Cryptosystem Components and Anticipation on Quantum Challenges in Modern Cryptographic Systems

Kaiyuan Xiao *

RDF International School, Shenzhen, Guangdong, Dapeng Kwai South Road, Longgang District, China

* Corresponding Author Email: xky440303@gmail.com

Abstract. Cybersecurity threats are considered one of the major dangers in internet, which are the major threats of modern communication systems. Data breaches and cyber threats endanger information in digital networks. Cryptography could ensure data protection during the transitions between parties by transforming readable text into protected forms. This paper analyzes and reviews symmetric and asymmetric cryptosystems, their components, the number theory behind cryptography, their representative applications, and emerging trends through literature analysis. Symmetric cryptosystems have the advantage of encryption's speed, while asymmetric cryptosystems such as RSA and ElGamal cryptosystem provide secure and stable key exchange. Applications extend to cloud computing and Internet of Things devices. Furthermore, this paper covers blockchain and machine learning privacy use tools like homomorphic encryption and Secure Multi-Party Computing. Emerging trends address quantum computing risks and privacy in blockchain and machine learning, jeopardize traditional cryptosystems, whereas scientists are conducting numerical research to explore new solutions through the post-quantum methods and AI integrations. Future developments should focus on efficiency enhancements for robust security of cryptography.

Keywords: Cryptography, Cryptosystem, Rivest-Shamir-Adleman, Quantum threats, Data security.

1. Introduction

Data security is essential in modern communication. Cyber threats, such as hacking and interception, leak sensitive information during transmission. Cryptography addresses these risks by encrypting data in unreadable cipher text to prevent unauthorized access. Its role has grown with the expansion of digital networks. Symmetric cryptography takes a single open key, the public key, for coding the plain texts into cipher texts and decoding the cipher texts into plain texts, cost less time in encrypt or decrypt than asymmetric cryptography especially in big amount of data. Asymmetric cryptography employs public and private keys, enabling secure key exchange without prior sharing. These cryptographies form the fundamental of digital communication and financial transactions [1][2].

Cryptography's skills matter to hold secret, complete, checked, and not rejected. These five characteristics also known as confidentiality, integrity, authentication, and non-repudiation. The first characteristics, confidentiality, holding the privacy of message and only allow the authorized parties to access. Integrity confirms message remains unchanged during transit. Authentication verifies sender and receiver identities. Non-repudiation prevents denial of message authenticity. These properties are crucial in environments such as digital communication and financial transactions, where data leaks cause financial or privacy losses. As technology advances, quantum computers pose new challenges by solving complex mathematical problems quickly [3][4].

Symmetric systems emphasize efficiency, while asymmetric systems such as RSA and ElGamal emphasize security. Both RSA and ElGamal rely on the number theory, RSA demand on prime factorization, and ElGamal utilizes discrete logarithms. Components include encryption and decryption of data, digital signatures for authenticity, hashing for integrity checks, public key infrastructure for key management, and protocols for standardized processes. Emerging trends involve quantum-resistant methods and privacy tools for blockchain and machine learning. This paper analyzes number theory foundations, RSA improvements, ElGamal mechanics, and modern

applications; compares algorithm strengths, such as speed versus security; and evaluation draws from studies on quantum threats, AI integrations, and privacy protections [4][5][6].

Objectives are to elaborate cryptosystem components, explain symmetric and asymmetric types, explore number theory and cryptographic applications, assess real-world uses in cloud and IoT, and evaluate emerging challenges like quantum computing. Structure follows: fundamentals in section 2, emerging technologies and evaluation in section 3, and conclusion in section 4. This provides a clear path to understanding cryptosystems' role in secure data transmission.

2. Fundamentals of Cryptosystems

Cryptography is the main today's info safe, with responsibility to guard data private and communicating from outside change or threat. Its importance in data security cannot be ignored; it maintains a stable security way to sending sensitive data through unguaranteed networks. It has two main types: symmetric and asymmetric, and it has five fundamental components, namely Encryption, Digital signatures, Hashing, Public key Infrasturcture (PKI), and Cryptographic protocols.

The five components are the foundations of cryptosystem. Confidential ensuring the context can only accessed by those with authorization. Integrity gives good that data will not alter while sent or saved. Authentication holding the data and only access to the authorized parties. By employing non-repudiation, it making sure a party cannot reject their message's real [4].

2.1. Symmetric & Asymmetric cryptography

Encryption is the process to make the message into hidden form of cipher text. Symmetric and asymmetric cryptosystems are two major foundations of cryptography.

In symmetric key cryptography, parties generate and use only one key for encryption.

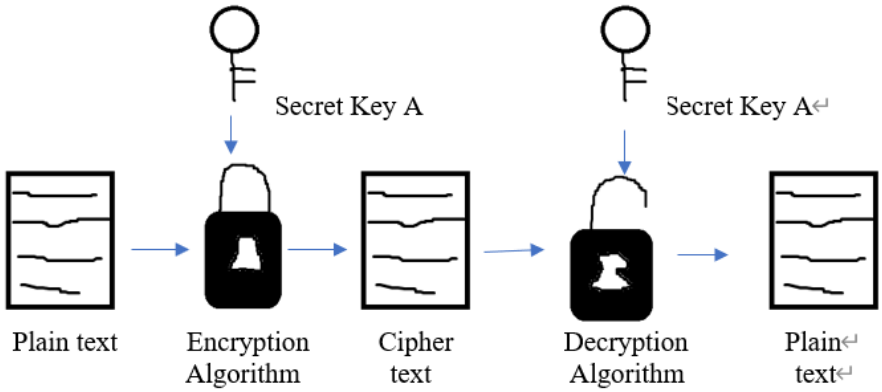

Figure. 1 Symmetric cryptography Data from: [5]

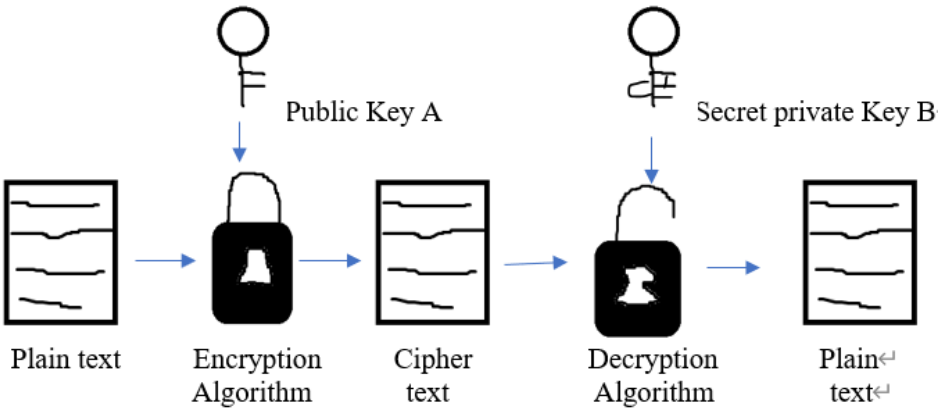

Figure. 2 Asymmetric cryptography Data from: [5]

Figure 1 shows how symmetric cryptosystem works, the encryption applies on the plain message in order to generate an unreadable cipher text, then the decryption apply on the cipher text to translate the text into human-readable message. AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES), RC4, Blowfish algorithm classes could be employed in implement symmetric encryption [5]. Symmetric cryptography has some benefits: Symmetric cryptography is generally faster and effective than asymmetric cryptography, because of the number of private keys; asymmetric cryptography has to generate private keys as much as the numbers of parties who take part in the message sending or receiving; consequently, it puts less computational load on computers than asymmetric cryptography. In addition, symmetric cryptosystem could be stable and securely as well as it combined with a trusted key management system. Notwithstanding, this cryptography could be rendered unsafe if the communicating parties accidentally reveal their secret key [5].

Figure 2 demonstrates how asymmetric cryptography works. It requires two distinguishing keys: the public keys and the private secrete keys. The public keys are employed to generate cipher text from plain text, while the private keys will hold by users secretly and employed to translate the cipher text into human message. All parties have authority to access the public key, however, each of the parties has their unique private secrete key that others have no authority to access. In general, the universal public key is employed in the encryption part of asymmetric cryptography, however, it can be utilized in decryption algorithm if the private key is applied in encryption algorithm. Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Digital Signature Algorithm (DSA) could be utilized in asymmetric cryptography [2]. Asymmetric cryptography has advantage in key distribution, digital signatures and secure communication. Under asymmetric cryptography, the encrypted text is sending without the needs of a stable channel for key exchange, to accomplish that, each parties have their own secrete private key instead of changing public key. Besides, asymmetric cryptography can guarantee the message's integrity and authenticity by sign the message through private key, and users can utilize the public key to confirm the signature. Furthermore, asymmetric cryptography is able to secure communications within an insecure channel, because of the confidential private key hold by individuals. Nevertheless, because of the tedious process and intricacy mathematical calculations of generating private key, asymmetric cryptosystem requires longer time than symmetric cryptosystem to complete its work, especially when they have to dealing with great amount of data quantities. Coupled with the difficulty to decipher encrypted data without private key, thus it requires demanding strict private key management [6].

2.2. Number Theory

Number Theory plays an indispensable role in cryptography, many concepts such as greatest common divisors, the notion of primes, Euler's phi function, and congruences are employed by cryptography.

Prime numbers are any positive integer that has only 2 factors, 1 and itself, except number 1.

Set Z be the set of integers. If a, b $\in$ Z, then the largest positive factor of both a and b is the greatest common divisor (GCD) of a and b, scientists apply the equation

$$gcd(a, b) \tag{1}$$

To indicate this biggest positive factor [3]. According to the definition of prime numbers, the GCD of any two distinguish primes is 1, and scientists name that a is coprime to b if gcd(a, b) = 1.

A remainder comes from the process of dividing a number by a number. The definition of congruence supports the situation that two integers have the same remainder when divide by a non-zero number. Set a, b, n $\in$ Z such that n = 0, a is congruent to b modulo n when a and b have the same remainder after divide by n. For this relationship, scientist denote that

$$a \equiv b \ (mod\ n) \tag{2}$$

Another formular

$$n \mid (a - b) \tag{3}$$

Is equivalent to state that n divides the difference of a and b. 69 ≡ 44 (mod 5) is a good example of the formular, in this case, the remainders are the same number upon the division of 69 and 44 with 5 [7].

The Euler's phi function is employed in the computation of the number of integers in a given range. Let n ∈ Z be positive, then Euler's phi function could determine the number of integers a, with $1 \leq a \leq n$, such that gcd(a, n) = 1, and denoted the number by ϕ(n) [8].

2.3. The Rivest-Shamir-Adleman Cryptosystem

The RSA cryptosystem represents the public key cryptosystem; it utilizes a public key to encrypt plain contexts and utilizes private keys to decrypt cipher contexts. Under RSA cryptosystem, parties distribute their public keys while holding their private secrete key. RSA apply techniques from elementary number theory to its encryption and decryption processes: To start with the process, RSA will choose two primes p and q and let n = pq, then it will set e ∈ Z be positive such that

$$gcd\ (e, \phi(n))\ =\ 1. \tag{4}$$

Subsequently, it will compute a value for d ∈ Z such that de ≡ 1 (mod ϕ(n)). Parties will get their public key and private key in these five variables, public key is the pair (n,e) and the private key is the triple (p,q,d). Then, for any non-zero number m<n, encrypt m using

$$c\ \equiv\ m\text{^}e\ (mod\ n). \tag{5}$$

Eventually, RSA can decrypt c using m ≡ c^d (mod n) [6].

2.3.1 Improved RSA Algorithm

People use the RSA public key system in variants of places, such as for browsing the web or in smart cords. This algorithm was published in 1976, thus many researchers kept exploring the vulnerabilities in the RSA cryptosystem. There are some significant attacks, Bonech (2002) and Coppersmith (2001), indicate that RSA cryptosystem could be violated. Admittedly, the RSA cryptosystem could be considered insecurity with the improvement of technology, but no attacks has totally wrecked the basic version yet [9]. However, with the threat of quantum computing which can easily break the cipher texts under RSA cryptography, some scientists have explored an Improved Rivest-Shamir-Adleman Cryptosystem (IRSA). RSA apply integers from 0 up to n-1 for both the original message and the encrypted one. However, in IRSA, the message M and encrypted C under the IRSA cryptosystem are in these following forms:

$$C\ =\ M\text{^}(y/x)\ mod\ n,\quad M\ =\ C\text{^}d\ mod\ n\ =\ (M\text{^}(y/x))\text{^}d\ mod\ n. \tag{6}$$

The sender and receiver both have to know n, y, and x, but only the receiver has the variable d [10].

To demonstrate the process of IRSA, here is a public key KU= {y,n}, {x} and a private key KR= {d,n}. Before the process of encryption, the values have to satisfy that it is possible to find y, x, d, n such that (M^(y/x)) ^d = M mod n for all M<n; It is reasonable to compute M^(y/x) and C^d for all values of M<n; y is a multiple of x and e. At the beginning of the process, IRSA will selecting two prime numbers p and q, then computing their product n, which is the modulus of the encryption and decryption. Then, it is necessary to have the quantity φ(n) which is referred to the Euler totient of n, the positive integers which are less than n and relatively prime ton, and select an integer e that is relatively prime to φ(n). After this, IRSA will select two numbers x and y such that y= xe, and using these numbers formulate two public keys {y,n}, {x}. Eventually, IRSA will compute the variable d as the multiplicative inverse of the variable e, modulo φ(n). Suppose the party A has published its public key and that the party B wishes to send the message M to A, then the party B will compute C = M^(y/x) mod n, and transmits C [10]. This tedious process will affect the time of generating keys; thus, IRSA cryptosystem will have a greater key generation time than RSA cryptosystem because of the additional variables x and y. Although the complicated process will delay the generation time, it

will benefit the security of the private keys, and prevent the potential dangers which might jeopardize the intimacy of users.

2.3.2 Other cryptosystems

Taher ElGamal came up with the ElGamal system in 1984, it is a cryptosystem based on the Discrete logarithm. This cryptosystem could be applied in the one direction encryption, means the sender or the receiver does not have to take part in the process of encryption when one party is already in the process [8]. To utilize ElGamal cryptosystem, a user needs a prime p, a generator g, and private key x. The public key is (p,g,h), where h = g^x mod p. A random variable k is necessary to make cipher text (c1, c2) = (g^k mod p, M*h^k mod p) for encryption. The user only needs to recover M by using x to decrypt the cipher text [11].

DSA cryptography is utilized by the recipient to ensure a message has not been interrupted by attackers during the transition of a communication and confirm the identity of sender. A digital signature is used by the receiver to verify the communication was signed by the sender in the form of electronic written signature. Furthermore, digital signatures could be created in the purpose of confirming the integrity of stored data and programs [12].

3. Emerging Technologies and Evaluation of cryptosystems

As the growth of technology, quantum computing and AI have significant impact on cryptography. These emerging technologies give challenges to cryptosystems but also boost the improvement of cryptosystems. This section explores their impact and evaluates cryptosystems.

3.1. Quantum Computing threats and solutions

Quantum computers run on qubits, or quantum bits, they can be created in several ways such as using superconductivity. Superconductive qubits require an extremely cold environment to work for long periods. Quantum cryptography based on the ordinary cryptography but has some breakthrough, it utilizes the principles of how quantum particles act to make communication super safe by nature. Classical cryptography could operate only based on bits in binary states, while quantum computers operate based on leverage quantum bits which can exist in multiple states. Thus, it can solve complicated problems exponentially faster than ordinary computers due to these unique properties. In fact, the quantum computers have the incredible rate of computing data, which will jeopardize the security of cryptosystems based on discrete logarithms, specifically it can crack the ordinary cryptosystems' codes in a moment. AI computing is one of the realizable solutions to the quantum threats of modern cybersecurity [13][14].

3.2. Artificial intelligence

Lately, scientists and cryptographic experts investigating the convergence of AI and quantum cryptography. AI has unique advantage on processing data, recognizing patterns, and make informed decisions . Pairing AI's computing strength with quantum cryptography's strong security could handle big amount of data transitions and prevent the growing potential cyber risks on data security. AI methodologies can contribute to quantum cryptography in cryptographic protocols. But AI still needs advances on stabilize the quantum processes. Quantum systems can provide a safe environment for AI computing, benefit the protection of data. The convergence of quantum cryptography and AI can help create new safe computing methods that predict, fix, and strongly fight quantum dangers[13].

4. Application, Evaluation and Comparison of Cryptosystems

The Internet of things (IoT) is a newly-developing technology; it links tons of through the public Internet; it requires data security to prevent from numerals attacks on the communications. Cryptography plays a significant role in it. Elliptic Curve Cryptography can cut down on the steps to generate keys, which can enhance the rate of encryption and decryption. Through ECC, the key-sizes

will be remarkable smaller than RSA cryptography's, the difference will grow exponentially to keep the same function as compared to the general computing power available [15][16]. Lattice-based cryptosystems have the ability to resist quantum attacks but require high computation because of the complicated process of generating keys [17].

Blockchain has been apply in variant area based on its property of Peer-to-peer trusted trading mechanism, with the disadvantage of insecurity and low privacy. The attack on Ethereum Classic in 2019 is good example that indicate the disadvantage of blockchain. Numerous cryptographic methods have been used to prevent these problems, such as Schnorr Signature, RSA, ECC, Ring signature. Machine learning promotes the improvements of artificial intelligence, but it faces serious privacy leakage problem because of the different data sources. Secure Multi-Party Computing (SMPC) allows two or more parties cooperate for computing the same computational tasks, with the characteristic of correctness, privacy, output accessibility and fairness. Homomorphic Encryption (HE) is the cryptography which can homomorphically map the algebraic system formed by plain text space and its operations to the algebraic system formed by cipher text space and corresponding operations. HE has the ability to compute the cipher text without the decryption process of cipher text, which will benefit the privacy protection. SMPC and HE provide a stable and secure environment for blockchain and machine learning [18][19].

5. Conclusion

Cryptosystems form the base of digital data security. Components such as encryption change data into unreadable cipher forms, while decryption change data back into readable plain form. Digital signatures test the authority of sender to prevent privacy leakage. Hashing prevent data losing by spot the changes of data during encryption or decryption processes. Public key infrastructure handles keys safely. These parts collaborate to block the potential threats during the transaction or communication.

Results indicated symmetric cryptography encrypts data with one key in a high speed. It suits big files but needs safe key exchange channels. Asymmetric cryptography utilizes two keys for more secure and robust exchange. RSA builds on prime factors and Euler's function. ElGamal employs discrete logarithm for strong signatures. New applications fit cloud for remote storage, and IoT for device links to realize innovations, such as furniture digitization. Emerging trends of quantum computing jeopardize the classical cryptosystem and generate quantum threats for data privacy. Artificial intelligence provides new solution of quantum threats by exploit its advantage of computing. Blockchain requires safety cryptography, such as SMPC, RSA, ECC. Machine learning promotes the improvement of ai and keeps data private with multi-party computing.

Cryptography has showed the impact of digital communications, which becomes the generally channel for communicating between people. Numbers are indispensable in human's life style, and it is indispensable in establishment of modern cryptography. The author analysis weighs speed against safety in distinguished cryptosystems, which are utilized by cloud computing and storage, the IoT uses; Analysis the benefit and potential threats of quantum computing; And analysis the demand of applications. Cryptography can defend communications and financial transaction that travel through the internet, prevent potential compromised via external attackers.

For the future outlook, it is necessary to have practical solutions, tougher builds, and tangible targets. Thus, exploring the convergence of quantum computing and artificial intelligence is crucial. The vital goal is to enhancing the security measures to store firmly and access information by keep tracing the changing environment of quantum computing. This paper has given a comprehensive review on cryptography, elaborating the processes of different cryptosystems, expound the principles of number theory, and forecast the conditions of quantum computing and artificial intelligence in the future.

References

[1] A. Jsv Sai Bhargav, Advin Manhar, A Review on Cryptography in Cloud Computing, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 6, Issue 6, 2020.

[2] Sherief H. Murad and Kamel H. Rahouma, Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment, 18th International Learning & Technology Conference 2021.

[3] Kyu-Seok Shim, Boseon Kim and Wonhyuk Lee, Research on Quantum Key, Distribution Key and Post-quantum Cryptography Key Applied Protocols for Data Science and Web Security, Journal of Web Engineering, Vol. 23_6, 813–830, 2024.

[4] Ali AZM. The Power of Cryptography: Hashing and Encryption for Data Protection [J]. Journal of Artificial Intelligence, Machine Learning and Data Science, 2023.

[5] Mohammad Rafeek Khan, Kamal Upreti, Mohammad Imran Alam, Haneef Khan, Shams Tabrez Siddiqui, Mustafizul Haque, and Jyoti Parashar, Analysis of Elliptic Curve Cryptography & RSA, Journal of ICT Standardization, Vol. 11_4, 355–378, 2023.

[6] Minh Van Nguyen, Number Theory and the RSA Public Key Cryptosystem, 05 November 2008.

[7] Z.I. Borevich and I.R. Shafarevich, Number Theory, Academic Press, INC. (London) LTD., 1966.

[8] J. Baskar Babujee, Euler's Phi Function and Graph Labeling, Math. Sciences, Vol. 5, no. 20, 977- 984, 2010

[9] Zheng Zhiyong, Liu Fengxia, and Chen Man, On the High Dimensional RSA Algorithm-A Public Key Cryptosystem Based on Lattice and Algebraic Number Theory, Proceedings of the Second International Forum on Financial Mathematics and Financial Technology, Financial Mathematics and Fintech, 2023.

[10] Israt Jahan, Mohammad Asif, Liton Jude Rozario, Improved RSA cryptosystem based on the study of number theory and public key cryptosystems, American Journal of Engineering Research, Volume-4, Issue-1, pp-143-149, 2015.

[11] Andreas V. Meier, The ElGamal Cryptosystem, June 8, 2005.

[12] Vipin Jain, A Review on Different Types of Cryptography Techniques, An International Multidisciplinary Research Journal ISSN: 2249-7137 Vol. 11, Issue 11, November 2021.

[13] Petar Radanliev, Artificial intelligence and quantum cryptography, Journal of Analytical Science and Technology, 2024.

[14] Shally Nagpal, Shivani Gaba, Ishan Budhiraja, Meenakshi Sharma, Akansha Sigh, Krishna Kant Singh, S. S. Aksar, Mohamed Abouhawwash, and Celestine Iwendi, Quantum Computing Integrated Patterns for Real-Time Cryptography in Assorted Domains, Volume 12, 2024.

[15] Nourah Almrezeq, Md Alimul Haque, A.A. Abd El-Aziz, Device Access Control and Key Exchange (DACK) Protocol for Internet of Things, International Journal of Cloud Applications and Computing, Volume 12 • Issue 1, 2022.

[16] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, Elliptic Curve Cryptography, ACM Ubiquity, Volume 9, Issue 20, 2008.

[17] Zhiyong Zheng, Modern Cryptography Volume 1 Forum, on Financial Mathematics and Financial Technology, 2022.

[18] Jiang Han, Liu Yiran, Song Xiangfu, Wang Hao, Zheng Zhihua, Xu Qiuliang, Cryptographic Approaches for Privacy-Preserving Machine Learning, Journal of Electronics & Information Technology, Vol. 42No. 5, May 2020.

[19] LIU F, YANG J, QI J Y, et al. Survey on blockchain privacy protection techniques in cryptography[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 29-44.