ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Research on the impact of quantum computing on the security of financial data encryption

Wuyun Zhaola

College of Finance, Inner Mongolia University of Finance and Economics, Hohhot, Inner Mongolia, 010070

Abstract: This paper introduces the impact of quantum computing on the security of financial data encryption and analyzes the potential threats that quantum computing may pose to traditional encryption algorithms. Firstly, the basic principles and advantages of quantum computing were briefly described, especially its potential to crack classical encryption algorithms such as RSA and ECC and improve computational efficiency. Secondly, the impact of quantum computing on financial transactions, payment systems, privacy protection, and identity authentication was explored, and the security risks faced by financial data were pointed out. Finally, countermeasures were proposed, including post quantum encryption technology, quantum key distribution (QKD), and cross domain cooperation, aimed at improving the security of the financial system. Although quantum computing brings challenges, the financial industry can address this emerging threat and ensure data security through technological innovation and strategic deployment.

Keywords: Quantum computing; Financial data; Encryption algorithm; Privacy protection

1. Introduction

With the rapid development of information technology, data encryption technology in the financial industry has become a core component in ensuring the security of financial transactions, protecting user privacy, and maintaining financial stability. However, quantum computing, as a new type of computing model, is triggering a revolution in encryption technology with its powerful computing power. Quantum computers can effectively solve some computational problems that traditional computers cannot cope with, but at the same time, they also pose serious challenges to the current encryption system. Especially in the financial field, the development of quantum computing may render existing encryption algorithms ineffective, leading to issues such as data breaches, payment security, and identity authentication.

2. Overview of quantum computing

Quantum computing is a computational method based on the principles of quantum mechanics. Compared to traditional classical computers, quantum computers utilize quantum bits for data processing. Quantum bits can not only be in a state of 0 or 1, but also represent multiple states simultaneously through quantum superposition states, greatly improving the parallel processing capability of computation. The quantum entanglement effect enables quantum computing to achieve more complex and high-speed computing tasks, providing new solutions for some problems that cannot be efficiently solved on traditional computers.

The core advantage of quantum computing lies in its ability to accelerate large-scale computations through quantum algorithms. For example, the Shor algorithm can decompose large integers in polynomial time and crack classical encryption algorithms; The Grover algorithm can perform square root level accelerated search on unordered data. Due to these advantages, quantum computing may have significant potential in cracking

traditional encryption algorithms, particularly posing a serious threat to the protection of financial data.

3. The impact of quantum computing on the security of financial data encryption

3.1. Cracking traditional encryption algorithms

Traditional encryption algorithms mainly rely on the computational complexity of mathematical problems to ensure security, such as RSA algorithm and asymmetric encryption algorithms like elliptic curve cryptography (ECC), as well as symmetric encryption algorithms like AES. The existing encryption system relies on mathematical problems such as large integer decomposition and discrete logarithm, but quantum computing can solve these problems in polynomial time through the Shor algorithm, making encryption algorithms based on these mathematical problems no longer secure.

Specifically, RSA encryption relies on the difficulty of decomposing large integers, but quantum computing can effectively decompose large integers through the Shor algorithm, breaking the security of RSA encryption. Similarly, ECC encryption algorithm also relies on the difficulty of elliptic curve discrete logarithm problem, while Shor algorithm can solve this problem in polynomial time. Therefore, the emergence of quantum computing poses significant security risks to the widely used asymmetric encryption technology in the financial industry[1].

3.2. Security risks of financial transactions and payment systems

Financial transactions and payment systems are the core of the financial industry, involving a large amount of sensitive information and fund transfers. Therefore, ensuring data security during the transaction process is crucial. Currently, most financial systems rely on SSL/TLS protocols and Public Key Infrastructure (PKI) to protect the security of data transmission. Due to the ability of quantum computing to decipher traditional encryption algorithms, these encryption protocols will not be able to effectively protect the security of financial transactions.

The impact of quantum computing on financial trading systems is mainly reflected in two aspects: firstly, quantum computing can crack the encryption algorithms used in data transmission, allowing hackers to steal transaction information. Secondly, quantum computing can bypass existing identity authentication mechanisms and forge user identities for fraudulent operations. With the further development of quantum computing, the security of financial payment systems is facing unprecedented threats, and timely measures need to be taken to ensure the security of financial transactions.

3.3. Challenges of privacy protection and identity authentication

The financial industry involves a large amount of sensitive data of individuals and businesses, including account information, transaction records, identity authentication information, etc. The existing authentication methods, such as digital signatures and certificates based on public key encryption, rely on encryption algorithms such as RSA and ECC to ensure the authenticity of identities and the integrity of data. However, the arrival of quantum computing may render these encryption methods ineffective in protecting the privacy and identity information of financial users.

Quantum computing, through Shor algorithm and other quantum algorithms, can easily crack traditional public key encryption and digital signatures, leading to the leakage of personal identity information and

the tampering of transactions. This challenge means that financial institutions must adopt new encryption technologies and authentication methods to ensure user privacy and identity security before quantum computing becomes a reality[2].

4. Application strategies of quantum computing to enhance the security of financial data encryption

4.1. Application of post quantum encryption technology

In order to address the threat of quantum computing to existing encryption systems, researchers have proposed post quantum encryption technology (PQC). The design of post quantum encryption algorithms aims to resist attacks from quantum computing. Currently, some post quantum encryption algorithms based on lattice theory, encoding theory, and hash functions have been proposed. The goal of post quantum encryption is to build secure encryption schemes even in quantum computing environments. Financial institutions can gradually adopt post quantum encryption technology in the future to protect the confidentiality and integrity of financial data. Especially in the fields of financial transactions, data storage, and user identity authentication, post quantum encryption is expected to provide new security guarantees for the financial industry[3].

4.2. Application of quantum key distribution (QKD) technology

Quantum Key Distribution (QKD) is an encryption technique that utilizes the principles of quantum mechanics to transmit keys. QKD can ensure that the key is not eavesdropped during transmission through the property of quantum entanglement, and once someone steals the key, the system will immediately detect it. This technology can provide extremely high security for financial data transmission. Financial institutions can adopt quantum key distribution technology in the future to protect sensitive information during financial transactions from being leaked. The development and application of QKD technology will become an important means to address the threat of quantum computing, especially in cross-border payments and international financial transactions[4].

4.3. Cross disciplinary cooperation promotes the development of quantum encryption technology

The combination of quantum computing and encryption technology is a complex and long-term process, and financial institutions, academia, and government departments need to work together to promote the research and standardization process of quantum encryption technology. Through cross disciplinary cooperation, the maturity of quantum computing technology can be accelerated, ensuring that the financial industry can maintain security in the era of quantum computing. The financial industry should strengthen cooperation with the field of quantum computing, promote the development of post quantum encryption standards, and ensure the smooth application of these new technologies in the financial system.

4.4. Gradual transition to quantum secure encryption system

Before quantum computing is fully applied, the financial industry needs to gradually transition to quantum secure encryption systems. This is not just a technical adjustment, but also requires corresponding preparations at the policy, legal, and regulatory levels. Financial institutions can gradually improve their system's resistance to quantum computing attacks by implementing hybrid encryption schemes that combine traditional encryption techniques with post quantum encryption techniques. Through this step, the financial industry can be fully

prepared for the future era of quantum computing and reduce potential security risks[5].

5. Conclusion

The emergence of quantum computing poses a huge challenge to the security of financial data encryption. Quantum computing can crack traditional encryption algorithms, threaten the security of financial transactions and payment systems, and bring many challenges in privacy protection and identity authentication. However, with the continuous development of new technologies such as post quantum encryption and quantum key distribution, the financial industry can adopt effective response strategies to ensure the security of financial data. In the future, the financial industry needs to strengthen cooperation with the field of quantum computing, accelerate research and application of technology, and gradually transition to quantum secure encryption systems.

About the author

Wunyun Zhaola (1989.-), female, Mongolian, from Chifeng, Inner Mongolia,Employer: School of Finance, Inner Mongolia University of Finance and EconomicsPhD, lecturer. Research directions: Computer Networks, Financial Technology, Quantum FinanceMailing

References

[1] Yang X .Optimisation method of IoT financial data transmission efficiency based on consensus algorithm of blockchain technology[J].International Journal of Grid and Utility Computing,2024,15(3-4):295-305.

[2] Wang M ,Zhu J .Legal Issues Regarding Financial Data Security and Privacy Protection under Blockchain Technology[J].The Frontiers of Society, Science and Technology,2023,5(16):

[3] Yanni L .Financial Data Security Management Method and Edge Computing Platform Based on Intelligent Edge Computing and Big Data[J].IETE Journal of Research,2023,69(8):5187-5195.

[4] You Z .Regional Financial Data Processing Based on Distributed Decoding Technology[J].Security and Communication Networks,2022,2022

[5] Yun W ,Limei W .Internet Financial Data Security and Economic Risk Prevention for Android Application Privacy Leakage Detection[J].Computational Intelligence and Neuroscience,2022,20226782281-6782281.