Cryptography in the Post Quantum Computing World

Jigyas Sharma
EECS
University of Kansas
Lawerence, Kansas
engineer@ku.edu

***Abstract*—In the field of cybersecurity, cryptographic primitives have long stood as a barrier that prevents digital threats, safeguarding the information, integrity, and confidentiality. These cryptographic methods, however, were founded on the basis that their security is based on the computational limitations of classic computing. The emergent field of quantum computing, with its paradigm-shifting computational power, presents an unprecedented challenge to these established cryptographic practices. This survey paper dives into the current state of the advancing quantum computing capabilities and the foundational aspects of current cryptographic systems. We examine the vulnerabilities of widely used cryptographic algorithms, such as RSA and AES, under the quantum lens, particularly focusing on the disruptive potential of quantum algorithms like Shor's and Grover's. Furthermore, the paper explores the emerging field of post-quantum cryptography (PQC), which seeks to develop cryptographic systems resilient to quantum computational attacks. By analyzing various PQC approaches, including lattice-based, hash-based, and code-based cryptography, we assess their viability and challenges in the face of quantum advancements. This survey also sheds light on the ongoing standardization efforts and the pragmatic aspects of transitioning to quantum-resistant cryptographic systems. As quantum computing strides from theoretical constructs to practical machines, this paper aims to provide a comprehensive overview of the shifting landscape of cryptography, highlighting both the imminent challenges and the innovative strides in securing digital assets in the quantum era.**

I. Introduction : Overview of Cryptography and Quantum Computing

Cryptography has long been a vital tool in securing communication and protecting information from a range of adversarial threats, such as cyberattacks and unauthorized access, in the digital age. According to [1], the field employs sophisticated mathematical algorithms to transform readable data into secure formats, thereby ensuring its confidentiality and integrity. Traditional cryptographic techniques, such as symmetric-key encryption and public-key cryptography, have been the cornerstone of data security across a spectrum of applications, including internet communication and e-commerce.

The emergence of quantum computing marks a significant paradigm shifts in computational capabilities. Unlike classical computers, which process information in binary bits, quantum computers utilize qubits, as stated in [3]. This allows them to leverage the principles of quantum mechanics— primarily superposition and entanglement—to process information in ways profoundly different from classical computers. This leap in computational power not only holds immense potential for various fields but also poses a significant threat to the existing cryptographic protocols. This is primarily because most cryptographic primitives are predicated on the assumption that certain computations, such as factoring large integers, are infeasible for classical computing.

The purpose of this survey is to examine the impact of quantum computing on current cryptographic methods. We investigate the potential vulnerabilities of cryptographic primitives in the face of normalized quantum computing, exploring the likelihood and implications of such attacks. This paper aims to explore how quantum computing might drive changes in cryptographic practices, evaluate the current state of post-quantum cryptography, and discuss the challenges and future directions in developing quantum-resistant cryptographic solutions. This exploration is crucial in foreseeing and preparing for the evolving landscape of digital security in the quantum era.

II. Background and Fundamentals

A. Quantum Computing Basics

Before exploring the impact of quantum computing on cryptography, it is essential to understand its fundamental principles and how they differ from classical computing. This subsection will introduce the key concepts of quantum computing, such as qubits, superposition, entanglement, and quantum supremacy. Additionally, the differences between quantum and classical computing in processing information will be discussed to provide a clear understanding of computational power.

Superposition in quantum mechanics is the fundamental principle which allows wave-particle duality on a quantum level. This allows the qubits in quantum computing to achieve multiple states simultaneously. This allows the computational power to increase in quantum computing as qubits can process multiple possibilities at the same time. For instance, if you had two bits, in classical computation, you would have to compute 00, 01, 10, 11 at separate time units, however, the qubits can achieve all these states at once due to superposition. This capability grows exponentially as the number of bits increases.

According to [2], Entanglement at the quantum state is a physical phenomenon that occurs when pairs or groups of particles are generated, interact, or share spatial proximity in ways such that the quantum state of each particle instantly correlates with the state of the others, regardless of the distance that separates them. Therefore, entangled qubits can represent complex, interrelated information more efficiently than classical bits. Furthermore, entangled qubits are also essential for quantum error correction, where entangled qubits can help maintain coherence and reduce errors in computations conducted on a quantum level. However, maintenance of entanglement is often challenging over time

and distance. However, for the scope of this survey, we would consider a perfect quantum system.

Quantum supremacy is the term that garnered significant attention in quantum computing community. This is referred to as the point where quantum computers can perform tasks that are beyond the reach of the most powerful classical computers. This concept is not about universal superiority over classical computers but rather highlights specific problem domains where quantum computing's unique capabilities can be leveraged. For cryptography, "the relevance of quantum supremacy lies in its potential to break cryptographic algorithms that are currently considered secure[4]". As a result, quantum computers hold the potential to solve problems like large integer factorization and discrete logarithms—problems that form the backbone of many cryptographic algorithms—much more efficiently.

B. Foundations of Modern Cryptography

Modern Cryptography was founded on the basic principle that the computational complexity of any given input-output should be infeasible. This section aims to explore two primary types of cryptography primitives: symmetric-key cryptography, where the same key is used for encryption as well as decryption, and public-key cryptography, which employs a pair of keys, public key for encryption and private key for decryption.

Symmetric-key cryptography dates the earliest cipher to Caeser Ciphers, where letters in a message were shifted a certain number of places. With the rise and normalization of computers, the 1970s saw the development of the Data Encryption Standard which became the first widely adopted symmetric encryption system in the digital era. Concerns over the short key length of DES led to the development of more advanced techniques leading to the development of Advanced Encryption Standard. AES remains one of the most secure and widely used symmetric encryption algorithms. The foundation of the algorithm was to generate keys in a way that is random and unpredictable, to prevent the deduction of future keys. The keys also had to be long enough to prevent brute-force attacks.

Public-key cryptography was developed in 1976 when Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in their paper "New Directions in Cryptography[5]". This concept allowed secure communication without needing to share a key beforehand. In 1977, Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA algorithm, which was the first practical method for public key encryption and digital signatures. The foundational method for the encryption was using one-way mathematical functions. For example, "multiplication of two large prime numbers, which is easy to compute in one direction, however, difficult to reverse without the private key[6]".

III. Quantum Threat to Cryptography

In Section II.B, both the algorithms employed the foundational concept of computational infeasibility to achieve security. In the larger context, these concepts may need revision[7]. The increased computational capability and efficiency could render these algorithms useless.

Let's consider the public-key cryptography system, particularly, the RSA algorithm. The public key consists of two components, a modulus (N) and an encryption exponent (e). The private key consists of the component modulus (N) and a decryption exponent (d). The security of the algorithm is based on the difficulty of factoring the modulus N into its prime factors (p and q) because computing (d) given e, p and q is difficult.

In 1994, mathematician Peter Shor devised an algorithm that a quantum computer could use to factor large numbers exponentially faster than the best-known algorithms on classical computers. The algorithm operates in the realm of modular arithmetic. Shor's algorithm solves the factoring problem by using the concept of "Period Finding". Shor's algorithm would potentially factor the modulus (N) into its component prime numbers (p) and (q). This would potentially break the RSA algorithm's security[9].

$$a^{\wedge}r \equiv 1 (\mathrm{mod}\ N) \tag{1}$$

Now, let's consider symmetric-key cryptography. AES is more resistant to attacks by quantum computers due to its symmetric encryption nature. Since the only component in symmetric-key cryptography is devised in a random and unpredictable manner, the key could not be calculated using a mathematical function[10]. However, the threat from quantum computing to this algorithm is posed from Grover's algorithm. The computational algorithm could potentially search an unsorted database, the AES keys in our case, in $\sqrt{N}$ steps. Comparing this to the classical brute-force approach, which would require a total of N steps, the decrease in the number of instructions to brute force is significantly less.

IV. Post-Quantum Cryptography

The above sections demonstrate the need for a new field in cybersecurity, or the advancement in the existing algorithms to account for the increase in computational power. The field of Post-Quantum Cryptography entails a new endeavor in the field of cyber security, where new algorithms could be developed to replace or complement the current existing cryptographic methods.

Post-Quantum Cryptography has a wide range of approaches that could be employed to achieve the security, confidentiality, and integrity of data in a world where quantum computing is normalized, including Lattice-based cryptography, Code-based cryptography, and Hash-based cryptography.

A. Lattice-based Cryptography

Lattice-based cryptography is one of the emerging fields that focuses on the lattices and vectors. Consider regularly spaced grid of points stretching out to infinity, this grid space is considered lattices[13]. The vector in this space is essentially a tuple of numbers that are the coordinates of a point in the grid. The two mathematical problems that relate to this field are Short Basis Problem and Closest Vector Problems. Short Basis Problem is based on the foundation, that given a long basis for some lattice L, the computation of finding a short basis in this infinitely large space is heavy even for quantum computers[11]. This mathematical problem holds the property that given some information about the vector, it should be accessible, however, if no information is made available, the only resort is to brute-

force. Given the space of operation of lattices could be infinitely large, brute-force will become computational difficult even with the capabilities of quantum computing.

B. Hash-based Cryptography

Hash-based cryptography is not a new field. The field has existed for a while and is based on the foundation which employs a function written such that given an input, either data or message, produces a fixed length output. The fixed length output, known as a hash, is generally based on three main properties, the first property is known as preimage resistance. Preimage resistance states that given the hash, it should be computationally infeasible to determine the original input(preimage). The second property is known as second preimage resistance, which ensures that it is computationally infeasible to find a different input that outputs the same hash value[14]. The last property is known as collision resistance and is placed to ensure that given an input the same hash should not be produced for another input. Hash-based cryptography technically is still based on computational infeasibility, however, currently there does not exist an algorithm that can efficiently break the concept of hash-based cryptography.

C. Code-based Cryptography

Code-based cryptography is a concept that was developed on hardness of certain problems related to error-correcting codes for its security. The foundational idea is to decode randomly generated linear code[15]. Consider a system where the secret key is capable of correcting errors for specific code. This error detection and correction are used for encryption and decryption techniques. On a ground level, the idea is to introduce redundancy to the data in a manner that will allow the correct party to identify and correct errors without needing to retransmit all the data. In the current state of quantum computing does not hold the potential to efficiently break this method as there are no existing algorithms that can detect randomly linear codes, which would be the first step to breaking the concept of code-based cryptography. Code-based cryptography has been around for several decades; however, its significance has grown in recent years due to its alignment with security in the Post-Quantum Computing age. Furthermore, code-based cryptography is considered one of the strongest candidates for Post-Quantum cryptography as the field has a strong, and well understood mathematical foundation, making development of code-based cryptographic methods more feasible given the urgency from quantum attacks.

V. Implications and Challenges to Post-Quantum Cryptography

Given the state of the world, there has been massive growth in the field of technology. The world has become functionally dependent on technology. From handling communications to massive global economic systems, the state of the world is dependent on technology. Due to the sheer dependence on technology, the integrity, security, and availability of digital infrastructure has become massively critical. As the world gradually transitions into an age where quantum computing becomes increasingly practical, the field of security must proactively work to protect and transition current infrastructure to a more secure level.

A. Security and Reliability

The algorithms that are the successors to the traditional cryptographic methods, are relatively new. Given the timeline of the inception of these concepts, there are currently no proofs of security for these algorithms[8]. Furthermore, since the concepts lack a proof of security, there is an understatement of the lack of reliability which in comparison to traditional methods, is one the most important challenges to consider during this transition.

B. Economic Implications

The world currently operates on over an exabyte of data per day which brings into scope the economic challenges that could be implied during the time of transition. The current market cap of the digital infrastructure is well over $3.6 trillion. The economic aspect is one of the more important considerations to be made from a humanitarian aspect.

C. Performance and Scalability

A critical aspect to Post-Quantum Cryptography lies in performance and scalability of the methods. When compared to traditional methods, the computational overhead of Post-Quantum Cryptography is significantly higher. Consider Lattice-based cryptography, the concept requires larger key sizes and more complex computations, which will increase the space and time complexity of these algorithms on older computer architecture. Furthermore, while traditional cryptographic methods are ingrained in the current digital infrastructure, Post-Quantum cryptography when applied to the same scale must be able to operate efficiently, while maintaining or increasing the level of security[12].

VI. Conclusion

The field of Quantum computing presents itself as an opportunity with remarkable growth potential. However, the field poses significant challenges in the field of cryptography and security. The traditional cryptographic methods, which have been the backbone of security and privacy in the last few decades face a worthy adversary in the form of quantum computing potential. Quantum computing and its potential to solve complex mathematical problems threatens the security of some of the most widely used systems in cryptography.

However, the field of Post-Quantum Cryptography has emerged as a beacon of hope in this era of quantum threats. The field has various approaches on how to tackle the security problem post quantum computing, such as Lattice-based Cryptography, Hash-based cryptography, Code-based cryptography and many more. Most of these methods still employ the same foundational strategy of infeasibility, however, account for the increased potential due to quantum computing. Most of the concepts theoretically ensure security and confidentiality of data.

Despite the emergence of Post-Quantum Cryptography, the field remains relatively new with some significant challenges. These challenges include the lack of proven security, the economic implications of transitioning to Post-Quantum Cryptographic methods, and the lack of proof for scalability and optimization in real life scenarios.

VII. Future Work

The current state of quantum computing and cryptography requires an urgent need for collaboration between academia and industry. Despite the challenges of Post-Quantum Cryptography, the transition to quantum-resistant security is imminent. Normalized quantum computation is not in the near future, however, the need for development of quantum-resistant security and cryptography should be planned. Being able to work on and create methods that are quantum resistant ahead of time will prepare the digital infrastructure for a gradual transition which will help with economic challenges. Lastly, there should be some importance given to cryptographic methods that are not founded on the principle of infeasibility to account for security which should not be directly proportional to computation power.

References

[1.] Balamurugan, Chithralekha, Kalpana Singh, Ganeshvani Ganesan, and Muttukrishnan Rajarajan. "Post-quantum and code-based cryptography—some prospective research directions." *Cryptography* 5, no. 4 (2021): 38.

[2.] S. Akhtar, S. Choudhury, S. Chowdhury et al., "Open quantum entanglement: a study of two atomic system in static patch of de Sitter space," *Eur. Phys. J. C*, vol. 80, 748, 2020.

[3.] Bellizia, Davide, Nadia El Mrabet, Apostolos P. Fournaris, Simon Pontié, Francesco Regazzoni, François-Xavier Standaert, Élise Tasso, and Emanuele Valea. "Post-quantum cryptography: Challenges and opportunities for robust and secure HW design." In *2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pp. 1-6. IEEE, 2021.

[4.] "The Impact of Quantum Computing on Present Cryptography," *arXiv preprint arXiv:1804.00200*, 2018.

[5.] W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

[6.] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216.

[7.] Bhattacharyya, Sawan, and Amlan 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." *Data Management, Analytics, and Innovation: Proceedings of ICDMAI 2021, Volume 2* (2022): 375-405.

[8.] Cavaliere, Fabio, John Mattsson, and Ben Smeets. "The security implications of quantum cryptography and quantum computing." *Network Security* 2020, no. 9 (2020): 9-15.

[9.] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

[10.] Meneghetti, Fábio CC. "An introduction to code-based cryptography." (2021).

[11.] Miller, Shaun. "Algorithms in Lattice-Based Cryptanalysis." PhD diss., Florida Atlantic University, 2020.

[12.] Naik, Abha, Esra Yeniaras, Gerhard Hellstern, Grishma Prasad, and Sanjay Kumar Lalta Prasad Vishwakarma. "From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance." *arXiv preprint arXiv:2307.01155* (2023).

[13.] Postlethwaite, Eamonn W. "Topics in Lattice Sieving." PhD diss., Royal Holloway, University of London, 2021.

[14.] Srivastava, Vikas, Anubhab Baksi, and Sumit Kumar Debnath. "An Overview of Hash Based Signatures." *Cryptology ePrint Archive* (2023).

[15.] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-quantum cryptography*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 95-145.