DOI: 10.23977/jeis.2025.100212
ISSN 2371-9524 Vol. 10 Num. 2

An Efficient Identity Authentication Mechanism Based on Algebraic Curves and Zero-Knowledge Proofs

Shi Wang[*]

Hainan Vocational University of Science and Technology, Haikou, 571126, China
**Corresponding author: ws10121@126.com*

Keywords: Algebraic Curves, Zero-Knowledge Proofs, Identity Authentication, Lightweight Security Protocols, Privacy Protection

Abstract: With the rapid development of the digital economy and the Internet of Things, identity authentication in resource-constrained environments faces challenges such as low efficiency and inadequate privacy protection. Addressing the high computational and communication overhead of traditional RSA and ECC authentication mechanisms, this study proposes an efficient identity authentication mechanism (AC-ZKP) based on algebraic curves and non-interactive zero-knowledge proofs (NIZK). This mechanism leverages algebraic curve group operations to achieve lightweight key management and employs zero-knowledge proofs to ensure information concealment and anti-forgery during identity verification. The paper conducts a systematic study across four dimensions: system modeling, algorithm design, security analysis, and performance evaluation. Experimental results demonstrate that while maintaining 128-bit security strength, the AC-ZKP mechanism reduces authentication latency by approximately 44% and communication overhead by about 40%. It also exhibits strong scalability and resistance to attacks, significantly outperforming traditional ECC schemes. These findings provide a viable solution for lightweight, high-security identity authentication in IoT, edge computing, and cross-border data exchange environments.

1. Introduction

With the deep integration of emerging technologies such as cloud computing, the Internet of Things, blockchain, and artificial intelligence, the global digital transformation is accelerating. Data has become a core resource driving economic and social development. Simultaneously, the complexity and openness of network environments continue to increase, making identity authentication mechanisms increasingly crucial for ensuring network communication security, access control, and data integrity. As a critical component of cybersecurity systems, identity authentication serves as the primary barrier to ensure user legitimacy, prevent unauthorized access, and defend against malicious attacks[1-3].

Traditional identity authentication mechanisms primarily rely on public key infrastructure (PKI) and digital signature algorithms, whose security depends on the difficulty of factoring large integers or solving the discrete logarithm problem. However, as network environments diversify and authentication scenarios become more complex, traditional approaches exhibit significant limitations. On one hand, in large-scale distributed systems or high-concurrency access environments, the PKI framework incurs substantial computational and communication overhead during certificate management and key verification. On the other hand, user identity information is susceptible to tracking or inference during authentication, posing privacy leakage risks [4-6]. Furthermore, the advancement of quantum computing poses a potential threat to traditional cryptographic systems, challenging their long-term reliability. In cross-border data flows, IoT device interconnectivity, and decentralized applications, identity authentication urgently requires achieving computational lightness and scalability while ensuring security and privacy. Traditional centralized authentication models struggle to meet the combined demands of multi-party mutual trust, cross-domain collaboration, and privacy protection.

Algebraic curve cryptography has garnered significant attention due to its low key length and high security strength. Compared to traditional elliptic curves, higher-order algebraic curves achieve equivalent security with smaller parameter sizes, thereby substantially reducing computational and communication costs. Their application potential is particularly prominent in the Internet of Things and resource-constrained terminals. The discrete logarithm problem can be constructed using algebraic curve group structures, providing a robust mathematical foundation for identity authentication. Simultaneously, the emergence of zero-knowledge proof technology has provided a feasible implementation path for privacy-preserving identity authentication. Zero-knowledge proofs enable a prover to demonstrate to a verifier that they possess certain knowledge or credentials without revealing any secret information. With the introduction of efficient protocols such as non-interactive zero-knowledge proofs and zk-SNARKs, zero-knowledge proofs have transitioned from theoretical concepts to practical applications, demonstrating advantages in fields like blockchain, e-government, and privacy-preserving computation.

This paper proposes an efficient identity authentication mechanism (AC-ZKP) that integrates algebraic curves with zero-knowledge proofs. The mechanism leverages efficient group operations on algebraic curves as its computational foundation, while employing zero-knowledge proofs to achieve information concealment and verifiability during the authentication process. This forms a novel authentication model that combines security, privacy, and lightweight characteristics. Compared to traditional RSA or ECC schemes, this mechanism reduces computational complexity and communication overhead while remaining applicable to resource-constrained scenarios such as IoT terminals, cross-border payments, and distributed ledgers. Against the backdrop of Hainan Free Trade Port's digital infrastructure development, cross-border data security and trustworthy identity authentication have become critical enablers for integrating free trade and the digital economy. The proposed mechanism not only provides security guarantees for cross-border data exchange within the Hainan Free Trade Port but also offers theoretical and technical references for constructing a distributed trust system within China's digital economy environment.

2. Design of Identity Authentication Mechanism

2.1 System Model and Parameter Configuration

To achieve efficient and secure identity authentication, the proposed AC-ZKP mechanism in this paper leverages the algebraic curve group structure over finite fields and combines it with non-interactive zero-knowledge proofs to implement identity verification. Within the system, the Registration Authority (RA), User, and Verifier constitute the three core roles. The RA is responsible for generating the system's master parameters and handling user registration; Users hold private and public keys and complete identity authentication through zero-knowledge proofs; The Verifier validates the received proof and decides whether to approve the authentication. System parameters include the finite field F_q, the algebraic curve $C: y^2 + h(x)y = f(x)$, the curve generator G, and the group order n. Auxiliary parameters such as the system public key $P = sG$ and the hash function $H(\cdot)$ are also made public. The efficient computational capabilities of algebraic curve groups provide the foundation for lightweight identity authentication, while the introduction of zero-knowledge proofs ensures the security of user privacy and the anonymity of the authentication process.

2.2 User Registration and Key Management System

During registration, users randomly generate a private key $x_i \in \mathbb{Z}_n^*$ and compute a public key $Xi = x_i G$. Subsequently, users submit the public key information to the registration center, which generates an identity credential $\sigma_i = Sign_s(X_i)$ and returns it to the user. This credential is used in subsequent zero-knowledge identity authentication to ensure the legitimacy of user registration. Algebraic curve cryptography achieves high security with shorter key lengths, reducing computational complexity and communication overhead. This makes it suitable for resource-constrained environments such as IoT devices and edge computing nodes. By leveraging this cryptographic framework, the AC-ZKP mechanism enables lightweight identity verification while maintaining security and resistance to attacks.

2.3 Zero-Knowledge Proof Identity Authentication Protocol

During the identity verification phase, users must prove possession of private key x_i corresponding to registered public key X_i without revealing the actual private key value. To achieve this, this paper employs a non-interactive zero-knowledge (NIZK) protocol, completing identity authentication through a “commit-challenge-response” process.

The specific steps are as follows: The user randomly selects a temporary value $r \in Z_n^*$, calculates a commitment value $R = rG$, and generates a challenge value $c = H(R \| X_i \| P)$ using a hash function. The user then computes the response $z = r + cx_i \mod n$ and sends the proof $\pi = (R, z)$ to the verifier. The verifier evaluates $zG \overset{?}{=} R + cX_i$ to determine whether the authentication is valid. This protocol leverages the computational infeasibility of the Algebraic Curve Discrete Logarithm Problem (ACDLP) to ensure secure identity verification while achieving zero-knowledge properties—meaning the verifier cannot derive the user's private key or other sensitive information from the proof.

2.4 Correctness and Security Analysis

Theoretically, the user's computed response $z = r + cx_i$ satisfying $zG = R + cX_i$ ensures the correctness of the authentication process. Zero-knowledge properties enable the simulator to construct distribution-consistent proofs without knowing c, thereby guaranteeing that verifiers cannot distinguish between genuine and fraudulent proofs. Anti-forgery relies on the unsolvability of the ACDLP problem, preventing attackers from fabricating valid proofs. The introduction of the random value r in the protocol guarantees uniqueness for each authentication, preventing replay attacks. Simultaneously, the verifier relies solely on mathematical relationships for authentication, inherently resisting man-in-the-middle attacks. The entire security design theoretically guarantees anonymity, untraceability, and authentication reliability.

2.5 Algorithm Flow Description

The AC-ZKP mechanism can be formalized into three core algorithms: the registration algorithm, the authentication algorithm, and the verification algorithm. During user registration, the user generates a key pair (x_i, X_i) and obtains a signature credential σ_i through the registration center. In the authentication phase, the user randomly generates a temporary value r, computes a commitment R and a response z, and generates a proof $\pi = (R, z)$. During verification, the verifier determines the validity of the proof based on formula $zG = R + cX_i$. This algorithm features a clear structural flow, low computational complexity, and minimal communication overhead, ensuring efficient authentication. The integration of formula derivation with the algorithmic flow facilitates both theoretical analysis and practical system implementation.

2.6 System Performance and Scalability

The AC-ZKP mechanism offers significant performance advantages. Due to the short key length of algebraic curves and efficient point operations, the computational load for authentication is substantially lower than traditional RSA or ECC schemes. Non-interactive zero-knowledge proofs reduce communication rounds, alleviating network bandwidth pressure. The system architecture is highly scalable, supporting multi-user group authentication and group signature extensions, making it suitable for IoT, cross-border data exchange, and blockchain smart contract scenarios. The overall mechanism achieves high efficiency and scalability while ensuring security and anonymity, providing a viable technical solution for identity authentication in resource-constrained environments.

3. Experimental Results and Analysis

3.1 Experimental Environment and Setup

The experimental platform utilizes an ARM Cortex-A53 embedded development board running Linux 5.10. Programming is conducted in C++, employing the GMP and PBC libraries to implement algebraic curve group operations and zero-knowledge proof algorithms. Test parameters are as follows: the finite field is , the algebraic curve selected is a high-order curve, the group order is n, the generator is G, and the system security strength is set to 128 bits. The non-interactive zero-knowledge proof employs a commitment-challenge-response scheme with SHA-256 as the hash function. The comparison scheme utilizes the standard ECC identity authentication protocol, matching the security level of the AC-ZKP mechanism. Each experimental run performs 1000 random authentication operations, recording average authentication latency, CPU utilization, communication overhead, and authentication success rate.

3.2 Single-User Authentication Performance

Table 1: Comparison of Single-User Authentication Experiment Results

Indicator	ECC	AC-ZKP	Improvement Ratio
Average Authentication Latency (ms)	14.6	8.2	↓43.8%
Average CPU Utilization (%)	47.3	26.9	↓43.1%
Communication Traffic (Bytes)	512	304	↓40.6%
Security Strength (Equivalent Digits)	128-bit	128-bit	—

The results of the single-user authentication experiment are shown in Table 1. As shown in the experimental data from Table 1, under single-user authentication scenarios, the AC-ZKP mechanism significantly reduces computational and communication overhead while maintaining 128-bit security strength. The average authentication latency decreases by approximately 44%, and communication traffic drops by about 41%, demonstrating the mechanism's proven efficiency on resource-constrained terminals.

3.3 Multi-User Group Authentication Performance

To evaluate the scalability of the mechanism in multi-user authentication environments, this paper conducted tests under group sizes of 10, 50, and 100 users. Experimental results demonstrate that the average authentication latency of the AC-ZKP mechanism increases linearly with the number of users, but at a rate significantly lower than traditional ECC schemes. Multi-user authentication experiments show that the mechanism maintains low latency and CPU utilization even as the group expands, making it suitable for multi-party authentication requirements in IoT gateways and distributed systems.

3.4 Performance in Bandwidth-Constrained Environments

In scenarios with limited network bandwidth, communication overhead is a critical metric. By simulating authentication processes under varying bandwidth constraints, the AC-ZKP mechanism significantly reduces communication rounds through non-interactive zero-knowledge proofs. This approach decreases total data volume by approximately 40% compared to standard ECC solutions, effectively alleviating network pressure. Additionally, the protocol's random number mechanism ensures uniqueness for each authentication, further avoiding communication overhead caused by redundant interactions.

3.5 Experimental Analysis and Discussion

The experimental results collectively demonstrate that the AC-ZKP mechanism exhibits distinct advantages in resource-constrained environments. First, it achieves computational efficiency: algebraic curve point operations and a lightweight key system reduce CPU load, resulting in significantly lower authentication latency compared to traditional ECC schemes. Second, it optimizes communication: non-interactive zero-knowledge proofs minimize interaction rounds, conserving network bandwidth and making it suitable for IoT and edge computing nodes. Third, it ensures security and reliability by leveraging the unsolvability of the discrete logarithm problem over algebraic curves, guaranteeing anti-forgery and zero-knowledge properties to protect user identity privacy. Fourth, it offers strong scalability, supporting multi-user group authentication and group signature extensions, making it adaptable for cross-border data exchange and distributed ledger scenarios.

Comprehensive experimental results and theoretical analysis demonstrate that the AC-ZKP mechanism exhibits superior performance advantages in single-user, multi-user, and bandwidth-constrained environments, fully validating its feasibility, effectiveness, and engineering application value.

4. Conclusions

This paper addresses the issues of low efficiency and insufficient privacy protection in traditional identity authentication mechanisms under resource-constrained environments by proposing an efficient identity authentication mechanism (AC-ZKP) based on algebraic curves and non-interactive zero-knowledge proofs. This mechanism fully leverages the high security density of algebraic curves and the privacy protection properties of zero-knowledge proofs to achieve lightweight identity authentication processes and enhanced information security. Through theoretical analysis, algorithmic design, and systematic experimentation, this paper demonstrates that the AC-ZKP mechanism exhibits performance advantages in single-user, multi-user group, and bandwidth-constrained scenarios. It achieves lower average authentication latency, CPU utilization, and communication overhead compared to traditional ECC schemes while maintaining 128-bit security strength, meeting practical engineering requirements. The AC-ZKP mechanism not only exhibits high computational efficiency and communication performance but also effectively resists replay attacks, man-in-the-middle attacks, and identity forgery risks, achieving user identity privacy protection and anonymity in the authentication process. The mechanism demonstrates excellent scalability in multi-user group authentication and cross-domain data interaction scenarios, providing a viable technical solution for IoT, edge computing, distributed ledgers, and cross-border data security.

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] Xing F.Y., Dong A., Sun Y.Y., Tong F., and Cheng G. A Review of Zero Trust Management for Large-Scale IoT. Acta Electronica Sinica, 2025, 1-33.

[2] Sun J.J., Zheng J.L., Yang Y., Li J.F., and Zhang X.M.(2025).Research and Practice on Security Management of the Unified Identity Authentication System in Higher Education Institutions. Network Security Technology & Application, 10, 93-95.

[3] Dou H.Z.(2025).Attribute-Based Encryption-Based Embedded Electronic Information System Access Authentication Method. Journal of Xi'an University(Natural Science Edition), 4, 46-53.

[4] Wang H.X., Wang H., Ma R., Liang X., and Li S.J.(2025).An Identity Authentication Method for Power Grid Terminals Based on Privacy-Preserving Homomorphic Encryption Algorithms. Electronic Design Engineering, 19, 141-145.

[5] Wang N.(2025). Design and Analysis of Secure Communication Protocols for the Internet of Things. Information & Computer, 19, 82-84.

[6] Xue T.T., Wang J.W., Zhang J., Dai X.T., and Hu X.(2025). Multi-Stage Identity Authentication Method for Cross-Platform File-Based Database User Access. Information Technology and Informatization, 9, 157-160.