

Verifiable Key Computation Scheme Based on Zero-Knowledge Proof in MA-CPABE

Xie Long¹

¹Yunnan University of Finance and Economics, Information Center, South Campus, Wuhua District, Kunming City, Yunnan Province, China

Keywords

Blockchain; MA-CPABE; Off-chain verification; Zk-snark

Abstract

In order to eliminate the reliance on centralized authorities the MA-CPABE ciphertext access control scheme based on blockchain technology has become a current research hotspot. However, the existing solutions still face challenges in terms of blockchain scalability and verifiable security. Therefore, this paper proposes a verifiable key calculation scheme based on zero-knowledge proof, aiming to achieve an efficient and verifiable new type of MA-CPABE access control scheme. Firstly, during the process of generating the user's private key on the blockchain node, computationally intensive operations such as public and private key calculation, hash calculation, and point addition are performed off-chain, achieving the functions of key generation and distribution. Secondly, with the aid of the non-interactive zero-knowledge proof system, the correctness of the off-chain calculation results is efficiently verified on-chain to ensure the reliability and transparency of the key generation process. Finally, this paper conducts a comprehensive analysis of the scheme from three aspects: security, off-chain computing efficiency, and on-chain cost. The simulation experiment results show that the scheme proposed in this paper can achieve trusted key generation and distribution in MA-CPABE, reduce the on-chain computing overhead, and ensure the execution efficiency of the CPABE scheme. It provides a new solution for blockchain-based ciphertext access control.

*Correspondence Email:

202302110719@stu.ynufe.edu.cn

1. Introduction

With the acceleration of the digital process, data security and privacy protection have become an important global issue. Attribute-Based Encryption (ABE) [1] technology shows unique advantages in the field of data protection by virtue of its flexible access control characteristics. As an important extension of ABE, Multilevel attribute-based Encryption (MA-CPABE) [2] effectively solves the access control problem in distributed environment by introducing multiple Attribute authorities. With the development of blockchain, blockchain-based MA-CPABE has become the research focus.

However, the existing MA-CPABE schemes still face key challenges such as insufficient decentralization and off-chain computing security. The emergence of blockchain technology provides new ideas for solving these problems [3-9]. Its decentralization, non-tampering and transparent verifiability have natural complementarity with MA-CPABE. Through blockchain technology, the process of key generation and

verification can be decentralized, and the consensus mechanism can be used to ensure system security and credibility. It is particularly worth noting that the introduction of zero-knowledge proofs (zk-SNARKs) technology makes it possible to verify the computation process without revealing any sensitive information, which provides a new technical support for system privacy protection.

In summary, in the existing research on multi-authority attribute-based encryption (MA-CPABE), although many schemes have improved the privacy and security to a certain extent, there are still several shortcomings. First of all, many schemes rely on a trusted third party or AA, a central Authority (CA) or a Master Authority, which makes the system vulnerable to a single point of failure or malicious attacks, thus compromising the security and reliability of the whole system. Secondly, the existing schemes usually cannot effectively verify the correctness of the attribute private key, resulting in potential security risks in the process of key management. The computational overhead of the existing schemes is large, especially in the stage of key generation and distribution, the client faces a high computational burden, especially in the cloud computing environment, which becomes a bottleneck that limits the practical application of the system. In addition, the application of blockchain technology is still relatively limited. Although some schemes simply integrate blockchain as a storage ledger, most researches only stay at the level of blockchain as an auxiliary tool, and do not deeply explore the deep integration and collaborative optimization of MA-CPABE and blockchain technology. Finally, in the system based on MA-CPABE, with the rapid growth of the number of access users, the total amount of zero-knowledge proof generation will show an exponential growth. If all zero-knowledge proofs are stored directly on the blockchain, it will not only bring huge storage pressure to the blockchain, but also lead to high Gas cost, which is not sustainable in practical applications.

1.1 Our Contributions

The contributions of this paper are as follows:

- (1). A decentralized MA-CPABE key management scheme combining blockchain and zero-knowledge proof is proposed. By replacing the authorized nodes in the traditional MA-CPABE with blockchain nodes, the key generation and verification process no longer rely on a centralized trusted entity.
- (2). In order to verify the correctness of off-chain key computation, we design a protocol based on circuitized zero-knowledge proof (CZKP). The operator node calculates and verifies the key generation and verification process in MA-CPABE, and transforms the key calculation process into a circuit model to ensure that the correctness of the calculation can be verified efficiently without revealing the calculation details.

2. Scheme Overview

2.1 System Description

The system architecture combines blockchain technology and multi-authority Attribute-based encryption (MA-CPABE) to realize decentralized attribute authorization and key distribution. This is shown in Fig. 1. In the blockchain, the nodes select the attribute authorization node AA through the pledge mechanism. Each attribute authorization node generates a secret key pair $\{PK_i, SK_i\}$ according to the attributes it manages, and uploads its public key PK_i to the blockchain. DO encrypts the information, obtains the ciphertext CT, uploads CT to IPFS, and publishes CID and (A, Δ) to the blockchain. The attribute authority node (AA) performs off-chain verification of the key generation process by adopting encryption methods such as public and private key verification and hash function, and generates a zero-knowledge proof CZKP. DU obtains the ciphertext CT from IPFS and proves to AA that it has some properties, requesting the corresponding decryption key set $SK_{\{GID, u\}}$. When DU meets the requirements, DU decrypts the ciphertext CT to obtain the message M.

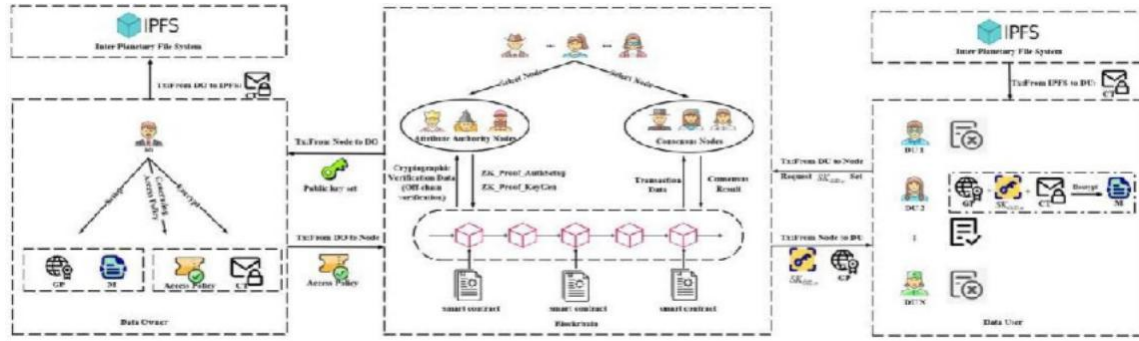


Fig. 1 System architecture

The framework consists of six main actors whose functions are as follows:

- (1) Data Owner (DO): When the data owner wants to share data M with the data user, they need to create an access policy (A, Δ) based on the LSSS matrix to grant access to the data user. The data owner executes GlobalSetup to generate GP , obtains $\{PK_{\theta}\}$, and executes Encrypt to generate CT , stores CT on IPFS, and obtains a CID. And send CID and access policy (A, Δ) to the nodes on the blockchain.
- (2) Data User (DU): When the data user accesses the shared data, it must first request the secret key set $SK_{\{GID, u\}}$ from the attribute authorization node on the blockchain. And obtain GP and CID uploaded by the data owner, and then obtain CT through CID. The user can then perform Decrypt on CT to obtain M .
- (3) Attribute Authority Node (AAs): A blockchain node is initially selected as an attribute authority node through a stake election. Each AA is responsible for the generation and distribution of keys according to the attributes it manages. AuthSetup generates $\{PK_i, SK_i\}$, and PK_i is uploaded to the blockchain. KeyGen generates $SK_{\{GID, u\}}$ for data users to decrypt. An off-chain key verification algorithm is performed to generate a zero-knowledge proof.
- (4) Storage IPFS: The main function of IPFS is to provide distributed storage services for all participants. It stores ciphertext CT and returns a CID. CID is a unique hash value representing the file or data content uploaded to IPFS.
- (5) Consensus Verification Node (CVN): It is responsible for verifying the user identity and the proof CZKP of the attribute key correctness, ensuring the legitimacy of the transaction.
- (6) Blockchain (BC): Nodes on the chain participate in the equity pool, and select appropriate nodes for roles such as operation nodes, consensus verification nodes and computing nodes. On the blockchain, reward settlement and punishment are carried out according to the contribution of each node.

2.2 Verifiable Off-chain Computation

Off-chain computation is mainly the verification calculation of key generation and distribution in KEYGEN and SETUP parts of MA-CPABE, and the correctness of the operation is verified by using public and private key verification and hash calculation.

- (1) Large integer representation and operation optimization: For a large integer α_{θ} , to optimize the constraints, in the intermediate circuit, it is represented as an array a of length k such that $\alpha_{\theta} = 2^0 * a[0] + 2^1 * a[1] + \dots + 2^{k-1} * a[k-1]$, where n denotes the register size, k denotes the number of registers, each $0 \leq a[i] < 2^n$, and each register $a[i]$ has a sign. Signed overflow representation and Prime Reduce template can compress array length, reduce constraints, and adapt to the circuit efficiency requirements of zero-knowledge proofs.

(2) Accelerating operations over finite fields: MA-CPABE relies on multiplication and modulo operations, and through the optimization of 'carry-free calculation + modulo compression', it reduces the constraints by 30%-50% compared with general circuits. The array length of a signed overflow BigInt is compressed by increasing the overflow size. In the exponent operation, the exponent is expressed as a polynomial, and the equation is verified by polynomial evaluation at multiple points, rather than stepwise convolution. According to if two polynomials of degree m agree on $m+1$ distinct points, they must be equal. Therefore, three constraint verifications are required: $Y(0) = y_g0$, $Y(1) = y_g0 + y_g1 + y_g2$, $Y(2) = y_g0 + 2*y_g1 + 4*y_g2$.

(3) The computation of scalar multiplication is optimized by window method: The binary representation of index t is grouped (stride=10), and the multiple of base point G is pre-cached. The number of operations is reduced by look-up table method and point addition. Running an exhaustive search for the stride that balances constraint usage in point addition and multiplexer reveals that the number of constraints reaches the minimized constraint at stride=10. (See Table 2 for the quantitative relationship between strides and constraints.)

2.2.2 AuthSetup Phase: Off-chain Public and Private Key Generation

The core of off-chain computation in the AuthSetup phase is to generate the authoritative public and private key pair $PK_{\theta} = \{e(g, g)^{\alpha_{\theta}}, g^{y_{\theta}}\}$. After introducing the zk-pairing arithmetic optimization, the problems of 'large exponential operation constraints' and 'complex pairing result verification' are solved. The specific integration scheme is as follows:

(1) Off-chain computation and zero-knowledge proof generation: Using a large integer representation, α_{θ} is represented as an array of signed registers, and the template CheckCarryToZero ensures that the final result is correct. When computing y_{θ} , the double addition algorithm and the unequal point addition optimization are performed by multiplexing the scalar multiplication template, and it is verified that $g^{y_{\theta}}$ belongs to the G_1 subgroup. During the pairing calculation, the MillerLoopFp2 template is called to achieve 'carry free line function calculation', avoiding the modular operation of intermediate results.

(2) Construction of zero-knowledge proof circuit: Algorithm 1 describes the template PrivToPub(n, k) that computes the public key from the private key. The algorithm takes a private key array as input, decomposes each register into binary, applies sliding window processing (stride=8), and accumulates point additions to compute the public key output. The BLS12_381_G2WindowMul template precomputes window multiplication tables for efficient scalar multiplication.

Algorithm 1: template PrivToPub(n, k) - Input: $privkey[k]$; Output: $pubkey[2][k]$. The algorithm decomposes each private key register into bits using Num2Bits, applies sliding window processing with stride=8 using windowSelectors, initializes a point accumulator to identity, and for each window computes the current window point using BLS12_381_G2WindowMul, adds it to the accumulator using BLS12_381_G2Add, and outputs the accumulated public key.

2.2.3 KeyGen Phase: Off-chain User Key Generation

The core of KeyGen phase off-chain computation is to generate user attribute key $SK_{\{GID, u\}} = \{K_{\{GID, u\}} = g^{\alpha_{\theta}} * H(GID)^{y_{\theta}} * F(u)^t, K'_{\{GID, u\}} = g^{y_{\theta}}\}$. When computing, three G_1 group element multiplications are involved, and the constraints are reduced by 'batch addition verification'. $g^{\alpha_{\theta}}$ is first verified by unequal point addition, then added to $H(GID)^{y_{\theta}}$, and scalar multiplication is optimized by a 'sliding window (stride=8)'. $H(GID)$ and $F(u)$ need to verify the legitimacy of the hash result. Through the Optimized simplified SWU map, the hash value of attribute u is mapped to the G_2 group point, and the 'carry free field operation' is used to reduce the constraint of Fp2 multiplication.

2.3 Storage Structure Construction

Due to the rapid expansion of blockchain users and the surge of the total amount of Zero Knowledge Proof (ZKP), the full on-chain storage will face two major challenges: 1) the blockchain storage pressure increases sharply and the Gas consumption is huge; 2) The construction of full proof tree leads to high addressing

overhead, which is difficult to be solved by traditional repository table or cross-chain scheme. This paper proposes Linked Event chain as a storage structure scheme:

1. Based on Solidity event mechanism: Adopt linked list design to store proof update records. The Event store of each block records the proof update corresponding to the current block height, and the reverse traversal is realized by the block height index.
2. Hierarchical storage architecture: The ZKP tree was stored in IPFS, and only the root ZKPRoot was uploaded to the blockchain. The Merkle tree root address was used as the index to record the latest updated block height of each proof in the contract. By updating the event record, the attribute and the preorder block height are proved, and the chain traceability structure is formed.
3. Query logic: get the latest block height by contract mapping, and reverse traverse the Event log to merge proof update records.

3. Experimental Analysis and Discussion

In this study, the performance was evaluated in a standardized experimental environment. The hardware platform is configured on a computer with Ubuntu 22.04 64-bit operating system, 32-core (vCPU) 256 GiB, ecs.r6.8xlarge. Circom 2.1.6 compiler is used to build arithmetic circuits in the software environment. The test case contains two core operations in the MA-CPABE scheme: the public and private key verification process and hash calculation. For each test scenario, we systematically measure the execution time of four key phases: Circuit Compilation, Witness Generation, Proving Time and Proof Verification. All time data are recorded in seconds. Each experiment was repeated 10 times and averaged to eliminate fluctuations.

3.1 Security Analysis

4.1.1 q-DPBDHE2 Hypothesis

This assumption is defined as follows: in a prime order bilinear group, an attacker cannot distinguish random $q+1$ elements in $\mathbb{Z}_p \times \mathbb{Z}_p$ from $e(g, g)^{(sa)}$, where sa is a random element in $\mathbb{Z}_p$ and q is the maximum size of the challenging access structure matrix. This assumption ensures that in the static security game, the challenger can turn the advantage of the attacker into the advantage of breaking the assumption of q-DPBDHE2 by 'simulating the attack environment', so as to prove the security of the scheme.

3.1.2 Static Security Analysis

The challenger is responsible for initializing the system, responding to the attacker's query, constructing the challenge ciphertext, and finally determining whether the underlying cryptographic assumption (q-DPBDHE2 assumption) can be broken through the attacker's guess results. It includes generating non-corrupt authority public key, user key, and encrypting challenge message randomly. The attacker outputs a guess b' , and the simulator results from the challenge of judging the hypothesis of q-DPBDHE2: If $b' = b$: indicates that the attacker successfully distinguishes M and M^* , that is, in CT is correctly identified as $e(g, g)^{(q+1)}(sa)$. If $b' \neq b$: indicates that the attacker did not distinguish successfully, T is regarded as a random element. If the attacker breaks the scheme statically with a non-negligible advantage, the simulator can distinguish the challenges of the q-DPBDHE2 assumption with the same advantage. However, the q-DPBDHE2 assumption is proved to be computationally difficult in the prime order bilinear group, so there is no such PPT attacker, and the scheme is secure under the static security model.

3.2 Performance Analysis

1) Performance comparison of elliptic curve: Fig. 2 shows the performance of different elliptic curves in public and private key verification tasks and hash calculation. In the task of public and private key verification, the BN254 curve shows a significant advantage in the proof generation stage (3s vs 5s), and the two curves have similar performance in other stages. This difference stems from the modulo operation overhead caused by the larger domain size of BLS12-381. In the hash computation task, BN254 also maintains about 20% performance advantage, especially in the proof generation phase (59s vs 71s).

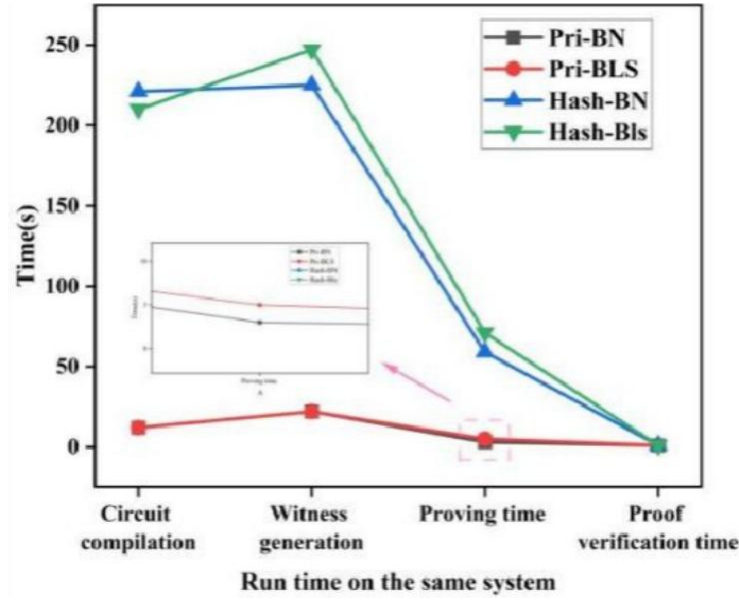


Fig. 2 Comparison of elliptic curve performance

2) Proof system performance comparison: A comparative test under the BN254 curve reveals significant differences in the proof systems. Groth16 takes only 3 seconds in the proof generation phase for public and private key verification, while Plonk takes 294 seconds, a difference of two orders of magnitude. This gap is further amplified in the hash computation task, where Groth16 (59s) is 93 times faster than Plonk (5535s), which is mainly attributed to the polynomial commitment computation overhead introduced by Plonk's universal trusted setting. It is worth noting that both systems maintain excellent performance of 1 second in the verification phase.

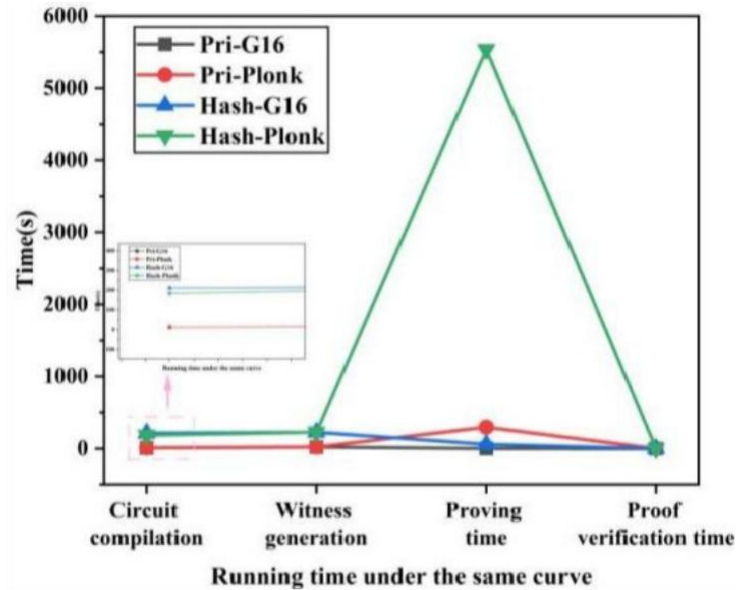


Fig. 3 Performance comparison of different proof systems

4. Conclusion

This paper focuses on the ciphertext access control scenario of the combination of blockchain and MA-CPABE. Aiming at the pain points of the existing schemes relying on a central authority, high computation overhead on the chain, and unverifiable key correctness, an innovative scheme with the core of 'intensive computation off chain + zero-knowledge verification on the chain + hybrid storage optimization' is proposed. The system generated attribute authorization nodes through the pledged election of blockchain nodes, moved the compute-intensive operations in the AuthSetup and KeyGen phases of MA-CPABE to the off-chain, used signed overflow representation to optimize large integer storage, and used window method (stride=10) to optimize scalar multiplication. Based on the Circom framework, a Circuit Zero-knowledge Proof (CZKP) protocol was designed to verify the correctness of the calculation. At the same time, the hybrid storage structure of 'zero-knowledge proof tree + event chain' is innovated, and the proof tree is stored at the root of IPFS only up-chain tree, and the storage and Gas overhead are greatly reduced by incremental updating of event chain records. Experiments show that under the combination of BN254 curve and Groth16 system, the generation of public and private key verification proof takes only 3 seconds, the Gas cost is reduced, and the anti-DDoS and anti-attack capabilities are verified by static security game. On the whole, the scheme achieves the balance of decentralized attribute authorization, trusted off-chain computation and low-cost on-chain verification, which provides an efficient and feasible solution for distributed data security sharing. However, the current static security model cannot deal with adaptive attacks, and the adaptive security mechanism and recursive zero-knowledge proof optimization can be further explored in the future.

5. References

- [1] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE symposium on security and privacy (SP'07). IEEE, 2007:321-334.
- [2] Chase M. Multi-authority attribute based encryption[C]//Theory of Cryptography: 4th Theory of Cryptography Conference, TCC 2007. Springer, 2007:515-534.
- [3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Satoshi Nakamoto, 2008.
- [4] Sandhia GK, Raja SVK. Secure sharing of data in cloud using MA-CPABE with elliptic curve cryptography[J]. Journal of Ambient Intelligence and Humanized Computing, 2022, 13(8):3893-3902.
- [5] Zou Y, Peng T, Wang G, et al. Blockchain-assisted multi-keyword fuzzy search encryption for secure data sharing[J]. Journal of Systems Architecture, 2023, 144:102984.
- [6] Hou X, Zhang L, Wu Q, et al. Collusion-resistant dynamic privacy-preserving attribute-access control scheme based on blockchain[J]. Journal of King Saud University-Computer and Information Sciences, 2023, 35(8):101658.
- [7] Chen T, Ren Z, Yu Y, et al. Lattices-Inspired CP-ABE from LWE Scheme for Data Access and Sharing Based on Blockchain[J]. Applied Sciences, 2023, 13(13):7765.
- [8] Xue J, Shi L, Zhang W, et al. Poly-ABE: A traceable and revocable fully hidden policy CP-ABE scheme[J]. Journal of Systems Architecture, 2023, 143:102982.
- [9] Ren Z, Yan E, Chen T, et al. Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof[J]. Journal of King Saud University-Computer and Information Sciences, 2024, 36(3):101969.
- [10] Hafid A, Hafid AS, Samih M. Scaling blockchains: A comprehensive survey[J]. IEEE access, 2020, 8:125244-125262.
- [11] Zhou Q, Huang H, Zheng Z, et al. Solutions to scalability of blockchain: A survey[J]. IEEE Access, 2020,

8:16440-16455.

- [12] Eberhardt J, Heiss J. Off-chaining models and approaches to off-chain computations[C]//Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. 2018:7-12.
- [13] Heiss J, Gruenwald E, Tai S, et al. Advancing blockchain-based federated learning through verifiable off-chain computations[C]//2022 IEEE International Conference on Blockchain. IEEE, 2022:194-201.
- [14] Zeng SQ, Huo R, Huang T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1):134-151.
- [15] Gao J, Yu H, Zhu X, et al. Blockchain-based digital rights management scheme via multiauthority ciphertext-policy attribute-based encryption and proxy re-encryption[J]. IEEE systems journal, 2021, 15(4):5233-5244.
- [16] Guo Z, Wang G, Li Y, et al. Accountable attribute-based data-sharing scheme based on blockchain for vehicular ad hoc network[J]. IEEE Internet of Things Journal, 2022, 10(8):7011-7026.
- [17] Zhang X, Du W, Moshayedi AJ. A traceable and revocable multi-authority attribute-based access control scheme for mineral industry data secure storage in blockchain[J]. The Journal of Supercomputing, 2023, 79(13):14743-14779.
- [18] Xu Z, Pan T, Han H, et al. Blockchain-Based Traceable Multi-Level Revocation Attribute-Based Encryption[J]. IEEE Access, 2024.
- [19] Yang Y, Chen X, Chen H, et al. Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing[J]. IEEE Access, 2018, 6:18009-18021.
- [20] Ren Z, Yu Y, Yan E, et al. L2-MA-CPABE: A ciphertext access control scheme integrating blockchain and off-chain computation with zero knowledge proof[J]. Journal of King Saud University-Computer and Information Sciences, 2024, 36(10):102247.
- [21] Rouselakis Y, Waters B. Efficient statically-secure large-universe multi-authority attribute-based encryption[C]//International Conference on Financial Cryptography and Data Security. Springer, 2015:315-332.
- [22] Belles-Munoz M, Isabel M, Munoz-Tapia JL, et al. Circom: A circuit description language for building zero-knowledge applications[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 20(6):4733-4751.