Cryptography of Blockchain

Ying Long[1,2],Yinyan Gong[1,2*], Weihong Huang[1,2], Jiahong Cai[1,2], Nengxiang Xu[1,2], Kuan-ching Li[1,2]

1 School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China

2 Hunan Key Laboratory for Service computing and Novel Software Technology, Xiangtan 411201, China

G18873530267@163.com,2820558906@qq.com,whhuang@hnust.edu.cn,jiahongcai@mail.hnust.edu.cn, 1113482768@qq.com, 2949380334@qq.com

Abstract. With the development of digital currencies and 5G technology, blockchain has gained widespread attention and is being used in areas such as healthcare, industry and smart vehicles. Many security issues have also been exposed in the course of blockchain applications. Cryptography can ensure the security of data on the blockchain, the integrity and validity of data as well as the ability to authenticate users and anonymize them. This article therefore examines the cryptography underlying blockchain security issues, providing an overview of cryptographic homomorphic encryption, zero-knowledge proofs and secure multi-party computation commonly used in blockchains. At the same time, the development of quantum computing is bound to affect existing cryptographic systems, and blockchains applying these cryptographic systems are bound to be hit hard, so this article discusses four of the most promising post-quantum cryptography techniques available: hash-based public key cryptography, code-based public key cryptography, multivariate public key cryptography, and lattice-based public key cryptography.

Keywords: Blockchain, Homomorphic encryption, Post quantum cryptography, Secure multi-party computation, Zero-knowledge proof.

1 Introduction

In 2008, Satoshi Nakamoto introduced the concept of Bitcoin, a decentralized virtual currency, in his published paper "Bitcoin: A Peer-to-Peer Electronic Money System" [1]. Blockchain is a data structure that organizes blocks of data in a chain in chronological order and is capable of verifying, tracing, and reliably storing data on the chain through cryptography to ensure that the data on the blockchain is not tampered with and cannot be forged. The consistency of data on the blockchain is ensured through transaction signatures, consensus mechanisms and cross-chain technologies [2]. Blockchain technology is decentralized, traceable, tamper-proof, complete and open and transparent [3], which have attracted the attention of academia and industry. Moreover,

blockchain technology will be a revolutionary technology to solve the trust crisis in the future society [4].

As blockchain continues to develop, there is a greater demand for data protection, anonymity and untraceability [5] in many fields. Blockchain is no longer only used for virtual currencies [6] but is also being extended to various fields such as healthcare, copyright protection and finance. For example, blockchain is currently the most effective solution for personal privacy protection and sharing [7]. As part of the big data trend [8], the growing scale of the Internet of Things (IoT) [9] and the sharing of its data requires the use of blockchain. Many insider attacks are caused by trust issues, and blockchain can solve the problem of trust between untrustworthy users [10]. However, the rise of blockchain technology in various fields has brought about many security issues. For example, privacy protection and transaction protection. Also, with the development of quantum computing, which may break many cryptographic systems [11], the cryptography of blockchain will be severely challenged. With the emergence of various attacks, various cryptography-based blockchain security protection techniques are gradually developed [12]. Therefore, this paper will study the cryptography techniques in blockchain.

2 Blockchain Overview

2.1 The data structure of Bitcoin

In blockchain technology, a great deal of cryptographic knowledge is used to ensure the system's security. Cryptography greatly protects the privacy of data on the blockchain [13]. The blockchain is actually made up of blocks connected one by one, each block generating a hash value from the previous block [14]. The user can then verify the correctness of the data on the chain. Furthermore, if an attacker wants to tamper with the data on the blockchain, he must change all the blocks after that one.

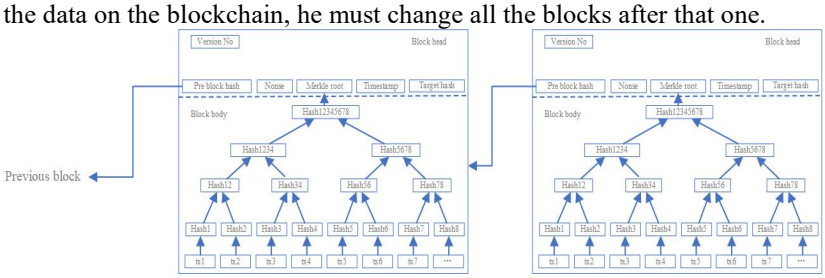

Fig. 1. Bitcoin structure diagram.

A block contains a block header and a block body. The block header holds the previous block's hash value, version number, random number Nonce, timestamp, Merkle root and the target hash value. In the block body is a Merkle tree, a typical binary tree. Its root is formed by the hashes of all the transactions in the block; the leaf nodes of the Merkle tree are the hashes generated by the transactions packed into the block, and the values of the non-leaf nodes are generated by concatenating the hashes of their children into a string and then hashing them, in this way working from the bottom up to generate the hash of the Merkle root. This structure allows a quick look at whether the

transactions packed in the block have been altered and, if found to have been altered, a quick way to locate the altered transaction.

2.2 Security challenges facing blockchain

Blockchain is a promising and growing technology but also faces many challenges. These challenges arise from the existing computer system [15-17] and network architecture [18-20], the consensus mechanisms used in the blockchain and the need for data protection [21-23]. With the development of blockchain and the development and promotion of the application of 5G technology, blockchain is gradually applied to various industries such as healthcare [24], industry [25], and finance [26]. While blockchain is widely used, it also raises a series of security and privacy issues. The digital currencies used in blockchain have also suffered many security threats, with attacks on trading platforms, theft of currencies and crimes committed by hackers and criminals using blockchain's anonymous transactions occurring frequently. At the same time, privacy breaches [27-28] in blockchain can also make the skeptical public of blockchain. These challenges are very detrimental to the development and innovation of blockchain.

3 Typical cryptography

3.1 Homomorphic encryption

The idea of homomorphic encryption was first introduced by Rivest, Adleman and Detouzos [29] (the R and A in "RSA") in 1978. Homomorphic data encryption allows direct manipulation of the encrypted data without the need for preliminary decryption of the operands. The effect of manipulating the encrypted data is the same as manipulating the data before encryption. In a blockchain, *FHE (fully homomorphic encryption)* ensures that the ledger information is not compromised but can be manipulated, even if the blockchain is attacked. *FHE* is a good solution to the problem of data being used on remote devices [30]. In 2009, Gentry [31] proposed a secure and reasonable *FHE* system that performs arbitrary addition and multiplication operations on the encrypted data while also acting on the pre-encrypted data. However, the performance of *FHE* algorithms is so poor that they are difficult to use in practice. In 2011, Brakerski et al. [32] proposed a new *FHE* algorithm, BVG, based on *Learning With Errors* (LWE), an alternative assumption to lattice encryption. The BGV system uses a somewhat more practical LWE assumption than the system proposed by Gentry in 2009. In 2013, Gentry [33] et al. proposed a simpler, *FHE* algorithm GSW based on LWE. In their scheme, they proposed a way to construct *FHE* of a new technique known as the approximate eigenvector method.

3.2 Zero-knowledge proofs

Zero-knowledge proof means that the prover does not need to reveal anything about the verification to the verifier who can also do the verification. With the use of zero-

knowledge proofs in blockchain, other nodes can verify the legitimacy and correctness of a transaction even if both parties do not reveal any information about the transaction. Zero-knowledge proofs are divided into interactive zero-knowledge proofs and non-interactive zero-knowledge proofs. Interactive zero-knowledge proofs require multiple interactions between the verifier and the prover, and the verifier improves the trustworthiness of the prover by performing multiple verifications to the prover. Non-interactive zero-knowledge proofs, on the other hand, allow the verifier and the prover to interact once with the aid of a machine. An overview of the development of zero-knowledge proofs is given next.

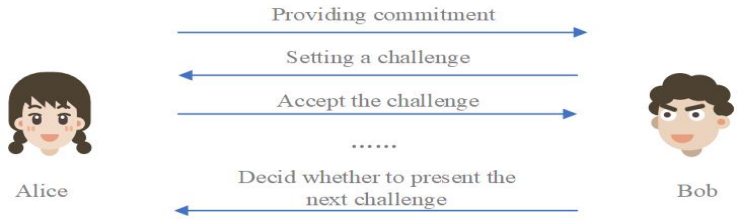

Fig. 2. Interactive zero-knowledge proof.

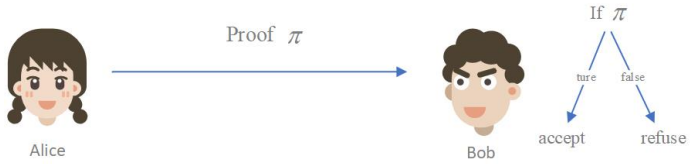

Fig. 3. Non-interactive zero-knowledge proof.

The concept of zero-knowledge proofs was introduced by S. Goldwasser, S. Micali and C. Rackoff [34] in 1988. After introducing this concept, zero-knowledge proofs have also been present in the overview of the theory. The emergence of blockchains and the need for data confidentiality has facilitated scholarly research on zero-knowledge proofs, which can address the difficulty of aligning blockchain privacy protection with data transparency [35]. In 2010, Groth proposed the key theory of zero-knowledge proofs ZK-SNARK [36] (zero-knowledge succinct non-interactive knowledge proofs). The provers can prove the correctness of their provided proofs mathematically to the verifiers without providing information about the proofs as the verifiers do. Subsequent scholars have worked on ZK-SNARK to reduce verification time and improve efficiency. the Pinocchio [37] protocol, proposed in 2013, is an improved version of ZK-SNARK, and in 2015 the blockchain application Zcash was used to build ZK-SNARK [38], a widespread application of zero-knowledge proofs. In 2016, Groth [39] proposed Groth16, which is also based on an improved version of ZK-SNARK with asymmetric pairing, and the proof will be more efficient.

ZK-SNARKS requires public reference strings for provers and verifiers for trustworthy settings when performing zero-knowledge proofs, but these public strings are again provided by a small group of people, and thus are vulnerable to attack by some malicious nodes [39]. As a result, research now prefers to discard trusted settings. In

2018, the Bulletproofs algorithm was introduced to eliminate the need for trusted settings. It is a more efficient algorithm that produces proofs of logarithmically transformed size, which would be very beneficial for storing proofs in the blockchain. Moreover, Bulletproofs can also merge and compress proofs of the same scope, reducing the size of the space occupied by the blockchain. In 2018, a new zero-knowledge proof scheme ZK-STARKS was also proposed [40], a zero-knowledge proof scheme that does not require trustworthy settings. ZK-STARKS has better scalability, and its proof and verification times are linearly and logarithmically related to the initial computation time, respectively. As the initial size increases, its proof and verification times do not increase significantly. The more widely used non-interactive zero-knowledge proofs for blockchain applications are ZK-SNARKS, Bulletproofs and ZK-STARKS.

3.3 Secure Muti-party Computation

Secure Muti-party Computation (SMPC) is derived from the "millionaire problem" proposed by Professor Yao in 1982, i.e.. Collaborative multi-party computing with third-party guarantees may carry the risk of information leakage from third-party organizations. SMPC enables distributed parties to jointly compute arbitrary functions without revealing their own private inputs and outputs. In the SMPC scenario, there are $n(n \geq 2)$ participants performing multi-party collaboration to compute an objective function $f(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n)$, where $x_1, x_2, ..., x_n$ are the input information of each party. When the computation is finished, each participant does not get any other information except its own corresponding output y_i, Also no input information can be deduced from the input results.

Fig. 4. Secure multi-party calculation.

SMPC provides input correctness, computational correctness and output independence to analyze and capture the value in the data while protecting the privacy of the data. Similar to blockchain, secure multi-party computing supports collaborative computing by uniting untrusted users without a trusted third party. SMPC can collaborate with untrusted users in the blockchain without compromising their privacy to perform analytical calculations, analytical modelling, etc., on some sensitive data. It is also beneficial for blockchain applications to industries that require data analysis and storage, such as healthcare and industry. SMPC can be used in multi-signature, secret sharing, and random number generation, and the wallet ZenGo [41], a wallet released by Kzen,

does not require the use of mnemonic word and keys, but rather uses a gated signature method that combines the advantages of multi-signature and secret sharing. However, there are still difficulties that need to be addressed in the application of SMPC in blockchain, such as the fact that SMPC requires the participation of multiple honest nodes, malicious nodes may collude in the computation [42], and the efficiency of SMPC is low when the network transmission rate is low.

4 Post-Quantum Cryptography

If quantum computing develops as expected, it will inevitably disrupt existing cryptographic systems. For example, Bernstein and Daniel J. [43] point out that quantum computing's well-known Shor [44] algorithm and Grover [45] algorithm will have an impact on existing cryptographic systems. The Shor algorithm can theoretically solve the underlying mathematical problems on which the security of public key cryptographic algorithms depends, such as discrete logarithms and large integer decomposition problems. So these public-key algorithms, such as RSA and DSA, should not be secure. And Grover's algorithm will halve the security effect of some symmetric cryptographic algorithms and hash algorithms, requiring an increase in key length. Although it is only for theoretical threats, to take a long-term view, it is necessary to research early cryptography that can resist quantum attacks.

Post-Quantum Cryptography (PQC) resists an attacker even if the attacker has a quantum computer, also known as anti-quantum cryptography. The current mainstream schemes for PQC are hash-based public key cryptography, code-based public key cryptography, multivariate public key cryptography and lattice-based public key cryptography.

4.1 Lattice based cryptography

A lattice is a set of points in a high-dimensional space. Let $b_1, b_2, ..., b_n$ be a linearly independent set of bases ($n \le m$) in R^m and the lattice be the set of all linear combinations of integer coefficients of this set of bases. That is.

$$L(B) = \left\{ \sum_{i=1}^{n} x_i b_i, x_i \in Z, i = 1, 2, ..., n \right\} \tag{1}$$

The security of cryptographic algorithms relies on the underlying mathematical problem. Furthermore, the two main difficulties in lattice problems: are the difficulty of solving the shortest vector and the difficulty of solving the nearest vector. These problems have worst-case difficulty [46]. Many scholars have conducted many studies on lattice problems. The most famous algorithm is the LLL proposed by H. Lenstra, A. Lenstra and Lovasz in 1982 [47], however it can only solve the shortest vector in polynomial time with an approximation factor $(1+\varepsilon)\sqrt{4/\sqrt{3}}^{(n-1)/2}$ of (where it is a constant). Thus lattice-based cryptography is quantum resistant.

In the "Third Status Report on the Post-NIST Quantum Cryptographic Standardization Process" - NISTIR 8413 published in July 2022, four algorithms to be standardized were announced. And three of these are all lattice-based cryptographic schemes. The lattice-based cryptography algorithms have a better balance of security, public and private key size, and computational speed and are considered one of the most promising post-quantum cryptographic algorithms [48].

4.2 Hash-based signature algorithm

The hash-based signature algorithm was proposed by Leslie Lamport in 1979, but compared to other signature schemes, it did not to be widely used because it could produce relatively long signatures. With the arrival of the threat of quantum computing, it is gradually gaining attention again because hash-based signature counting has quantum-resistant properties, such as being resistant to attacks by Shor algorithms. It is one of the algorithms that have the potential to replace the traditional signature algorithm [49]. The one proposed by Leslie Lamport is a single hash signature, which cannot sign multiple messages, and was later improved by Ralph Merkle to form a multiple signature algorithm based on the Merkle tree. The public key is the root of the Merkle, and the key is each leaf node in the Merkle tree. The quantum resistance of Hash-based signature algorithm is based on the collision resistance of the Hash function because the current quantum algorithms cannot find the collision of the Hash. Swati Kumari [50] proposed an enhanced hash-based post-quantum cipher (PQC) architecture called signature-based Merkle hash multiplication (SMHM) algorithm. The hash Merkle signature-based algorithm is enhanced by using the Bernoulli-Karatsuba multiplication algorithm. Konstantinos Chalkias [51] proposed a scalable post-quantum cryptography scheme based on Merkle tree signatures suitable for blockchains and distributed ledgers, which can utilize dedicated chains or image structures to reduce the cost of key generation, signing, verification, and the size of signatures.

4.3 Code based cryptography

The code-based cryptosystem is derived from McEliece [52]. The algorithm is based on the integrable binary Goppa code called classical McEliece. The encryption and decryption of the McEliece cryptosystem are fast and secure. However, it is rarely used in practice because of the large size of the key, so one of the subsequent directions of research on code-based cryptography is to reduce the size of its key. The general linear decoding hard problem on which McEliece cryptographic algorithm is based is the NP-hard problem [53], so coding-based cryptography is very promising in quantum-resistant cryptography. Moreover, the NIST post-quantum cryptographic algorithm standard collection has coding-based cryptography second only to lattice-based cryptography. It is mainly used in public key encryption algorithms and only two for signature algorithms.

4.4 Multivariate-based Cryptography Regime

The security of the multivariate-based cryptography regime relies on solving the mathematical problem of solving a system of random multivariate quadratic polynomial equations over a finite field, which is nondeterministic polynomial time-hard. There is no finite algorithm for solving this problem. The *multivariate quadratic* polynomial problem is to find a solution in a system of quadratic polynomial equations in a given finite field. Since multivariate based cryptographic systems emerged late, they still need a lot of research and experiments to prove their security [54]. Although earlier multivariable-based signature systems have been breached and are no longer secure, multivariable-based signature algorithms are small in signature size and fast in inflammation. Therefore, multivariate based signature schemes are still very promising, and multivariate based signature algorithms are the most numerous in the NIST post-quantum cryptographic algorithm standards collection.

5 Conclusion

With the application of the blockchain, the blockchain needs to meet various different needs for data protection, multi-party participation and collaboration, and identity authentication in the face of different scenarios, and cryptography is crucial to the development of blockchain applications. In this paper, some classical cryptography and post-quantum cryptography in blockchain were studied. First, the origin of blockchain and its concepts were introduced, and the structure of Bitcoin and the security challenges it faces were presented. Subsequently, some classical cryptographic homomorphic encryption, zero-knowledge proofs and secure multi-party computation used in blockchains were investigated. Finally, four more promising post-quantum cryptograms were introduced for quantum computing attacks.

References

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.
2. Liang W, Xiao L, Zhang K, et al. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems[J]. IEEE Internet of Things Journal, 2021.
3. P Kumar, R Kumar, et al., PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities, IEEE Transactions on Network Science and Engineering 8 (3), 2326-2341, 2021.
4. He W, Zheng H. Literature Review on Block Chain: Technology, Principle and Development[C]//Journal of Physics: Conference Series. IOP Publishing, 2021, 1848(1): 012166.
5. Xu Z, Liang W, Li K C, et al. A Time-sensitive Token-Based Anonymous Authentication and Dynamic Group Key Agreement Scheme for Industry 5.0[J]. IEEE TII, 2021.
6. Gorkhali A, Li L, Shrestha A. Blockchain: A literature review[J]. Journal of Management Analytics, 2020, 7(3): 321-343.
7. W. Liang, Y. Yang, C. Yang, Y. Hu, S. Xie, K. C. Li, and J. Cao, "PDPChain: A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data," IEEE Transactions on Reliability, pp. 1-13, 2022, doi: 10.1109/TR.2022.3190932.

8. Long J, Liang W, Li K C, et al. A Regularized Cross-Layer Ladder Network for Intrusion Detection in Industrial Internet-of-Things[J]. IEEE Trans. on Industrial Informatics, 2022.
9. Liang W, Xie S, Cai J, et al. Novel private data access control scheme suitable for mobile edge computing[J]. China Communications, 2021, 18(11): 92-103.
10. J. Zhao, J. Huang, et al., An effective exponential-based trust and reputation evaluation system in wireless sensor networks, IEEE Access 7, 33859-33869, 2019.
11. Nejatollahi H, Dutt N, Ray S, et al. Post-quantum lattice-based cryptography implementations: A survey[J]. ACM Computing Surveys (CSUR), 2019, 51(6): 1-41.
12. Li X, Liao J, et al. A New Dynamic ID-Based User Authentication Scheme Using Mobile Device: Cryptanalysis, the Principles and Design. Wire. Per. Comm, 2015, 85(1): 263-288.
13. Liang W, Xie S, Cai J, et al. Deep neural network security collaborative filtering scheme for service recommendation in intelligent cyber-physical systems. IEEE IoT J., 2021.
14. Liang W, Ning Z, Xie S, et al. Secure fusion approach for the internet of things in smart autonomous multi-robot systems[J]. Information Sciences, 2021, 579: 468-482.
15. M. Qiu, Z. Jia, et al., "Voltage assignment with guaranteed probability satisfying timing constraint for real-time multiproceesor DSP", J. of Signal Proc. Systems, 2007
16. M. Qiu, L. Yang, et al., "Dynamic and leakage energy minimization with soft real-time loop scheduling and voltage assignment", IEEE TVLSI, 18 (3), 501-504, 2009
17. M. Qiu, C. Xue, et al., “Energy minimization with soft real-time and DVS for uniprocessor and multiprocessor embedded systems,” IEEE DATE Conf., 1-6, 2007
18. M. Qiu, Z. Chen, et al., "Energy-aware data allocation with hybrid memory for mobile cloud systems", IEEE Systems J., 11 (2), 813-822, 2014
19. M. Qiu, C Xue, Z Shao, et al., "Efficient algorithm of energy minimization for heterogeneous wireless sensor network", IEEE EUC, 25-34, 2006
20. J. Li, Z. Ming, et al., "Resource allocation robustness in multi-core embedded systems with inaccurate information", Journal of Systems Architecture 57 (9), 840-849, 2011
21. Raikwar M, Gligoroski D, Kralevska K. SoK of used cryptography in blockchain[J]. IEEE Access, 2019, 7: 148550-148575.
22. H. Qiu, T. Dong, et al, "Adversarial attacks against network intrusion detection in IoT systems," IEEE Internet of Things Journal 8(13), 10327-10335, 2020
23. K. Gai, M. Qiu, S. Elnagdy, “A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance,” IEEE BigDataSecurity 2016
24. F. Hu, S. Lakdawala, et al., Low-power, intelligent sensor hardware interface for medical data preprocessing, IEEE Trans. on Info. Tech. in Biomedicine 13 (4), 656-663, 2009
25. H. Qiu, Q. Zheng, et al., "Topological graph convolutional network-based urban traffic flow and density prediction", IEEE Trans. on ITS, 2020
26. Y. Li, K. Gai, et al., "Intercrossed access controls for secure financial services on multimedia big data in cloud systems", ACM Trans. on Multimedia Comp., Comm., and App., 2016
27. M. Qiu, H. Qiu, et al., “Secure Data Sharing Through Untrusted Clouds with Blockchain-enabled Key Management”, the 3rd SmartBlock pp. 11-16, Oct. 2020, Zhengzhou, China.
28. K. Gai, Y. Zhang, et al., “Blockchain-enabled Service Optimizations in Supply Chain Digital Twin”, IEEE Transactions on Service Computing, 2022
29. Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of secure computation, 1978, 4(11): 169-180.
30. Gai K, Qiu M. Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers[J]. IEEE Transactions on Industrial Informatics, 2017, 14(8): 3590-3598.
31. Gentry C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009: 169-178.

32. Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages, Crypto. Conf., Springer, Heidelberg, 2011: 505-524.
33. Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]//Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2013: 75-92.
34. Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems, Providing Sound Found. for Crypto.: On the Work of Shafi Goldwasser and Silvio Micali. 2019: 203-225.
35. Chor B, Goldwasser S, Micali S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults, 26th IEEE Sym. on Found. of Comp. Sci. (SFCS), 1985: 383-395.
36. Groth J. Short pairing-based non-interactive zero-knowledge arguments, Int'l Conf. on the Theory and Appl. of Crypt. and Info. Security. Springer, Berlin, Heidelberg, 2010: 321-340.
37. Parno B, Howell J, Gentry C, et al. Pinocchio: Nearly practical verifiable computation[J]. Communications of the ACM, 2016, 59(2): 103-112.
38. Banerjee A, Clear M, Tewari H. Demystifying the Role of zk-SNARKs in Zcash, IEEE conf. on application, info. and network security (AINS), 2020: 12-19.
39. Groth J. On the size of pairing-based non-interactive arguments, Int'l conf. on the theory and applications of crypto. techniques. Springer, Berlin, Heidelberg, 2016: 305-326.
40. Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin[C]//2014 IEEE symposium on security and privacy. IEEE, 2014: 459-474.
41. Lindell Y. Fast secure two-party ECDSA signing[C]//Annual International Cryptology Conference. Springer, Cham, 2017: 613-644.
42. Wang Z, Cheung S C S, Luo Y. Information-theoretic secure multi-party computation with collusion deterrence, IEEE Trans. on Info. Forensics and Security, 2016, 12(4): 980-995.
43. Bernstein D J, Lange T. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188-194.
44. Shor P W. Algorithms for quantum computation: discrete logarithms and factoring, 35th annual symposium on foundations of computer science. IEEE, 1994: 124-134.
45. Grover L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996: 212-219.
46. Esgin M F, Steinfeld R, et al. Short lattice-based one-out-of-many proofs and applications to ring signatures, Int'l Conf. on Applied Crypto. and Netw. Secu., Springer, 2019: 67-88.
47. Lenstra A K, Lenstra H W, Lovász L. Factoring polynomials with rational coefficients[J]. Mathematische annalen, 1982, 261(ARTICLE): 515-534.
48. Micciancio D, Regev O. Lattice-based cryptography[M]//Post-quantum cryptography. Springer, Berlin, Heidelberg, 2009: 147-191.
49. Merkle R C. Secrecy, authentication, and public key systems[M]. Stanford university, 1979.
50. Kumari S, Singh M, Singh R, et al. Signature based Merkle Hash Multiplication algorithm to secure the communication in IoT devices, Knowledge-Based Syst., 2022, 253: 109543.
51. Chalkias K, Brown J, Hearn M, et al. Blockchained post-quantum signatures, IEEE iThings/GreenCom/CPSCom/SmartData, 2018: 1196-1203.
52. McEliece R J. A public-key cryptosystem based on algebraic[J]. Coding Thv, 1978, 4244: 114-116.
53. Chaulet J, Sendrier N. Worst case QC-MDPC decoder for McEliece cryptosystem[C]//2016 IEEE International Symposium on Information Theory (ISIT). IEEE, 2016: 1366-1370.
54. Ding J, Yang B Y. Multivariate public key cryptography[M]//Post-quantum cryptography. Springer, Berlin, Heidelberg, 2009: 193-241., last accessed 2016/11/21.