Lattice-Based Secret Sharing Scheme (Chinese Remainder Theorem)

Songshou Dong[1,2,3], Yanqing Yao[1,2,3(✉)], Yihua Zhou[4,5], and Yuguang Yang[4,5]

[1] State Key Laboratory of Software Development Environment, Beihang University, Beijing 100191, China
yaoyq@buaa.edu.cn
[2] State Key Laboratory of Cryptology, Beijing 100878, China
[3] Key Laboratory of Aerospace Network Security, Ministry of Industry and Information Technology, School of Cyber Science and Technology, Beihang University, Beijing 100191, China
[4] Faculty of Information Technology, Beijing University of Technology, Bejing 100124, China
{zhouyh,yangyang7357}@bjut.edu.cn
[5] Beijing Key Laboratory of Trusted Computing, Beijing 100124, China

Abstract. Secret sharing schemes are used as a tool in many cryptographic protocols including revocable electronic cash, electronic voting, cloud computing and key management in sensor networks. But the existing post-quantum secret sharing schemes are all based on Shamir's (t, n) threshold scheme, there is currently no post-quantum secret sharing scheme based on the Chinese Remainder Theorem (CRT), so we construct a verifiable lattice-based secret sharing scheme using some number theory methods and interaction methods. Furthermore, we prove our scheme is safe in the post-quantum era. Finally, we compare our scheme with other schemes. And the comparison shows that our scheme is more efficient and occupies less memory.

Keywords: Chinese remainder theorem · secret sharing · lattice · post-quantum · verifiable

1 Introduction

Secret sharing is an important means in information security and data confidentiality. In 1979, its concept was first proposed by Shamir [1] and Beimel [2]. It refers to dividing the secret s into several shares and distributing them among a group of participants $P = \{P_1, P_1, \cdots, P_n\}$, so that each participant gets a secret share about the secret s, and only P's some specific subsets (called qualified subsets or authorized subsets) can effectively recover s, while other subsets of P (non-qualified subsets) cannot effectively recover s, or even get any useful information about the secret s.

A secret sharing system, consists of secret distributors, participant set P, access structure Γ, secret space S, share space T, distribution algorithm, recovery algorithm, and so on. The secret space gives the value range of the secret: the set of participants

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 571, pp. 54–62, 2024.
https://doi.org/10.1007/978-3-031-56583-0_4

gives the members who participate in the secret sharing; the access structure Γ points out which participants can recover the secret together, and Γ has properties: if $A \in \Gamma$ and $A \subset B$, then $B \in \Gamma$; the share space gives the value range of the secret share; the distribution algorithm gives the probability polynomial time algorithm for generating the secret share from the secret; the recovery algorithm is deterministic. The subset of P in the access structure is called a qualified subset. According to the containment relationship, the minimal element in Γ is called the minimum qualified subset, and Γ is uniquely determined by its minimal element set Γ_0, and Γ_0 is called the basis of Γ. A secret-sharing scheme is said to be complete if all non-qualified subsets do not have any information about the secret s. We call $\rho = \log|T|/\log|S|$ the information rate of a secret sharing scheme. A secret sharing scheme is said to be ideal if its information rate is 1.

The threshold method is the most common in secret sharing systems. There are many threshold systems proposed, among which Shamir's Lagrange interpolation polynomial method [1], Blakley's vector method [3], Asmuth et al.'s congruence class method [4, 5], and Karnin's matrix method [6] are the main representatives, and these have been widely used. There are two main problems [7–25] in the usual secret sharing scheme: one is that it cannot resist the sharer's cheating well, that is, some sharers will provide false shares when recovering the secret, so some members of the qualified subset cannot recover the correct share. Second, it cannot effectively prevent distributors from cheating, that is, distributors may distribute false shares to some sharers when distributing secret shares. To solve these problems, Chor et al. [7] proposed the concept of verifiable secret sharing. The verifiable secret sharing scheme is composed of an additional verification algorithm based on the usual secret sharing scheme. A verifiable secret sharing scheme is a basic tool for designing multi-party security protocols. It has been widely used in many aspects such as multi-party secure computing, group-oriented cryptosystem, key escrow system, and electronic commerce. In the verifiable secret sharing scheme, the sharer can check whether the secret share he receives is valid (whether it is compatible with other shares) through the verification algorithm. Let $P_1, P_2, \ldots, P_n$ be the sharers, s is the secret to be shared, and the access structure is Γ, then the verification algorithm satisfies

$$\exists u \forall A \in \Gamma : (\forall P_i \in A : Verify(s_i = 1) \rightarrow Rcover(\{s_i; P_i \in A\}) = u$$

When the distributor is honest, $u = s$. If there is no need to exchange information between sharers or between sharer and distributor when running the verification algorithm, the corresponding verifiable secret sharing scheme is called non-interactive. The first verifiable secret sharing scheme is interactive, and Benloh [26] gave the first non-interactive verifiable secret sharing scheme, but this scheme has a trusted center. Afterwards, Feldman [12], Pedersen [13] and others successively proposed some non-interactive verifiable secret sharing schemes that do not require the trusted center. Lin et al. [10] proposed a verifiable multiple secret sharing scheme. In the usual verifiable secret sharing scheme, only the sharer himself can verify the validity of the shares he gets, which limits the verifiability greatly. To solve this problem, Stadler [23] further proposed the concept of publicly verifiable secret sharing. In a publicly verifiable secret sharing scheme, the verifier can verify the correctness of the distribution of the secret share, and the sharer can verify the validity of the shares held by himself. Stadler [23]

gave two publicly verifiable secret sharing schemes, Fuiisaki et al. [24] gave a practical provably secure publicly verifiable secret sharing scheme and its application. In these schemes, the verification algorithm relies on tools such as public key encryption and zero-knowledge proof, and the structure is relatively complex, so the efficiency is not ideal.

According to Ref. [17], a verifiable secret sharing scheme must satisfy the following two security properties:

1) If the distributor is honest, the share distribution process will always succeed, and the attacker (including the malicious sharer) will not get any information about the shared secret during the share distribution process. During the recovery process, no matter how the attacker behaves, the honest sharer can always recover the shared secret correctly.
2) If the distributor is colluded by the attacker (distributor is malicious), then either the malicious behavior of the distributor is discovered by the honest sharers, causing all honest sharers to withdraw from the share distribution process; or the distribution process is accepted by the honest sharer, as a result of the distribution process, a certain secret is uniquely fixed by the information held by the honest sharer, and during the recovery process, the honest sharer is able to reconstruct the secret.

The present secret sharing scheme based on classical number theory problem is threatened by quantum computer. Lattice structure is considered to be resistant to attacks by quantum computers. In recent years, some sharing schemes based on lattice secrets have been put forward [27–36]. In 2015, Pilaram et al. [34] proposed a lattice based (t, n) threshold multi-stage secret sharing (MSSS) scheme according to Ajtai's construction for one-way functions. The principle of his scheme is based on Shamir's secret sharing method. In 2022, Yang et al. [35] pointed out that there were loopholes in Pilaram et al. [34]'s scheme and proposed a filling method. In the same year, Kiamari et al. [36] proposed a non-interactive verifiable LWE-based multi secret sharing scheme. It is the first LWE based threshold multi secret sharing scheme that has formal security in the standard model.

But none of them are constructed based on the Chinese remainder theorem (CRT), and there are some security and efficiency issues. Therefore, we construct a verifiable secret sharing scheme based on the CRT that is secure in the post-quantum era. Our contributions are as follows:

1) We use number theory knowledge and interaction method to propose a post-quantum secure verifiable secret sharing scheme based on the CRT, which makes the post-quantum secret sharing scheme based on the CRT one more alternative;
2) We analyzed the security of our scheme and compared it with other schemes;

2 Preliminaries

2.1 Notations

Table 1 describes some system parameter notations needed by our scheme.

Table 1. System parameter notations

Notation	Description
n	Total number of people
$p_1, p_2, \cdots, p_n$	n primes which satisfied $p_1 < p_2 < \cdots < p_n$
ϕ	Empty set
$\Lambda, \Lambda_1, \Lambda_2, \cdots, \Lambda_n$	Lattice $\Lambda_1 = p_1 Z^n$, $\Lambda_2 = p_2 Z^n, \cdots, \Lambda_n = p_n Z^n$, $p_1 Z^n \cap p_2 Z^n \cap \cdots \cap p_n Z^n = p_1 p_2 \cdots p_n Z^n \neq \varnothing$
t	Threshold size
s	Secret value
m	The size of matrix
ϕ	Empty set
σ	Gaussian parameter
$D_{\Lambda,\sigma,v}(\cdot)$	Discrete Gaussian distribution
$\|\cdot\|$	l_2 norm
log	The logarithm based on 2
O and ω	the growth of functions

2.2 Algorithm Model and Security Model

1) Secret Sharing

A secret sharing scheme is a method of sharing secrets among a set of parties called participants. A trusted third party, called a dealer, assigns a private value (called a share), to each participant. Only the authorized subset of the participant can recover the secret by running a pre-specified algorithm. The set of all authorization subsets is called the access structure. In general, the access structure is a subset of the power set of participants.

A concrete instance of a general access structure is the threshold structure. A (t, n) threshold secret sharing scheme is called perfect if less than t participants cannot obtain information about the secret. A secret sharing scheme is said to be ideal when the entropy of each share is equal to the entropy of the secret.

A secret sharing scheme usually consists of two phases:

(1) Share distribution: In this phase, the dealer computes the shares using a prespecified algorithm and sends them securely to the participants.
(2) Secret reconstruction: In this phase, the authorized subsets of participants send their shares to a combiner to recover the secret by running the algorithm.

2) Security Requirements

Each secret can only be recovered by any t or more participants who receive shares, and fewer than t participants cannot get any information about the secret.

2.3 Lattice

Lattice [37]: $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$ are n linearly independent vectors in R^n, let $\boldsymbol{B} = [\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n]$, $\Lambda(\boldsymbol{B}) = \{\boldsymbol{Bc} = \sum_{i=1}^{n} \boldsymbol{b_i c_i} | \boldsymbol{c} \in \mathrm{Z}^n\}$ represent the n-dimensional lattice Λ generated by the basis $\boldsymbol{B}$, where $\boldsymbol{B}$ is a basis of the lattice $\Lambda^{\perp}(\boldsymbol{B})$. The orthogonal lattice $\Lambda^{\perp}(\boldsymbol{B}) = \{\boldsymbol{e} \in \mathrm{R}^m | \boldsymbol{Be} = \boldsymbol{0} \bmod q, \boldsymbol{B} \in \mathrm{R}_q^{n \times m}\}$.

Discrete Gaussian Distribution [37]: For any $\sigma > 0$ and $\boldsymbol{x} \in \mathrm{R}^{\mathrm{m}}$, the discrete Gaussian distribution with σ as the parameter and $\boldsymbol{v} \in \mathrm{R}^{\mathrm{m}}$ as the center is defined as $\rho_{\boldsymbol{v},\sigma}(\boldsymbol{x}) = \exp(-\pi \|\boldsymbol{x} - \boldsymbol{v}\|^2 / \sigma^2)$.

The discrete Gaussian distribution on lattice $\Lambda \subseteq \mathrm{Z}^m$ is defined as $\forall \boldsymbol{x} \in \Lambda$, $\mathrm{D}_{\Lambda,\sigma,v}(x) = \rho_{\sigma,v}(\boldsymbol{x}) / \rho_{\sigma,v}(\Lambda)$, where $\rho_{\sigma,v}(\Lambda) = \sum_{\mathrm{z} \in \Lambda} \rho_{\sigma,v}(z)$.

In particular, when representing a Gaussian distribution centered at 0, we often omit 0.

Intersection Method [38]: Λ_1 and Λ_2 are two lattices such that $\Lambda_1 + \Lambda_2 = Z^m$ and $\Lambda_1 \bigcap \Lambda_2 \neq \phi$; here, the addition is elementwise. For $\boldsymbol{v}_1, \boldsymbol{v}_2 \in Z^m$, which provide two co-sets Λ_1 and Λ_2, a vector $\boldsymbol{e} \in Z^m$ exists such that $\boldsymbol{e} = \boldsymbol{v}_1 \bmod \Lambda_1$ and $\boldsymbol{e} = \boldsymbol{v}_2 \bmod \Lambda_2$. This result can be generalized from two lattices to multiple lattices.

About more than two lattices, [39] can be viewed an example.

3 Our Scheme

3.1 Proposed Algorithm

1) Setup

In terms of $n \geq 2$, let $\Lambda_1 = p_1 Z^n, \Lambda_2 = p_2 Z^n, \cdots, \Lambda_n = p_n Z^n$ with n primes $p_1, p_2, \cdots, p_n (p_1 < p_2 < \cdots < p_n)$. Because $p_1, p_2, \cdots, p_k$ are different primes, $p_1 Z^n + p_2 Z^n + \cdots + p_n Z^n = Z^n$ and $p_1 Z^n \cap p_2 Z^n \cap \cdots \cap p_n Z^n = p_1 p_2 \cdots p_n Z^n \neq \varnothing$. Let $\boldsymbol{v} = \underbrace{[1, 1, \cdots 1]}_{n}^{T}$, $N = p_1 \times p_2 \times \cdots \times p_t$, $M = p_{n-t+2} \times p_{n-t+3} \times \cdots \times p_n$. Secret s satisfies $N > s > M$. Let $H : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is a collision-resistant hash function.

2) Share distribution

For secrets s,the trusted center computing $\begin{cases} s_1 v \equiv sv (mod\ \Lambda_1) \\ \vdots \\ s_n v \equiv sv (mod\ \Lambda_n) \end{cases}$.

Then the sub-secret of secret s is (Λ_i, s_i) $(i \in [n])$.

The trusted center sends the sub-secret (Λ_i, s_i) to participants P_i and publish $\boldsymbol{h_i} = H(s_i \boldsymbol{v})$ $(i \in [n])$

3) Verification

Upon receiving the sharing, the participant P_i verifies whether the hash value of his share is the same as that on the bulletin board, i.e., $H(s_i \boldsymbol{v})? = \boldsymbol{h_i}$

4) Secret reconstruction

Aggregators randomly select t sub-secrets from n participants, $(\Lambda_1, s_1), (\Lambda_2, s_2), \cdots, (\Lambda_t, s_t)$,

use the intersection method to calculate the solution sv of $\begin{cases} sv \equiv s_1 v(mod\ \Lambda_1) \\ \vdots \\ sv \equiv s_t v(mod\ \Lambda_t) \end{cases}$, and recover the secret $s \equiv s(\mathrm{mod}N_1)$, $N_1 = p_1 p_2 \cdots p_{\mathrm{t}}$.

3.2 Correctness and Security

1) Correctness

In our scheme, according to the ordinary secret sharing scheme based on the CRT, a secret is divided into n parts, so that at least t of n parts can obtain the secret s.

For any t sub-secrets:

$$(s_1, p_1), (s_2, p_2), \cdots, (s_t, p_t)$$

Calculate $s \equiv s(\mathrm{mod}N_1)$, $N_1 = p_1 p_2 \cdots p_{\mathrm{t}}$, since $N_1 \geq N > s > M$, then the secret s can be determined.

And the same goes for expanding into the scheme based on lattice.

2) Security

Theorem 1. In the proposed scheme, any less than t participants cannot recover the undisclosed secret s.

Proof. In our scheme, according to the ordinary secret sharing scheme based on the CRT, a secret is divided into n parts, so that at least t parts can obtain the secret s.

For any $t - 1$ sub-secrets:

$$(s_1, p_1), (s_2, p_2), \cdots, (s_{t-1}, p_{t-1})$$

Calculate $s \equiv s(\mathrm{mod}M_1)$, $M_1 = p_1 p_2 \cdots p_{\mathrm{t}-1}$, since $N_1 \geq N > s > M \geq M_1$, then there is not enough information to determine s.

And the same goes for expanding into the scheme based on lattice.

Theorem 2. The scheme which we proposed is post-quantum safe.

Proof. The security of our scheme depends on the intersection method. The intersection method [38] is post-quantum safe, so our scheme is also post-quantum safe.

4 Cost Analysis

In this section, we mainly compare the memory cost and time cost of our scheme with other schemes. The comparison is shown in Table 2.

Table 2. Cost requirements for different schemes

Schemes	Size of shares	Time of share distribution	Time of secret reconstruction
Our scheme	$O(1)$	$O(n)$	$O(t\log t)$
Pilaram et al. [34]	$O(n)$	$O(n^3)$	$O(t^3)$
Kiamari et al. [36]	$O(1)$	$O(nt)$	$O(t\log t)$

5 Conclusion

In this paper, we construct a verifiable lattice-based secret sharing scheme using some number theory methods and interaction method. Our scheme is safe in the post-quantum era. Furthermore, we analyse the security of our scheme. Finally, we compared our scheme with other schemes, and the comparison shows that our scheme is more efficient and occupies less memory.

Acknowledgement. This work is supported by the National Natural Science Foundation of China (grant no. 62072023), the Open Project Fund of the State Key Laboratory of Cryptology (grant no. MMKFKT202120), Beijing Municipal Natural Science Foundation, the Exploratory Optional Project Fund of the State Key Laboratory of Software Development Environment, and the Fundamental Research Funds of Beihang University (grant nos. YWF-20-BJ-J-1040, YWF-21-BJ-J-1041, etc.).

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
2. Beimel, A., Chor, B.: Secret sharing with public reconstruction. IEEE Trans. Inf. Theory **44**(5), 1887–1896 (1998)
3. Blakley, G.R.: Safeguarding cryptographic keys. In: International Workshop on Managing Requirements Knowledge, p. 313. IEEE Computer Society (1979)
4. Asmuth, C.A., Blakley, G.R.: Pooling, splitting, and restituting information to overcome total failure of some channels of communication. In: 1982 IEEE Symposium on Security and Privacy, p. 156. IEEE (1982)
5. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Inf. Theory **29**(2), 208–210 (1983)
6. Jackson, W.A., Martin, K.M.: Perfect secret sharing schemes on five participants. Des. Codes Crypt. **9**, 267–286 (1996)
7. Chor, B., Goldwasser, S., Micali, S., et al.: Verifiable secret sharing and achieving simultaneity in the presence of faults. In: 26th Annual Symposium on Foundations of Computer Science (SFCS 1985), pp. 383–395. IEEE (1985)
8. Shieh, S.P., Sun, H.M.: On constructing secret sharing schemes. In: Infocom 94 Networking for Global Communications. IEEE (1994)
9. Sun, H.M., Shieh, S.P.: On dynamic threshold schemes. Inf. Process. Lett. **52**(4), 201–206 (1994)
10. Lin, T.Y., Wu, T.C.: (t, n) threshold verifiable multisecret sharing scheme based on the factorisation intractability and discrete logarithm modulo a composite problem. IEE Proc.-Comput. Digit. Tech. **146**(5), 264–268 (1999)

11. Wu, T.C., Wu, T.S.: Cheating detection and cheater identification in secret sharing schemes. IEE Proc.-Comput. Digit. Tech. **142**(5), 367–369 (1995)
12. Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: 28th Annual Symposium on Foundations of Computer Science (SFCS 1987), pp. 427–438. IEEE (1987)
13. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-46766-1_9
14. Cramer, R., Damgård, I., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_22
15. Cramer R: Introduction to secure computation. In: Damgård, I.B. (ed.) Lectures on Data Security. EEF School 1998. LNCS, vol. 1561, pp. 16–62. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48969-X_2
16. Gennaro, R., Micali, S.: Verifiable secret sharing as secure computation. In: Guillou, L.C., Quisquater, J.J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 168–182. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-49264-X_14
17. Gennaro, R.: Theory and practice of verifiable secret sharing. Massachusetts Institute of Technology (1996)
18. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, pp. 73–85. ACM, New York (1989)
19. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game, or a completeness theorem for protocols with honest majority. In: Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, pp. 307–328. ACM, New York (2019)
20. Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Robust threshold DSS signatures. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 354–371. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_31
21. Gennaro, R., Jarecki, S., Krawczyk, H., et al.: Secure distributed key generation for discrete-log based cryptosystems. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 295–310. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-x_21
22. Gennaro, R., Rabin, M.O., Rabin, T.: Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing, pp. 101–111. ACM, Puerto Vallarta (1998)
23. Stadler, M.: Publicly verifiable secret sharing. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 190–199. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_17
24. Fujisaki, E., Okamoto, T.: A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 32–46. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054115
25. Schoenmakers, B.: A simple publicly verifiable secret sharing scheme and its application to electronic voting. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 148–164. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_10
26. Benaloh, J.C.: Secret sharing homomorphisms: keeping shares of a secret secret. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 251–260. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-47721-7_19
27. Georgescu A: A LWE-based secret sharing scheme. Netw. Secur. Cryptogr. (2011)
28. El Bansarkhani, R., Meziani, M.: An efficient lattice-based secret sharing construction. In: Askoxylakis, I., Pöhls, H.C., Posegga, J. (eds.) WISTP 2012. Lecture Notes in Computer

Science, vol. 7322, pp. 160–168. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30955-7_14
29. Khorasgani, H.A., Asaad, S., Eghlidos, T., et al.: A lattice-based threshold secret sharing scheme. In: 2014 11th International ISC Conference on Information Security and Cryptology, pp. 173–179. IEEE, Tehran (2014)
30. Asaad, S., Khorasgani, H.A., Eghlidos, T., et al.: Sharing secret using lattice construction. In: 7th International Symposium on Telecommunications (IST 2014), pp. 901–906. IEEE, Tehran (2014)
31. Babai, L.: On Lovász'lattice reduction and the nearest lattice point problem. Combinatorica **6**, 1–13 (1986)
32. Bendlin, R., Damgård, I.: Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 201–218. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_13
33. Bendlin, R., Krehbiel, S., Peikert, C.: How to share a lattice trapdoor: threshold protocols for signatures and (H) IBE. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, vol. 7954, pp. 218–236. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38980-1_14
34. Pilaram, H., Eghlidos, T.: An efficient lattice based multi-stage secret sharing scheme. IEEE Trans. Dependable Secure Comput. **14**(1), 2–8 (2015)
35. Yang, Z., He, D., Qu, L., et al.: On the security of a lattice-based multi-stage secret sharing scheme. IEEE Trans. Dependable Secure Comput. (2022)
36. Kiamari, N., Hadian, M., Mashhadi, S.: Non-interactive verifiable LWE-based multi secret sharing scheme. Multimed. Tools Appl. 1–13 (2022)
37. Ajtai, M.: Generating hard instances of the short basis problem. In: Wiedermann, J., van Emde Boas, P., Nielsen, M. (eds.) ICALP 1999. LNCS, vol. 1644, pp. 1–9. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48523-6_1
38. Boneh, D., Freeman, D.M.: Homomorphic signatures for polynomial functions. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 149–168. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_10
39. Lu, X., Yin, W., Wen, Q., et al.: A lattice-based unordered aggregate signature scheme based on the intersection method. IEEE Access **6**, 33986–33994 (2018)