Mathematical Modelling and Adaptation Strategies in the Confrontation between Cryptocurrencies and Quantum Computers*

Valeriy Lakhno[1,*,†], Alona Desiatko[2,†], Vitaliy Chubaievskyi[2,†], Andrii Roskladka[2,†] and Serhii Kaminskyi[2,†]

[1] National University of Life and Environmental Sciences of Ukraine, 19/1 Horikhuvatskyi shliakh str., 03041 Kyiv, Ukraine
[2] State University of Trade and Economics, 19 Kyoto str., 02156 Kyiv, Ukraine

Abstract

The research is devoted to analyzing the stability of cryptocurrency systems under threats associated with the development of quantum computing. The paper proposes a differential game model to formalize the interaction between cryptocurrency systems and quantum computers (QCs). The methodology uses differential game theory to model the dynamics of the parties' resource allocation and evaluate their player strategies. During the modeling process, scenarios of confrontation between cryptocurrency technologies and quantum computing were analyzed to identify key patterns and factors affecting the effectiveness of cryptographic protection and the computational capabilities of attackers. The results obtained may become the basis for the development of new cryptographic security standards and the formation of adaptive strategies for the protection of digital assets in the context of the growing capabilities of quantum computing and quantum computers.

Keywords

quantum computing, cryptocurrencies, cryptographic stability, post-quantum cryptography, Shor's algorithm, differential games, mathematical modeling, allocation resources, quantum threats, adaptive protection strategies

1. Introduction

Modern challenges in the field of information security (referred to as IS), associated with the development of quantum computing, threaten the stability of cryptographic methods that underlie most digital systems, including cryptocurrencies [1]. Cryptocurrencies (referred to as CCs), according to [2] may become particularly vulnerable in the face of the emergence of quantum computers (referred to as QCs) capable of performing computations inaccessible to traditional systems. The main problem is that quantum algorithms, such as Shor's algorithm [3, 4], can efficiently solve problems on which asymmetric cryptographic schemes are based, such as factorization of integers and calculation of discrete logarithms, which potentially will allow attackers to use quantum computing power to bypass cryptographic protections and gain access to confidential information or digital assets. With this in mind, research into modeling the interactions between CCs and QCs is relevant as it will predict the dynamics of the confrontation between data protection technologies and threats caused by the development of quantum computing. And, in particular, modeling using differential game theory methods provides a unique tool to analyze the adaptive strategies of the parties, taking into account resource constraints and dynamic changes in system parameters. In such models, the resources of the parties can be classified into several categories, e.g., for CC, these are primarily cryptographic defense methods and tools, including encryption algorithms that are resistant to attacks. This also includes resources

*CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
lva964@nubip.edu.ua (V. Lakhno); desyatko@gmail.com (A. Desiatko); chubaievskyi_vi@knute.edu.ua (V. Chubaievskyi); a.roskladka@knute.edu.ua (A. Roskladka) s.kaminskyj@knute.edu.ua (S. Kaminskyi)
0000-0001-9695-4543 (V. Lakhno); 0000-0003-2860-2188 (A. Desiatko); 0000-0001-8078-2652 (V. Chubaievskyi); 0000-0002-1297-377X (A. Roskladka); 0000-0002-4884-1517 (S. Kaminskyi)

aimed at modernizing cryptographic mechanisms in response to new threats. Correspondingly, for quantum computing, resources include QC computing power, as well as infrastructure and research efforts aimed at developing this technology.

The analysis methodology proposed in this research involves the construction of a mathematical model describing the interaction between the parties, where the CCs and QCs act as players. This model allows us to formalize the resource allocation processes and predict the outcomes of the confrontation, taking into account different scenarios. This approach can open new opportunities for developing adaptation and protection strategies aimed at minimizing the risks associated with quantum threats to CCs.

Thus, based on the above, the study of the problem of the stability of cryptocurrency systems under quantum computing conditions not only has theoretical significance but also has a high practical value, since the results of such an analysis can be subsequently used to develop new standards of cryptographic security, create protocols for the protection of digital assets and form a long-term strategy for adapting cryptocurrency systems to quantum threats.

2. A review of prior research

With the rapid development of quantum computing [5, 6], there is an increasing need to investigate mechanisms to counter the threats associated with the use of QC to attack existing cryptographic systems [7, 8]. Quantum algorithms, such as Shor's algorithm [9] and Grover's algorithm [10], provide significant advantages in solving factorization and search problems, which puts the security of traditional cryptographic algorithms such as RSA, ECC, and AES under threat.

On the other hand, the development of post-quantum algorithms [11] and the modernization of cryptographic systems, as shown in [9–18], provide an active counter to these threats. However, the dynamics of the confrontation between defenses and attacking technologies require careful mathematical modeling to predict the behavior of both sides in different scenarios. Therefore, new research in this direction is relevant.

3. Purpose, object, and subject of the study

The study aims to develop a mathematical model of interaction between cryptocurrency systems and quantum computers based on differential game theory to analyze the dynamics of the parties' resource allocation and to form effective strategies for adapting cryptographic mechanisms to quantum threats.

The object of the study is cryptographic and computing systems interacting in the context of quantum computing development, focusing on cryptocurrency platforms as the most vulnerable to attack by quantum computers.

The subject of the study is the mechanisms of resource allocation between parties (cryptocurrencies and quantum computers) in dynamic interaction, including adaptive strategies for cryptographic security and increasing computing power.

4. Methods and models

4.1. SLAM algorithms

The research methodology is based on applying differential game theory [15–21] to model the interaction between two parties—CC systems and QCs. Differential games, as a section of optimal control theory, allow for the description of dynamic processes, where the strategic behavior of participants is determined by the change of system parameters over time. Using the system of differential equations proposed in this paper to describe the state of resources of the parties provides the possibility of taking into account such factors as the limited resources, their purposeful distribution, and time characteristics of adaptation. Within the framework of the constructed model, CC systems and QCs are considered players pursuing opposite goals. For CCs,

the goal is to maximize the level of protection by applying stable cryptographic algorithms and upgrading security mechanisms. For QCs, the goal is to achieve computing power sufficient to bypass cryptographic barriers successfully.

In this paper, the interaction process between the parties is described by a set of control functions that characterize the expenditure of resources on the corresponding strategies. The dynamics of parameter changes are represented as a system of ordinary differential equations, where each model variable reflects the level of resources of the party (e.g., the level of cryptographic protection, modernization resources of CC, quantum computing power, and infrastructure resources). Numerical analysis and programming techniques are applied to determine the optimal strategies, allowing us to study the system's evolution in different scenarios. The computational experiment results were visualized using cybernetic modeling tools, which allowed us to interpret the obtained dependencies and identify key patterns in the parties' confrontation.

4.2. A differential game model of cryptographic resistance to quantum threats

For a detailed analysis of the players' confrontation, it is necessary to consider the key variables describing the active cryptographic security and quantum computers and their mutual influence.

For cryptocurrencies and quantum computers, let's define variables.

For the CC:

CC Active Means:

- $z_1(t)$ is the effectiveness of the current cryptographic algorithm.
- $z_2(t)$ is resources for modernization (e.g. transition to post-quantum algorithms).

Active means of quantum computers:

- $z_3(t)$ is computing power of a quantum computer.
- $z_4(t)$ is resources to increase computing power.

Active cryptographic defenses characterize the current and potential capabilities of cryptographic defense systems in countering threats, including attacks by quantum computers. Two main aspects describe them. The first is the effectiveness of the current cryptographic algorithm. This variable reflects how resistant the current cryptographic algorithm is to attacks, including those using quantum computing. For example, RSA and ECC (elliptic curve) algorithms resist classical attacks but are vulnerable to attacks using quantum computers, such as Shor's algorithm. The effectiveness can be expressed in bits of cryptographic strength, e.g. 128-bit AES is considered resistant to most attacks, but its strength must be re-evaluated in the face of a quantum threat. If a system uses the 256-bit AES algorithm to encrypt sensitive data, the effectiveness of the algorithm is judged by its ability to prevent attacks in a given time under existing quantum computing power. The second aspect is the resources for modernizing cryptographic algorithms. These resources include the costs (time, computational, financial) to move to more secure cryptographic standards. For example, introducing post-quantum algorithms such as lattice-based cryptography [22] will require significant investments in training [23], hardware upgrades, and software modifications [24–27]. Let us illustrate this with a small example. Say an organization is considering a move to the CRYSTALS-Kyber algorithm [28], certified by NIST as a post-quantum standard, this, consequently, will require the purchase of new hardware encryption modules and updates to communication protocols.

The same reasoning holds true for active QC tools. These variables describe the ability of the attacker (e.g., the QC) to perform the computations required to break existing cryptographic algorithms. Two key aspects can also be distinguished here. The first aspect is the computational power of the QC. This variable reflects the current state of quantum computing, including the number of qubits and their coherence level. Thus, the more qubits and higher their coherence, the greater the capacity to perform complex computations such as factorizing large numbers or searching for collisions in hash functions. For example, Google's quantum computer Sycamore [29], with 53 qubits, achieved "quantum supremacy" in 2019 by solving a problem inaccessible to

classical computers. Accordingly, a QC with 1000 stable qubits can factorize a 2048-bit RSA key in a few hours, which is impossible for a classical computer in a reasonable time. The second aspect is the resources to increase the computing power of the QC. These resources include the costs of developing more powerful QCs, such as funding research, improving cooling techniques to reduce noise, and optimizing quantum algorithms. For example, creating superconductor-based qubits will require significant material and energy costs. The company's investment in creating a new generation of qubits will increase the system's processing power from 256 to 512 qubits, which will lead to a dramatic increase in attack capabilities.

Then, the system of differential equations will look as follows:

$$\begin{aligned} \dot{z}_1 &= -p_{41} z_4 v_1 + c_1, \\ \dot{z}_2 &= -p_{42} z_4 v_2 + c_2, \\ \dot{z}_3 &= -p_{23} z_2 u_1 + c_3, \\ \dot{z}_4 &= -p_{24} z_2 u_2 + c_4, \end{aligned} \tag{1}$$

where p_{ij} is effectiveness of one party's means against the other (for the considered model describes how successfully the resources and strategies of one party (for example, cryptocurrency systems or QC) can counteract the efforts of the opposite party. For QC it can be, for example, the level of resistance of cryptographic algorithms to hacking by quantum computers, which is expressed through the probability of successfully preventing an attack at a given level of computing power of the attacking party. And for QC it is an indicator characterizing the ability of their algorithms and computing power to overcome existing cryptographic defenses).

u_1, u_2, v_1, and v_2 are resource shares (representing the proportions of the total available resources of each party (e.g., CC systems or QCs) allocated to specific tasks or strategies in their interactions. For cryptocurrencies, the proportions of resources may include, inter alia, the particular amount devoted to maintaining current cryptographic mechanisms, such as implementing stronger encryption algorithms, as well as, resources devoted to developing and implementing post-quantum cryptographic standards that will be able to withstand attacks from QCs. For QC, these are resources devoted to increasing computational power, for example, increasing the number of qubits or improving their coherence, as well as the unit cost of optimizing algorithms to accelerate the cracking of cryptographic systems. Note that the total resource shares do not exceed 1 (or 100%) since resources are limited and their allocation between different tasks requires optimization within the individual task);

c_1, c_2, c_3, and c_4 are resource replenishment capabilities (i.e., the parties' ability to increase the available resources needed to fulfill their strategic objectives. These resources may include financial, technical, computational, or human resources that sustain or develop the parties in an adversarial environment. For example, for CCs, resource replenishment capabilities reflect investments in developing new cryptographic algorithms resistant to quantum attacks, particularly post-quantum standards, and infrastructure upgrades to integrate more secure protocols, among others. For QC, replenishment opportunities include the development of quantum technologies, such as increasing the number of qubits or increasing their coherence, as well as funding research to optimize quantum algorithms (e.g. to speed up the Shor algorithm), etc.

Then the win function of the parties can be written as follows.

For cryptocurrencies:

$$J_A = \left[z_1(T) - z_3(T) \right]. \tag{2}$$

The goal of cryptocurrencies (CCs) is to minimize the loss of their cryptocurrencies and maximize the damage done to the QCs' computing facilities.

For quantum computers (QCs):

$$J_B = \left[z_3(T) - z_1(T) \right]. \tag{3}$$

The QC's goal is to maximize the efficiency of its computations and minimize the damage from CC countermeasures.

The model describes a zero-sum differential game, where the dynamic interaction of the parties and the equilibrium are defined through optimal resource allocation strategies. Note that an analytical solution may not be available, so an iterative process will be used to find the equilibrium state, and the construction algorithm can be based on the maximum principle of L. S. Pontryagin [20, 21].

5. Computational experiments

The main objective of the computational experiment (referred to as CE), the results of which are shown in Fig. 1, was to evaluate the dynamic interaction between the parties and answer the question—"How do cryptocurrencies adapt their defenses in response to QC attacks, and how do QCs strengthen their computing power to overcome these defenses?". In addition, the CE should identify the key dependencies and identify which factors, in particular, cryptocurrency modernization resources or QC computing power) have the greatest impact on the outcome of the confrontation.

The experiment involved setting initial values of variables (e.g., initially high level of cryptographic protection $z_1(0)$ and computing power $z_3(0)$. Resource allocation scenarios, i.e., testing different parties' strategies, such as maximizing the concentration of resources on one area, e.g., QC focuses entirely on increasing capacity and CC focuses on upgrading the defense. Also, CE investigated interaction parameters, i.e. considering the effectiveness of one party's means against the other, which allows for assessing the real threat and the degree of countermeasures.

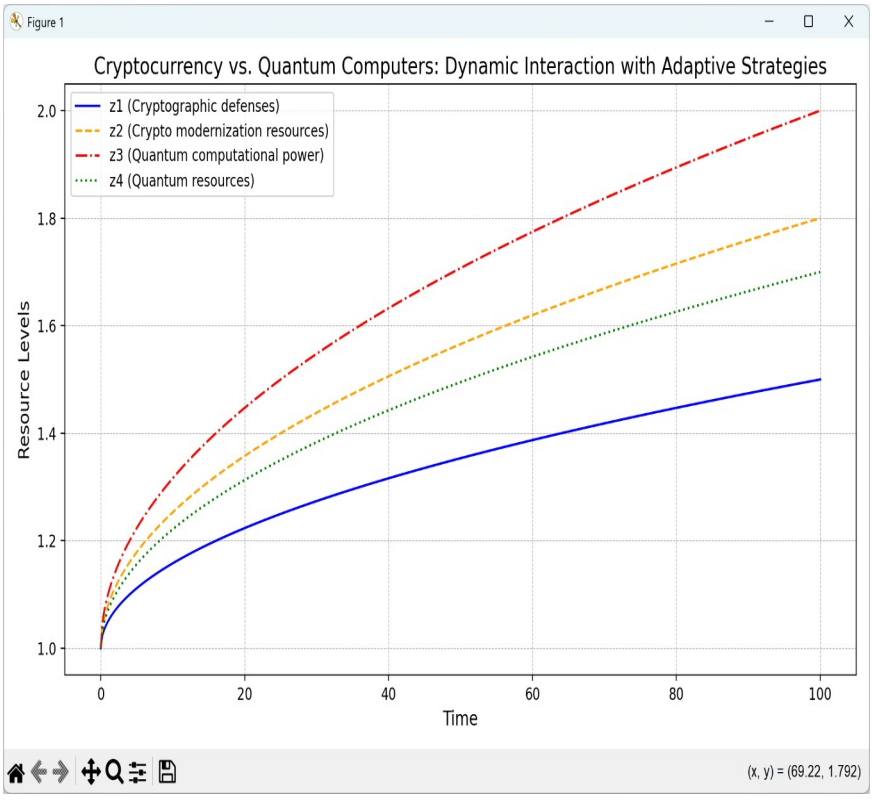

Figure 1: The dynamics of cryptographic and quantum computing resources under confrontation

The results of CE, in general, will provide insight into the dynamics of party interactions, and identify key factors affecting the resilience of cryptocurrency systems, which in future research will enable the development of specific practical recommendations for optimal resource allocation and implementation of adaptive defense strategies in the face of quantum threats to CCs.

6. Discussion of the results obtained in the course of computational experiments

The results of modeling are presented in Fig. 1 in the form of time dependencies of resource levels of the parties involved in the confrontation, i.e. cryptocurrency technologies and quantum computing, respectively. The graphs show changes in four key variables: cryptographic defenses $z_1(t)$, cryptographic modernization resources $z_2(t)$, and the computing power of quantum computers $z_3(t)$ and their resources $z_4(t)$. The graph of cryptographic defenses $z_1(t)$ shows how the level of CC resistance changes under the influence of attacks from quantum computers. At the initial stages of the confrontation, there is a noticeable decrease in the values of $z_1(t)$, which is caused by the active actions of the side of quantum technologies implementing attack strategies with a high level of priority. However, the availability of resources for the modernization of cryptography $z_2(t)$ allows for compensating losses, which leads to stabilization or even growth of $z_1(t)$ in later periods.

The dynamics of $z_2(t)$ modernization resources demonstrate their critical role in the standoff. In the initial stages, there is a gradual decrease of $z_2(t)$ due to the reallocation of resources for the recovery and defense of cryptographic systems. However, the replenishment of resources described in the model allows $z_2(t)$ to be maintained at a level sufficient for an effective counter-strategy.

Changes in the computing power of quantum computers $z_3(t)$ reflect their high initial efficiency, which gradually decreases under the influence of attacks from cryptocurrency technology. This dynamic illustrates the effectiveness of the cryptocurrency side's adaptive strategies aimed at weakening the attacker's capabilities.

The resources of quantum computers $z_4(t)$ are characterized by similar dynamics. Their use for attacking actions leads to gradual depletion, but replenishment of resources allows the parties to maintain activity throughout the simulation period.

The results demonstrate complex interactions between parties with variable degrees of dominance depending on the strategies employed and resource replenishment and confirm that adaptive strategies that depend on the current state of the system can significantly influence the outcome of the confrontation and provide a dynamic equilibrium between the parties.

Conclusions

The study demonstrated that the development of quantum computing poses significant security risks to cryptocurrency systems, as quantum algorithms, such as Shor's algorithm, can effectively circumvent existing cryptographic mechanisms. The differential game model proposed as part of the work showed that the dynamics of the confrontation between cryptocurrencies and quantum computers are determined by the resource allocation strategies of the parties. The key finding is to confirm the effectiveness of adaptive strategies that will minimize the loss of cryptographic stability and slow down the development of the attacking party's computing power. The results obtained in the computational experiments highlight the need to implement post-quantum cryptographic algorithms and infrastructure modernization to improve the resilience of digital systems. In addition, the proposed methodology, based on the development of models built using differential games, can be used to predict long-term scenarios of quantum threats and develop preventive measures.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] D. Virovets, et al., Integration of smart contracts and artificial intelligence using cryptographic oracles, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3829 (2024) 39–46.

[2] A. Osipovich, A looming threat to Bitcoin: The risk of a quantum hack, The Wall Street Journal, 2024. URL: https://www.wsj.com/tech/cybersecurity/a-looming-threat-to-bitcoin-the-risk-of-a-quantum-hack-24637e29

[3] C. H. Ugwuishiwu, et al., An overview of quantum cryptography and Shor's algorithm, Int. J. Adv. Trends Comput. Sci. Eng. 9(5) (2020) 7487–7495. doi:10.30534/ijatcse/2020/214952020

[4] V. Bhatia, K. R. Ramkumar, An efficient quantum computing technique for cracking RSA using Shor's algorithm, in: 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), 2020, 89–94. doi:10.1109/ICCCA49541.2020.9250806

[5] S. Holmes, L. Chen, Assessment of quantum threat to Bitcoin and derived cryptocurrencies, Cryptology ePrint Archive, 2021. URL: https://eprint.iacr.org/2021/967

[6] J. J. Tom, et al., Quantum computers and algorithms: A threat to classical cryptographic systems, Int. J. Eng. Adv. Technol. 12(5) (2023) 25–38. doi:10.35940/ijeat.E4153.0612523

[7] K. Denker, A. Y. Javaid, Quantum computing as a threat to modern cryptography techniques, in: International Conference on Foundations of Computer Science (FCS), 2019, 3–8.

[8] H. Khodaiemehr, K. Bagheri, C. Feng, Navigating the quantum computing threat landscape for blockchains: A comprehensive survey, Authorea Preprints (2023). doi:10.36227/techrxiv.24136440.v1

[9] F. Raheman, Futureproofing blockchain & cryptocurrencies against growing vulnerabilities & Q-Day threat with quantum-safe ledger technology (QLT), J. Comput. Commun. 12(7) (2024) 59–77. doi:10.4236/jcc.2024.127005

[10] A. I. Weinberg, A. Faccia, Quantum algorithms: A new frontier in financial crime prevention, arXiv, 2024. doi:10.48550/arXiv.2403.18322

[11] K. D. Gupta, et al., Utilizing computational complexity to protect cryptocurrency against quantum threats: A review, IT Prof. 23(5) (2021) 50–55. doi:10.1109/MITP.2021.3089494

[12] A. Naik, et al., From portfolio optimisation to quantum blockchain and security: A systematic review of quantum computing in finance, arXiv, 2023. doi:10.48550/arXiv.2307.01155

[13] S. Szatmáry, Quantum computers—security threats and solutions, in: Critical Infrastructure Protection in the Light of the Armed Conflicts, HCC 2022, Advanced Sciences and Technologies for Security Applications, 2024. doi:10.1007/978-3-031-47990-8_38

[14] D. Claudiu, et al., Enhancing the financial sector with quantum computing: A comprehensive review of current and future applications, in: 22nd International Conference on Informatics in Economy (IE 2023), IE 2023, Smart Innovation, Systems and Technologies, vol. 367, 2024. doi:10.1007/978-981-99-6529-8_17

[15] V. Malyukov, et al., Multifactor model of the digital cryptocurrency market as a computational core of the information system, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, 2023, 200–208.

[16] V. Malyukov, et al., Managing the purchase-sale process of digital currencies under fuzzy conditions, in: Intelligent Computing and Optimization, ICO 2023, Lecture Notes in Networks and Systems, vol. 729, 2023. doi:10.1007/978-3-031-36246-0_11

[17] B. Bebeshko, et al., Application of game theory, fuzzy logic and neural networks for assessing risks and forecasting rates of digital currency, J. Theor. Appl. Inf. Technol. 100(24) (2024) 7390–7404.

[18] B. Bebeshko, K. Khorolska, A. Desiatko, Analysis and modeling of price changes on the exchange market based on structural market data, in: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology, 2021, 151–156. doi:10.1109/PICST54195.2021.9772208
[19] L. A. Petrosjan, Differential games of pursuit, vol. 2, 1993. doi:10.1142/1670
[20] L. S. Pontryagin, On some differential games, J. Society Industrial Appl. Math. Series A: Control 3(1) (1965) 49–52. doi:10.1137/0303005
[21] L. S. Pontryagin, Mathematical theory of optimal processes, Routledge, 2018. doi:10.1201/9780203749319
[22] D. Micciancio, O. Regev, Lattice-based cryptography, in: Post-quantum Cryptography, 2009, 147–191. doi:10.1007/978-3-540-88702-7_5
[23] M. Iavich, et al., Classical and post-quantum encryption for GDPR, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3829 (2024) 70–78.
[24] A. Bessalov, et al., Computing of odd degree isogenies on supersingular twisted Edwards curves, in: Cybersecurity Information and Telecommunication Systems, vol. 2923 (2021) 1–11.
[25] A. Bessalov, et al., Implementation of the CSIDH algorithm model on supersingular twisted and quadratic Edwards curves, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.
[26] A. Bessalov, et al., Modeling CSIKE algorithm on non-cyclic Edwards curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
[27] A. Bessalov, et al., Multifunctional CRS encryption scheme on isogenies of non-supersingular Edwards curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.
[28] J. Bos, et al., CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM, in: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), 2018, 353–367. doi:10.1109/EuroSP.2018.00032
[29] F. Pan, P. Zhang, Simulating the Sycamore quantum supremacy circuits, arXiv, 2021. doi:10.48550/arXiv.2103.03074