New Trends for Securing Cybersecurity Data

Saba Alaa Abdulwahhab Qasim Mohammed Hussien Emad F. Taha

Department of Computer Science, Tikrit University, Iraq

International Islamic University Malysia

saba.a.abdalwahab35529@st.tu.edu.iq kasimalshamry@tu.edu.iq imadf@iium.edu.my

Abstract

After most of the data has become widely transmitted in digital devices, which affects the security of this data due to a large number of hackers, and to protect it, encryption is used as one of the reliable methods to ensure data security. The important condition of the encryption system depended on time, amount of data, and cost of encryption.

However, the development in computational capabilities led to the thinking of a new type of cryptography is called quantum cryptography (QC), it is a technology that allows for quicker, more effective, and secure communication than the traditional way. so the term post-quantum cryptography (PQC) refers to the usage of a cryptographic method that is thought to be immune to quantum assaults. as a result, Quantum-era cybersecurity will be capable of detecting and deflecting quantum-era cyberattacks before they do harm using the most efficient algorithm, the study goal is to highlight developments in cryptography systems and compare them in time execution using the same amount of data.

Keywords: Cryptography**,** Quantum cryptography, Post Quantum cryptography, Classical cryptography, cybersecurity.

الاتجاهات الجديدة لتأمين بيانات الأمن السيبراني

صبا علاء عبدالوهاب قاسم محمد حسين عماد فخري طه

قسم علوم الحاسوب ، جامعة تكريت ، العراق الجامعة الإسلامية العالمية ماليزيا – ماليزيا

الخلاصة

بعد أن أصبحت معظم البيانات تنتقل على نطاق واسع في الأجهزة الرقمية ، مما يؤثر على أمن هذه البيانات بسبب كثرة المتسللين ، ولحمايتها ، يتم استخدام التشفير كإحدى الطرق الموثوقة لضمان أمن البيانات. تعتمد الحالة المهمة لنظام التشفير على الوقت وكمية البيانات وتكلفة التشفير .ومع ذلك ، أدى التطور في القدرات الحسابية إلى التفكير في نوع جديد من التشفير يسمى التشفير الكمي (QC) ، وهي تقنية تسمح باتصال أسرع وأكثر فعالية وأمانًا من الطريقة التقليدية. لذا فإن مصطلح تشفير ما بعد الكم (PQC) يشير إلى استخدام طريقة تشفير يُعتقد أنها محصنة ضد الهجمات الكمية. وعليه ، سيكون الأمن السيبراني في العصر الكمي قادرًا على اكتشاف وتحويل الهجمات الإلكترونية في الحقبة الكمية قبل أن تتسبب في ضرر باستخدام الخوارزمية الأكثر كفاءة ، فالهدف من الدراسة هو تسليط الضوء على التطورات في أنظمة التشفير ومقارنتها مع بعضها في التنفيذ الزمني باستخدام نفس المقدار من بيانات .

الكلمات المفتاحية: التشفير ، التشفير الكمي ، التشفير اللاحق للكم ، التشفير الكلاسيكي ، الأمن السيبراني.

1. Introduction

The art and science of ensuring security by encrypting communications to make them legible are known as cryptography. The rapid advancement of networking technologies has resulted in a highly widespread culture for data exchange. As a result, it is more vulnerable to data duplication and re-distribution by hackers. Therefore the information must be safeguarded while being sent. Credit cards, financial transactions, and social security numbers are all examples of sensitive information that must be safeguarded.[1].

The aim of cryptography is confidentiality, integrity, availability, authenticity[7].

The process of encryption and decryption depends solely on a single key which is known as symmetric-key cryptography, this key is used for encryption and decryption [2]. Others are dependent on using two keys one called the public key and the private key called the asymmetric-key [3].

Before the invention of the Quantum Computer, several cryptographic methods were developed based on an understanding of number theory; this whole pre-Quantum Cryptographic era is founded on two basic mathematical concepts. Discrete Logarithmic Problem, Factoring Problem[4]. After that Quantum computer research and development have been active in recent years all over the world [5],

We conclude perfect information security cannot be guaranteed in current cryptography. Because most of the data on the internet is vulnerable to quantum computer attacks[6].

In this paper, we investigate the previous, current cryptography, and future cryptography, then compare between algorithm, in Arithmetic ability data and execution time, the amount of data, unlike the rest of the previous studies that they discussed individually. As a result of these reasons mentioned above, we need this new cryptography called post-quantum cryptography (PQC) as soon as possible, The rest of the sections contain, a literature review of previous work, different methods in classical, risk on the broken system, new Trends that proposed, advantages and disadvantages of quantum cryptography, the Step of post-quantum system, finally quantum system and conclusion.

2. Literature Review

Many works and studies are investigated and related with this paper discussing the most important parameter of cryptography, compare between them, because of new advances in the field of cryptography, Kan and Une in 2021 discuss contemporary trends in quantum computer research and development, as well as the security dangers of public-key cryptography methods [5]. Sann, Soe et al in 2019 compare the outcomes of various methods in terms of encryption time, decryption time, and memory use over variable file sizes. In addition to all past and ongoing advances [8], Bhardwaj and Som in 2016 writers provide a history of all data concealing techniques employed throughout history, as well as how these techniques developed from Caesar cipher through DES, Triple-DES, AES, and contemporary algorithms [9]. Mitali and Sharma in 2014 undertake a study of some of the more prominent and intriguing cryptographic algorithms that are currently in use, as well as examined their benefits and drawbacks [1].

Lakshmi and Murali in 2017 compare classically and Quantum Cryptography utilizing several cryptographic algorithms to find the best method in classical or quantum cryptography. Predominantly, post-quantum state-of-the-art is built on related problems [10], Portmann and Renner in

2021 They go through the concept of security, with a focus on quantum key distribution and secure communication [11].

Borges, Reis et al. in 2020 the goal of their study is to offer an evaluation of security and performance for the sorts of cryptographic systems declared secure against quantum attacks in the second round of the NIST Post-Quantum Standardization Process [12]. Stigsson in 2018 suggest their extraction of knowledge a taxonomy of 31 algorithms. Each algorithm is divided into several categories [13].

3. Different Methods in Classical

In this section, we survey traditional algorithms such as AES, DES, RSA, and Elliptic curve algorithms and compare them based on basic features such as key size, block size, and the number of rounds required to encrypt or decrypt data by those algorithms, but before comparison, most of the study divided the cryptography into two main types of algorithm Symmetric Key Cryptography (SKC), we choice [AES, DES] for our study which is used one key called secret key this type of encryption is faster and difficult to attack. And asymmetric Key Cryptography (AKC), we chose [RSA, ECC] for our study which is used with two different keys (public, private) as the revised study that depended on these types of encryption is increasing security and rendered less vulnerable to infiltration, finally, blew we summarize cryptanalysis techniques capable of compromising the security of choosing algorithms based on several studies [3, 14-16][1, 15-18].

Table (1) Comparison between choosing algorithm.

Algorithm Choosing	processing capacity	Average time in ms	Attack
AES	2^{128} 2^{192} 2^{256}	542.38	A side-channel attack is possible
DES	2^{56}	663.31	Brute force attacks are possible. Linear cryptanalysis and plain text knowledge
RAS	2^{1024} to 2^{4096}	110	Using random probability theory and side-channel attacks, to decrypt the data.
ECC	2^{155}	1.3	Side-channel attacks are possible

4. Risk on the Broken System

When a quantum computer becomes accessible, Shor's algorithm will pose a security threat to all classical cryptography protocols. Following Shor's algorithm and Grover's search method, research in quantum computing increased[19], even there are currently no known mathematical shortcuts to these methods, which means that every feasible combination (or brute force) must be evaluated to obtain the key number that will unlock the algorithm [20]. So Information in a quantum system cannot be copied (Nocloning Theorem) or read by an unauthorized party[19]. As a result without quantum-resistance encryption, confidence in information systems that manage vital information will be unattainable shortly [21].

5. The Workflow Of the system

If Alice wishes to transmit a message to Bob, she will need to use two communication channels, the quantum channel and the classical channel,. a 20-qubit register could simultaneously hold a million values (2^{20} = 1,048,576) while four classical bits generally represented 2^4as for or 16 bits [24], as a result, A normal quantum will be 10,000 times faster than classical[25]. Also, Quantum Protocol must be correct, secure, and robust. Correction and security are the key concerns of the traditional protocol. [19].

as illustrated in figure 3 shows the process of transmission needs to work together with classic algorithms work with their keys as well as their transport channels along with post-quantum and their key using a combined function to make System compatibility.

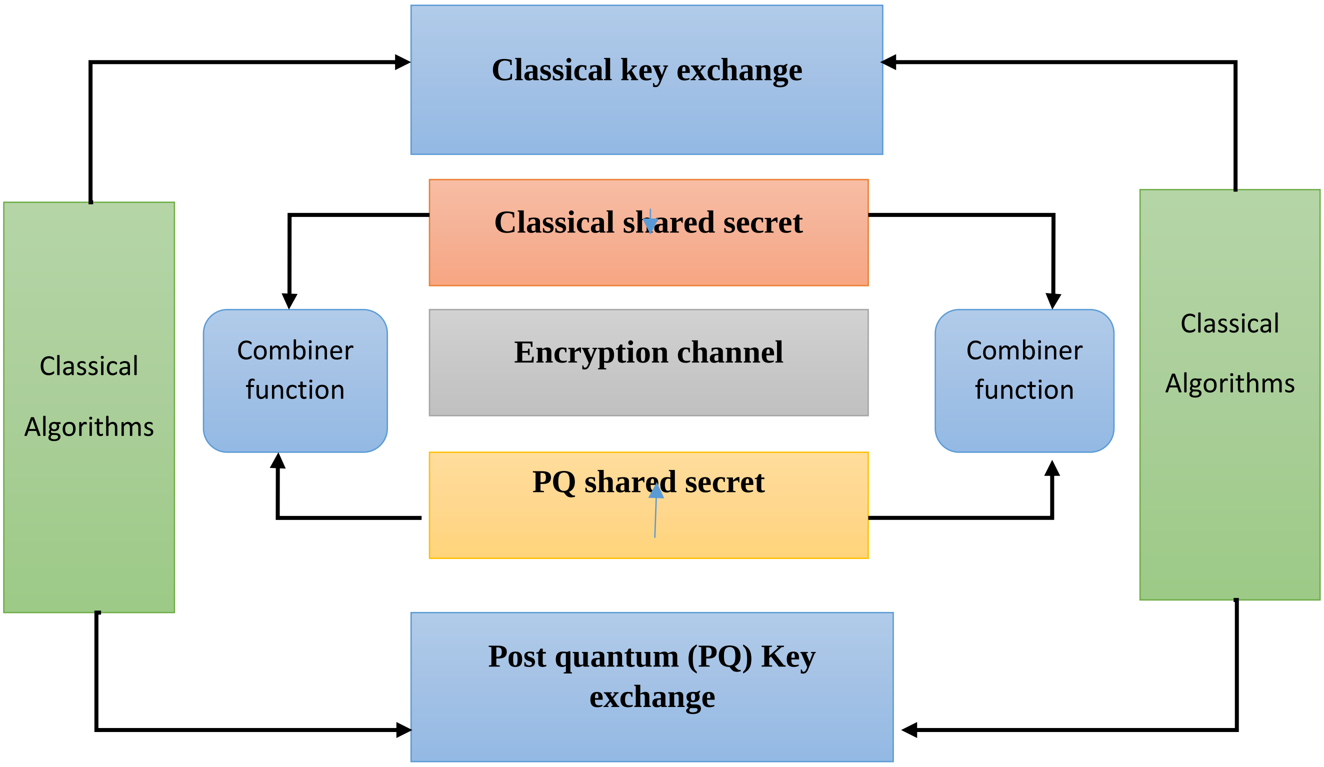

Figure (2) Workflow of Post-Quantum[34].

6. Quantum Computing and Cryptography

Quantum computing is a field that combines concepts from classical information theory, computer science, and quantum physics [23]. The strength of quantum computing derives, in theory, from parallel computing that makes use of three features of quantum states: superposition, entanglement, and interference. By monitoring the states, the computing process manipulates quantum states and acquires required information. In quantum computers, a quantum bit (qubit) denotes the quantum state that corresponds to the fundamental unit of information[5][25], so the advent of large-scale quantum computers will result in a significant reduction in the security of the most previous algorithm[5, 26]

Quantum cryptography uses quantum physics concepts to protect information processing [11]. The quantum system is built on the dispersion of single particles or photons, and the polarization of a photon encodes the value of a classical bit[6]. As a result, The majority of the studies in quantum cryptography are centered on quantum key distribution[23], the advantage of quantum cryptography is presented as 100% a completely safe cryptographic technology, it is considered difficult to crack [27]. in Table 2 summary a Comparative between quantum and classical cryptography.

Table (2) Comparative of Quantum Cryptography with Classical Cryptography

Ref	principle	Quantum	classical
[10]	Theory	Depended on physics	Depended on mathematic
[29]	computation	High arithmetic capabilities	Low computational capabilities compared to quantum computers
[30]	security	It is very safe because it uses the properties of quantum physics	There is no guarantee of its safety due to the presence of quantum computers
[31]	Data	Treat data as Q-bit	Treat data as a bit

7. Post-Quantum Cryptography (PQC)

From 2017 until 2020 NIST tried to make Standardization of post-quantum cryptography by choosing the most efficient algorithm this round one, two, and finally round three [32][28, 33],

So Post-quantum cryptography refers to any kind of cryptography, classical or quantum, that can withstand quantum computer assaults [23].is still based on developing conventional cryptography methods that are difficult for a quantum computer to crack. Although the history of such evaluation is short, in this section, we describe the basic methodology for evaluating PQC algorithms by their problems [11]. PQC can be classified into different fields of study with hug different algorithms, first lattice-based cryptography with algorithm e.g. Crystal-kayber, NTRU, and Saber[5], second is code-based cryptography with algorithm e.g. LEDAcrypt, RQC, then third multivariate cryptography with a Rainbow algorithm[28], forth Isogeny-based cryptography with algorithm e.g. SIKE, finally hash-based cryptography with algorithm e.g. SPHINCS, depending on mathematical problems, it could take more than 10 years to complete the migration in case of this new system [5], In table 3 shows the most efficient algorithms in post-quantum round3 depend on lattice base comparative with key generation and timely execution of these algorithms.

Table (3) Efficient algorithms in postquantum round3

Algorithm	Key Generation	Average Time in Ms
KYBER	512 , 768, 1024	90
SABER	519, 943, 1531	33.8 , 35.3 , 42.1
NTRU	443 , 743	25.9 , 39.7

8. Calculation of ability

We note that in classical computers, it takes years to solve a specific problem, unlike quantum computers, which greatly shorten time compared to a classical computer, In Table 2 presents the needed time required for Exhaustive Key it is the main reason to create a quantum computer Due to its high arithmetic abilities that can solve hard problems as fast as we can imagine using a quantum computer the way of this calculation is Calculate the number of keys raised to the power of the number of bits if we have 32 bit then 2^{32}

After that divided by 10^{6} the result is divided by 60 to get 35.8 minutes, 35.8 to convert in 10^{6} Decryptions/μs it also needs to multiply by 60 and then divided by 10^{3} to get 2.15 milliseconds The operations are repeated in 56,128,165 bits .

Table (4) Arithmetic abilities on classical computer [22]

Key Size in (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years

And now the same capabilities are calculated but using quantum computers that use qubits, where first we convert the bits to Q-bits and then perform the same method as before to find the output In Table 5

Table (5) Arithmetic abilities on quantum computer

Key Size in(Q-bits)	Number of Alternative q-bit	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
$32=2^5$	5	16×10^4	96×10^8
$56=2^6$	6	5.33×10^6	32×10^8
$128=2^7$	7	6.67×10^6	6.4002×10^8
$168 = 2^8$	8	2.1333×10^6	1.28×10^8

9. Conclusion

The development of classical computers and the beginning of the era of quantum computers led to thinking about how to preserve data from any type of attack, with these quantum computers and with this huge amount of data led to the emergence of a new generation of cryptography which is quantum cryptography (QC) and post-quantum cryptography (PQC). In this paper, we survey the previous concepts of cryptography with the current and the future trends of this cryptography as we reviewed, and made a comparison with these cryptography systems. Then we study how to calculate the ability of this cryptography, with a focus on the advantages and disadvantages that we face during time and cost, amount of data in this cryptography, Prove that quantum computers have incredibly shortened time, Compared with classical computers at the same time and amount of data

Reference

1. V. K. Mitali and A. Sharma, "A survey on various cryptography techniques," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, pp. 307-312, 2014.
2. O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, pp. 495-516, 2018.
3. B. Mandal, S. Chandra, S. S. Alam, and S. S. Patra, "A comparative and analytical study on symmetric-key cryptography," in *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 2014, pp. 131-136.
4. S. Bhattacharyya and A. Chakrabarti, "POST QUANTUM CRYPTOGRAPHY A brief survey of classical cryptosystems, their fallacy and the advent of post-quantum cryptography with the deep insight into hashed based signature scheme."
5. K. Kan and M. Une, "Recent Trends on Research and Development of Quantum Computers and

Standardization of Post-Quantum Cryptography," Institute for Monetary and Economic Studies, Bank of Japan2021.

6. M. S. Sharbaf, "Quantum cryptography: An emerging technology in network security," in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, 2011, pp. 13-19.
7. Dr. Abdul Monem S.Rahma and Dr. Qasim Mohammed Hussein , "A New Attack on NTRU Public Key Cryptosystem Depend on Using Public Key and Public Information" , Eng.& Tech. Journal, Vol.28, No.6, (2010).
8. Z. Sann, T. Soe, K. Knin, and Z. Win, "Performance comparison of asymmetric cryptography (case study-mail message)," *APTIKOM Journal on Computer Science and Information Technologies*, vol. 4, pp. 105-111, 2019.
9. A. Bhardwaj and S. Som, "Study of different cryptographic technique and challenges in future," in *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, 2016, pp. 208-212.
10. P. S. Lakshmi and G. Murali, "Comparison of classical and quantum cryptography using QKD simulator," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2017, pp. 3543-3547.
11. C. Portmann and R. Renner, "Security in quantum cryptography," *arXiv preprint arXiv:2102.00021*, 2021.
12. F. Borges, P. R. Reis, and D. Pereira, "A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography," *IEEE Access*, vol. 8, pp. 142413-142422, 2020.
13. A. Stigsson, "A Taxonomy of Quantum Algorithms-The core ideas of existing quantum algorithms and their implications on cryptography," 2018.
14. V. Kannan, S. JHAJHARIA, and D. S. VERMA, "Review and Recent Trends in Cryptography," *International Journal of Scientific Engineering and Technology Research*, vol. 3, pp. 4450-4455, 2014.
15. N. Arora and Y. Gigras, "Block and Stream Cipher Based Cryptographic Algorithms: A Survey," *International Journal of Information and Computation Technology*, vol. 4, pp. 189-196, 2014.
16. N. Jirwan, A. Singh, and S. Vijay, "Review and analysis of cryptography techniques," *International Journal of Scientific & Engineering Research*, vol. 4, pp. 1-6, 2013.
17. M. N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish for guessing attacks prevention," *Journal Computer Science Applications and Information Technology*, vol. 3, pp. 1-7, 2018.
18. D. Cheung, D. Maslov, J. Mathew, and D. K. Pradhan, "On the design and optimization of a quantum polynomial-time attack on elliptic curve cryptography," in *Workshop on Quantum Computation, Communication, and Cryptography*, 2008, pp. 96-104.
19. A. Kumar and S. Garhwal, "State-of-the-Art Survey of Quantum Cryptography," *Archives of Computational Methods in Engineering*, pp. 1-38, 2021.
20. L. O'Connor, C. Dukatz, L. DiValentin, and N. Farhady, "Cryptography in a post-quantum world: preparing intelligent

enterprises now for a secure future. Accenture Labs," ed, 2018.

21. K. Isirova and O. Potii, "Requirements and Security Models for Post-Quantum Cryptography Analysis," in *Proceedings of the PhD Symposium at 13th International Conference on ICT in Education, Research, and Industrial Applications co-located with 13th International Conference on ICT in Education, Research, and Industrial Applications (ICTERI 2017)*, 2017, pp. 36-41.
22. A. Kahate, *Cryptography and network security*: Tata McGraw-Hill Education, 2013.
23. D. Alvarez and Y. Kim, "Survey of the Development of Quantum Cryptography and Its Applications," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, pp. 1074-1080.
24. C. Ugwuishiwu, U. Orji, C. Ugwu, and C. Asogwa, "An overview of Quantum Cryptography and Shor's Algorithm," *Int. J. Adv. Trends Comput. Sci. Eng*, vol. 9, 2020.
25. J. Kaur and R. K. KR, "The Recent Trends in CyberSecurity: A Review," *Journal of King Saud University-Computer and Information Sciences*, 2021.
26. N. Shinohara and S. Moriai, "Trends in Post-Quantum Cryptography: Cryptosystems for the Quantum Computing Era," *the magazine of New Breeze, PP*, pp. 9-11, 2019.
27. E. GÜMÜŞ, G. Z. Aydin, and M. A. Aydin, "Quantum cryptography and comparison of quantum key distribution protocols," *IU-Journal of Electrical & Electronics Engineering*, vol. 8, pp. 503-510, 2012.
28. G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, *et al.*, "Status report on the second round of the NIST post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2020.
29. S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," in *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, 2017, pp. 1-7.
30. https://quantumxc.com/blog/quantum-cryptography-explained/.
31. https://semiengineering.com/the-great-quantum-computing-race/.
32. G. Alagic, G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, *et al.*, *Status report on the first round of the NIST post-quantum cryptography standardization process*: US Department of Commerce, National Institute of Standards and Technology …, 2019.
33. M. Imran, Z. U. Abideen, and S. Pagliarini, "An experimental study of building blocks of lattice-based nist post-quantum cryptographic algorithms," *Electronics*, vol. 9, p. 1953, 2020.
34. https://www.entrust.com/resources/certificate-solutions/learn/post-quantum-cryptography.