Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8849363, 7 pages
https://doi.org/10.1155/2020/8849363

WILEY | Hindawi

Research Article

A Novel Blockchain Identity Authentication Scheme Implemented in Fog Computing

Huijuan Wang and Yong Jiang

Information Security Department of the First Research Institute of the Ministry of Public Security of P.R.C., Beijing 100084, China

Correspondence should be addressed to Huijuan Wang; whj409@163.com

Received 18 April 2020; Revised 16 June 2020; Accepted 9 July 2020; Published 1 August 2020

Academic Editor: Fuhong Lin

In a fog computing environment, lots of devices need to be authenticated in order to keep the platform being secured. To solve this problem, we turn to blockchain techniques. Unlike the identification cryptographic scheme based on elliptic curves, the proposed 2-adic ring identity authentication scheme inherits the high verification efficiency and high key distribution of sequence ciphers of 2-adic ring theory, and this algorithm adds identity hiding function and trading node supervision function by design. The main designed application scenario of this solution is applicable to the consortium blockchain, and the master nodes are mutually trusting cooperative relations. The node transaction verification and block generation consensus algorithm designed in this solution can be implemented in a set of algorithms, which has higher verification efficiency and easier to be deployed than other solutions. This scheme can be widely used in the fog computing environment.

1. Introduction

Security is very important in each network. The fog computing, which extends the function of cloud computing, has attracted lots of attention [1]. The main idea is pushing the centralized function to decentralized function. There are many varieties, such as edge computing and cloudlet [2–4]. The decentralized network means that there needs to be an identity authentication scheme to keep the environments being secured. The blockchain has built a new trusted large-scale assistance method based on the information Internet to solve the trust problem of the development of the digital economy. As a new technology, blockchain technology has the characteristics required by various application scenarios such as transparency and credibility, tamper resistance, traceability, and decentralization. Applications have been extended from the financial field to supply chain management, government services, energy copyright storage, Internet of Things [5], fog computing, and other fields. In a narrow sense, a blockchain is a type of chained data that combines data blocks in a chronological order in a sequential manner and uses cryptography to ensure a tamper-proof and unforgeable distributed ledger. Broadly speaking, blockchain technology uses blockchain data structure blocks to verify and store data, uses distributed node consensus algorithms to generate and update data, and uses cryptography to ensure the security of data transmission and access. A smart contract composed of script code turns into and operates a new distributed infrastructure and computing paradigm for data. Unlike the traditional centralized structure, the blockchain mechanism does not rely on a specific central node to process and store data, so information leakage caused by malicious centers or other reasons can be avoided. In the actual application scenarios of blockchain, hash functions and digital signature algorithms are widely used in blockchain to verify the correctness of blocks and transactions. The traditional PKI mechanism does not conform to the "decentralized" characteristics of the blockchain because the weight of the trusted center is too large, so certificateless encryption and signature schemes are mostly used in blockchain technology.

There are actually two functions in the blockchain that need to be appropriately adapted to the practical application. One is how to increase the supervision function in the decentralized architecture, and the other is how to ensure the

privacy of user information under supervision. In 2012, Yu et al. [6] proposed a certificateless signature scheme that can be proved safe under the standard model. However, this scheme requires more than 5 bilinear pairing operations, and the calculation efficiency is low. In the same year, Gong and Li [7] proposed a certificateless password mechanism based on elliptic curves, but the resistance to participating node attacks was weak. In 2013, Miers and others [8] proposed an anonymous blockchain digital currency scheme based on Bitcoin. This scheme uses zero-knowledge proof cryptography technology to ensure the transaction by hiding the user address and cutting off the contact between the two parties. The nonrelevance of the system can achieve the untraceable effect, but the scheme needs to maintain the currency revocation list at the node to ensure the uniqueness of the transaction, which affects the efficiency of the transaction to a certain extent. In 2016, Shen and Adam proposed ring-based signatures. In 2016, Shen and Adam [9] proposed a ring-based signature secret transaction scheme. This scheme randomly selects irrelevant addresses and performs ring signatures together with the transaction initiator to achieve the purpose of confusing the identity of the transaction user. However, both the scheme and the zero-coin scheme have the problem of poor traceability due to the cutoff of the transaction association, which is difficult to be applied in actual scenarios, and the amount of single transaction information is too large. The anonymity of the scheme depends on the number of addresses participating in the ring signature. To reduce the amount of transaction information and reduce the number of addresses, you will also face the risk of deanonymization. The combination of blockchain and identification password can solve part of the problem of blockchain decentralization supervision. SM9 is an identification password, and there are a large number of blockchain identification password systems designed based on SM9 at home and abroad. Taking the consortium blockchain in the blockchain as the application environment, performing exponential operation and bilinear pairing operation can be the consortium blockchain. The application provides effective security and privacy protection support.

In this paper, we introduce an identification cryptographic scheme suitable for consortium blockchain based on the 2-adic ring algorithm. The 2-adic ring [10] is a finite ring that can correspond to any bit string in a finite field. When designing with this theoretical basis, it can inherit the recognition and verification efficiency of binary sequence ciphers in computer communication and can solve a large number of node verification of key distribution issues. Part of the security of passwords is based on the 2-adic ring theory. For an attacker, you need to be familiar with the 2-adic ring theory to recognize the algorithm and increase the difficulty of supply.

This article is mainly composed of the following parts. The second part introduces the basic preliminaries; this part introduces the blockchain and consortium blockchain and the identification password and introduces the basic knowledge of the 2-adic ring to facilitate the reader to understand the subsequent security proof; the third part describes the design of the main cryptographic scheme in this article, the blockchain identification authentication scheme based on the 2-adic ring algorithm, and introduces the node composition and transaction implementation process of the scheme in the consortium blockchain; the fourth part proves and analyzes the security of the scheme attack resistance and finally summarizes the applicable scenarios of the program and suggestions for improvement.

2. Preliminary Knowledge

2.1. Blockchain and Consortium Blockchain. Blockchain technology is built on the Internet. Using P2P, distributed storage, and distributed key ideas, a chronological sequence of data blocks is combined into a specific data structure in a chain. The chain structure of the blockchain uses cryptographic signatures to ensure that the chain connection of the data cannot be tampered with or forged. It can store a full amount of light time-series fingerprint data. The blockchain can be used as a data record database. The database is shared by network nodes. When nodes update data, they submit data records. Through the consensus mechanism, the data consistency between nodes is ensured. After the consistency is determined, the records like blockchain will never be changed or deleted.

The blockchain will also have different architectures due to different deployment environment models, such as public chain/consortium chain/private chain and side chain/crosschain. The encryption scheme in this article is mainly implemented in the consortium chain. In the consortium chain, the validity of the blockchain and the validity of the transaction are determined by a predetermined group of validators. This verification group forms a consortium chain. The consortium chain has the verification nodes and data changes initiated by the group of validators. The shared participating nodes are composed together.

2.2. Identification Password Algorithm. The identification cryptosystem means that the signer holds an identification and a corresponding private key. The private key is generated by the Key Generation Center (KGC) through the combination of the private key and the signer's identification. The signer uses his own private key to generate a digital signature on the data, and the verifier uses the signer's logo to generate his public key to verify the validity/authenticity/integrity and legal identity of the signature. SM9 logo ciphers generally involve the calculation of bilinear pairs on finite fields/elliptic curves/elliptic curves. The 2-adic ring algorithm logo ciphers designed in this paper involve knowledge of finite field 2-adic rings.

Identification password verification steps are as follows:

(i) Create a polynomial identification cryptographic algorithm to produce public and private keys

(ii) Set up a management node and establish an interactive protocol with the user. Executing this protocol can generate the private key and member certificate of the management node and use the private key of the group member of the group administrator

(iii) Using an identification password signature algorithm, after entering a message and a member private key, the signature of the message is output

(iv) Verify the original message/message signature/public key

(v) Confirm the legality of the signature

2.3. 2-Adic Integer and Arithmetic Crosscorrelation. Let binary strictly periodic sequence $\underline{s} = s(0), s(1), s(2), s(3), \cdots$, have the least period T, $s(t+T) = s(t)$. A 2-adic integer is a formal power series $\omega = \sum_{t=0}^{\infty} s(t) \bullet 2^t$, with $s(t) \in \{0, 1\}$. The set Z_2 of the 2-adic integers forms a ring under the operations of addition and multiplication with carry [11], the string $000\cdots$ as merely, and the string $100\cdots$ as 1, and define $1 + 2 + 2^2 \bullet\bullet\bullet = -1$, the infinite string $111\cdots$ is a base 2 expansion of a negative integer -1.

Specifically, the addition of Z_2 integers is given by

$$\sum_{t=0}^{\infty} s_1(t) \bullet 2^t + \sum_{t=0}^{\infty} s_2(t) \bullet 2^t = \sum_{t=0}^{\infty} s_3(t) \bullet 2^t, \quad s_1(t) + s_2(t) = s_3(t) + 2d_{t+1} - d_t. \tag{1}$$

$d_0, d_1, d_2, \bullet\bullet\bullet$, are carry integers, such that $d_0 = 0$, and for all $t \geq 0$.

Similarly, there are multiplications of Z_2 integers [11].

Let $q = 1 + q_1 2 + q_2 2^3 + \bullet\bullet\bullet + q_r 2^r$ be an odd integer, then the negative integer $-q$ is associated to the product

$$-q = \left(1 + 2 + 2^2 + 2^3 + \bullet\bullet\bullet\right)\left(1 + q_1 2 + q_2 2^2 + \bullet\bullet\bullet + q_r 2^r\right). \tag{2}$$

In Z_2, the formal power series $-q$ has a unique (multiplicative) inverse

$$(-q)^{-1} = 1 \bullet 2^0 + b_1 \bullet 2^1 + b_2 \bullet 2^2 + b_3 \bullet 2^3 + \bullet\bullet\bullet. \tag{3}$$

Thus, the ring Z_2 contains every rational number h/q provided q is odd.

Proposition 1 (see [11]). *There is a one-to-one correspondence between rational numbers $\omega = h/q$ (where q is an odd number) and eventually periodic binary sequences $\underline{s}$, which associates to each rational number ω and the bit sequence $\underline{s} = s(0), s(1), s(2)\bullet\bullet\bullet$ of its 2-adic expansion. The sequence $\underline{s}$ is strictly periodic if and only if $\omega \leq 0$ and $|\omega| \leq 1$.*

In this correspondence, we use the operations in Z_2 to introduce the arithmetic crosscorrelation.

Definition 2 (see [11]). Let $\underline{s}_1$ and $\underline{s}_2$ be two strictly binary periodic sequences with period T, and let $0 \leq \tau < T$ and $\underline{s}_2^{\tau}$ be the τ shift of $\underline{s}_2$. Denote $\underline{\omega}_1$ and ω_2^{τ} as the 2-adic integers corresponding to the sequences $\underline{s}_1$ and $\underline{s}_2^{\tau}$. Then, the corresponding sequence $\underline{s}_3$ of $\omega_1 - \omega_2^{\tau}$ is strictly periodic or eventually periodic, and its period divides T. The shift arithmetic crosscorrelation $C^a_{s_1,s_2}(\tau)$ of $\underline{s}_1$ and $\underline{s}_2$ is the number of zeros minus the number of ones in one period of length T of $\underline{s}_3$.

3. Identity Authentication Scheme Based on 2-Adic Ring AC Algorithm

This paper proposes an information authentication scheme suitable for consortium blockchain technology. By broadcasting transaction information encrypted by user identity information in transaction information, multi-KGC signature calculation is performed to hide user identity and transaction continuity.

3.1. Node Composition. The nodes in this scheme are divided into a primary node and a secondary node. The primary node is responsible for initializing the parameters of the AC algorithm and KGC signature used in the blockchain, executing the consensus algorithm for generating new blocks in the blockchain, participating in the continuous generation of blocks, and managing the joining of secondary nodes and distribution of related key. There can be multiple KGCs in a system, and new KGCs can only be added after they are approved by other KGCs. Each KGC has its own specific ID number and at a fixed time interval randomly generates an ID-based ID based on an algorithm P_i, $P_i = H(\mathrm{ID}_i \| \mathrm{hid}, N)$. In a fixed period of time, KGC generates a large prime P based on $(P_1, P_2, \bullet\bullet\bullet, P_i, \bullet\bullet\bullet, P_N)$ according to the self-energy contract code. The secondary node A and B transaction information generates random numbers k_A and k_B and generates $(F(P, k_A), F(P, k_B))$. Each KGC generates its own key $(F(P_i, k_A), F(P_i, k_B))$. Secondary node A receives $F(P, k_A)$, and secondary node B receives $F(P, k_B)$.

Secondary nodes A and B generate e_A and e_B based on their ID numbers. Generate verification key pairs $(F(P, k_A, e_A), S_A)$ and $(F(P, k_B, e_B), S_B)$ according to contract algorithm. The secondary node holds its own signature key pair, and the secondary node is the user who signs the KGC. Conduct transactions between secondary nodes to complete the peer-to-peer transaction information transfer process. After the KGC negotiates the transaction, it will be broadcasted to the entire network, and the new block will write the transaction, which will be confirmed and effective by each KGC master node.

3.2. Transaction Process. The network transaction process is as follows.

3.2.1. Signature Generation. The secondary node A has to conduct transactions with the secondary node B, and the transaction task is n_{AB}. The secondary nodes A and B broadcast to the primary node KGC, and the secondary nodes A and B generate verification keys $e_A = H(\mathrm{ID}_A, n_{AB})$ and $e_B = H(\mathrm{ID}_B, n_{AB})$ according to their unique ID numbers IDA and IDB. Secondary node A retains e_A and secondary node B retains e_B. The main node KGC has its own characteristic ID number and generates an identification number identifier P_i during the time period of transaction n_{AB}, $P_i = H(\mathrm{ID}_i \| \mathrm{hid}, N)$. The contract can generate a large prime number P based on the identification $P_1, P_2, \bullet\bullet\bullet, P_i, \bullet\bullet\bullet, P_N$, and send $(F(P_i, k_A), F(P_i, k_B))$ to each KGC, $F(P, k_A)$ to the secondary node A, and $F(P, k_B)$ to the secondary node B. The primary node KGC holds $(F(P_i, k_A), F(P_i, k_B), n_{AB})$,

the secondary node A holds $(F(P, k_A), e_A)$, and the secondary node B holds $(F(P, k_B), e_B)$.

3.2.2. Signature Verification. The secondary nodes A and B conduct transactions, the secondary node A generates a key sequence $S_A = S(F(P, k_A), e_A, n_{AB})$ based on $(F(P, k_A), e_A)$, the secondary node B generates a key sequence $S_B = S(F(P, k_B), e_B, n_{AB})$ based on $(F(P, k_B), e_B)$, and the secondary nodes A and B send S_A and S_B to each other. The secondary node verifies the legality of the other party, and the formula is $C(S_A, S_B) = 0$ then the identity is legal. If $C(S_A, S_B) \neq 0$, it means that the secondary nodes A and B have not obtained the identification key issued by KGC and are not in the transaction, or the transaction has expired.

Compared with the verification algorithm of the identification standard, considering that there can be multiple KGC functional requirements in the consortium blockchain, the main KGC functions of the multi-KGC mode in this paper are allocated to the master node. The master node jointly participates in parameter maintenance and key generation, which meets the requirements of partial decentralization of the consortium blockchain. After verifying the identity and transaction legitimacy of the secondary nodes A and B, they are sent S_A, S_B, n_{AB} to KGC. Each KGC is calculated according to the competition and broadcasted to the main node KGC of the entire network. Each KGC writes a block after verification and broadcasts the secondary to the entire network. The transactions of nodes A and B are successfully included in the blockchain, and each KGC stores transaction information. Each KGC calculates (e_A, e_B) according to the competition of S_A, S_B, n_{AB} and broadcasts it to the main node KGC of the whole network. Each KGC writes the block after verification and broadcasts the transactions of the secondary nodes A and B to the whole network, storing transaction information.

In a blockchain transaction, when a node interacts with information, it needs to check the other party's information. KGC can find the key to which user A belongs according to the user information IDA it holds and check whether it is revoked and changed to determine the time of the transaction and legality. When revoking the secondary node, record the "obsolete" mark in the ID number of the member information to be revoked. Second, when the system parameters need to be updated, KGC can regenerate the system parameters and update the user information while retaining the system coefficients that were used.

3.3. Blockchain Generation and Verification. This paper proposes an authentication scheme based on the 2-adic ring algorithm, which is mainly applicable to the design architecture of the consortium blockchain. The main node KGC is responsible for the generation of the blockchain. Since the designed scenario is a cooperative relationship of KGC for mutual trust, the consensus algorithm for block generation designed by this scheme does not have strong block generation rewards and competition. We use semicompetitive and semirandom blockchain accounting right allocation to complete block generation. Since the various KGCs do not trust and cooperate with each other, we rule out malicious forks of the blockchain.

When the secondary nodes A and B initiate the transaction n_{AB}, the number $n_{*_{AB}}$ to which the last associated transaction information belongs and the hash value $H(n_{*_{AB}})$ to which A belongs to in the last associated transaction need to be added. The master node KGC needs to publish whether transaction n_{AB} is the last related transaction of $n_{*_{AB}}$ and confirm whether the transaction between nodes A and B is legal. The block record information $H(n_{AB}) = H(e_A, e_B, n_{AB} H(n_{AB}))$ of n_{AB} is generated after the transaction.

The new block needs to record the number and hash value of the previous block to ensure the continuity of the block. Each node needs to confirm the legality of generating the identity of the master node when receiving the heart block, and after the latest block is associated, the transaction information verification process is performed.

3.4. Specific Process. Based on the ID number of the secondary node in this solution, the identification authentication key e can be generated, which can protect the privacy information of the secondary node, and can be designed to add the identification information of KGC to the ID when generating e, so that KGC can be authorized under certain conditions and it can identify the identity of secondary nodes and realize the supervision of individuals and transactions. In actual scenarios, it can be used for Internet transactions based on citizen ID numbers. Each KGC can include a supervisory unit that issues citizen ID numbers. Internet applications that require identification, banks, governments, communication companies, schools, and other departments, need to confirm their identities and business handling and transactions.

The specific process is as follows (Figure 1):

(i) The secondary nodes A and B initiate the creation of transaction n_{AB}, and the secondary nodes A and B each verify the legitimacy of n_{AB}. According to the last associated transaction $n_{*_{AB}}$, both parties send a transaction request n_{AB} to the primary node, KGC, after authentication by both parties

(ii) After receiving the transaction request n_{AB}, each KGC generates a time-stamped large prime number P at a time interval and generates a verification key $(F(P, k_A), F(P, k_B))$; each KGC generates its own key $(F(P_i, k_A), F(P_i, k_B))$, sends $F(P, k_A)$ to the secondary node A, and sends $F(P, k_B)$ to the secondary node B

(iii) The secondary nodes A and B generate e_A and e_B through the smart contract encryption algorithm according to their respective ID numbers, generate authentication keys S_A and S_B, and send it to each other

(iv) Secondary nodes A and B verify if each other's identity is legal and send $F(F(P, k_A), F(P, k_B), e_A, e_B)$ to all KGC after authentication

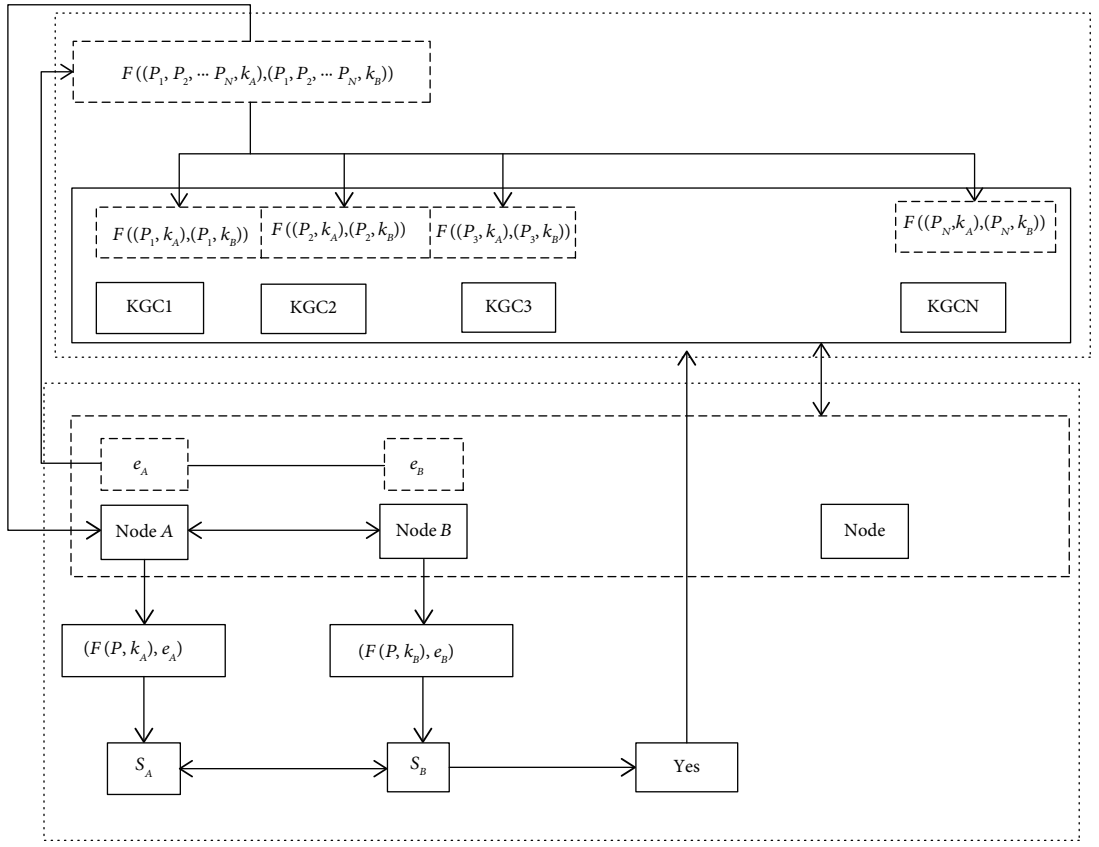

Figure 1: The flowchart of 2-adic ring AC algorithm.

(v) After each KGC receives $F(F(P, k_A), F(P, k_B), e_A, e_B)$, it competes to calculate (e_A, e_B), obtain accounting power, and broadcast $H(n_{AB}) = H(e_A, e_B, n_{AB}, H(n_{AB}))$ to the entire network, and the transaction validation process ends

4. Solution Security Analysis

4.1. Proof of Correctness. We introduce the nature of the S_A sequence; for the detailed proof, please refer to the literature [12].

For each integer n, p is satisfied $(p > 7, 4/p - 1)$ on the Galois ring $Z/(p^e)$. There is a maximum period sequence $\underline{a} = \{a(t)\}_{t\geq 0}$, $\alpha(t) \epsilon GR(p^e, n)$ sequence $\underline{a} = \{a(t)\}_{t\geq 0}$ maximum period is $p^{e-1}(p^{n-1} - 1)$. Ring $Z/(p^e)$ maximum sequence $\underline{a} = \{a(t)\}_{t\geq 0}$ composition of the sequence set is defined as $A_{p^e,n}$. The sequence $\underline{s} = \{s(t)\}_{t\geq 0}$ generated by $\underline{a} = \{a(t)\}_{t\geq 0}$ is defined by the following:

$$s(t) = \begin{cases} 1, & a(t) \epsilon C_0 \cup D_0, \\ 0, & a(t) \epsilon C_1 \cup D_1, \end{cases} \quad (4)$$

where $C_0 = \{a_t \epsilon Z/(p^e) | a(t) \bmod p = 0 \text{ and } t \bmod 4 = 0 \text{ or } t \bmod 4 = 3\}$; $C_1 = \{a_t \epsilon Z/(p^e) | a(t) \bmod p = 0 \text{ and } t \bmod 4 = 0 \text{ or } t \bmod 4 = 2\}$; $D_0 = \{a_t \epsilon Z/(p^e) | a(t) \bmod p \neq 0 \text{ and } a(t) \text{ is quadratic residual}\}$; $D_1 = \{a_t \epsilon Z/(p^e) | a(t) \bmod p \neq 0 \text{ and } a(t) \text{ is nonquadratic residual}\}$.

The sequences generated by the largest periodic sequence of integers n in the $Z/(p^e)$ form a binary periodic sequence set. The largest periodic sequences make up the set $S(p^{e_1}, n)$ and period is $2 \bullet p^{e-1}(p^n - 1)/(p - 1)$. Any two sequences $\underline{s}_1$, $\underline{s}_2$ in set $S(p^{e_1}, n_1)$, $S(p^{e_1}, n_2)$ $(e_1 \neq e_2, n_1 \neq n_2)$ satisfy $C_{\underline{s}_1 \underline{s}_2}{}^{a} = 0$ [12].

The key point of the 2-adic ring AC algorithm proves is the arithmetic correlation property of sequence S, it has been proven readers may refer to [12].

4.2. Solution Security Analysis

4.2.1. Unforgeability Analysis. Identification signature e_A of the secondary node A: because the IDA number is generated based on identity e_A, if the attacker forges identity e'_A and forges the verification sequence password S'_A, it is necessary to verify whether it is legal. Because the attacker cannot get $F(P, k_A)$, so this scheme can resist identity forgery.

Forged identity signature on KGC attack on master node P'_A: due to the overall design of the scheme, each KGC does not participate in the transaction, but only serves as transaction authentication and block generation, and the generation of block accounting rights is semirandom and does not rely too much on computing power and rights. Therefore, the attacker attacks KGC to obtain its own possibility of accounting rights. During the attack, there is no valuable information interaction between the malicious primary node and the malicious secondary node.

Table 1: Scheme efficiency and safety comparison.

Program	Signature efficiency	Verification efficiency	Forgery attack	Transaction information
SM9	$T_M + T_E$	$T_B + T_M + 2T_E$	Satisfy	25 KB
CPKC [3]	$4T_M + 7T_E$	$5T_B + T_M + T_E$	Satisfy	15 KB
CSS [13]	$T_M + 4T_E$	$3T_B + T_M + T_E$	Satisfy	20 KB
2-Adic ring arithmetic authentication scheme	$2T_M + T_E$	$2T_B + T_M$	Satisfy	5 KB-10 KB

Therefore, as long as there is any credible KGC, this scheme can resist forged malicious attacks.

4.2.2. Forward and Backward Security. When the system parameters of the identification password scheme need to be updated, KGC needs to renegotiate a new random number, determine a new identification signature based on its ID number, and issue new transaction keys to participating nodes. The previous system parameters should still be retained, and the node can verify the signature before the update based on the parameters in effect at the time. As for the system parameters, since the random numbers are randomly selected, there is no connection between the two before and after the update, and the attacker cannot forge the key before the update based on the key at the current stage. If the attacker holds the key before the update, he cannot join the participating nodes to forge the signature at the current stage.

4.3. Solution Efficiency and Safety Analysis. This solution is based on the 2-adic arithmetic correlation algorithm design. The legality verification key between nodes is a binary sequence string, which inherits the efficiency of sequence verification in communication. And each KGC competes to generate blocks with a simple polynomial time complexity, so the overall design scheme has higher verification block efficiency. In order to illustrate the operational efficiency and safety of this solution, this article lists several typical solutions for comparison (Table 1); T_E represents exponential calculation time, T_M represents the dot multiplication operation time of the elements in the ring, and T_B represents the homomorphic mapping operation time. Performance comparison and analysis table is available.

5. Conclusion

This article turns to the basic design ideas of the identification password and the functions of the main nodes of the consortium blockchain as the entry point. Using 2-adic ring theory and arithmetic related algorithms, a new identification password authentication scheme applied in consortium blockchain is designed to serve the fog computing devices. Under the premise that the master node trusts each other, the scheme designs the master node to bear the relevant functions of KGC and bear the responsibility of block generation and accounting. Through security proof and efficiency analysis, this scheme has signatures that cannot be forged, transaction node anonymity, and forward security. Because the scheme is designed to be in a trusted environment, transaction authentication and consensus protocols can be implemented with a set of algorithm schemes, so the computational efficiency is greatly improved compared to classic identification passwords such as SM9. This solution can realize the identity verification between nodes in terms of computing time and security and protect the privacy of the nodes, which meets the functional requirements of consortium blockchain multicentralization and protection of node identity information. How to generate blocks between master nodes with competitive interests will be the next step of research work.

Data Availability

The mathematical formula data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] X. An, X. Zhou, X. Lü, F. Lin, and L. Yang, "Sample selected extreme learning machine based intrusion detection in fog computing and MEC," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7472095, 2018.

[2] H. Hui, C. Zhou, S. Xu, and F. Lin, "A novel secure data transmission scheme in industrial Internet of things," *China Communications*, vol. 17, no. 1, pp. 73–88, 2020.

[3] M. Anwesha, D. Debashis, and G. Deepsubhra, "A power and latency aware cloudlet selection strategy for multi-cloudlet environment," *IEEE Transactions on Cloud Computing*, vol. 7, no. 1, pp. 141–154, 2019.

[4] F. Lin, Y. Zhou, X. An, I. You, and K.-K. R. Choo, "Fair resource allocation in an intrusion-detection system for edge computing: ensuring the security of Internet of things devices," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 45–50, 2018.

[5] C. Gong, F. Lin, X. Gong, and Y. Lu, "Intelligent cooperative edge computing in the Internet of things," *IEEE Internet of Things Journal*, 2020.

[6] Y. Yu, Y. Mu, G. Wang, Q. Xia, and B. Yang, "Improved certificateless signature scheme provably secure in the standard model," *IET Information Security*, vol. 6, no. 2, pp. 102–110, 2012.

[7] P. Gong and P. Li, "Further improvement of a certificateless signature scheme without pairing," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 2083–2091, 2014.

[8] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: anonymous distributed E-cash from Bitcoin," in *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2013.

[9] N. Shen and M. Adam, "Ring confidential transactions," *Ledger*, vol. 1, no. 1, pp. 1–18, 2016.

[10] M. Goresky and A. Klapper, "Arithmetic crosscorrelations of feedback with carry shift register sequences," *IEEE Transactions on Information Theory*, vol. 43, no. 4, pp. 1342–1345, 1997.

[11] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *Journal of Cryptology*, vol. 10, no. 2, pp. 111–147, 1997.

[12] H. J. Wang, Q. Y. Wen, and J. Zhang, "GLS: new class of generalized Legendre sequences with optimal arithmetic cross-correlation," *RAIRO - Theoretical Informatics and Applications*, vol. 47, no. 4, pp. 371–388, 2013.

[13] Y. Q. Li, J. G. Li, and Y. C. Zhang, "Certificateless signature scheme without random oracles," *Journal on Communications*, vol. 36, no. 4, pp. 185–194, 2015.