I.J. Wireless and Microwave Technologies, **2022, 5, 10-20**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2022.05.02

Quantum Computers' threat on Current Cryptographic Measures and Possible Solutions

Tohfa Niraula
Department of Computer Science and Engineering, Kathmandu University Dhulikhel, Nepal
E-mail: tohfa.niraula1@gmail.com

Aditi Pokharel
Department of Computer Science and Engineering, Kathmandu University Dhulikhel, Nepal
E-mail: aditipokh13@gmail.com

Ashmita Phuyal
Department of Computer Science and Engineering, Kathmandu University Dhulikhel, Nepal
E-mail: ashmitaphuyal9@gmail.com

Pratistha Palikhel
Department of Computer Science and Engineering, Kathmandu University Dhulikhel, Nepal
E-mail: pratisthapalikhel@gmail.com

Manish Pokharel
Department of Computer Science and Engineering, Kathmandu University Dhulikhel, Nepal
E-mail: manish@ku.edu.np

Received: 15 April 2022; Accepted: 25 May 2022; Published: 08 October 2022

Abstract: Cryptography is a requirement for confidentiality and authentic communication, and it is an indispensable technology used to protect data security. Quantum computing is a hypothetical model, still in tentative analysis but is rapidly gaining traction among scientific communities. Quantum computers have the potential to become a pre-eminent threat to all secure communication because their performance exceeds that of conventional computers. Consequently, quantum computers are capable of iterating through a large number of keys to search for secret keys or quickly calculate cryptographic keys, thereby endangering cloud security measures. This paper's main target is to summarize the vulnerability of current cryptographic measures in front of a quantum computer. The paper also aims to cover the fundamental concept of potential quantum-resilient cryptographic techniques and explain how they can be a solution to complete secure key distribution in a post-quantum future.

Index Terms: Cloud computing, security, cryptography, encryption, quantum computing

1. Introduction

Cryptography is a secure communication technique that allows only the sender and receiver to view the contents of their messages. Cryptography is an integral part of today's information security. Quantum computing is a conceptual model that exploits quantum physics phenomena, such as superposition and entanglement, to process data. Due to these phenomena, adding just a few extra qubits can lead to exponential leaps in processing power, reducing the processing time of ten thousand years into minutes[7]. Quantum computers will eventually surpass their current capacity and become a pre-eminent threat to security with the potential of iterating through all possible permutations of a cryptographic key within seconds.

1.1 Motivation

With the rapid advancement of quantum computers, an urgent question emerges. What are the effects it has on cyber security and its current data encryption techniques? It also raises questions concerning the future of data security in the post-quantum world. One of the most viable solutions to withstand quantum attacks is to enhance the most currently used AES encryption algorithm. I. Vajda's research on classical cryptography in a quantum era demonstrates this solution [29]. I. Vajda, in their paper, proposes a solution to making AES algorithm quantum resilient by increasing

its key length and making it more difficult to break through brute force. However, this solution has a drawback, that is, it takes a lot of processing power and time to create larger key lengths of AES encryption. Hence, enhancing existing cryptographic systems is not the best solution for security in a post-quantum era. Then, what can ensure data security and safe communication in the post-quantum era?

1.2 Research Objective

The objective of this research is to show: How current cryptographies are vulnerable in the face of quantum computing and quantum algorithms? What are the possible cryptographic solutions in a post-quantum era?

This paper summarizes the threat of quantum computing to current cryptographic measures and explores possible solutions to security in a post-quantum era. The findings of this study can directly benefit academic instructors by providing an introductory summary of current cryptography's limitations and cryptography in the post-quantum era. The paper also benefits companies providing secure communication services by shedding light on the vulnerabilities of their current security measure and briefly introducing possible alternatives. Finally, the paper emphasizes that current data security will be void in the presence of commercial availability of quantum computers and stresses that it is urgent for tech companies everywhere to switch to quantum-resilient cryptography.

2. Literature Review

There has been traction in the research of quantum computing due to the $1.02 billion budget allocation by major nations towards the development of quantum computing for cybersecurity in 2020 and 2021 [1]. Quantum computing can pose a devastating threat to current cryptographic systems[6]. Ref [28] demonstrates the performance difference between a classical computer and quantum computers. Ref [28] provides evidence that a solution for NP-problems achieved through the classical algorithm in exponential time, can be achieved by quantum algorithms in polynomial time. With this, there is an urgent need to develop quantum-resilient cryptographies. One solution can be to improve existing classical cryptographies by modifying them to be quantum-resilient. I. Vajda's research on classical cryptographies in a quantum era [29], demonstrates how a popular encryption technique, AES encryption, can be modified to resist attack from an adversary with quantum computing measures. Vajda exemplifies how AES encryption can resist attacks from the quantum computer by increasing its key length accordingly. However, Vajda mentions that it is notoriously time-consuming to run public-key primitives on classical computers, let alone those public keys that are quantum-resilient. Hence, we aim to focus on the recently emerging quantum-resilient cryptographic solutions.

In our research, we have also considered the work of M. Campagna and C. Xing, Ref[11], which explores cryptographies that are quantum-safe algorithms, like QKD, and cryptographic primitives that are Multivariate, Hashedbased, Lattice-based and Code-based. In their paper, they have also explored the possible upgrades that can be done to cryptographic tools available at the current time to make them quantum-safe. And, the work of H. Singh, D. Gupta, and A. Singh, Ref[20] prospects quantum key distribution as the way to provide a secure key exchange. In their paper, they briefly go through 10 different quantum key distribution protocols. The work done by J. Aditya and P. Shankar Rao of Andhra University [30], mentions the limitations of modern cryptosystems and introduces the concept of Quantum Cryptography along with the attributes of an ideal Quantum Key Distribution.

Our approach is more mathematical in demonstrating the threat, how quantum computers along with quantum algorithms can break two widely used encryptions, RSA and AES. We aim to show the vulnerabilities of current cryptographies and explore possible quantum-resilient cryptographic solutions both in the form of quantum cryptography and post-quantum cryptography. In this paper, we will also explain how Quantum Key Distribution works with the BB84 protocol and go through popular, most feasible post-quantum cryptographic solutions.

3. Methodology

The sources of primary studies vary from indexed repositories (IJCNIS, Research Gate, Science Direct, JCIS, JACM, NIST, IJRTER etc) to articles published by QuTech and Quantiki. QuTech is a research institute for quantum computing. Quantiki is the world's most comprehensive resource portal for anyone interested in quantum information science. We have downloaded 100 papers out of which, we have considered ten papers. We have limited our paper to discussing threats posed by quantum computers to current cryptographic measures, and quantum cryptography as its solution. Since it is not feasible to explore all the possible solutions to quantum computers' threat to cryptography, we have listed some prominent post-quantum cryptographic solutions. In this paper, we have considered "Talk about quantum computing's threat on cryptography and talk about quantum cryptography as its solution" given by various researchers in their research work. Here the reference point is the information available in research papers.

Firstly, we used the reference of "Analysis of Quantum Algorithms with Classical Systems Counterpart"[28] by S. R. Sihare and V. V Nath, to understand the gap in the performance of classical and quantum computers. And with the help of reference of "NIST: Report on PostQuantum Cryptography"[10], we understood how quantum computers impacted currently used cryptographies. We decided to look into the two more commonly used encryption algorithms: AES and RSA. With the articles "Shor's factoring algorithm" [5], by Quantiki and "Why we should be scared of Shor's Algorithm" [6], by the lead developer, we learned about Shor's Algorithm's impact on RSA. With the paper, "The

Imminent Obsolescence of Cryptographic Algorithms and the Arrival of Quantum Computation" [2], by Herrera, D., Fandiño, J. and Torres, N., we learned about Lov Grover's Algorithm's impact on AES.

After learning of the threats posed by quantum computers to today's cryptographic systems, we looked for their solutions. M. Campagna and C. Xing's "Quantum-Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges" [11] gave us an insight into cryptographic solutions that are quantum-resilient. "On Classical Cryptographic Protocols in Post-Quantum World" [29] by I.Vajda explored the concept of upgrading current cryptographic measures to withstand quantum attacks. The paper, "Quantum key distribution protocols: A review" [20] by H. Singh, D. Gupta, and A. Singh, and the article, "Quantum Key Distribution" [25] by Qutech, gave us an understanding of quantum key distribution. And, the paper by P. Shankar Rao and J. Aditya, "Quantum Cryptography"[30], gave us the idea of the attributes of an ideal Quantum Key Distribution System. "A single quantum cannot be cloned" [27], by W.K. Wootters and W.H. Zurek, gave us further insight into quantum cryptography and solidified its position as the best possible quantum resilient solution.

2. Cryptography

Cryptography is a large-scale distributed computing model that guarantees the security and privacy of information during resource sharing. Cryptography is a component of cloud computing that is essential for the protection of sensitive data at the system level. There are two types of cryptosystems currently in use: symmetric and asymmetric.

2.1. Symmetric Key Algorithm

The Symmetric Key Algorithm is single-key encryption which means the sender and the receiver have identical keys to encrypt and decrypt data. Symmetric-key algorithms are of two types: Block cipher and Stream cipher. Block cipher sets the length of bits that are encrypted in blocks of electronic data using a specific secret key. During the encryption process, the system stores data in its memory while it retrieves the complete blocks. In the case of a stream cipher one bit encrypts data at a particular time [3]. Some popular Symmetric-key algorithms used in cloud computing include Data Encryption Standard (DES), Triple-DES, Advanced Encryption Standard (AES) and blowfish algorithm. The encryption technique used for data storage in popular cloud platforms such as Amazon Web Services (AWS), Google or Azure is either AES256 or AES128.

2.2. Asymmetric Key Algorithm

The asymmetric key algorithm uses a public key to encrypt messages sent to the receiver and a private key, with which the receiver decrypts messages. The receiver is the sole holder of their private key. So, In asymmetric encryption, each receiver possesses a decryption key of its own, this is the private key. A receiver needs to generate an encryption key, referred to as their public key. Ordinarily, this type of cryptosystem involves a trusted third party that officially declares that a particular public key belongs to a specific person or entity only. Some popular Asymmetric-key algorithms used in cloud computing include RSA, DSA, Elliptic curve techniques and PKCS.

3. Quantum Computing

An ordinary computer uses bits. Bits can either be in the "off" state, represented by a zero or in the "on" state, represented by a one. All applications and websites are created, using millions of these bits, in some combination of ones and zeroes. Instead of bits, quantum computers use qubits. Qubits can be in superposition, which means they are in an "on" and an "off" state at the same time or, they are somewhere on a spectrum between those two states, rather than just being "on" or "off". The qubits can be entangled. In entanglement, two particles can be linked together, even if they are physically separate. These phenomena assist in making quantum computers behave in a radically different way than classical computers and promote the development of algorithms that take into account the quantum mechanics of quantum computers.

3.1. Cryptosystems vulnerable to quantum algorithms

Quantum computers endanger the principal goal of all secure and authentic communication because they can do computations at a rate that classical computers cannot. Cryptography is a critical component of today's advanced communication systems. The security of emails, passwords, or financial transactions has the objectives of confidentiality and integrity [11]. Cryptography makes sure that only parties that have exchanged keys can read the encrypted message, thereby preserving the purpose of secure communication. Consequently, quantum computers can break the cryptographic keys quickly, using brute force alone, by calculating or searching for all secret keys. Quantum computers are a double-edged sword and eavesdroppers are likely to exploit quantum algorithms to optimize certain tasks that threaten secure communication. One such algorithm, published by Peter Shor, helps quantum machines find the prime factors of integers incredibly fast. Another algorithm, by Lov Grover, helps quantum computers iterate through possible permutations at a faster rate. The impact of such algorithms on today's security is discussed below.

3.1.1. Shor's algorithm:

In 1994, Peter Shor, an MIT mathematician, discovered Shor's algorithm, and in 2001, IBM factored 15 into 3 and 5 using a seven-qubit quantum computer with Shor's algorithm. That was one of the preeminent proofs of how quantum computers could break existing encryption methods. Many currently in wide use, asymmetric cryptography use prime factorization as a base for their security. In a classical computer, prime factorization is a near-impossible task to achieve by brute force alone. However, Shor's algorithm with a quantum computer can make modern asymmetric cryptography collapse since it can quickly solve prime integer factorization or the discrete logarithm problem [6].

3.1.2. Lov Grover's Algorithm:

In 1996, a renowned computer scientist Lov Grover introduced a database search algorithm based on quantum techniques which solve the problem of random search faster than the search techniques using classical computers. Symmetric cryptographic algorithms, like Advanced Encryption Standard (AES), have a security that depends on the design and strength of key lengths of the AES algorithm. AES algorithm of key length 18 is considered sufficient to protect classified information. Grover's algorithm could potentially break this with the help of quantum computers by speeding up the process and turning the 128-bit key into the quantum-computational equivalent of a 64-bit key. It utilizes quantum computing to search unsorted databases. Classically searching an unsorted database requires linear search, which takes O(*N*) time but the Lov Grover algorithm takes *N*/2 searches to find a specific entry in an unsorted database of *N* entries using $O(\log N)+1$ storage. Grover's algorithm reduces the complexity of symmetric ciphers from O(N) to O(*N*/2), endangering symmetric cryptography-based security.

4. Quantum Algorithm Breaking Encryption

4.1. Shor's Algorithm and Asymmetric cryptography (RSA)

Shor's algorithm makes asymmetric algorithms vulnerable to quantum attacks. Take an example of one of the asymmetric algorithms: RSA Cryptosystem. It uses two cryptographic keys; a public key and a private key. The public key is used for encrypting messages and can be decrypted only by using the private key. The private keys are two large primes, *p* and *q*. These numbers multiply to give the public key *N* of the RSA algorithm. It is an effortless task to multiply the private keys to calculate the public key but near impossible to factorize the public key to give the private key. Shor's algorithm makes it easier to do that factorization. It starts with a random number, *g*. Then uses the Euclidean algorithm to find gcd of g and *N*, where *N* is the public key. In the case of g being a factor of *N* or sharing a factor with *N*: the gcd finds one of the prime factors of *N*, say *q*, then finding the other factor will be the problem of a simple mathematical division of *N* by *q*. But in the case of *g* and *N* being relatively prime, a random number g is guessed. The probability of a random number, *g* having a factor with *N*, can be increased through the mathematical fact that if two numbers, *a* and *b*, are relatively prime then,

$$a^n = m \times b + 1 \tag{1}$$

For some whole numbers, n and m. Putting this in terms of *g* and *N*:

$$\begin{gathered} g^p = m \times b + 1 \\ \text{or, } g^p - 1 = m \times b \\ \text{or, } (g^{\frac{p}{2}} + 1) \times (g^{\frac{p}{2}} - 1) = m \times b \end{gathered} \tag{2}$$

This implies that $(g^{\frac{p}{2}}+1)$ shares a factor with *N*, and gcd $(g^{\frac{p}{2}}+1, N)$ will give a prime factor of *N*. But to compute gcd $(g^{\frac{p}{2}}+1, N)$, the period p is needed to be found. By the mathematical fact that $a^m \pmod b$ for two relatively prime numbers, *a* and *b*, where m = 0, 1, 2, . . . and so on, [12] gives a periodic sequence of remainders. This can be seen using the numbers $2^a \pmod{15}$ below:

$2^a \pmod{15}$	Output
$2^0 \pmod{15}$	1
$2^1 \pmod{15}$	2
$2^2 \pmod{15}$	4
$2^3 \pmod{15}$	8
$2^4 \pmod{15}$	1

Here, the remainders repeat after the interval of 4. Hence, the period is 4. But that is for a small number. For a large number of 516 digits or above, finding the period will be difficult. But using quantum computing, this can be overcome. Shor's algorithm with quantum computing can convert a random, probably unlikely guess, g to $(g^{\frac{p}{2}}+1)$, which has a high probability of sharing a factor with N, where p is the period of repetition of reminders. For a large number of 516 digits or more, finding a period by a classical computer will be time-consuming. But a quantum computer can complete that task in minutes by taking a superposition of input. First takes input of: $1>+2>+3>+...$ and raises the initial number's power by the input and gives an output: $g^1>+g^2>+g^3>+...$, which is the superposition of the initial number's powers raised to the input numbers. These superpositions are passed into another quantum computer. The second quantum computer computes $g^x \pmod{N}$ and gives an output of superposition of remainders with the power of g with which, $g^x \pmod{N}$ gave that remainder.

$$1>+2>+3>+...\longrightarrow \boxed{g^x} \longrightarrow g^1>+g^2>+g^3>+...,$$

$$1>+2>+3>+...\longrightarrow \boxed{g^x} \longrightarrow g^1>+g^2>+g^3>+...\longrightarrow \boxed{g^x \bmod N} \longrightarrow (1,r_1)>+(2,r_2)>+(3,r_3)+...$$

As seen in the example above with g = 2 and N = 15, their output for the second quantum computer would be:

$$(0,1)>+(1,2)>+(2,4)>+(3,8)>+(4,1)>(5,2)>+(6,4)>+(7,8)>+(8,1)>+(9,2)>+...$$

In the above example, the numbers repeat after a period of 4. Similarly, for a large number N and g, the reminders repeat after a period, p. If the superposition of all possible powers is taken to measure just the remainder, then the quantum computer gives one of the possible remainder r as output. That doesn't solve the problem but reduces the superposition of states in the quantum computer to only the powers of g that result in the remainder, r. The remainders that repeat periodically with period p remain in the superposition. This superposition can be treated as a wave, having period p and frequency f. The frequency of the superposition can be calculated using the Quantum Fourier Transform (QFT) to give a single quantum state as output $(\frac{1}{p})$. With the value of p known, the guesses can be improved from g to $(g^{\frac{p}{2}}+1)$, again the GCD of $(g^{\frac{p}{2}}+1, N)$ is taken, which gives us one of the prime factors of N, p then by dividing N by p we get the other prime factor, q [5]. Hence, it's impending that anyone using Shor's algorithm with a working quantum computer could efficiently break any asymmetric algorithms used for data encryption.

4.2. Lov Grover's Algorithm on Symmetric cryptography (AES)

Grover's algorithm implementation on quantum computers poses a threat to symmetric key algorithms (AES) that offer a square root speedup over classical brute force algorithms, so the cryptographic key length is reduced by 50 percent. Grover's quantum search algorithm can search a key space in $O(n1)$, a quadratic speedup. For example, for an n-bit symmetric cryptographic algorithm, the quantum computer operates in $2n$ possible ways. After implementing Grover's algorithm on a quantum computer, the AES 128- bit, the attack time reduces to 264, and for the AES-256, the attack time reduces to 2128. The Advanced Encryption Standard supports two other key lengths of 192-bit and 256-bit, and increasing the size of AES symmetric keys can increase the security of AES against brute force. However, the purpose of Grover's algorithm is not only searching a database but describing it as inverting a function. Suppose we have a function $y = f(x)$, Grover's algorithm calculates x for a known y. Here, solving the inverse function is equivalent to searching a database for a value of x that produces the given y. With this, it is not improbable to say that

with Grover's algorithm, there is a chance that encryption by symmetric algorithms can also be broken by quantum computers in a time frame much quicker than that of classical computers. The only defense mechanism is to increase the size of the symmetric key, so the brute force approach by Lov Grover's algorithm would require a longer time to break the encryption.

Table 1. Impact Analysis of Quantum Computing on encryption schemes (Adapted from [10])

Cryptographic Algorithm	Type	Purpose	Impact of Quantum Computing	Quantum Algorithm used
AES	Symmetric key	Encryption, Decryption	Larger Key size needed	Lov Grover's algorithm
RSA	Public Key	Signature Key Establishment	No longer secure	Shor's algorithm
DSA	Public Key	Signature Key Exchange	No longer secure	Shor's algorithm
ECDSA, ECDH	Public Key	Signature Key Exchange	No longer secure	Shor's algorithm
SHA-2, SHA-3	Hash Function	Signature Key Exchange	Large output needed	Lov Grover's algorithm

5. Cryptography with Quantum Computing

Quantum computers exceed the performance of traditional supercomputers, and with the above-mentioned algorithms, they can pose a threat to existing cloud security. Fortunately, quantum computers will not be commercially available any time soon. The cost of setting up infrastructure and hardware for an operational quantum computer is high. So, it is unlikely that quantum computers will be a household device in the near future. But this also opens the opportunity for quantum computing services to be deployed through the cloud [23]. Since it is probable that early quantum computing services will be deployed through the cloud, the urgency to create a quantum-resistant, secure ecosystem is felt most by cloud security. It is possible to utilize the exponential advantage that quantum computing possesses at solving certain problems and elevating cloud security to a greater height. The cryptographic system that makes use of quantum phenomena to distribute quantum keys, quantum cryptography is already in existence and gaining attention as a potential solution in the post-quantum era.

5.1. Quantum cryptography

Quantum cryptography is based on the principle of quantum mechanics and physics to distribute quantum keys. Quantum cryptographic systems use photons to carry quantum keys and photons only exist as moving particles that cannot be duplicated or altered. Quantum cryptography's security relies on this property of photon which makes it unbreachable. The most important and proposed application of quantum cryptography is Quantum Key Distribution (QKD). Quantum Key Distribution is process 6 of using an authenticated communication channel to establish a secret key. Quantum key distribution uses a series of photons to transmit data from sender to receiver over a fiber optic cable [20,21].

One of the promising systems for Quantum Key Distribution is the BB84 protocol. The BB84 protocol was developed by Charles Bennett and Gilles Brassard and is used for generating a secure shared key. In BB84 protocol, qubits are used for encoding information and photons are used to carry that information. The BB84 protocol can ensure confidential communication based on two fundamental properties of light, which are the indeterminacy principle and the no-cloning theorem. The indeterminacy principle states that the position and the velocity of photons in a system cannot both be measured with absolute precision, without disturbing the system irreversibly [20]. And the no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state [27]. Hence, the former principle ensures a level of security in the BB84 protocol and the latter protects the shared quantum key from eavesdroppers.

The following are the steps of the BB84 protocol [25]:

1. In the BB84 protocol, the sender uses a light source to create a random sequence of photons.
2. The photons on the sender side pass through a polarizer which randomly gives one of four possible combinations of four polarizations: Vertical, Horizontal, positive 45 degrees, or negative 45 degrees. The sender now has a sequence with these polarizations. Horizontal and positive 45 degrees have value zero bit and Vertical and negative 45 degrees have value zero.
3. The photon is received by the receiver where two beam splitters exist to read the polarization of each photon, the beam splitter at the receiver's side is also chosen at random.

4. The above process is iterated till the whole key is transferred to the receiver.
5. The receiver informs the sender about the sequence of beam splitters used and the sender compares that information with the sequence of polarizers used to send the key.
6. The sender then communicates with the receiver where the right beam splitter is being used in the sequence of photons and they eliminate the photons with different beam splitters and polarizers.
7. The resulting sequence of bits, which is the same for the sender and receiver, becomes their shared secret key.

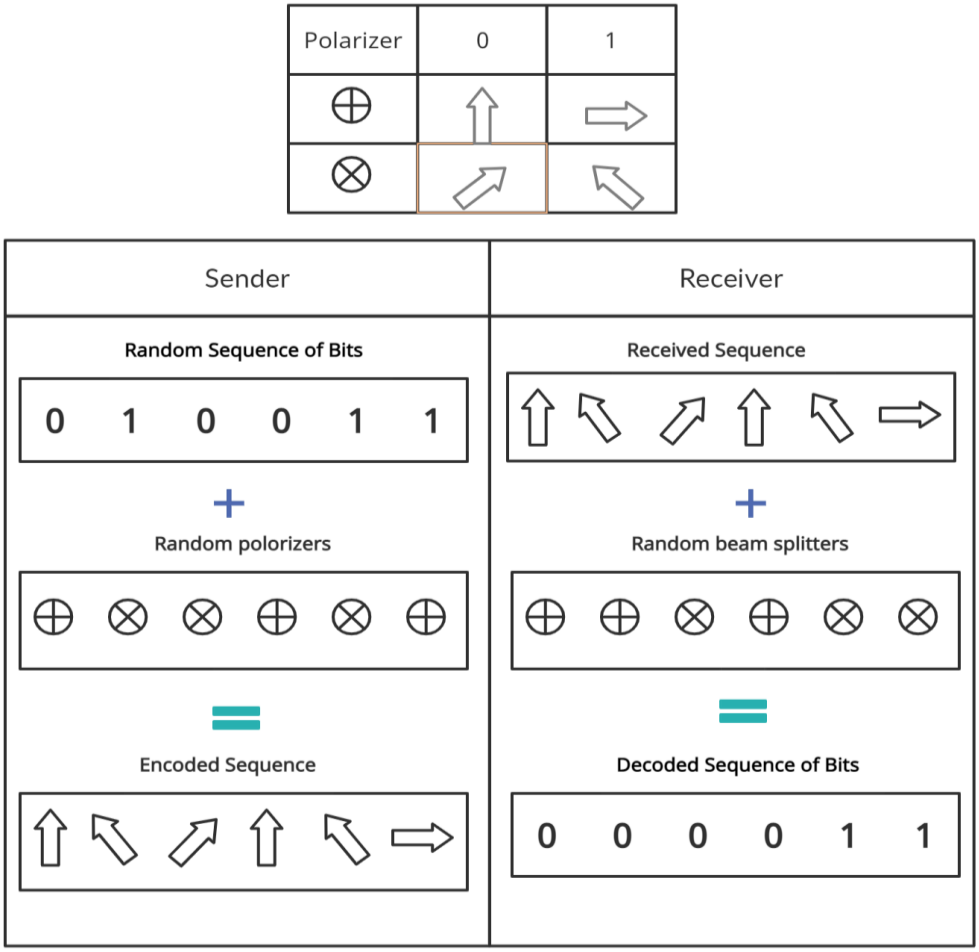

Fig.1. Step 1 to 4 of BB84 protocol.

Quantum key distribution is secure against eavesdropping, since the state of the photon will be changed if it is copied or tampered with, and the sender will be able to observe this change and send a new key to the receiver. The development of efficient networks that allow secure communication using Quantum Key Distribution is still in its early stages. However, the feasible architecture for implementing a network of quantum key distribution using optical wavelength division multiplexing (WDM) is already under research [26]. Quantum Key Distribution is a promising and soon viable solution that can create a quantum resilient security and communication ecosystem, as a quantum-based cryptosystem that is virtually unbreakable even with a quantum computer [24].

5.2. Challenges of Quantum Computing

Quantum computers can solve complex computational problems within a short period and perform multiple transactions, for which a classical computer can take years to solve. On the other hand, quantum computers are still evolving, and the researchers are far away from building quantum computers that can perform at their theorized potential [12], the limitation of quantum can be deduced as follows:

1. Quantum based cryptography requires a quantum channel between the sender and receiver, and such infrastructures are yet to be developed and available for general use.
2. Quantum computers are sensitive to noise distortion and environmental effects, which can lead to information degeneration.
3. Quantum Computers developed are of limited use and simply only for certain types of demonstration. Due to the concept of decoherence which limits the operations needed to perform before losing the stored information, many researchers are exasperated.

4. Without the mechanisms such as fault tolerance and quantum error correction, it is impossible to deduce the error rate caused by quantum computers.

6. Cryptography in Post-quantum Era

Although quantum computers, at their current ability may not be capable of breaking currently in use cryptosystems, they are growing fast, and they will inevitably reach that potential. And the threat that Shor's and Grover's algorithms pose on existing cryptographic systems still remains. Quantum computers have an advantage over conventional supercomputers when it comes to solving many problems, by processing large amounts of data and coming to one solution. But there are algorithms that quantum computers cannot outperform traditional supercomputers on, like problems with multiple solutions [8,9]. Researchers are working towards developing such algorithms that can supersede existing algorithms and can survive in the post-quantum era. There are five cryptographic systems that are gaining traction as possible solutions in the post-quantum era.

6.1. Post-quantum Cryptography

Post-quantum cryptography is the development of cryptographic approaches by improving existing mathematical algorithms that can be executed in classical computers and will be quantum-resistant. Their security relies on mathematical problems that are believed to be intractable even for a large-scale quantum computer [4]. Following are some of the more promising and feasible post-quantum cryptography systems:

6.1.1. Lattice-based Cryptography

Lattice-Based Cryptography is a complex cryptographic scheme designed to protect data from the threat of crypto breaking by fault-tolerant universal quantum computers with millions of qubits. Unlike RSA, rather than multiplying primes, lattice-based encryption schemes involve multiplying matrices. The shortest vector problem (SVP) is an NP-hard problem, and its objective is to find the smallest non-zero vector in the lattice. Lattice-based cryptosystems' security relies on coordinates within a lattice system that are difficult to solve [18]. Currently, existing algorithms for solving SVP take exponential time in the dimension of the lattice. Since quantum computers are not quick at solving problems with multiple solutions, it also takes exponential time on a quantum computer [17]. Researchers are investigating new emerging cryptosystems [16] like New-Hop [14] and Frodo [15] of the NIST post-quantum crypto project to understand lattice-based systems. As per their report, the system added 20 milliseconds per key exchange for 95 percent of users, but the promise of post-quantum security of the system outweighs the minor delay. The lattice algorithm depends on how hard it is to find hidden information in a lattice with hundreds of spatial dimensions unless you know the secret route. This does not imply that quantum computers cannot decrypt lattice encryption, but as Chris Peikert, one of the developers of CRYSTALS said, there is no known quantum algorithm to this day that can break the lattice algorithm.

6.1.2. Multivariate-based Cryptography

Multivariate-based Cryptography is a public-key cryptosystem that uses a multivariate system of equations over a finite field as its public map. Its security relies on the NP-hardness of quadratic polynomial equations over a finite field. The multivariate encryption scheme is currently the simple matrix encryption scheme, and the decryption process consists only of the solution of linear systems. Multivariate cryptosystems can be used for digital signatures as well. The most promising signature schemes include UOV and Rainbow.

6.1.3. Hash-based Cryptography

Hash-based cryptography is an alternative quantum-proof cryptographic scheme whose primary focus is on digital signatures used to verify documents. The digital signatures such as LamportDiffie or Winternitz signatures that hash-based cryptography produces are only for one time use as they are unaffected by the quantum attacks like Shor's algorithm to break the current encryption, unlike signatures-based RSA [22]. Even with quantum computers, it will be laborious to supersede the collision-resistance of cryptographic hash functions. In the post-quantum era, hash-based cryptography seems to be gaining confidence for its security against quantum algorithms. Hash-based cryptography has become a plausible alternative to existing RSA and ECDSA, and several software vendors might choose to switch to hash-based cryptography in the near future.

6.1.4. Code-based Cryptography

Code-based cryptography uses error-correcting codes for encryption and decryption. It lets two parties communicate over a noisy channel. The sender sends an encoded message to the receiver over a noisy channel, and the receiver decodes the message with error-correcting codes. As code-based cryptography gained traction, difficulty in decoding some encoding schemes became evident. Despite using the best decoding algorithms for such schemes, it takes exponential time to decode in a classical computer. Decoding those schemes is a highly strenuous task, even for a quantum computer. Taking that into account, cryptographers rely on creating problems that are hard to decode. One of the most popular code-based cryptosystems is the McEliece cryptosystem [19], and it can be used for encryption key

exchange post-quantum. It introduced an encryption scheme built on (binary) Goppa codes, and its security is based on the syndrome decoding problem. It processes encryption and decryption swiftly because it has relatively lower complexity compared to other systems in the code-based cryptography family.

7. Conclusion and Future Scope

Understanding quantum technologies have become essential for researchers to procure the benefits of quantum research and innovation for security. Concurrently, the continuous research and development of quantum computing lead to threats to data encryption. Quantum computing based on quantum mechanics as compared to classical computing has ultimate advantages like virtually unimpeded security that can solve cyberspace security problems for the future Internet. It could transform the world by revolutionizing communications and artificial intelligence besides breaking encryptions. As quantum encryption becomes plausible, it will bring technological revolution as well as have daunting effects on the traditional encryption keys that can no longer be considered safe.

In this paper, we have elucidated the risk posed by quantum computers on classical cryptographies, by demonstrating how quantum computers can easily break existing cryptographic measures, such as RSA and AES. Quantum Computing uses qubits to carry out processing and can compute solutions in polynomial time, where it takes classical computers' exponential time. Hence, they can make current cryptographies vulnerable. We have also assessed some quantum and post-quantum crypto protocols that could provide a solution to secure communication in a post-quantum world. The most prominent of which, Quantum Key Distribution, can ensure confidential communication by utilizing quantum mechanics and keeping transmissions secure from even quantum attacks.

The paper comprehends the state of current security measures in the face of emerging quantum computing technologies and suggests that tech companies should switch to quantum-safe cryptography in near future. This paper serves as a summary of progress made in cryptography in preparation for the post-quantum era for reference to future works. In the next step, a feasibility analysis can be done on the suggested quantum-safe cryptographies based on current progress in those cryptosystems, to determine the post-quantum cryptography that can be applied in a post-quantum era.

References

[1] "VCs make record bets on quantum computing | PitchBook", Pitchbook.com, 2022. [Online]. Available: https://pitchbook.com/news/articles/quantum-computing-venture-capital-funding. [Accessed: 06- Dec- 2021].

[2] Herrera, D., Fandiño, J. and Torres, N., 2021. The Imminent Obsolescence of Cryptographic Algorithms and the Arrival of Quantum Computation. International Journal of Engineering Research and Technology, Volume 14(Number 7), pp.593-600.

[3] "CRYPTOGRAPHY IN CLOUD: A METHOD TO ASSURE SECU9 RITY IN CLOUD COMPUTING PLATFORM", International Journal of Recent Trends in Engineering and Research, pp. 132-136, 2018. Available: 10.23883/ijrter.conf.20171201.026.c1tsk.

[4] "Explainer: What is post-quantum cryptography?", Föhrenbergkreis ¨ Finanzwirtschaft, 2020. [Online].Available:https://fbkfinanzwir tschaft.wordpress.com/2019/07/18/exp lainer-what-is-post-quantumcryptography/. [Accessed: 16- Mar2020].

[5] "Shor's factoring algorithm", Quantiki, 2020. [Online]. Available: https://www.quantiki.org/wiki/shorsfactoring-algorithm. [Accessed: 22- Feb - 2020]

[6] "The Lead Developer, Why We Should Be Scared of Shor's Algorithm", Kunlabora.be, 2020. [Online]. Available: https://www.kunlabora.be/blog/2019/07/ 19/the-lead-developer-london-2019- must-watch-presentations/. [Accessed: 22- Feb - 2020].

[7] M. Wall, "Supremacy' Achieved: Quantum Computer Notches Epic Milestone", Space.com, 2020. [Online]. Available: https://www.space.com/quantumcomputer-milestone-supremacy.html. [Accessed: 02- Mar- 2020].

[8] S. Bushwick, "New Encryption System Protects Data from Quantum Computers", Scientific American, 2020. [Online]. Available: https://www.scientificamerican.com/ article/new-encryption-systemprotects-data-from-quantumcomputers/. [Accessed: 06- Mar2020].

[9] S. Aaronson, "The Limits of Quantum Computers", Scientific American, vol. 298, no. 3, pp. 62-69, 2008. Available: 10.1038/scientificamerican0308-62.

[10] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "NIST: Report on PostQuantum Cryptography," NIST, Tech. Rep., 2016.

[11] M. Campagna and C. Xing, "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges," ETSI, Tech. Rep. 8, 2015.

[12] "List of QC simulators", Quantiki, 2020. [Online]. Available: https://quantiki.org/wiki/list-qcsimulators. [Accessed: 18- Feb2020]

[13] U. (Author), "GRIN - Capabilities and Limitations of Quantum Computers", Grin.com, 2020. [Online]. Available: https://www.grin.com/document/2727 38. [Accessed: 18- Mar- 2020].

[14] E. Alkim, T. Poppelmann, and P. ¨ Schwabe, 2016, "Post-Quantum Key Exchange—A New Hope," USENIX Security Symposium on August 10-12, 2016, in Austin, TX.

[15] J. Bos, C. Coestello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, 2016, "Frodo: Take Off the Ring! Practical, Quantum-Secure Key Exchange from LWE," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 24- 28, 2016, in Vienna, Austria.

[16] "Experimenting with Post-Quantum Cryptography", Google Online Security Blog, 2020. [Online]. Available: https://security.googleblog.com/2016/ 07/experimenting-with-postquantum.html. [Accessed: 19- Mar2020].
[17] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography", Journal of the ACM, vol. 10 56, no. 6, pp. 1-40, 2009. Available: 10.1145/1568318.1568324.
[18] D. Micciancio, "Lattice-Based Cryptography," in Post-Quantum Cryptography, 2009, no. 015848, pp. 147–192.
[19] D. Bernstein and T. Lange, "Post Quantum cryptography", Nature, vol. 549, no. 7671, pp. 188-194, 2017. Available: 10.1038/nature23461.
[20] H. Singh, D. Gupta, and A. Singh, "Quantum key distribution protocols: A review," Journal of Computational Information Systems, vol. 8, pp. 2839–2849, 2012.
[21] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Physical Review Letters, vol. 81, no. 14, p. 3018, 1998.
[22] "M. Green, "Hash-based Signatures: An illustrated Primer", A Few Thoughts on Cryptographic Engineering, 2020. [Online]. Available: https://blog.cryptographyengineering.com /2018/04/07/hash-based-signaturesan-illustrated-primer/. [Accessed: 14-Mar- 2020]"
[23] M. Lee, "Quantum Computing and Cybersecurity", Belfer Center for Science and International Affairs Harvard Kennedy School, Cambridge, 2021. [Accessed: 07- Sep-2021]
[24] K. Shannon, E. Towe and O. Tonguz, On the Use of Quantum Entanglement in Secure Communications: A Survey. 2020.
[25] QuTech Academy, Quantum Key Distribution. 2021.
[26] P. Kumar Reddy, B. Bhupal Reddy and S. Krishna, "Multi-User Quantum Key Distribution Using Wavelength Division Multiplexing", International Journal of Computer Network and Information Security, vol. 4, no. 6, pp. 43-48, 2012. Available: 10.5815/ijcnis.2012.06.06 [Accessed-4 Dec-2021].
[27] W.K. Wootters and W.H. Zurek, ―A Single quantum cannot be cloned‖, Nature 299, pp.802- 803, 1982.
[28] S. R. Sihare and V. V Nath, "Analysis of Quantum Algorithms with Classical Systems Counterpart", International Journal of Information Engineering and Electronic Business, vol. 9, no. 2, pp. 20-26, 2017. Available: 10.5815/ijieeb.2017.02.03 [Accessed 11 December 2021].
[29] I. Vajda, "On Classical Cryptographic Protocols in Post-Quantum World", International Journal of Computer Network and Information Security, vol. 9, no. 8, pp. 1-8, 2017. Available: 10.5815/ijcnis.2017.08.01 [Accessed 9 December 2021].
[30] P. Shankar Rao and J. Aditya, "Quantum Cryptography", Computer Society of India, 2005. [Accessed 10 December 2021].

Authors' Profiles

Tohfa Niraula born in Biratnagar, Nepal in 1998. She received her B.Sc. in computer science from Kathmandu University, Dhulikhel in 2021.

She has worked as a Net Coordinator in Kathmandu University's Girls' Hostel and a Quality Assurance Engineer and Web developer in Eightsquare as well as Front End Developer in Ants Pvt Ltd. She has published a paper titled "Analysis of Factors Influencing Airfare of Domestic Airlines: Data from Local Ticket Booking Agency", in the Journal of Network Security and Data Mining in 2021. Her research interests include Data mining, Quantum Computing and Cryptography.

Aditi Pokharel is a software engineer with knowledge in software engineering practices such as coding, testing, code reviews, etc. She completed her Bachelor's degree in computer science from Kathmandu University, Dhulikhel in 2020. She has published a paper titled "Analysis of Stock Market using Data Mining Techniques", in the Journal of Network Security and Data Mining in 2021. Her research interests include Data mining, Quantum Computing and Cyber Security.

Ashmita Phuyal Ashmita Phuyal is a data analyst with knowledge in data analytics and visualization. She completed her Bachelor's degree in computer science from Kathmandu University, Dhulikhel. Her research interests include Data mining, Data Visualization, Knowledge Retrieval and Quantum Computing.

Pratistha Palikhel was born in Bhaktapur, Nepal in 1998. She received her Bachelor's degree in Computer Science from Kathmandu University, Nepal. She is currently working as a Technical Writer in Compliance Quest Software Company.

She has volunteered in the localization of LibreOffice. She has published a paper titled "Analysis of Factors Influencing Airfare of Domestic Airlines: Data from Local Ticket Booking Agency", in the Journal of Network Security and Data Mining in 2021. Her research interests include Illustration, Quantum Computing and Data Mining.

Manish Pokharel received his postdoctoral degree from Korea Aerospace University, South Korea. He is currently the Dean of the School of Engineering at Kathmandu University.

He has been involved in the IT sector since 1995. He has worked as a consultant in NIPA[National IT Industry Promotion Agency] to develop the E-Government Master Plan for Costa Rica and the Philippines. Appointed as a member of the High-Level ICT Council under the chairmanship of Honorable Prime Minister of Nepal. His research interests include Digital Governance, SMART City, Internet of Things (IoT), Artificial Intelligence (AI), Cloud Computing, Big Data and Software Technology.

How to cite this paper: Tohfa Niraula, Aditi Pokharel, Ashmita Phuyal, Pratistha Palikhel, Manish Pokharel, "Quantum Computers' threat on Current Cryptographic Measures and Possible Solutions", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.12, No.5, pp. 10-20, 2022. DOI:10.5815/ijwmt.2022.05.02