Chapter 4

Book Chapter

Quantum Safe cryptography – An Overview

S.Pandikumar [*1], Pallavi M O [†2], Dhanush C [‡3], and M.Arun [§4]

[1]Associate Professor, Dept. of MCA, Acharya Institute of Technology, Bangalore
[2]Assistant Professor, Dept. of MCA, Acharya Institute of Technology, Bangalore
[3]Dept. of MCA, Acharya Institute of Technology, Bangalore
[4]Assistant Professor, Dept. of Computer Science, Sri Krishna Adithya College of Arts and Science, Coimbatore

Abstract

Quantum-safe cryptography is the term that specifies cryptographic methods secured against the threats of quantum computing. Among them are Quantum Key Distribution, which provides information-theoretic security, and Post-Quantum Cryptography, which provides scalable authentication in high-density networks but lacks the same level of theoretical security as the former. In this context, a hybrid cryptosystem that integrally combines QKD and PQC should be created to build a robust quantum-safe system. Moreover, in blockchain technology and machine learning models, quantum algorithms play an important role by improving encryption and key generation. Quantum-safe cryptography represents an important step toward the future-proofing of digital communications and systems.

Keywords: Cryptography. QKD. PQC. Machine Learning Models.

[*]Email: spandikumar@gmail.com Corresponding Author
[†]Email: pallavi2570@acharya.ac.in
[‡]Email: dhanushchandru28@gmail.com
[§]Email: arunm@skacas.ac.in

1 Introduction

Very fast progress is being made in development of quantum computers, putting under threat many existing cryptographic systems. Quantum computers can break widely used types of encryptions such as RSA and ECC, because Shor's algorithms are actually able to perform tasks which are extremely difficult under classical computation: integer factorization and discrete logarithms. This threat has given rise to what is known as quantum-safe cryptography—that is, specifically devoted to cryptographic methods that can withstand power of a quantum computer (Mavroeidis et al., 2018) . There are two primary methods used in quantum-safe cryptography: Quantum Key Distribution and Post-Quantum Cryptography. The former is a technique that provides information-theoretic security: its security is derived from the laws of quantum mechanics, rather than from the infeasibility of computation; because QKD relies on this physical principle, it resists classic attacks almost in addition to quantum attacks. PQC, alternatively, refers to designing mathematical algorithms resistant to a quantum attack but scalable and practical enough for use in modern digital networks on a wide scale. Since, however, PQC does not share the same theoretical guarantees of security as QKD, the best combination of both techniques makes for a robust security system (Wang et al., 2022) .

Quantum-safe cryptography is applied in the process f safeguarding blockchain technologies, which natively are susceptible to quantum attacks since such technologies rely on public-key cryptography (see Figure 1). The aim is the use of post-quantum algorithms within blockchain systems to secure transactions and other digital assets against advancements in quantum computation. Quantum-safe algorithms are being developed to aim towards maximizing the efficacy of machine learning models in encryption, decryption, and key generation techniques (Yang et al., 2024) . Quantum-safe cryptographic techniques also play a great role in unique and challenging environments, such as underwater communication. Algorithms post-quantum is being adapted in conditions where traditional methods of cryptography may not work to maintain integrity and security of data. Given this new wave of quantum-safe cryptography development and integration, safeguarding digital communications, financial systems, and sensitive data from future quantum threats is an important factor. Thus, with the world being thrust headfirst into the quantum computing era, the usage of quantum-safe cryptographic solutions would be practically necessary to ensure the long-term security and reliability of our digital infrastructure (Mavroeidis et al., 2018) .

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

Figure 1. Quantum Safe Cryptography

2 Background And Theoretical Framework

Quantum computing is on its way, bringing a totally new landscape of digital security. In order to understand why quantum-safe cryptography is necessary and how it is built, one needs to understand some of the underlying principles of classical cryptography, quantum mechanics, and in general, the quantum algorithms threatening our current cryptographic systems.

1. Fundamentals of Cryptography

   Cryptography is the art and science of safe guarding information, based on which the privacy, accuracy and validity of data in digital communications have been established. Traditional cryptographic systems are generally classified into symmetric and asymmetric (public-key) cryptography (Mosca, 2018) . Symmetric Cryptography: A single key is utilized for encryption and decryption. Among the most widely used are for their speed and strength the AES. But the main concern of symmetric cryptography is the secure key management and key distribution, which is difficult especially in big networks (Moody et al., 2020) . Asymmetric Cryptography: Employs a set of keys—a public key for encryption and one private key for decryption. Prominent algorithms include RSA (Rivest–Shamir–Adleman) and ECC i.e. Elliptic Curve Cryptography. These systems facilitate secure key exchange and digital signatures, enabling secure communications through unprotected channels without prior key sharing (Bernstein, Buchmann, & Dahmen, 2009) . The protection of these classical methods of cryptographic systems is founded on a presumption that specific mathematical problems are computationally hard. For example, RSA operates on the problem of factoring large composite numbers, whereas ECC performs its operations on the difficulty of the elliptic curve discrete logarithm problem. These

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

presuppositions guarantee that as of current computing capabilities, it's almost infeasible to get unauthorized decryption or derivation of keys (Bernstein, Buchmann, & Dahmen, 2009) .

2. Introduction to Quantum Computing

   Quantum computing is a paradigm shift from the classical model, in that it is founded on principles drawn from quantum mechanics. Quantum bits or qubits do not exist in 0 or 1 states as do regular bits; instead, they may be in any state simultaneously because of superposition. Another occurence that allows two qubits to be linked in a manner that if one qubit's state changes, it immediately affects the other helps quantum computers perform and store huge amounts of data better than their classical counterparts. Quantum computers take advantage of these properties for parallel exponential computation that is designed to solve problems beyond the capabilities of current computer systems much faster. So far, this unparalleled computational power has opened up opportunities as well as threats to innovations in potentially disparate fields and cryptographic systems.

3. Quantum Algorithms Threatening Cryptography

   Several quantum algorithms use quantum computers to address problems that cannot be solved with classical machines; thus, they weaken the security foundations of classical cryptography directly. Shor's Algorithm was found by Peter Shor in 1994. This algorithm could factor large integers efficiently, and it can also calculate discrete logarithms-a mathematical foundation of widely used cryptographic systems such as RSA and ECC-putting the security of these cryptographic schemes under breach if strong quantum computers are realized (Moody et al., 2020) . Grover's Algorithm: Grover proposed Grover's algorithm in the year 1996. It provides a quadratic accleration for unstructured search problems. In the context of cryptography, Grover's algorithm reduces the security of symmetric key algorithms in effect by letting them half the key lengths. For example, a 256-bit key would provide the strength of a 128-bit key against an attacker using Grover's algorithm; hence longer keys are required to maintain the same level of security (Shor, 1994) . Such quantum algorithms believed to be threatening possibility, hence an urgent need to switch over to quantum-resistant cryptographic systems against quantum attacks. The sensitive data transport today could be decrypted the future using such advances, making the privacy violations in financial security and national security to become a significant issue (Grover, 1996) .

4. The Demand for Quantum-Resistant Cryptography

   Quantum-safe cryptography, otherwise referred to as post-quantum cryptography,

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

PQC, therefore aims at producing cryptographic algorithms with resistance against the actual quantum capability threat. While PQC focuses on developing classical algorithms, that can be implemented within existing infrastructure and has resistance against both classical and quantum attacks, QKD in turn relies solely on quantum mechanics for security but does not require a form of specialized hardware.[3] Theoretical building blocks for PQC include a number of very heterogeneous mathematical problems which are considered to be unsolvable by an adversary on a quantum computer, namely lattice-based problems and hash-based constructions, code-based schemes, and multivariate polynomial equations. In this way, each category provides different advantages in security, efficiency, and applicability, thus contributing to a powerful, heterogeneous cryptographic ecosystem capable of resisting future quantum threats (Mosca, 2018) .

5. Quantum Mechanics and Cryptography

   While a threat of quantum algorithms is the main reason to extend the interplay between quantum mechanics and cryptography, quantum mechanics brings new approaches to secure communications as well, such as Quantum Key Distribution (QKD), offering information-theoretic security. According to principles of quantum measurement, QKD allows eavesdropping detection, but implementing QKD has serious requirements for specialized hardware and infrastructure, hence not scalable at the same pace as PQC (Moody et al., 2020) . Such integration might imply hybrid systems combining the key strengths of both approaches in order to offer improved overall security and practicality. Such hybrid systems seek to deliver solid security assurances with compatibility towards current digital communication infrastructures, for seamless transition towards a quantum-safe future (Chen et al., 2016) .

6. Present and Future Drift

   That is why research and standardization are very fundamental to the developments of quantum-safe cryptography. This has, for instance included organizations such as NIST that evaluates and selects various algorithms toward the foundation of standardized protocols that can, in turn be embraced more widely. This calls for the careful analysis of the security, performance, and feasibility of the implementation for the selected algorithms in terms of catering for modern requirements of digital systems . Optimizing algorithm efficiency, easy functionality with existing technologies, and ease of practical problems such as key management and protocol interoperability are considered to be in future direction for quantum-safe cryptography (Shah et al., 2023) .

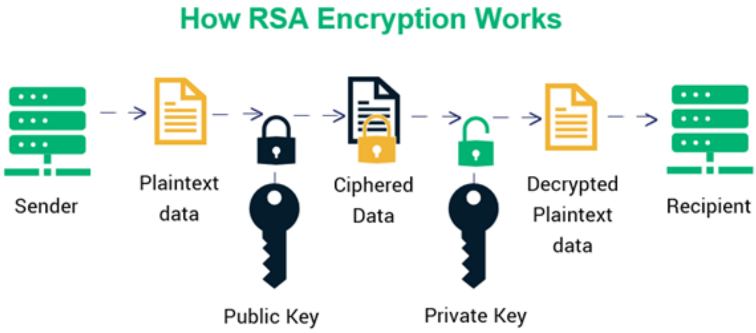

Figure 2. RSA Encryption

3 Threats Posed By Quantum Computing

Quantum computers hold much more impressive implications for improvement in the study of chemistry, material science, and artificial intelligence. They represent a comprehensive challenge, anew in modern cryptographic systems. The latter point to challenging probabilistic queries to the problem instance of the system, establishing the path for cryptanalysis only when solutions are created to fit these queries. So far, so unremarkable: classical cryptographic algorithms depend on the hard nature of some mathematical problems related to assured communication and data protection. But quantum computers promise powerful algorithms destroying these cryptographic systems while making the latter insecure in a post-quantum world (Chen et al., 2016) .

1. Shor's Algorithm and Public-Key Cryptography

   The most significant threat to classical cryptography comes from Shor's quantum algorithm, which solves the integer factorization problem and the seperate logarithm problem efficiently, both problems being significant in the safety of widely used public-key cryptographic systems, such as RSA (see Figure 2), Elliptic Curve Cryptography (ECC)(Shor, 1994) .

   - RSA Vulnerability: The safety of RSA relies on the apparent hardness of finding prime factors of very large composite numbers. Factoring a number with hundreds of digits is computationally infeasible on classical computer that exists or could exist at any time in foreseeable future. Shor's algorithm, when run on a sufficiently powerful quantum computer, can factor large numbers in polynomial time and break RSA encryption. This threatens the security of communications, including messages, signatures, and key exchanges (Shor, 1994) .

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

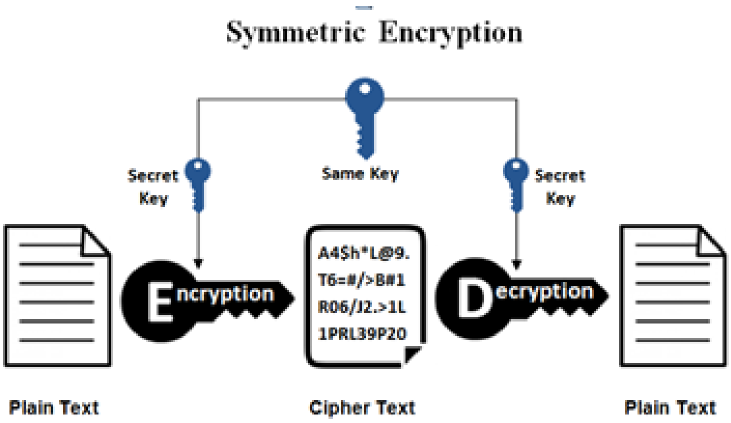

Figure 3. Symmetric Encryption

- ECC Vulnerability: ECC, having better safety with smaller key sizes than its competitor RSA, is also vulnerable to Shor's algorithm. ECC security depends upon the hardness of elliptic curve discrete logarithm problem. However, Shor's algorithm runs efficiently on this problem and hence makes ECC based encryption, key exchange protocols insecure. This might allow someone to decrypt whatever data encrypted with RSA or ECC algorithms before the availability of such large-scale quantum computers, thereby accessing sensitive data, such as personal data, financial transactions, and secret communications (Shor, 1994) .

2. Grover's Algorithm and Symmetric Key Encryption

   While the key concept which symmetric key cryptographic systems like AES possess is not quite vulnerable to quantum attacks as in comparison to public-key schemes, they are still a danger because of Grover's algorithm. The quantum search algorithm gives a quadratic speedup over classical search algorithms by allowing it to reduce the effective key length of symmetric encryption schemes (as shown in Figure 3)(Grover, 1996) .

   - On AES: Grover's algorithm would be able to cut the security of AES encryption in half. For example, the figure considered secure in the classical computing world AES-256, would yield to a quantum attacker using Grover's algorithm only 128-bit security. AES-128 would yield only 64-bit security, which is insufficient for most security applications. Thus, longer key lengths, such as AES-512, might be required to ensure security against a quantum adversary (Grover, 1996) .
     Whereas the threat to symmetric key cryptography is not more pressing than that

mounted by Shor's algorithm for public-key schemes, it cannot be overlooked and thus warrants increased scrutiny in cases wherein security of long-term data is paramount (Shor, 1997) .

3. Implications on Digital Security The potential for quantum computers to break both public-key and symmetric-key encryption gives rise to the following monumental threats:
   - Data Privacy Compromised: Data that is stored or transmitted encrypted today could be decrypted using a sufficiently advanced quantum computer. This would include sensitive personal information, financial records, and all confidential business data. Even though the quantum computers can't decrypt this encryption in real time, an adversary may capture and store encrypted communications that can be decrypted later when the required quantum computers are available.
   - Infrastructure Break-down: Public-key cryptography forms the basis for safe communications over the internet. It is used in those protocols, including TLS (Transport Layer Security), which encrypts web browsing, and SSH (Secure Shell), which encrypts remote login. The global digital infrastructure would utterly break down in such a scenario that would cause complete disruption.
   - Threat to Cryptocurrencies and Blockchain: Blockchain technology, on which many cryptocurrencies depend, including Bitcoin and Ethereum, has its basis in cryptographic techniques including digital signatures and hash functions. Shor's algorithm might break the elliptic curve signatures currently applied in most blockchain systems, and quantum attackers would be able to forge transactions and compromise the integrity of the blockchain.
   - National security threats: Nations and their militaries depend on cryptography to ensure secrecy in classified communications, sensitive operations, military strategies, and operations. Quantum computers can compromise national security in that they will decrypt secret communications, revealing diplomatic communications and intelligence operations (Shor, 1997) .

4 Quantum-Safe Cryptography Overview

Cryptography which is post-quantum, or PQC for short, refers to cryptography that has been designed to be secure against current computational powers of quantum computers. Classical systems for encryption, such as RSA and ECC, rely on math problems that appear to be infeasible to solve, at least classically, including integer factorization and discrete logarithms. Quantum computers can readily solve them using Shor's algorithm, making existing encryption technologies vulnerable to quantum attacks. Quantum-safe cryptography aims at protecting information by means of new algorithms that are said to

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

be unbreakable, even if a powerful quantum machine exists. These algorithms depend on problems that are difficult to solve for the quantum computer due to their mathematical structure. Included here are the following:

1. Origins of Lattice-Based Cryptography: This is the field of cryptography based on intricate geometric structures called lattices. Its difficulty in being solved for classical, quantum computers include well-known schemes such as Learning With Errors (LWE), and Ring-LWE.

2. Hash-Based Cryptography: This focuses on quantum-resistant cryptographic hash functions. Hash-based digital signatures such as the Merkle signature scheme are just a few of those examples.

3. Code-Based Cryptography: This relies on the hardness of decoding random linear codes. The most famous example of this type of cryptography is the McEliece cryptosystem, which has proven safe from quantum threats since a few decades ago.

4. Multivariate Quadratic Equations: This includes solving systems of polynomial multivariate equations, which, decidedly, is not an easy problem for quantum computers

Quantum-resistant cryptographic algorithms have been extensively researched and standardized. Certainly, considerable work has been done by the National Institute of Standards and Technology (NIST) toward the evaluation and selection of post-quantum algorithms with the result that future secure digital communications, financial transactions, and national security systems will be ensured in presence of a quantum-enabled world. In comparison to QKD, where the concepts of quantum mechanics are applied to ensure key exchange securely but requires specific hardware, quantum-safe cryptography is typically designed to run on a classical computer and integrate with current infrastructures. Therefore, PQC represents a scalable and realistic means for preventing losses against future quantum attacks. While Quantum Safe Cryptography is busy developing cryptographic algorithms will remain secure against the potential future threats of malicious quantum usage, it is just as important to deal with how the keys are safely distributed in the first place. Here is where Quantum Key Distribution comes into action; QKD utilizes principles related to quantum mechanics for the establishment of a communication channel that is secure for interchange of cryptographic keys. Based on basic properties of quantum states such as superposition, entanglement, QKD can be applied as an intrinsic mechanism for key generation as well as secure sharing, proving itself secure against eavesdropping by design. Instead, although QSC attempts to build strong cryptographic algorithms, this will still allow QKD to be used as an alternative for securing key transmission—thereby enhancing security architecture across the post-quantum world.

5 Quantum Key Distribution

The QKD is among of the revolutionary ways to implement secure communication because it is based on the principles of quantum mechanics in order to allow two parties to generate and share a secret key with the highest possible safety assurance. Unlike other classical methods of key distribution, which are based on difficulty of some computational mathematical problems, the safety of QKD lies upon a basis of the laws of physics, making it theoretically safe from any potential computing breakthrough, such as those that are probable in quantum computers (Ricci et al., 2024) . At the core of QKD are two main protagonists: Alice, the sender, and Bob, the receiver. The aim of the protocol should be to allow Alice and Bob to generate shared secret key to be used for encrypting and decrypting purposes while making sure that presence of Eve-the inevitable eavesdropper-is bound to be detected (as shown in Figure 4). It begins with the qubit preparation. Qubits are widely represented by photons in polarization states. A qubit travels through a quantum channel, such as an optical fibre or free-space link. The properties of qubits-superposition and entanglement-that seem so fascinating are the basis of security in QKD (Scarani et al., 2009) After receiving the qubits, Bob measures their states in randomly chosen bases. Due to principles of quantum mechanics, any measurement by Bob must disturb the state of qubits, in particular if Eve tries to intercept and measure them. This disturbance appears as errors in the key which can be detected by Alice and Bob by comparison of a fraction of their measurements via a public classical channel (Ricci et al., 2024) . Then, presuming that the rate of error is not surpassing a threshold-that is to say no real eavesdropping occurred, then Alice and Bob go on with error correction, privacy amplification of key, to perform it securely identical. At last, the result going to be the shared secret key who will be free of any knowledge of Eve, to be used as good base for secure communication (Scarani et al., 2009). QKD is remarkable also for its information-theoretic security; that is, its security does not depend on the computational limits of would-be adversaries. With improvements in quantum technologies, QKD will also be useful to come as a means of protecting sensitive information, which it will assist in laying the foundation for communications that are quantum-proofed against an increasingly quantum-enabled world (Scarani et al., 2009).

The QKD process can be broken down into several key steps:

1. Sending Qubits

   The qubit transmission process is the first step of action in building the secret key for QKD. Qubits are termed quantum bits. The elements carrying information in quantum systems are qubits, the closest comparisons to bits but with so much richer properties than them. Contrary to classical bits, qubits can exist in superposition and hence, simultaneously, can represent 0 and also be 1 (see Figure 5). This

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

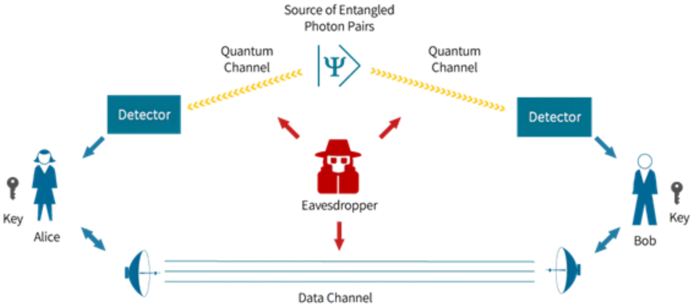

Figure 4. Quantum Key Distribution

property forms the basis of QKD for conducting a highly secure key exchange. Alice traditionally is known as sender and prepares a sequence of photons; each photon can be considered as qubit. Such photons are polarized in specific ways representing the information that is supposed to be encoded. For example, the very popular BB84 protocol, Alice selects one of four potential polarization states: horizontal, vertical, diagonal, or anti-diagonal. Each polarization would correspond to a bit value with different polarizations corresponding to different bits. Such randomness in polarization choice is important because it brings it uncertainty so that any potential eavesdropper, Eve, wouldn't know what the exact states were when she was looking at these photons so wouldn't know precisely what to clone. Once ready, Alice sends the qubits to the receiver, Bob, through a quantum channel. While any sort of channel is a quantum channel, choices often include optical fibers or free-space links because such media permit transmission of photons with minimal loss over appreciable distances. The physical transmission of photons is sensitive in such a way that even interference or disturbance could change quantum states. This sensitivity has both positive and negative sides; it ensures that any attempted interception by an unauthorized party will definitely perturb the qubits, thus raising suspicion of an eavesdropper's presence. In other words, the sending of qubits in QKD is more or less a precisely choreographed process that involves introducing the quantum property of photons to initiate a secure key. Encoding information on the polarization states of photons and their transmission through a well-controlled quantum channel by Alice and Bob forms the basis of a basically secure cryptographic key against any attempt at eavesdropping with the principles of quantum mechanics.

2. Transmission & Eavesdropping Protection The transmission of qubits in QKD is

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

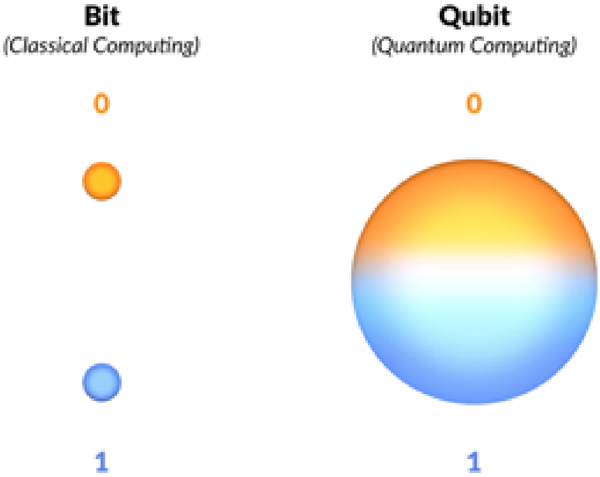

Figure 5. Qubits

not an easy point-to-point information transfer from Alice to Bob but inherently relates with the detection of any eavesdropping attempt on behalf of an adversary, Eve. In this sense, such a dual-purpose transmission establishes the main difference between QKD and classical approaches to key distribution, hence providing a great mechanism for both key sharing and security assurance (see Figure 6) .

Now that Alice has generated her polarization sequence of photons, she sends them over a quantum channel to Bob. The chosen quantum channel may be an optical fiber or a free-space link, optimized for maximum efficiency in photon transmission with minimal loss and noise. Preserving the integrity of the transmission is important since all of QKD relies on preserving the quantum properties of the qubits during transit. As a fundamental feature, any attempt on Eve's part to intercept and measure the qubits will inherently disturb the quantum states. In fact, such an attempt on the part of Eve would be based on Heisenberg Uncertainty Principle that relates certain pairs of physical properties that cannot, in principle, both be known to arbitrary precision. In QKD, if Eve requires the determination of photons' polarization, she will inevitably disturb the states by introducing measurable abnormalities in the transmission. The disturbance caused by the eavesdropper appears as errors in key generation algorithm. If Bob assesses the incoming qubits and, later on, looks at his measurement bases against Alice's then a rate of error greater than

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

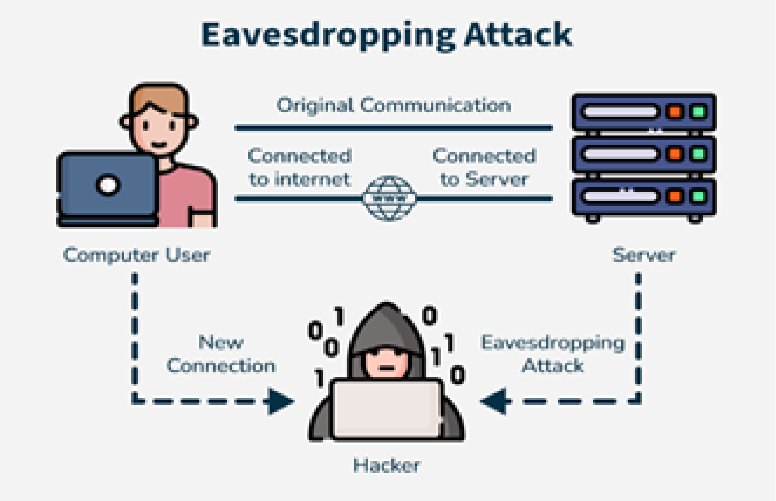

Figure 6. Eavesdropping Attack

what is expected implies the presence of Eve. Since any attempt at eavesdropping leads to, by its nature, disturbance of quantum states of qubits, QKD will automatically always be an eavesdropping-resilient method. Advanced technologies and methods apply to fortify the security and robustness of qubit transfer. Quantum repeaters and entanglement swapping, for example, allow QKD to move a much longer distance without losing a noticeable amount of quantum information. Then error correction protocols can flag and minimize the undesired impact of both noises caused by legitimate processes, along with any malicious eavesdropping. In effect, the procedure of qubit transfer in QKD serves a dual function: it transmits quantum information while simultaneously revealing any unauthorized intercept of that information. This dual function is one of the bedrock principles that make sure QKD can indeed have Alice and Bob generate a shared secret key to which both Alice and Bob can have confidence its confidentiality and integrity are assured (Ricci et al., 2024) .

3. Bob measures the Qubits Now, Bob Measures Qubits. In a QKD protocol, measurement carried by Bob on the qubits is a critical step in converting the quantum information obtained from Alice into a secret key to be applied in production (as shown in Figure 7). This process follows the principles of quantum mechanics - with special attention placed on the principle of superposition and the probabilistic

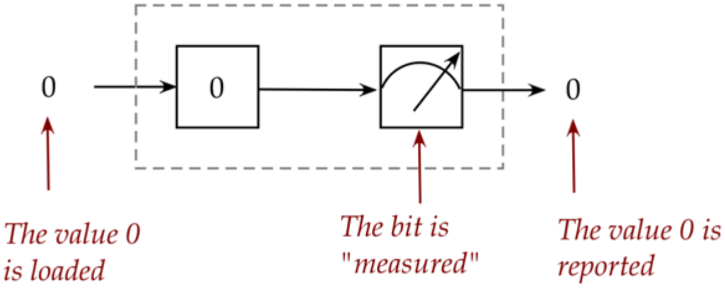

Figure 7. Measurement of Qubits

nature of quantum measurements.

When Bob receives these polarized photons from Alice, his work is to measure the polarization states so that information there may be retrieved. Now, how he goes about making these measurements becomes of critical importance for the process of QKD to be secure and feasible. Since Bob does not know which of the polarization states Alice has chosen, he has to make his measurement basis on every incoming qubit independently. Usually, Bob uses some arbitrary set of measurement bases. Typically, he uses a protocol which is analogous to Alice's encoding scheme. For illustration of the BB84 protocol, the two bases are: rectilinear (horizontal/vertical) and diagonal (45-degree/135-degree). Bob randomly selects one of the above bases to measure every polarization of the photons he receives. His randomness in selection ensures that, in the absence of knowledge of the correct basis, any form of eavesdropping and qubit measurement by an eavesdropper would introduce errors detectable. By measuring the polarization of a photon, Bob writes down the outcome as a bit value, 0 or 1, depending on the state detected. When Bob measures in the same basis that Alice has encoded, her bit will be perfectly reflected. Otherwise, the measurement is effectively random and not informative about the qubit Alice sent. This built-in uncertainty has turned out to be an important feature of QKD when detecting eavesdropping. After the measurement phase, Bob communicates his chosen measurement bases with Alice over the classical public channel. Important to note here is that he has not communicated the results of measurements; only the bases chosen are communicated. Alice then reports back which of her sent qubits were prepared in the same bases as Bob's measurements. Only the bits where Alice and Bob used matching bases are kept for further processing and form the raw shared

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

key. The bits that have been measured using mismatched bases are rejected. Those do not preserve correlated information. The quality and security of the final secret key depend on Bob's measurements being correct and reliable. Advanced techniques and meticulous calibration are taken to minimize measurement errors so that bits recorded by Bob can potentially match the original ones in Alice just where the bases agree. Although measurement is basically governed by the probabilistic nature of quantum mechanics, the precision required for the high security guarantees offered by QKD is cardinal. The process in measuring qubits by Bob is randomly selecting measurement bases, then there should be a proper and precise interpretation of polarization states, and finally, the actual outcomes are recorded. In the process of establishing a shared secret key that is secure and reliable, this step provides the basis for encrypted communication resistant to eavesdropping (Ricci et al., 2024) .

4. Public Discussion and Key Sifting Besides transmission and measurement steps in Quantum Key Distribution, the public discussion and key sifting are two procedures Alice and Bob execute in the process. The latter eliminates the possibility of an eavesdropper and will provide both of them with a shared secret key. It entails both quantum and classical channels, where both Alice and Bob compare their respective measurements. Once Bob has measured the polarization states of the received qubits, he and Alice engage in some kind of public discussion over a classical channel. Let me mention once again that this classical channel is authenticated. This means that Eve can listen to the communication but cannot alter it without any traces. Over the course of this discussion, Alice and Bob will reveal the bases that they used for each qubit; Alice will reveal which polarization states she sent and Bob will reveal which bases he used to measure each qubit. However, they do not reveal what the corresponding bit values are that are obtained from their measurements.

   The goal of this conversation is to determine which of the qubits were measured in matching bases. The corresponding bit values can only be trusted to be correlated if Alice and Bob have used the same basis for encoding and for measuring a qubit. For example, suppose Alice encoded a qubit using the rectilinear basis, and Bob measured in the rectilinear basis. Then, Bob's measurement corresponds to Alice's original bit. Conversely, if they chose the same bases then the result of the measurement is random and is useless for the generation of the key. This process called key sifting consists in comparing the sequences of chosen bases and keeping only the bits in which both Alice and Bob agreed upon the same base. Those bits that correspond to mismatched bases are discarded since they do not carry any meaningful information and do not contribute to the shared secret key. This removes the likely wrong bits and makes the remaining bits highly correlated to be used as a basis of

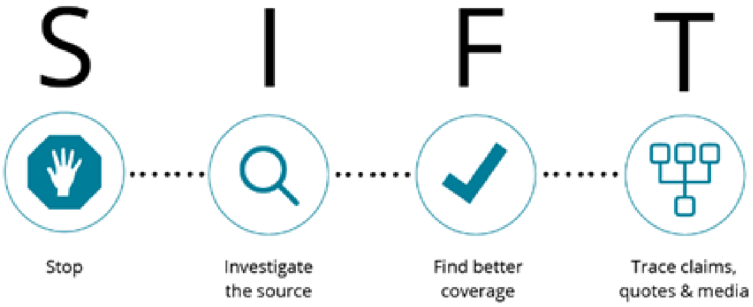

Figure 8. Working of SIFT

the secure key (see Figure 8).

Key sifting is essential in removing the probability that Eve has gained information through transmission. If Eve attempted to measure and capture the qubits, her interference would have changed some of the states of the qubits so the bases would have been mismatched, and the error rate in the key would have been higher. Discarding those bits where the bases were mismatched and retaining only those bits where the bases were correctly aligned, Alice and Bob could isolate a subset of their data that is likely free of eavesdropping attempts .

Efficiency, in short, is directly proportional to the choice of protocol selected and the quality of the quantum channel used. In protocols like BB84, approximately 50% of the qubits are likely to correspond to the same basis due to pure chance; hence half the length raw key after sifting. Utilize techniques that may include additional bases or optimized selection process to improve the effectiveness of the key sifting so that Alice and Bob can produce longer secret keys with greater security. In a nutshell, public discussion and key sifting are the two fundamental steps in QKD that will enable Alice and Bob to sift out the correlated bits that they can use as a secret key. They ensure a final secure and reliable key by publicly sending the measurement bases with the filtering of mismatched bits, thus allowing communication in encrypted terms with immunity to eavesdropping (Ricci et al., 2024) .

5. Error Checking & Security After the public discussion and key sifting, Alice and Bob then perform the error verification and security, which is an important step in the process of creating their shared secret key. These steps are actually meant to verify for any form of eavesdropping and correct errors that would otherwise give rise to

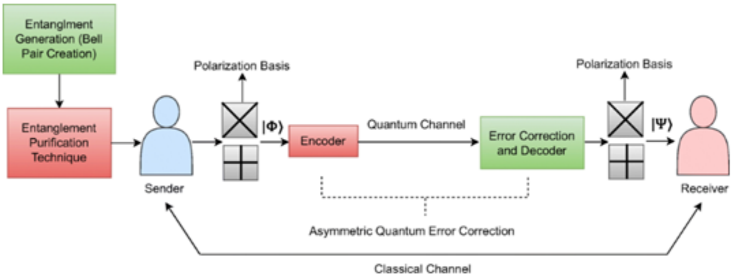
Entanglment Generation (Bell Pair Creation)
Entanglement Purification Technique
Sender
Polarization Basis
|Φ⟩
Encoder
Quantum Channel
Error Correction and Decoder
Polarization Basis
|Ψ⟩
Receiver
Asymmetric Quantum Error Correction
Classical Channel

Figure 9. Asymmetric Quantum Error Correction

defects along the quantum channel or through the measurement process (see Figure 9).

After the process of key sifting, Alice and Bob have raw shared key in bits representing their respective inputs, for which the respective bases happened to match while measurement. However, the raw key will possibly remain uncorrected for errors arising from a number of possible reasons. These include intrinsic noise in the quantum channel resulting from factors like photon loss or interference. A more diabolical reason may be for an adversary like Eve who sets out intentionally to eavesdrop on the communication. To address such differences, Alice and Bob carry out:

i Sample for Errors

Alice and Bob begin with the arbitrary selection of a subset of their sifted key bits, comparing this subset over the classical public channel. This subset is used as a sample with which to estimate the overall error rate in their key distribution. They are thus able to infer whether the error rate exceeds the threshold that may indicate the presence of an eavesdropper. If the error rate is good enough to lie well within acceptable limits, Alice and Bob may consider the key secure. On the other hand, if the error rate is significantly larger than this expectation, it could be a sign of Eve's actions to intercept and measure qubits with detectably disturbing disturbances on them; Alice and Bob could therefore abort the generation of the key to avoid possible misuse of a compromised key.

ii Error Correction

Assuming the error rate is sufficiently small, Alice and Bob advance into the error correction phase of the protocol. The objective at this stage is to locate and correct any errors between their raw key versions that will make sure the secret key shared between them is identical. Of course, there are many kinds of error

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

correction protocols that may be used, including the Cascade protocol wherein bit errors are iteratively corrected through controlled comparisons of bits. Alice and Bob can communicate through the classical channel with the aim of finding and correcting mismatched bits without revealing too much information regarding the key in the process of error correction. This is one of the highly required steps to ensure that at the end, the secret key perfectly synchronizes between the parties involved and eliminates residual errors that might creep and make it insecure.

iii Privacy Amplification

Alice and Bob then privacily amplify their secret key, even after error correction. That is, even with low error rates, Eve could have gained partial information about the key in this attempt. Privacily amplification generally employs cryptographic hash functions to the corrected key. Here, the length of the key reduces and thereby the possible information obtained by Eve minimizes too. Through compression in this way, Alice and Bob now are convinced that the final secret key is not only shorter but also secure, and any partial knowledge Eve may have of it is negligible. This step transforms raw key into an extremely secured final key that can surely be employed with confidence in encrypting and decrypting messages.

iv Security Assurance

Error checking, error correction, and privacy amplification together form a secure framework for QKD. All these have the result that: All Eve's attempts at eavesdropping are made with probabilities above threshold as the error rates would be increased. Error sources introduced at the quantum channel get corrected in such a manner that keys remain lossless Information that Eve might hold from before gets washed out, and whatever is left as a consequence is an adequate secure key. The security of QKD is independent of computational assumptions but remains completely guaranteed by the fundamental laws of quantum mechanics. This simply means that even as quantum computing will continue to advance, the secret key stays secure; hence, the future-proof solution in communicating securely.

Conclusively, error checking and security in QKD form a set of necessary processes that are aimed at proving whether the established shared key is correct or not and secure from possible eavesdropping or transmission errors. By means of careful sampling correction and amplification, Alice and Bob are thus able to build a secret key safely and reliably to ensure privacy and the trustworthiness of their encrypted communications (Ricci et al., 2024) .

6. Final Secret Key After passing through key sifting, error checking, and security enhancement phases of Quantum Key Distribution, Alice and Bob end their hard work: the final secret key. This key is the basis of secure communication, binding messages exchanged between them to remain confidential and tamper-proof.

   i Secure Key Establishment

   The final error correction and privacy amplification are performed at the point at which Alice and Bob have a sifted key-that is, a subset of bits where the measurement basis matched. Error correction reconciles all discrepancies that noise or potential eavesdropping may have caused so that both parties share the identical sequence of bits. Privacy amplification strengthens the key by shrinking the size of the key but deleting any partial information which an eavesdropper may have as well.

   Now, the key is both identical and secure, so no differing bits for Alice and Bob, and the key contains no important knowledge Eve may hold. Typically, the final key is much shorter than the raw key due to the loss during privacy amplification but is still long enough to achieve high-security levels for encryption purposes.

   ii Use of the Key

   Now, with the final secret key in hand, Alice and Bob can use this key classically to encrypt and decrypt their messages with an appropriate encryption technique, like OTP or AES. Theoretically, OTP is an encryption technique in which the key is used just once; the length of this key is equal to the length of the message itself, and it theoretically grants unbreakable security if appropriately deployed. For example, Alice can use the secret key in encrypting a plaintext message by mixing it up with the key using an XOR operation. Bob having access to the same secret key can then decrypt the ciphertext using the same XOR operation thus retrieving back the plaintext message. Security on this method depends solely on the secrecy of the key, an aspect perfectly guaranteed by the QKD process.

   iii Continuous Security and Key Renewal

   The secret key produced at the end of the QKD process can be used many times to encrypt several messages unless its privacy is breached in some form of reuse. In order to offer a better security, Alice and Bob can send new secret keys produced during the QKD process between their pairs at quite frequent intervals, so in each session of communication a new, secure key will be used to guard the communication. Further, with advancing quantum technologies as well as emerging threats, security parameters of the QKD system would be updated to maintain the strength of the secret key. This robustness ensures that the

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

secret key remains a valuable resource even in the event of shifting landscapes of technology.

iv Practical Considerations

Therefore, putting all this together into a real-world application involves integrating QKD into existing communication infrastructures. In particular, to establish the final secret key, generation and transmission of qubits may require specialized hardware and appropriate secure channels for the classical communications that are required during the phases of key sifting and error correction. Then, the system's efficiency and scalability determine how effectively the final secret key can be used by different platforms in different distances. Quantum repeaters, satellite-based QKD, and others are being explored more and more to bring out practical applications of QKD-generated secret keys further.

v Security Assurance

The last of these keys, then, is the realization of the promise of QKD: It's a fundamentally secure share of a secret key that's protected from any attempt at eavesdropping-proofed in principle by the absolute laws of quantum mechanics. Such assurance makes QKD one such cornerstone for future-proof secure communications that offers a level of security far beyond the limits of possible computation based on classical cryptographic methods.

In summary, the final key is an accurately derived and well-secure sequence of bits that Alice and Bob can safely use for protecting communications. Since this key is identical and free from the eavesdropping knowledge, QKD will successfully create a solid base for protected interactions that can provide safety against advanced threats for data (Ricci et al., 2024) .

6 Applications Of QKD

Quantum Key Distribution has emerged as an important technology toward strengthening the security aspects of communication systems (Wehner, Elkouss, & Hanson, 2018). Its special capability to detect eavesdropping and protect communications, based on the principles of quantum mechanics, makes it a candidate for a broad group of high-security applications. Some important applications of QKD are described below:

1. Secure Government and Military Communications

   Government and military establishments require secure and unidirectional communication channels to prevent the interception of any sensitive information that might be threatened by cyber-attacks. QKD offers an advanced technique that ensures confident communication in the face of prospective quantum computing threats (see

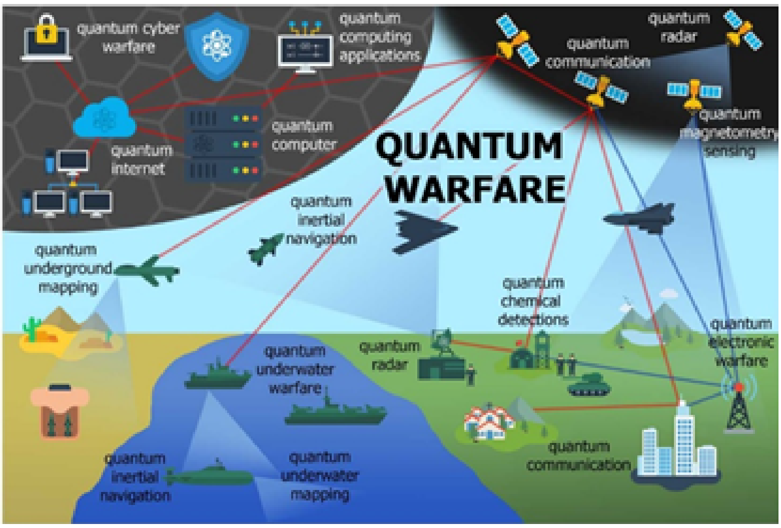
quantum cyber warfare
quantum computing applications
quantum radar
quantum communication
quantum internet
quantum computer
quantum magnetometry sensing
QUANTUM WARFARE
quantum inertial navigation
quantum underground mapping
quantum chemical detections
quantum radar
quantum underwater warfare
quantum electronic warfare
quantum communication
quantum inertial navigation
quantum underwater mapping

Figure 10. QKD in Military Communications

Figure 10). A government institution would use QKD for confidential encryption key-sharing, as one avenue for securing sensitive national security information against quantum attacks and from classical threats(Wehner, Elkouss, & Hanson, 2018).

2. Financial Transactions and Banking

   Data transmission over the financial sector is highly dependent on secure communication for online banking, share trading, and interbank communications. QKD can ensure that the encryption keys for secret financial information utilized in transaction protocols will not be transmitted to the attackers. QKD implementation in financial institutions will protect against potential quantum attacks and improve security and information privacy over digital payment systems and customer data (see Figure 11) (Wehner, Elkouss, & Hanson, 2018).

3. Healthcare Data Security

   The more digitized healthcare gets, the need to protect medical records and patient data requires fast and secure protection of such information. QKD can be applied in protecting sensitive health data exchanged between hospitals, laboratories, and other medical centres within and outside the walls of a hospital. This protects a patient's medical records' confidentiality and integrity while preventing cyber-attacks on healthcare databases (see Figure 12) (Wehner, Elkouss, & Hanson, 2018).

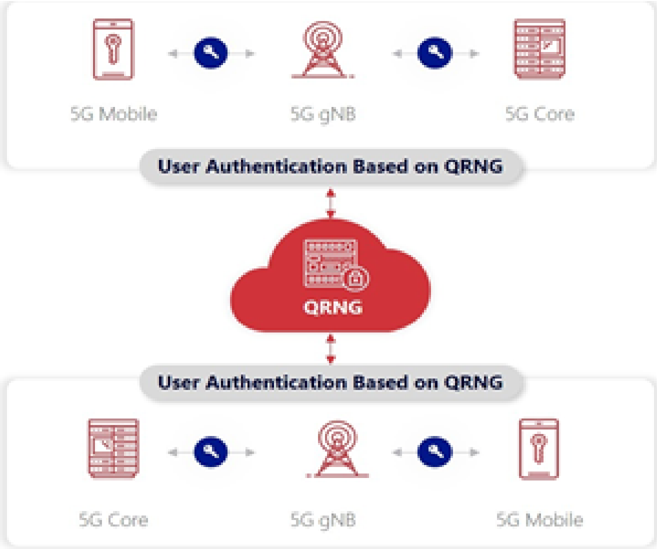
5G Mobile
5G gNB
5G Core
User Authentication Based on QRNG
QRNG
User Authentication Based on QRNG
5G Core
5G gNB
5G Mobile

Figure 11. QKD in Banking

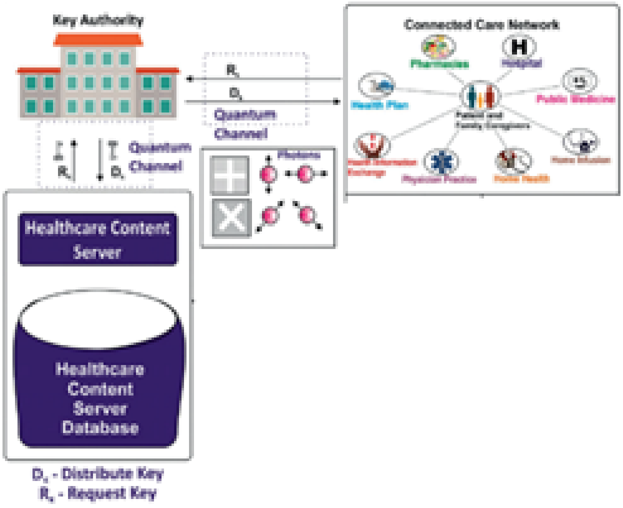

Figure 12. QKD in Healthcare

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

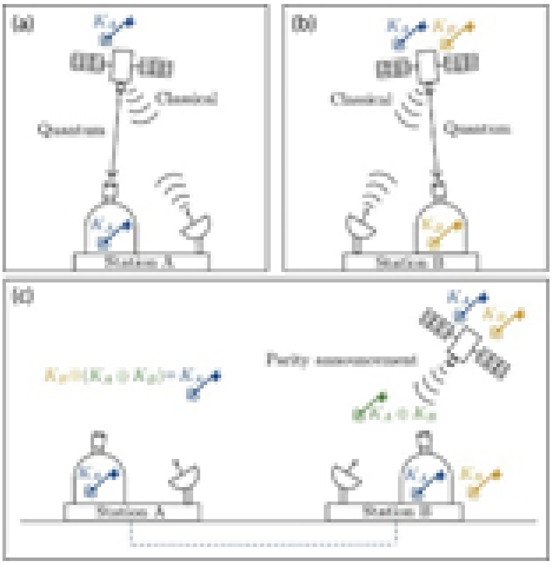

Figure 13. QKD in Telecommunications

4. Telecommunications Infrastructure

   Telecommunications networks carry very large amounts of data and are now highly vulnerable to advanced cyberattacks. QKD can be incorporated into these networks to protect communications of voice, video, and data over long distances. This can advance the protection of optical fiber networks against interception and eavesdropping of communications critical to governments and organizations (see Figure 13) (Wehner, Elkouss, & Hanson, 2018).

5. Secure Blockchain Technology

   However, blockchain technology is also vulnerable to attacks from quantum computers that have the capability of breaking algorithms which are in use today. QKD would provide a mechanism for extending the lifecycle of blockchain networks so that its cryptographic keys securing blockchain transactions remain impervious to quantum threats (Wehner, Elkouss, & Hanson, 2018) .

6. Protection of Critical Infrastructure

   In critical infrastructures, such as power grids, water systems, and transportation

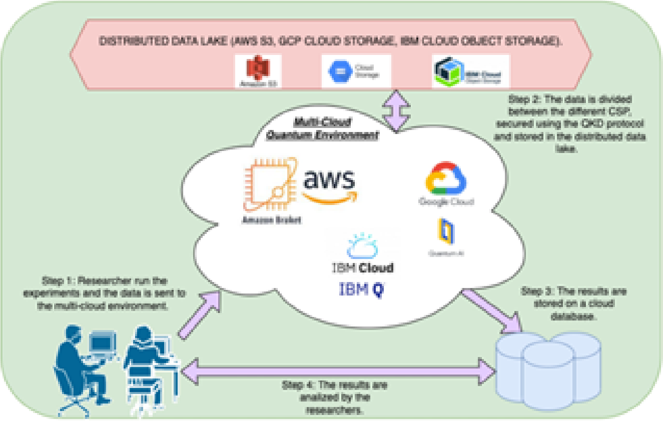
DISTRIBUTED DATA LAKE (AWS S3, GCP CLOUD STORAGE, IBM CLOUD OBJECT STORAGE).
Amazon S3
Cloud Storage
IBM Cloud Object Storage
Step 2: The data is divided between the different CSP, secured using the QKD protocol and stored in the distributed data lake.
Multi-Cloud Quantum Environment
aws
Amazon Braket
Google Cloud
Quantum AI
IBM Cloud
IBM Q
Step 1: Researcher run the experiments and the data is sent to the multi-cloud environment.
Step 3: The results are stored on a cloud database.
Step 4: The results are analized by the researchers.

Figure 14. QKD in Cloud Computing

networks, secure communication channels would be established. QKD would provide means of encryption of control systems and data flows in these infrastructures, thereby protecting against cyber-attacks that could lead to service disruptions or security breaches (Wehner, Elkouss, & Hanson, 2018).

7. Securing Cloud Computing

   As organizations keep more and more workloads in the cloud, they also create potential threats regarding data security. QKD can be introduced into the services of the cloud so that encryption keys for securing communications and data stored within cloud environments would be completely safe from eavesdropping, even future all-purposed quantum computers (see Figure 14) (Wehner, Elkouss, & Hanson, 2018) .

8. Defence Against Threats By Quantum Computing

   Much of the currently used encryption will be broken, including RSA and ECC (Elliptic Curve Cryptography), in large-scale quantum computers. QKD has an advantage because it provides a defense against these kinds of attacks since encryption keys are sent in a secure way and cannot be intercepted by an adversary no matter how big their computer is (Wehner, Elkouss, & Hanson, 2018).

In short, Quantum Key Distribution has a very wide area of application across sectors where the security of communication has to be guaranteed. All this ranges from secure

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

financial systems, national security, and cloud computing. QKD offers future-proof means of defense against the rise of quantum computing, with data being transmitted securely and reliably (Wehner, Elkouss, & Hanson, 2018).

7 The Transition To Quantum-Safe Cryptography

Some of the most important developments that are happening in the field of cybersecurity today including quantum-safe cryptography, also known as post-quantum cryptography. This is going to be a key development as we prepare for the advent of quantum computers. A quantum computer, unlike its classical counterpart that deals with information in bits (0s and 1s), operates on qubits, which can be in multiple states simultaneously because of an effect called superposition. Quantum computers are going to do some types of calculations exponentially faster than any possible classical machine could. The primary issue with quantum computers is the ability to break most of the encryption systems currently in use, including RSA and Elliptic Curve Cryptography (ECC). Specifically, these encryption schemes depend on problems that a standard computer cannot solve easily-such as factorizing large numbers for RSA or finding solutions for discrete logarithm problems for ECC. Here again, quantum algorithms such as Shor's algorithm are efficient for solving such problems, which puts these cryptographic systems at risk. To mitigate this risk, scholars have developed quantum-resistant cryptographic algorithms that are purported to resist all forms of quantum attacks. Such new algorithms exploit problems that are believed to be hard for both classical and quantum computers to solve. The main approaches include lattice-based cryptography and code-based cryptography, multivariate quadratic equations, hash-based cryptography, and isogeny-based cryptography, each presenting a different solution to the security challenges posed by the feature of quantum computing. Recent moves, for instance, have seen organizations such as the National Institute of Standards and Technology recognize the need to transition urgently towards quantum-safe cryptography. In 2016, NIST began a coordinated international effort to evaluate and standardize quantum-resistant algorithms. The process for selection and finalization of such algorithms continues to date for the establishment of safe standards well before the onset of large-scale computers. This transition to quantum-safe cryptography poses several challenges. First, some of the post-quantum algorithms require bigger keys and more computations than current methods, which could slow down systems and make the potential implementation complicated in environments like IoT devices. Further, updates to organizational infrastructure and protocols will be necessary, which will be a time-consuming effort requiring broad industrywide effort. Despite these challenges, transitioning to quantum-safe cryptography is important to preserving the privacy and integrity of digital communications in the future. Although quantum computers capable of breaking classical encryption have yet to enter reality, the cryptographic community

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

should take steps now to secure its future in a world where quantum threats may arise. Quantum-resistant algorithms and updating cryptographic systems could be adopted by organizations to protect their data and communications from any future quantum threats (Wehner, Elkouss, & Hanson, 2018).

8 Conclusion

Quantum computers will be shown to be a severe threat to modern cryptographic schemes like RSA and ECC, which are built around hard mathematical problems that are not possible to solve or are impractical to solve with classical computers but are easy to break using quantum algorithms like Shor's. This may indicate problems with secure communication, privacy of data, and even the integrity of systems. Quantum-safe or post-quantum cryptography is therefore being developed based on quantum-computer-resistant algorithms. Candidate families that have been promising are lattice-based, code-based, hash-based, and isogeny-based cryptography. These systems are being selected through efforts headed by NIST, but migration to these systems turns out to be daunting due to an increase in key sizes and computational demands. The migration to quantum safe cryptography is proactive in a proactive process in securing critical infrastructure, transactional financial processes, and digital communications well ahead of the development and deployment of quantum computers that can break classical encryption. Continued research and worldwide collaboration will ensure that the encryption remains strong for the quantum future.

References

Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-Quantum Cryptography. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-88702-7

Chen, L., L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, & D. Smith-Tone. (2016). Report on post-quantum cryptography (tech. rep.). NIST.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the Annual ACM Symposium on Theory of Computing, Part F1294, 212–219. https://doi.org/10.1145/237814.237866

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. International Journal of Advanced Computer Science and Applications, 9(3), 405–414. https://doi.org/10.14569/IJACSA.2018.090354

Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., Liu, Y.-K., Miller, C. A., Peralta, R. C., Perlner, R. A., Robinson, A. Y., Smith-Tone, D. C., & Alperin-Sheriff, J. (2020, July). Status report on the second round of the NIST post-quantum cryptography standardization process (tech. rep. No. 210).

DOI:10.48001/978-81-980647-5-2-4 | ISBN: 978-81-980647-5-2 | Copyright ©2024 QTanalytics®

National Institute of Standards and Technology. Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8309

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security and Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. IEEE Access, 12, 23206–23219. https://doi.org/10.1109/ACCESS.2024.3364520

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301

Shah, S., Munir, A., Waheed, A., Alabrah, A., Mukred, M., Amin, F., & Salam, A. (2023). Enhancing Security and Efficiency in Underwater Wireless Sensor Networks: A Lightweight Key Management Framework. Symmetry, 15(8). https://doi.org/10.3390/sym15081484

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS, 124–134. https://doi.org/10.1109/SFCS.1994.365700

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Wang, L.-J., Zhou, Y.-Y., Yin, J.-M., & Chen, Q. (2022). Authentication of quantum key distribution with post-quantum cryptography and replay attacks. https://doi.org/10.48550/arXiv.2206.01164

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412). https://doi.org/10.1126/science.aam9288

Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Pietro, R. D., & Erbad, A. (2024). A Survey and Comparison of Post-Quantum and Quantum Blockchains. IEEE Communications Surveys and Tutorials, 26(2), 967–1002. https://doi.org/10.1109/COMST.2023.3325761