World Journal of Innovation and Modern Technology, Vol. 8, Issue 1, (Jan) 2025
ISSN 2682-5910
DOI: 10.53469/wjimt.2025.08(01).09

With Mathematics as Key: A Path to Unlock the Secret Power of Cryptography

Yijia Xiong

Tinjin No.20 Middle School, No.59, Hubei Road, Heping District, Tianjin.
(Near the Former Site of Hong Kong Tower)
Xyj070226@163.com

Abstract: ***In this paper, the core role of mathematics in cryptography is deeply discussed, and how the mathematical branches such as number theory, group theory and elliptic curve theory provide solid theoretical foundation and construction methods for cryptography algorithms is elaborated in detail. By analyzing the mathematical principles of classical and modern cryptosystems, this paper reveals the mathematical mysteries behind the technology from simple alternative encryption to advanced public key encryption, and shows the key applications of mathematical tools in ensuring information security, realizing secure communication, digital signature and key exchange, etc., providing in-depth insights from the mathematical perspective for further understanding and development of cryptography technology.***

Keywords: Cryptography; Mathematical principles; Encryption algorithm; Quantum computing; Information security.

1. INTRODUCTION

As an ancient and modern subject, cryptography is devoted to the study of information encryption, decryption and communication security, and its development is closely related to mathematics. Mathematical theory is the theoretical basis supporting cryptography technology, and the in-depth study of mathematical theory is the premise and basis to ensure the security of cryptography algorithms [1]. In 1949, Shannon, an American mathematician, introduced information theory into cryptography in her article Information Theory of Security Systems [2], and proposed the theory of symmetric key cryptosystem, which laid a solid theoretical foundation for cryptography. In 1976, Diffie and Hellman, in New Directions in Cryptography [3], demonstrated for the first time that secure communication is possible with keyless transmission between the sender and receiver, ushering in a new era of public key cryptography. In 1977, the National Bureau of Standards (NIST) of the United States announced the data encryption standard [4] developed by IBM, referred to as DES. It is the most commonly used encryption algorithm for commercial secure communications and computer communications in the world. In the mid-1880s, Neal Koblitz [5] and Victor Miller [6] both introduced elliptic curves into cryptography and independently proposed elliptic curve cryptography ECC. In 1984, Bennett and Brassard proposed the first quantum cryptographic protocol, the BB84 scheme [7], and a new member of cryptography was born. In 2001, the National Institute of Standards and Technology officially announced the Advanced Encryption Standard AES [8]. Subsequently, countries such as Europe, Japan, and South Korea also launched the collection of cryptographic standards, and cryptography entered a period of prosperity and development.

2. THE KEY POSITION OF MATHEMATICAL FOUNDATION IN CRYPTOGRAPHY

2.1 Number Theory: The Cryptographic Value of Integer Properties

Number theory mainly studies the properties and laws of integers and has a wide and profound application in cryptography. For example, Euclidean algorithm to find the greatest common divisor (GCD) is an important fundamental step of RSA algorithm. The RSA algorithm takes advantage of the number theoretic property that it is easy to multiply two large prime numbers, but extremely difficult to factor their product. Given two large prime numbers p and q, calculating $n = pq$ is quick and easy, but it is computationally almost impossible to factor p and q when p and q are large enough. This ensures the security of cryptographic systems built on n.

2.2 Group Theory: The Structural Cornerstone of Symmetric Encryption

A group in group theory is a set with specific operational rules and properties. In symmetric encryption algorithms

such as AES (Advanced Encryption Standard), byte substitution and substitution operations can be viewed as operations on specific finite field group structures. By defining appropriate addition and multiplication rules, bytes can be confused and diffused after a series of group operations, so as to achieve the purpose of encrypting data. The encryption operation based on group structure ensures the reversibility of the encryption process (decryption by corresponding reverse operation) and the resistance to various attacks. Its rigorous group operation rules provide a clear logical framework and strong encryption ability for the design of encryption algorithms.

2.3 Elliptic Curve Theory: Mathematical Frontiers of Emerging Cryptographic Applications

Elliptic curve cryptography (ECC) is based on the elliptic curve discrete logarithm problem (ECDLP), which provides comparable or even higher security at shorter key lengths than traditional cryptography based on integer decomposition or discrete logarithm problems. The points of an elliptic curve over a finite field form an Abelian group with a unique addition rule, and cryptography takes advantage of the relatively easy scalar multiplication of points over this group, but given two points, finding their discrete logarithm (i.e., satisfying \(k\) in \(Q = kP\), Where \(P,Q\) is a point on an elliptic curve), this property is very difficult. This makes elliptic curve cryptosystems a significant advantage in resource-constrained environments (e.g., mobile devices, iot devices), as shorter keys can be used to achieve high-strength encryption, reducing computational overhead and storage requirements, while maintaining password security.

3. ANALYSIS OF MATHEMATICAL PRINCIPLES OF CLASSICAL CRYPTOSYSTEM

3.1 Caesar Cipher: Mathematical Description of Simple Shift Transformations

Caesar cipher is a simple alternative encryption method, which replaces each letter of the plaintext by a fixed number of digits. From a mathematical point of view, this can be precisely described by modular operations. Suppose the alphabet have \ n \ () A letter (e.g., English letters \ (n = 26 \)), the shift key for \ \) (k, for clear letters \ \ (x) (with digital \ \ (0) to the \ \ (n - 1), said \ \) (A = 0, for example, \ (B = 1 \), etc.), The encrypted ciphertext \(y\) can be expressed as \(y=(x + k)\bmod n\). This simple mathematical transformation provided a certain degree of confidentiality at the time, but because its key space was too small (only \(n\) possible shifts), it was easy to crack by brute force, and is a simple example of the early application of mathematics in cryptography, showing the basic mathematical abstract form of the encryption process.

3.2 Virginia Cipher: Mathematical Logic of Multi-Table Encryption

The Virginia cipher encrypts the plaintext by using a combination of multiple Caesar ciphers, with the key being a sequence of letters. Let the plaintext be \(m = m_1m_2\cdots m_l\), the key be \(k = k_1k_2\cdots k_d\) (length \(d\)), when encrypting, Cipher \ (c = c_1c_2 \ cdots c_l \) each character in the \ (c_i \) by \ (c_i = k_ (m_i + {j}) \ n \ bmod) calculated, including \ (j = I \ \ d bmod). This multi-table encryption method increases the complexity of the key space and password, and is more difficult to crack than the Caesar cipher. However, with the development of mathematical analysis methods, it is still possible to carry out effective attacks on ciphertext by means of frequency analysis and key length prediction. This reflects the reverse role of mathematical methods in cryptanalysis, that is, by revealing the mathematical logic of the encryption process to find a way to crack, and promotes the development of cryptography from simple encryption to more complex and more secure encryption methods.

4. THE MATHEMATICAL MAGIC OF MODERN CRYPTOGRAPHY

4.1 RSA Algorithm: The Number Theoretic Wonder of Public Key Cryptography

The core of RSA algorithm lies in Euler's theorem and modular power operation in number theory, and its exquisite mathematical structure realizes the separation of encryption and decryption process, which lays a solid foundation for modern secure communication. First choose two large prime Numbers \, p \ and \ \ (q), computing \ (n = pq \) and euler function \ (\ varphi (n) = (p - 1) (q 1) \). Then choose an integer \(e\) that is prime to \(\varphi(n)\) as part of the public key, where \(e\) must meet certain conditions. For example, (1 < < e, varphi (n) and \ \) (GCD (e \ varphi (n)) = 1 \) (\ greatest common divisor (GCD) \ said). Then by extending Euclid's algorithm to find \(d\) such that \(ed\equiv 1\bmod\varphi(n)\), that \(ed = k\varphi(n)+1\) (\(k\) is an integer), \(d\) is the private key.

The encryption process is \(c = m^e\bmod n\) (where \(m\) is plaintext), this step takes advantage of the unidirectivity of modular exponentiation, and it is difficult to backmap the plaintext \(m\) from the ciphertext \(c\) without knowing the private key. Decryption is \ (m = c ^ d \ n \ bmod), its validity is based on euler's theorem: if \ (a) \ \ n \ co-prime, is \ (a ^ {\ varphi (n)} n \ \ 1 \ bmod equiv). For the encrypted cryptograph \ (c = m ^ e \ n \ bmod), when the decryption \ (c ^ d = (m ^ e) = m ^ ^ d {of} Ed \), due to the \ \ varphi (Ed = k (n) + 1 \), so the \ (m ^ {of} Ed = m ^ {k \ varphi (n) + 1} \). When \ [m \ with the \ n \) co-prime, according to euler's theorem is \ (m ^ {\ varphi (n)} n \ \ 1 \ bmod equiv), is \ (m ^ {k \ varphi (n)} n \ \ 1 \ bmod equiv), So \ (m ^ {k \ varphi (n) + 1} \ \ bmod equiv m n \), which successfully restore clear \ [m \). When \(m\) and \(n\) are not mutually prime, which is very rare and can be dealt with by some technical means, the correctness of the decryption can be proved by similar number theoretic reasoning.

Its security depends on the difficulty of factoring large integers, which mathematically guarantees that the plaintext \(m\) cannot be easily derived from the public key \(e\) and \(n\) without knowing the private key \(d\). With the improvement of computer computing power, in order to ensure the security of RSA algorithm, the number of prime numbers \(p\) and \(q\) is also increasing, and it is recommended to use at least 2048 bits \(n\). RSA algorithm provides a reliable foundation for secure transmission (such as data encryption in HTTPS protocol) and digital signature in modern network communication. It is one of the most representative successful applications of mathematical theory in cryptography, realizing a major breakthrough in public key cryptography, and changing the mode of traditional cryptography that encryption and decryption keys must be the same and need to be shared in secret. It has greatly promoted the development of e-commerce, e-government and other fields, making secure remote communication and data exchange possible.

4.2 Diffie-Hellman Key Exchange: Secure Negotiation of Discrete Logarithms

Diffie-Hellman key exchange is based on the discrete logarithm problem, which solves the difficult problem of secure key sharing negotiation between two communication parties on insecure channels. The communicating parties (Alice and Bob) choose a common large prime \(p\) and a generator \(g\) (\(g\) is the primary root of \(p\)), which has important mathematical properties, that is, for \(1\leqslant i\leqslant p-1 \), The result of \(g^i\bmod p\) varies, producing a complete sequence of loops from \(1\) to \(p-1 \).

Alice selects a secret integer \(a\) and computes \(a = g^a\bmod p\) to send to Bob, and Bob selects the secret integer \(b\) and computes \(b = g^b\bmod p\) to send to Alice. Then Alice calculation \ (s = B ^ a \ bmod p = (g ^ B) ^ ^ a \ bmod p = g {ab} \ bmod p \), Bob calculation \ (s = ^ B \ bmod p = (g ^ a) ^ ^ B \ bmod p = g {ab} \ bmod p \), The \(s\) obtained by both parties is the same and can be used as a shared session key for subsequent encrypted communications.

Due to the discrete logarithm problem (known \ \ (g), A \ [p \) and \ [g ^ x \ bmod p \ \ \) (x) on the computing difficulty, even if the attacker had intercepted \ (A) \ and \ [B \), is also difficult to deduce the \ (A) \ and \ [B \) to get the Shared secret \ (\ s). Currently, for large prime numbers \(p\), the solution of the discrete logarithm problem is computationally time-consuming, making Diffie-Hellman key exchange relatively secure in practical applications. This key exchange method cleverly uses the discrete logarithm problem in number theory to solve the problem of secure negotiation of shared keys on insecure channels. It is a key technology in modern cryptography to ensure the initial stage of communication security, and supports the key establishment process in many network protocols, such as IPsec (IP security protocol) and TLS (Transport layer security protocol). The secure communication can be realized in an open network environment, which provides an important guarantee for the confidentiality and integrity of network communication. It is widely used in various network application scenarios, from enterprise-level remote office systems to ordinary users' online banking transactions and social media communications, etc., to ensure the privacy protection of data in the transmission process.

5. APPLICATION EXPANSION AND CHALLENGE OF MATHEMATICAL TOOLS IN CRYPTOGRAPHY

5.1 Changes in Cryptography Mathematics in the Era of Quantum Computing

With the rapid development of quantum computing technology, traditional cryptosystems based on mathematical problems (such as large integer decomposition in RSA, discrete logarithm problem, etc.) are faced with unprecedented severe challenges. Quantum computers use quantum bits and quantum gates to handle a large

number of computing tasks in parallel, and their computing power has been exponentially improved compared to traditional computers. For the large integer decomposition problem that RSA relies on, quantum computers can run the Shor algorithm to complete the decomposition in polynomial time, which makes many existing cryptographic algorithms vulnerable in the quantum computing environment.

This change has prompted the cryptography community to actively explore cryptosystems based on new mathematical problems or quantum resistance. For example, lattice based cryptography, a lattice is a discrete set of points in a \(n\) dimensional space with rich mathematical structure and complex geometric properties. Lattice-based cryptosystems take advantage of difficult problems in lattices, such as the shortest vector problem (SVP) and the nearest vector problem (CVP). Mathematically, given a lattice basis (a set of linearly independent vectors generating a lattice), finding the shortest non-zero vector in a lattice or the nearest vector in a lattice to a given vector are computationally difficult problems, and are considered to have a high level of security even in quantum computing environments.

The mathematical principles of lattice cryptography involve the integration of complex geometric, algebraic and number theory knowledge. In the aspect of algorithm design, it is necessary to deeply study the lattice structure, such as how to construct appropriate lattice bases, so that the cryptographic algorithms based on these lattice bases are both secure and efficient. At the same time, algorithms on the lattice, such as the lattice basis reduction algorithm (such as LLL algorithm and its variants), need to be continuously optimized to improve the computational efficiency while ensuring their security in cryptography applications. In addition, it is also necessary to study the compatibility of lattice cryptography with other cryptographic requirements, such as key management, digital signature, homomorphic encryption and other functions, in order to build new encryption algorithms and protocols that can resist quantum attacks.

Multivariable cryptography is also a research direction of quantum resistant cryptosystems, which is based on the solution of multivariable polynomial equations over finite fields. In a multivariable cryptosystem, the encryption process maps the plaintext to the solution of a set of multivariable polynomial equations, while decryption is solving those equations to recover the plaintext. Since solving multivariable polynomial equations is NP-hard in general, it has certain security even in the face of the powerful computing power of quantum computers. However, multivariable cryptography is faced with the problems of large key size and relatively low algorithm efficiency, so it needs to be further optimized from mathematical theory and algorithm design, such as clever selection of polynomial forms and optimization of solving algorithms, so as to improve its feasibility and performance in practical applications.

Quantum key distribution (QKD) uses the principle of quantum mechanics to achieve secure key distribution. Its core principles are based on the non-cloning theorem of quantum states and the Heisenberg uncertainty Principle. In the QKD process, the two communication parties transmit quantum states (such as the polarization state of photons, etc.) through quantum channels, and use classical channels to assist information exchange and key negotiation. Due to the special properties of quantum states, any eavesdropping behavior on quantum states will inevitably introduce interference. Communication parties can detect whether there is eavesdropping by detecting the integrity of quantum states, so as to ensure the security of key distribution. From a mathematical point of view, QKD involves the knowledge of quantum information theory, probability theory, error correction code and other mathematical fields, and needs to accurately design the coding, transmission, measurement and key extraction processes of quantum states to maximize the key generation rate and minimize the bit error rate, while ensuring security. This represents the innovative development direction and key research hotspot of mathematics in the field of cryptography in response to the challenges of emerging technologies, and provides new hopes and solutions for information security in the post-quantum era.

5.2 Optimization of Mathematical Efficiency in Cryptography Applications

In practical applications, cryptographic algorithms should not only ensure security, but also fully consider computing efficiency and storage efficiency to meet diverse requirements in different scenarios. For example, encryption applications on mobile devices or iot devices have more demanding performance requirements for cryptographic algorithms due to their limited resources (computing power, battery power, storage space, etc.).

Taking elliptic curve cryptosystem (ECC) as an example, optimizing the dot multiplication algorithm is very important in resource-constrained environment. The dot product operation (i.e. \(kP\), where \(k\) is an integer and \(P\) is a point on an elliptic curve) is one of the most time-consuming operations in ECC. The calculation

efficiency can be significantly improved by selecting a suitable coordinate system. In affine coordinate system, the addition and multiplication of elliptic curve points need to carry out complex fraction operation, which involves inverting operation, and the calculation cost is high. By introducing additional coordinate components, the projective coordinate system can represent the elliptic curve equation in a homogeneous way, so that the addition and multiplication of points can be transformed into simpler integral operations, avoiding frequent inverse operations, and thus greatly improving the calculation speed.

In addition, computational techniques such as Montgomery algorithm and window algorithm can be used to further optimize the dot multiplication operation. Montgomery algorithm makes use of the special property of elliptic curve point operation, and reduces the number of multiplication operations in the process of point multiplication by precalculation and clever transformation. The window algorithm represents the integer \(k\) as a binary window form. By calculating some fixed multiples of points (such as \(2^iP\)) in advance, the corresponding predicted points are quickly selected for addition operation according to the window value during the dot multiplication process, which reduces the actual number of point operations.

In symmetric encryption, it is also necessary to use mathematical optimization method to improve the efficiency of encryption. For example, in AES algorithm, the performance is improved by improving the wheel function design. Operations such as byte substitution, row shifting, and column obfuscation in a round function can be viewed as linear and nonlinear transformations over a particular finite field. By optimizing the matrix representation and operation order of these transformations, using mathematically fast algorithms (such as fast multiplication algorithms over finite fields), it is possible to reduce the amount of computation for each round of encryption, thereby increasing the overall encryption speed. At the same time, for large-scale data encryption scenarios, such as data storage encryption in the cloud computing environment, it is also necessary to consider how to use parallel computing, distributed computing and other technologies combined with cryptography algorithms. Mathematically, this involves task decomposition and the design of collaborative computing strategies. For example, a large data block can be divided into multiple subblocks, which are encrypted in parallel on different computing units, and then the encryption results of each subblock are integrated into the final ciphertext by appropriate mathematical methods (such as key management and ciphertext merging algorithm). Or the use of data redundancy and coding technology in distributed computing, combined with cryptographic encryption algorithms, to improve the overall efficiency of encryption under the premise of ensuring data security, in order to meet the diversified needs of practical applications for cryptographic performance. This is an important research topic in the field of mathematics application in cryptography engineering, which is related to whether cryptography technology can be widely and efficiently deployed and applied in various practical scenarios, and is of great significance for promoting the security development of information technology.

6. CONCLUSION

As the cornerstone and soul of cryptography, mathematics runs through the development of cryptography. From the simple transformation of classical cryptography to the complex structure of modern cryptography, every major breakthrough in cryptography relies on the innovation and application of mathematical theory. Number theory, group theory, elliptic curve theory and other mathematical branches provide rich tools and solid theoretical support for cryptography algorithms, so that cryptography can play a key role in the field of information security, to cope with increasingly complex security threats and diversified application needs. However, with the continuous progress of technology, especially the arrival of the era of quantum computing, cryptography is facing new challenges and opportunities, requiring mathematicians and cryptographers to work closely together, continue to explore new mathematical principles and methods, optimize existing algorithms, develop quantum resistant cryptography, open a new chapter of cryptography with mathematical wisdom, and continue to protect the security and privacy of the information world. To ensure that in the ever-changing wave of technology, the mysterious power of cryptography can always be accurately harnelled to escort human digital life.

REFERENCES

[1] Zhang Anyuan. Research on Several Mathematical Problems in Advanced Data Encryption Standard [D]. Xidian University,2011.
[2] Claude Elwood Shannon. Communication theory of secrecy systems [J]. Bell System Technical Joumal, 1949,28: 656-715.
[3] Whitfield Diffie, Martin E. Holmall. New directions in cryptography [J]. IEEE Transactions on Information Theory,1976,22(6):644-654.

[4] National Bureau of Standards. Data Encryption Standard [J]. Federal Information Processing Stan (lard, U. S. Department of Commerce, FIPS PUB 46, Washington, DC, 1977.
[5] Neal Koblitz Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987,48:203-209.
[6] Victor S.Miller. Uses of elliptic curves in cryptography [J]. Advances in Cryptology - CRYPTO '85, Springer - Verlag, LNCS218, 1986417-426.
[7] Charles H Bennett, Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing [J]. Processing of the lEEE International Conference on Computers Systems and Signal Processing, Bangalore India, 1984,12:175-179.
[8] National Institute of Standards and Technology. Federal Information Processing Standards Publication 197. Specification for the Advanced Encryption Standard.2001