article also has some shortcomings. Firstly, regarding the latest

DOI: 10.54254/2755-2721/88/20241746

research progress on secret sharing technology, although dynamic secret sharing and anti quantum secret sharing are mentioned, the specific implementation details and performance evaluation of these technologies have not been discussed in detail. Secondly, this article does not emphasize the importance of combining blockchain and multi-party computing when predicting future research directions, and lacks specific case studies and empirical research to support this viewpoint. In order to improve this article, future research can further explore the specific implementation mechanisms of dynamic secret sharing and anti-quantum secret sharing, and evaluate their performance and security in practical applications. At the same time, practical cases can be combined to analyze the combined application of secret sharing technology with blockchain, multi-party computing and other technologies, providing more detailed and powerful support for the future development of secret sharing technology. In addition, with the continuous development of quantum computing technology, studying the long-term security, and stability of anti-quantum secret sharing technology will also become an important research direction in the future.

References

[1] Yanhong, Liu. (2012). Analysis and Design of Verifiable Secret Sharing Schemes without Secret Channels. Master's thesis, Nanjing Normal University, 2.
[2] Shamir A. How to share a secret[.Communications ofthe ACM, 1979, 22(11): 612-613.
[3] Chao, Xue. (2020). Research on Secure Cloud Storage Scheme Based on Secret Sharing. Master's thesis, Shaanxi University of Science & Technology, 16.
[4] Blakley G. Safeguarding cryptographic keys[C]. AFIPS ,79 National Computer Conference, 1979: 313-317.
[5] E.F.BRICKELL. Some ideal secret sharing schemes. Journal of Combinatorial Mathematics and Combinatorial Computing, 9(1989), 105-113.
[6] Li Lele, Han Zhaowei, Li Zhihui, Guan Feiting & Zhang Li. (2024). Authenticable dynamic quantum multi-secret sharing based on the Chinese remainder theorem. Quantum Information Processing 2.
[7] Qiqi Wu. (2012). New Proof and Expansion of Polynomial Theorem. Journal of Foshan University of Science and Technology (Natural Science Edition), (06): 24-32.
[8] Li Zhao, Na Sun, Liping Li&Jie Cui. (2022). Application of Lagrange Interpolation Method in Data Cleaning. Journal of Liaoning University of Technology (Natural Science Edition), (02): 102-105+117.
[9] Zhenyuan Zuo&Qi Xie. (2008). Analysis of a Dynamic (t, n) Threshold Multi Secret Sharing Scheme. Journal of Hangzhou Normal University (Natural Science Edition), (06): 430-432.
[10] Feng Liu, Yefeng He & Xuehan Cheng. (2008). Dynamic (t, n) threshold multi secret sharing scheme. Computer Application Research, (01): 241-242+245.
[11] Zhen Guo & Jianzhong Zhang. (2010). A dynamic multi secret sharing scheme for fraud prevention based on RSA. Computer Engineering and Applications, (12): 97-98+102.
[12] Jianzhong Zhang & Juan Qu. (2010). Weakness analysis and improvement of three secret sharing schemes. Computer Engineering, (07): 126-128.
[13] Kehua Huang & Hefeng Chen. (2020). A verifiable secret sharing scheme without a trusted center. Journal of Ludong University (Natural Science Edition), (03): 220-223+264.
[14] Chungen Xu, Yanjiong Yang, Bennian Dou & Mou Han. (2009). Dynamic Secret Sharing Scheme with (t, n) Threshold. Computer Engineering and Applications, (22): 66-67+171.
[15] Zhenjun Ye. (2008). Research on Financial Information Security: Models, Solutions, and Management Strategies. Doctor's thesis, Tianjin University, 32.
[16] Yong Peng, Peinan Shao, Xiang Li, Jianfeng Bai & Keju Meng. (2020). Lattice based verifiable secret sharing scheme. Computer Systems & Applications, (01): 225-230.