Quantum Cryptography in Modern Cybersecurity

Md Shariar Sozol[1], Md Mostafizur Rahman[2], Md Minhazul Islam[3], Golam Mostafa Saki[4]

[1] Master of Cybersecurity (Extension) & University of Technology Sydney (UTS), Australia
[2] Master of Engineering (Extension) & University of Technology Sydney (UTS), Australia
[3] Master of Information Technology (Extension) & University of Technology Sydney (UTS), Australia
[4] MSc in Engineering Management & University of South Wales, United Kingdom (UK)

---***---

Abstract - This article tends to deal with the fast-evolving world of quantum cryptography, specifically the concept of quantum key distribution (QKD), which has significant importance in modern-day cybersecurity scenarios. The most notable feature of quantum cryptography is its ability to ensure safe communication through principles borrowed from quantum mechanics such as entanglement and superposition. The research comprehensively analyses discrete-variable protocols (DVQKD) and continuous-variable ones (CVQKD), closely investigating their potential roles as re-inventors of secure communications owing to increasing cyber threats. In principle, quantum cryptography is invulnerable to all forms of attacks; however, there are numerous challenges to its implementation including high deployment costs, technology limitations and complex integration with existing systems for protecting data. This paper presents an elaborate state of today's quantum cryptography capturing its advancements, active research efforts as well as barriers towards increased use in build systems based on resistance against attacks utilizing properties specific to quantum mechanics.

Key Words: Quantum Key Distribution (QKD), Post – Quantum Cryptography (PQC), Discrete-Variable (DVQKD) and Continuous-Variable (CVQKD), Quantum Superposition, Crypto-Attacks.

1. INTRODUCTION

People need more secure message delivery techniques due to the overwhelming importance of private communication in today’s world. Encrypting with secret keys is an essential aspect of cryptography that allows secure transmission via public channels even when there is a possible enemy. In modern cryptography secure ways to communicate between two distant users in the presence of other parties are not only researched but also implemented. These protocols are in such a way that any third party will not understand an encrypted message passed through public channels because it only displays unidentified messages just understood by sender and recipient.

Originating before the internet was invented, cryptography's primary purpose was to make messages not understandable to any third parties who might intercept them. Today, the field encompasses integrity checking, identity identification, secured computation and more alongside communication and military privacy. To do this they’re both sender and receiver use secure keys for encrypting and decrypting messages with these keys being determined through either intricate algorithms or real-world constraints such as the factorization of large numbers in modern cryptography. Although lengthy periods may be necessary for even present-day computers in order to compute key decryption, it cannot be assured that no one else has received it thus making it possible for an eavesdropper to know what it says.

1.1. Historical Background

Almost 49 years ago, Wiesner introduced the idea behind quantum cryptography, and today, there are commercially available devices for key distribution. Although written in 1970, the paper was never published until 1983 because no one was interested in it (Kumar et al., 2021). He spoke about the possibility of multiplexing two or three messages using quantum codes which can be used to generate profits by reading one message at a time and destroying the rest. In addition, he pointed out that quantum money is likely to have serial numbers as well as twenty perfectly reflecting boxes containing one single photon in any of four possible states: vertical, horizontal, right-handed circular or left-handed circular (Kumar et al., 2021). The first quantum cryptography protocol came into existence through Charles Bennet and Gilles Brassard with name BB84 in 1984 to use Heisenberg's uncertainty principle (Ciesla et al., 2020). But Richard Feynman of MIT created cryptography in 1981 when he suggested a basic design for a quantum computer (Ugwuishiwu et al., 2020). Feynman was able to sketch the possibility of ten times faster performance than that achieved by traditional computers. Since then many studies have been undertaken within the field of quantum mechanics following Feynman’s discovery of the concept.

Along similar lines, Ugwuishiwu et al. (2020) evaluated simultaneous. Shor’s algorithm was created in 1994 by American mathematician Peter Shor while he was employed at Bell Laboratory (New Jersey). The purpose of this specific algorithm was integer factorization. Shor even went ahead to argue that with optimal working conditions, i.e., without external noise or other forms of quantum interference, a quantum computer could easily break classical cryptographic systems like RSA. One huge drawback of classical encryption has been the big integer factorization problem that quantum computers solve through Shor’s method.

As such, there has been developed a concept known as quantum cryptography which aims at shielding conventional cryptographic systems from increasingly powerful computational attacks, including those launched by quantum computers. The theoretical foundations of quantum cryptography use concepts from quantum mechanics, such as quantum entanglement and the uncertainty principle, allowing for secure communication that supposedly cannot be hacked without leaving detectable traces.

1.2. Current Research

Quantum Key Distribution (QKD) remains a critical element of quantum communications. There are two kinds of protocols: the continuous variable (CV) QKD protocol and the discrete-variable (DV) QKD protocol (Djordjevic et al., 2022). In theory, quantum cryptography combines the protection provided by one-time pads with public key infrastructure (PKI) key exchanges and capabilities for rapidly spotting any efforts to mount a Man-in-the-Middle (MITM) attack on the transferred keys (Badhwar et al., 2021). The application of Quantum Cryptography is also known as Quantum Key Distribution (QKD) (Bloom et al., 2022) and comes with numerous forms of attacks such as breaking QKD, photon number splitting (PNS), denial of service (DoS), Trojan horse, intercept and resend (IR), thermal blinding attack among others (Ciesla et al., 2020). In theory, quantum key distribution (QKD) can still offer information-secure key exchange even in the age of quantum computers. Unfortunately, pre-sharing symmetric keys is the present method that helps to authenticate the classical channel required by QKD (Wang et al., 2021). All the aspects of quantum cryptography, especially through quantum key distribution (QKD), were reviewed as well as their operational mechanisms and weaknesses. Two broad categories of quantum communication networks have been recognized; one is known as “free space” quantum communications, which involves using QKD to facilitate communication amongst nodes linked by fiber (Ugwuishiwu et al., 2020).
Recent years have seen considerable advances in the potential of Distributed Ledger Technologies (DLTs) to guarantee accountability, redundancy and transparency, and as a result its use for a range of applications is becoming more widespread. The implementation of blockchain technology security relies mainly on public-key cryptography and hash functions. One area of concern that may arise from the rapid advances made in quantum computing are the powers of Grover’s and Shor’s algorithms, which are likely to compromise the foundations of hash functions and public-key cryptography in future (Fernandez-Carames et al., 2020). In order to overcome such challenges, it becomes necessary to develop a new blockchain system design incorporating cryptosystems against quantum attacks. This gave rise to the term post-quantum or quantum-proof or quantum-safe or resistant cryptosystems themselves (Fernandez-Carames et al., 2020). The current state and market prospects for quantum key distribution (QKD) and associated quantum communications technologies were also examined. So far, there have been various documented testbeds for quantum key distribution (QKD), such as Tokyo QKD Network; DARPA QKD Network; SECOQC Network based on Secure Communication Based on Quantum Cryptography (SECOQC). Unfortunately, these several QKD networks rely on dark fiber infrastructure alone (Djordjevic et al., 2022).

1.3. Knowledge Gap

Despite the fact that considerable strides have been made in the design and evaluation of protocols such as BB84 and its subsequent variations, this quickly progressing area within quantum cryptography has many questions yet unanswered. One of the key areas for development is how to incorporate quantum cryptography methods into the existing cybersecurity frameworks. There is little research on how scalable, secure and practical quantum technologies can be integrated into the digital infrastructure today. Another less explored financial aspect is the cost of universal implementation of quantum cryptography. These include expenses for building new facilities as well as their maintenance and employee training. By not addressing these concerns, governments and companies may risk becoming victims of this discrepancy if they do not consider changes in their cybersecurity measures before widespread utilization of quantum computers. For now, it appears that until post-quantum cryptography (PQC) systems advance beyond demonstrability challenges while evolving new security paradigms together with investigatory frameworks (are needed – potentially non-trivial to establish or may take time to develop and span periods or age periods); object that could otherwise prove to be insecurable should be replaced should such construction eventually become established.

Security levels relying on several years of thorough research (for instance, continuing to apply current reliable cryptographic systems like the ECC) or financial, temporal and computational resources (for instance, using a double encryption or signature scheme for deployment and application) (Bernstein et al., 2022). Furthermore, identity-based cryptosystems may benefit from new users joining a network. The Key Generation Center (KGC) is not involved in other stages such as issuing master key and user key using the identity of the user (like e-mail, job number, credit card number, smart card, MAC address, IO/EO etc.) (Johansson et al., 2023).

1.4. Hypothesis

This research paper review's underlying hypothesis states that although quantum cryptography provides a theoretically infallible means of safeguarding communications, it is difficult to integrate these technologies into current cybersecurity systems. Its overall efficacy and adoption rate in practical situations may be greatly impacted by a number of obstacles. This theory is based on the knowledge that quantum cryptography, in particular Quantum Key Distribution (QKD), offers a level of security that ensures that any attempt to intercept communications will be discovered. However, there are significant obstacles to the actual implementation and use of quantum cryptography technologies:

Technological Complexity: Since quantum cryptography systems are also complicated, it will need to change existing communication infrastructure significantly. This complexity can hinder scalability and quick deployment. For example, zero trust implementations such as access reviews that are continuous, least privilege access, and micro segmentation of networks can lead to high levels of intricacy. Thus, it increases recovery time from failure, veiling up on deployment schedules, increasing administrative expenses and operational expenditures as well requiring specialized engineering and operational capabilities (Badhwar et al. 2021). Furthermore, security analysis focuses on two important tasks: providing assurance that no honest channel user will lose money ever for participating in it; ensuring synchronization with time imposed by processing delay of blockchain (Xagawa et al. 2021).

High Costs: Taking into consideration the high cost of installation and maintenance of quantum cryptography systems, it is apparent that organizations aiming at using these technologies would incur some costs due to the specific tools and know-how required. For instance, any optical technology can be industrialized if devices for optical fibres and adaptive optical systems are developed. In fact, modern QKD tools have similar characteristics because of high costs related to their integrability. Generally, modern QKD systems include factors such as optical tables, precision optics, expensive and fragile single photon sources, as well as superconducting wire detectors. Basically, only professionals can operate these components hence they demand great attention on a constant basis (Bloom et al., 2022).

Integration Challenges: There are technological difficulties in amalgamating quantum cryptography with conventional cryptographic systems. Some of these barriers would include handling mixed systems, which call for simultaneous classical and quantum abilities, along with conformity to the existing structure. The accomplishment of incorporating quantum resistant materials into existing electronic devices will command most attention soon. Companies such as Microsoft and Google are engaged in developing possible additional hardware crypto processor solutions (Ciesla et al., 2020).

Restricted Practical Experiences: In contrast to traditional encryption methods, quantum encryption is still relatively fresh in real-life scenarios. Therefore, there is not much empirical evidence about its security and longevity against increasing classical and quantum threats. The underlying complexities necessitate a high-level skill set; thus, deploying it needs practical know-how (Badhwar et al., 2021).

1.5. Related Works

This section centers around the noteworthy contributions that have shaped contemporary quantum cryptography, particularly in its application to cybersecurity. The way of communicating openly through authorized classical public or insecure quantum channels can enable two parties to generate a secret key using a QKD protocol (Grasselli et al., 2021). Thus, for both parties to use the same symmetric key for encrypting and decrypting messages, there must be symmetry in key distribution between them and safe Ko-distribution protocols must be used (Wang et al. 2021). Many other techniques have since then emerged and applied himself, making QKD become the best example of quantum cryptography as well as one of the main uses of Quantum Information Technology. Within the context of one-time pad encryption, the Quantum Key Distribution (QKD) approach is often regarded as a reliable method for conveying a confidential key from one party to another. This protocol can be proven to be secure under two conditions: it is possible to collect information through the interference of signals with the aim of distinguishing between two non-orthogonal states and there is an authenticated public classical channel (Bloom et al., 2022). There are various transmission protocols available for QKD, including BB84, B92, Six-State Protocol (SSP), Ekert Protocol (E91), Continuous Variable Protocol (CV), among others (Ciesla et al., 2020). Similarly, there are many consensus protocols such as the most popular Proof-of-Work (PoW), which can be seen in Bitcoin), Proof-of-Stake (PoS) and different variations of Byzantine Fault Tolerance (BFT) techniques (Fernandez-Carames et al., 2020). Therefore the designer of any system intended for application should always take into consideration some potential trade-offs while keeping two things in mind; the frequency at which these codes are sent out concerning cipher-texts or signed messages utilizing them against the calculation speed when compared with available bandwidth (Bernstein et al., 2022). However, incidentally, the researchers have demonstrated that even quantum encryption can be susceptible to cyber-attacks. According to a recent study, quantum bit errors are among the greatest challenges to the advancement of quantum cryptography protocols (Alhayani et al., 2023). Consequently, it is imperative for quantum protocol to be trustworthy, precise and shielded against interference. The two principal issues in classical protocols are security and rectification (Kumar et al., 2021).

2. Quantum Cryptography Theory

Information is secured through quantum cryptography, which relies on laws of physics rather than on algorithms' complexity. In this regard a new paradigm for information safeguarding appears. Quantum theory of cryptography includes such fundamental quantum concepts as superposition, entanglement and quantum measurement's intrinsic uncertainty. Because of these properties it is possible to create cryptographic systems where measuring or intercepting quantum communications by an eavesdropper will always change their data state thus informing the legitimate users about a security breach. Moreover, this feature of quantum cryptography enhances the security itself while providing a novel approach to identifying and eliminating the risks. One of its most prominent applications is quantum key distribution (QKD), which embodies the use of quantum physics in creating secure communication channels. QKD defends against possible eavesdroppers strongly because it enables the exchange of cryptographic keys under security guaranteed by quantum principles. In this way, it may ensure fast detection of any intercepted communications.

2.1. Quantum Mechanics in Cryptography

Quantum cryptography's theoretical principles are extensively explored with a focus on the no-cloning theorem, quantum superposition and entanglement. Encrypting data while it is in transit or at rest is one of the cornerstones of data security in (cyber) security. In contrast to the traditional method of using a mathematical algorithm and an encryption key to “encrypt” data, quantum cryptography is a (new) type of encryption using the laws of quantum physics (Badhwar et al., 2021). Figure 2.1 shows major developments in quantum cryptography while figure 2.2 demonstrates key improvements in quantum key distribution protocols.

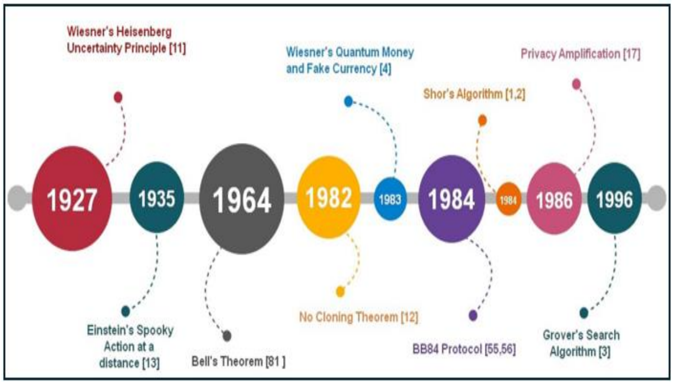

Wiesner's Heisenberg Uncertainty Principle [11]
Wiesner's Quantum Money and Fake Currency [4]
Privacy Amplification [17]
Shor's Algorithm [1,2]
1927
1935
1964
1982
1983
1984
1984
1986
1996
Einstein's Spooky Action at a distance [13]
Bell's Theorem [81]
No Cloning Theorem [12]
BB84 Protocol [55,56]
Grover's Search Algorithm [3]

Figure 2.1: Development Phases in Quantum Cryptography (Kumar et al., 2021)

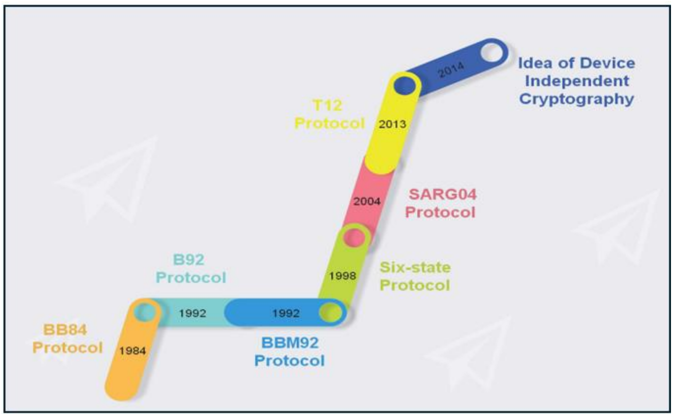


Figure 2.2: Development Phases in Quantum Key Distribution (Kumar et al., 2021)

2.2. Quantum Superposition Theory

A quantum is explained by a probabilistic wave function, also called the Schrodinger equation. The quantum’s exact position isn’t revealed by this function; instead, it displays how likely it is to find that particle in certain areas. With no observer, a quantum can be in any of its possible states, but quantum superposition could explain how it is possible for them to coexist (Alhayani et al., 2023).

Based on quantum superposition theory, quantum system could exist in numerous states at once until it is observed. When it comes to encoding data, this principle is extremely important in quantum cryptography. Quantum bits (qubits) are what make up the basic units of quantum information while classical bits are nothing more than a mere reflection thereof. The property that enables qubits to represent both ‘0’ and ‘1’ states at once is an example of why they differ from their classical counterparts (bi- bits). When we measure a qubit we finally arrive at one of two states that are determined by the measurement basis (Biasse, et al., 2023). Eavesdropping is always detected through these tools since transmission modifications disclose any graphical disorder encountered during verification processes. The abbreviation for “quantum bit”, or in short “qubit”, refers to the least unit of quantum information. Thus, this qubit is analogous with its classical counterpart; that is to say, they are alike in every respect possible. However, a qubit can exist in either of two basic computational modes represented as |0⟩ and |1⟩ symbols or even exist as some sort of mix-up between them. At its core, classical bits can only fall under such two states represented just like 0s or 1s (Biasse et al., 2023).

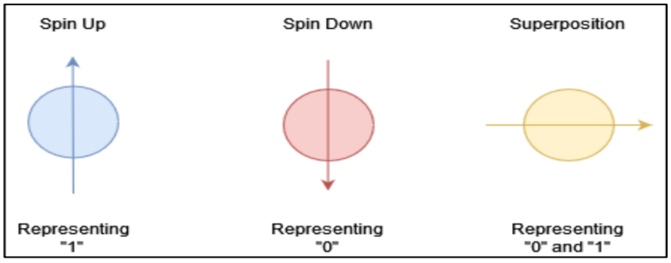


Figure 2.3: Superposition in Quantum Computing (Eka et al., 2022)

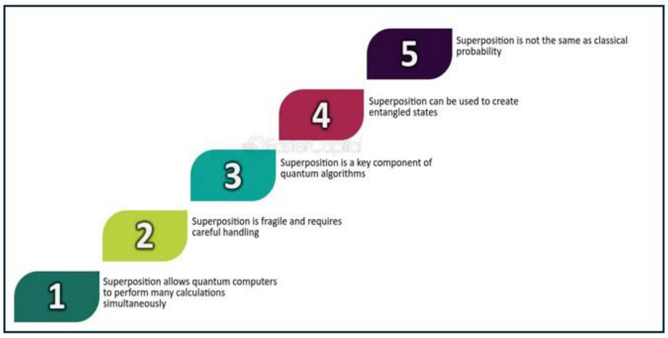

5
Superposition is not the same as classical probability
4
Superposition can be used to create entangled states
3
Superposition is a key component of quantum algorithms
2
Superposition is fragile and requires careful handling
1
Superposition allows quantum computers to perform many calculations simultaneously

Figure 2.4: The Concept of Superposition in Quantum Computing (FasterCapital, Blog Post)

Superposition is not just a theoretical concept; it is an actual occurrence that has physical proof behind it. In quantum science, it is possible for a particle to be simultaneously in two or more states. For instance, in contrast to traditional bits which must be either one or zero at all times, qubits can take on any value between the two. However, the states of superposition are not random or arbitrary. They depend on the particular quantum algorithm that one is working with. After processing all possible solutions at the same time using a quantum computer, its final output will measure qubits’ ultimate condition to determine the answer. This approach is much quicker than classical computation where possible solutions are analyzed step by step.

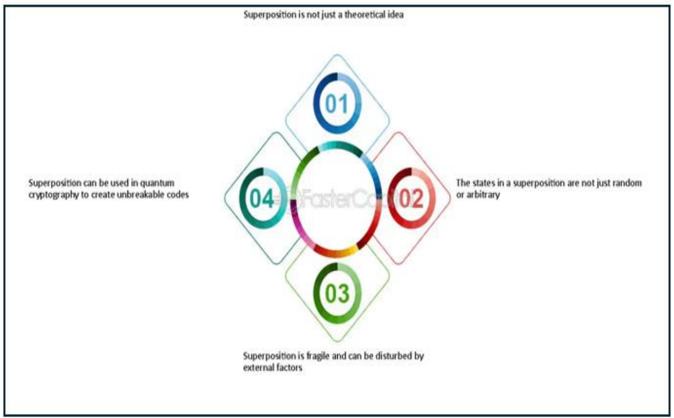

Superposition is not just a theoretical idea
01
Superposition can be used in quantum cryptography to create unbreakable codes
04
02
The states in a superposition are not just random or arbitrary
03
Superposition is fragile and can be disturbed by external factors

Figure 2.5: Role of Superposition in Quantum Cryptography (FasterCapital, Blog Post)

2.3. Quantum Entanglement Theory

Entanglement (more than one particle interacts) are pairs or multiple particles interacting with themselves even to pairs. Even when widely stretched, the particles cannot be separately defined, hence affecting their exclusive behavior. This is the power of quantum mechanics. Bell states, or EPR pairs, are some of the most basic examples of quantum entanglement (Djordjevic et al., 2022). More so, Djordjevic et al.,2022 stated that when qubit from a pair got measured then an instant collapse will happen at another regardless of how far apart, they are. This property is why we can use quantum entanglement for encryption. The E91 protocol was presented by Ekert as an application in quantum key distribution where it uses this unique characteristic of quantum July 2023. Therefore, several EPR pairs will be needed for quantum key distribution.

In a prospect, it is expected that scholars will come up with large quantum webs where all the members of that group can have one-to-one privacy in their conversations through QKD due to quantum entanglement (Grasselli et al., 2021). The last thing is that long-distance quantum key distribution mostly depends on quantum entanglement. Eavesdropper-absent entanglement can be achieved when there is perfect connection between two qubits. Entangled states serve as a basis for quantum cryptography (Kumar et al., 2021). BBM92 and E91 are examples of entanglement-based protocols (GSMA, 2021).

2.4. The No-Cloning Theory

In 1970, scientist James Park discovered the no-cloning theorem (Ciesla et al., 2020). This theorem states that it is not possible to copy any random unknown quantum state. Likewise, Ugwuishiwu et al. (2020) say that the inability to clone a quantum system is called a quantum no-cloning feature. Unlike in classical Internet where bits can be copied within a node or between nodes of the network, GSMA (2021) noted that no-cloning theorem prohibits the duplication of unknown qubits thus it is not possible with Quantum Internet. Consequently, although a qubit (which is a photon’s inner state with information) can be sent directly to a distant node along its fibre link, it may degenerate due to attenuation or noise meaning that there would not be any possible way to recover quantum information by measuring or duplicating it. According to this theorem arbitrary unknown quantum states cannot be replicated exactly. This property of quantum information distinguishes it from classical information which can be duplicated in full and serves as the basis for quantum communication security techniques. However, Ciesla et al., (2020) asserts that there are no copying ways in this area based on the premise of no-cloning theorem.

3. Quantum Cryptoanalysis

Modern cryptography relies on key security to be determined by practical constraints like number factorization or complex algorithms. Quantum cryptoanalysis looks closely at conventional cryptographic schemes using unique abilities of quantum computers. Grover’s Algorithm and Shor’s Algorithm can be viewed as important algorithms that indicate how cryptoanalysis might be conducted through quantum computing. The two of them greatly alter the security protocols of contemporary cryptographic procedures.

3.1. Shor’s Algorithm

The quantum method that is known as Shor’s algorithm was developed in 1994 by Peter Shor (Ciesla et al., 2020). It is capable of efficiently computing discrete logarithms and factoring large integers. In essence, Shor’s algorithm was devised to find any given number’s prime factors. Shor's algorithm has capability to factoring big integers and it also computes discrete logarithms with efficiency. This capability is essential since it has immediate effect to the security system of encryption techniques such as RSA and ECC that allow for the problems solving difficulty in their foundations (Ciesla et al, 2020). The first part can be done using a classical computer and all of its operations are carried out through logical gates (Ciesla et al., 2020). In addition, Ciesla et al. mentioned two parts into which Shor’s algorithm can be divided: the first is possible to perform on classical computers while in June 2001 IBM was able with a 7-qubit quantum computer implement the second part of Shor's algorithm.

3.1.1. Rivest-Shamir-Adelman (RSA)

RSA stands for Rivest-Shamir-Adelman. This PKI cryptosystem serves to secure and transport sensitive data in transit (Badhwar et al., 2021). It was in the year 1978 when the RSA algorithm was first made public and it included each component that is presently found in public-key cryptosystems (Ciesla et al., 2020). At the same time, Ciesla et al (2020) also clarified that the RSA technique creates a pair of keys using two huge prime numbers. One of the keys is referred to as the public key while the other key is called a private key. The public key does not reveal any information about how to get the private one from it. According to Ciesla et al.(2020), multiplying 397 by 661 gives 262,417 which is an easy answer but factoring back to get 262,417 is much harder (Badwar et al 2021). This makes it harder as you increase the size of the prime numbers. In 2012 two research teams from US and Europe made the unbelievable revelation that around 27,000 of these RSA had been dumped into the open (Ciesla et al., 2020): there was no security in those keys. Researchers used multiple databases including some keys found at Michigan Institute Technology (MIT). Moreover, they are in addition to those provided by the Electronic Frontier Foundation (EFF). The researchers analyzed a total of seven million public keys. Yet, one may assert that the RSA remains a secure cryptosystem largely; it has not been almost completely broken into. Presently, there are no good reasons to give up on it (Ciesla et al., 2020).

3.1.2. Employs Elliptic-Curve (ECC)

In cryptosystems with security based on classical hard problems for any polynomial time algorithm, Elliptic Curve Cryptography (ECC), thus employs a collection of elliptic curves that are non-trivial over finite fields (Ciesla et al., 2020). The effect of quantum computers on IT systems has been warned by organizations such as NSA and some cryptographic suites heightened to the ECC level (Fernandez-Carames et al., 2020). On the contrary, Alhayani et al. (2023) argued on the QSS protocols for using well-known security techniques like elliptic curve encryption. The implementation of elliptic curve cryptography in real-time applications is complicated and assessing whether its implementation exist is even more complicated. Although ECC-based QSS has less error rates than four-party QSS, it does not have high security information. In order to overcome this limitation, hyper elliptic curve encryption has been suggested. Evaluation of quantum secret sharing in two, three and four parties. Based on total time, encryption time, error rate and decryption time hyper elliptic curve cryptography is applied.

3.1.3. Post – Quantum Cryptography (PQC)

Post-Quantum Cryptography is an urgent requirement as evidenced through the threat posed by Shor's algorithm to existing cryptographic frameworks. Post-quantum cryptography (PQC) is a different strategy to QKD. PQC denotes a range of cryptographic techniques believed to be immune from attacks using quantum computers. Alas, as hinted at here earlier, PQC also depends upon unproven hypotheses; hence there are some algorithms that could become useless if more sophisticated quantum algorithms were designed (Ciesla et al., 2020). At the same time, Cheon et al. (2022) argue that when implementing Post-Quantum Cryptography (PQC) systems on embedded devices, traditional encryption methods also face similar challenges using embedded devices. On the other hand, since Shor's method can address factorization together with discrete logarithms on a quantum machine, it is indeed a threat to conventional public-key encryption. This is because scalable quantum computers will eventually become available. Our drive towards moving from standard public key cryptography towards post quantum cryptography (PQC) has been compelled by the burgeoning development of quantum machines (Xagawa et al., 2021).

3.1.3.1. Hash Based Cryptography

The hash-based cryptography has the aim of taking advantage of digital signatures together with the security features of cryptographic hash functions. Hashing-based techniques are distinguished by being simple and resistant to quantum attacks. They basically deal with stateful systems like Extended Merkle Signature Scheme (XMSS) and stateless systems like Leighton-Micali Signatures (LMS) (Ciesla et al., 2020). There exists a Merkle tree structure in which a single top hash, known as the Merkle Root, can authenticate a whole tree of hashes produced from signed messages. These algorithms that are recognized by NIST are ideal for environments requiring high level of protection against quantum assault especially in applications where long-term security is crucial; this includes digital signatures.

3.1.3.2. Code Based Cryptography

The use of error-correcting codes in code-based cryptography, which was first proposed by McEliece in 1978, is a way to ensure security of digital communication (Ciesla et al., 2020). The well-known security of this method has to do with the fact that it's extremely difficult to decode the message – or rather syndrome decoding. This is code-based systems' key advantage since its fundamental methodologies remain intact against possible quantum attacks. Historically, such systems have been known for their large key sizes; however, contemporary modifications aim at making them more user-friendly and efficient even when they are used in secure transmissions involving quantum computing contexts.

3.1.3.3. Multivariate Cryptography

The difficulty with multivariate polynomial equation systems over finite fields serves as a foundation in multivariate cryptography, and it is a problem that neither classical nor quantum attacks can crack at the moment. This kind of cryptography has primarily been applied in encryption algorithms and digital signatures. Among the oldest and best-known systems are Hidden Field Equations (HFE) proposed by Jacques Patarin (Badhwar et al., 2021). By using complex polynomial equations, they increase security by concealing the link between public and private keys. Thus, there is much respect for the efficiency of multivariate methods and their boundless possibility to ensure safety after the advent of quantum computers.

3.1.3.4. Lattice Based Cryptography

Lattice-based cryptography is grounded in the complex issues associated with lattices such as Closest Vector Problem (CVP) and Shortest Vector Problem (SVP), which resist attempts to crack them made by quantum computers. Examples of lattice based types of this technology includes digital signatures, homomorphic encryption schemes entirely and encryption algorithms among others. Lattice methods have strong security and wide flexibility since they can encode information in a way that makes it feasible for computers with encoding abilities but very hard to decrypt without correct keys. These are necessary for cryptography that will survive beyond its time due to their various uses ranging from securing cloud data to enabling private computations on encrypted information (Ciesla et al., 2020).

3.1.3.5. Homomorphic Encryption

Homomorphic encryption permits processing of encrypted data in a way that would yield the same result if they were decrypted. This type of encryption is particularly important in cloud computing, where users can perform computations on their data without accessing its unencrypted versions, as well as in privacy-preserving data analysis. It makes it possible to carry out very advanced arithmetic on encrypted data through operations such as addition and multiplication. However despite the fact that fully homomorphic encryption (FHE) techniques are becoming more popular, there are still several issues related to computational efficiency and noise management during encryption stages (Ciesla et al., 2020).

3.1.3.6. Device Independent Cryptography

Zhao and others have experimentally shown the very first hacking attempt in quantum, also known as the time-shift attack against a commercial QKD system (Kumar et al., 2021). Lydersen and others were the first to come up with an idea of using detector blinding attacks for obtaining entire secret keys. There is a loophole in QKD system that makes side-channel attacks possible. To avoid these types of attacks it was suggested to employ full-device independent QKD. In Full-device Independent Quantum Key Distribution (DIQKD), quantum apparatuses are perceived as black boxes receiving classical input while emitting classical output. Moreover, implementing entanglement-based devices over long distances becomes more complicated than for other distance-based communication. The security of quantum key distribution mechanism depends on how trustworthy the device are. In device independent cryptography (Kumar et al., 2021) there is no guarantee that the quantum device will work as it should be.

3.2. Grover’s Algorithm

Cao and Ma first discussed multiparty quantum key agreement using Grover's search method (Kumar et al., 2021). They explained how their protocol worked on a five-party system in addition to comparing it with current protocols. Grover's approach enables an unstructured key searching problem to be solved using few plaintext-ciphertext pairs (Biasse et al., 2023). In the future, integrating quantum resistance into present-day electronics is one of the major concerns. In order to find a possible option for additional hardware cryptographic processor solution, large companies such as Microsoft and Google are currently doing research works. Nowadays, many hash algorithms are assumed to remain safe against quantum-based attacks. However, there might be some ways to go around them though; for instance, Grover’s method can still be more efficient (Fiasse et al.,2023).

The way Grover’s algorithm works is that it brings apparent security down in symmetric cryptography but still not as much as Shor’s algorithm. For example, if one were to use a 256-bit encryption key which is believed to be resistant against conventional attack, this will still have the same level of vulnerability when compared to an attack using Grover’s method with a 128-bit key (Ciesla et al., 2020). The simple way of making cryptographic systems resistant against threats posed by this method is by doubling the lengths of keys. In this way, the increase in computer speed gained through Grover’s method can be offset to some extent with regard to maintaining close security levels (Cheon et al., 2022).

4. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is one of the most capable services for security in the quantum age, particularly focusing on data transmission in network systems. A mutual secret key can be created between two persons that can be used to encrypt or decrypt respective messages. In addition, there is a predicted increase in market size of QKD to USD 12 billion within five years which has led to increased interests towards its highly secured Use cases (Johansson et al., 2023). Badhwar et al. (2021) mention that QKD was the technology applied in establishing secure keys through secure point-to-point or link communication networks; whereas Djordjevic et al. argue that QKD is not yet widespread among common techniques due to some constraints like slow production rates of long keys and frequent operation on large distances. One major weakness of QKD technology lies in its ability to collect relevant data despite quantum channel noise towards the establishment of a secret key. For this reason, various cryptographic protocols exist.

4.1. BB84 Protocol

Charles Bennett and Gilles Brassard brought forth the first quantum cryptography protocol known as the BB84 (Ciesla et al. 2020) in 1984. Four distinct states of photon polarization, which can represent two different forms of data, are incorporated into it. In such a way that Alice who sends them randomly chooses photons in one of these four possible states and sends them to Bob who is the receiver (Cheon et al., 2022; Djordjevic et al., 2022). Bob makes random measurements on photons that enter either of the two bases where he may consider measuring them on arrival. After broadcasting, Alice and Bob compare their respective bases publicly without telling each other about their measurements; only those results using identical bases will be retained while all others will be discarded. Thus, is formed the common secret key from this group of measurements.

4.2. E91 Protocol

Artur Ekert's E91 protocol is based on the quantum entanglement of particles (Kumar et al., 2021). On the other hand, BB84 employs prepared quantum states while E91 utilizes pairs of entangled photons that sent and receive by both parties (Ciesla et al., 2020). This means that when measuring them randomly, people will find out that measurements are not independent but correlated. Breaking Bell's inequalities (Kumar et al., 2021) can be used to inform when there is an intercepting spy using quantum mechanics principles which suggests that local systems in classical physics cannot fully explain certain correlations between entangled particles.

4.3. B92 Protocol

The B92 is in essence a more advanced version of the Charles Bennett protocol (Ciesla et al., 2020) who is famous for developing BB84. B92 has two polarized states contrary to the BB84 which has four polarized states, Moreover, no basis (rectilinear or diagonal) needs to transmit in order to sift. Though it is less secure than BB84; easier to implement.

4.4. Six State Protocol

Despite containing only four states of polarization BB84 comprises six states of polarization (comprising three orthogonal bases) (Ciesla et al., 2020). Because whenever eavesdropping is performed on SSP implementation, error rates are very high and thus it is highly successful in revealing perceive malicious actors. This technique still presents an added risk of data loss, despite being regarded as one of the safest protocols.

4.5. Continuous - Variable (CV) Protocol

In fact, the measurement of amplitudes instead of individual photons using continuous variable (CV) method is another way to do it. In continuous variable protocols, there is no need for any photon counting devices; in discrete variable protocols however, these devices tend to slow down the process. Although they are usually faster while in operation (Ciesla et al., 2020). CV procedures typically lead to more errors than they do in the case of those that are discreet.

5. Crypto Attacks

We will discuss several kinds of QKD-focused crypto-attacks because these will be an issue in the coming future.

Photon Number Splitting (PNS): In an ideal world, when transmitting Bob one photon of time, Alice would make use of the BB84 protocol. However, during this transmission and because it is difficult to produce single photons in most instances, more than one photon are occasionally sent in BB84. This makes splitting the photon numbers possible. In this way, some of the photons are intended for Bob while others are intercepted by Eve who acts as a spy. On account of the very low rates of quantum mistakes (that is, loss of a photon) in this attack vector, both legitimate parties will think that they are the only ones engaged in on the transmission (Ciesla et al., 2020). In turn this leads to a situation where Eve who is completely invisible knows exactly what Alice is trying to say to Bob.

Denial of Service (DoS): Compared to bombarding a server with requests, as is done during a traditional denial-of-service attack (DoS), quantum environments make it easier for attackers to break open fibre optic cables (Ciesla et al., 2020). In this case, the unsealed optical quantum transmission devices would be so blocked that the light could not go through. The goal of a quantum denial of service attack is simply to disrupt any operations without acquiring any information phone number.

Trojan Horse Attack: A big pulse attack is another term for a Trojan horse attack in the context of QKDs. However, there are important differences between quantum and classical Trojan horses with regard to the method used by them (Ciesla et al., 2020). During an instance of this kind quantum based Trojans would involve shooting powerful beam of laser light into some quantum channel before analyzing its return reflections a far cry from using some malware package. Just a few reflected photons are enough for an eavesdropper to find out one of the legitimate parties' fundamental choices.

Intercept and Resend (IR) Attack: Eve, the eavesdropper, intercepts Alice's intended photons to Bob and uses a different set that she has measured already. Statistically, Eve can identify the basis right 50% of the time, while Bob's estimation for Eve's base is 50% accurate only. This means, therefore, there would be a noticeable error rate of 25% (Ciesla et al., 2020). The Intercept and Resend with Faked States (IRFS) attack variant does not prioritize guessing original basis states. Instead, it is aimed at producing light pulses that are detectable by Bob. Alice and Bob think they are working with pristine quantum states oblivious to what Eve is doing during their interactions giving room for spying.

Thermal Blinding Attack: Thermal blinding entails manipulating voltages in quantum circuits using short strong triggering pulses and continuous-wave light. At times even without raising the qubit error rate which would have served otherwise as an alert, this approach can break open a complete key or password. The Clavis 2 QKD system has been breached by this type of attack vector at least since 2020 along with other technologies like quantum entanglement (Ciesla et al., 2020).

Man in the Middle Attack: Man in the middle attacks are common occurrences in the classical realm and can take place on any unauthenticated application of QKD (Ciesla et al., 2020). This type of attack might focus on the calibration step for establishing a QKD link specifically. By initiating a wicked condition in the transmission of the signal, an eavesdropper may gain explicit information about the final key. The BB84 protocol and its offsprints is specifically pointed by this attack.

6. Applications of Quantum Cryptography

Quantum cryptography holds great promise for transforming cybersecurity in the face of evolving threats. There are a wide range of uses for quantum cryptography. A few practical uses for quantum cryptography are shown in the table below –

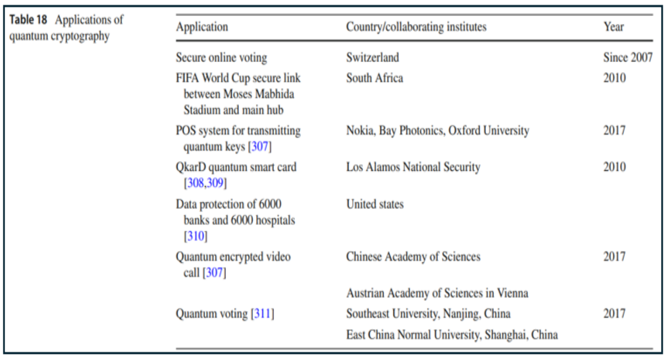


Table 18 Applications of quantum cryptography

Application	Country/collaborating institutes	Year
Secure online voting	Switzerland	Since 2007
FIFA World Cup secure link between Moses Mabhida Stadium and main hub	South Africa	2010
POS system for transmitting quantum keys [307]	Nokia, Bay Photonics, Oxford University	2017
QkarD quantum smart card [308,309]	Los Alamos National Security	2010
Data protection of 6000 banks and 6000 hospitals [310]	United states	
Quantum encrypted video call [307]	Chinese Academy of Sciences	2017
Quantum voting [311]	Austrian Academy of Sciences in Vienna Southeast University, Nanjing, China East China Normal University, Shanghai, China	2017

Figure 6.1: Applications of Quantum Cryptography (Kumar et al., 2021)

6.1. Quantum Communication Network (QCN)

In the past decade, there has been a lot of progress in the area of quantum key distribution (QKD). Basically, QKD is about preserving the secrecy of communication by using quantum mechanics principles. It is believed that extending existing telecommunications networks with QKD will make them safe from eavesdropping (Kołodyńska & et.al., 2017). In this paper we will discuss how global governments are investing heavily in establishing secure quantum communication networks. Among other things, QCN will enable to tackle problems related to both discrete variable and continuous variable QKD schemes (Cai et al., 2017). They say that the heterogeneous cluster-like QCN has two uses (Khan et al., 2019): teleporting any arbitrary quantum state between two nodes within the QCN; enabling distributed quantum computing; and enabling next generation cyber security systems. The first quantum internet demonstration was carried out by the Chinese Academy of Sciences along with its Austrian counterpart.

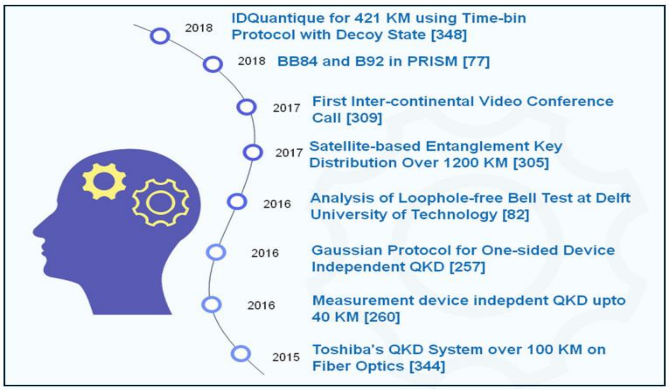

2018 IDQuantique for 421 KM using Time-bin Protocol with Decoy State [348]
2018 BB84 and B92 in PRISM [77]
2017 First Inter-continental Video Conference Call [309]
2017 Satellite-based Entanglement Key Distribution Over 1200 KM [305]
2016 Analysis of Loophole-free Bell Test at Delft University of Technology [82]
2016 Gaussian Protocol for One-sided Device Independent QKD [257]
2016 Measurement device indepdent QKD upto 40 KM [260]
2015 Toshiba's QKD System over 100 KM on Fiber Optics [344]

Figure 6.2: Major Experimental Work Progress in Quantum Cryptography (Kumar et al., 2021)

In an endeavor to build a secure video calling system, the universities tested intercontinental quantum communications. The initial packets of light were sent successfully to Micius satellite located in China from as far as 1,200 kilometers away. Thereafter, they were beamed towards Europe by the satellite after it passed over China (Ugwuishiwu et al., 2020). This led to the establishment of a truly reliable fiber-optic connection that extended 7600 kilometers between Austria and China (Kumar et al., 2021). Such a development improved chances for establishment of a possible quantum internet (Ugwuishiwu et al., 2020). The subsequent diagram illustrates the various experimental attempts in quantum cryptography.

6.2. Quantum Key Distribution (QKD)

Primarily, Quantum Key Distribution (QKD) gets a lot of attention from scientists and researchers, although one of the key applications in this field is secure communications. In QKD, qubits known as polarized photons serve as a medium for delivering data signals. This allows for high security because any action of measurement or duplication on these qubits that are themselves in an uncertain state alerts both sender and receiver about an ongoing wiretapping mechanism (Djordjevic et al., 2022). As an extreme secure use-case, Quantum Key Distribution (QKD) has been on rise during the past few years; within a decade period $12 billion USD are expected to add value to the market (Johansson et al., 2023). A recently established EuroQCI aims at establishing a European quantum communication infrastructure. Good thing about systems based on QKD is that they guarantee information-theoretic security (ITS), while other post-quantum primitives assume computational security (Johansson et al., 2023). It was quantum-mechanical principles use that sparked off Quantum Key Distribution (QKD), a major milestone in safe communications increasing data protection drastically. The main two groups into which QKD protocols fall are Discrete-Variable (DVQKD) or Continuous-Variable (CVQKD) (Djordjevic et al., 2022).

The BB84 protocol has pioneered DVQKD that employs unique photons' quantum states for information encoding. However, it comes with disadvantages such as noise sensitivity in the environment and difficulty in producing single photon sources. In contrast, Continuous variable QKD (CVQKD) which modulates continuous quantum variables like phases and amplitudes is gaining popularity in quantum communication because of its advantages against noise and capability of integrating seamlessly with existing optical communication systems (Djordjevic et al., 2022). The various application areas of QKD have varying timelines, target costs and system requirements. QKD Optical links are probably the most recognized application as well as the first likely to enter the market. For example, data centers can be located at a distance of several kilometers from one another, something that can easily be achieved via Qkd. Large service providers might also incur little effort in constructing infrastructure dedicated solely to quantum communications (GSMA, 2021).

6.3. Point-to-Point Link

For securing point-to-point communication lines, quantum key distribution (QKD), the main method of quantum cryptography, is widely studied. To secure the transmission of sensitive information, banks, insurance groups and health care providers are examining QKD systems. In 2008, the SECOQC project in Europe utilized quantum encryption to maintain data integrity and confidentiality (Badhwar et al., 2021). This project aimed at establishing a universal communication channel utilizing quantum cryptography for secure communications and information transfer by preventing sniffing, decryption or illegal cryptanalysis of data packets. The technique used to provide a safe key through secure point-to-point or link communication networks was enabled by QKD (Badhwar et al., 2021). In the figure below, QKD systems in the point-to-point configuration are shown.

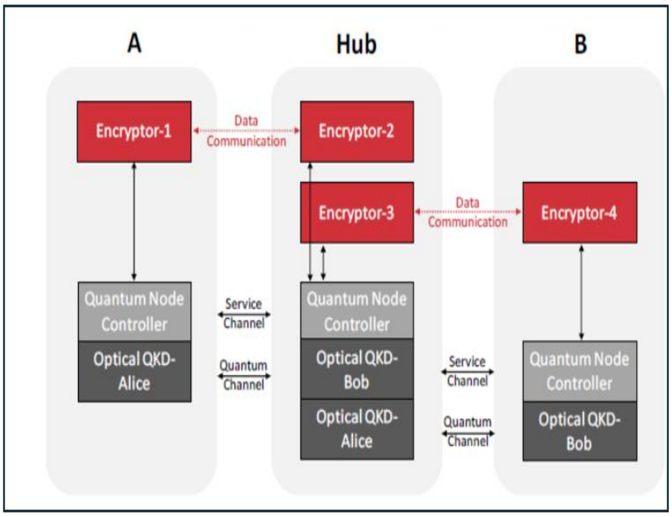


Figure 6.3: QKD systems in Point – to – Point Configuration (GSMA, 2021).

6.4. Key Generation

The creation of random numbers is an imperative task due to its utilization in most cryptographic protocols. And besides, random numbers are applied in games, lotteries, simulations and numerous other fields. However, it is not easy to create them and may lead to problems in certain applications (Pirandola et al., 2020) since low quality random numbers are not recommended as a matter of importance for some uses. On the other hand, two distinct prime numbers are utilized by RSA algorithm to generate numbers. Quantum key distribution (QKD), which is a part of quantum cryptography that uses principles of quantum mechanics, alters key production and ensures very secure distribution between the parties that are communicating. Unlike conventional means such as RSA where key generation depends on the difficulty level of computation problems- this method employs particle's quantum states for safe key exchange. This RSA algorithm was first developed in 1978 (Ciesla et al., 2020) as it contained all the components used by present-day public key cryptosystems. Rivest-Shamir-Adleman can be abbreviated as RSA and this was introduced by three people (Fernandez-Carames et al., 2020). Ciesla et al . (2020) also stated that despite its strong security features, RSA is a very slow approach to encryption of large datasets.

In fact, this method is often employed to encrypt passwords that are used in symmetric, faster algorithms like Advanced Encryption Standard (AES). The main feature of quantum mechanics ensuring security during coding by means of attributes such as photon polarization or phase is that any measurement of a quantum system necessarily alters its state. Therefore, any attempt to listen on the key exchange can thus be detected because it produces measurable disturbances. Thus, protocols such as BB84 and its descendants combine randomness with polarizations, measurements and public reconciliation of measurement bases to create a common secret key that is later used in classical ciphering techniques for data encryption and decoding purposes. QKD should become indispensable for secure communications against the potential dangers posed by quantum computers because it is not vulnerable to them.

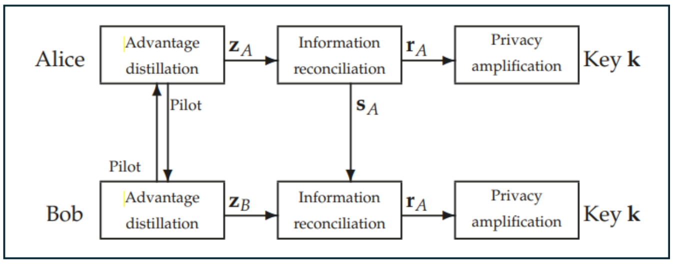


Figure 6.4: Secret Key Generation Process (Djordjevic et al., 2022)

6.5. Quantum Digital Signature (QDS) and Blockchain

Just like how a handwritten signature confirms the legitimacy of physical writing, a Quantum Digital Signature (QDS) ensures the integrity and authenticity of tractable electronic data. In 1994, they invented this Digital Signature Algorithm (Ciesla et al., 2020). This cryptographic primitive called digital signature guarantees three significant points for electronic messages: (i) authenticity – that it was actually created by the specified sender; (ii) integrity – that the message was not changed; and (iii) non-repudiation – which indicates that the sender cannot take back his/her own actions concerning the delivery of that specific document or e-mail (Pirandola et al., 2020). In subsequent years, Badhwar et al. (2021) provided an example of why Digital Signatures are crucial:

- To verify its authenticity, a computation using the public key associated with the private key which created the signature may be performed.
- It cannot be forged if the private key is kept confidential.
- It cannot be considered to be a signature for other data since it is a function of the signed data.
- Once signed, such data cannot be altered. If any modification occurs, there can be no way of verifying whether such is true or not.

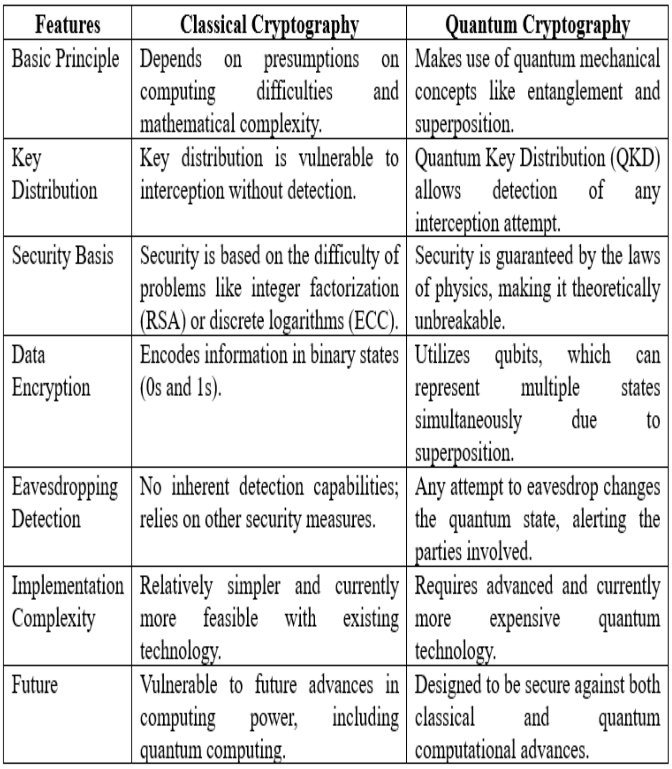
At the same time, blockchain users use public keys or asymmetric cryptography for secure communication with the blockchain system as this practice makes it possible to authenticate transactions. Similarly, hash functions are fundamental to a blockchain because they allow for digital signatures and linking blocks together within these systems. The concern is that hash functions and public-key cryptosystems are threatened by the rise of quantum computing. For instance, if an attacker uses quantum computing methods in future times; he/she could quickly obtain secure transaction information especially in case where one considers public-key cryptosystems (Fernandez-Carames et al., 2020).

6.6. Quantum Devices

Quantum devices are a significant leap in the area of cybersecurity. Building on the foundations of quantum mechanics, this technology offers a way to improve digital communications security by orders of magnitude, as well as protect sensitive information against new threats, such as those presented by quantum computers. There is a lot of potential for quantum devices to revolutionize cybersecurity through quantum cryptography. The development of these technologies is essential for long-term security of digital infrastructures in the quantum age, besides enhancing ongoing securities measures. One of the key issues confronting global cyber security community is enabling practical implementations of such devices, while at the same time overcoming current limitations. A protocol like QKD can maintain its information-theoretic security so long as its experimental implementation meets up with conditions under which it has been proved secure. To comply, users must ensure that their quantum devices are trustworthy (Grasselli et al., 2021).

7. Classical Cryptography vs Quantum Cryptography

The following table depicts the comparison between Classical Cryptography and Quantum Cryptography in details –



Features	Classical Cryptography	Quantum Cryptography
Basic Principle	Depends on presumptions on computing difficulties and mathematical complexity.	Makes use of quantum mechanical concepts like entanglement and superposition.
Key Distribution	Key distribution is vulnerable to interception without detection.	Quantum Key Distribution (QKD) allows detection of any interception attempt.
Security Basis	Security is based on the difficulty of problems like integer factorization (RSA) or discrete logarithms (ECC).	Security is guaranteed by the laws of physics, making it theoretically unbreakable.
Data Encryption	Encodes information in binary states (0s and 1s).	Utilizes qubits, which can represent multiple states simultaneously due to superposition.
Eavesdropping Detection	No inherent detection capabilities; relies on other security measures.	Any attempt to eavesdrop changes the quantum state, alerting the parties involved.
Implementation Complexity	Relatively simpler and currently more feasible with existing technology.	Requires advanced and currently more expensive quantum technology.
Future	Vulnerable to future advances in computing power, including quantum computing.	Designed to be secure against both classical and quantum computational advances.

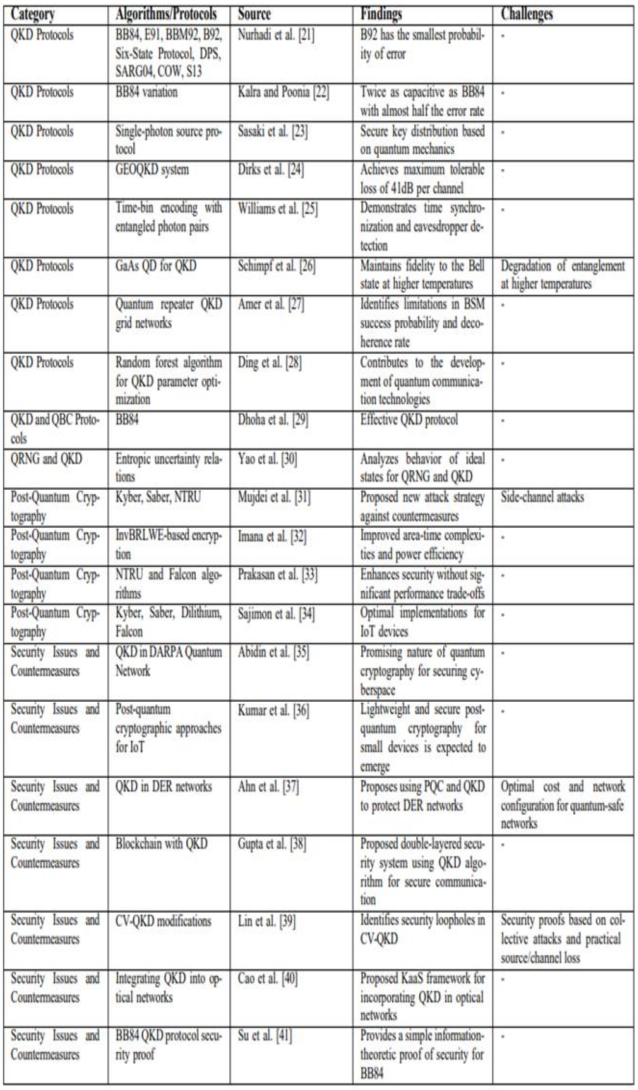
Table 7.1: Classical Cryptography and Quantum Cryptography Comparison.

8. Advancement and Challenges in Quantum Cryptography

With extraordinary communication networks that are potentially unbreakable in terms of security, Quantum Cryptography in particular through Quantum Key Distribution (QKD) is totally revolutionizing the world of cybersecurity. This kind of technology has an ability to detect any interception instantly while transferring data hence providing utmost level of safety during exchange operations. Some examples include adding quantum systems into existing networks; worldwide commercialization; and organizations' international standardization efforts directed at streamlining cross-border protocols.

However, there are many challenges to quantum cryptography. High sensitivity to environmental disturbances and technological limitations complicates its implementation. Therefore, its limited range for secure communications combined with costly quantum devices and specialized infrastructure have prevented its extensive utilization so far. Furthermore, security problems still exist such as possible quantum hacking threats like time shift attacks, while integration with present-day cyber protection systems is still quite a tall order.

The following table represents an overview of the advancement and challenges in quantum cryptography -



Category	Algorithms/Protocols	Source	Findings	Challenges
QKD Protocols	BB84, E91, BBM92, B92, Six-State Protocol, DPS, SARG04, COW, S13	Nurhadi et al. [21]	B92 has the smallest probability of error	-
QKD Protocols	BB84 variation	Kalra and Poonia [22]	Twice as capacitive as BB84 with almost half the error rate	-
QKD Protocols	Single-photon source protocol	Sasaki et al. [23]	Secure key distribution based on quantum mechanics	-
QKD Protocols	GEOQKD system	Dirks et al. [24]	Achieves maximum tolerable loss of 41dB per channel	-
QKD Protocols	Time-bin encoding with entangled photon pairs	Williams et al. [25]	Demonstrates time synchronization and eavesdropper detection	-
QKD Protocols	GaAs QD for QKD	Schimpf et al. [26]	Maintains fidelity to the Bell state at higher temperatures	Degradation of entanglement at higher temperatures
QKD Protocols	Quantum repeater QKD grid networks	Amer et al. [27]	Identifies limitations in BSM success probability and decoherence rate	-
QKD Protocols	Random forest algorithm for QKD parameter optimization	Ding et al. [28]	Contributes to the development of quantum communication technologies	-
QKD and QBC Protocols	BB84	Dhoha et al. [29]	Effective QKD protocol	-
QRNG and QKD	Entropic uncertainty relations	Yao et al. [30]	Analyzes behavior of ideal states for QRNG and QKD	-
Post-Quantum Cryptography	Kyber, Saber, NTRU	Mujdei et al. [31]	Proposed new attack strategy against countermeasures	Side-channel attacks
Post-Quantum Cryptography	InvBRLWE-based encryption	Imana et al. [32]	Improved area-time complexities and power efficiency	-
Post-Quantum Cryptography	NTRU and Falcon algorithms	Prakasan et al. [33]	Enhances security without significant performance trade-offs	-
Post-Quantum Cryptography	Kyber, Saber, Dilithium, Falcon	Sajimon et al. [34]	Optimal implementations for IoT devices	-
Security Issues and Countermeasures	QKD in DARPA Quantum Network	Abidin et al. [35]	Promising nature of quantum cryptography for securing cyberspace	-
Security Issues and Countermeasures	Post-quantum cryptographic approaches for IoT	Kumar et al. [36]	Lightweight and secure post-quantum cryptography for small devices is expected to emerge	-
Security Issues and Countermeasures	QKD in DER networks	Ahn et al. [37]	Proposes using PQC and QKD to protect DER networks	Optimal cost and network configuration for quantum-safe networks
Security Issues and Countermeasures	Blockchain with QKD	Gupta et al. [38]	Proposed double-layered security system using QKD algorithm for secure communication	-
Security Issues and Countermeasures	CV-QKD modifications	Lin et al. [39]	Identifies security loopholes in CV-QKD	Security proofs based on collective attacks and practical source/channel loss
Security Issues and Countermeasures	Integrating QKD into optical networks	Cao et al. [40]	Proposed KaaS framework for incorporating QKD in optical networks	-
Security Issues and Countermeasures	BB84 QKD protocol security proof	Su et al. [41]	Provides a simple information-theoretic proof of security for BB84	-

Table 3.2: Summary of gradual advancements and existing challenges in Quantum Cryptography (Akter et al., 2023)

9. Future Directions for Quantum Cryptography

The first physical quantum computer, Kumar et al. (2021) predicted, would eventually lead to the replacement of traditional cryptographic techniques with quantum cryptography. It was also predicted by him that new code-based cryptography techniques could be developed at some point in the future for resisting quantum attacks. Moreover, in future, quantum protocols may have authentication restrictions such as quantum digital signatures and their verification may be done (Alhayani et al., 2023). Similarly, Ahn et al. (2022) cautioned about being alert to possible quantum infiltrations within the computer networks system making it imperative to anticipate them and uncover any weaknesses. In addition, any weaknesses detected should ensure that other new methods of encryption are applied together with management measures including privacy arrangements on the Internet. According to Akter et al., future studies should strive towards creating quantum keys capable of smooth integration into the existing networks for practical reasons (2023). There will be a need for both actual implementations and experiments in order to validate the constraints and performance parameters associated with protocols and algorithms used in this form of cryptography. It shall be fundamentally important tackle possible vulnerabilities within quantum cryptography systems as quantum hacking so as establish relevant counteractions this involves preparing us for the new climate which is characterized by the advancement of technology and electronic devices that have transcended from just machines to become almost part of us. Their mastery has necessitated a shift from subject-based approaches where the learners used to memorize for exams and afterwards forgot everything into experiential learning on understanding how other forms of technology work before starting to investigate this new genre of gadgets (Abushgra et al., 2023). In an effort to combat these threats much research has over the years emanated out research institutions and organisations including Google, IBM, Microsoft, Intel corporation Atos along with other large corporations like Baidu as well as Alibaba.

10. CONCLUSIONS

Quantum cryptography appears to be a solid road towards stronger cyber security. Cybersecurity structures could benefit a lot from incorporating quantum cryptography, particularly QKD based systems for defending against threats whether they are quantum or classical in nature. However, this promising technology has not yet attained its full potential because of hindrances such as technical complexity, high cost and challenges associated with practical implementations. These obstacles can be addressed through developing scalable and cost-effective solutions, conducting continuous research and devising international regulations. To ensure that quantum cryptography technologies work reliably while enhancing current cybersecurity measures, upcoming projects must concentrate on developing their resistance levels, ease-of-use aspects and compatibility features.

ACKNOWLEDGEMENT

We gratefully acknowledge to the International Journal of Scientific Research in Engineering and Management (IJSREM) for publishing our research paper on "Quantum Cryptography in Modern Cybersecurity.”

REFERENCES

1. Abushgra, A.: How quantum computing impacts cyber security. In: IEEE International Conference on Information Management and System Analytics, pp. 74-79 (2023). https://doi.org/10.1109/IMSA58542.2023.10217756
2. Ahn, J., Kwon, H.-Y., Ahn, B., Park, K., Kim, T., Lee, M.-K., Kim, J., Chung, J.: Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). Energies 15(3), 714 (2022). https://doi.org/10.3390/en15030714
3. Akter, M. S.: Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions. arXiv (2023). https://arxiv.org/pdf/2306.09248
4. Alhayani, B.A., AlKawak, O.A., Mahajan, H.B., et al.: Design of Quantum Communication Protocols in Quantum Cryptography. Wireless Pers Commun (2023). https://doi.org/10.1007/s11277-023-10587-x
5. Badhwar, R.: The CISO’s Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. 1st edn. Springer International Publishing AG (2021). https://doi.org/10.1007/978-3-030-75354-2
6. Bernstein, D. J., Hülsing, A., Lange, T., Rekleitis, E.: Post-quantum cryptography: integration study. Publications Office (2022). https://search.lib.uts.edu.au/discovery/fulldisplay?docid=cdi_officepubeu_primary_vtls000542756&context=PC&vid=61UTS_INST:61UTS&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,Quantum%20Cryptography&offset=100
7. Biasse, J.-F., Bonnetain, X., Kirshanova, E., Schrottenloher, A., Song, F.: Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography. IET Information Security 17(2), 171–209 (2023). https://doi.org/10.1049/ise2.12081
8. Bloom, Y., Fields, I., Maslennikov, A., Rozenman, G. G.: Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation. Physics (Online) 4(1), 104–123 (2022). https://doi.org/10.3390/physics4010009
9. Ciesla, R.: Encryption for Organizations and Individuals Basics of Contemporary and Quantum Cryptography. 1st edn. Apress (2020). https://doi.org/10.1007/978-1-4842-6056-2
10. Cheon, J. H., Johansson, T.: Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28-30, 2022, Proceedings. In: ELLIIT: the Linköping-Lund initiative on IT and mobile communication, vol. 13512. Springer International Publishing AG (2022). https://doi.org/10.1007/978-3-031-17234-2
11. Djordjevic, I. B., Djordjevic, I. B.: Physical-Layer Security, Quantum Key Distribution and Post-quantum Cryptography. MDPI Books (2022). https://search.lib.uts.edu.au/discovery/fulldisplay?docid=alma991007202298005671&context=L&vid=61UTS_INST:61UTS&lang=en&search_scope=MyInst_and_CI&adaptor=Local%20Search%20Engine&tab=Everything&query=any,contains,Quantum%20Cryptography&offset=0
12. Eka Pratama, I. P. A., Krisna, A.: Post Quantum Cryptography: Comparison between RSA and McEliece. In: Proceedings of the International Conference on Information Systems Security (2022). 01-05. https://doi.org/10.1109/ICISS55894.2022.9915232
13. FasterCapital: The role of superposition in quantum cryptography. https://fastercapital.com/topics/the-role-of-superposition-in-quantum-cryptography.html
14. Fernandez-Carames, T. M., Fraga-Lamas, P.: Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 8, 21091-21116 (2020). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8967098
15. Grasselli, F.: Quantum Cryptography: From Key Distribution to Conference Key Agreement. 1st edn. Springer International Publishing AG (2021). https://doi.org/10.1007/978-3-030-64360-7
16. Johansson, T., Smith-Tone, D.: Post-Quantum Cryptography: 14th International Workshop, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings. 1st edn. Springer Nature Switzerland (2023). https://doi.org/10.1007/978-3-031-40003-2

17. Kronberg, D. A.: Vulnerability of quantum cryptography with phase–time coding under attenuation conditions. Theoretical and Mathematical Physics 214(1), 121–131 (2023). https://doi.org/10.1134/S0040577923010075
18. Kumar, A., Garhwal, S.: State-of-the-Art Survey of Quantum Cryptography. Archives of Computational Methods in Engineering 28, 3831–3868 (2021). https://doi.org/10.1007/s11831-021-09561-2
19. Kurniawan, D., Triyanto, D., Wahyudi, M., Pujiastuti, L.: Quantum computing in cryptography: Exploring vulnerabilities and countermeasures. Jurnal Teknik Informatika CIT Medicom 15(4), 206-213 (2023).
20. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... Gehring, T.: Advances in quantum cryptography. Advances in Optics and Photonics 12(4), 1012-1236 (2020). https://doi.org/10.48550/arXiv.1906.01645
21. Rogers, D.: Broadband Quantum Cryptography. 1st edn. Springer Nature (2022). https://search.lib.uts.edu.au/discovery/fulldisplay?docid=cdi_askewsholts_vlebooks_9783031025136&context=PC&vid=61UTS_INST:61UTS&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,Quantum%20Cryptography&offset=100
22. Ugwuishiwu, C. H., Orji, U. E., Ugwu, C. I., Asogwa, C. N.: An overview of quantum cryptography and shor's algorithm. International Journal of Advanced Trends in Computer Science and Engineering 9(5) (2020). https://d1wqtxts1xzle7.cloudfront.net/84737888/ijatcse82952020-libre.pdf?1650725999=&response-content-disposition=inline%3B+filename%3DAn_overview_of_Quantum_Cryptography_and.pdf&Expires=1714159631&Signature=agdBBBocZ3TLubb2td43adfW9bREK2VB89E7iaSBVVdKlTxvEG~u0vOSUxKIfqSDo7wW59~OlyIrJK8~rHsI~c8ohGaZjuhhEvdohUlMtK~IFXWOnCnfz5OKpYyFbn5SZaL05WDxREU5ASKgxRuXAGS~8FjoHlcJ59H69xL2eyUGEdCBwsbWJ5q8YVRYBWoS-QOstyHkEwLiEDDH9HUudihvFachlLieWvci9cbn9IwPwOGfTJwwYLWijFNmdlPsDVfBz6M8YBM~GGIvKwJgw7Z58kdZQqpg6Ivasm7wLSJq4dvXPWD0AOuLgDpltyXsMTrrWKwnM~IAFmbBWnH6Iw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
23. Wang, L.-J., Zhang, K.-Y., Wang, J.-Y., Cheng, J., Yang, Y.-H., Tang, S.-B., Yan, D., Tang, Y.-L., Liu, Z., Yu, Y., Zhang, Q., & Pan, J.-W. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. Npj Quantum Information, 7(1), 1–7. https://doi.org/10.1038/s41534-021-00400-7
24. Xagawa, K., Ito, A., Ueno, R., Takahashi, J., & Homma, N. (n.d.). Fault-Injection Attacks Against NIST's Post-Quantum Cryptography Round 3 KEM Candidates. Advances in Cryptology – ASIACRYPT 2021, 33–61. https://doi.org/10.1007/978-3-030-92075-3_2

BIOGRAPHIES

Md Shariar Sozol is currently pursuing a Master of Cybersecurity (Extension) and he has got over a years' professional experience in the cybersecurity industry. He specializes in cryptography and blockchain.

Md Mostafizur Rahman is currently pursuing a Master of Engineering (Extension) at University of Technology Sydney, Australia.

Md Minhazul Islam is currently pursuing a Master of Information Technology (Extension) and got over a year of professional experience in the cybersecurity, specializing in cryptography and data analysis.

Golam Mostafa Saki has completed his MSc in Engineering Management from the University of South Wales, UK.