Advances in Computer, Signals and Systems (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2025.090405
ISSN 2371-8838 Vol. 9 Num. 4

Research on Privacy-Preserving Identity Authentication Algorithm Based on Elliptic Curves and Zero-Knowledge Proofs

Shi Wang*

Hainan Vocational University of Science and Technology, Haikou, 571126, China
**Corresponding author*

Keywords: Elliptic Curves, Zero-Knowledge Proofs, Identity Authentication, Privacy Protection, Lightweight Algorithms

Abstract: Traditional identity authentication algorithms that rely on centralized trust authorities and plaintext identity verification often suffer from privacy leakage, key misuse, and single-point-of-failure risks. This study proposes a lightweight, privacy-preserving authentication algorithm based on elliptic curve and zero-knowledge proofs to address these issues. The proposed scheme introduces a random challenge and an anonymous verification mechanism during the authentication process to ensure both identity privacy and authentication security. While maintaining high levels of security and verifiability, the algorithm effectively reduces computational complexity and communication overhead. Experimental results demonstrate that the proposed method significantly outperforms traditional RSA and ECDSA in terms of authentication delay, communication cost, and security robustness. This approach is practical and scalable, offering a promising solution for secure authentication in environments with limited resource.

1. Introduction

With the rapid development of the digital economy and intelligent networks, identity authentication mechanisms for information systems have become a critical technological foundation for ensuring cybersecurity and enabling trustworthy data exchange. In application scenarios such as the Internet of Things, vehicle-to-everything networks, smart manufacturing, smart cities, and cross-border finance, identity authentication must not only verify the authenticity and integrity of communicating entities but also balance privacy protection and anonymity. However, traditional authentication mechanisms—such as password-based, token-based, or public key infrastructure (PKI)-based solutions—often rely on centralized trust models. These approaches suffer from high computational complexity, significant communication overhead, single points of failure, and privacy leakage, making them ill-suited for meeting security demands in distributed and resource-constrained environments[1-3].

In recent years, researchers have proposed various lightweight identity authentication solutions to address these challenges. Among them, elliptic curve cryptography (ECC) has emerged as the most representative cryptographic technology for IoT and edge computing scenarios due to its high

security assurance at shorter key lengths. ECC is based on the elliptic curve discrete logarithm problem, offering security comparable to 2048-bit RSA while requiring only 256-bit keys, significantly reducing computational and storage costs. Concurrently, the emergence of zero-knowledge proofs (ZKP) technology has introduced novel approaches to privacy protection[4-8]. It enables users to prove to a verifier that possess a legitimate credential without revealing any identifying information, achieving secure verification where "the existence is known, but the identity is not."

This study proposes a privacy-preserving identity authentication algorithm that integrates ECC with ZKP. Designed to balance theoretical rigor and engineering practicality, the algorithm introduces a non-interactive zero-knowledge proofs mechanism during authentication, effectively achieving identity anonymization and private key non-inference. The algorithm possesses multiple security properties including anti-forgery, anti-tampering, replay resistance, and anonymous authentication. It reduces computational and communication overhead, offering a practical solution for building a trustworthy, low-power, secure, and scalable next-generation identity authentication system.

2. Algorithm Design and Implementation

2.1 Overall Design Approach

This study proposes a privacy-preserving identity authentication algorithm based on elliptic curve cryptography and zero-knowledge proofs. It aims to achieve a highly secure, low-overhead, and robust privacy-preserving identity authentication mechanism in resource-constrained environments. The overall algorithm design adheres to three core principles: lightweight computation, decentralized trust, and zero-knowledge privacy. This approach maximizes the reduction of storage, computational, and communication burdens on the device side while ensuring authentication reliability.

First, in terms of lightweight computation design, the algorithm adopts elliptic curve cryptography as its underlying public-key framework. Compared to traditional RSA, ECC provides equivalent security strength with shorter key lengths. This characteristic enables efficient operation on low-power chips or embedded systems. By optimizing point multiplication operations and random number generation modules, the algorithm effectively reduces computational latency and energy consumption, ensuring rapid response in mobile devices and wireless network environments.

Second, in privacy protection and anonymous authentication design, the algorithm incorporates a zero-knowledge proofs mechanism, enabling users to complete identity verification without revealing their true identity or private keys. Users only need to send a mathematically constructed, randomness-based proof to the verifier, which allows for identity verification without the verifier obtaining any additional information. This design fundamentally eliminates the risks associated with traditional plaintext authentication based on passwords or digital signatures, preventing identity correlation analysis and data traceability attacks.

Furthermore, in designing the secure interaction process, the system adopts a three-entity architecture: the certificate authority (CA), the user, and the verifier. The CA handles system parameter initialization and user registration; the user generates and submits the zero-knowledge authentication proof; and the verifier validates the proof's validity using the public key and a challenge-response mechanism. The entire process incorporates random challenges via secure hash functions and session identifiers (Session ID) to resist replay attacks and man-in-the-middle attacks. The system communication structure adheres to the "minimum interaction principle," requiring only a single message exchange to complete identity authentication, significantly reducing communication rounds and bandwidth consumption.

Furthermore, the algorithm design prioritizes cross-domain trust and multi-platform deployment for scalability and deployability. Digital certificates issued by the CA are compatible with existing X.509 structures, facilitating integration with blockchain identity systems or cloud access control frameworks. The algorithm supports batch authentication and concurrent processing. Through session sharding and hash indexing mechanisms, it maintains linear scalability in large-scale device access scenarios.

Finally, for security and verifiability, the algorithm incorporates the random oracle model (ROM) assumption in its design and defines system security based on the elliptic curve discrete logarithm problem (ECDLP). The algorithm's security proof demonstrates that even with full control over the communication channel, an attacker cannot recover private keys or generate valid authentication information within polynomial time. Simultaneously, its zero-knowledge properties ensure the non-interactivity and untraceability of the authentication process, preventing the correlation of messages across different authentication sessions. This achieves strong anonymity and anti-tracking protection.

2.2 Mathematical Modeling and Symbolic Definitions

Let E denote an elliptic curve defined over a finite field F_p , of the form $E: y^2 = x^3 + ax + b \,(mod\ p)$, where p is a large prime, and $4a^3 + 27b^2 \neq 0$ ensures the curve is non-singular.

Let G be the base point of the curve and q be its order. The system parameters are $Param = (p, a, b, G, q, H)$, where $H(\cdot)$ is a secure hash function.

The user randomly selects a private key $x \in [1, q-1]$ and computes the corresponding public key $P = xG$. The goal of the proof is for the user to demonstrate to the verifier that possess this private key without revealing x.

The zero-knowledge proofs condition is $sG = R + cP$. If the equation holds, the verifier is convinced that the user possesses the corresponding private key but cannot deduce its value.

2.3 Algorithm Flowchart

The algorithm comprises four primary phases, with the specific workflow as follows:

Step 1: System Initialization Phase.

System initialization is performed by the Certificate Authority (CA). The CA selects the secure elliptic curve E, the base point G, and the order q, then publishes the system parameters and the hash function $H(\cdot)$. Subsequently, the CA generates its own key pair (sk_{CA}, pk_{CA}) for subsequent certificate issuance and verification. This phase also establishes the certificate format $Cert = Sign_{CA}(ID_u, P, meta)$ and configures either a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) to support certificate status queries. System parameters are publicly disclosed across the network, while private keys are securely retained solely by the CA.

Step 2: Registration Phase.

User U generates a random private key $x \in_R [1, q-1]$ locally and calculates the public key $P = xG$. The user then submits a registration request to the CA, including the identity identifier ID_u and public key P. After verifying the identity's legitimacy, the CA generates and returns the digital certificate F. Upon receipt, the user validates the signature's correctness and securely stores

$Cert_u = Sign_{CA}(ID_u, P, valid\_time)$. Once registration is complete, the user can utilize the certificate for anonymous identity verification in subsequent authentication processes.

Step 3: Authentication Phase.

When a user needs to prove their identity to verifier V, it first generates a random number $x \in_R [1, q-1]$ and computes a commitment point $R = rG$. It then calculates a challenge value $c = H(R, P, session\_id)$ and derives a response value $s = (r + c \cdot x) \bmod q$. The user sends the proof message $(R, s, Cert_u)$ to the verifier. This process does not disclose the private key x, achieving authentication solely through group operations, thereby ensuring zero-knowledge properties. If the non-interactive variant (Fiat–Shamir transformation) is used, the challenge value is computed locally by the user without requiring additional interaction.

Step 4: Verification Phase.

Upon receiving the $(R, s, Cert_u)$, the verifier first validates the certificate's integrity (correct signature, not expired, not revoked). It then recalculates challenge $c' = H(R, P, session\_id)$ and checks whether it satisfies condition $sG = R + c'P$. If the equation holds true, verification succeeds, confirming the user possesses the corresponding private key; otherwise, authentication fails. This entire process requires no transmission of plaintext keys or passwords, offering resistance to replay attacks, forgery, and enabling anonymous authentication.

2.4 Pseudocode Implementation

```
Algorithm: ECC + ZKP Identity Authentication
def setup():
    return curve, G, q, H
def keygen():
    x = random_scalar()
    P = x * G
    return x, P
def register(ID_u, P, CA):
    Cert_u = CA.sign(ID_u, P)
    return Cert_u
def prove(x, P, session_id):
    r = random_scalar()
    R = r * G
    c = H(R, P, session_id) % q
    s = (r + c * x) % q
    return (R, s)
def verify(P, Cert_u, R, s, session_id):
    c = H(R, P, session_id) % q
    return (s * G == R + c * P) and CA.verify(P, Cert_u)
```

3. Experimental Results and Analysis

To validate the performance and security of the proposed algorithm, experiments were conducted on a computational environment featuring an Intel Core i7-13700H processor and 16 GB of memory, with Python 3.11 as the software environment. The experiments employed the secp256k1 elliptic curve and SHA-256 hash function as underlying security components. To evaluate the algorithm's comprehensive performance, it was compared against traditional RSA-2048 and

ECDSA-256 authentication schemes. Test metrics included authentication time, verification time, message length, and communication overhead.

Table 1: Comparison of Algorithm Performance Test Results

Algorithm Type	Authentication Time (ms)	Verification Time (ms)	Message Length (Bytes)	Communication Overhead (KB)
RSA-2048	9.52	10.87	256	12.4
ECDSA-256	4.25	4.98	128	6.3
Algorithm of this study	2.11	2.87	64	3.5

As shown in Table 1, the proposed algorithm demonstrates significant efficiency advantages in both authentication and verification phases. Compared to RSA-2048, authentication time is reduced by approximately 78% and verification time by about 73%. Compared to ECDSA-256, authentication latency is reduced by nearly 50% and communication overhead by approximately 45%. The algorithm maintains an average CPU utilization below 15% and memory consumption within 48 MB during 1000 consecutive authentication scenarios, validating its scalability and operational stability in resource-constrained environments. The proposed elliptic curve-based zero-knowledge authentication algorithm outperforms traditional approaches in computational efficiency, bandwidth utilization, and security protection capabilities.

4. Conclusions

This study designs and implements a lightweight identity authentication algorithm based on elliptic curves and zero-knowledge proofs, effectively balancing system security and computational efficiency. Leveraging the high security of algebraic curves and the privacy properties of zero-knowledge proofs, the algorithm enables anonymous authentication of user identities and verifiable interactions while reducing computational and communication overhead during the authentication process. Experimental results demonstrate that the proposed scheme outperforms traditional RSA and ECDSA algorithms in terms of authentication latency, communication load, and resource consumption. It is particularly well-suited for resource-constrained environments such as the Internet of Things, edge computing, and mobile terminals.

Acknowledgements

Project supported by the University-Level Scientific Research Funding Project of Hainan Vocational University of Science and Technology (Project No. HKKY2024-ZD-22).

References

[1] Anqi Chi, Lin Bi, Gopal Verma & Xiaoqiang Di.(2025). Enhanced QKD protocol based on zero-knowledge proof and post-quantum signature. Optics Communications, 596, 132431.
[2] Shangping Wang, Qi Huang, Ruoxin Yan, Juanjuan Ma & Xiaoling Xie.(2025). A privacy-enhanced authentication scheme for VANETs based on blockchain and zero-knowledge proof. Vehicular Communications, 56, 100976.
[3] Cyprian Omukhwaya Sakwa, Andrew Omala Anyembe & Fagen Li.(2025). A survey of folding-based zero-knowledge proofs. Information Sciences, 724, 122698.
[4] Khizar Hameed, Faiqa Maqsood & Zhenfei Wang.(2025). Artificial intelligence-enhanced zero-knowledge proofs for privacy-preserving digital forensics in cloud environments. Journal of Network and Computer Applications, 243,104331.
[5] Xiaohua Wu, Tingbo Zhang, Lei Chen & Zirui Wang.(2025). Privacy-preserving cross-chain asset transfers using notary schemes and zero-knowledge proofs. Cluster Computing, 28(6),387.
[6] Li Chunlei, Xing Zhibo, Liu Jiamou, Russello Giovanni, Li Zhen, Wu Yan & Asghar Muhammad Rizwan.(2025). Integrating zero-knowledge proofs into federated learning: a path to on-chain verifiable and privacy-preserving

federated learning frameworks. International Journal of Web Information Systems,21(3),275-297.
[7] Butrus Mbimbi, David Murray & Michael Wilson.(2025). Preserving Whistleblower Anonymity through Zero-Knowledge Proofs and Private Blockchain: A Secure Digital Evidence Management Framework. Blockchains, 3(2), 7.
[8] Yangyang Bao, Lingrui Pan, Xiaochun Cheng & Liming Nie.(2025). Enabling privacy-preserving and distributed intelligent credit scoring by zero-knowledge proof and functional encryption. Peer-to-Peer Networking and Applications, 18(3),138.