Iraqi Journal of Science, 2024, Vol. 65, No. 7, pp: 3975-3992
DOI: 10.24996/ijs.2024.65.7.35

ISSN: 0067-2904

A Systematic Review: Post Quantum Cryptography to Secure Data Transmission

Asma Ibrahim Hussein [1]*, Abeer Tariq MaoLood[2], Ekhlas Khalaf Gbash[2]
[1]*Ministry of Higher Education and Scientific Research, Bagdad, Iraq*
[2] *Computer Science, University of Technology, Bagdad, Iraq*

Received: 8/11/2022 Accepted: 20/6/2023 Published: 30/7/2024

Abstract

A significant topic of contemporary cryptography research and standardization is the development of public key crypto systems that resist attacks from quantum computers. Protocols and applications should start investigating the use of quantum-resistant key exchange and encryption to protect the confidentiality of current communications against future quantum computers utilizing post-quantum cryptography for a particular key exchange. Since they operate harder and need fewer steps compared to conventional computers, quantum algorithms are more secure and robust. Attackers who use quantum computers have powerful computing capabilities, and a quantum allows for simple cryptographic system breaking. Security algorithms that are quantum secure are resistant to attacks from conventional, as well as quantum computers. This work has surveyed, summarized, and analysed previous research to provide readers of this study an integrated understanding of quantum cryptography. It also discusses quantum attacks, which could be used in place of more conventional cryptography techniques, such as quantum key distribution, which takes advantage of quantum mechanics' properties to ensure secure exchanges of the secret keys, and various quantum algorithms. With quantum computation becoming a very real threat, this should motivate more people to show an early interest in the future of cryptography.

Keywords: Post-quantum cryptography, public key, cryptographic, quantum-attacks.

مراجعة منهجية: التشفير ما بعد الكم لتأمين نقل البيانات

اسماء ابراهيم حسين[1]*, عبير طارق مولود[2], اخلاص خلف كباشي[2]
[1]وزارة التعليم العالي والبحث العلمي, بغداد, العراق
[2]قسم علوم الحاسوب, علوم الحاسوب, الجامعة التكنولوجية, بغداد, العراق

الخلاصة

يعد تطوير أنظمة تشفير المفتاح العام التي تقاوم الهجمات من أجهزة الحاسوب الكمومية أحد الموضوعات المهمة في البحث المعاصر في مجال التشفير والتوحيد القياسي. يجب أن تبدأ البروتوكولات والتطبيقات في التحقيق في استخدام تبادل المفاتيح والتشفير المقاوم للكم لحماية سرية الاتصالات الحالية ضد أجهزة الحاسوب

*Email: Cs.20.10@grad.uotechnology.edu.iq

الكمومية في المستقبل. استخدمت التشفير مابعد الكم لتبادل المفاتيح. نظرًا لأنها تعمل بجهد أكبر وتحتاج إلى خطوات أقل مقارنة بأجهزة الحاسوب التقليدية، فإن الخوارزميات الكمومية أكثر أمانًا وقوة. يتمتع المهاجمون الذين يستخدمون أجهزة الحاسوب الكمومية بقدرات حوسبة قوية، ويسمح الكم بكسر نظام التشفير البسيط. تقاوم خوارزميات الأمان الآمنة الكمومية الهجمات من أجهزة الحاسوب التقليدية وكذلك أجهزة الحاسوب الكمومية. تم في هذا العمل جمع المصادر وتلخيصه وتحليله لمنح قراء هذه الدراسة فهماً متكاملاً للتشفير الكمومي. كما يناقش الهجمات الكمية، والتي يمكن استخدامها بدلاً من تقنيات التشفير الأكثر تقليدية؛ توزيع المفاتيح الكمومية، والذي يستفيد من خصائص ميكانيكا الكم لضمان التبادل الآمن للمفاتيح السرية؛ والعديد من الخوارزميات الكمومية. نظرًا لأن الحساب الكمي أصبح تهديدًا حقيقيًا للغاية، يجب أن يحفز هذا المزيد من الأشخاص لإظهار اهتمام مبكر بمستقبل التشفير.

1. Introduction

To choose public-key encryption algorithms, as well as key-encapsulation mechanisms (KEM) and digital signature systems, which have resistance to quantum computing attacks, the NIST started a standardization process in the year 2016 [1].This is a timely response to the challenge posed by quantum computers, which are capable of breaking the public key cryptography algorithms currently in use. Post-quantum cryptography (PQC) has attracted much interest as a result of this standardization process, with a particular emphasis on strengthening the security of the PQC algorithms and the effectiveness of their implementation.

Devices that are based on the quantum bits, or qubits, which are 2-state quantum systems that could exist in any quantum superposition of 1 and 0, have been made possible using quantum mechanics. These devices, known as quantum computers, offer the possibility for solving some problems significantly more quickly compared to "classical" (non-quantum) computers. All widely used public key cryptosystems were broken by the quantum algorithm, which is efficiently in polynomial factored big numbers and computed discrete logarithms [2]. The NIST started a standardization process in the year 2016 to choose public-key encryption algorithms as well as key-encapsulation mechanisms (KEM) and digital signature systems that have resistance to quantum computing attacks. This is a timely response to the challenge posed by quantum computers, which are capable of breaking the public key cryptography algorithms currently in use [3]. Post-quantum cryptography (PQC) has attracted much interest due to this standardization process, with a particular emphasis on strengthening the security of the PQC algorithms and the effectiveness of their implementation [4].

A contemporary problem for both theoretical and applied cryptography is the development of post-quantum public-key cryptographic protocols and algorithms[5].

On the other hand, the majority of public-key cryptographic algorithms currently depend on mathematical problems that could be solved with highly efficient quantum algorithms. Hence, such public-key cryptography algorithms are not secure anymore. For instance, the Grover Quantum Algorithm, suggested in 1996 by Grover, could search exhaustively and swiftly, endangering symmetric cryptography algorithms [6], and the Shor Quantum Algorithm, suggested in 1994 by P. W. Shor, challenges public-key cryptography algorithms.
This research primarily advances post-quantum cryptography for security, and discuss the structural designs of the decentralized quantum in this way using numerous components [7].like research objectives, research methodology, eligibility criteria, data sources, classification of research articles, and the QPC algorithm. Because almost all of the problems are related to PQC in security, the suggested solutions are checked to see if they meet the system's needs.

2. Methodology of Research

The state-of-the-art integrated post-quantum cryptography technology used in data transmission is thoroughly reviewed and detailed in this paper. The research questions and goals made it possible to learn more about post-quantum technology about the secure transmission of data.

2.1 Research Objectives

This study analysed the most recent findings about the application of post-quantum cryptography. The following are the goals of this systematic review:

- Based on several case studies, define the classification of relevant studies.
- Determine challenges, motivations, and future work regarding post-quantum cryptography.
- Identify quantum attack types, security attacks, and explain QKD.

2.2 Data Sources

Electronic databases such as Springer, IEEE Explore, ACM, Elsevier Science Direct, Scopus, and Web of Science Show were used for a systematic search (Figure 1). These databases were chosen based on the substantial number of articles and conferences on cutting-edge subjects, such as quantum cryptography.

2.3 Study Selection

It can be challenging to choose the relevant studies, especially when considering various study fields. This phase is the most crucial and could also be the one that is most disregarded when examining a particular subject. To exclude irrelevant and duplicate research articles, the first stage involved screening research article abstracts and titles (32). Full-text reading of the chosen research papers (63) was the second stage. The relevant studies are shown in the next section.

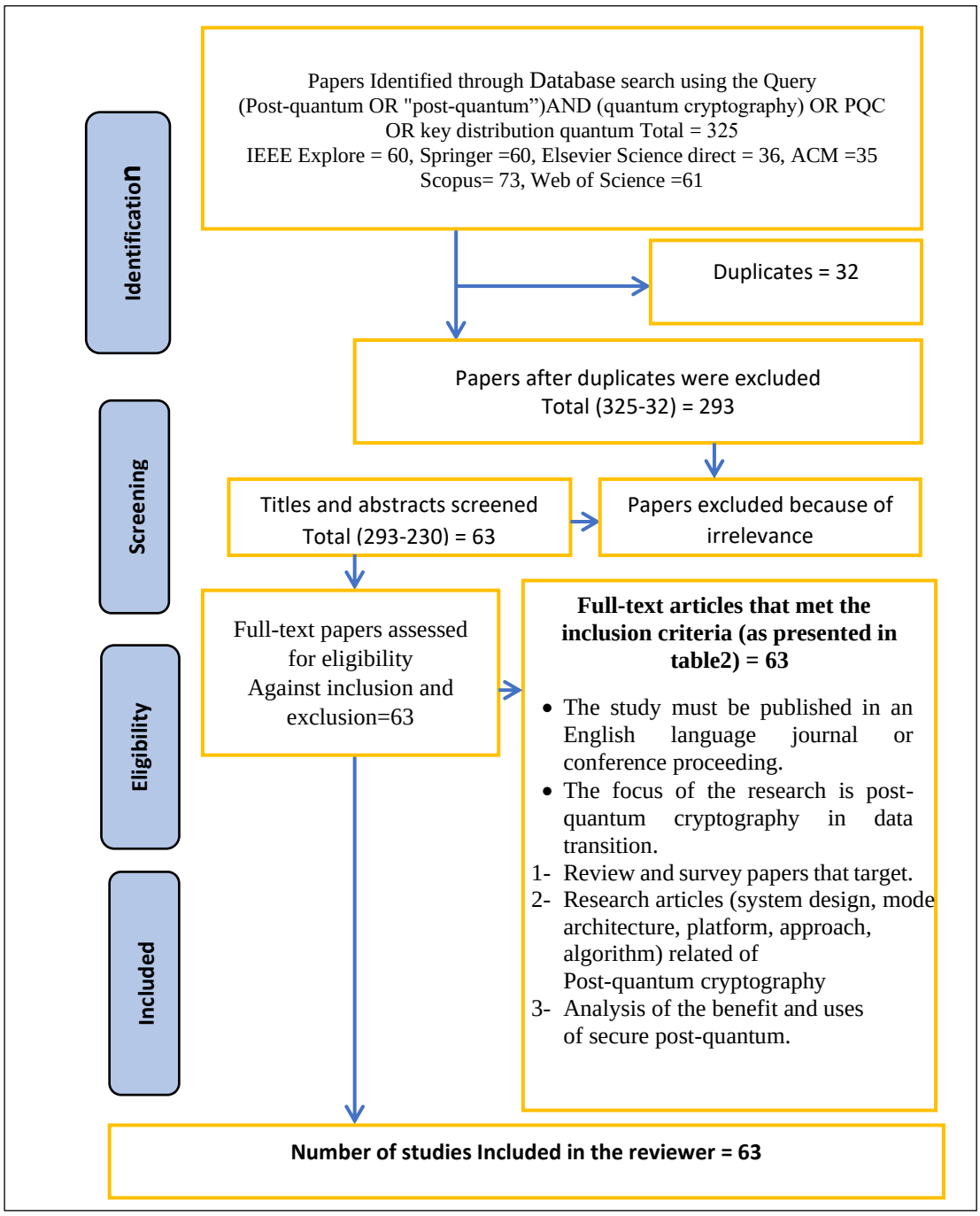

Figure 1: Block diagram of study selection

2.4 The relevant studies

• LTCI, Telecom ParisTech, 2018 [8]: In this study, a method for evaluating candidates for the NIST post-quantum standardization project's resistance to cache-timing attacks is provided. It runs static analysis with the sensitive variables being spread throughout the source code and looks for patterns of leakage. It is utilized to evaluate security regarding projects that have been submitted to NIST for post-quantum cryptography. The findings reveal that over 80% of examined implementations have a minimum of one possible problem, and 3 submissions have a combined total of over 1,000 flaws that have been documented. Lastly, this thorough analysis

of the candidates' security lets the most common problems among applicants be found and suggests ways to fix them.

- Markku-JuhaniO. Saarinen, 2020: this work presents measurements and recommendations for the usage of the PQC algorithm in the (IOT) and mobile systems [9]. There is evidence to support the idea that fast structured-lattice PQC schemes are the best choice for most cloud-connected mobile devices, even when the energy costs per bit of data transmission are quite high.
- Fabio Borges,2020,[10]: In the second NIST Post-Quantum Standardization Process round, three different types of cryptographic systems—isogeny crypto-systems that have been based upon super singular elliptic curves(lattice-based ring learning with errors, and error correction code-based encryption systems) were determined to be safe from quantum attacks. This study provided an assessment of the security and performance of such systems. Key agreements methods based upon those 3 post-quantum cryptographic primitives were compared in terms of security to the problems of integer factorization and discrete logarithms.
- Hamid Nejatollahi, Felipe Valencia,2020: This paper proposes an approach to create energy-efficient and flexible post-quantum cache-based accelerators for the Khyber [11]. New Hope, Lithium, Key Consensus from the Lattice (KCL), and R. EMBLEM using programmable hardware for the lattice-based algorithms. The findings offer recommendations for the hardware designers, identifying optimization areas to focus on for maximizing energy minimization and performance improvement.
- Crystal Andrea Roma, CHI-EN, 2021,[12]: The article discusses PQC's energy usage. Depending on their suggested level of security and cryptographic functionality, the energy measurements are divided into different categories. The most energy-efficient methods are then further split among the findings according to the underlying process. Finally, it is used to reveal potential areas for improvement by highlighting the most energy-intensive subroutines in a selected number of submissions.
- Sergey E. Yunakovsky, Maxim Kit, 2021: The effects of quantum threats on PKIs, a component of security systems used to protect production settings, was discussed in this study[13]. Also, it examined the security concerns with the current models with an emphasis on the conditions for a quick switch to post-quantum solutions. Even though the attacks using quantum computing are the main focus, there are other security concerns that, while not directly associated with the cryptographic algorithms utilized, are nonetheless crucial for the PKI's overall security. They also propose a group of security recommendations for PKI from the perspective of quantum computing attacks.
- Chithralekha Balamurugan, Kalpana Singh, 2021, [14]: This study provides an overview of the various post-quantum cryptography research directions that were investigated, with a focus on the numerous code-based cryptography research dimensions that were examined. This study makes two key contributions to the roadmap of post-quantum computing studies by highlighting certain unexplored possible research directions in code-based cryptographic research from the standpoint of the codes.
- Bertrand Cambou, Michael Gowanlock, 2021[15]: Discussed the effective methods to produce keys for lattice and code-based cryptography from physically impossible functions. Sets of addressable positions in PUFs are chosen through handshakes between the client devices that contain PUFs and a server. The PQC algorithms looked at in this study can also take advantage of high-performance computing, distributed memories, and parallel computing. All of these have the potential to lower RBC latencies even more.
- Stefan Balogh, Ondrej Gallo 2021,[16]: Reviewed existing IOT security challenges in this article with an eye toward potential risks in the future. The study detects three key trends that require special attention: security concerns arising from IOT integration with the cloud and block chain, the quick evolution of cryptography brought on by quantum computing, and lastly,

the development of AI and evolution techniques in the context of IOT security. They provide a summary of the threats found, as well as suggesting solutions for IOT security.

- Jungmin Park, N. Nalla Ananda Kumar, and Dipayan Saha, 2022,[17]: This work discusses PQC to create cryptographic algorithms that could withstand both conventional and quantum attacks. The theory of cryptographic algorithms has increasingly given way to their implementation on hardware platforms as a result of the latest advancements in the PQC field.

2.5 Eligibility Criteria

this paper focuses on post-quantum cryptography by including all of the research articles that meet the criteria that have been presented in Table 1 and Figure 2.Those categories were determined from a detailed study of the literature sources and surveys. After the exclusion of duplicate research, research that failed to meet the specified criteria was excluded [32–63].

Table 1: Criteria of Eligibility

Criterion	Specified	Grey Literature
Inclusion	• Reviews and surveys that are relevant to the utilization of this work. • Research articles (system designs, architecture, scheme, framework, approach, platform, model, protocol, and algorithm) that are relevant to this topic	• According to scientific studies, PQC has significantly improved the efficiency of data transmission across networks.
Exclusion	Books, thesis, and chapters of books • Unrelated articles • Non-English articles	Non-English articles, theses, unrelated articles, books, and book chapters have been excluded

3. Classification of Research Articles

The final group of research articles is categorized and discussed in this section based on the following criteria: (1) the authors (2) the publishers (3) the year of publication. The spread of article publications across the six websites (Science Direct, IEEE Explore, Web of Science, Springer, Scopes, and ACM) is depicted in Figure 2 .It v=can be seen that, for the period 2018 to 2022, the number of publications is rising annually. Consequently, academics' interest in post-quantum technologies has grown recently. In 2021, there was considerable growth in the use of quantum applications, and more research is anticipated to be done.

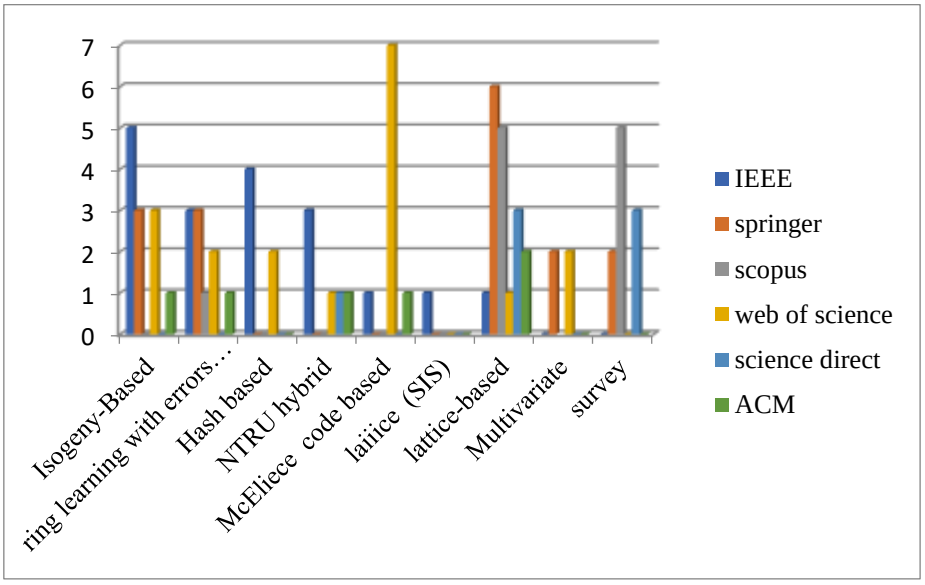

Figure 2: Publication Trends

3.1 Distribution by Author Publication

The distribution of the research articles about digital databases is shown in Figure 3. The way most of the articles in PQC were spread out shows that Gyongyosi was the most productive author in terms of how often they were published. Through the analysis of the researchs published in the international publishing sites and their number regarding the subject of post quantum cryptography, it is noted that the researcher Gyongyosi was distinguished by the research, analysis and the many works that he prepared and implemented with regard to this topic, and he published in the Publication Trends in comparison with other works.

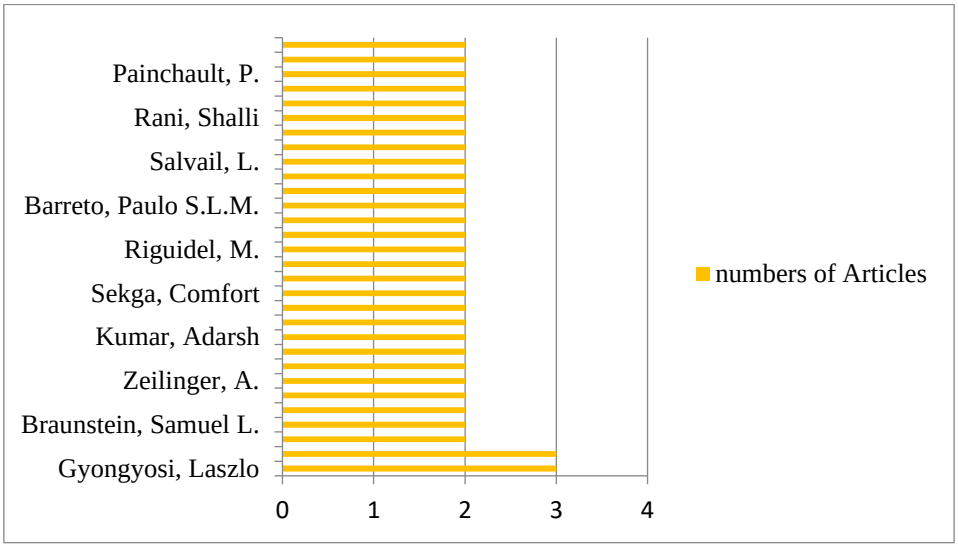

Figure 3: distribution of articles on Authors (x-number of Articles, y- names of Authors)

3.2 Distribution by Publishing Journal

According to publishers' scientific conferences and publications, the research articles were categorized, as shown in Table 2. To help researchers focus on the journals relevant to the topic of a specific work. Figure 4 shows the distribution of articles in various journals. Theoretical computers have high rates of articles related to PQC.

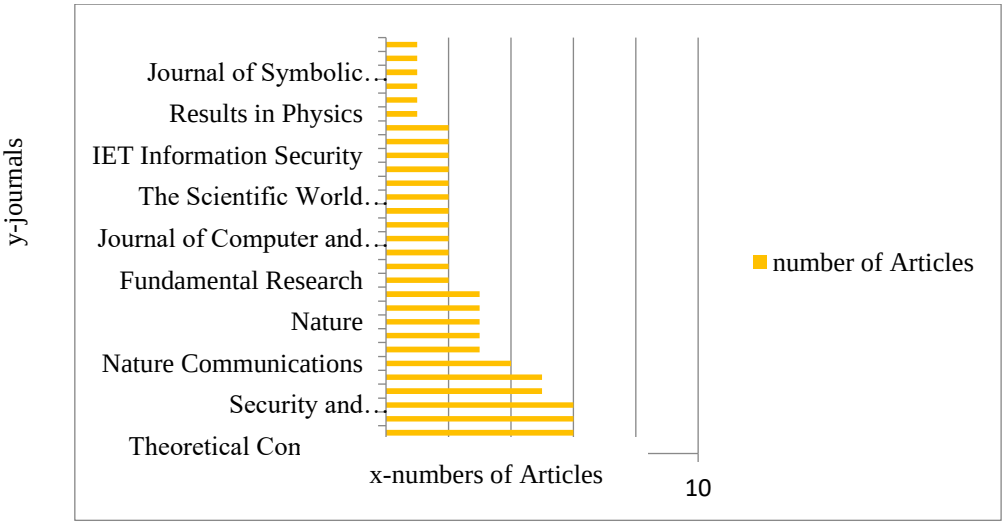

Figure 4: distribution of articles in different journals (x-number of Articles, y- journals)

Table 2: Categorisation of the Articles by Publishers, Journals, and Scientific Conferences

Journal	number of Articles	References
Theoretical Computer Science	8	[18][19][20][21][22][23][24][25]
EPJ Quantum Technology	6	[26][27][28][29][30][31]
Advances in High Energy Physics	6	[32][33][34][35][36][37]
Security and Communication Networks	6	[38][39] [40] [41], [42][43]
npj Quantum Information	5	[44][45][46][47][48]
Chinese Journal of Electronics	5	[49] [50][51][52][53]
Procedia Computer Science	3	[54][55][56]
Nature Photonics	3	[57][58][59]
Array	3	[60][61][62]
Advances in Mathematical Physics	3	[63][64][65]
Nature	2	[66][67]
Fundamental Research	2	[68][69]
International Journal of Mathematics and Mathematical Sciences	2	[70][71]
Journal of King Saud University - Computer and Information Sciences	2	[72][73]
ISRN Mathematical Physics	2	[74][75]
The Scientific World Journal	2	[76][77]
International Journal of Distributed Sensor Networks	2	[78][79]
Wireless Communications and Mobile Computing	2	[80][81]
Mathematical Problems in Engineering	2	[82][83]
Journal of Computer and System Sciences	1	[84]
IET Quantum Communication	1	[85]
IET Information Security	1	[86]
Vehicular Communications	1	[87]
Complexity	1	[88]
Advances in Condensed Matter Physics	1	[89]
Journal of Symbolic Computation	1	[90]
Quantum Information Processing	1	[91]
Journal of Sensors	1	[92]

3.3 Distribution Type of PQC For Each Study by Publishers

Numerous researchers have discovered various issues with PQC and security and have suggested workable solutions. The type of PQC that researchers use is explained in this section. Figure 5 is a chart that shows how the Mc Eliece code is used by researchers a lot. It shows how the research numbers are spread out by PQC type.

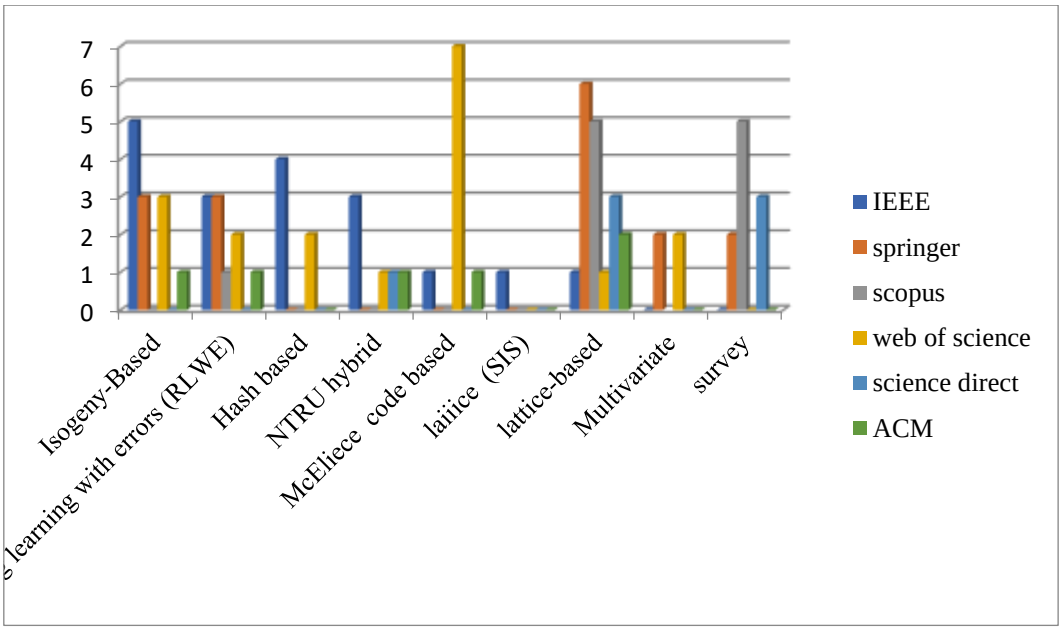

Figure 5: Distribution Type of PQC for each study on Publishers.

4. Security Considerations

The new PQ algorithms open previously undiscovered attack surfaces and add new mathematical concepts to the field of cryptography. New risks that might come with such concepts have to be investigated [93]. They are as follows:

- Cryptanalysis is used to assess the security of cryptographic methods when a sophisticated attacker is capable of conducting practical and/or analytical attacks. Numerous candidates who were submitted for the NIST challenge's first round were defeated by different cryptanalysis techniques. Most of the time, either the scheme was completely broken and the attackers were able to get the private key, or the attacked methods didn't have enough security to meet NIST criteria [94] [95].
- Side-Channel Attacks SCA targets particular aspects of algorithm execution, such as time and power usage. In this respect, PQC algorithms create new attack surfaces and must be examined for flaws both generally and in specific hardware situations. SCAs were discovered for all classes of PQC algorithms, and efficient defences against these attacks were put in place. However, according to the research, the exploration on SCAs on PQC algorithms and their countermeasures are still in their very early stages. The present countermeasures typically involve ad-hoc designs that offer protection against some SCAs yet leave users exposed to others, and various SCAs on PQC have not yet been assessed [96].
- Possible downgrade attacks against security protocols like TLS could force communication parties to revert to prior iterations of the standard. Attacks of this nature can be particularly harmful in the event of a switch from PQC to classical cryptography. There is a need to identify the three basic situations in which the server, the client, or both are aware of the new protocols whether they are this suggests that the side that is already utilizing a new protocol may be about to be downgraded [97].

4.1 Quantum Attacks

This section discusses quantum attacks that could be applied to lightweight or traditional cryptographic techniques in this area. These techniques can be used in IoT networks to make sure that integrity, privacy, availability, authentication, and non-repudiation are all taken care of.

1) Side-Channel Attack: Instead of attacking the mathematical structures, the eavesdropper attempts to take advantage of implementation or environmental flaws. An attacker's objective is to introduce faults into cryptosystems or algorithms. Here, an attacker attempts to track the results of the system after purposefully introducing faults that could reveal important data. The area of post-quantum cryptography commonly discusses this type of attack. For traditional ways to share quantum keys, like BB84-like techniques, SCA is a very big problem [98].
2) Attack Strategies for Quantum Key Distribution: The promise of quantum cryptography to provide a secret key that is perfectly secure is only true from a theoretical perspective. Practically speaking, QKD protocols are never flawless, and based on assumptions that have been made to apply security proofs to devices that are utilized in real-world implementation, there can be trade-offs between key-rate performance and security. Other things that could affect security and performance are how well post-processing is done, how many signals are exchanged, and how much noise is in the signals that are exchanged [99].

4.2 Quantum Key Distribution

A cutting-edge method known as QKD uses features of quantum mechanics to ensure secure exchanges of secret keys. Gilles Brassard and Charles Bennet, two computer scientists, believed in the early 1980s that a cipher providing complete security for all time might have been possible if the quantum theory had been applied to the field of cryptography. Polarized light photons are used in the cryptosystem created by Brassard and Bennet to transmit data between two points. It is employed to generate a secret key that Brassard and Bennett characterize as completely secure. Brassard and Bennett's 1984 paper, called BB84, was the first to show how these ideas could be used in a cryptographic system to solve the key distribution problem [100].

The primary benefit of quantum cryptography is that it provides a solution to the key distribution problem. By providing a string of randomly polarized photons, a user can offer a key. The key for encryption could then be generated using this sequence. QKD is the name of the procedure. Following the secure receipt of the final key, it could be utilized for encrypting messages that could be sent via traditional channels like email, phone, etc. Below is a description of how the BB84 QKD protocol works. There are two primary stages to it [101]:
1- Quantum Channel (1-way communications)
2- Classical Channel (2-way communications). To distribute the key in the first phase, Bob and Alice established a quantum channel. They find the final key in the second channel, also referred to as the classical channel. Figure 6 displays this configuration.

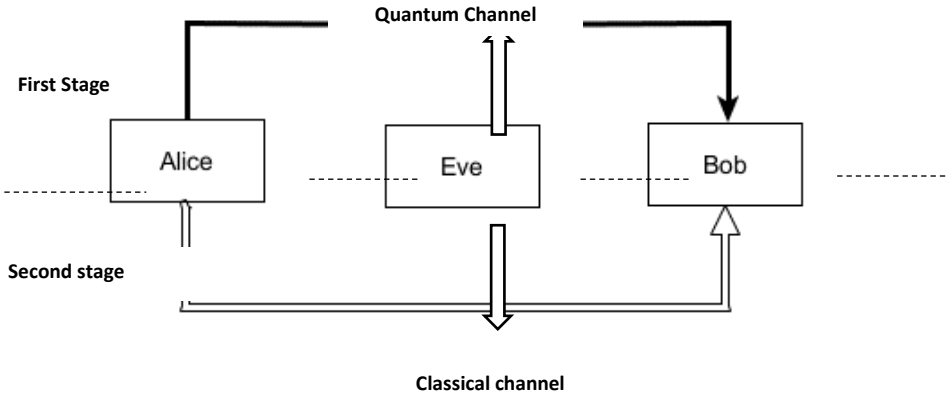

Figure 6: Quantum communication [102]

This process comprises 4 major phases, which are:
1. Sifting
2. Error Estimation
3. Reconciliation
4. Privacy Amplification

4.3 Post-Quantum Cryptography Types

To resist attacks based on quantum computing and quantum computers, PQC is being developed. ICT has already adopted several PQC techniques. Figure 7 depicts flowcharts of several forms of PQC are the main subcategories of PQC.

- **Lattice-based Cryptography**

The lattice-based crypto-system represents an excellent choice for the future due to its broad applicability, robust security, and effectiveness in thwarting attacks. Many different cryptosystems typically employ the random key generation procedure. Lattice-based cryptography has the average-case intractability or hard problems needed for this random key generation technique [103].For smart IoT devices, choosing the proper parameters that are easier is necessary for worst-case reduction to the average-case hard problem, since quick activities demand size, which is typically smaller. Lattice-based algorithms are also like vectors and matrices in short-order fields or rings that have small-size parameters.

- **Code-based Cryptography**

The Goppa code and random generator matrices utilizing that code are used in the McEliece crypto system, which represents the first cryptosystem to be suggested in an asymmetric key encryption technique. In comparison to lattice-based cryptography, code-based crypto-systems are thought to be unsuitable for devices with limited resources due to their high memory requirements, lengthy cipher texts, and huge public key sizes. The Niederreiter cryptosystem and the McEliece cryptosystem are two different code-based cryptography techniques. The McEliece cryptosystem and its variant, the Niederreiter cryptosystem, both offer the same level of security.

- **Multivariate Polynomial Cryptography** Simple arithmetic processes are used in multivariate polynomial cryptography schemes' security primitives and protocols. In small finite fields, such operations include multiplication and addition. Because it is easy to use and calculate, this could be a good way to keep security in devices with limited resources, like sensors, RFID cards, actuators, and smart cards.
- **Hash-based Signatures:** several aspects of the hash-based approach that are advantageous to the IoT ecosystem are identified. Hash-based techniques make no further cryptographic assumptions and only depend on cryptographic hash functions. As a result, it limits the potential for cryptanalysis. This lessens the system's overall complexity. To attain the required performance, the hash-based scheme must be flexible in the hash function it chooses because it is intrinsically dependent on the application-specific environment. This system protects the application against numerous attacks thanks to the collision resistance, pre-image resistance, and second-pre-image resistance characteristics of the hash functions.
- **Isogeny-based Cryptosystem:** This cryptosystem depends on super singular elliptic curve isogenies. This system could be applied to the digital signature or key exchange methods. Based on super singular isogeny graphs, the super singular Isogeny Diffie-Hellman Key Exchange (SIDH) method is resistant to cryptanalytic attacks from any adversary. Small key sizes and 128-bit quantum security levels are both possible with SIDH. The characteristics of this post-quantum cryptosystem, such as attack resistance and minimal-size cryptography implementation, make it a practical choice for IoT networks' resource-constrained devices.

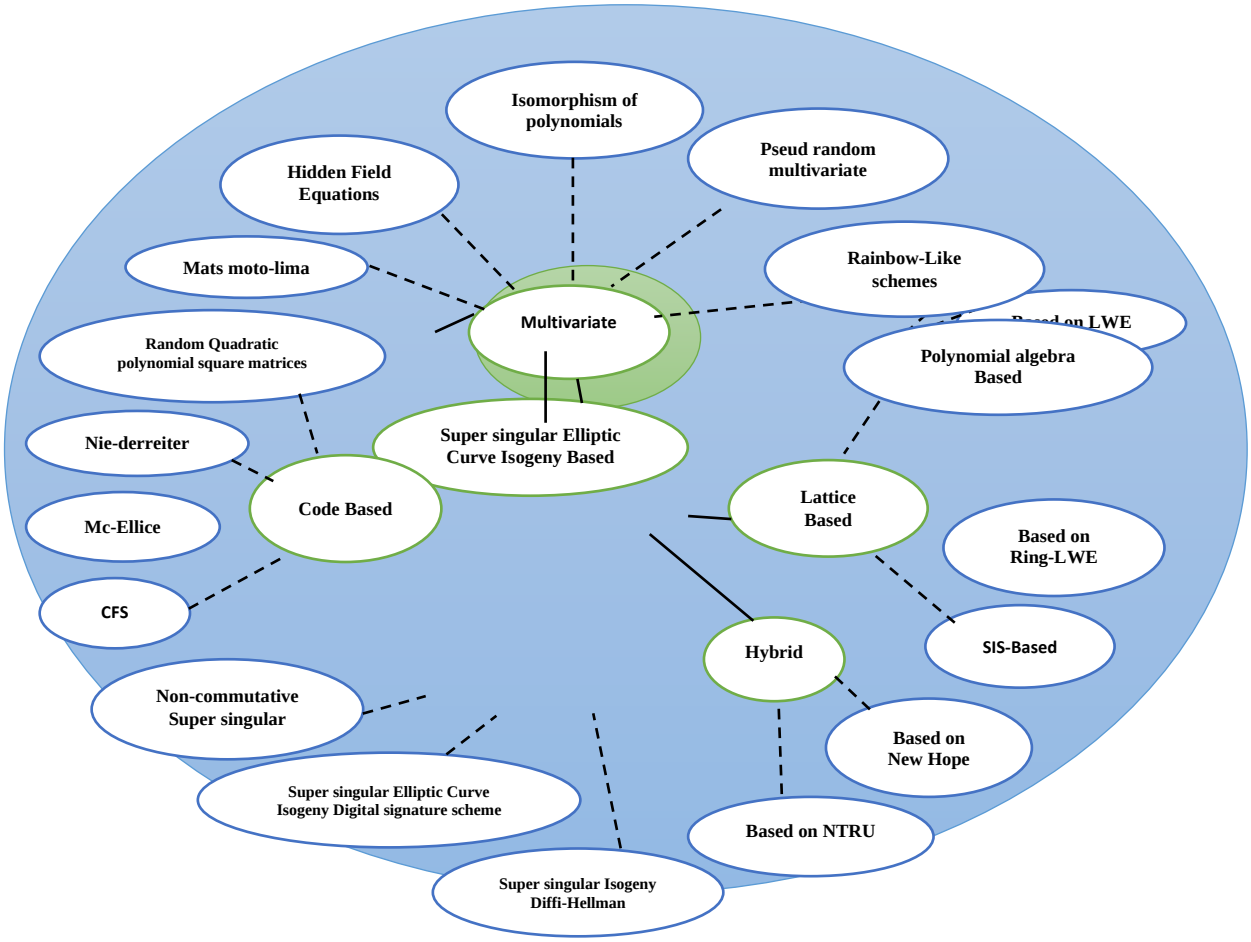

Figure 7: Types of post-quantum cryptography

4.4 PQC Algorithms

1) Shor's Algorithm: The Discrete Logarithm Problem and the Prime Factorization Problem are the two main hard problems on which the security of modern cryptosystems has been based. Shor created two distinct quantum algorithms that can solve these difficulties. These problems have better solutions to the classical solutions. These probabilistic algorithms were created by Shor in polynomial time with the use of period discovery via Quantum Fourier Transformation. The best classical method could not crack the factoring number problem in polynomial time until Shor's algorithm could. There are two main components in the two algorithms: The problem must first be transformed into a period-finding problem in the first portion, which is a conventional step [104].The second component, which utilizes quantum parallelism to solve the period-finding problem, is known as the quantum component. The period is determined using the quantum Fourier transformation algorithm. The algorithm used by Shor is probabilistic. It doesn't often take the initial calculation into account. The probability of receiving a factor grows as the algorithm is run more frequently [105].

2) Grover's Algorithm: It is a quantum search algorithm that performs O (n 1/2) searches in an unsorted database. On traditional computers, searching through an unordered database is an O (n) problem. Grover's algorithm is probabilistic as well and could be used multiple times to guarantee that the search is finished. Grover iteration is used to search. To improve the probability of discovering the element in a database, iterations can be repeated. Grover's algorithm could be utilized to determine the median, mean, and inverse value of a function,

among other things. Quantum cryptanalysts could utilize such technologies to crack algorithms. Additionally, it could be applied to find keys in a symmetric crypto system.

3) Simon's Algorithm a quantum circuit called Simon's algorithm finds, according to the function's property, an XOR of two input values that map to the same output to produce the constant b. It becomes a 1-to-1 function if b contains just zeroes; otherwise, it becomes a 2-to-1 function. Finding a collision in the classical solution takes O (2n1 + 1). The exponential speedup is offered by the quantum algorithm. Simon's algorithm served as a model for Shor's algorithm. If a suitable query access model is present, Simon's algorithm itself has applications in cryptography [106].

5. Conclusions and Future Work

Studies on PQC in security are becoming more prevalent, but they still have issues that need to be resolved. PQC is a developing subject that needs more research. The primary contribution of this work is the thorough analysis and categorization of relevant PQC research articles. In this study, different PQCs were reviewed systematically. Once large-scale quantum computers are constructed, it is anticipated that the security of widely utilized public-key cryptographic algorithms (such as RSA and elliptic-curve cryptography) may decrease. A serious threat exists because modern society's IT infrastructure is supported by these algorithms. The security of certain classes of new PQC algorithms, even against attackers utilizing just classical computers, has not yet been adequately studied. PQC algorithms are predicted to continue to be secure against attackers with ideal quantum computers. As a result, it is necessary to assess the security of PQC algorithms against both classical and quantum computer attackers. Quantum cryptography research was studied and summarized in this study. To provide readers with comprehensive knowledge regarding quantum computing. Quantum computing is becoming a real threat, which should encourage more people to start thinking about the future of cryptography now and future work for this paper. By looking at the studies on PQC, it is suggested that one of the algorithms be used in the future to allow for highly secret data transit between server and client while using QKD.

References

[1] B. Cambou *et al.*, "Post quantum cryptographic keys generated with physical unclonable functions," *Appl. Sci.*, vol. 11, no. 6, 2021, doi: 10.3390/app11062801.

[2] J. Park *et al.*, "PQC-SEP : Power Side-channel Evaluation Platform for Post-Quantum Cryptography Algorithms," no. December 2017, pp. 1–38, 2020.

[3] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, "Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions," *Cryptography*, vol. 5, no. 4, pp. 1–30, 2021, doi: 10.3390/cryptography5040038.

[4] C. A. Roma, C. A. M. Y. Tai, M. A. Hasan, and S. Member, "Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms," pp. 71295–71317, 2021.

[5] M. J. Saarinen, "Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards," *Proc. - 2020 8th IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2020*, pp. 23–30, 2020, doi: 10.1109/MobileCloud48802.2020.00012.

[6] F. Borges, S. Member, and P. R. Reis, "A Comparison of Security and Its Performance for Key Agreements in Post-Quantum Cryptography," 2020, doi: 10.1109/ACCESS.2020.3013250.

[7] A. Facon, S. Guilley, M. Lec'hvien, A. Schaub, and Y. Souissi, "Detecting cache-timing vulnerabilities in post-quantum cryptography algorithms," *2018 IEEE 3rd Int. Verif. Secur. Work. IVSW 2018*, no. July, pp. 7–12, 2018, doi: 10.1109/IVSW.2018.8494855.

[8] S. Balogh, O. Gallo, R. Ploszek, P. Špaček, and P. Zajac, "Iot security challenges: Cloud and blockchain, postquantum cryptography, and evolutionary techniques," *Electron.*, vol. 10, no. 21, 2021, doi: 10.3390/electronics10212647.

[9] S. E. Yunakovsky *et al.*, "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era," *EPJ Quantum Technol.*, vol. 8, no. 1, 2021,

doi: 10.1140/epjqt/s40507-021-00104-z.
[10] H. Nejatollahi, F. Valencia, S. Banik, F. Regazzoni, R. Cammarota, and N. Dutt, "Synthesis of flexible accelerators for early adoption of ring-LWE post-quantum cryptography," *ACM Trans. Embed. Comput. Syst.*, vol. 19, no. 2, 2020, doi: 10.1145/3378164.
[11] Y. Takeuchi, T. Morimae, and S. Tani, "Sumcheck-based delegation of quantum computing to rational server," *Theor. Comput. Sci.*, vol. 924, pp. 46–67, 2022, doi: 10.1016/j.tcs.2022.04.016.
[12] L. Gyongyosi, "Post-processing optimization for continuous-variable quantum key distribution," *Theor. Comput. Sci.*, vol. 893, pp. 146–158, 2021, doi: 10.1016/j.tcs.2021.08.023.
[13] L. Gyongyosi, "Multicarrier continuous-variable quantum key distribution," *Theor. Comput. Sci.*, vol. 816, pp. 67–95, 2019, doi: 10.1016/j.tcs.2019.11.026.
[14] R. Alléaume *et al.*, "Using quantum key distribution for cryptographic purposes: A survey," *Theor. Comput. Sci.*, vol. 560, no. P1, pp. 62–81, 2014, doi: 10.1016/j.tcs.2014.09.018.
[15] O. Izmerly and T. Mor, "Chosen ciphertext attacks on lattice-based public key encryption and modern (non-quantum) cryptography in a quantum environment," *Theor. Comput. Sci.*, vol. 367, no. 3, pp. 308–323, 2006, doi: 10.1016/j.tcs.2006.07.060.
[16] A. Takayasu and Y. Watanabe, "Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more," *Theor. Comput. Sci.*, vol. 849, pp. 64–98, 2021, doi: 10.1016/j.tcs.2020.10.010.
[17] S. Mishra, K. Thapliyal, A. Parakh, and A. Pathak, "Quantum anonymous veto: a set of new protocols," *EPJ Quantum Technol.*, vol. 9, no. 1, 2022, doi: 10.1140/epjqt/s40507-022-00133-2.
[18] R. Shi, "Privacy-preserving quantum protocol for finding the maximum value," *EPJ Quantum Technol.*, 2022, doi: 10.1140/epjqt/s40507-022-00132-3.
[19] M. Krelina, "Quantum technology for military applications," *EPJ Quantum Technol.*, vol. 8, no. 1, 2021, doi: 10.1140/epjqt/s40507-021-00113-y.
[20] D. Lowndes, S. Frick, A. Hart, and J. Rarity, "A low cost, short range quantum key distribution system," *EPJ Quantum Technol.*, vol. 8, no. 1, 2021, doi: 10.1140/epjqt/s40507-021-00101-2.
[21] A. B. Price, J. G. Rarity, and C. Erven, "A quantum key distribution protocol for rapid denial of service detection," *EPJ Quantum Technol.*, vol. 7, no. 1, 2020, doi: 10.1140/epjqt/s40507-020-00084-6.
[22] M. Polnik, L. Mazzarella, M. Di Carlo, D. K. Oi, A. Riccardi, and A. Arulselvan, "Scheduling of space to ground quantum key distribution," *EPJ Quantum Technol.*, vol. 7, no. 1, 2020, doi: 10.1140/epjqt/s40507-020-0079-6.
[23] X. Guo, B. Lv, J. Tao, and P. Wang, "Quantum Tunneling in Deformed Quantum Mechanics with Minimal Length," vol. 2016, no. 7, 2016.
[24] C. S. Chew, O. C. W. Kong, and J. Payne, "A Quantum Space behind Simple Quantum Mechanics," vol. 2017, 2017.
[25] R. Z. Khalaf and A. A. Abdullah, "Novel Quantum Encryption Algorithm Based on Multiqubit Quantum Shift Register and Hill Cipher," vol. 2014, 2014.
[26] E. T. Akhmedov, S. Minter, P. Nicolini, and D. Singleton, "Experimental tests of quantum gravity and exotic quantum field theory effects," *Adv. High Energy Phys.*, vol. 2014, pp. 2–4, 2014, doi: 10.1155/2014/192712.
[27] D. Arteaga, "Quantum Brownian Representation for the Quantum Field Modes," *Adv. High Energy Phys.*, vol. 2009, pp. 1–29, 2009, doi: 10.1155/2009/278759.
[28] O. Dănilă, P. E. Sterian, and A. R. Sterian, "Perspectives on entangled nuclear particle pairs generation and manipulation in quantum communication and cryptography systems," *Adv. High Energy Phys.*, vol. 2012, 2012, doi: 10.1155/2012/801982.
[29] H. Wang, Y. Li, and L.-P. Wang, "Post-Quantum Secure Password-Authenticated Key Exchange Based on Ouroboros," *Secur. Commun. Networks*, vol. 2022, pp. 1–11, 2022, doi: 10.1155/2022/9257443.
[30] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum Cryptography for the Future Internet and the Security Analysis," vol. 2018, 2018.
[31] T. Park, H. Seo, J. Kim, H. Park, and H. Kim, "Efficient Parallel Implementation of Matrix Multiplication for Lattice-Based Cryptography on Modern ARM Processor," vol. 2018, 2018.
[32] W. Gao and L. Yang, "Quantum Election Protocol Based on Quantum Public Key Cryptosystem," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/5551249.

[33] D. Dharminder, A. K. Das, S. Saha, B. Bera, and A. V Vasilakos, "Post-Quantum Secure Identity-Based Encryption Scheme using Random Integer Lattices for IoT-enabled AI Applications," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/5498058.

[34] H. Abulkasim *et al.*, "Cryptanalysis and Improvements on Quantum Key Agreement Protocol Based on Quantum Search Algorithm," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/3803621.

[35] P. J. Cavalcanti, J. H. Selby, J. Sikora, T. D. Galley, and A. B. Sainz, "Post-quantum steering is a stronger-than-quantum resource for information processing," *npj Quantum Inf.*, vol. 8, no. 1, pp. 1–10, 2022, doi: 10.1038/s41534-022-00574-8.

[36] E. Y. Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C. W. Lim, "Computing secure key rates for quantum cryptography with untrusted devices," *npj Quantum Inf.*, vol. 7, no. 1, pp. 1–6, 2021, doi: 10.1038/s41534-021-00494-z.

[37] L. J. Wang *et al.*, "Experimental authentication of quantum key distribution with post-quantum cryptography," *npj Quantum Inf.*, vol. 7, no. 1, 2021, doi: 10.1038/s41534-021-00400-7.

[38] M. Curty and H. K. Lo, "Foiling covert channels and malicious classical post-processing units in quantum key distribution," *npj Quantum Inf.*, vol. 5, no. 1, 2019, doi: 10.1038/s41534-019-0131-5.

[39] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum Cryptography for the Future Internet and the Security Analysis," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/8214619.

[40] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," *npj Quantum Inf.*, vol. 4, no. 1, pp. 1–9, 2018, doi: 10.1038/s41534-018-0070-6.

[41] H. Iqbal and W. O. Krawec, *Semi-quantum cryptography*, vol. 19, no. 3. Springer US, 2020. doi: 10.1007/s11128-020-2595-9.

[42] L. Hongxin *et al.*, "Fair efficiency comparisons of decoy-state quantum key distribution protocols," *Chinese J. Electron.*, vol. 27, no. 2, pp. 241–249, 2018, doi: 10.1049/cje.2017.07.011.

[43] L. Leilei, Z. Yu, W. Shuang, L. Na, Y. Jiayu, and L. Jian, "Deterministic quantum secure direct communication and authentication protocol based on W-class state," *Chinese J. Electron.*, vol. 27, no. 2, pp. 276–280, 2018, doi: 10.1049/cje.2017.10.006.

[44] C. Yan, X. Jinxin, G. A. O. Xiang, Z. Shibin, and Y. A. N. Lili, "Quantum Private Query Protocol Based on EPR Pairs ∗," vol. 27, no. 2, 2018, doi: 10.1049/cje.2018.01.016.

[45] F. Muheidat, K. Dajani, and L. A. Tawalbeh, "Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication," *Procedia Comput. Sci.*, vol. 203, pp. 32–40, 2022, doi: 10.1016/j.procs.2022.07.007.

[46] D. C. Bastos and L. A. Brasil Kowada, "How to detect whether Shor's algorithm succeeds against large integers without a quantum computer," *Procedia Comput. Sci.*, vol. 195, pp. 145–151, 2021, doi: 10.1016/j.procs.2021.11.020.

[47] J. Bobrysheva and S. Zapechnikov, "On the key composition for post-quantum group messaging and file exchange," *Procedia Comput. Sci.*, vol. 190, no. 2019, pp. 102–106, 2021, doi: 10.1016/j.procs.2021.06.012.

[48] S. Pirandola *et al.*, "correspondence Reply to ' Discrete and continuous variables for measurement-device-independent quantum cryptography ,'" *Nat. Publ. Gr.*, pp. 1–2, 2015, doi: 10.1038/nphoton.2015.207.

[49] S. Pirandola *et al.*, "Reply to 'Discrete and continuous variables for measurement-device-independent quantum cryptography,'" *Nat. Photonics*, vol. 9, no. 12, pp. 773–775, 2015, doi: 10.1038/nphoton.2015.207.

[50] B. Cambou *et al.*, "Securing additive manufacturing with blockchains and distributed physically unclonable functions," *Cryptography*, vol. 4, no. 2, pp. 1–26, 2020, doi: 10.3390/cryptography4020017.

[51] M. Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," *Array*, vol. 15, no. August, p. 100242, 2022, doi: 10.1016/j.array.2022.100242.

[52] D. A. Bard, J. J. Kearney, and C. A. Perez-Delgado, "Quantum advantage on proof of work," *Array*, vol. 15, no. December 2021, p. 100225, 2022, doi: 10.1016/j.array.2022.100225.

[53] J. J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," *Array*, vol. 10, no. November 2020, p. 100065, 2021, doi: 10.1016/j.array.2021.100065.

[54] J. C. Baez, "Quantum techniques for reaction networks," *Adv. Math. Phys.*, vol. 2018, 2018, doi: 10.1155/2018/7676309.
[55] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," *Nat. Commun.*, vol. 7, no. May, pp. 1–9, 2016, doi: 10.1038/ncomms11712.
[56] J. Yin *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, 2020, doi: 10.1038/s41586-020-2401-y.
[57] C. Wang, "Quantum secure direct communication: Intersection of communication and cryptography," *Fundam. Res.*, vol. 1, no. 1, pp. 91–92, 2021, doi: 10.1016/j.fmre.2021.01.002.
[58] J. Bos *et al.*, "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," *Proc. - 3rd IEEE Eur. Symp. Secur. Privacy, EURO S P 2018*, pp. 353–367, 2018, doi: 10.1109/EuroSP.2018.00032.
[59] D. Fukuda and K. Kuga, "Twisted quantum doubles," *Int. J. Math. Math. Sci.*, vol. 2004, no. 28, pp. 1477–1486, 2004, doi: 10.1155/S016117120430236X.
[60] M. Fujio, "A comparison of implications in orthomodular quantum logic-morphological analysis of quantum logic," *Int. J. Math. Math. Sci.*, vol. 2012, 2012, doi: 10.1155/2012/259541.
[61] M. S. Şahin and S. Akleylek, "A constant-size lattice-based partially-dynamic group signature scheme in quantum random oracle model," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2022, doi: 10.1016/j.jksuci.2021.12.014.
[62] C. Mangla, S. Rani, N. M. Faseeh Qureshi, and A. Singh, "Mitigating 5G security challenges for next-gen industry using quantum computing," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2022, doi: 10.1016/j.jksuci.2022.07.009.
[63] C. Kiefer, "Conceptual Problems in Quantum Gravity and Quantum Cosmology," *ISRN Math. Phys.*, vol. 2013, pp. 1–17, 2013, doi: 10.1155/2013/509316.
[64] D. Georgiev, "Quantum Histories and Quantum Complementarity," *ISRN Math. Phys.*, vol. 2012, pp. 1–37, 2012, doi: 10.5402/2012/327278.
[65] D. Dong, C. Chen, M. Jiang, and L. C. Wang, "Quantum control and quantum information technology," *Sci. World J.*, vol. 2013, no. 12, pp. 3–5, 2013, doi: 10.1155/2013/525631.
[66] M. Li, "Simulation of quantum dynamics based on the quantum stochastic differential equation," *Sci. World J.*, vol. 2013, 2013, doi: 10.1155/2013/424137.
[67] M. E. Rivero-Angeles, "Quantum-based wireless sensor networks: A review and open questions," *Int. J. Distrib. Sens. Networks*, vol. 17, no. 10, 2021, doi: 10.1177/15501477211052210.
[68] C. Zhou, L. Wang, and L. Wang, "Lattice-based provable data possession in the standard model for cloud-based smart grid data management systems," *Int. J. Distrib. Sens. Networks*, vol. 18, no. 4, 2022, doi: 10.1177/15501329221092940.
[69] Z. Li, C. Xiang, and C. Wang, "Oblivious Transfer via Lossy Encryption from Lattice-Based Cryptography," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018, doi: 10.1155/2018/5973285.
[70] C. Mangla, S. Rani, and H. K. Atiglah, "Secure Data Transmission Using Quantum Cryptography in Fog Computing," vol. 2022, 2022.
[71] V. Tkachuk, "Quantum Genetic Algorithm on Multilevel Quantum Systems," vol. 2018, 2018.
[72] H. Kalsoom, M. A. Ali, M. Idrees, P. Agarwal, and M. Arif, "New Post Quantum Analogues of Hermite – Hadamard Type Inequalities for Interval-Valued Convex Functions," vol. 2021, 2021.
[73] R. T. Possignolo, C. B. Margi, and P. S. L. M. Barreto, "Quantum-assisted QD-CFS signatures," *J. Comput. Syst. Sci.*, vol. 81, no. 2, pp. 458–467, 2015, doi: 10.1016/j.jcss.2014.10.003.
[74] V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, and M. Guizani, "Present landscape of quantum computing," vol. 1, no. September, pp. 42–48, 2020, doi: 10.1049/iet-qtc.2020.0027.
[75] H. Xie and L. Yang, "Witness indistinguishability and witness hiding against quantum attacks," pp. 579–590, 2019, doi: 10.1049/iet-ifs.2018.5460.
[76] A. Kumar, D. Augusto de Jesus Pacheco, K. Kaushik, and J. J. P. C. Rodrigues, "Futuristic view of the Internet of Quantum Drones: Review, challenges and research agenda," *Veh. Commun.*, vol. 36, p. 100487, 2022, doi: 10.1016/j.vehcom.2022.100487.
[77] C. Li, M. Shi, Y. Zhou, and E. Wang, "Quantum Particle Swarm Optimization Extraction Algorithm Based on Quantum Chaos Encryption," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/6627804.
[78] M. J. Wang, F. Y. Yue, and F. M. Guo, "Photoelectric Characteristics of Double Barrier Quantum Dots-Quantum Well Photodetector," vol. 2015, 2015.

[79] T. Kubota, Y. Kakutani, G. Kato, Y. Kawano, and H. Sakurada, "Semi-automated verification of security proofs of quantum cryptographic protocols," *J. Symb. Comput.*, vol. 73, no. 13, pp. 192–220, 2016, doi: 10.1016/j.jsc.2015.05.001.
[80] C. Wang, C. Wang, S. Ren, and Y. Tang, "Open quantum random walk in terms of quantum Bernoulli noise," *Quantum Inf. Process.*, vol. 17, no. 3, 2018, doi: 10.1007/s11128-018-1820-2.
[81] D. S. Simon, "Quantum sensors: Improved optical measurement via specialized quantum states," *J. Sensors*, vol. 2016, 2016, doi: 10.1155/2016/6051286.
[82] R. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, 2021, doi: 10.3390/iot2010005.
[83] S. Wijesekera, "Quantum Cryptography for Secure Communication in IEEE 802 . 11 Wireless Networks," no. June, 2011.
[84] W. Barker and W. Polk, "Getting Ready for Post-Quantum Cryptography :," 2021.
[85] P. Ravi, "Authentication Protocol for Secure Automotive Systems : Benchmarking Post-Quantum Cryptography," pp. 0–4, 2020.
[86] D. Heo, S. Kim, K. Yoon, Y. H. Park, and S. Hong, "Optimized csidh implementation using a 2-torsion point," *Cryptography*, vol. 4, no. 3, pp. 1–13, 2020, doi: 10.3390/cryptography4030020.
[87] A. Gagnidze, M. Iavich, and G. Iashvili, "Analysis of Post-Quantum Cryptography Use in Practice Analysis of Post-Quantum Cryptography Use in Practice," no. April, 2021.
[88] J. L. Imaña *et al.*, "Efficient Hardware Arithmetic for Inverted Binary Ring-LWE Based Post-Quantum Cryptography," pp. 1–11, 2022.
[89] K. Xagawa, A. Ito, R. Ueno, J. Takahashi, and N. Homma, "Fault-Injection Attacks against NIST ' s Post-Quantum Cryptography Round 3 KEM Candidates Table of Contents," no. Crypto 2020, pp. 1–42.
[90] A. B. Chowdhury, A. Mahapatra, D. Soni, and R. Karri, "Fuzzing + Hardware Performance Counters-Based Detection of Algorithm Subversion Attacks on Post-Quantum Signature Schemes," pp. 1–12.
[91] J. Vakarjuk, N. Snetkov, and J. Willemson, "DiLizium : A Two-Party Lattice-Based Signature Scheme," pp. 1–30, 2021.
[92] V. Ustimenko, "On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography .," vol. 1.
[93] T. A. Khaleel and A. A. Al-Shumam, "A study of graph theory applications in IT security," *Iraqi Journal of Science*, vol. 61, no. 10. pp. 2705–2714, 2020. doi: 10.24996/ijs.2020.61.10.28.
[94] E. T. L. S. Crypto-processor, U. Banerjee, S. Das, and A. P. Chandrakasan, "Accelerating Post-Quantum Cryptography using an Energy-Efficient TLS Crypto-Processor," 2020.
[95] S. A. B. Salman, S. Al-Janabi, and A. M. Sagheer, "A Review on E-Voting Based on Blockchain Models," *Iraqi Journal of Science*, vol. 63, no. 3. pp. 1362–1375, 2022. doi: 10.24996/ijs.2022.63.3.38.
[96] "A Review of Assured Data Deletion Security Techniques in Cloud Storage.pdf."
[97] M. C. Amazon, B. Lamacchia, and D. Ott, "Post Quantum Cryptography : Readiness Challenges and the Approaching Storm," no. Ccc.
[98] J. Partala, "Chapter 20 Post-quantum Cryptography in 6G".
[99] B. Schneider, "Post-Quantum Cryptography : An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms," vol. 84, pp. 61–71, 2022.
[100] M. H. Al Hasani and K. A. M. Al Naimee, "Quantum key distribution and chaos bandwidth effects on impact security of quantum communications," *Iraqi Journal of Science*, vol. 60, no. 6. pp. 1266–1273, 2019. doi: 10.24996/ijs.2019.60.6.10.
[101] Y. Zhu, Y. Liu, M. Wu, J. Li, S. Liu, and J. Zhao, "Research on Secure Communication on In-Vehicle Ethernet Based on Post-Quantum Algorithm NTRUEncrypt," 2022.
[102] L. Bettale *et al.*, "Safe-Error Analysis of Post-Quantum Cryptography Mechanisms To cite this version : HAL Id : hal-03330189," 2021.
[103] C. Mujdei, L. Wouters, A. Karmakar, A. Beckers, J. M. B. Mera, and I. Verbauwhede, "Side-Channel Analysis of Lattice-Based Post-Quantum Cryptography: Exploiting Polynomial Multiplication," *ACM Trans. Embed. Comput. Syst.*, 2022, doi: 10.1145/3569420.
[104] T. Fritzmann, M. Van Beirendonck, D. B. Roy, T. Schamberger, I. Verbauwhede, and G. Sigl, "Masked Accelerators and Instruction Set Extensions for Post-Quantum Cryptography," vol. 2022,

no. 1, pp. 414–460, 2022, doi: 10.46586/tches.v2022.i1.414-460.

[105] R. N. Pontaza Rodas, Y. D. Lin, S. L. Lu, and K. J. Chang, "O2MD^2: A New Post-Quantum Cryptosystem with One-to-Many Distributed Key Management Based on Prime Modulo Double Encapsulation," *IEEE Access*, vol. 9, pp. 109260–109288, 2021, doi: 10.1109/ACCESS.2021.3100551.

[106] C. T. M. Choi *et al.*, "Analysis of the applicability of artificial neural networks for the post-quantum cryptography algorithms development Analysis of the applicability of artificial neural networks for the post-quantum cryptography algorithms development", doi: 10.1088/1742-6596/2032/1/012026.