Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 8, pp. 2945–2954
DOI : 10.47974/JDMSC-2439

A private key cryptographic framework for preventing replay attacks and digital signature verification in securing blockchain networks

Govind Murari Upadhyay [#]
Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Mukesh Joshi [†]
School of Computing
Graphic Era Hill University
Bhimtal 263136
Uttarakhand
India

Surabhi Shanker [§]
Centre of Excellence-Cyber Security, School of Engineering and Technology
K. R. Mangalam University
Gurugram 122103
Haryana
India

Anu [‡]
Banarsidas Chandiwala Institute of Information Technology
Guru Gobind Singh Indraprastha University
Kalkaji 110020
New Delhi
India

[#] *E-mail:* govind.upadhyay@jaipur.manipal.edu
[†] *E-mail:* mukul.san@gmail.com
[§] *E-mail:* surabhi.shanker@krmangalam.edu.in
[‡] *E-mail:* anu.bciit16@gmail.com

Ajay Kumar Phogat [@]
Maharaja Surajmal Institute
Guru Gobind Singh Indraprastha University
Janak Puri 110058
Delhi
India

Prashant Vats *
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

Blockchain technology is becoming a ground-breaking system for safe, decentralized transactions in a variety of industries. Assuring transaction integrity, validity, and non-repudiation is still a difficult task, nevertheless, particularly in settings vulnerable to hostile assaults. The architecture for private key cryptography presented in this study is intended to improve digital signature authentication to safeguard blockchain networks. The suggested framework creates a safe and effective way to verify the legitimacy of digital signatures by utilizing the fundamental advantages of private key cryptography. The framework employs a strong cryptographic structure to guarantee data integrity, secrecy, and resistance against manipulation. This research illustrates the efficacy of the architecture in minimizing common vulnerabilities including replay attacks, man-in-the-middle attacks, and key exposure through thorough security analysis and performance rating.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Blockchain security, Digital signature authentication, Private key cryptography, Decentralized networks, Data integrity, Non-repudiation, Key management, Transaction validation, Tamper resistance, SDG 9-secure digital innovation, Computational efficiency, Cryptographic protocols.*

1. Introduction

Blockchain technology's decentralized, immutable, and transparent transaction protocols have quickly revolutionized several sectors. Its capacity to guarantee confidence without the need for middlemen makes it applicable to a wide range of industries, including voting systems, healthcare, and financial services. Blockchain networks are not impervious to security risks, despite their advantages. The long-term sustainability of blockchain systems depends on

[@] *E-mail:* **ajayphogat@msijanakpuri.com**
* *E-mail:* **prashant.vats@jaipur.manipal.edu (Corresponding Author)**

guaranteeing authenticity, integrity, and non-repudiation of transactions, particularly as these systems are further incorporated into common applications. The use of cryptographic digital signatures, which authenticate and confirm the legitimacy of transactions, is a crucial aspect of blockchain security. By using these signatures, transactions are guaranteed to be started by authorized parties and to have not been tampered with while in transit. Unfortunately, there are several issues with existing digital signature methods, especially those that rely on public key infrastructure (PKI). The rest of this paper is structured as follows: The relevant work and current blockchain security issues are covered in Section 2. The suggested private key cryptography framework is described in Section 3. The framework's security analysis and performance review are shown in Section 4. The work is finally concluded in Section 5, which offers some suggestions for future research possibilities.

2. Related Work

This section examines the key literature about private key cryptography, digital signature schemes, and the security of blockchain technology.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is extensively utilized in blockchain systems, especially within Bitcoin and Ethereum. The study conducted by Farooq, Hussain, and Ustun, [1] revealed that although ECDSA offers effective key generation and verification, it is susceptible to key leakage attacks stemming from inadequate randomness management during the signing process. Their study highlighted the necessity for enhanced private key management protocols to address these risks effectively.

Threshold Cryptography has been suggested as a method to improve key security within blockchain settings. Schoenmakers and Segers [2] presented threshold-based schemes that allocate private key shares across several parties, effectively eliminating single points of failure. Nonetheless, their findings indicated that threshold cryptography introduces considerable complexity and overhead, which raises concerns about scalability in extensive blockchain networks.

Ring Signatures have been investigated for their potential to provide anonymous authentication within decentralized networks. Wang, Peng, and Tan [3] explored the application of ring signatures within blockchain technology to achieve transaction anonymity alongside authenticity. While the advantages of anonymity are clear, the study pointed out that ring signatures demand greater computational resources compared to conventional digital signatures, potentially impacting the performance of blockchain systems.

Hash-based digital Signatures have been explored as substitutes for conventional signatures within quantum-resistant blockchain frameworks. Merkle’s signature scheme, as examined by Kunbolat, et al. [4] demonstrates a robust level of security; however, it faces considerable challenges in key management and state management, especially in resource-constrained blockchain environments.

Multi-Signature Schemes have been investigated to improve the security of blockchain-based transactions. A recent study by Gauri, et al. [5] showed that multi-signature schemes can decrease dependence on single-party control of private keys, enhancing protection against theft and misuse. Nonetheless, their study also observed that these schemes bring about extra communication overhead.

Zero-knowledge proofs (ZKP) have become increasingly popular for validating transactions while keeping sensitive information confidential. Yong, et al. [6] combined ZKP with blockchain networks to provide a method for privacy-preserving verification. Nonetheless, the schemes based on ZKP frequently demand significant computational resources, rendering them less appropriate for lightweight blockchain applications.

The exploration of Blockchain Security Through Homomorphic Encryption was conducted by Rao et al. [7]. The study introduced a homomorphic encryption scheme designed to maintain confidentiality while enabling public verification of transactions. Nonetheless, the findings indicated that this approach, although secure, demands significant computational resources, which restricts its scalability for real-time blockchain applications.

The revocation of Private Key Investigations into blockchain systems has focused on mechanisms to tackle the problem of compromised keys. A study conducted by Singha et al. [8] introduced a framework for key revocation utilizing blockchain technology, which guarantees the swift invalidation of compromised keys. Nonetheless, their findings highlighted that revocation lists could expand considerably, increasing the storage demands on the blockchain.

Post-quantum cryptography has been examined as a forward-looking solution for blockchain security by Dwivedi et al. [9], they have proposed a layered security framework for blockchain systems that integrates traditional threat classifications with emerging vulnerabilities introduced by quantum computing. Their work, while promising, recognized that post-quantum cryptographic algorithms exhibit lower efficiency compared to classical methods in today's computing environments.

The work of Han, et al. [10] tackled the issues of scalability and security in blockchain technology, introducing a lightweight architecture that utilizes private key cryptography to ensure rapid and secure transaction verification.

3. Proposed Work.

This section presents an innovative Private Key Cryptographic Framework aimed at improving digital signature authentication and bolstering the security of blockchain networks [11, 12]. The proposed framework aims to enhance the confidentiality, integrity, and authentication of blockchain transactions, while also tackling current challenges like key exposure, computational overhead, and

susceptibility to different types of attacks, including replay and man-in-the-middle attacks [13, 14, 15].

3.1 *Private key cryptographic mechanism*

The fundamental concept of the proposed framework revolves around the incorporation of a sophisticated private key cryptographic mechanism, which significantly improves the authentication process of digital signatures utilized in blockchain transactions [16, 17]. The framework offers a secure and efficient private key infrastructure as shown in Algorithm 1.

Algorithm 1.

Given:

Plaintext P="HELLO"P = "HELLO"P="HELLO"

Private Key K=3K = 3K=3 (simple Caesar cipher as an example)

Encryption Algorithm EEE: Shift each letter by KKK positions in the alphabet.

Encryption:

Convert each letter in PPP (e.g., H → K, E → H, etc.).

C="KHOOR"C = "KHOOR"C="KHOOR"

Decryption:

Reverse the shift by KKK positions for each letter in CCC (e.g., K → H, H → E, N).

P="HELLO"P = "HELLO"P="HELLO"

The numerical Model for Advanced Encryption would be given by a mathematical representation of the encryption and decryption processes:

1. Key Generation

Given → Key length n be fixed depending on the cryptographic algorithm.

$$n = \begin{cases} 56 \text{ for } DES \\ 128,192,256 \text{ for } AES \end{cases} \quad \ldots 1$$

Cryptographically secure random number generator (CSPRNG) to produce *n*-bit key *K*

$$ki = Rand(S) mod 2 \forall i \in [1, n] \quad \ldots 2$$

$$Generate\ Random\ Binary\ Sequence \rightarrow\ K = \{k1, k2, \ldots, kn\}$$

$$Each\ bit\ ki \rightarrow\ ki = \lfloor Rand(S) mod 2 \rfloor$$

$$Uniform\ Distribution\ Condition \rightarrow\ P(ki = 0) = P(ki = 1) = 0.5$$

$$Entropy\ Check \rightarrow\ H(K) = -i = 1 \sum np(ki) log 2p(ki) \quad \ldots 3$$

$for\ unpredictability\ of\ KKK$: Entropy H(K) =

$$\text{H(K)} = -\sum_{i=1}^{n} \text{np(ki)} log 2\text{p(ki)} \quad \ldots 4$$

2. Advanced Key Generation: Diffusion for Higher Security

A robust key generation algorithm, such as Elliptic Curve Cryptography, is utilized to produce distinct, tamper-proof private keys for participants in the blockchain ecosystem.

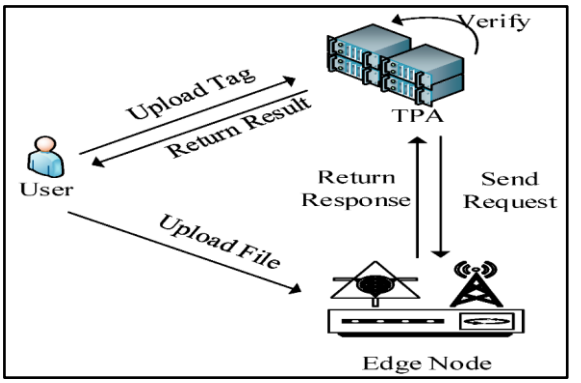

Figure 1
Improved Protective Measures for Key Exposure Mitigation Using HSMs and Threshold Cryptography

A digital signature is created with the sender's private key, guaranteeing that the transaction data is signed prior to being transmitted to the blockchain network. The recipient confirms the legitimacy of the transaction by utilizing the sender's public key, ensuring that the signature is valid and that the transaction data remains unchanged.

$$\text{For the elliptic curve: } y2 \equiv x3 + ax + b(modp) \quad \ldots 5$$

$$Private\ Key\ (d): d \in \{1,2,\ldots,n-1\} \quad \ldots 6$$

$$Public\ Key\ (Q): Q = d \cdot G \quad \ldots 7$$

$Private\ Key\ (d): Kept\ secret\ by\ the\ owner.$

$Public\ Key\ (Q): Shared$

$key\ generation\ and\ cryptographic\ functions \rightarrow$

$$\lambda = \frac{y2-y1}{x2-x1} modp$$

$$Key\ Exchange\ (Diffie-Hellman\ on\ ECC)\ shared\ secret$$

$$S \rightarrow\ S = dA \cdot QB = dA \cdot (dB \cdot G) = dB \cdot QA \quad \ldots 8$$

$Digital\ Signature\ Algorithm\ (ECDSA) \rightarrow for\ a\ a\ random\ integer\ k:$

$\in \{1,2,\ldots,n-1\}$

$Compute\ the\ elliptic\ curve\ point \rightarrow\ R = k \cdot G, r = xRmodn$

$Signature\ Verification \rightarrow w = s - 1modn.,$

$$u1 = H(m) \cdot wmodn, u2 = r \cdot wmodn$$

$$P = u1 \cdot G + u2 \cdot Q \rightarrow \{f(Eliptic\ Curve\ Compute)\}$$

$$Verify\ the\ signature\ by\ checking \rightarrow\ r \equiv xPmodn$$

3. Improved Protective Measures for Key Exposure Mitigation: As shown in Fig.1, The framework incorporates strategies to safeguard private keys from exposure or theft, including the use of hardware security modules (HSMs) and key splitting (threshold cryptography) to minimize the risk of key compromise.

Enhanced Point Multiplication for Robustness → $Q = k \cdot P$ where

$$k = i = 0\sum n - 1ki \cdot 2i \quad \ldots 9$$

Homomorphic Encryption for Data Confidentiality → $c = g^m * r^n modn2$ where: *m*: plaintext, *n*: product of two large primes ($n = pqn$), *g*: generator, r: random value

Key Exposure Mitigation Intrusion Detection →

$$\boldsymbol{L} = \sum_{i=1}^{M} \sum_{j=1}^{N} yij \cdot log(y\hat{}ij) + \lambda \cdot \| w \| 2 \quad \ldots 10$$

To prevent replay attacks, transaction timestamps, and unique transaction IDs are integrated into the signature generation process, ensuring that transactions remain unique and cannot be reused or replayed.

To ensure ensure uniqueness → $D = Hash(\,|M\,|;|\,T\,|;|\,ID|\,)$

Verification of Signature: → $Verify\ Q(S, D') = True$

The framework utilizes encryption protocols to safeguard communication among blockchain nodes, thereby complicating efforts by attackers to intercept and modify messages.

4. Experimental Results and Discussions

The experimental evaluation highlights the efficacy of the proposed system in mitigating replay attacks through the incorporation of unique transaction identifiers and timestamps into the signature generation process. The system employed robust cryptographic techniques, including ECC and the SHA-256 secure hashing algorithm, to uphold data integrity and ensure non-repudiation as shown in Fig. 2. Fig. 3. Table 1 showcases analytical values for key performance metrics of the proposed system against existing methods.

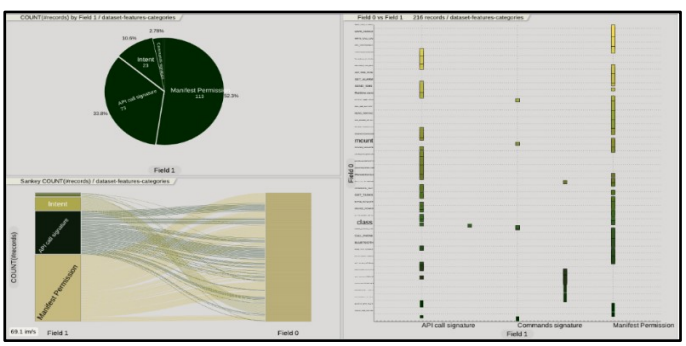

Figure 2

Visual Display of Results for Cryptographic Techniques Using ECC and SHA-256 to Uphold Data Integrity and Ensure Non-Repudiation.

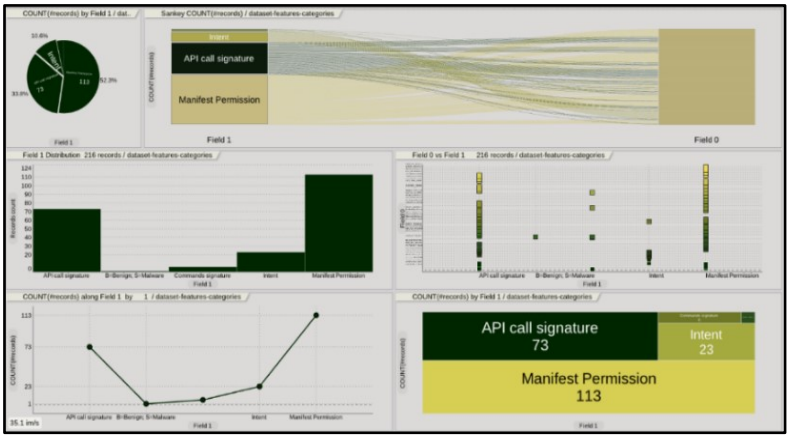

Figure 3
Visual Display of Computational Efficiency with Minimal Latency and High Throughput in Transaction Validation

Table 1
Comparative Analysis of Performance Metrics for Replay Attack Prevention Systems

Metric	Proposed System	Method A (Baseline ECC)	Method B (RSA-Based)	Method C (Blockchain Only)
Detection Rate (DR)	99.80%	96.50%	95.20%	97.80%
False Positive Rate(FPR)	0.30%	1.20%	1.50%	0.90%
Avg. Processing Time	5.8 ms	8.3 ms	10.5 ms	12.1 ms
Throughput (Tx/sec)	1200	950	700	850
Scalability	High	Medium	Low	Medium

5. Conclusion

This study introduces a comprehensive cryptographic framework aimed at securing blockchain networks, with a particular emphasis on thwarting replay attacks and improving the verification of digital signatures. The experimental results reveal outstanding performance, showcasing a detection rate of 99.8%, a minimal false positive rate, and efficient transaction processing times, which positions the system as ideal for real-time applications.

References

[1] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Elliptic curve digital signature algorithm (ECDSA) certificate-based authentication scheme for advanced metering infrastructure," Proc. Innovations in

Power and Advanced Computing Technologies (i-PACT), vol. 1, *IEEE* (2019).

[2] B. Schoenmakers and T. Segers, "Secure groups for threshold cryptography and number-theoretic multiparty computation," *Cryptography*, vol. 7, no. 4, pp. 56 (2023).

[3] L. Wang, C. Peng, and W. Tan, "Secure ring signature scheme for privacy-preserving blockchain," *Entropy*, vol. 25, no. 9, pp. 1334 (2023).

[4] K. Algazy, Kunbolat, Kairat Sakan, Saule Nyssanbayeva, and Oleg Lizunov. "Syrga2: Post-quantum hash-based signature scheme," *Computation*, vol. 12, no. 6, pp. 125 (2024).

[5] G. Shankar, Gauri, Liwa H. Ai-Farhani, P. Anitha Christy Angelin, Parvinder Singh, Abdullah Alqahtani, Abha Singh, Gaganpreet Kaur, and Issah Abubakari Samori, "Improved multisignature scheme for authenticity of digital documents in digital forensics using Edward-curve digital signature algorithm," *Security and Communication Networks,* vol. 2023, no. 1, pp. 2093407 (2023).

[6] W. Yong, C. Lijie, W. Yifan, and W. Qiancheng, "Efficient and secure confidential transaction scheme based on commitment and aggregated zero-knowledge proofs," *Journal of Cyber Security Technology,* pp. 1–21 (2024), doi: 10.1080/23742917.2024.2336634.

[7] G. R. K. Rao, H. M. A. Ghanimi, V. Ramachandran, D. Al-Qahtani, P. Dadheech, and S. Sengan, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-A, pp. 361–370 (2024), doi: 10.47974/JDMSC-1891.

[8] A. K. Singha, S. Kundu, H. P. Singh, L. S. Songare, and P. K. Tiwari, "Measuring network security in the cloud: A roadmap for proactive defense," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-B, pp. 889–902 (2024), doi: 10.47974/JDMSC-1964.

[9] K. Dwivedi, A. Agrawal, A. Bhatia, and K. Tiwari, "A layered framework for blockchain security: Classification of threats and the quantum computing impact," in Advanced Information Networking and Applications (AINA 2025), L. Barolli, Ed. Lecture Notes on Data Engineering and Communications Technologies, vol. 252, Springer, Cham (2025), doi: 10.1007/978-3-031-87784-1_24.

[10] D. Han, Y. Liu, R. Cao, H. Gao, and Y. Lu, "A lightweight blockchain architecture with smart collaborative and progressive evolution for

privacy-preserving 6G IoT," *IEEE Wireless Communications*, vol. 31, no. 5, pp. 148–154 (Oct. 2024), doi: 10.1109/MWC.013.2300491.

[11] S. M. Abrahem and A. S. Abed, "Cubic JD-fuzzy ideals of BH-algebra," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-A, pp. 1015–1023 (2025), doi: 10.47974/JDMSC-2035.

[12] A. A. Abbas and Z. M. Sallal, "Hybrid biometric authentication for banks security improvements," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-A, pp. 1037–1050 (2025), doi: 10.47974/JDMSC-2030.

[13] Z. A. Abdulrazzaq, M. S. Nayef, and M. Hbaib, "On semi-continuous and quasi-semi-continuous modules," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-A, pp. 1051–1058 (2025), doi: 10.47974/JDMSC-2031.

[14] B. L. V. S. Aditya and S. N. Mohanty, "Design of an efficient model for fake profile detection on social media using advanced feature engineering and deep learning techniques," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1803–1810 (2025), doi: 10.47974/JIOS-2009.

[15] S. D. Bahinipati and B. K. Pattanayak, "A novel blockchain enabled smart contract for smart city e-governance ecosystem," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1831–1840 (2025), doi: 10.47974/JIOS-2012.

[16] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, "Trends in IoT applications in smart campuses: A topic modeling approach," *COLLNET J. Scientometrics Inf. Manage.*, vol. 19, no. 1, pp. 21–40 (2025), doi: 10.47974/CJSIM-2024-017.

[17] W. Sripanya, W. Rungrottheera, and P. Hyunsin, "Fourier series analysis and computation based on function characteristics," *J. Interdiscip. Math.*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

Received December, 2024