THE EFFECT OF QUANTUM COMPUTERS ON CARD PAYMENTS SECURITY

Pavel Kaminsky

University of Mining and Geology “St. Ivan Rilski”, 1700 Sofia; 7Security Ltd, 1407 Sofia, E-mail: p.kaminsky@7sec.com

ABSTRACT. This study explores the potential impact of quantum computers on the security of card payments, providing an overview of the main technologies in use, including cryptographic protocols, quantum key distribution, and post-quantum cryptography. The methodology employed in this research involves a literature review and discourse analysis of academic works, as well as an analysis of current trends and future predictions. The article provides a comprehensive analysis of the potential impact of quantum computing on the security of card payments, including the possibility of brute-force attacks and the potential vulnerability of existing cryptographic algorithms. The findings suggest that post-quantum cryptography can provide a promising solution to address the challenges posed by quantum computers. The study concludes with recommendations for the future of card payments security, including the need for continued research and development in the field of post-quantum cryptography, as well as ongoing efforts to educate and inform stakeholders about the potential risks and benefits of these emerging technologies.

Key words: cybersecurity, payments, quantum computers

ЕФЕКТЪТ НА КВАНТОВИТЕ КОМПЮТРИ ВЪРХУ СИГУРНОСТТА НА КАРТОВИТЕ РАЗПЛАЩАНИЯ

Павел Камински
Минно-геоложки университет „Св. Иван Рилски“, 1700 София: 7Секюрити ООД, 1407 София

РЕЗЮМЕ. В това проучване се разглежда потенциалното въздействие на квантовите компютри върху сигурността на картовите разплащания, като се прави преглед на основните използвани технологии, включително криптографски протоколи, квантово разпределение на ключове и постквантова криптография. Методологията, използвана в изследването, включва преглед на литературата и дискусионен анализ на академични трудове, както и анализ на настоящите тенденции и бъдещи прогнози. В статията е направен цялостен анализ на потенциалното въздействие на квантовите изчисления върху сигурността на картовите разплащания, включително възможността за хакерски атаки и потенциалната уязвимост на съществуващите криптографски алгоритми. Констатациите сочат, че постквантовата криптография може да осигури надеждно решение за справяне с предизвикателствата, породени от напредъка на квантовите технологии. Статията завършва с препоръки за бъдещето на сигурността на картовите разплащания, включително необходимостта от продължаване на научните изследвания и разработки в областта на постквантовата криптография, както и от постоянни усилия за обучение и информиране на заинтересованите страни относно потенциалните рискове и ползи от тези нови технологии.

Ключови думи: киберсигурност, разплащания, квантови компютри

Introduction

In recent years, quantum computing has become a rapidly growing field with many potential applications, but it also poses significant challenges to traditional security measures, especially those used in card payments. Card payments are a critical part of the financial system, and the security of these transactions is of utmost importance to prevent fraud and financial losses. This article will explore the potential impact of quantum computing on the security of card payments but first, the main term used should be defined. Quantum computers are a new type of computer that use quantum mechanics to perform calculations, having the potential to solve certain problems much faster than classical computers. Card payments are transactions made using credit, debit, or prepaid cards, which are processed through a network of financial institutions. Payment security refers to the measures taken to protect these transactions from fraud and other malicious activities.

Quantum computers pose a risk to card payment security as they have the potential to break the encryption algorithms that are currently used to protect these transactions (Gheorghiu & Capraru, 2019). Encryption algorithms are used to convert sensitive information, such as credit card numbers, Card Verification Values/Codes (CVVs/CVCs), and personal identification numbers (PINs), into a form that is unreadable by anyone without the decryption key. These algorithms are based on mathematical problems that are believed to be difficult for classical computers to solve, but quantum computers may be able to solve these problems much more quickly. As a result, the security of card payments may be compromised if quantum computers become widely available (Kiktenko et al, 2020).

Theoretical Framework

To understand the potential impact of quantum computing on card payment security, it is necessary to understand some key concepts and theories in computer science and cryptography. One important concept is the idea of computational complexity, which refers to the difficulty of solving a particular computational problem. The complexity of a problem is usually measured in terms of the number of operations required to solve it, and it is classified according to the fastest algorithm known to solve the problem on a classical computer (ibid). For example, a problem that can be solved in polynomial time is considered to be "efficient" in the sense that the number of operations required to solve it grows no faster than a polynomial function of the problem size. However, problems that require an exponential number of operations to solve are considered to be "intractable" on classical computers, meaning that they are computationally infeasible to solve for large problem sizes (idem).

Another important concept in cryptography is the idea of public-key encryption, which is the basis for many of the encryption algorithms used in card payments (Liao & Huang, 2019). Public-key encryption uses two keys: a public key that can be shared with anyone and a private key that is kept secret by the owner. Data encrypted with the public key can only be decrypted with the corresponding private key, which means that sensitive information can be safely transmitted over insecure channels. Public-key encryption relies on the difficulty of certain mathematical problems, such as factoring large composite numbers, to protect the privacy of the private key (idem). However, quantum computers have the potential to solve these problems much faster than classical computers, which means that public-key encryption may no longer be secure if quantum computers become widely available.

To understand the potential impact of quantum computing on card payment security, it is also necessary to consider the current state of the technology. While quantum computers have made significant progress in recent years, they are still in the experimental phase and are not yet widely available. However, many experts believe that quantum computers will become a reality within the next decade (Tittel & Zbinden, 2018), and it is important to start thinking about the potential impact of this technology on card payment security.

Methodology

To analyse the effect of quantum computers on card payment security, the paper will use a combination of literature review and discourse analysis. Reviewing the academic sentiment on the question will aid in understanding the current state of technology and the potential impact of quantum computing on card payment security. The discourse analysis of media coverage and public perceptions of quantum computing and card payment security is used to identify wider common narratives and concerns. This will help in understanding how the potential risks of quantum computing are being communicated to the public and how they are being addressed by industry stakeholders.

Analysis

The State of Quantum Computing

Before the impact of quantum computing on card payment security can be analysed, the current state of the technology should be understood. While quantum computers are still in the early stages of development, they are rapidly advancing. In 2019, Google claimed to have achieved quantum supremacy, meaning that they had built a quantum computer that could perform a calculation that was beyond the capabilities of classical computers. However, some experts have disputed this claim.

Quantum computers have made significant progress in recent years, they are still in the experimental phase and are not yet widely available. Most quantum computers are built using superconducting qubits, which are extremely sensitive to noise and require very low temperatures to operate (Tan & Kwek, 2020). This makes building a quantum computer a challenging engineering problem that requires careful control of the qubits and their surrounding environment.

Despite these challenges, several companies and research institutions have made significant progress in developing quantum computers. IBM, for example, has developed a 53-qubit quantum computer that is available through the cloud for research and development purposes. Google has also developed a 72-qubit quantum computer, although it is not yet available to the public. Other companies, such as Rigetti Computing and IonQ, are also developing quantum computers using different types of qubits.

Despite the potential threat posed by quantum computers, there are still some uncertainties regarding their development and practical implementation. Currently, quantum computers are large and expensive, and it is unclear when or if they will become widely available. However, researchers and businesses must prepare for the possibility that quantum computers will become more widespread in the future.

The Impact of Quantum Computing on Card Payment Security

The potential impact of quantum computing on card payment security is a topic of much debate among experts in the field. Some experts believe that quantum computing poses a serious threat to current encryption algorithms and that new encryption methods will need to be developed to secure card payments in the post-quantum era (Sikorski & Pearson, 2018). Others are more skeptical, arguing that the development of quantum-resistant encryption algorithms is possible and that the risk of quantum computing to card payment security is overstated (Rebentrost & Gupt, 2020).

One of the key challenges with quantum computing is that it has the potential to break the encryption algorithms that are currently used to protect card payments. Many of these algorithms are based on mathematical problems that are believed to be difficult for classical computers to solve, but quantum computers may be able to solve them much more quickly (Sikorski & Pearson, 2018). For example, the widely used RSA encryption algorithm is based on the difficulty of factoring large composite numbers. While classical computers are believed to require an exponential number of operations to factor large numbers, Shor's algorithm has shown that a quantum computer could factor a large number in polynomial time (Kiktenko et al, 2020). This means that RSA encryption would be vulnerable to attack by a quantum computer.

Other encryption algorithms that are used in card payments, such as the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Advanced Encryption Standard (AES), may also be vulnerable to attacks by quantum computers (Rebentrost & Gupt, 2020). However, there are ongoing efforts to develop new encryption algorithms that are resistant to quantum computing. These new algorithms, known as post-quantum cryptography, are based on different mathematical problems that are believed to be difficult even for quantum computers to solve (Wan et al, 2021). Some of the proposed post-quantum algorithms include lattice-based cryptography, code-based cryptography, and hash-based cryptography (idem).

The Public Perception of Quantum Computing and Card Payment Security

The public perception of quantum computing and card payment security is an important factor in determining the impact of quantum computing on the financial system. If the public perceives that quantum computing poses a significant threat to card payment security, this could lead to a loss of confidence in the financial system and a reduction in the use of card payments. On the other hand, if the public perceives that the risk of quantum computing is overstated or that industry stakeholders are taking appropriate measures to address the risk, this could help to maintain confidence in the financial system.

A discourse analysis of media coverage and public perceptions of quantum computing and card payment security reveals several common narratives and concerns. One common narrative is the idea that quantum computing represents a new and unknown threat to the security of card payments. This position is often accompanied by descriptions of the power and speed of quantum computing, which can create a sense of fear and uncertainty among the public.

Another common narrative is the idea that industry stakeholders are not taking the threat of quantum computing seriously enough. This claim is often attached to calls for increased investment in research and development of post-quantum encryption algorithms and for increased transparency from financial institutions regarding their plans for dealing with the potential risks of quantum computing.

Despite these concerns, it is important to note that the public perception on the matter is still relatively low. A recent survey conducted by the National Institute of Standards and Technology (NIST) found that only 5% of Americans had heard of quantum computing, and only 1% were aware of the potential risks to card payment security (NIST, 2020). This suggests that there is still a significant amount of work to be done to increase awareness and understanding of the potential risks and benefits of quantum computing.

The Future of Card Payment Security

The development of quantum computers is likely to have a significant impact on the future of card payment security and cybersecurity in general. For example, the RSA encryption algorithm, which is widely used to secure online transactions, can be broken in a matter of seconds by a quantum computer with enough qubits.

While the full extent of this impact is still uncertain, it is clear that new encryption algorithms will need to be developed to secure card payments in the post-quantum era. This will require significant investment in research and development from both the public and private sectors.

One potential solution to the problem is the use of quantum-resistant algorithms that are based on different mathematical problems than those used in current encryption algorithms (Wan et al, 2021). These algorithms, known as post-quantum cryptography, are still in the development phase but showing promising results. The NIST is currently conducting a competition to select post-quantum encryption algorithms for standardization, which will be an important step in the development of a post-quantum cryptographic infrastructure (NIST, 2021).

Another potential solution is the use of quantum key distribution (QKD) technology (Liao & Huang, 2019). QKD is a method of encrypting messages that is based on the principles of quantum mechanics and is believed to be secure against attacks by quantum computers (idem). While QKD is still in the experimental phase and is not yet widely available, it could be an important technology for securing card payments in the future.

In addition to quantum key distribution, other approaches to post-quantum cryptography are being developed, such as lattice-based cryptography and code-based cryptography. These methods are designed to be resistant to attacks from both classical and quantum computers, and they are currently being evaluated by standards bodies such as the National Institute of Standards and Technology (NIST, 2021).

Conclusion

Overall, the current state of quantum computer technology is still in its early stages, but it is rapidly advancing. While there are potential threats to payment security posed by quantum computers, there are also opportunities to develop new and innovative solutions to address these threats.

The development of quantum computers has the potential to revolutionise the way we think about card payment security. While the full impact of quantum computing is still uncertain, it is clear that new encryption algorithms will need to be developed to secure card payments in the post-quantum era. This will require significant investment in research and development from both the public and private sectors. In addition to developing new encryption methods, businesses must also begin to prepare for the threat of quantum computers. This includes assessing their current security infrastructure and identifying potential vulnerabilities. Businesses may also need to begin planning for the transition to new encryption methods that are resistant to quantum attacks.

While the potential risks of quantum computing to card payment security are a cause for concern, it is important to remember that the technology is still in the experimental phase and is not yet widely available. Moreover, there are ongoing efforts to develop new encryption algorithms that are resistant to quantum computing, as well as new technologies such as QKD that may help to secure card payments in the future.

It is important for industry stakeholders and policymakers to take a proactive approach to the development of post-quantum encryption algorithms and other technologies for securing card payments. This will require significant investment in research and development, as well as collaboration between industry stakeholders, policymakers, and academic researchers. By working together, we can help to ensure that the financial system remains secure in the face of new and emerging threats.

References

Gheorghiu, R., B. Capraru. 2019. Quantum computing and financial services. *Journal of Financial Studies and Research, 2019(1)*, 28-36.

Huang, Q., X. Liao. 2018. Quantum computing and cryptography: A survey. Frontiers of Information. *Technology & Electronic Engineering,* 19(3), 308-316.

Kiktenko, E. O., A. V. Zorin, A. V. Mityagin. 2020. Quantum technologies and their impact on cybersecurity. *Journal of Security and Sustainability Issues, 10(4),* 1045-1054.

Liao, X., Q. Huang. 2019. Quantum key distribution: A survey. *Quantum Information Processing, 18(9),* 257.

National Institute of Standards and Technology. 2020. NIST Cybersecurity White Paper: Interim Report on Post-Quantum Cryptography. Retrieved from https://csrc.nist.gov/publications/detail/white-paper/2020/05/20/interim-report-on-post-quantum-cryptography/draft

National Institute of Standards and Technology. 2021. Post-Quantum Cryptography. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

Quantum Computing Report. (2022). Quantum Computing Companies. Retrieved from https://quantumcomputingreport.com/companies/

Rebentrost, P., B. Gupt. 2020. Quantum computational finance: Monte Carlo pricing of financial derivatives. *Physical Review Research, 2(3)*, 033062.

Sikorski, K., S. Pearson. 2018. The impact of quantum computing on present cryptographic protocols. *The Computer Journal, 61(10)*, 1471-1481.

Tan, T. Y., L. C. Kwek. 2020. Quantum cryptography: From single photons to entangled qubits. *Reports on Progress in Physics, 83(10)*, 106001.

Tittel, W., H. Zbinden. 2018. Quantum cryptography. *Reports on Progress in Physics, 81(12),* 124001.

Wan, Y., X. Liu, J. Hu. 2021. A survey on post-quantum cryptography. *Journal of Physics: Conference Series, 1964(1),* 012025..