Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.12 n.57, p. 984-992. January/February, 2026.
DOI: https://doi.org/10.5935/jetia. v12i57.3145

RESEARCH ARTICLE OPEN ACCESS

A LIGHTWEIGHT PRIVACY-PRESERVING DATA STORAGE USING MODIFIED RING SIGNATURE SCHEME BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

Vasughi T.S*[1] and Muthulakshmi P[2]

[1, 2]Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, India.

[1]http://orcid.org/0009-0000-5808-628X, [2]http://orcid.org/0000-0001-5422-6716

Email: *vt7068@srmist.edu.in, muthulap@srmist.edu.in

ARTICLE INFO

Article History
Received: December 15, 2025
Revised: January 10, 2026
Accepted: January 15, 2026
Published: February 28, 2026

Keywords:
Anonymity
Blockchain
Elliptic curve cryptography
Ring signature
Unforgeability

ABSTRACT

Blockchain operates in a decentralized manner that provides the potential data available to the public. Privacy protection is an open challenge for data transparency. Applying Blockchain-based cryptographic algorithms in various applications can increase or protect data storage privacy. This paper constructs a lightweight privacy preserving data storage using Modified Ring signature Scheme based on Elliptic Curve Cryptography (MRSS-ECC). This solution built an anonymous user data storage to ensure the user information with highly secure and user identity privacy and validate the signature in the Blockchain network using the smart contract. Therefore, Security analysis of the scheme to verify correctness, unconditional anonymity, and unforgeability. The proposed system incorporates efficient key generation, signature formation, and verification processes to reduce computational overhead. Experimental evaluation demonstrates reduced signature size and improved verification time compared to related approaches. This framework can be adapted for e-governance, healthcare, and financial systems requiring secure, privacy-preserving public ledger integration.

I. INTRODUCTION

In the current blockchain technology, digital services such as electronic voting, electronic lottery, electronic bidding, electronic payment transactions of various virtual cryptocurrencies, and complaint reporting features are achieved by cryptographic construction such as ring signatures to facilitate protecting the anonymity of users. Chaum and van Heyst introduced the concept of group signatures, in which users in a group leak secrets; the signer's anonymity might weaken the anonymity of innocent users. Ring signature was first introduced by Rivest, Shamir, and Tauman [1] in 2001. [2] A ring signature is a specific cryptographic digital signature that simplifies the group signature. In the ring signature scheme, the signer randomly selects a user to conceal multiple numbers of members in the ring and no group managers with a unique key. At the same time, the signer combines the public key and private key to complete the signature without indicating their own identity. Only this signature set can be verified by the verifier, but it is not known who signed the signature. At present, the Blockchain network address of the data sender and receiver is a completely transparent transaction and raises the possibility of data privacy leaks; however, it ensures the authenticity of the on-chain data. Elliptic curve cryptography integrates with ring signature to provide high security and low computational load, plus it endows anonymity of the signers. The ring signature scheme will avoid the data privacy leaks of the data sender as well as the receiver can realize anonymous transactions on the blockchain. The proposed solution offers these security properties correctness, unconditional anonymity, and unforgeability. This paper proposes a lightweight privacy-preserving data storage based on the Ring signature scheme in Blockchain.

The ring signature is operating to secure the information of the transaction initiator and ensure the blockchain's privacy. The rest of the paper is structured as follows. Related works are presented in Section 2. Section 3,4 describes the proposed scheme as Modified Ring Signature Scheme based on Elliptic Curve Cryptography. Section 5 discusses the performance and evaluation metrics.

II. RELATED WORKS

Ring signatures are modern cryptographic primitives from the cryptographic community that are addressed as more significant attention for innovation and manufacturing societies due to the user privacy-preserving authentication feature and protection against malicious user actions. Ring signature also plays a vital role in many applications such as electronic payment, e-voting, and auctions. [3] proposed an e-voting system using a smart contract, threshold encryption, and linkable ring signature with a trusted bulletin board to provide greater privacy.[4]To preserve individual privacy when exchanging data combined with forward security and identity ring signature to increase data security. The regular ring signature remains undetectable double votes in the e-voting and anonymous transactions as they are unlinkable. A linkable ring signature solves this problem and ensures the linkability of two ring signatures signed by the same signer, but the identities of the signers remain anonymous. [5] Two valid signatures on the same message m with private or public key pair linked by the key image. A trusted third party detects the dishonest signer and provides double-spending protection for each transaction or voting. [6] A blockchain-based voting system uses a Paillier system to count the ballots without leaking the candidate's information. Proof of knowledge convinces the voting system that the vote cast by a voter is valid or not without revealing the content of the vote. A linkable ring signature ensures no one can trace the vote's owner and verify the genuine vote.[7] Efficient linkable and/or threshold ring signature without random oracles providing stronger anonymity and accountability. However, the signature size is sublinear with O (d.$\sqrt{n}$) where n is the number of users in the ring and d is the threshold value.

A blind signature is well-suited for creating untraceable systems in blockchain-enabled systems. A blind signature guarantees the anonymity of the user's sensitive information. The blind signature scheme has been in many applications as e-cash and e-voting, and untraceable payment systems, which are more suitable for privacy preservation in blockchain-enabled systems.[8] adopted an anti-quantum blind signature scheme based on the lattice assumption using reject sampling and the bimodal Gaussian distribution to improve security and efficiency and is more secure against quantum attacks.[9] Proposed a privacy-preserving scheme in a smart grid based on group blind signature to meet the requirements of Anonymous authentication and conditional anonymity without revealing the real identity and tracing the malicious users efficiently.[10]The signature size is independent of the ring size using a constant size ring signature scheme with an efficient implementation based on the strong RSA assumption in the random oracle model (ROM) for anonymous identification in ad-hoc groups.[11] Developed a brand-new supply chain traceability system that uses the MLSAG ring signature protocol to protect the privacy of sensitive data and achieves traceability by obscuring participants in publicly available data on previous transactions. The goal of using ring signature in privacy oriented cryptocurrencies is to protect the privacy of a sender of a transaction by making it computationally infeasible to determine the senders address given the signature [12]. The Verge currency employs stealth addressing, which enables a user to construct a one-time address based on a stealth address provided by the recipient to send money.

The address verified its ownership is only visible to the sender and recipient. Only the recipient has access to recover and use the funds at that particular address. [13] Another popular digital cryptocurrency Monero provides un-trackability means all possible signers have the same probability of each transaction. Tracing the sender transaction is protected to provide a higher level of privacy.[14] Dash is a digital cryptocurrency for protecting user privacy. It provides strong anonymity using a chained approach, PrivateSend mixing service reduces the correlation between addresses.[15] zcash anonymous cryptocurrency is needed to provide privacy, untraceability using zk-SNARKs. It provides a shield for the transaction addresses of the sender, receiver, and amount of coins sent. [16] Distributed key generation and elliptic curve cryptography are combined to provide ECC-based signature with stronger security. The use of distributed key agreement avoids to trust third party authorizer to distributed the key. The distributed generation center (KDC) is responsible for generating the system parameter, validate and manage the cluster members and verify the signature and upload them into the blockchain network.[17] A smart contract-based ring signature algorithm employs multiparty secure computation to preserver signer privacy. To prevent forgery "one encryption per signature is used and also address the issue of large signature size, reduced the signature size by two times and signature generation time and verification time by 3 three times compared to ECC ring signature[18]. A secure medical data sharing scheme is proposed that uses certificateless traceable ring signatures, IPFS for data storage, and smart contracts for access control.

Self-Controlling Objects (SCO) enable decryption and controlled data sharing, while distributed key generation ensures data integrity and preserves patient privacy. [19] An ECC-based ring signature is designed for blockchain to protect stored user data without revealing actual identities, only metadata is stored on-chain and smart contract enforces the privacy rules. This scheme is formally proven secure against unforgeability and anonymity under the random oracle model and also resists key expose attacks. This method also reduced signature size and computation time compared to pairing based schemes.[20] Linkable Ring Signature scheme with unconditional anonymity based on the e-NTRU problem under the random oracle model using preimage sampling, trapdoor generation and rejection sampling algorithm to improve the efficiency as well as shorter signature size. An aggregate ring signature is the combination of multiple ring signatures from different message and different rings into a short single signature to maintain the anonymity of each signer. It allows verification of single aggregated signature rather than of each signature of different ring, [21] smart grids face privacy risks from attacker, to address this issue, Certificate aggregate ring signature scheme provides unconditional anonymity, key management and remove key escrow, also ensure message integrity and efficiency with very low verification costs. [22] Two schemes are designed of privacy-focused blockchain transaction, first an aggregated ring signature that reduces signature space complexity with proven security. Second a compact multi message ring signature based on the lock principle to improve the efficiency. Aggregated linkable tags are proposed to detect double-spending in blockchain transactions.

II.1 PRELIMINARIES

Elliptic curve modulo a prime

Let q denote a large prime number, E denote an elliptic curve over an integer finite field F_q,the set of solutions $E_q(a, b) \in F_q$ defined an equation as follows:

$$y^2 = x^3+ax+b \ (mod\ q) \text{ and } 4a^3+27b^2 \neq 0 \ (mod\ q) \text{ where a and b are constants } a, b, x, y \in F_q.$$

Suppose $P(x_1, y_1)$ and $Q(x_2, y_2) \in E_q(a,b)$. The point $P(x, y)$ on an elliptic curve that satisfies the $E_q(a, b)$. If $P = -Q$ the point $Q(x, -y)$ is the negative point of $P(x, y)$ The line l_n passes through P, Q and intersect the elliptic curve at a point $R'(x_3, y_3)$symmetrical about x axis then $P+Q = R(x_3, y_3)$ The point O called the point of infinity form an additive cyclic group

$$G=\{(x, y): a, b, x, y \in F_q, E(x, y)=0\} \cup \{O\}.$$

Definition 1:(Discrete logarithm problem). Let $G = (P) \leq g$. $P \in g$, P is a point with prime order q , Given a point $aP \in G$. Compute $a \in Zq^*$.

Security Model

The security requirements of a ring signature scheme, Consider the attacker **A** has access to the private keys of some users but also has access to all public keys of ring members.

Game1 Unforgeability of ring signature.

For Attacker A, $Succ_{RS,A}$ is defined as its probability of success in the following game between the challenger R and attacker A.

1. **Setup:** Given a security parameter l_n , challenger R runs the setup algorithm to obtain a list of system parameters and then challenger R sends system parameters to the attacker A.
2. **Hash Query:** Attacker A submits any value he chooses and challenger R returns the corresponding hash value to him.
3. **User Public Key Query:** The attacker A requests any user's public key whom he chooses and challenger R returns the corresponding public key pk_i to him.
4. **Private Key Query:** The attacker A requests a user's private key sk_i and the challenger R returns the corresponding private key sk_i .
5. **Ring Signature Query:** The attacker A submits any message he chooses, and challenger R returns the corresponding ring signature to him.
6. **Forge:** Eventually, the attacker outputs the ring signature σ* on a message m* such that

1. σ* is a valid signature
2. m* has never been submitted to the ring signature query

Definition 2:

A Forge $A(t, q_H, q_U, q_P, q_{RS}, \epsilon)$ breaks a ring signature scheme means that if A runs in maximum time, A makes at most q_H hash queries, at most q_U users public key queries, at most q_P private key queries, at most q_{RS} ring signature queries then $Succ_{RS,A}$ is at least €. A ring signature scheme is $A(t, q_H, q_U, q_P, q_{RS}, \epsilon)$ existentially unforgeable under an adaptively chosen message attack if no forger $A(t, q_H, q_U, q_P, q_{RS}, \epsilon)$ breaks it.

Game 2 Anonymity of ring signature.

Let $U=U_1, U_2, \ldots\ldots U_n$ b be n signers. A is an attacker and R is Challenger who all are involved in game 2.

1. The challenger R runs the setup algorithm to obtain a list of system parameters and sends them to the attacker A.
2. The attacker A adaptively makes a polynomially bounded number of ring signature query.
3. In the challenge phase, the attacker outputs a message m, a group of n user's public key and two different public key $pk_1, pk_2 \in R$ to the challenger R. The challenger R randomly chooses a bit $\mu \in \{0,1\}$ and sends A to a ring signature $\sigma \leftarrow (m, R, x_\mu)$.
4. The attacker A can make a polynomially bounded number of ring signature queries.
5. Finally, Attacker A outputs a bit $\mu' \in \{0,1\}$.
6. Attacker A wins the above game if and only if $\mu=\mu'$.

Definition 3:

Define the probability of success in game 2 of attacker A Succ(A)= Pr[μ=μ′] = ½+∈. A ring signature is said to have unconditional anonymity if no attacker can win game 2 with a no non negligible probability advantage. This is to say, for A ring signature scheme is said to have unconditional anonymity if $\epsilon=0$.

III. PROPOSED METHOD

This section constructs a MRSS-ECC for anonymous user data storage which can ensure the privacy of user information in the blockchain environment with high security and smart contract preset conditions is triggered to execute transactions T in the blockchain network. Furthermore, in order to increase user anonymity add the public key and private key random generation using Fisher-Yates shuffling algorithm during the signing messages. As illustrated in Algorithm 1, the specific model is described as follows:

1. **Setup:** Enter a security parameter l_n. l_n is a large prime number. Choose a large prime number $q_0 > l_n$ .The output parameter per={q_0, G_1, G_2, P, H_1, H_2, H_3} Where G_1 is a base point of elliptic curve E. G_2 is a large prime q_0 additive cyclic order group. P is the generator of G_2 Picks three secure hash functions for resisting collision H_1, H_2, H_3:

   $H_1 : E(F_q) \rightarrow E(F_q)$
   $H_2 : \{0,1\} \rightarrow F_q$
   $H_3 : \{0,1\}^* * G_1 \rightarrow Z_q^*$
   Z_q^* the finite field with q elements.

2. **KeyGen:** Let a users set as U_i $\{0,1\}^*$ bas random ring members $(U_1, U_2, \ldots\ldots U_n)$. blockchain system picks at random xZ_q^*band compute $pk_i \leftarrow x_i * P$. The user's public and private key (pk_i, sk_i).

3. **A ring:** The public key set $pk_i = pk_1, pk_2 . pk_n$. R is the set of ring members public key Randomly select $a, b, c \in Z_q^*$ and then calculate

$$L_i = \begin{cases} (a_i + b_i + c_i) * G & if\ i = s \\ (a_i + b_i + c_i) * G + (a_i + b_i + c_i) * pk_i & if\ i \neq s \end{cases} \quad (1)$$

$$R_i = \begin{cases} (a_i + b_i + c_i) * H_1(pk_i) & if\ i = s \\ (a_i + b_i + c_i) * H_1(pk_i) + (a_i + b_i + c_i) * KI & if\ i \neq s \end{cases} \quad (2)$$

Among them: $KI = sk_s * H_1 (pk_s)$, which serves as the message's signature picture and prevents double spending threats to the system. $H_1 (pk_i)$converts pk_i to a point on the finite field's elliptic curve. Randomly select $r \in Z_q^*$ and then calculate as follows

$$h = H_3(m \| r) \quad (3)$$

$$C = H_2(h, L_1, \ldots, L_n, R_1, \ldots, R_n) \quad (4)$$

The signer computes

$$\alpha_i = \begin{cases} C - \sum_{i=1}^{n} \alpha_i & if\ i = s \\ (a_i + b_i + c_i) * H_1(pk_i) + (a_i + b_i + c_i) * KI & if\ i \neq s \end{cases} \quad (5)$$

$$\beta_i = \begin{cases} (a_i + b_i + c_i) - \alpha_i * sk_i & if\ i = s \\ (a_i + b_i + c_i) & if\ i \neq s \end{cases} \quad (6)$$

4. **Averify :** Anyone of the verifiers can compute the transaction signature T_σ

$$\begin{cases} L_i' = \beta_i * G + \alpha_i * pk_i & i \in [1, n] \\ R_i' = \beta_i * H_1(pk_i) + \alpha_i * KI \end{cases} \quad (7)$$

Then check the signature is valid or invalid as follows:

$$\sum_{i=1}^{n} \alpha_i = H_2(h, L_i', \ldots, L_n', R_i', \ldots, R_n') \quad (8)$$

Algorithm 1: Modified Ring Signature Scheme based on Elliptic Curve Cryptography (MRSS-ECC).

Input: a security parameter
Output: open parameter per = (q_0, G_2, P, H_1, H_2, H_3);

1. Number of participants = n
2. **For** all n do
3. randomly shuffle the ring members
4. **End for**
5. **For** all U_i generate the public key and private key do
6. calculate $keyGen(par) \rightarrow (pk_i , sk_i)$
7. **End for**
8. signature image of the message to prevent double spend attack calculate
9. $KI = sk_s * H_1 (pk_s)$,
10. **For** each involved in the ring do
11. Randomly select $a, b, c \in Z_q^*$ and then generate a ring signature

Transaction initiator start signing and then calculate

Source: Authors, (2026).

$$L_i = \begin{cases} (a_i + b_i + c_i) * G & if\ i = s \\ (a_i + b_i + c_i) * G + (a_i + b_i + c_i) * pk_i & if\ i \neq s \end{cases}$$
$$R_i = \begin{cases} (a_i + b_i + c_i) * H_1(pk_i) & if\ i = s \\ (a_i + b_i + c_i) * H_1(pk_i) + (a_i + b_i + c_i) * KI & if i \neq s \end{cases}$$

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

$$h = H_3(m||r)$$
$$C = H_2(h, L_1, \ldots, L_n, R_1, \ldots, R_n)$$

The signer computes

$$\alpha_i = \begin{cases} C - \sum_{i=1}^{n} \alpha_i & if\ i = s \\ (a_i + b_i + c_i) * H_1(pk_i) + (a_i + b_i + c_i) * KI & if\ i \neq s \end{cases}$$
$$\beta_i = \begin{cases} (a_i + b_i + c_i) - \alpha_i * \mathrm{sk_i} & if\ i = s \\ (a_i + b_i + c_i) & if\ i \neq s \end{cases}$$

End for

12. Finally, the generated one-time ring signature becomes the transaction initiator s to the message m as $T_\sigma = (KI, \alpha_1, \alpha_2, \ldots \alpha_s \ldots . \alpha_n, \beta_1, \beta_2, \ldots \beta_s \ldots . \beta_n)$
13. **For** verify Anyone of the verifiers can compute the transaction signature T_σ do
14. **While**
15.

$$\begin{cases} L_i' = \beta_i * G + \alpha_i * pk_i & i \in [1, n] \\ R_i' = \beta_i * H_1(pk_i) + \alpha_i * KI \end{cases}$$

Then check the signature is valid or invalid as follows:

$$\sum_{i=1}^{n} \alpha_i = H_2(h, L_i', \ldots, L_n', R_i', \ldots, R_n')$$

16. **End while**
17. **End for**

Security Analysis

In this section, we mainly focus on the three aspects of correctness, unforgeability and unconditional anonymity.

Unforgeability Analysis

The ring signature Aring T_σ is generated by a signature algorithm. Since three hash function H_1, H_2, H_3 then $\alpha i = H2(h, L1, L2, \ldots \ldots Ln, R1, R2, \ldots \ldots Rn)$ and hash $h = H_3(m||r)$ are distributed over G and Z_q^* respectively. Randomly select $a, b, c \in Z_q^*$ and then calculate $L_i, R_i, \alpha_i, \beta_i$. Randomly select the private key of the signer $sk_i \in Z_q^*$. The probability of guessing the original signer is negligibly greater than 1/n. The attacker A only knows the public key and not others private key. The probability of guessing the original signer is negligibly greater than 1/n+1. So it is concluded that the attacker A has no advantage of guessing the original signer.

Theorem 1: If the discrete logarithm problem is hard, then the scheme is unforgettable against the attacker A in game 1 can adaptively choose a message to attack in the random oracle model.

Proof: Suppose the challenger R receives a random instance*(a,aP)* of the discrete logarithm problem and has to compute the value of a. Challenger R set the public key $pk_i^* = a*P$. R will run A as a subroutine and act as challenger of A in game 1. Without loss of generality, we assume that all the queries are distinct. Now we will show challenger R answer to the attacker A.

1. **Setup:** Given a security parameter l_n, challenger R runs the setup algorithm to obtain a list of system parameters and then challenger R sends system parameters to the attacker A.
2. **Hash Query:** Challenger R maintains the list $L(\alpha_i, \beta_i)$. The list is initially empty. When the attacker A makes a query $H(\alpha_i)$, challenger R selects a value β_i randomly and sets $H_1(\alpha_i) = \beta_i$. Then challenger R adds (α_i, β_i) to the h list and returns β_i to A.
3. **User Public Key Query:** Challenger R maintains the list $L(\alpha_i, \beta_i)$. The list is initially empty. When the attacker A makes a query $H(\alpha_i)$, challenger R selects a value β_i randomly and sets $H(\alpha_i) = \beta_i$. Then challenger R adds (α_i, β_i) to the L list and returns β_i to A.
4. **Private Key Query:** The attacker A makes a user's public key query if $pk_s \neq pk_i^*$, challenger R fails and stops. Otherwise challenger R returns sk_i to A.
5. **Ring Signature Query:** The attacker A submits any message m and a set of n users, and challenger R outputs T_σ ring signature. If there exists a user identity pk_s such that $pk_s \neq pk_i^*$, then the challenger R returns the ring signature T_σ by calling the signing algorithm, where the original signer. Otherwise, challenger R does as follows:

$$L_i = \begin{cases} (a_i + b_i + c_i) * G & if\ i = s \\ (a_i + b_i + c_i) * G + (a_i + b_i + c_i) * pk_i^* & if\ i \neq s \end{cases} \quad (9)$$

$$R_i = \begin{cases} (a_i + b_i + c_i) * H_1(pk_i) & if\ i = s \\ (a_i + b_i + c_i) * H_1(pk_i) + (a_i + b_i + c_i) * KI^* & if\ i \neq s \end{cases} \quad (10)$$

$$h = H_3(m||r) \quad (11)$$

$$C = H_2(h, L_1, \ldots, L_n, R_1, \ldots, R_n) \quad (12)$$

$$\alpha_i = \begin{cases} C - \sum_{i=1}^{n} \alpha_i & if\ i = s \\ (a_i + b_i + c_i) * H_1(pk_i) + (a_i + b_i + c_i) * KI^* & if\ i \neq s \end{cases} \quad (13)$$

$$\beta_i = \begin{cases} (a_i + b_i + c_i) - \alpha_i * sk_i^* & if\ i = s \\ (a_i + b_i + c_i) & if\ i \neq s \end{cases} \quad (14)$$

Finally the ring signature T_σ for message m

$$T_\sigma^* = (KI^*, \alpha_1^*, \alpha_2^*, \ldots \alpha_s^* \ldots \alpha_n^*, \beta_1^*, \beta_2^*, \ldots \beta_s^* \ldots \beta_n^*)$$

Unconditional Anonymity Analysis

Theorem 2: Our ring signature scheme has the property of unconditional anonymity of the signer, For any algorithm A,any set of signers $U = U_1, U_2, \ldots\ldots U_n$ and a random $U_s \in U$,the probability $Pr[\mu = \mu'] = ½$ where $T_\sigma = (KI, \alpha_1, \alpha_2, \ldots \alpha_s \ldots \alpha_n, \beta_1, \beta_2, \ldots \beta_s \ldots \beta_n)$is a ring signature U generated by U_s .

Proof:

1. The challenger R runs the setup algorithm to obtain a list of system parameters and sends them to the attacker A.
2. The attacker A adaptively makes a polynomial bounded number of ring signature query.
3. In the challenge phase, the attacker outputs a message m, a group of n user's public key and two different public keys $pk_1, pk_2 \in R$ to the challenger R. The challenger R randomly chooses a bit $\mu \in \{0,1\}$ and sends A to a ring signature $\sigma \leftarrow Aring(m, R, x_\mu)$.
4. The attacker A can make a polynomial bounded number of ring signature queries.
5. Finally, Attacker A outputs a bit $\mu' \in \{0,1\}$.
6. Attacker A wins the above game if and only if $\mu = \mu'$.

Correctness Analysis

Anyone of the verifiers can compute the transaction signature T_σ **i**f it is true to this formula

$$\sum_{i=1}^{n} \alpha_i = H_2(h, L_i', \ldots, L_n', R_i', \ldots, R_n')$$

When $i = s$

$$\begin{gathered} L_i' = \beta_i * G + \alpha_i * pk_i \\ = [(a_i + b_i + c_i) - \alpha_i * \mathrm{sk_i}] * \mathrm{G} + \alpha_i * pk_i] \\ = [(a_i + b_i + c_i) * G - \alpha_i * \mathrm{sk_i} * \mathrm{G} + \alpha_i * pk_i] \\ = L_i \end{gathered} \quad (15)$$

$$\begin{gathered} R_i' = \beta_i * H_1(pk_i) + \alpha_i * KI \\ = [(a_i + b_i + c_i) - \alpha_i * \mathrm{sk_i}] * H_1(pk_i) + \alpha_i * \mathrm{sk_s} * H_1(pk_s) \\ = [(a_i + b_i + c_i) * H_1(pk_i) - \alpha i * \mathrm{sk_i} * H_1(pk_i) + \alpha_i * \mathrm{sk_s} * H_1(pk_s) \\ = [(ai + bi + ci) * H_1(pk_i)] \end{gathered}$$

$$= R_i \quad (16)$$

When i ≠ s

$$\begin{gathered} L_i' = \beta_i * G + \alpha_i * pk_i \\ = (a_i + b_i + c_i) * G + (a_i + b_i + c_i) * pk_i \\ = L_i \end{gathered} \quad (17)$$

$$Ri' = \beta i * \mathrm{H1}(\mathrm{pki}) + \alpha i * \mathrm{KI} = (a_i + b_i + c_i) * H_1(pk_i) - \alpha_i * \mathrm{KI} = R_i \quad (18)$$

$$\mathrm{H_2}(\mathrm{h}, \mathrm{L_1}, \ldots, \mathrm{L_n}, \mathrm{R_1}, \ldots, \mathrm{R_n}) = H_2(h, L_i', \ldots, L_n', R_i', \ldots, R_n')$$

$$= C_s + \sum_{i=1 i \neq s}^{n} \alpha_i$$
$$= \sum_{i=1}^{n} \alpha_i$$

IV. PERFORMANCE AND EVALUATION

This section discusses all experiments were conducted on a system equipped with an Intel Core @2.6GHz, 16GB RAM, running Ubuntu 22.04 LTS. The computational complexity of the proposed solution written in Python and the complexity of the most significant phases: key generation time, signing time, and verification time. The implementation used secp256k1 parameters for the elliptic curve scalar multiplication of group G over a 256-bit prime field. The cryptographic hash functions H1, H2, H3 were implemented using SHA-256 with H1 configured for hash-to-curve mapping. The computation running time of the number of ring members in each ring in milliseconds. The Ring size(n) of 5,10,20,50,100 of participants for plaintext message "Hello" were tested and average timings were recorded. The figure.1 shows the output of the signature validity. The figure.2 shows the number of ring members increases the corresponding signature time and verification of the ring signature is gradually increase that is shown in the linear relationship. The result shows that the verification of the ring signature consumes less time than the signature time.

Figure 1: Output of Signature Validity.
Source: Authors, (2026).

Table 1: Cryptography Operation Notations.

Notation in Time	Cryptography operation
T_{SME}	ECC-based Scalar Multiplication Operation
T_{AE}	ECC-based Point Addition Operation
T_{HP}	Map-to Point Operation
T_M	Multiplication Operation
T_P	Bilinear-pair Operation
T_E	Exponential Calculation Time

Source: Authors, (2026).

Table 2: Cryptography Operation time in milliseconds.

Cryptography Operation	T_{SME}	T_{AE}	T_{HP}	T_M	T_P	T_E
Execution Time(ms)	1.674	1.234	3.812	-----	-----	-----

Source: Authors, (2026).

In our proposed scheme, the user signature requires the ECC-based scalar multiplication operation 3+(n-1)*4=(4n-1)T_{SME} , ECC-based point Addition operation 2(n-1)T_{AE} ,a hash operation mapping to points on elliptic curves 1T_{HP} , the signature verification requires the ECC-based scalar multiplication operation 4nT_{SME} , ECC-based point Addition operation 2nT_{AE} ,a hash operation mapping to points on elliptic curves 1T_{HP} , and a one-way hash operation mapping to a finite field of prime numbers, with the last three having negligible computational overhead. Therefore, the computational overhead of generating and verification of a signature is

$$T_{sign} = (4n-1)\, T_{SME} + 2(n-1)T_{AE} + T_{HP}$$
$$T_{verify} = 4nT_{SME} + 2nT_{AE} + T_{HP}$$

Table 3: Efficiency analysis of Ring Signature scheme from Elliptic Curve Group.

Algorithm	Signature Generation	Signature Verification
[18]	$(4n-1)T_M + (4n+6)\, T_E$	$nT_E + 2T_P$
[16]	$4(n-1)\, T_{SME} + 2(n-1)\, T_{AE} + T_{HP} + T_M$	$4nT_{SME}$
[17]	$4(n-1)\, T_{SME} + 2(n-1)\, T_{AE} + 2nT_{HP}$	$4nT_{SME} + 2nT_{AE} + T_{HP} + T_M$
[OURS]	$4(n-1)\, T_{SME} + 2(n-1)\, T_{AE} + T_{HP}$	$4nT_{SME} + 2nT_{AE} + T_{HP}$

Source: Authors, (2026).

To conclude, the time consumption of different ring signature schemes in the signature-generation and signature-verification steps is summarized in Table 3. It was observed that our scheme took less time than the other schemes [16][17] [18], in the signature generation phase Compare with[18] [16] our scheme takes less signature time and slightly more verification time. This indicates that our signature scheme possesses higher signing and verification efficiency.

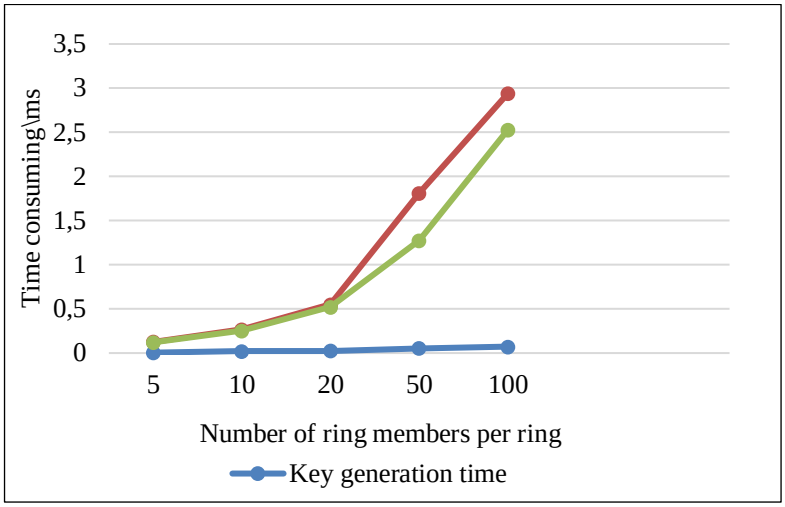

Figure 2: Number of Ring Members per ring for Ring signature scheme from Elliptic curve group.
Source: Authors, (2026).

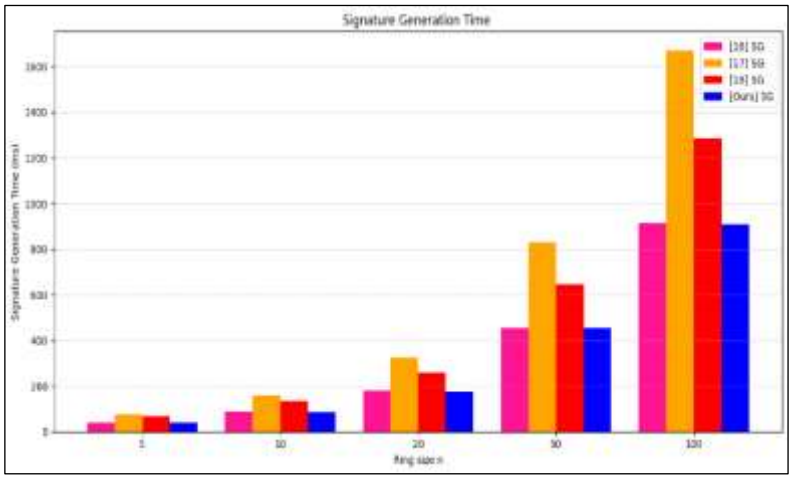

Figure 3: Comparison of Signature Generation time.
Source: Authors, (2026).

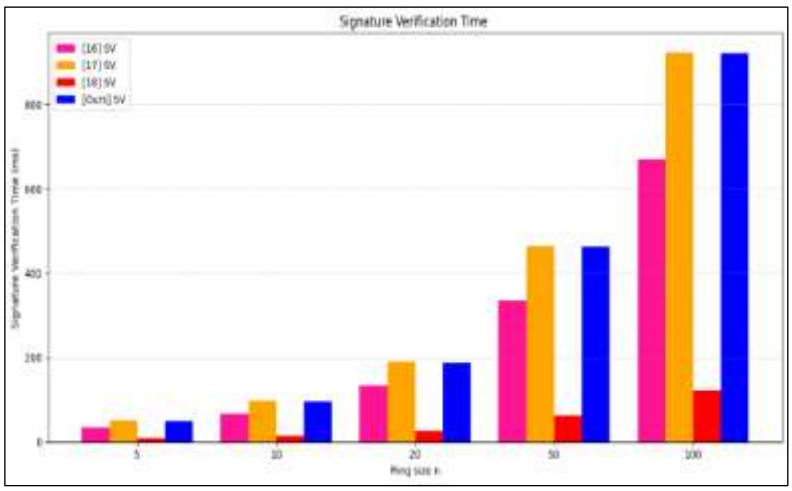

Figure 4: Comparison of Signature verification time.
Source: Authors, (2026).

IV. CONCLUSION

This article constructs a Modified Ring Signature Scheme based on the Elliptic Curve Cryptography (MRSS-ECC) for anonymous user data storage which can ensure the privacy of user information in the blockchain environment with high security and smart contract preset conditions is triggered to execute transactions T in the blockchain network. Our scheme achieves a concealment of user identity and provides anonymity, uniqueness, and unforgeability and can be applied in application with double spending protection. Finally, by comparing with related signature schemes, our scheme achieves faster signature generation and verification time and higher efficiency. However, since the efficiency and communication overhead grow as the number of users increases, future work will focus on developing an aggregated ring signature approach to enhance both verification speed and communication performance.

V. REFERENCES

[1] R. L. Rivest, A. Shamir, and Y. Tauman, “How to leak a secret,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2248, pp. 552–565, 2001, doi: 10.1007/3-540-45682-1_32.

[2] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C. M. Cheng, and K. Sakurai, “A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity,” Cryptography, vol. 6, no. 1, pp. 1–22, 2022, doi: 10.3390/cryptography6010003.

[3] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, “A Secure Decentralized Trustless E-Voting System Based on Smart Contract,” 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng., pp. 570–577, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00082.

[4] J. Herranz, “Identity-based ring signatures from RSA,” vol. 389, pp. 100–117, 2007, doi: 10.1016/j.tcs.2007.08.002.

[5] L. Malina, J. Hajny, P. Dzurenda, and S. Ricci, “Lightweight ring signatures for decentralized privacy-preserving transactions,” ICETE 2018 - Proc. 15th Int. Jt. Conf. E-bus. Telecommun., vol. 2, no. Icete, pp. 526–531, 2018, doi: 10.5220/0006890505260531.

[6] B. Yu et al., “Platform-Independent Secure Blockchain-Based Voting System,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11060 LNCS, pp. 369–386, 2018, doi: 10.1007/978-3-319-99136-8_20.

[7] T. H. Yuen, J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, “Efficient Linkable and/or Threshold Ring Signature Without Random Oracles,” Comput. J., vol. 56, no. 4, pp. 407–421, 2013, doi: 10.1093/comjnl/bxs115.

[8] C. Li, Y. Tian, X. Chen, and J. Li, “An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems,” Inf. Sci. (Ny)., vol. 546, pp. 253–264, 2021, doi: 10.1016/j.ins.2020.08.032.

[9] J. P. D. Comput, W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, “A practical group blind signature scheme for privacy protection in smart grid,” J. Parallel Distrib. Comput., vol. 136, pp. 29–39, 2020, doi: 10.1016/j.jpdc.2019.09.016.

[10] Q. Wu, W. Susilo, Y. Mu, and F. Zhang, “LNCS 4266 - Ad Hoc Group Signatures,” no. 60403007, pp. 120–135, 2006.

[11] M. El Maouchi, “DECOUPLES : A Decentralized , Unlinkable and Privacy-preserving Traceability System for the Supply Chain,” pp. 364–373, 2019.

[12] W. Koerhuis, T. Kechadi, and N. Le-khac, “Forensic Science International : Digital Investigation Forensic analysis of privacy-oriented cryptocurrencies,” Forensic Sci. Int. Digit. Investig., no. xxxx, p. 200891, 2019, doi: 10.1016/j.fsidi.2019.200891.

[13] S. Tople and P. Saxena, “A Traceability Analysis of Monero ’ s Blockchain,” pp. 153–173, 2017, doi: 10.1007/978-3-319-66399-9.

[14] E. Duffield and D. Diaz, “Whitepaper Dash : A Privacy-Centric Crypto-Currency”.

[15] A. Banerjee and M. Clear, “Demystifying the Role of zk-SNARKs in Zcash,” pp. 12–19, 2020.

[16] L. Wang, C. Peng, and W. Tan, “Secure Ring Signature Scheme for Privacy-Preserving blockchain,” Entropy, vol. 25, no. 9, p. 1334, Sep. 2023, doi: 10.3390/e25091334.

[17] Li, Q., Yi, W., Zhao, X., Yin, H., & Gerasimov, I. (2022). Representative Ring Signature Algorithm Based on Smart Contract. Sensors, 22(18). https://doi.org/10.3390/s22186805

[18] Lai, C.; Ma, Z.; Guo, R.; Zheng, D. Secure medical data sharing scheme based on traceable ring signature and blockchain. Peer Netw. Appl. 2022, 15, 1562–1576

[19] Li, X., Mei, Y., Gong, J., Xiang, F., & Sun, Z. (2020). A blockchain privacy protection scheme based on ring signature. IEEE Access, 8, 76765–76772. https://doi.or./10.1109/ACCESS.2020.2987831.

[20] Ye, Q., Wang, M., Meng, H., Xia, F., & Yan, X. (2022). Efficient Linkable Ring Signature Scheme over NTRU Lattice with Unconditional Anonymity. Computational Intelligence and Neuroscience, 2022. https://doi.org/10.1155/2022/8431874.

[21] Wang, H., Wang, L., Wen, M., Chen, K., & Luo, Y. (n.d.). A Lightweight Certificateless Aggregate Ring Signature Scheme for Privacy-preserving in Smart Grids.

[22] Teng, D., Yao, Y., & Huang, C. (2025). Optimizing signature space performance in privacy-enhanced blockchains: novel ring signature solutions. Eurasip Journal on Information Security, 2025(1). https://doi.org/10.1186/s13635-025-00192-9