

Received March 23, 2020, accepted April 6, 2020, date of publication April 14, 2020, date of current version May 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987831

A Blockchain Privacy Protection Scheme Based on Ring Signature

XIAOFANG LI¹, YURONG MEI², JING GONG³, FENG XIANG⁴, AND ZHIXIN SUN^{2,3}

¹School of Computer Information Engineering, Changzhou Institute of Technology, Changzhou 213032, China

²Technology Research and Development Center of Postal Industry (Internet of Things), State Post Bureau, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

³Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

⁴National Engineering Laboratory for Logistics Information Technology, YTO Express Co., Ltd, Shanghai 200000, China

Corresponding author: Zhixin Sun (sunzx@njupt.edu.cn)


This work was supported in part by the National Natural Science Foundation of China under Grant 61972208 and Grant 61672299, and in part by the Jiangsu Collaborative Innovation Center for Cultural Creativity Fund under Grant XYN1902.

ABSTRACT Blockchain is a point-to-point distributed ledger technology based on cryptographic algorithms. However, the open and transparent blockchain ledger supplemented by statistical methods such as sociological mining and data mining has caused users' privacy to face major threats. Therefore, privacy protection has become a focus of current blockchain technology research. Ring signature technology is a commonly used encryption technology in the field of privacy protection. Therefore, this paper constructs a blockchain privacy protection scheme based on ring signature. This solution built a privacy data storage protocol based on the ring signature on the elliptic curve, and used the complete anonymity of the ring signature to ensure the security of data and user identity privacy in blockchain applications. The correctness and safety proof analysis of the proposed scheme were also carried out.

INDEX TERMS Blockchain, privacy protection, ring signature, elliptic curve.

I. INTRODUCTION

The concept of blockchain first appeared in the Bitcoin white paper of Nakamoto [1] in 2009. It is a new technology system derived from the underlying technology of Bitcoin. In essence, the blockchain is a decentralized, tamper-resistant distributed database, and the bottom layer is a chain structure of data blocks arranged in chronological order. The security of each link of the system is guaranteed by technologies such as cryptography. Because the blockchain has the characteristics of decentralization, tamper resistance, anonymity, and public verifiability, it has become the core technology of digital cryptocurrencies such as Bitcoin and Ethereum. Through the use of P2P networks, data encryption, time stamping, distributed consensus, and incentive mechanisms, nodes in the system can complete point-to-point transactions. This solves the problems of high trust, low efficiency, and insecure data storage in the centralized system [2]. With the widespread circulation of bitcoin, the research and application of bitcoin's core technology blockchain has shown explosive growth.

The associate editor coordinating the review of this manuscript and approving it for publication was Wenbing Zhao .

It is considered to be the fifth disruptive innovation in the computing paradigm after mainframes, personal computers, the Internet, and mobile social networks [3].

The high-quality technical characteristics of the blockchain make it widely used in fields other than digital cryptocurrencies. In the financial field, central banks of various countries attach great importance to blockchain technology, design their respective digital currencies through reference to research or direct applications, and use blockchain technology to improve the problems of long reconciliation and clearing time, low cross-border settlement efficiency, and high maintenance cost of central ledger data in traditional financial systems. In the field of the Internet of Things, the characteristics of point-to-point transactions and intelligent verification of blockchain technology are used to achieve different types of transactions between Internet of Things devices [4]. IBM has proposed to combine blockchain technology with IoT applications to form a "decentralized autonomous IoT." In the field of intellectual property, researchers have used blockchain's time stamping, anti-tampering and anti-forgery features to achieve data storage, copyright protection, and work identification. In addition, supply chain, judicial,

information authentication and other fields are gradually applying blockchain technology to improve existing industry problems [5].

With the deepening of research, while the blockchain has shown its vigorous vitality, its own security issues have gradually emerged. In the blockchain system, because there is no centralized organization to process and maintain data, all transactions in the system are open and transparent in order for each node to reach a consensus quickly. So it brings the problem of data privacy leakage. Although the address of the user in the blockchain is the hash value of its public key, which can avoid the exposure of the IP address of the transaction entity, the simplest pseudo anonymity mechanism is used to protect the privacy of the user's address in the blockchain. The attacker can speculate the real identity information of the user through big data analysis, cluster analysis and certain network attack means [6]. The inadequate protection of the privacy issues of the blockchain has led to frequent security issues such as blockchain privacy leakage in recent years. On June 17, 2016, more than 1/3 of the ETH in the Dao, a distributed autonomous organization with more than 150 million US dollars obtained through crowdfunding, were stolen by hackers, leading to the failure of the project [7]. On December 18, 2017, North Korean hackers attacked South Korea's cryptocurrency exchange, resulting in the theft of cryptocurrency worth 7.6 billion won (about 6.69 million US dollars) at the time and causing a large number of user privacy leaks. The open and transparent nature of the blockchain allows users to obtain all transaction information and material supply information, including amount, contract content, etc., thereby posing a threat to personal and national security. In the field of privacy protection, encryption is the most commonly used solution by researchers. Therefore, while using the blockchain technology, encryption technology should be used to provide a good solution for the privacy issue of the blockchain and ensure the user's information security.

The ring signature algorithm is a digital signature scheme, first proposed by Rivest *et al.* [8] in 2001. Ring signature technology belongs to a simplified group signature [9], which is a signature algorithm that leaks secrets anonymously. The ring signature contains only ring members and no managers. In this signature scheme, the signer randomly selects the public keys of multiple ring members, combines their public and private keys, random numbers, and other technologies to complete the signature. The verifier of the signature can only verify that the signature comes from this signature set, but does not know who signed the signature. Therefore, ring signature is very suitable for complaint reporting, election voting, electronic currency and other fields. Blockchain, as a public and transparent record ledger, brings open and transparent transactions as well as data privacy leaks. Therefore, this scheme adopts a ring signature transaction signature scheme to ensure the absolute anonymity of the user, thereby protecting the privacy of the users.

Aiming at the problem of data privacy leakage facing the current blockchain, combined with the characteristics of

ring signature technology, this paper proposes a blockchain privacy protection scheme based on ring signature. The ring signature is used to protect the information of the transaction initiator, thereby protecting the privacy of the blockchain. The remainder of this paper is organized as follows. Related works is reviewed in Section II. The preliminary knowledge and the scheme of this paper are given in Section III. In Section IV, the correctness and safety of the proposed scheme are theoretically proved. Finally, the conclusion is drawn in Section V.

II. RELATED WORKS

Blockchain privacy leaks and other security issues have prevented the development of blockchain technology in existing industries. In order to improve the anonymity of blockchain technology and protect the privacy of user identity and transaction data privacy, a variety of blockchain privacy protection schemes have been proposed. The currency mixing mechanism in digital currencies borrows from the idea of Chaum [10] published in 1981, mixing multiple unrelated inputs between the input address and the output address, making it impossible for the outside world to correlate the input and output of the transaction, so the flow of digital currency cannot be distinguished. Currently, Bitlaunder [11], Bitcoin Flog [12], Blockchain.inf [13] and other websites provide this mixed currency technology. Bonneau *et al.* [14] proposed a centralized coin mixing solution with audit function Mixcoin. As long as the third party node operates illegally, the user can publish the signature data and the funds can be returned to the user. At the same time, the third party node will lose its credibility and cannot provide services as a trusted third party. Valenta and Rowan [15] proposed a Blindcoin scheme using blind signature technology [16] to improve Mixcoin. The user uses a blind signature for the output address, so that a third party can provide coin mixing services without connecting the user's input address to the output address. Maxwell Gregory [17] proposed the CoinJoin scheme. The core of the scheme is to combine multiple transaction inputs to form a transaction. When the output address required by the user appears in the output address list, the user will sign the transaction. This scheme hides the relationship between transaction input addresses and output addresses. However, all the above-mentioned coin mixing schemes require the participation of a third party. As a third party providing mixed currency services, grasping the connection between the user's input address and the output address cannot evade cheating by third parties, and the problem of leaking user privacy still exists.

Dash [18] is a kind of "digital currency" for the purpose of protecting user privacy. It adopts chained hybrid and blind technology to realize the process of coin mixing and reduce the correlation between addresses. But Dash is a centralized method of mixing coins, which is vulnerable to attacks by malicious master nodes. Ruffing *et al.* [19] proposed a decentralized coin mixing scheme, CoinShuffle, which added the output address shuffle mechanism on the basis of CoinJoin, which can guarantee the completion of the coin mixing

function without the need for a third-party nodes to join. However, during the coin mixing process, participants are required to be online at the same time, so they are vulnerable to denial of service attacks.

Miers *et al.* [20] proposed a zero-coin protocol based on zero-knowledge proof [21] to solve the problem of user transaction address leakage. Users can hide the addresses of both parties to the transaction through Zerocoin, making the transaction un-link-able. However, Zerocoin can only mint and exchange fixed-value currency, and the data of Zerocoin's zero-knowledge proof is relatively large, which requires additional blockchain storage space and computing resources. Sasson *et al.* [22] proposed a new type of digital currency Zerocash based on Zerocoin. Zerocash encapsulate the trend and transaction amount of each transaction as a number of parameters into a commitment function to achieve the purpose of keeping the addresses and transaction amounts of both parties of the transaction confidential. At the same time, Zerocash applied the simple non-interactive zero-knowledge proof technology (zk-SNARK) to "digital currency" to achieve the highest degree of privacy and anonymity in current "digital currency" transactions. However, the process of generating a proof using a zero-knowledge proof algorithm is very slow. It usually takes 1 minute to generate a new proof, and there is a bottleneck in efficiency.

The data in the blockchain is stored in the public distributed ledger. As long as the user's private information and transaction information are deleted from the public database, the privacy issue of the blockchain will be fundamentally solved. Based on this idea, many off-chain payment schemes were proposed. Lightning network [23], two-way micro payment channel [24], Sprites [25], Bolt [26] and other off-chain payment technologies are used to provide reliable off-chain transactions, that is, most of the transaction details between users are in completed off-chain, users only need to record the first transaction and the last transaction process in the blockchain ledger. However, the existing off-chain transaction technologies all implement anonymous transactions between users through third parties, so there are still many shortcomings. For example, when an error occurs in a transaction, the user's transaction information needs to be publicly verified, and how to ensure the fairness of the transaction without leaking the user's privacy needs further improvement by researchers.

Ring signature is a special group signature. Compared to a general group signature, the unconditional anonymity and unforgeability of the ring signature make it more prominent in terms of privacy. Among digital currencies, Monero [27] used ring signature, ring confidential transactions, and encrypted addresses to obfuscate the source, amount, and destination of all transactions, providing users with greater privacy. Ring signature also play a very important role in business activities such as electronic payments and auctions. Thomas and Boyen [28] proposed a practical remote voting scheme called VOTOR, which used linkable ring signature and product anonymity channels to provide a higher level of privacy for this setting. Mourad *et al.* [29] introduced a new supply chain

traceability system based on the existence of privacy-sensitive information. The system used the MLSAG ring signature protocol to achieve confidentiality of privacy-sensitive information, and achieves traceability by hiding participants in public information of past transactions. Patil and Wasnik [30] used the ID-based ring signature technology to delete the certificate verification process and built a secure and reliable data sharing system, which guaranteed the privacy of the applicant. Aiming at the bottleneck of current PKI system that cannot support many users and their data, [31] adopted identity-based ring signature technology to protect personal anonymity during data sharing, and used forward security together with identity ring signature to improve data security. Reference [32] proposed a new ring signature scheme based on lattice difficulty to protect the privacy in the Internet of Vehicles. This scheme was different from the traditional public-key cryptography scheme for privacy protection, but was designed based on the problem of false learning on a lattice ring, which can ensure its security under the quantum algorithm attack. Compared with other schemes, the Gregory ring signature scheme achieves unconditional anonymity, and can also provide traceability for authorized parties when necessary. Surmila and Dilip [33] proposed an effective audit scheme based on CDH's ring signature for checking the integrity of dynamic data shared between a group of static and static users outsourced in untrusted cloud storage. This solution enabled third-party auditors to audit customer data without knowing the content, while retaining the privacy of the identity of auditors and members of the group who signed the data from the cloud server.

To sum up, this paper analyzes the related theories of ring signatures, uses the anonymity of ring signature technology, proposes a ring signature scheme based on Elliptic Curve Cryptography (ECC), and applies it to the privacy protection of blockchain. The advantages of this scheme are listed as following.

1. Compared with the bilinear pair-based scheme, it has better security under a key of the same length.
2. The protection of the identity of the signer is strengthened and improved
3. Compared with the scheme based on bilinear pairings, the unforgeability of the scheme is strengthened, which makes the probability of the attacker successfully cracking the key reduced.

III. ALGORITHM DESCRIPTION

A. PRELIMINARIES

1) ELLIPTIC CURVE

Suppose that there is a large prime number q , the integer field F_q takes q as the module, and there is a nonsingular elliptic curve $E_q(a, b)$ on the integer field F_q . The equation is as follows:

$$y^2 \bmod q = (x^3 + ax + b) \bmod q$$

Among them, $a, b, x, y \in F_q$ and $\Delta = (4a^3 + 27b^2) \bmod q \neq 0$.

If a point $P(x, y)$ satisfies the $E_q(a, b)$ equation, then the point $P(x, y)$ is a point on an elliptic curve, and the point $Q(x, -y)$ is the negative point of $P(x, y)$, that is $P = -Q$. Let points $P(x_1, y_1)$ and $Q(x_2, y_2)$ be points on the elliptic curves $E_q(a, b)$ and $P \neq Q$, the line l passes through the point P, Q and intersects the elliptic curve at the point $R' = (x_3, -y_3)$, the points of R' symmetrical about the x-axis are $R = (x_3, y_3)$ and $R = P + Q$.

The points on the elliptic curve $E_q(a, b)$ and the infinite point O together form an additive cyclic group of prime order q as follows:

$$G_q = (x, y) : a, b, x, y \in F_q, (x, y) \in F_q, (a, b).$$

Correspondingly, the double point operation defined on G_q is:

$$kP = P + P + \dots + P (k \in \mathbb{Z}_q^*).$$

2) PROBLEM-BASED ASSUMPTIONS

Definition 1: Define a function $\varepsilon(k)$. When k_0 exists for any $c > 0$, and $k \geq k_0$ exists, so that $\varepsilon(k) \leq 1/k^c$, $\varepsilon(k)$ is called the ignore function.

Definition 2 (Elliptic Curve Discrete Logarithm Problem (ECDLP)): P is the generator of G_q , there are $P, aP \in G_q$, the probability of the polynomial algorithm A solving the ECDLP problem in a limited time is $Adv_{A, G_q}^{ECDLP}(k) = P_r \left[A(P, aP) = a : a \in \mathbb{Z}_q^* \right]$

Definition 3 Discrete Logarithmic Assumption of Elliptic Curve: For all polynomial algorithms A within a limited time, there are some ignoring functions ε , $Adv_{A, G_q}^{ECDLP}(k) \leq \varepsilon$ exists, so the probability $Adv_{A, G_q}^{ECDLP}(k)$ is negligible.

3) SECURITY MODEL OF RING SIGNATURE

In this ring signature scheme, we will consider that the attacker \mathcal{A} : \mathcal{A} has not only the public keys of n signers, but also the private keys of some signers.

* **Gamer 1: the unforgeability of ring signature**

For \mathcal{A} , $Succ_{RS, \mathcal{A}}$ is defined as the probability that he and a challenger \mathcal{R} will succeed in Game 1 below.

1. **Initialization:** Given a security parameter l , the challenger \mathcal{R} runs the initialization algorithm to obtain the system parameters, and then the challenger \mathcal{R} sends the system parameters to the attacker \mathcal{A} ;
2. **Hash query:** When the attacker \mathcal{A} selects any value, challenger \mathcal{R} returns the corresponding hash value to \mathcal{A} .
3. **User public key query:** The attacker \mathcal{A} selects and asks a user's private key sk_i , and the challenger \mathcal{R} returns the corresponding public key pk_i to \mathcal{A} ;
4. **Private key query:** The attacker \mathcal{A} queries a user's private key sk_i , and the challenger \mathcal{R} returns the corresponding private key sk_i ;
5. **Ring signature query:** The attacker \mathcal{A} selects and submits a message m , and the challenger \mathcal{R} returns the corresponding ring signature σ to \mathcal{A} ;

6. **Forgery:** Finally, the attacker \mathcal{A} outputs the signature σ^* of another message m^* that satisfies the following conditions:
 - a. σ^* is a valid ring signature generated by the attacker \mathcal{A} ;
 - b. m^* does not appear in the ring signature query;

Definition 4: If the attacker \mathcal{A} makes a maximum of q_H hash queries, a maximum of q_U user public key queries, a maximum of q_P private key queries, and a maximum of q_{RS} ring signature queries within the maximum time T , \mathcal{A} can break the ring signature, then the probability of his success $Succ_{RS, \mathcal{A}}$ is at least ε . If no attacker can have $(T, q_H, q_U, q_P, q_{RS}, \varepsilon)$ break a ring signature, then we call the ring signature is $(T, q_H, q_U, q_P, q_{RS}, \varepsilon)$ existence unforgeable under adaptive selection message attack.

* **Gamer 2: the anonymity of ring signature**

Let $U = U_1, U_2, \dots, U_n$ be n users. In game 2, \mathcal{A} is an attacker and \mathcal{R} is a challenger.

1. The challenger \mathcal{R} performs initialization to calculate system parameters and sends it to the attacker \mathcal{A} .
2. The attacker \mathcal{A} adaptively makes a polynomial limited-order ring signature query.
3. In the challenge phase, the adversary outputs a message m , the public key set R of n users, two different public keys $pk_1, pk_2 \in R$, and sends all of them to the challenger \mathcal{R} . The challenger \mathcal{R} randomly selects a bit $pk \in \{0, 1\}$ and returns the ring signature $\sigma = \mathbf{A}ring(m, R, sk_u)$ to the attacker \mathcal{A} .
4. The attacker \mathcal{A} adaptively makes a polynomial limited-order ring signature query.
5. In the end, the attacker \mathcal{A} outputs a bit $pk' \in \{0, 1\}$.
6. Rival \mathcal{A} succeeded in this game if and only if $pk = pk'$.

Definition 5: Define the probability that an attacker \mathcal{A} succeeds in game 2: $Succ(\mathcal{A}) = P_r[pk = pk'] = 1/2 + \varepsilon$. The precondition for a ring signature to have unconditional anonymity is that no attacker can win Game 2 with a non-negligible probability advantage. In other words, for any polynomial time attacker, the advantage ε of winning Game 2 is negligible.

B. BLOCKCHAIN PRIVACY PROTECTION SCHEME BASED ON RING SIGNATURE

This section mainly introduces the use of ring signature technology to design a completely anonymous user data storage protocol under the blockchain architecture to ensure the privacy of user information in the blockchain. A smart contract is deployed in the blockchain network to monitor the dynamics in the network, and when preset conditions are met, a preset instruction is triggered to execute transaction T . As shown in Algorithm 1, the specific model is constructed as follows:

1. **SetUp(l):** Enter the safety parameter l . The safety parameter l is a large prime number large enough. Randomly select a large prime number $q > l$. G is a base point on the

elliptic curve. G_1 is a large prime q -order cyclic addition group. Output system parameters $par=\{q, G, G_1, P, H_0, H_1, H_2\}$, where P is the generator of G_1 , and the hash function are: $H_0: E(F_q) \rightarrow E(F_q)$, $H_1: \{0, 1\} \rightarrow F_q$, $H_2: \{0, 1\}^* \times G_1 \rightarrow Z_q^*$.

2. **KeyGen**(par) $\rightarrow (pk_i, sk_i)$: User $U_i(1 \leq i \leq n)$ in the blockchain system randomly selects $x_i \in Z_q^*$, calculate $pk_i \leftarrow x_i * P$, the user's public key is defined as $pk_i \in G$, and the private key is $sk_i = x_i \in Z_q^*$.
3. **Aring** $\rightarrow T_\sigma$: The transaction initiator s chooses a public key set $R=pk_1, pk_2, \dots, pk_n$, R is a set of public keys of members participating in the ring signature, and R does not include the public key pk_s of the transaction initiator, set the corresponding attribute values L_i, R_i for each public key pk_i according to the following steps:

- Randomly select $u_i, v_i, w_i \in Z_q^*$, and then calculate:

$$L_i = \begin{cases} (u_i + v_i) * G, & \text{if } i = s \\ u_i * G + (v_i + w_i) * pk_i & \text{if } i \neq s \end{cases} \quad (1)$$

$$R_i = \begin{cases} (u_i + w_i) * H_0(pk_i), & \text{if } i = s \\ u_i * H_0(pk_i) + (v_i + w_i) * I_s & \text{if } i \neq s \end{cases} \quad (2)$$

Among them: $I_s = sk_s * H_0(pk_s)$, which is a signature image of the message, is used to prevent double spend attacks in the system. $H_0(pk_i)$ maps pk_i to a point on the elliptic curve of the finite field.

- Randomly select $r \in Z_q^*$ and then calculate as follows:

$$h = H_2(m||r). \quad (3)$$

$$c_i = \begin{cases} H_1(h, L_1, \dots, L_n, R_1, \dots, R_n) - \sum_{i=1}^n c_i & \text{if } i = s \\ u_i * H_0(pk_i) + (v_i + w_i) * I_s & \text{if } i \neq s \end{cases} \quad (4)$$

$$d_i = \begin{cases} (u_i + v_i) - c_i * sk_i, & \text{if } i = s \\ u_i & \text{if } i \neq s \end{cases} \quad (5)$$

Among them: m represents the content of the signature, and finally the ring signature of the transaction initiator s to the message m is output as $T_\sigma=(I_s, c_1, c_2, \dots, c_s, \dots, c_n, d_1, d_2, \dots, d_s, \dots, d_n)$.

4. **Averify**: Anyone who has the public keys of all members participating in the ring signature can verify the transaction signature T_σ as follows:

$$\begin{cases} \gamma_i = d_i * G + c_i * pk_i \\ \delta_i = d_i * H_0(pk_i) + c_i * I_s \end{cases} \quad (6)$$

$$\sum_{i=1}^n c_i = H_1(h, \gamma_1, \gamma_2, \dots, \gamma_n, \delta_1, \delta_2, \dots, \delta_n) \quad (7)$$

Calculate γ_i, δ_i by formula 6, and then verify whether formula 7 is true. If it is true, verify whether the signature image I_s in the signature has been used. If it has not been used, the signature is valid, otherwise it is considered invalid signature.

The miner nodes in the blockchain network package the transaction set $T = (T_1, T_2, \dots, T_n)$ for a period of time, and then continuously calculate the random numbers that meet the conditions to construct blocks that meet the preset conditions for confirming transactions. After the new block is successfully constructed within the specified time, it is broadcast to the blockchain network. The node verifies the legality of the new block according to the block construction mechanism. If the new block is legal, the new block is added to the blockchain, other nodes in the blockchain network need to synchronize new blocks to get the next billing.

IV. ANALYSIS OF CORRECTNESS AND SAFETY PROOF

A secure ring signature scheme should meet the three aspects of correctness, unconditional anonymity, and unforgeability.

A. CORRECTNESS ANALYSIS

The verifier verifies the transaction signature T_σ according to the formula, and if it is true, the verification is passed.

$$\sum_{i=1}^n c_i = H_1(h, \gamma_1, \gamma_2, \dots, \gamma_n, \delta_1, \delta_2, \dots, \delta_n) \quad (8)$$

When $i \neq s$, the conversion of γ_i, δ_i is as follows:

$$\gamma_i = d_i * G + c_i * pk_i = u_i * G + (v_i + w_i) * pk_i = L_i \quad (9)$$

$$\delta_i = d_i * H_0(pk_i) + c_i * I_s = u_i * H_0(pk_i) + (v_i + w_i) * I_s = R_i \quad (10)$$

When $i = s$, the conversion of γ_i, δ_i is as follows:

$$\begin{aligned} \gamma_i &= d_i * G + c_i * pk_i \\ &= [(u_i + v_i) - c_i * sk_i] * G + c_i * pk_i \\ &= u_i * G + v_i * G \\ &= L_i \end{aligned} \quad (11)$$

$$\begin{aligned} \delta_i &= d_i * H_0(pk_i) + c_i * I_s \\ &= [(u_i + v_i) - c_i * sk_i] * H_0(pk_i) + c_i * sk_s * H_0(pk_s) \\ &= u_i * H_0(pk_i) + v_i * H_0(pk_i) \\ &= R_i \end{aligned} \quad (12)$$

Therefore, according to the above relationship, the correctness of the ring signature scheme proposed in this paper can be verified as follows:

$$\begin{aligned} &H_1(h, \gamma_1, \gamma_2, \dots, \gamma_s, \dots, \gamma_n, \delta_1, \delta_2, \dots, \delta_s, \dots, \delta_n) \\ &= H_1(h, L_1, L_2, \dots, L_s, \dots, L_n, R_1, R_2, \dots, R_s, \dots, R_n) \\ &= c_s + \sum_{i=1, i \neq s}^n c_i \\ &= \sum_{i=1}^n c_i \end{aligned} \quad (13)$$

B. UNFORGEABILITY ANALYSIS

Theorem 1: In the random oracle model, the attacker \mathcal{A} in Game 1 can adaptively choose a message to attack. Assuming

Algorithm 1 Elliptic Curve Cryptography-Based Ring Signature Algorithm

Input: a security parameter l ;
Output: a globally open parameter $par = (q, G_1, P, H_0, H_1, H_2)$;

- 1: **for all** U_i **do**
- 2: calculate $(pk_i, sk_i) \leftarrow \mathbf{KeyGen}(par)$;
- 3: **end for**
- 4: **for each** U_i involved in the transactions **do**
- 5: select ring signature members, and follow the steps below to generate a ring signature
- 6: randomly select $u_i, v_i, w_i \in Z_q^*$, and then calculate:
- 7:

$$L_i = \begin{cases} (u_i + v_i) * G, & \text{if } i = s \\ u_i * G + (v_i + w_i) * pk_i & \text{if } i \neq s \end{cases}$$
- 8:

$$R_i = \begin{cases} (u_i + w_i) * H_0(pk_i), & \text{if } i = s \\ u_i * H_0(pk_i) + (v_i + w_i) * I_s & \text{if } i \neq s \end{cases}$$
- 9: randomly select $r \in Z_q^*$ and then calculate as follows:
- 10:

$$h = H_2(m||r)$$
- 11:

$$c_i = \begin{cases} H_1(h, L_1, \dots, L_n, R_1, \dots, R_n) - \sum_{i=1}^n c_i, & \text{if } i = s \\ u_i * H_0(pk_i) + (v_i + w_i) * I_s & \text{if } i \neq s \end{cases}$$
- 12:

$$d_i = \begin{cases} (u_i + v_i) - c_i * sk_i, & \text{if } i = s \\ u_i & \text{if } i \neq s \end{cases}$$
- 13: **end for**
- 14: **for** anyone who owns the public keys of all participating ring signing members **do**
- 15: **while**

$$\begin{cases} \gamma_i = d_i * G + c_i * pk_i \\ \delta_i = d_i * H_0(pk_i) + c_i * I_s \\ \sum_{i=1}^n c_i = H_1(h, \gamma_1, \gamma_2, \dots, \gamma_n, \delta_1, \delta_2, \dots, \delta_n) \end{cases}$$
- 16: **do** receive this signature and complete the transaction
- 17: **end while**
- 18: **end for**

that the ECDLP game is successfully won within a valid polynomial time T , ECDLP can be successfully solved with a non-negligible probability.

Proof: If the challenger \mathcal{R} receives a random instance of the discrete logarithm problem $(P, a * P)$, the purpose is

to calculate the value of a . The challenger \mathcal{R} sets the public key of the signer U_* as: $pk_{i^*} = a * P$. \mathcal{R} is a subroutine of \mathcal{A} and plays the challenger of \mathcal{A} in Game 1. Without loss of generality, we assume that all inquiries are different. Now we will show how the challenger responds to the attacker \mathcal{A} 's query.

1. **Initialization:** Given a security parameter l , the challenger \mathcal{R} runs the initialization algorithm to obtain the system parameters, and then the challenger \mathcal{R} sends the system parameters to the attacker \mathcal{A} ;
2. **Hash query:** The challenger \mathcal{R} has an L list (α_i, β_i) . This list is initially empty. When the opponent \mathcal{A} asks $H(\alpha_i)$, the challenger \mathcal{R} chooses a random value β_i and sets $H_1(\alpha_i) = \beta_i$. The challenger \mathcal{R} adds (α_i, β_i) to the L list and returns β_i to \mathcal{A} .
3. **User public key query:** The challenger \mathcal{R} has an L list (α_i, β_i) . This list is initially empty. When the opponent \mathcal{A} asks $H(\alpha_i)$, the challenger \mathcal{R} chooses a random value β_i and sets $H_1(\alpha_i) = \beta_i$. The challenger \mathcal{R} adds (α_i, β_i) to the L list and returns β_i to \mathcal{A} .
4. **Private key query:** When the attacker \mathcal{A} makes a public key query to the user, if $pk_i = pk_{i^*}$, then \mathcal{R} stops operating, otherwise the challenger \mathcal{R} returns the corresponding private key sk_i to \mathcal{A} .
5. **Ring signature query:** The attacker \mathcal{A} submits a message m and the public key set R of n users, and the challenger \mathcal{R} outputs a ring signature T_σ , if a user identity $pk_s \in R$ satisfies $pk_s \neq pk_{i^*}$, then the challenger \mathcal{A} performs a signature algorithm to reply to the signature T_σ , where pk_s is the real signer. Otherwise, the challenger \mathcal{A} performs the following steps:
 - Randomly select $u_i, v_i, w_i \in Z_q^*$, and then calculate:

$$L_i = \begin{cases} (u_i + v_i) * G, & \text{if } i = s \\ u_i * G + (v_i + w_i) * pk_{i^*} & \text{if } i \neq s \end{cases} \quad (14)$$

$$R_i = \begin{cases} (u_i + w_i) * H_0(pk_{i^*}), & \text{if } i = s \\ u_i * H_0(pk_{i^*}) + (v_i + w_i) * I_s^* & \text{if } i \neq s \end{cases} \quad (15)$$

$$h = H_2(m||r). \quad (16)$$

$$c_i = \begin{cases} H_1(h, L_1, \dots, L_n, R_1, \dots, R_n) - \sum_{i=1}^n c_i & \text{if } i = s \\ u_i * H_0(pk_{i^*}) + (v_i + w_i) * I_s^* & \text{if } i \neq s \end{cases} \quad (17)$$

$$d_i = \begin{cases} (u_i + v_i) - c_i * sk_{i^*}, & \text{if } i = s \\ u_i & \text{if } i \neq s \end{cases} \quad (18)$$

- Finally, the ring signature for message m is output as $T_{\sigma^*} = (I_s^*, c_1, c_2, \dots, c_s^*, \dots, c_n, d_1, d_2, \dots, d_s^*, \dots, d_n)$.
6. **Forgery:** Finally, the attacker \mathcal{A} outputs the signature of another message m^* for the signer pk_{i^*} , with a similar

construction, the challenger \mathcal{R} can get the same result, T_σ and T_σ^* are the following two valid ring signatures:

- $T_\sigma = (I_s, c_1, c_2, \dots, c_s, \dots, c_n, d_1, d_2, \dots, d_s, \dots, d_n)$
- $T_\sigma^* = (I_s^*, c_1, c_2, \dots, c_s^*, \dots, c_n, d_1, d_2, \dots, d_s^*, \dots, d_n)$

Challenger \mathcal{R} outputs the value of $a = sk_s$.

Therefore, the attacker \mathcal{A} for a given instance $(P, a * P)$ can successfully solve $a = sk_s$, that is, the ECDLP problem is successfully solved.

Assuming that the attacker \mathcal{A} successfully forges a valid signature with a non-negligible probability, there is an algorithm \mathcal{R} that can successfully solve the ECDLP problem with a non-negligible probability. However, ECDLP is recognized as a difficult problem, so the ring signature constructed in this paper has a negligible probability under the random prediction model. In signature $T_\sigma = (I_s, c_1, c_2, \dots, c_s, \dots, c_n, d_1, d_2, \dots, d_s, \dots, d_n)$, even if the attacker randomly chooses u_i, v_i, w_i to fake L_i, R_i, L_s, R_s and d_s , the signer's private key is required to be obtained in the calculation. And it is impossible to calculate the key image $I_s = sk_s * H_0(pk_s)$ under the condition of unknown key, so it is impossible for an attacker to forge the signature T_σ . That is, the scheme in this paper satisfies unforgeability.

C. UNCONDITIONAL ANONYMITY ANALYSIS

Theorem 2: The ring signature in this paper has the unconditional anonymity of the signer, that is, for any algorithm \mathcal{F} , any set of user sets $R = pk_1, pk_2, \dots, pk_n$ and a random $pk_s \in R$, the probability $P_r[pk = pk']$ is all $\frac{1}{2}$, where $T_\sigma = (I_s, c_1, c_2, \dots, c_s, \dots, c_n, d_1, d_2, \dots, d_s, \dots, d_n)$ is a ring signature generated by pk_s .

Proof:

- The challenger \mathcal{R} performs initialization to calculate system parameters and sends it to the attacker \mathcal{A} .
- The attacker \mathcal{A} adaptively makes a polynomial limited-order ring signature query.
- In the challenge phase, the adversary outputs a message m , the public key set R of n users, two different public keys $pk_1, pk_2 \in R$, and sends all of them to the challenger \mathcal{R} . The challenger \mathcal{R} randomly selects a bit $pk \in \{0, 1\}$, and the ring signature $\sigma = \mathbf{A}ring(m, R, sk_u)$ returns to the attacker \mathcal{A} .
- The attacker \mathcal{A} adaptively makes a polynomial limited-order ring signature query.
- In the end, the attacker \mathcal{A} outputs a bit $pk' \in \{0, 1\}$.
- Rival \mathcal{A} succeeded in this game if and only if $pk = pk'$.

Before the signer actively disclosed all the information himself, the signature of the output was obscure to any third party. In the ring signature generation **A**ring, the L_i and R_i values required to calculate c_i and d_i are calculated by the signer by randomly selecting the corresponding $u_i, v_i, w_i \in Z_q^*$, and the private key of the signer is also obtained by randomly selecting $sk_i \in Z_q^*$, so the result of signature T_σ is evenly distributed in G . The probability that outside the ring signature member can guess the actual

signer does not exceed $1/(n + 1)$, and the probability that the members inside the ring guess the actual signer does not exceed $1/n$, so the signature scheme in this paper meets unconditional anonymity.

V. CONCLUSION

This article constructs a ring signature scheme based on Elliptic Curve Cryptography (ECC), combining ring signature technology, based on the existing blockchain system architecture. This article integrates the ring signature technology, which can ensure the privacy of user data in the environment of blockchain sharing and transparency. Compared to the application of traditional bilinear pairing-based ring signature schemes in blockchain privacy, the scheme in this paper occupies a greater advantage in terms of security and the concealment of the identity of the signer.

REFERENCES

- [1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Oct. 5, 2018. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [2] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future trends," *Acta Autom. Sinica*, vol. 42, no. 4, pp. 481–494, 2016.
- [3] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly Media, Inc., 2015, pp. 212–235.
- [4] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
- [5] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, pp. 6–10, Jun. 2016.
- [6] C. Natoli and V. Gramoli, "The balance attack against proof-of-work blockchains: The R3 testbed as an example," 2016, *arXiv:1612.09426*. [Online]. Available: <https://arxiv.org/abs/1612.09426>
- [7] V. Dhillon, D. Metcalf, and M. Hooper, "The DAO hacked," 2017, doi: [10.1007/978-1-4842-3081-7_6](https://doi.org/10.1007/978-1-4842-3081-7_6).
- [8] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in *Proc. ASICRYPT*. New York, NY, USA: Springer-Verlag, 2001, pp. 552–565.
- [9] G. Bleumer, "Group signatures," in *Advances in Cryptology—EUROCRYPT*. New York, NY, USA: Springer-Verlag, 1991, pp. 250–252.
- [10] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.
- [11] BitLauder. *BitLauder's Mixer Vs Major Exchanges, Mixer*. Accessed: Jun. 10, 2017. [Online]. Available: <https://bitcoin.stackexchange.com/questions/25722/bitlauders-mixer-vs-major-exchanges-mixer/25753>
- [12] Bitcoin Fog. *Accessing Bitcoin Fog*. Accessed: Jun. 10, 2017. [Online]. Available: <http://bitcoinfog.info/>
- [13] Blockchain. *Wallet*. Accessed: Jun. 10, 2017. [Online]. Available: <https://Blockchain.info/wallet/>
- [14] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 486–504.
- [15] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2015, pp. 112–126.
- [16] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Boston, MA, USA: Springer, 1983, pp. 199–203.
- [17] G. Maxwell. *CoinJoin: Bitcoin Privacy for the Real World*. Accessed: Oct. 5, 2018. [Online]. Available: <https://bitcointalk.org/index.php>
- [18] E. Duffield and D. Diaz, "Dash: A privacy centric crypto currency," pp. 1–22, 2014. [Online]. Available: <https://cryptorum.com/resources/dash-whitepaper-privacycentric-cryptocurrency.10/>
- [19] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical decentralized coin mixing for bitcoin," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2014, pp. 345–364.
- [20] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411.

- [21] C. Rackoff and D. R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1991, pp. 433–444.
- [22] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 459–474.
- [23] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Proc. Symp. Self-Stabilizing Syst.* Cham, Switzerland: Springer, 2015, pp. 3–18.
- [24] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," *Draft Version 0.5*, vol. 9, p. 14, 2016. [Online]. Available: <https://lightning.network/lightning-network-paper.pdf>
- [25] A. Miller et al., "Sprites: Payment channels that go faster than lightning," pp. 1–23, Feb. 2017.
- [26] M. Green and I. Miers, "Bolt: Anonymous payment channels for decentralized currencies," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*. New York, NY, USA: ACM, 2017, pp. 473–489.
- [27] *A Note on Chain Reactions in Traceability in CryptoNote 2.0*, Monero, Monero Res. Lab, Jun. 2017.
- [28] T. Haines and X. Boyen, "VOTOR: Conceptually simple remote voting against tiny tyrants," in *Proc. Australas. Comput. Sci. Week Multiconf. (ACSW)*, vol. 32. New York, NY, USA: Association for Computing Machinery, 2016, pp. 1–13.
- [29] M. E. Maouchi, O. Ersoy, and Z. Erkin, "DECOUPLES: A decentralized, unlinkable and privacy-preserving traceability system for the supply chain," in *Proc. 34th ACM/SIGAPP Symp. Appl. Comput. (SAC)*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 364–373.
- [30] K. Patil and C. T. Wasnik, "An ID-based block ring signature system for secret sharing of data," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Coimbatore, India, Jan. 2017, pp. 1–5.
- [31] V. Pandey and U. Kulkarni, "Effective data sharing with forward security: Identity based ring signature using different algorithms," in *Proc. Int. Conf. Intell. Comput. Control (I2C2)*, Coimbatore, India, Jun. 2017, pp. 1–6.
- [32] Y. Q. Cui, L. Cao, X. Y. Zhang, and G. X. Zeng, "Ring signature based on lattice and VANET privacy preservation," *Chin. J. Comput.*, vol. 42, no. 5, pp. 980–992, 2019.
- [33] S. Thokchom and D. K. Saikia, "Efficient scheme for dynamic cloud data shared within a static group with privacy preserving auditing and traceability," in *Proc. Int. Conf. Cloud Comput. Internet Things (CCIOT)*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 25–32.



YURONG MEI was born in Xuancheng, China. She is currently pursuing the master's degree with the College of Modern Posts and the Institute of Modern Posts, Nanjing University of Posts and Telecommunications. Her current research interests include blockchain technology and its applications.



JING GONG received the Ph.D. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2016. She is currently an Associate Professor with the School of Modern Posts, Nanjing University of Posts and Telecommunications. Her current research interests include computer network and security, network multimedia communication, and network management and its protocols.



FENG XIANG received the B.A. degree from Nanjing University and the master's degree in public administration from the JFK School of Government, Harvard University. He is currently the CEO of YTO Express Co., Ltd., and the Director of the National Engineering Laboratory for Logistics Information Technology. His research interests include logistics engineering and the strategic management of a business.



ZHIXIN SUN received the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 1998. He held a postdoctoral position at Seoul National University, in 2002. He is currently a Professor with the School of Modern Posts, Nanjing University of Posts and Telecommunications. His current research interests include computer network and security, network multimedia communication, and network management and protocol.



XIAOFANG LI received the B.Sc. degree in computer science and technology, the M.Sc. degree in power system automation, and the Ph.D. degree in hydro informatics from Hohai University, in 1995, 2004, and 2011, respectively. She is currently a Professor with the Changzhou Institute of Technology, Changzhou, China. Her research areas include information acquisition and wireless sensor networks. She is a Senior Member of the China Computer Federation.

...