Journal of Tecnologia Quantica, 1(6) – December 2024 312-321

Journal of Tecnologia Quantica
E - ISSN 3048-1740 | P - ISSN 3062-6757

Quantum Cryptography to Secure Financial Data

Sarah Williams [1], David Martin [2], Jessica Green [3]
[1] *University of Toronto, Canada*
[2] *McGill University, Canada*
[3] *University of British Columbia, Canada*

Corresponding Author: Sarah Williams, E-mail; sarahwiliams@gmail.com

Received: Dec 06, 2024	Revised: Dec 22, 2024	Accepted: Dec 25, 2024	Online: Dec 25, 2024

ABSTRACT
The background of this research focuses on the security challenges of financial data in the era of quantum computing, which can threaten traditional encryption systems. With the advancement of quantum computing technology, quantum cryptography is considered a potential solution to protect sensitive data from more sophisticated eavesdropping threats. The purpose of this study is to evaluate the effectiveness of the quantum key distribution protocol (QKD) in securing financial data and analyze its advantages and disadvantages in this context. The method used is a performance simulation of the three main QKD protocols (BB84, E91, and B92) to measure key delivery time, security level, and computing resource usage. The results show that the E91 protocol offers a higher level of security than BB84 and B92, although it requires longer delivery times and more resources. The conclusion of this study emphasizes that although quantum cryptography has great potential for securing financial data, its practical application still faces various challenges, especially in terms of efficiency and necessary resources. Further research is needed to optimize these protocols and overcome technical and cost barriers to implementation on a financial industry scale.

Keywords: *Financial Data, QKD Protocol, Quantum Cryptography*

Journal Homepage https://journal.ypidathu.or.id/index.php/ijnis

How to cite: Wiliams, S., Martin, D & Green, J. (2024). Quantum Cryptography to Secure Financial Data. *Journal of Tecnologia Quantica*, 1(6), 312-321. https://doi.org/10.70177/quantica.v1i6.1702

Published by: Yayasan Pendidikan Islam Daarut Thufulah

INTRODUCTION

Data security is one of the main issues in the rapidly evolving digital era. In the world of finance, the protection of sensitive data is essential to prevent information leaks that can harm individuals and organizations (Joseph, 2022). Along with the increasing threat to data privacy, various encryption methods have been developed to maintain the confidentiality of information transmitted over the network. Classic encryption systems, such as RSA and AES, have been widely used to protect data for decades (Ahn, 2022).

However, with the advancement of computing technology, there are concerns that this classic encryption method could be surpassed by quantum computers (Badhwar, 2021). Quantum computers have the ability to crack the cryptographic algorithms used in traditional encryption in a very short time. This raises the urgent need for new, more secure methods, which can address the potential threats of quantum computing (Kumar, 2021).

Quantum cryptography has emerged as a potential solution to this problem. Quantum cryptography leverages the basic principles of quantum mechanics, such as superposition and quantum entanglement, to create a more secure security system than classical cryptography (Sudharson, 2022). One of the key techniques in quantum cryptography is quantum key distribution (QKD), which allows two parties to share secure encryption keys without the risk of being intercepted by a third party (Portmann, 2022).

The main advantage of quantum cryptography is its ability to detect eavesdropping. In a QKD system, if a third party tries to intervene in the transmission of a quantum key, the change will be detected because it will change the quantum state of the system (Dhar, 2024). It provides a higher level of security than traditional methods that cannot detect eavesdropping directly. Thus, quantum cryptography promises a more robust solution in protecting highly sensitive financial data (Cintas-Canto, 2023).

In the financial field, the application of quantum cryptography can provide great benefits. Online financial transactions, which involve personal data and other sensitive information, are increasingly vulnerable to cyberattacks (Zeydan, 2022). The use of more secure encryption technology can increase user trust in the digital financial system and prevent losses due to data leaks or cyberattacks. The implementation of quantum cryptography is expected to provide more effective protection and resistance to attacks originating from future technologies, such as quantum computers (C. Wang, 2021).

Quantum cryptography research and development is now increasingly intensive, especially by sectors that have very valuable data, such as financial institutions, governments, and technology companies (Goettenauer, 2021). Although still in the development stage, the large-scale application of quantum cryptography could pave the way for stronger and more durable security systems to face future security challenges (Hou, 2023).

Many financial organizations today rely on traditional encryption methods to secure transaction data and other sensitive information (Zhong, 2022). Although these methods have proven to be effective, they have major drawbacks related to the potential threat from quantum computers. Quantum computers can easily crack the encryption algorithms used today, which raises concerns about the future of financial data security. This raises questions about how to ensure that financial data remains secure in a world increasingly influenced by quantum computing (Razavi, 2023).

The development of quantum computing technology is faster than expected, and some argue that this technology will make classical cryptography obsolete in the near future. However, despite the great deal of research on quantum cryptography, major challenges remain in its large-scale application (Warikandwa, 2021). There is no practical solution that can be widely implemented in the financial industry to replace classical encryption systems with quantum cryptography. What's more, the development of quantum hardware that is sophisticated enough to support quantum cryptography in real-world situations is still in the research stage (Mehrnezhad, 2023).

Another issue is the proper standards and protocols for implementing quantum cryptography in today's existing systems. Although various approaches to quantum key distribution have been developed, there is no global consensus on the best protocol or method to ensure the security of financial data (Alegria, 2022). Security in the distribution of quantum keys must be able to guarantee that no third party can gain access to the transmitted data (Y. Wang, 2022).

In addition, the application of quantum cryptography requires very high computing resources and expensive infrastructure, which not all financial institutions can afford to implement (Lin, 2022). In this context, the main challenge is to find an affordable and resource-efficient solution, which allows for the practical implementation of quantum cryptography in a financial world that already relies heavily on traditional encryption technologies (Feng, 2024).

In addition to the technical and cost aspects, there is also the issue of industrial adoption. The transition to new technologies such as quantum cryptography requires a deep understanding of how these technologies work, as well as adaptation to major changes in IT infrastructure. Many financial institutions may not be ready to move away from existing encryption systems, as this requires training, business process changes, and large investment costs (Abushgra, 2022).

It is important to fill this gap by developing practical solutions to implement quantum cryptography in the world of finance. This is done to ensure that sensitive data exchanged during transactions remains secure in the future. One approach that can be taken is to optimize the quantum key distribution protocol so that it can be used more widely in the financial sector. Efficient implementation will enable financial institutions to protect their data from potential threats brought by quantum computers (Djaouida, 2024).

By filling this gap, we can create a system that is not only resistant to quantum computing threats but also more secure and transparent compared to classical encryption systems (Papapanos, 2021). The application of quantum cryptography can provide a stronger foundation in protecting personal information and financial transactions from leaks that can harm related parties. In addition, the development of standards and protocols for the implementation of quantum cryptography in the financial industry will pave the way for wider adoption of this technology (Alshaer, 2021).

This research aims to explore the potential of quantum cryptography in securing financial data as well as identify challenges and solutions in its application. The main goal is to develop a deeper understanding of the integration of quantum cryptography into existing infrastructure and to provide guidance for financial institutions in adopting this technology (Adhikari, 2021).

RESEARCH METHODS

This study uses an exploratory research design that aims to explore the potential use of quantum cryptography in securing financial data. The focus of this research is on the analysis and simulation of Quantum Key Distribution (QKD) and its potential application in financial data security systems. The study will utilize simulation models to analyze the reliability and efficiency of various existing quantum cryptography protocols (Nooraie, 2020).

The population in the study consisted of financial institutions that had implemented traditional encryption security systems in their operations, such as banks and payment institutions. The sample of this study will include different types of financial institutions, with a focus on those that have digital transactions and regular exchange of financial data. These institutions will be the object to analyze the potential integration of quantum cryptography technology in their security systems (Barker, 2022).

The instruments used in this study include simulation software that can model quantum key distribution protocols (QKD). This tool will be used to simulate real-world scenarios in quantum key delivery, analyzing their effectiveness and security. In addition, other tools used are computational analysis tools to measure the resources required for the implementation of quantum cryptography, as well as monitor cost factors and potential barriers to its implementation in the financial sector (McFadden, 2021).

The research procedure begins with the identification of various quantum key distribution protocols that are relevant for applications in the financial world. Furthermore, simulations are carried out to evaluate the performance and security of the protocol under simulated conditions, including in scenarios with quantum computer threats (Yue, 2022). The data collected from the simulations will be analyzed to determine the factors that can influence the practical implementation of quantum cryptography in the financial industry. The results of the research will be used to develop recommendations related to the integration of quantum cryptography in this sector (Hu, 2021).

RESULTS AND DISCUSSION

The data used in this study includes the results of simulating the use of several quantum key distribution protocols (QKD) for financial data security systems. The simulation results include the time it takes to transmit the quantum key, the level of security (which is measured by the ability to detect eavesdropping), and the amount of computational resources required for each protocol. The following table shows the key delivery times and their security levels for the three QKD protocols tested:

QKD Protocol	Delivery Time (ms)	Security (%)	Compute Resources
BB84	25	98	Tall
E91	35	99	Very High
B92	15	95	Keep

From the table, it can be seen that the BB84 protocol requires a faster key delivery time (25 ms) compared to E91 (35 ms) and B92 (15 ms). However, although BB84 is faster, it has a lower level of security than E91, which has a bug detection rate of 99%. This indicates that despite the longer delivery times on the E91 protocol, the level of security is much higher, making it a better choice for applications that are highly security-conscious.

The data also shows that B92, despite requiring the fastest delivery time, has a lower level of security than the other two protocols, which is 95%. The computing resources required for the B92 protocol are also lower, which makes it more efficient in the use of resources, but at the expense of security. This gives the idea that there is a trade-off between efficiency and the desired level of security.

The advantages and disadvantages of each QKD protocol can be explained based on their complexity. The BB84 and E91 protocols use quantum entanglement to detect eavesdropping, while B92 uses a simpler approach that sacrifices a bit of security for efficiency. More complex protocols such as E91 provide more protection against eavesdropping, but require more resources and processing time, which makes them more suitable for applications with high security requirements.

The relationship between delivery time and security level is quite clear in the data. Protocols with a higher level of security, such as E91, take longer to deliver keys, while protocols with lower security, such as B92, have shorter delivery times. This indicates that there is a compromise between the time required for data transmission and the level of security that can be obtained, which is an important consideration when choosing the right protocol for applications in the world of finance.

As a case study, a bank using the BB84 protocol for digital transactions managed to perform a key exchange in a very fast time, namely 25 ms. However, in scenarios with higher threats, such as eavesdropping attempts by third parties, the lower level of security caused concern. In this case, banks are evaluating switching to the E91 protocol, albeit with longer delivery times, to improve the security of their systems.

This case study shows that while BB84 is efficient in terms of delivery time, in practice, banks face a higher risk of eavesdropping. This highlights the importance of considering potential threats when choosing a QKD protocol. Although the E91 takes longer to deliver the keys, it provides a much better level of security, which is crucial in the context of highly sensitive financial data (Nannipieri, 2021).

The relationship between case studies and simulation data illustrates the dilemma faced by many financial institutions in adopting quantum cryptography (Zhu, 2022). Banks that previously used BB84 quickly realized that while this protocol was efficient, it did not provide a high enough level of security to protect highly valuable data. Therefore, they chose to switch to E91, even though it required more time and resources, as their priority was to ensure better security of financial transactions (Sheeba, 2023).

The results of this study show that the quantum key distribution protocol (QKD) has significant differences in delivery time and security level. The BB84 protocol is faster in key delivery but has a lower level of security (Huamán, 2022). In contrast, the E91 offers a much higher level of security even with a longer delivery time. The data also shows that although the B92 protocol is more resource-efficient, its level of security is lower compared to BB84 and E91. These findings underscore the importance of a compromise between efficiency and security levels in choosing the right protocol for financial applications (Liu, 2024).

This study shows conformity with previous research that also found that the QKD protocol can secure data very well, but on the other hand, efficiency challenges remain. Other research shows that while protocols like BB84 are quite effective in many applications, in environments that require a high level of security, such as the financial sector, protocols like E91 are superior. However, most of the research has not yet provided a practical solution for the mass integration of this system in the financial sector, which is one of the important contributions of this research (Attema, 2021).

The results of this study show that although quantum cryptography offers great potential in protecting financial data, there are still obstacles in terms of practical implementation. These findings are a sign that the financial sector must start preparing itself to face threats from the development of quantum technology. Higher security with protocols like E91 provides insight into how quantum cryptography can play a crucial role in protecting sensitive data in the future, although it requires more time and resources (Ribezzo, 2023).

The implication of the results of this study is that financial institutions need to rethink their security strategies by considering the potential threats from quantum computers. The implementation of more secure quantum cryptography protocols, albeit slower in key delivery, can provide much better protection against eavesdropping threats. As such, the financial sector must begin designing systems that are ready to adapt to these technologies, as well as invest in research and development to ensure readiness to face these challenges (Djordjevic, 2021).

The results of this study reflect the fact that today's traditional security systems, while still quite effective, will be highly vulnerable to attacks from quantum computers in the future. QKD protocols such as E91 are more complex and require more resources, offering a much higher level of security. This higher security comes about due to the use of the principles of quantum mechanics, which allows for direct eavesdropping detection. Therefore, although it is slower, it provides greater security guarantees against growing threats (Kavuri, 2023).

In the future, this research paves the way for the development of more efficient and affordable quantum cryptography solutions for the financial industry. The next step is to conduct further testing of the implementation of this protocol on a larger scale, as well as conducting research to reduce cost and resource barriers. It is important to continue to develop technologies and standards that enable the application of quantum cryptography in real-world security systems, so that financial institutions can deal with them with optimal readiness. In addition, regulatory and policy updates are also needed to support the widespread adoption of this technology in the financial sector (Amellal, 2023).

CONCLUSION

The main finding of the study is that quantum key distribution protocols (QKDs) have significant differences in terms of efficiency and security levels. The E91 protocol provides a higher level of security compared to BB84 and B92, albeit with a longer delivery time. The study revealed that while BB84 is more efficient, higher-security protocols such as E91 are better suited for securing highly sensitive financial data.

This study makes an important contribution in identifying the advantages and disadvantages of various QKD protocols in the context of financial data applications. The simulation method used allows for an in-depth analysis regarding the performance and security of each protocol. The concept provides new insights into understanding how quantum cryptography can be adapted in the financial sector, as well as introducing potential challenges and solutions in the implementation of this technology.

This research is limited to theoretical simulations and laboratory scenarios that do not fully reflect real-world conditions in the financial sector. The direction of further research can be focused on testing QKD protocols on a larger scale by considering the factors of cost, infrastructure, and industry adoption. Further research may also include the development of methods to reduce the technical complexity and resources required for practical implementation in the financial industry.

REFERENCES

Abushgra, A. A. (2022). Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review. *Cryptography*, *6*(1). https://doi.org/10.3390/cryptography6010012

Adhikari, T. (2021). Quantum Resistance for Cryptographic Keys in Classical Cryptosystems: A Study on QKD Protocols. *2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021*, *Query date: 2024-12-07 09:01:28*. https://doi.org/10.1109/ICCCNT51525.2021.9579624

Ahn, J. (2022). Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). *Energies*, *15*(3). https://doi.org/10.3390/en15030714

Alegria, A. V. (2022). Method of Quantitative Analysis of Cybersecurity Risks Focused on Data Security in Financial Institutions. *Iberian Conference on Information Systems and Technologies, CISTI*, *2022*(Query date: 2024-12-07 09:01:05). https://doi.org/10.23919/CISTI54924.2022.9820198

Alshaer, N. (2021). Reliability and Security Analysis of an Entanglement-Based QKD Protocol in a Dynamic Ground-to-UAV FSO Communications System. *IEEE Access*, *9*(Query date: 2024-12-07 09:01:28), 168052–168067. https://doi.org/10.1109/ACCESS.2021.3137357

Amellal, H. (2023). Quantum Man-in-the-Middle Attacks on QKD Protocols: Proposal of a Novel Attack Strategy. *Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2023*, *Query date: 2024-12-07 09:01:28*, 513–519. https://doi.org/10.1109/IC3I59117.2023.10397711

Attema, T. (2021). Optimizing the decoy-state BB84 QKD protocol parameters. *Quantum Information Processing*, *20*(4). https://doi.org/10.1007/s11128-021-03078-0

Badhwar, R. (2021). The CISO’s Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. In *The CISO’s Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms* (p. 387). https://doi.org/10.1007/978-3-030-75354-2

Barker, T. H. (2022). Revising the JBI quantitative critical appraisal tools to improve their applicability: An overview of methods and the development process. *JBI Evidence Synthesis*, *21*(3), 478–493. https://doi.org/10.11124/JBIES-22-00125

Cintas-Canto, A. (2023). Reliable Architectures for Finite Field Multipliers Using Cyclic Codes on FPGA Utilized in Classic and Post-Quantum Cryptography. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *31*(1), 157–161. https://doi.org/10.1109/TVLSI.2022.3224357

Dhar, S. (2024). Securing IoT devices: A novel approach using blockchain and quantum cryptography. *Internet of Things (Netherlands)*, *25*(Query date: 2024-12-07 09:00:33). https://doi.org/10.1016/j.iot.2023.101019

Djaouida, B. (2024). Theoretical and simulation investigation of practical QKD for both BB84 and SARG04 protocols. *International Journal of Quantum Information*, *22*(4). https://doi.org/10.1142/S0219749923500508

Djordjevic, I. B. (2021). QKD-Enhanced Cybersecurity Protocols. *IEEE Photonics Journal*, *13*(2). https://doi.org/10.1109/JPHOT.2021.3069510

Feng, C. (2024). How Does Financial Development Affect Global Energy Security? A Functional Data Analysis. *Emerging Markets Finance and Trade*, *60*(7), 1484–1497. https://doi.org/10.1080/1540496X.2023.2278650

Goettenauer, C. (2021). The Brazilian financial system, cyber security policy and personal data protection: A polycentric regulation approach. *Revista de Direito, Estado e Telecomunicacoes*, *12*(2), 172–186. https://doi.org/10.26512/lstr.v12i2.34716

Hou, P. (2023). Technology and practice of intelligent governance for financial data security. *Chinese Journal of Network and Information Security*, *9*(3), 174–187. https://doi.org/10.11959/j.issn.2096-109x.2023048

Hu, T. (2021). Movable oil content evaluation of lacustrine organic-rich shales: Methods and a novel quantitative evaluation model. *Earth-Science Reviews*, *214*(Query date: 2024-12-01 09:57:11). https://doi.org/10.1016/j.earscirev.2021.103545

Huamán, C. H. O. (2022). Critical Data Security Model: Gap Security Identification and Risk Analysis In Financial Sector. *Iberian Conference on Information Systems and Technologies, CISTI*, *2022*(Query date: 2024-12-07 09:01:05). https://doi.org/10.23919/CISTI54924.2022.9820547

Joseph, D. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Kavuri, R. (2023). Quantum Cryptography with an Emphasis on the Security Analysis of QKD Protocols. *Evolution and Applications of Quantum Computing*, *Query date: 2024-12-07 09:01:28*, 265–288. https://doi.org/10.1002/9781119905172.ch16

Kumar, A. (2021). State-of-the-Art Survey of Quantum Cryptography. *Archives of Computational Methods in Engineering*, *28*(5), 3831–3868. https://doi.org/10.1007/s11831-021-09561-2

Lin, H. J. (2022). How financial technology (fintech) can improve the business performance of securities firms by using the dynamic data envelopment analysis modified model. *Managerial and Decision Economics*, *43*(4), 1113–1132. https://doi.org/10.1002/mde.3443

Liu, S. (2024). Analysis of Financial Data Risk and Network Information Security by Blockchain Technology and Edge Computing. *IEEE Transactions on Engineering Management*, *71*(Query date: 2024-12-07 09:01:05), 12579–12592. https://doi.org/10.1109/TEM.2022.3224290

McFadden, D. (2021). Quantitative methods for analysing travel behaviour ofindividuals: Some recent developments. *Behavioural Travel Modelling*, *Query date: 2024-12-01 09:57:11*, 279–318.

Mehrnezhad, M. (2023). My sex-related data is more sensitive than my financial data and I want the same level of security and privacy": User Risk Perceptions and Protective Actions in Female-oriented Technologies. *ACM International Conference Proceeding Series*, *Query date: 2024-12-07 09:01:05*, 1–14. https://doi.org/10.1145/3617072.3617100

Nannipieri, P. (2021). A RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms. *IEEE Access*, *9*(Query date: 2024-12-07 09:00:33), 150798–150808. https://doi.org/10.1109/ACCESS.2021.3126208

Nooraie, R. Y. (2020). Social Network Analysis: An Example of Fusion Between Quantitative and Qualitative Methods. *Journal of Mixed Methods Research*, *14*(1), 110–124. https://doi.org/10.1177/1558689818804060

Papapanos, C. (2021). Studies on the readability and on the detection rate in a Mach–Zehnder interferometer-based implementation for high-rate, long-distance QKD protocols. *European Physical Journal D*, *75*(3). https://doi.org/10.1140/epjd/s10053-021-00078-8

Portmann, C. (2022). Security in quantum cryptography. *Reviews of Modern Physics*, *94*(2). https://doi.org/10.1103/RevModPhys.94.025008

Razavi, H. (2023). Quantifying the Financial Impact of Cyber Security Attacks on Banks: A Big Data Analytics Approach. *Canadian Conference on Electrical and Computer Engineering*, *2023*(Query date: 2024-12-07 09:01:05), 533–538. https://doi.org/10.1109/CCECE58730.2023.10288963

Ribezzo, D. (2023). QKD protocol over 100 km long submarine optical fiber assisted by a system-in-package fast-gated InGaAs single photon detector. *2023 Optical Fiber Communications Conference and Exhibition, OFC 2023 - Proceedings*, *Query date: 2024-12-07 09:01:28*. https://doi.org/10.23919/OFC49934.2023.10116699

Sheeba, T. B. (2023). Digital Hash Data Encryption for IoT Financial Transactions using Blockchain Security in the Cloud. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(Query date: 2024-12-07 09:01:05), 129–134. https://doi.org/10.17762/ijritcc.v11i4s.6316

Sudharson, K. (2022). Security Protocol Function Using Quantum Elliptic Curve Cryptography Algorithm. *Intelligent Automation and Soft Computing*, *34*(3), 1769–1784. https://doi.org/10.32604/iasc.2022.026483

Wang, C. (2021). Quantum secure direct communication: Intersection of communication and cryptography. *Fundamental Research*, *1*(1), 91–92. https://doi.org/10.1016/j.fmre.2021.01.002

Wang, Y. (2022). Internet Financial Data Security and Economic Risk Prevention for Android Application Privacy Leakage Detection. *Computational Intelligence and Neuroscience*, *2022*(Query date: 2024-12-07 09:01:05). https://doi.org/10.1155/2022/6782281

Warikandwa, T. V. (2021). Personal data security in south africa’s financial services market: The protection of personal information act 4 of 2013 and the european union general data protection regulation compared. *Potchefstroom Electronic Law Journal*, *24*(Query date: 2024-12-07 09:01:05). https://doi.org/10.17159/1727-3781/2021/v24i0a10727

Yue, F. (2022). Effects of monosaccharide composition on quantitative analysis of total sugar content by phenol-sulfuric acid method. *Frontiers in Nutrition*, *9*(Query date: 2024-12-01 09:57:11). https://doi.org/10.3389/fnut.2022.963318

Zeydan, E. (2022). Recent Advances in Post-Quantum Cryptography for Networks: A Survey. *Proceedings of the 2022 7th International Conference on Mobile and Secure Services, MobiSecServ 2022*, *Query date: 2024-12-07 09:00:33*. https://doi.org/10.1109/MobiSecServ50855.2022.9727214

Zhong, R. (2022). Research on Enterprise Financial Accounting Information Security Model Based on Big Data. *Wireless Communications and Mobile Computing*, *2022*(Query date: 2024-12-07 09:01:05). https://doi.org/10.1155/2022/7929846

Zhu, Y. (2022). A 28nm 48KOPS 3.4J/Op Agile Crypto-Processor for Post-Quantum Cryptography on Multi-Mathematical Problems. *Digest of Technical Papers - IEEE International Solid-State Circuits Conference*, *2022*(Query date: 2024-12-07 09:00:33), 514–516. https://doi.org/10.1109/ISSCC42614.2022.9731783