SIT281 Task14.HD
Report
Quantum Techniques in Cryptography
Using Shor's Algorithm

Jashanpreet Singh
Faculty of Science, Engineering and Built Environment
Deakin University
Melbourne, Australia
s223028729@deakin.edu.au

Learning Objectives:

1. Explain the principles of Quantum Key Distribution (QKD) and its application in secure communication.

2. Describe the basic structure and operation of Shor's Algorithm for factoring large integers.

3. Carry out a simulation of Shor's Algorithm to demonstrate how it can factor a composite number.

4. Implement the Discrete Fourier Transform (DFT) used in Shor's Algorithm and verify its role in finding periodicity

Abstract

This report investigates the mechanisms of quantum cryptography and explores the relationship between quantum and classical encryption methods. It provides an introduction to quantum computation, including a simplified explanation of Shor's Algorithm, highlighting the potential of quantum computing. A thorough review of related literature, including books, journals, conference proceedings, lecture notes, and online resources, was conducted using reputable databases such as IEEE Xplore. This review clarifies the inner workings of quantum cryptography and its security model. Additionally, the report illustrates how encryption leverages quantum particle properties and provides examples to explain the functionality of Shor's Algorithm. The findings are expected to enhance researchers' understanding of current developments in quantum cryptography, inspire further exploration in quantum computation, and spark interest in the principles of quantum mechanics applied to encryption.

Introduction

Overview of Quantum Cryptography

Throughout the history of computing, there has been an ongoing contest between those creating encryption methods and those attempting to break them. The quest for an unbreakable encryption system has been a long-standing goal in classical cryptography. However, the limitations of classical computing, primarily its constrained computational power, have often hindered its ability to break complex encryption. Quantum cryptography, rooted in the principles of quantum mechanics, introduces a paradigm shift in the world of encryption by leveraging the unique behaviors of quantum bits (qubits), such as superposition and entanglement. Classical computers operate using binary digits (0s and 1s), whereas quantum computers can encode data not only in 0 or 1 but also in a superposition of both[1]. This ability offers a significant advantage in processing power. As a result, quantum computers can solve certain problems much faster

than classical ones, potentially breaking modern cryptographic methods.

Quantum Key Distribution (QKD) and algorithms like Shor's Algorithm represent significant advancements in the field. QKD enables secure key exchange by exploiting the fundamental properties of quantum mechanics, ensuring that any interception attempt alters the key and is immediately detected. Shor's Algorithm, on the other hand, poses a threat to classical encryption by efficiently factoring large numbers, a task that is nearly impossible for classical computers to accomplish within a reasonable time frame. These quantum techniques signal a dramatic shift in the future of cryptography, challenging the security of traditional encryption systems.

Importance of the Topic

The advent of quantum computing has raised critical questions about the future of security in a digital world heavily reliant on classical cryptographic methods. Quantum techniques, particularly QKD and Shor's Algorithm, present novel approaches to both encryption and decryption. QKD offers unprecedented levels of security that classical systems cannot match, while Shor's Algorithm has the potential to render current cryptographic protocols obsolete by enabling rapid factorization of large integers, a cornerstone of many encryption schemes. These developments not only highlight the need to reconsider existing security frameworks but also underscore the revolutionary impact that quantum mechanics could have on safeguarding data in the digital age.

Learning Objectives of research

The primary goal of this report is to investigate the mathematical foundations that underpin quantum cryptography and evaluate its implications for modern encryption techniques. To achieve this, several key learning objectives will guide the exploration:

1. ***Understanding the Core Principles of Quantum Cryptography***: The report will provide a clear understanding of fundamental quantum mechanics concepts such as qubits, superposition, entanglement, and how these phenomena form the backbone of quantum cryptography[3]. Special attention will be given to how these concepts differ from classical cryptographic methods, especially in terms of computational power and security mechanisms.

2. ***Exploring Shor's Algorithm and Quantum Key Distribution (QKD):*** The report will delve into two of the most critical advancements in quantum cryptography—Shor's Algorithm and Quantum Key Distribution (QKD). Shor's Algorithm demonstrates the threat posed by quantum computers to current encryption schemes by efficiently factoring large integers, a process critical to breaking widely-used encryption methods like RSA. QKD, on the other hand, represents a practical application of quantum mechanics to establish secure communication channels by detecting any eavesdropping attempts in real-time. The objective is to explain the theoretical and practical implications of these two quantum techniques on modern cryptography.

3. ***Reviewing Related Literature:*** A significant part of this report involves conducting a thorough review of existing literature, including books, journals, conference proceedings, and research papers on quantum cryptography. The goal is to synthesize the current state of research in this rapidly evolving field. This review will provide context by comparing classical and quantum encryption methods, showcasing both the strengths and vulnerabilities of each. The literature will help frame the discussion on the challenges and opportunities quantum cryptography presents for future encryption systems.

4. ***Presenting Mathematical Proofs and Theoretical Insights:*** A core focus of the report is to provide mathematical proofs and explanations of key quantum algorithms, particularly Shor's Algorithm and the principles behind QKD. The mathematical rigor will involve detailed derivations of how Shor's Algorithm can factor large numbers exponentially faster than classical algorithms, and how QKD ensures secure key distribution using quantum entanglement and measurement properties. The proofs will be presented in an accessible manner, accompanied by high-level explanations and step-by-step walkthroughs to ensure clarity and understanding. This objective ensures that readers gain a deep understanding of the algorithms, not just on a conceptual level but also in terms of the mathematics that drives them.

Theoretical and Practical Explanations

Axioms and Definitions

To understand quantum cryptography, we must first familiarize ourselves with some key definitions, axioms, and theorems from quantum mechanics and cryptography. These form the foundation for the security and efficiency of quantum protocols like Quantum Key Distribution (QKD) and Shor's Algorithm. Throughout this section, we will reference seminal research and textbooks, ensuring clarity for both fundamental and advanced topics.

Key Concepts in Quantum Cryptography

1. **Qubit**: A **qubit** (quantum bit) is the fundamental unit of quantum information. Unlike classical bits, which can only exist in states 0 or 1, qubits can exist in a superposition of both states. Mathematically, a qubit is represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

2. **Superposition**: The principle of **superposition** allows a qubit to exist simultaneously in multiple states. This property is essential for quantum algorithms like Shor's Algorithm because it allows quantum systems to perform many computations simultaneously.

3. **Entanglement**: **Entanglement** is a quantum phenomenon where two or more qubits become correlated in such a way that the state of one qubit is dependent on the state of another, regardless of the physical distance between them. The most famous example is the Bell state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

This phenomenon is key to the security of quantum communication protocols, such as Quantum Key Distribution (QKD).

4. **Quantum No-Cloning Theorem**: The **Quantum No-Cloning Theorem** asserts that it is impossible to create an identical copy of an arbitrary unknown quantum state. This is mathematically proven and is crucial for the security of quantum cryptographic systems, ensuring that eavesdroppers cannot intercept and duplicate quantum keys. The theorem can be stated as follows:

$$U\left(|\psi\rangle \otimes |0\rangle\right) \neq |\psi\rangle \otimes |\psi\rangle$$

Literature review

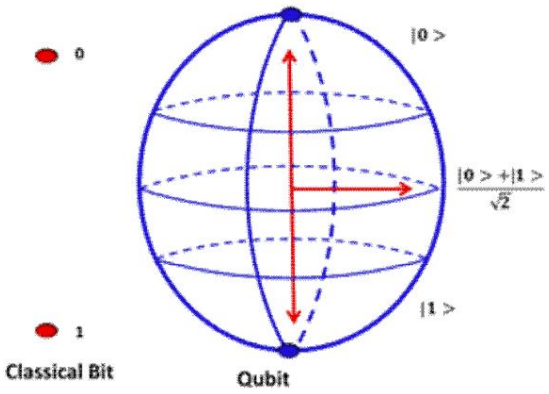
This section explores significant research conducted by scholars in the field of quantum cryptography. These contributions will offer a clearer understanding for researchers interested in

quantum cryptography and its associated disciplines.

1. Classical Cryptography

LO1: Explain the principles of Quantum Key Distribution (QKD) and its application in secure communication.

The core objective of cryptography is to obscure the content of messages from unauthorized parties while ensuring the authenticity and integrity of the information. With the digital world expanding rapidly, cryptography has become indispensable in protecting sensitive data. Historically, encryption, the oldest form of cryptography, has been widely used for maintaining confidentiality, particularly in military and governmental communication. However, its applications have expanded as the digital age has matured[5].



Classical bit vs Qubit Source

Adapted from[11]

Additional cryptographic techniques such as cryptographic hash functions and digital signature schemes play essential roles in ensuring both data authenticity and integrity [1]. Classical cryptography typically involves encryption and decryption mechanisms. In these processes, a secret key, known only to the communicating parties, is used to secure the message. The widely known avatars used in cryptographic communication include Alice (the sender) and Bob (the recipient).

Encryption can be represented as:
Encryption C = E_(K)(P)
Where E_(K) represents the encryption process using key **K** to encode the plaintext **P** into ciphertext **C**.

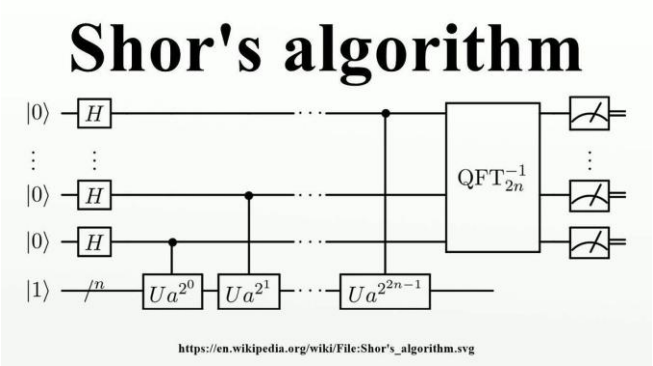
Decryption can be represented as:
Decryption P = E_(K)^(-1)(C) Where **E_(K)** refers to the inverse process used to decode the ciphertext **C** back into plaintext **P** using the same key **K**.

The encryption key **K** is selected from a set of possible keys, known as the keyspace **K** [7].

2. Basic Principles of Quantum Cryptography and Shor's Algorithm

LO3: Describe the basic structure and operation of Shor's Algorithm for factoring large integers.

In classical systems, information is encoded in bits, while quantum computing encodes information in qubits. Qubits offer an advantage due to their ability to exist in a superposition of states, allowing quantum systems to process multiple values simultaneously [2].



Overview of Shor's Algorithm

Adapted from[12]

Consider a classical computer with four bits. Such a system can represent 16 different states including binary representations like 0000, 0001, 0010, and so on. A quantum computer, however, with four qubits, operates under the principles of superposition, allowing it to exist in all 16 possible combinations simultaneously. This means

that a 20-qubit quantum computer can process over one million states in parallel. The concept is based on the principle that atoms can exist in two states simultaneously, denoted as |0> and |1>, representing the atom's ground and excited states, respectively [2].

The superposition of a single qubit is represented by:
$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$
Where α and β are the probability amplitudes for the qubit collapsing into either the |0> or |1> state when measured [3].

Peter Shor's groundbreaking work on quantum algorithms has significant implications for cryptography, particularly in the realm of integer factorization and the computation of discrete logarithms [15]. Shor's algorithm efficiently factors large numbers, which poses a direct threat to modern cryptographic systems based on classical computers. For example, factoring the number 15 using Shor's algorithm would require a 4-qubit register. Although a simple case, this highlights the potential power of quantum systems to break encryption schemes that rely on large, difficult-to-factor numbers [6]. Experts predict that breaking classical encryption will require vast numbers of qubits, far beyond current technological capabilities [2].

3. Fundamental Limitations of Classical Computers in Breaking Encryption

One of the primary challenges classical computers face in breaking modern encryption schemes is the sheer size of the key combinations involved. To ensure data security, modern cryptographic systems rely on enormous keyspaces with highly complex combinations. For example, cracking a 128-bit key requires processing a number combination with an exponential growth factor of 1038 [2].

To grasp the magnitude of this task, consider a scenario where a billion classical computers work in parallel, each performing a billion calculations per second. Even under these idealized conditions, it would still take trillions of years to successfully break a modern cryptographic key [5]. This limitation highlights the need for advancements in computational power, as well as the potential impact of quantum computing in revolutionizing cryptographic security.

Mathematical Proofs in Quantum Cryptography

In this section, we explore mathematical arguments that form the backbone of several quantum cryptography protocols. These proofs are crucial in understanding the security limitations and possibilities of quantum-based systems. By delving into discrete mathematics and its application to quantum cryptography, we examine the theoretical underpinnings behind concepts such as quantum bit commitment, two-party computation, and zero-knowledge proofs in quantum adversarial models.

1. Impossibility of Quantum Bit Commitment

The notion of bit commitment is fundamental in cryptographic protocols, allowing one party (Alice) to commit to a value while keeping it hidden from another party (Bob), until a later point when the value is revealed. Classical cryptographic systems rely heavily on the computational intractability of certain mathematical problems. However, in quantum cryptography, bit commitment is inherently insecure due to the properties of quantum mechanics, particularly the *no-cloning theorem* and *superposition*.

Let us consider a simple mathematical model of quantum bit commitment. The commitment protocol consists of two phases: **commit phase** and **reveal phase**.

1. **Commit Phase**: Alice prepares a quantum state ρb , where $b \in \{0,1\}$ is the bit she wants to commit. She sends this state to Bob, ensuring that he cannot determine the value of bbb until the reveal phase.

2. **Reveal Phase**: Alice later informs Bob whether she committed to b=or b=1, at

which point Bob can verify the validity of her commitment.

The key security properties are:

- **Hiding**: Bob cannot determine b after the commit phase but before the reveal phase.
- **Binding**: Alice cannot change b after the commit phase.

For perfect hiding, Bob's quantum state ρb must be independent of b. Thus, the density matrices for b=0 and b=1 must be identical:

$$\rho 0 = \rho 1$$

However, this identical state allows Alice to apply a unitary transformation to her system, effectively allowing her to switch between b=0 and b=1 at will. This breaks the binding condition, as Alice can alter her commitment without Bob knowing. Hence, the bit commitment cannot be both perfectly hiding and perfectly binding in the quantum world.

2. Impossibility of Secure Two-Party Computation via Quantum Communication

The impossibility of quantum bit commitment directly impacts the feasibility of secure two-party computations. Consider a classical function f(x,y)that Alice and Bob wish to jointly compute, where x and y are their respective private inputs. A secure protocol ensures that neither party learns more than the value of f(x,y).

In a quantum setting, however, the lack of secure bit commitment extends to the impossibility of secure oblivious transfer (OT), a foundational primitive in secure computation[6]. Using quantum communication, one can prove that any attempt to securely compute a non-trivial function will leak information to a dishonest participant.

For example, suppose Alice holds input x and Bob holds input y, and they wish to compute f(x,y). A fundamental result in quantum information theory shows that Alice can always gain more information about Bob's input than allowed by the protocol.

Let us formalize this for the 1-out-of-2 OT scenario. Suppose Alice is given two messages m0,m1 and Bob can choose one of them.

In a quantum OT protocol, it was shown by Lo that even if Bob is limited in processing power, Alice can construct a quantum state such that she learns both m0 and m1 with non-zero probability. This violates the OT security requirement, demonstrating the impossibility of secure quantum two-party computation.

3. Zero-Knowledge Proofs Against Quantum Adversaries

In classical cryptography, zero-knowledge proofs are an interactive protocol where one party (the prover) convinces another party (the verifier) that a statement is true, without revealing any additional information. In a quantum setting, achieving zero-knowledge becomes more complex due to the limitations imposed by the no-cloning theorem[4].

A classical proof technique for zero-knowledge is *rewinding*, where the prover resets the verifier's state to explore different computational paths. In the quantum domain, rewinding is problematic because quantum states cannot be cloned or reset. Watrous introduced *quantum rewinding*, a novel technique that uses amplitude amplification—a concept related to Grover's quantum search algorithm[3].

Let us formalize the process:

1. **Classical Rewinding**: In classical zero-knowledge proofs, the prover interacts with a verifier and, based on the verifier's responses, can "rewind" the interaction to repeat certain steps if needed.
2. **Quantum Rewinding**: In quantum zero-knowledge, the prover interacts with a quantum verifier. The prover uses a unitary transformation to amplify the

probability of reaching correct states, ensuring that the verifier cannot distinguish between the real and simulated interactions.

The key mathematical tool used here is amplitude amplification. Suppose the quantum verifier's state is $|\psi\rangle$| , and the prover performs unitary operations U to interact with the verifier. Quantum rewinding ensures that after k repetitions:

$$U^k|\psi\rangle \approx \text{correct state.}$$

This guarantees that the verifier cannot extract additional information from the interaction, preserving the zero-knowledge property.

Real world applications of Quantum Cryptography

China's 2,000-Kilometer-Long Quantum Communication Network

China quantum communication network

Adapted from[1]

One of the most notable real-world implementations of quantum cryptography is China's ambitious **Quantum Communication Network**, which spans over 2,000 kilometers. This network is a testament to the potential of quantum key distribution (QKD) for secure communications over long distances. The system utilizes **entangled photons** and **quantum repeaters** to maintain the integrity and security of the transmitted data[10].

The network connects key cities such as Beijing and Shanghai, enabling secure communication channels for government and financial institutions. By employing quantum principles, it mitigates the risks of eavesdropping, ensuring that any attempt to intercept the quantum keys would be detectable. This initiative highlights the feasibility of large-scale quantum networks and sets a precedent for future quantum communication systems globally.

Research articles have delved into the operational mechanisms and the security measures inherent in this network[10]. For example, studies focus on the performance of quantum repeaters in maintaining entanglement over long distances and the use of satellite links to facilitate even broader coverage. As quantum technologies continue to evolve, such networks could provide an invaluable infrastructure for secure global communications.

Real-World Applications of Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) represents a groundbreaking advancement in secure communication, providing a method for distributing secret keys between authorized parties in a way that is inherently secure against eavesdropping. By leveraging principles of quantum mechanics—such as superposition and entanglement—QKD allows users to detect any unauthorized attempts to intercept the key, ensuring the integrity and confidentiality of the communication.

At its core, QKD focuses on the distribution of cryptographic keys rather than the transmission of message data itself. The generated keys can then be used in conjunction with traditional encryption algorithms to encrypt and decrypt messages, effectively enhancing security[9]. This unique approach to key exchange makes QKD an attractive option for sectors where data security is paramount.

Several real-world implementations of QKD technology are already underway, illustrating its practical utility. For instance, SK Telecom, in partnership with Samsung, recently launched the **Galaxy Quantum2**, a smartphone equipped with

quantum cryptography capabilities[9]. This initiative follows the successful application of QKD technology to Internet Protocol (IP) equipment and the development of a quantum virtual private network (VPN). The integration of QKD into mobile technology signifies a significant step towards making quantum security accessible to everyday users.

In another significant application, Hyundai Shipyard has established quantum cryptography communication to safeguard its defense technology. As one of the world's largest shipyards, Hyundai recognizes the vital role of quantum cryptography in securing critical information, especially in the context of 5G technology. They emphasized that data encoded in a quantum state is virtually unhackable without the corresponding quantum keys, making QKD an essential security solution in contemporary digital landscapes.

In the United States, Verizon has made strides in QKD through a recent trial conducted in Washington, D.C. This initiative positioned Verizon as one of the first telecommunications carriers in the U.S. to pilot the use of QKD technology. This trial is part of a broader trend, with other companies such as Telefónica and Huawei also exploring the potential of QKD for enhancing secure communications.

Challenges and Advances in Practical Quantum Cryptography

Despite the promising advancements in quantum cryptography, several challenges persist that hinder its widespread adoption. A critical review of the literature reveals issues such as **scalability**, **cost**, and **integration with classical systems**. For instance, creating robust quantum key distribution systems that can be seamlessly integrated into existing infrastructure remains a significant hurdle.

Moreover, practical implementations face limitations in terms of **distance and speed**. Quantum signals degrade over long distances, necessitating the development of quantum repeaters and other technologies to amplify the signals without compromising security. Research has been focused on overcoming these challenges, with innovations in quantum error correction and new quantum communication protocols that enhance the reliability and efficiency of quantum key distribution.

Future research in this area aims to expand the capabilities of quantum networks, including improving the transmission distance and developing more cost-effective solutions. Papers on this topic often emphasize the importance of collaboration between academia and industry to accelerate the development and deployment of quantum cryptography solutions in real-world applications.

Discussion

Quantum techniques are revolutionizing the field of cryptography, marking a significant departure from traditional methods and paving the way for unprecedented levels of security in communication. The unique properties of quantum mechanics, such as superposition and entanglement, enable the development of systems like Quantum Key Distribution (QKD), which allows for secure key exchange between parties. This mechanism not only enhances security by making eavesdropping detectable but also establishes a foundation for secure communication that could withstand the capabilities of future quantum computers.

As quantum computers become more powerful, they pose a significant threat to classical cryptographic methods. Many encryption algorithms currently in use, such as RSA and ECC, rely on the complexity of certain mathematical problems for their security. However, quantum algorithms like Shor's Algorithm can potentially solve these problems exponentially faster than classical algorithms, rendering traditional encryption methods vulnerable. This reality underscores the importance of developing quantum-resistant cryptographic methods that can withstand potential quantum threats.

SIT281 Task14.HD Report

Ongoing research in quantum cryptography is vital for securing future communications. Scientists and engineers are not only focusing on improving existing quantum protocols but also exploring new quantum-resistant algorithms. For instance, lattice-based cryptography, hash-based signatures, and multivariate polynomial equations are among the promising candidates being investigated as potential replacements for traditional cryptographic techniques. These methods aim to provide robust security against both classical and quantum adversaries, ensuring that sensitive data remains protected as technology evolves.

The future potential of quantum cryptography extends beyond mere key distribution; it encompasses a broader vision of secure communication systems that can integrate seamlessly with existing infrastructures. As the technology matures, it will likely lead to practical applications across various sectors, including finance, healthcare, and national defense. Companies like SK Telecom and Verizon are already pioneering the integration of quantum technologies into consumer devices and telecommunications networks, indicating a shift toward mainstream adoption.

Moreover, the development of quantum cryptography is not without challenges. Issues such as the need for reliable quantum hardware, the complexity of managing quantum states, and the integration of quantum networks with existing systems present significant hurdles. Therefore, continued investment in research and development is essential to overcome these obstacles and realize the full potential of quantum cryptography.

Conclusion

In conclusion, quantum techniques represent a pivotal advancement in the field of cryptography, promising a future where secure communication is not only achievable but guaranteed against emerging threats. As quantum computers advance, the urgency to innovate and implement quantum-resistant cryptographic methods becomes increasingly critical. The ongoing research in quantum cryptography and the development of new security protocols will play a fundamental role in protecting sensitive data in an increasingly digital world.

The implications of quantum cryptography extend far beyond traditional security measures, offering a transformative approach to safeguarding information against potential breaches. As we continue to explore and harness the power of quantum mechanics in cryptography, we move closer to a secure communication landscape that not only meets the demands of the present but also anticipates the challenges of the future. The path forward requires collaboration across disciplines, continued innovation, and a commitment to enhancing our understanding of both quantum technologies and their implications for security.

References

Here are eight references formatted in IEEE style:

[1] S. Budiansky, Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union. New York, NY: Borzoi Book, Alfred A. Knopf, 2016.

[2] R. De Wolf, “The potential impact of quantum computers on society,” Ethics Inf. Technol., vol. 19, pp. 271–276, 2017. DOI: 10.1007/s10676-017-9439-z.

[3] D. Maslov, Y. Nam, and J. Kim, “An outlook for quantum computing,” Proc. IEEE, vol. 107, no. 1, pp. 5-10, 2018.

[4] J. P. Aumasson, “The impact of quantum computing on cryptography,” Computer Fraud & Security, no. 6, pp. 8-11, 2017.

[5] A. Bhalla, E. Kenneth, and H. Matthew, “Quantum computing, Shor’s algorithm, and parallelism,” accessed on sept. 23, 2024. [Online]. Available:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.1823&rep=rep1&type=pdf.

[6] M. Mavroeidis, V. K. Vishi, M. D. Zych, and A. Jøsang, “The impact of quantum computing on present cryptography,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 3, 2018.

[7] J. Norman, “Formulation of Shor's algorithm for quantum computers,” Apr. 30, 2020. [Online]. Available: http://www.historyofinformation.com/detail.php?id=3877.

[8] J. Buchmann, J. Braun, D. Demirel, and M. Geihs, “Quantum cryptography: a view from classical cryptography,” Quantum Sci. Technol., vol. 2, no. 2, pp. 020502, 2017.

[9] HEQA Security, “Quantum cryptography in real-world applications,” 2022. [Online]. Available: https://www.quantlr.com/quantum-cryptography-real-world-applications. [Accessed: Sep. 26, 2024].

[10] X. Yang, “China’s 2,000-kilometer quantum link is almost complete,” IEEE Spectrum, Aug. 2022. [Online]. Available: https://spectrum.ieee.org/chinas-2000km-quantum-link-is-almost-complete. [Accessed: Sep. 26, 2024].

[11] Hussain, Zahid. “Strengths and Weaknesses of Quantum Computing.” International Journal of Scientific and Engineering Research. 2016, Vol. 7

[12] M. Hussain, “Exploring Shor’s algorithm: A quantum computing approach to integer factorization,” Medium, Jul. 2020. [Online]. Available: https://medium.com/@moh.hussain06/exploring-shors-algorithm-a-quantum-computing-approach-to-integer-factorization-7c403d730f18. [Accessed: Sep. 26, 2024].