Journal of Electronics and Information Science (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2025.100111
ISSN 2371-9524 Vol. 10 Num. 1

Application and Research of Algebraic Curve in Identity Authentication Security

Xiaoyan Li*, Shi Wang

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

Keywords: Algebraic curve; Elliptic curve cryptography (ECC); Identity authentication; information security

Abstract: In the field of information security, the security of identity authentication is crucial. We focus on the application of algebraic curves in the field of identity authentication security and explore their core content in depth. Starting from the basic theory of algebraic curves, we explain the group structure and discrete logarithmic properties of elliptic curves. Then, we conduct a detailed analysis of its application mode, including key generation, encryption and decryption, and digital signature processes based on elliptic curve cryptography (ECC). This is aimed at building a secure defense line for identity authentication. Meanwhile, by using algebraic curves to construct a zero - knowledge identity authentication protocol, we can achieve identity verification under privacy protection. Compared to traditional methods, this application has obvious advantages and can effectively resist quantum computing attacks, improving efficiency with shorter key lengths and faster computation speeds. However, in the process of application promotion, there are challenges such as the urgent need to complete mathematical theories, optimize algorithms, and ensure compatibility.Conduct research on the application of algebraic curves in identity authentication security, providing both theoretical foundations and practical guidance for promoting technological innovation in this field and further enhancing the security and reliability of identity authentication.

1. Introduction

In the digital age, information security has become a crucial issue. From personal privacy to national security, protecting the confidentiality, integrity, and availability of information is a top priority. As an important part of information security, identity authentication is the first gateway to protect network assets and provides strong protection for information security in the network. However, traditional identity authentication methods such as username and password have extremely low security issues and are easily stolen and cracked. Therefore, finding more secure and efficient identity authentication technologies has become an urgent need[1].

Algebraic curves have always been a hot topic of research for mathematicians, with profound influence in the field of mathematics and playing a key role in many practical applications such as computer graphics and information security. In the field of information security, algebraic curves are widely used in encryption algorithms and authentication techniques. By utilizing the properties

of algebraic curves, information security experts can design more secure and efficient encryption algorithms and authentication schemes[2].

Elliptic curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory. It utilizes the Abel group of discrete logarithms composed of points on elliptic curves over a finite field to achieve encryption, decryption, and digital signatures. Compared to other high security encryption algorithms such as RSA, ECC requires fewer data bits and faster processing speed for the same amount of storage data and computing resources. Therefore, ECC has significant advantages in identity authentication security[3].

In identity authentication security, algebraic curves are used to construct secure and efficient identity authentication protocols. For example, in identity authentication schemes based on zero knowledge proofs, algebraic operations can be used to prove possession of certain secret information without revealing the specific content of this information. In addition, elliptic curve cryptography is widely used in network identity authentication systems, which have the characteristics of high security, fast speed, good flexibility, and strong applicability[4].

In summary, the application and research background of algebraic curves in identity authentication security mainly stem from the importance and challenges of information security, the widespread application of algebraic curves in mathematics and information security, the rise of elliptic curve cryptography, and the specific application of algebraic curves in identity authentication. With the continuous advancement of technology and the increasing demand for information security, in-depth research on algebraic curves in identity authentication security will be of great significance. This not only helps to enhance the security and efficiency of identity authentication technology, but also lays a solid foundation for building a secure digital world[5].

2. Basic knowledge of algebraic curves

Algebraic curves are an important foundation in the field of cryptography. Simply put, algebraic curves can be seen as line shapes described by mathematical equations. For example, the lines, circles, ellipses, hyperbolas, parabolas, etc. that we see on a plane all belong to algebraic curves. Algebraic curves have different levels of complexity, expressed in terms of degree. Straight lines are linear, while circles, ellipses, hyperbolas, and parabolas are quadratic. The higher the degree, the more complex the shape of the curve may be. On algebraic curves, there are some special points called singular points. If at a certain point on the curve, the change in the curve is very special, like suddenly having a sharp point or a bend, this point is a singular point, and other normal points are non singular points[6].

Algebraic curves can be understood as a kind of "characteristic value" of algebraic curves, which can reflect the complexity of the curve. For example, simple curves like lines and circles have a genus of 0. The genus of elliptic curves is 1, which is more complex than straight lines and circles; If the coordinates of a point on an algebraic curve are integers or fractions (i.e. rational numbers), then that point is called a rational point. In cryptography, we often focus on rational points on algebraic curves within a limited range, and the number and distribution of these points have an impact on the security and efficiency of cryptography; For some special algebraic curves, such as elliptic curves, the points on them have a special pattern that allows them to form a queue like structure, and these points operate according to specific rules, just like queuing to play games, with a certain order and pattern. This is called group structure.

In the field of cryptography, some special properties of elliptic curves can be utilized to design cryptographic systems. For example, based on the characteristic that it is difficult to reverse the original number by performing certain mathematical operations on elliptic curves, the security of passwords can be ensured, and functions such as encryption, decryption, and digital signatures can

be achieved. Super elliptic curves are more complex than elliptic curves and can also be used to design cryptographic systems. Passwords designed with hyperelliptic curves can be shorter in length and more efficient to use while ensuring the same level of security. Combine algebraic curves and other related knowledge with cryptography to create new cryptographic methods. For example, there is an encryption method based on algebraic curves that allows us to perform some calculations on encrypted data without completely decrypting it, which is very useful in protecting data privacy and other aspects.

3. Elliptic curve cryptography (ECC)

The elliptic curve cryptosystem is a cryptographic algorithm based on the elliptic curve discrete logarithm problem. The security of ECC is based on the difficulty of elliptic curve discrete logarithm problem, which has not yet discovered an effective sub exponential time attack method. Elliptical Curve Cryptography (ECC) is a public key cryptographic system based on the mathematical theory of elliptic curves. Its main features include:

High security: Based on the difficulty of elliptic curve discrete logarithm problem, the cracking difficulty is high. Under the same security strength, the key length is shorter than RSA and other systems.

Low computational cost: Under the same security level, ECC has relatively low computational and communication overhead, making it suitable for resource constrained devices such as IoT devices, smart cards, etc.

Good flexibility: Suitable elliptical curves and parameters can be selected according to different security requirements and application scenarios, with a high degree of customization.

The main application scenarios include:

Data encryption: Protecting the security of sensitive data such as financial transaction information, medical records, enterprise trade secrets, etc. during transmission and storage.

Digital signature: Digital signatures are used to verify the source and integrity of messages, ensuring that data has not been tampered with, and are widely used in fields such as electronic contracts and e - government.

Key exchange: In an insecure network environment, both parties can securely exchange keys, laying the foundation for subsequent encrypted communication, such as in TLS/SSL protocols used to establish secure connections.

4. Identity authentication security

In the digital age, identity authentication is a crucial defense line for information security, and its importance is self-evident. With the rapid development of information technology, identity authentication technology is also constantly evolving, gradually evolving from traditional methods based on passwords and SMS verification codes to the current multi factor authentication system based on emerging technologies such as biometric recognition, quantum encryption, and blockchain. In this context, algebraic curves, especially elliptic curves, have shown unique advantages and broad application prospects in the field of identity authentication security.

4.1 Overview of Identity Authentication Technology

Identity authentication refers to the process by which a system identifies and verifies the identity of a user, with the aim of ensuring that only legitimate users can access restricted data resources, preventing illegal access and data leakage. Common identity authentication methods include password based authentication, biometric authentication (such as fingerprint recognition, facial

recognition, iris recognition, etc.), smart card based authentication, and token based dynamic password authentication. Each authentication method has its own advantages and disadvantages, such as password authentication being simple and easy to use, but easily cracked or forgotten; Biometric authentication has the characteristics of uniqueness and difficulty in forgery, but may be affected by environmental factors and device accuracy; Smart card authentication has high security, but the cost is relatively high and there is a risk of loss or damage.

With the increasing complexity of network attack methods, a single identity authentication method is no longer sufficient to meet the growing security needs. Multi factor authentication (MFA) has emerged, combining various authentication methods such as password+fingerprint recognition, SMS verification code+facial recognition, etc. By increasing the diversity of authentication factors, it greatly improves the security of identity authentication. For example, in financial trading scenarios, users not only need to enter passwords, but also need to perform secondary verification through fingerprint recognition or SMS verification codes to ensure the security of transactions.

4.2 Application principle of algebraic curves in identity authentication

4.2.1 Fundamentals of elliptic curve cryptography (ECC)

Elliptic curve cryptography is a public key cryptographic system based on the elliptic curve discrete logarithm problem (ECDLP). The difficulty of the elliptic curve discrete logarithm problem lies in the fact that it is computationally challenging to calculate the integer k such that Q=kP given two points P and Q on the elliptic curve. This characteristic makes elliptic curves highly secure in the field of cryptography.

4.2.2 Application of ECC in Identity Authentication

In identity authentication, ECC is mainly used for digital signatures and key exchange. Taking digital signature as an example, the user first generates a pair of public and private keys (d, Q), where d is the private key and Q=dP (P is the base point on the elliptic curve) is the public key. If the equation holds, the signature is valid, proving that the message indeed comes from the user who holds the private key.

ECC also plays an important role in key exchange. For example, the Diffie Hellman key exchange protocol can be implemented based on elliptic curves, where the communicating parties can negotiate a shared key over an insecure channel for subsequent encrypted communication. The specific process is as follows: User A and User B first select the same elliptic curve and base point P. User A generates the private key a and calculates the public key A=aP; User B generates private key b and calculates public key B=bP. Then, User A sends Public Key A to User B, and User B sends Public Key B to User A. User A calculates the shared key K=aB=abP, and User B calculates the shared key K=bA=baP. Due to the multiplication exchange law, the shared key obtained by both parties is the same.

4.3 Example of Identity Authentication Scheme Based on Algebraic Curve 5.3

4.3.1 ECC based digital identity authentication system

A certain financial institution has adopted an ECC based digital identity authentication system for customer login and transaction authentication. The workflow of the system is as follows: When the customer registers, the system generates a pair of public-private keys based on elliptic curves, stores the public key on the server side, and securely stores the private key on the customer's smart device (such as a mobile phone security chip). When the customer logs in, they first enter their

username and password. After the system verifies that the password is correct, it sends a challenge message to the customer's smart device. The client's smart device uses a private key to sign the challenge message and returns the signature result to the server. The server uses the client's public key to verify the signature, and if the verification is successful, the client is allowed to log in. During the transaction process, customers also need to sign the transaction information to ensure the non repudiation and integrity of the transaction.

4.3.2 Combining blockchain and ECC for distributed identity authentication

In a distributed identity authentication system, blockchain technology and ECC are combined. The user's identity information is stored in encrypted form on the blockchain, and each user has a unique digital identity identifier (DID) generated based on an elliptic curve. When a user needs to authenticate their identity, they first send an authentication request to the authentication authority, which obtains the user's public key and related identity information from the blockchain. The user signs the challenge message sent by the authentication authority using the private key, and the authentication authority verifies the validity of the signature using the public key. Due to the decentralized and tamper proof nature of blockchain, as well as the high security of ECC, this distributed identity authentication system can effectively protect user privacy and identity information security, while improving the credibility and efficiency of authentication.

4.4 Security Analysis and Challenges

4.4.1 Security Analysis

The identity authentication scheme based on algebraic curves has significant advantages in terms of security. Firstly, the computational difficulty of elliptic curve discrete logarithm problem ensures the security of the private key, making it difficult for attackers to crack the private key through computation. Secondly, the encryption algorithms used in digital signatures and key exchange further ensure the confidentiality, integrity, and non repudiation of communication. For example, in digital signatures, the use of hash functions ensures the integrity of messages, and the verification process of signatures ensures the source and authenticity of messages.

4.4.2 Challenges Faced

Although algebraic curve based identity authentication has many advantages, it also faces some challenges. One is the demand for computing resources. The elliptic curve cryptography algorithm has a high computational complexity, which may make it difficult for some resource constrained devices (such as IoT devices) to meet the requirements of real-time computing. The second is the threat of quantum computing. With the development of quantum computing technology, traditional cryptographic systems based on discrete logarithm problems are facing the risk of being cracked. Although quantum computers are currently unable to completely crack elliptic curve cryptography, future development trends still need to be closely monitored. The third is the issue of standards and compatibility. Currently, there may be differences in the implementation of different algebraic curve ciphers, and there is a lack of unified standards, which brings certain difficulties to the integration and interoperability of the system.

4.5 Future Development Trends

4.5.1 Research on Quantum Resistance Cryptography Algorithm

To address the threat of quantum computing, researchers are actively exploring quantum resistant cryptographic algorithms, among which new cryptographic systems based on lattice cryptography, encoding cryptography, etc. are expected to be combined with algebraic curve cryptography to form a more powerful quantum resistant identity authentication scheme. For example, lattice based cryptography utilizes difficult problems on lattices to construct cryptographic algorithms with high quantum resistance. Combining it with elliptic curve cryptography can enhance resistance to quantum attacks while ensuring existing security.

4.5.2 Multimodal Fusion Identity Authentication Technology

In the future, identity authentication will pay more attention to multimodal fusion, combining algebraic curve cryptography with biometric recognition, behavior analysis and other technologies to achieve more accurate and secure identity authentication. For example, combining biometric features such as facial recognition and fingerprint recognition with ECC based digital signatures can not only improve the accuracy of authentication, but also increase the difficulty for attackers to forge identities. Meanwhile, by analyzing user behavior patterns such as typing habits and mouse movement trajectories, the security and reliability of identity authentication can be further enhanced.

Algebraic curves have shown great potential and application value in the field of identity authentication security. Through in-depth research and continuous innovation, identity authentication technology based on algebraic curves will play a more important role in the future field of information security, providing solid support for safeguarding user privacy and data security.

5. Future research

5.1 Directions and challenges

ECC based digital signature is a technique used to verify information integrity and sender identity. The ECC based digital signature algorithm has high efficiency and security, and is widely used in fields such as e-commerce and e-government.

Key exchange protocol based on ECC is an important part of identity authentication, used to generate and exchange keys during communication between both parties. The ECC based key exchange protocol has high efficiency and security, and can resist various attacks.

Identity authentication based on zero knowledge proof. Zero knowledge proof is a cryptographic technique used to prove a fact during the authentication process without revealing any useful information. The identity authentication technology based on elliptic curve zero knowledge proof can effectively solve security risks such as replay attacks.

5.2 Future research directions and challenges

Although ECC based identity authentication technology has achieved significant research results, it still faces some challenges. With the continuous improvement of computing power and the development of quantum computing, traditional cryptographic algorithms based on algebraic structures may face threats. Therefore, it is necessary to constantly explore new algebraic structures and challenges to address future information security challenges.

To address the threat of quantum computing, it is necessary to explore new algebraic structures and challenges, such as quantum secure cryptographic algorithms.

The integration of algebraic structures with other technologies will be more widely and deeply applied in information security. The integration with other technologies such as artificial intelligence and blockchain will bring new ideas and methods to information security.

6. Conclusion

This study explores the application of algebraic curves, particularly elliptic curves, in identity authentication security. By providing a detailed introduction to the algorithm principles and security analysis of elliptic curve cryptography (ECC), as well as the specific implementation and experimental results analysis of ECC based identity authentication technology, this study demonstrates the effectiveness and security of ECC based identity authentication technology in the field of information security. In the future, with the continuous advancement of technology and the emergence of new challenges, we need to continue researching and innovating to fully leverage the advantages of algebraic structures and lay a solid foundation for building a secure digital world.

Acknowledgement

Fund Project: Hainan Vocational University of Science and Technology Research Fund (Project No.: HKKY2024-ZD-22).

References

[1] V. Gopar Processor, system, method, and device for secure elliptic curve cryptography instructions: CN201780045957.X[P].CN109479003B[2025-02-26].

[2] Liu Ziyao, Chen Jianhua, Wei Yongshuang Authentication Protocol Based on Elliptic Curve Cryptography in Multi Server Environment [J]. Journal of Mathematics, 2024, 44(3):212-224.

[3] Yang Guotao, Cao Chong, Han Tao, etc Password security authentication method based on hybrid encryption in the Internet of Things [J]. Application of microcontrollers and embedded systems, 2024, 000(4):7.

[4] Yang Qing, Wang Haoxuan, Liang Lei, etc Improved elliptic curve digital signature scheme and case analysis [J]. Computer applications and software, 2023, 40(1):327-330.

[5] Lin Tingting Secure execution of elliptic curve cryptography processes CN202210111179.2[2025-02-26].

[6] Dong Jiankuo, Liu Zhe, Lu Sheng, etc Research progress on efficient software implementation technology of elliptic curve cryptography [J]. Journal of Computer Science, 2023, 46 (5): 909-928