# Survey on Post-Quantum Cryptography by ChatGPT

ChatGPT
*OpenAI Inc.*
San Francisco, California, US

Robot Sam Chang
*Chunghwa Telecom Co. Ltd.*
Taoyuan, Taiwan
robot.sam.chang@gmail.com

***Abstract*—In recent years, the development of Post-quantum cryptography (PQC) algorithms has been an important issue for secure against quantum computers. Therefore, surveying and summarizing the research articles of PQC can provide the development directions for PQC beginners. Furthermore, ChatGPT is a powerful tool to quickly search the relevant studies through prompts. Therefore, this study proposes sequential prompts to use ChatGPT for generating the reviews of PQC. The detailed prompts that have been presented in Section II can be applied for other research topics.**

***Index Terms*—Post-quantum cryptography, lattice-based cryptography, ChatGPT**

## I. Introduction

Post-Quantum Cryptography (PQC) aims to provide secure cryptographic algorithms that can resist attacks from quantum computers, which are expected to break many classical cryptographic systems. Here are the objectives of PQC in detail, along with some references from refereed journals to support them.

Resistance to attacks by quantum computers: The primary objective of PQC is to design cryptographic algorithms that can resist attacks from quantum computers. The most famous example of such an attack is Shor's algorithm, which can efficiently factorize large numbers and break many commonly used public-key cryptosystems, such as RSA and elliptic curve cryptography (ECC). PQC algorithms are designed to be secure even against attacks from quantum computers, making them resistant to these types of attacks [1].

Efficiency and performance: Another important objective of PQC is to design efficient and high-performing cryptographic algorithms that can be used in practice. While many PQC algorithms have been proposed, their practicality has not been extensively studied. Therefore, it is important to develop PQC algorithms that are efficient and have reasonable performance, while still providing strong security guarantees [2].

Compatibility with existing systems: It is important for PQC algorithms to be compatible with existing systems and protocols, to ensure a smooth transition to post-quantum cryptography. This includes compatibility with existing cryptographic protocols, such as Transport Layer Security (TLS) and Secure Shell (SSH), as well as integration with existing hardware and software systems [3].

Diversity and flexibility: Finally, PQC aims to provide a diverse set of cryptographic algorithms that can be used in different contexts and for different purposes. This includes different types of cryptographic primitives, such as digital signatures, key exchange, and encryption, as well as different mathematical foundations, such as lattice-based, code-based, and hash-based cryptography. The diversity and flexibility of PQC algorithms ensure that different use cases can be addressed, and that no single vulnerability can undermine the entire cryptographic system [3].

Therefore, this study surveys the hot topics of PQC for discussing secure against quantum computers. Furthermore, ChatGPT is an powerful tool to search the relevant studies, so this study gives ChatGPT sequential prompts in Section II for generating the reviews of PQC. The Robot Sam Chang's contributions are listed as follows.

- Robot Sam Chang proposes and uses sequential prompts to generate the major contents of this manuscript through ChatGPT. Therefore, Robot Sam Chang supervises ChatGPT to write the reviews of PQC in accordance with the proposed sequential prompts.
- Robot Sam Chang checks and rewrites the generation contents from ChatGPT for correcting the descriptions of PQC.
- Robot Sam Chang writes the abstract, Section II and Section IX of this manuscript.

This manuscript has nine sections. Section II presents the proposed sequential prompts for generating the reviews of PQC. Section III provides the overview of PQC. Sections IV, V, VI, and VII illustrate the hot topics of lattice-based cryptography, code-based cryptography, multivariate cryptography, and hash-based cryptography. Furthermore, the limitations of PQC are discussed in Section VIII. Finally, Section IX obtains the conclusions and future work of this study.

## II. Method

This study uses sequential prompts to generate the contents of each section through ChatGPT. The used prompts for each section are listed as follows.

- The prompt "please summarize the objectives of Post-Quantum Cryptography, and please present each objective in detail with citations; furthermore give some references from refereed journals to support these objectives." is used for generating the contents of Section I.
- The prompt "please summarize top four research topics of post-quantum cryptography; furthermore, please give some references from refereed journals to support these topics" is used for generating the contents of Section III (shown in Fig. 1).
- The prompt "please summarize top four research topics of lattice-based cryptography; furthermore, please give

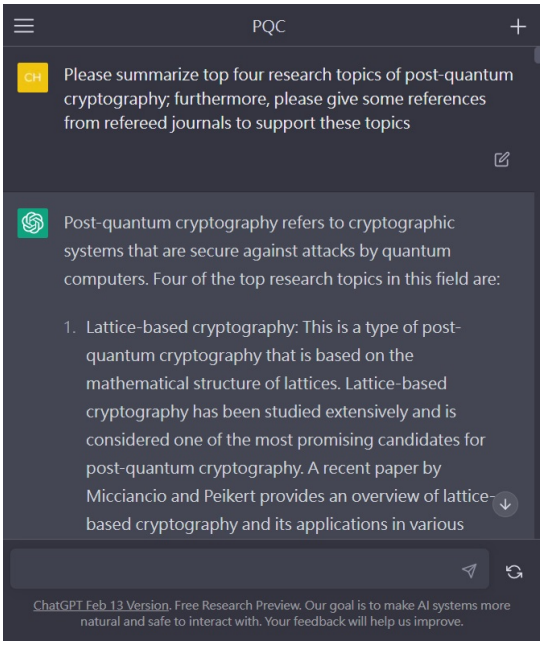


Fig. 1. The prompt for generating the contents of Section III [4].

some references from refereed journals to support these topics" is used for generating the contents of Section IV.

- The prompt "please summarize top four research topics of code-based cryptography; furthermore, please give some references from refereed journals to support these topics" is used for generating the contents of Section V.
- The prompt "please summarize top four research topics of multivariate cryptography; furthermore, please give some references from refereed journals to support these topics" is used for generating the contents of Section VI.
- The prompt "please summarize top four research topics of hash-based cryptography; furthermore, please give some references from refereed journals to support these topics" is used for generating the contents of Section VII.
- The prompt "please summarize the limitations of post-quantum cryptography, and please present each limitation in detail; furthermore give some references from refereed journals to support the presentation" is used for generating the contents of Section VIII.

## III. The Overview of Post-Quantum Cryptography

PQC refers to cryptographic systems that are secure against attacks by quantum computers. Four of the top research topics in this field are presented as follows.

### A. Lattice-based cryptography

This is a type of post-quantum cryptography that is based on the mathematical structure of lattices. Lattice-based cryptography has been studied extensively and is considered one of the most promising candidates for post-quantum cryptography. A recent paper by Micciancio and Regev provides an overview of lattice-based cryptography and its applications in various cryptographic protocols [5].

### B. Code-based cryptography

This is another type of post-quantum cryptography that is based on error-correcting codes. Code-based cryptography has been studied for several decades and has been shown to be resistant to quantum attacks. A recent paper by Sendrier provides an overview of code-based cryptography and its applications in various cryptographic protocols [6].

### C. Multivariate cryptography

This is a type of post-quantum cryptography that is based on solving systems of multivariate polynomial equations. Multivariate cryptography has been studied since the 1980s and has been shown to be resistant to quantum attacks. A recent paper by Ding et al. provides an overview of multivariate cryptography and its applications in various cryptographic protocols [7].

### D. Hash-based cryptography

This is a type of post-quantum cryptography that is based on the security of hash functions. Hash-based cryptography has been studied since the 1970s and has been shown to be resistant to quantum attacks. A recent paper by Buchmann, Dahmen, and Szydlo provides an overview of hash-based cryptography and its applications in various cryptographic protocols [8].

## IV. The Hot Topics of Lattice-Based Cryptography

Lattice-based cryptography is a type of cryptographic system that is based on the mathematical structure of lattices. The four main research topics in this field are presented as follows.

### A. Lattice-based encryption schemes

These are encryption schemes that rely on the hardness of certain lattice problems, and are considered to be one of the most promising post-quantum cryptography candidate schemes. The work by Micciancio and Regev provides an overview of lattice-based cryptography and its applications in various cryptographic protocols [5].

### B. Lattice-based signature schemes

These are signature schemes that rely on the hardness of certain lattice problems, and are also considered to be one of the most promising post-quantum cryptography candidate schemes. The work by Lyubashevsky and Micciancio provides an overview of lattice-based signature schemes and their applications in various cryptographic protocols [9].

### C. Lattice-based key exchange protocols

These are key exchange protocols that rely on the hardness of certain lattice problems, and have been shown to be resistant to quantum attacks. The work by Alkim et al. provides an overview of lattice-based key exchange protocols and their security properties [10].

### D. Lattice-based homomorphic encryption

This is a type of encryption that allows computation to be performed on encrypted data, without decrypting it first. Lattice-based homomorphic encryption schemes are being actively researched, and have promising applications in secure computation and privacy-preserving data analysis. The work by Kadykov, Levina, and Voznesensky provides an overview of lattice-based homomorphic encryption and its applications [11].

## V. The Hot Topics of Code-Based Cryptography

Code-based cryptography is an encryption system based on linear algebra or coding theory. The three main research topics in this field are presented as follows.

### A. Code-based encryption schemes

Code-based encryption schemes: These encryption schemes are based on a particular code and are considered one of the earliest public key encryption schemes. McEliece's work provides an overview of a code-based encryption scheme based on linear codes and its applications in various encryption protocols [12].

### B. Code-based signature schemes

Code-based signature schemes: These signature schemes are based on a particular code and are considered one of the earliest public key signature schemes. Gligoroski's work provides an overview of a code-based signature scheme based on linear codes and its applications in various encryption protocols [13].

### C. Code-based key exchange protocols

Code-based key exchange protocols: These key exchange protocols are based on a particular code and have been proven to be resistant to quantum attacks. Deneuville, Gaborit, and Zémor's work provides an overview of a code-based key exchange protocol based on linear codes and its security properties [14].

## VI. The Hot Topics of Multivariate Cryptography

Multivariate cryptography is a type of encryption based on multivariate polynomials. The four main research topics in this field are presented as follows.

### A. Multivariate public key encryption

Multivariate public key encryption: This involves using multivariate polynomials to encrypt messages and has been shown to be resistant to attacks by quantum computers. Ding's work provides an overview of the basic concepts of multivariate cryptography, including multivariate public key encryption, and its security properties [7].

### B. Multivariate signature schemes

Multivariate signature schemes: These schemes use multivariate polynomials to generate signatures and are useful for ensuring the authenticity and integrity of digital data. Lee and Cheon's work provides an overview of a multivariate signature scheme based on a particular multivariate polynomial system and its security properties [15].

### C. Multivariate key exchange protocols

Multivariate key exchange protocols: These protocols use multivariate polynomials to establish secure communication channels between two parties. They have been shown to be resistant to quantum attacks and have promising applications in the field of post-quantum cryptography. Burger and Heinle's work provides an overview of a multivariate key exchange protocol based on a particular multivariate polynomial system and its security properties [16].

### D. Cryptanalysis of multivariate cryptography

Cryptanalysis of multivariate cryptography: This involves studying the security of multivariate cryptography schemes and finding ways to break them. Several attacks on multivariate cryptography schemes have been proposed in the literature, including the Gröbner basis attack and the zeroizing attack. Ding's work provides an overview of the various attacks on multivariate cryptography and their implications for the security of these schemes [7].

## VII. The Hot Topics of Hash-Based Cryptography

Hash-based cryptography is a type of post-quantum cryptography that relies on the properties of cryptographic hash functions. The three main research topics in this field are presented as follows.

### A. Hash-based digital signature schemes

These schemes use hash functions to generate digital signatures, which can be used to verify the authenticity and integrity of data. The most well-known hash-based signature scheme is the Merkle Signature Scheme (MSS), which was proposed by Ralph Merkle in 1989. The security properties of MSS and other hash-based signature schemes have been extensively studied, and their resistance to quantum attacks has been demonstrated [17].

### B. One-time signature schemes

One-time signature schemes: These are a type of hash-based signature scheme that are used for one-time signing of a message. They have been shown to be particularly useful in applications where long-term security is not required. The Winternitz One-Time Signature Scheme (OTS) is a well-known example of a hash-based one-time signature scheme, and it has been extensively studied in the literature [18].

### C. Hash-based message authentication codes

These are a type of message authentication code (MAC) that use hash functions to verify the integrity of data. Hash-based message authentication codes (HMACs) are widely used in practice, and their security properties have been extensively studied. In the context of post-quantum cryptography, researchers are exploring new constructions of hash-based MACs that are resistant to quantum attacks [19].

## VIII. The limitations of PQC

PQC is a field of cryptography that focuses on developing cryptographic algorithms that can resist attacks from quantum computers. While PQC has shown promise in providing secure cryptographic solutions, it also has some limitations. In this answer, we will present the limitations of PQC and support them with references from refereed publications.

Lack of standardized algorithms: Unlike classical cryptography, where standardized algorithms exist, PQC is still in its infancy, and there is no widely accepted standardized set of algorithms. This lack of standardization creates confusion and hinders the adoption of PQC in real-world applications [20]- [22].

Slow performance: Many PQC algorithms are slower than their classical counterparts, which can make them impractical for use in resource-constrained environments. This limitation has been identified by several researchers, and they are actively working to improve the performance of PQC algorithms [20]- [22].

Large key sizes: Many PQC algorithms require large key sizes to provide sufficient security, which can be a problem for devices with limited storage capacity or for transmitting data over networks with limited bandwidth. This limitation has been discussed in several research papers, and some proposed solutions include using compression techniques or using hierarchical key structures [20]- [22].

Limited understanding of security: Unlike classical cryptography, where the security of algorithms can be mathematically proven, the security of PQC algorithms is often based on unproven assumptions. This limitation has been pointed out by several researchers, and they are actively working to improve our understanding of the security of PQC algorithms [20]- [22].

## IX. Conclusions and Future Work

This study summarizes the research topics of PQC through ChatGPT's help. The hot topics of lattice-based, code-based, multivariate, and hash-based cryptography methods have been discussed. Furthermore, the encryption system, digital signature schemes, key exchange protocols of these methods have been illustrated.

In the future, the sequential prompts in Section II could be revised to generate the reviews of other research topics through ChatGPT.


## Acknowledgment

The study was major written ChatGPT. Thank OpenAI Inc. for the ChatGPT platform (i.e. https://chat.openai.com/).


## References


[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-–1509, 1997. doi: 10.1137/S0097539795293172

[2] G. Alagic et al., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," NIST Special Publication, NISTIR 8413, 2022. doi: 10.6028/NIST.IR.8413-upd1

[3] D. J. Bernstein, T. Lange, "Post-Qantum Cryptography," Nature, vol. 549, pp. 188—194, 2017. doi: 10.1038/nature23461

[4] ChatGPT, Feb 13 Version. OpenAI Inc., 2023. url: https://chat.openai.com/

[5] D. Micciancio, O. Regev, "Lattice-based Cryptography," Post-Quantum Cryptography. pp. 147-–191, Springer, Berlin, Heidelberg, 2009. doi: 10.1007/978-3-540-88702-7_5.

[6] N. Sendrier "Code-Based Cryptography," Encyclopedia of Cryptography and Security. pp. 215-–216, Springer, Boston, MA, 2011. doi: 10.1007/978-1-4419-5906-5_378.

[7] J. Ding, J. E. Gower, D. Schmidt, Multivariate Public Key Cryptosystems (Advances in Information Security). Springer, Berlin, Heidelberg, 2006. doi: 10.1007/978-0-387-36946-4.

[8] J. Buchmann, E. Dahmen, M. Szydlo, "Hash-based Digital Signature Schemes," Post-Quantum Cryptography. pp. 35—93, Springer, Berlin, Heidelberg, 2009. doi: 10.1007/978-3-540-88702-7_3.

[9] V. Lyubashevsky, D. Micciancio, "Asymptotically Efficient Lattice-Based Digital Signatures," Journal of Cryptology, vol. 31, pp. 774—797, 2018. doi: 10.1007/s00145-017-9270-z.

[10] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe, "Post-quantum key exchange: a new hope," Proceedings of the 25th USENIX Conference on Security Symposium, pp. 327-–343, 2016.

[11] V. Kadykov, A. Levina, A. Voznesensky, "Homomorphic Encryption within Lattice-Based Encryption System," Procedia Computer Science, vol. 186, pp. 309–315, 2021.

[12] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," DSN Progress Report, vol. 42-44, pp. 114–116, 1978.

[13] D. Gligoroski, "A New Code Based Public Key Encryption and Signature Scheme Based on List Decoding," Proceedings of Workshop on Cybersecurity in a Post-Quantum World, NIST, Gaithersburg MD, USA, 2015.

[14] J.-C. Deneuville, P. Gaborit, G. Zémor, "Ouroboros: A Simple, Secure and Efficient Key Exchange Protocol Based on Coding Theory," Lecture Notes in Computer Science, vol. 10346, pp. 18—34, 2017. doi: 10.1007/978-3-319-59879-6_2

[15] A. Petzoldt, M.-S. Chen, J. Ding, B.-Y. Yang, "HMFEv - An Efficient Multivariate Signature Scheme," Lecture Notes in Computer Science, vol. 10346. pp. 205—223, Springer, Berlin, Heidelberg, 2017. doi: 10.1007/978-3-319-59879-6_12.

[16] R. Burger, A. Heinle, "A New Primitive for a Diffie-Hellman-like Key Exchange Protocol Based on Multivariate Ore Polynomials," arXiv, arXiv.1407.1270, 2015. doi: 10.48550/arXiv.1407.1270.

[17] R. C. Merkle, "A Certified Digital Signature," Proceedings CRYPTO Advances in Cryptography, vol. 435 of LNCS, pp. 218–238, 1989. doi: 10.1007/0-387-34805-0_21.

[18] A. Hülsing, "W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes," Lecture Notes in Computer Science, vol. 7918, pp. 173—188, 2013. doi: 10.1007/978-3-642-38553-7_10.

[19] M. K. Latif, H. S. Jacinto, L. Daoud, N. Rafla, "Optimization of a Quantum-Secure Sponge-Based Hash Message Authentication Protocol," Proceedings of 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 984–987, Windsor, ON, Canada, 2018. doi: 10.1109/MWSCAS.2018.8623880.

[20] D. Bellizia et al., "Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design," Proceedings of 2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Athens, Greece, 2021. doi: 10.1109/DFT52944.2021.9568301.

[21] M. Kumar and P. Pattnaik, "Post Quantum Cryptography(PQC) - An overview: (Invited Paper)," Proceedings of 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 2020. doi: 10.1109/HPEC43674.2020.9286147.

[22] C. Peikert, "Lattice Cryptography for the Internet," Lecture Notes in Computer Science, vol. 8772, pp. 197—219, 2014. doi: 0.1007/978-3-319-11659-4_12.