Journal of Quantum Algorithms and Cryptography (JQAC)

https://utilitasmathematicapublishing.com

Vol: 1, ISSUE: 1, 2025

Pg No: 16-24

Quantum Cryptography: A General Introduction and Shor's Algorithm

A. Vignesh [1], D. Kanchana [2], PM. Kavitha [3], M. Anitha [4], D.B. Shanmugam [5]

[1] Assistant Professor, Department of Computer Science and Applications, SRM IST, Ramapuram Campus, Chennai

[2] Assistant Professor, Department of Computer Science and Applications, SRM IST, Ramapuram Campus, Chennai

[3] Assistant Professor, Department of Computer Science and Applications, SRM IST, Ramapuram Campus, Chennai

[4] Assistant Professor, SRM TRP Engineering College, Trichy

[5] Assistant Professor, Department of Computer Science and Applications, SRM IST, Ramapuram Campus, Chennai

ABSTRACT

The purpose of this article is to take a look at how quantum cryptography works and how it compares to traditional encryption methods. We provide a quick overview of quantum computing and highlight its promise using a simplified description of Shor's Algorithm. Prominent databases such as IEEE Xplore, ScienceDirect, and JSTOR were used to gather relevant material, which included books, journals, conferences, lecture notes, and websites, all pertaining to quantum cryptography. The workings of quantum cryptography and Shor's algorithm were therefore better understood. Using examples to illustrate the complexities of Shor's method, the authors provided a concise description of quantum cryptography and showed how encryption is accomplished by using the features of quantum particles. By staying up-to-date on the latest findings in quantum cryptography, interested academics might encourage future cryptography scholars to go further into quantum computing, quantum cryptography, and other quantum theory concepts.

Keywords: Concepts such as quantum public key distribution, quantum theory, cryptography, and Shor's algorithm are essential.

1. INTRODUCTION

The struggle between those who create new codes and those who attempt to crack them has persisted throughout the history of computer science [1]. The classical computer community has long considered the development of an unbreakable encryption algorithm to be the pinnacle of cryptography. The poor processing power of classical computing is the reason why it is difficult to crack the encryption [2]. The goal of this work is to provide light on the concepts underlying encryption and cryptography as they pertain to classical and quantum computers. In order to understand the computational difficulty of quantum cryptography, we also reviewed Shor's algorithm. Classical computers are known to exclusively store binary data (0 or 1), however quantum computers Data may be encoded in one of three possible states: 1, 0, or a combination of the two (superposition states) [3]. Some have speculated that quantum computers possess the necessary enormous computational capacity to crack conventional computer encryption [2] [4].

Some classical encryption techniques may be impossible for classical machines to break in this day and age. using the other hand, the same program would execute in a tenth of the time using quantum computers. The square root of the time it takes the classical method to calculate is about how much time the quantum algorithm would require, according to realistic estimations [5]. Additionally, it should be noted that algorithms expressly characterized by or dependent on a key aspect of quantum processing, such as quantum superposition or entanglement, are specifically referred to as quantum algorithms. Digital signatures are among the most important basic cryptographic schemes that are currently accessible. The discrete logarithm assumption (DSA) and the RSA algorithm form the basis of these cryptographic techniques. According to Shor's groundbreaking research [6], none of the aforementioned will be safe when the quantum computer finally appears. So, Post-Quantum cryptographic techniques are becoming more and more of a priority for cryptography experts.
It follows that the superposition/entanglement property of quantum computers is crucial to quantum cryptography and Shor's method.

1.1 A Brief History of Cryptography and Shor's Algorithm

Since 1900 BC, some form of cryptography have been in use for a long time, with its roots traced back to the Egyptian mummy traditions [7]. The purpose has always been to find a secure means of passing messages.
It all started in 1981 by Richard Feynman at MIT, where he proposed a basic model for a quantum computer. Feynman was able to outline the possibility to outpace classical computers exponentially. Since Feynman came up with the quantum concept, lots of researches have been done on the field. As already pointed out, quantum computers are considered the destructor of the present-day classical cryptography [8].

Peter Shor, an American Mathematician while working in Bell Labs, New Jersey in 1994, formulated the Shor's algorithm. The algorithm was designed for integer factorization. Shor proved that a quantum computer when operating optimally (without succumbing to environmental noise or another quantum related interference) could effectively break classical cryptography schemes such as the RSA. A large integer factorization problem has been a major limitation of classical cryptography, but quantum computers take advantage of Shor's algorithm to solve this problem [9].

2. LITERATURE REVIEW

Scholarly works on quantum cryptography are included in this section. It is expected that this will assist scholars in the subject of quantum cryptography and related areas in better understanding the nature of quantum cryptography.

2—Traditional Cypher

A message's information may be concealed from prying eyes using cryptography, which also serves to authenticate the message's correctness. As our society becomes more and more digital, cryptography is crucial for keeping sensitive information secure. The primary goal of encryption, the first cryptographic method, was to ensure the privacy of its users. It has been around for a while, but prior to the digitization boom, it was mostly used to secure government and military communications. To further guarantee the authenticity and integrity of data, cryptographic hash functions and digital signature algorithms are used [10].

With the introduction of the avatars, Alice (the sender) and Bob (the receiver), classical cryptography introduces the idea of encryption and decryption, where a parameter called the key is set by the parties involved. Cryptanalysis = E_(K)(P) An example of a cryptographic system is the decryption function P = E_(K)^(-1)(C). Using a keyspace K as a parameter, the particular transformation is selected [11].

Section 2.1.1: Cryptography Fundamentals and Shor's Algorithm

In contrast to quantum computers, which use qubits to encode data, classical systems use bits. In this case, superposition allows for the encoding of more than two states in a single qubit [12]. Take, for example, a computer having four classical bits; in most cases, you may describe it as 24 or 16, among other permutations. Sequences like 0000, 0001, 0010, 0011, etc., are examples. Any one of the sixteen states might be this. Nonetheless, the theory of quantum computing dictates that a superposition of four quantum bits (qubits) may exist in any one of the sixteen conceivable configurations at the same time. According to this idea, a 20-qubit register could simultaneously hold 1,048,576 values, which is one million. This is plausible because, as seen in figure 1, an atom may coexist in two states (superposition) at the same time, |0> and |1> [12]. Here, the two states stand in for the two atomic energy levels.

So, the ground state is represented by |0> and the excited state is |1>. The fact that one Qubit may stand in for two states at once has been proven: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. In this case, α and H represent the measured probabilities of the superposition collapsing to |0> or |1>, respectively [13].

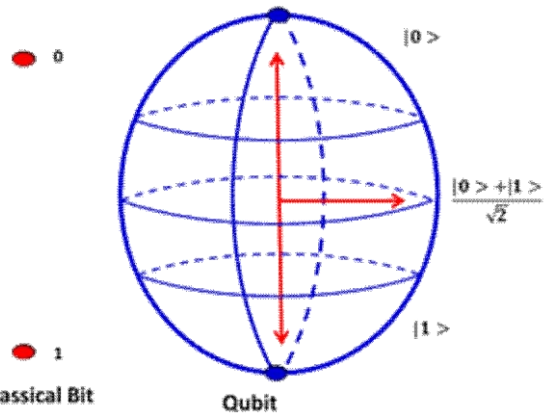

Figure 1: Comparing Classical bit and Qubit Source: [14]

Integer factoring and discrete logarithm computations benefited from Peter Shor's research on polynomial-time quantum computer methods [15]. Here is an example of how numbers may be factorized using Shor's algorithm:

A 4-qubit register is required to determine prime factors of 15 using Shor's method [16]. As an example, the binary representation of the number 15 is 1111. This is because a 4-qubit register is conceptually similar to a 4-bit register in a classical computer. Therefore, the prime factorization of 15 is computed using a 4-qubit register. For each possible number between zero and fifteen, this kind of calculation is executed in parallel [17]. The present state of classical computer encryption is insecure, and cracking it will need millions—if not thousands—of error-free qubits [2].

2.1 The Traditional Approach to Classical Computer Cryptography

As a result of concerns about privacy while transmitting sensitive information, numerous intriguing and unconventional methods of data encryption have been developed. Take the Nazis' production of a massive typewriter-like device called "the Enigma" during WWII as an example. Notable pre-computer era ciphers (encoded communications) were created with the device [18]. During the height of the war, Polish block resistance fighters built identical devices, complete with instructions on how to use the Enigma. It took a long time to decipher the communications, but it was ultimately cracked. This was an extraordinary effort given the circumstances back then. That was the first step in what would

become an endless loop of encryption and decryption [19]. Very quickly, public keys became the de facto standard for data encryption. However, there is a catch: There are many potential applications for keys in cryptology. Research into codes with the goal of enhancing data secrecy and integrity is known as cryptology. Currently, the most popular forms of cryptography are public-key and secret-key. In both of these approaches, the person sending the message is called Alice and the person receiving it is called Bob. The public-key cryptography (PKC) approach requires the user to choose two related keys, which are thereafter shared with anybody wishing to communicate with them. So, although it's theoretically feasible for Alice to communicate with Bob, only the keyholder would be able to decipher their communications. The ideal situation is when not even the sender knows the decryption code.
For clarity, consider the following analogy: Imagine a mailbox with two keys: one opens the front door, and anybody with the key can put mail in the box. The second key, which is accessible to the recipient, opens the mailbox's rear and allows them to retrieve messages stored within. Let us now have a look at secret-key cryptology (SKC), another classic approach to cryptography. For SKC to work, Alice and Bob must share a single key for encoding and decoding. Without the key, eavesdroppers will still be unable to decipher the message, regardless of how secure the channel is that the encryption technique uses [*00]. To elaborate further, consider the following analogy: Imagine a mailbox with a message and a key inside; anyone can open the box, but only the keyholder can read the message. The One-Time-Pad (OTP) method follows. As an encryption method, one-time passwords (OTPs) utilize a secret key that is at least as lengthy as the original message. In [20], Claude Shannon demonstrated that the OTP is completely secure. The fact that you can only use this random key once is a downside as it means you'll have to buy more keys in the future. In conclusion, classical computers are very susceptible to eavesdropping when keys are sent via an unsecured channel. There is no foolproof method to detect whether Eve (an eavesdropper) has duplicated the keys that Alice and Bob communicate over an unsecured channel.

2.3. Fundamental Principles in Classical Computers that Limits its Power to Break Encryption

The major obstacle in breaking today's encryption scheme by classical computers is as a result of the massive size numbers used in the combination of the keys. It was deliberately made to ensure data security. The combination of numbers in modern keys is very complex and intricately designed. For instance, to crack a 128-bit key, the number combination has an exponential power 1038 [20].
You can now imagine the computational power of a system that can get the correct combination and how long it could possibly take. Researchers estimate that it will take a billion computers working in parallel and with each processing as much as a billion calculations per second and will still take a trillion years to crack a key [20]

2.4 Review on Related Literature on Classical Cryptography

Different researches have been published in the field of classical cryptography. In this section, we will present a few of this literature.
In [22], a description of the conventional cryptography fundamentals and its concepts was made.
The book described the basic terminologies and cryptographic schemes, including symmetric and asymmetric cryptography. The authors also highlighted the basic ciphers such as substitution and transposition ciphers, and one-time pads. Information-theoretic approach to cryptography was also talked about.
Authors [10] explained how long-term confidentiality of information had become a major challenge for classical cryptography. This is because of the complexity-based nature of current cryptography methods. This is attributed to the fact that classical cryptographic security is dependent on the intractability of certain algorithms.
Work done in [23] discussed the classical cryptography and techniques connected to it. How to use data string (Key) to secure the transmission of messages between interested parties were discussed. The two main techniques of classical cryptography, namely; Asymmetric and symmetric were also discussed in detail as shown in figure 2.

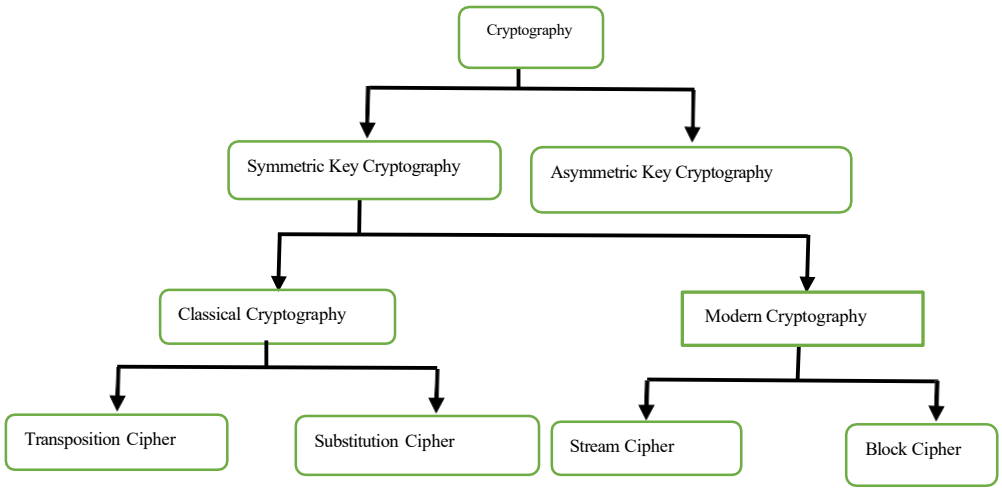

Figure 2: Classical Cryptographic Algorithm [21]

The article demonstrated that symmetric cryptography relies on a single key for both encryption and decryption, but asymmetric cryptography use a key pair.
The authors provided a concise explanation of the uses of hash functions, symmetric algorithms, and asymmetric algorithms in contemporary cryptography in [16]. Factorizing big numbers, such as RSA numbers, is both fascinating and challenging, as discussed in this article. Also covered extensively was the discrete logarithm issue and the basics of powerful asymmetric ciphers. A concise overview of cryptography, a mathematical mechanism that ensures data transit between computers remains secret, was provided by the author in [24]. Also covered were the early ciphers devised by Augustus and Julius Caesar. The author discussed cryptography, key use, the Enigma cipher and its decipherment, symmetric-key and public-key cryptosystems, and their respective benefits and drawbacks.
A thorough overview of current cryptography systems and the underlying mathematical ideas was given in [25]. Ciphers, including how to encrypt and decode them, were covered in the study. In addition, they contrasted digital signatures, public-key cryptography, the RSA cryptosystem, data encryption standards (DES and AES), and stream and block ciphers.
Cryptography, cryptanalysis, decryption, and encryption were all discussed by the author in [26]. Both symmetric and asymmetric key cryptography, as well as other cryptographic methods, were covered. Digital signature implementation, RSA algorithm, hash function/algorithm, and potential cryptography attacks were also covered in the article.

Part 2.5: The Fundamentals of Quantum Cryptography The goal of cryptography as a whole is to ensure the delivery of unbroken messages. The three main players in cryptography are the sender (Alice), the receiver (Bob), and the possible eavesdropper (Eve), according to the layman's definition. The symmetric system allows for the encryption and decryption of messages by the sharing of a key, which consists of random bits, between Alice and Bob [27]. If Eve manages to get her hands on the key, the whole encryption system will be rendered useless. Therefore, secure key distribution is critical for conventional cryptography, and this is precisely the problem that quantum cryptography aims to solve.
Despite popular belief, quantum cryptography is impenetrable because it relies on key distribution via single-photon transmission rather than encryption techniques [28]. For optimal digital data transmission, single photons are used, as each photon encodes either a 0 or a 1. Because even a little amount of ambient light may distort the signal, it is very unpredictable and difficult for eavesdroppers to detect [29].
Quantum computing and encryption have emerged as a result of the significant contributions made by quantum scientists in recent years. Both make use of entanglement and superposition, two cornerstones of quantum mechanics. A photon may exist in all four conceivable states simultaneously (0, 1, 0, and 1), a phenomenon known as superposition.

whereby entanglement delineates the connection of two or more attributes of particles that have become interdependent [30]. In contrast to conventional cryptography, which relies on mathematical techniques to encrypt data, quantum cryptography uses the laws of quantum physics. Sending data via insecure networks in this way is a safer mission [31].

2.6 Encryption and Quantum Computers
The one-time password (OTP) is the only foolproof method for evading classical cryptography's encryption algorithm issue, as previously stated. But we have listed the potential downside of that specific approach, particularly with respect to its one-time usage. Through the manipulation of quantum particle properties, quantum cryptography is able to resolve all key distribution concerns. Regarding this, one photon may stand in for a qubit, and to determine the qubit's value, one must measure the photon's properties, such as its polarization. The tough part comes now because, in most circumstances, measuring a photon's qualities changes its properties. Since both Alice (the sender) and Bob (the receiver) can notice any changes that occur from the measurement, it becomes exceedingly difficult for anybody attempting to eavesdrop on the message. Alice and Bob will undoubtedly get different values for the qubits when they compare them, allowing them to dismiss the qubit, even if an eavesdropper named Eve attempts to measure or copy the key. Thus, quantum cryptography remains impenetrable at this time. Nonetheless, a technique for monitoring quantum particles that does not impact their state could be found in the future. Experts in the field are now focusing on this.

Distributing Quantum Public Keys (2.7)
Classical encryption has a number of problems, the most significant of which is that it cannot assume anything about an attacker's capabilities since its fundamental design depends on the power of the mathematical calculation used to create it [32]. By using quantum features to communicate secret information like cryptographic keys, Quantum Key Distribution emerges as a brilliant solution to the problems encountered by traditional encryption. Messages sent across unsecured routes may subsequently be encrypted using this. A quantum transmission is accomplished by use of a series of rectilinear or diagonal photon locations that serve as polarization bases. A binary bit of 0 is represented by a photon at 45 degrees horizontally, while a binary bit of 1 is represented by a photon at 135 degrees vertically [33].
Since light consists of indestructible particles called photons, its polarization makes it an excellent medium for encoding quantum information. Researchers in the quantum field may encrypt quantum bits of information into the polarization of individual photons and produce them one by one. We can construct trustworthy quantum networks by exchanging photons that have been polarization-encoded [34]. Even several photons' polarizations may be entangled by laboratories researching quantum light.

https://utilitasmathematicapublishing.com
Vol: 1, ISSUE: 1, 2025
Pg No: 16-24

The random max of rectilinear and diagonal photons in a quantum transmission means any interference will alter the transmission and stir up disagreements between Alice and Bob on some of the bits as shown in figure 3 [35].

Quantum entanglement and non-locality, a phenomenon that ensures that each particle's quantum state cannot be individually identified, was also discussed. Other important topics from the research paper include; quantum cryptographic constructions, and quantum cryptographic limitations and challenges.

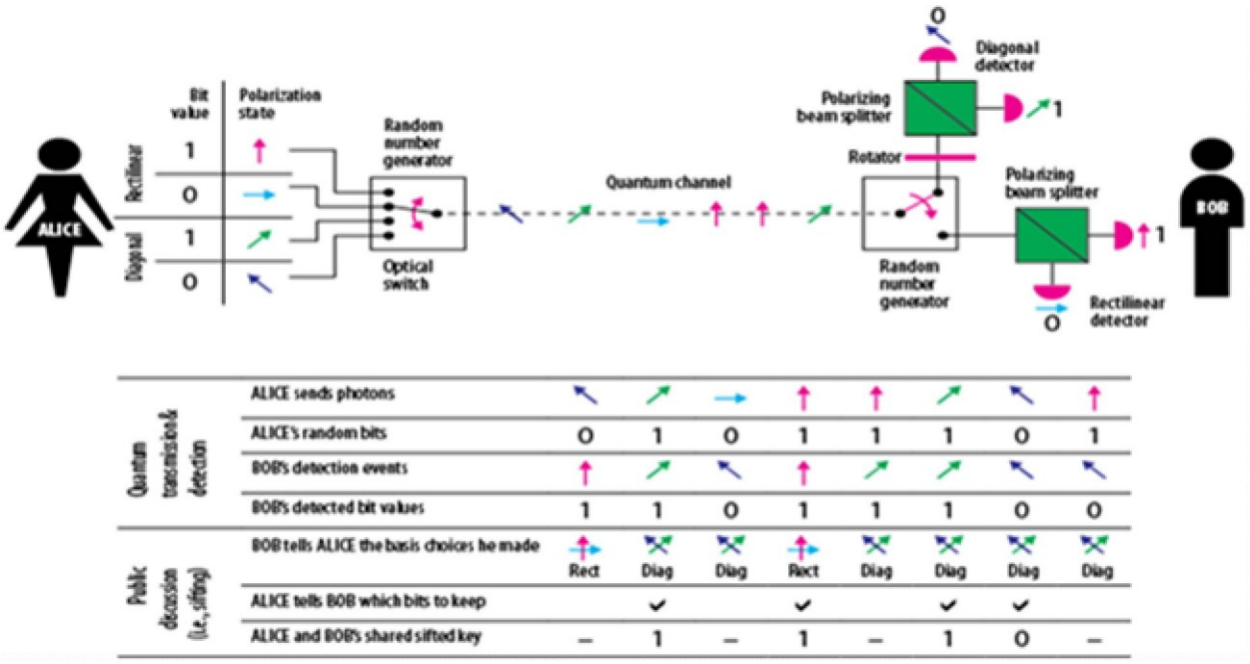

Figure 3: Quantum Public Key Distribution BB84 protocol [36]

2.5 Review on Related Literature on Quantum Cryptography

This section covers some research papers published on Quantum cryptography.

The paper [35] discussed the properties of polarized photons, which is a key element of a quantum system. Polarized light is generated by sending an ordinary light beam through a polarizing apparatus. Although polarization is a continuous variable; however, the uncertainty principle ensures that no photon can reveal more than one bit about its polarization on measurement. This is one of the reasons why quantum cryptography is highly secured when compared to classical cryptography. In quantum public key distribution, the quantum channel is not directly used to send messages. Instead, it is used to transmit a supply of random bits between users. Then, when investigated subsequently subject to passive eavesdropping, the users can detect with high probability if the original quantum transmission has been disturbed in transit.

In [37], the basics of quantum information in detail, including the unitary evolution and circuits in the linear operation of a quantum system. The quantum no-cloning feature which makes it physically impossible to clone a quantum system.

The authors in [30] discussed the general principles of quantum science and quantum technologies. They explained in detail the principles of quantum cryptography, especially quantum key distribution (QKD), how it works, and its weaknesses. They identified the two primary forms of a quantum communication network; the use of QKD across nodes with fiber connection and then, the "free space" quantum communications via open air. The authors also discussed the advances in the research on "quantum materials" and their potential impact on quantum science.

The current and prospective markets for quantum key distribution (QKD) and related quantum communications technologies was examined in [38]. The work showed how distance impacted the widespread use of QKD and compared the overall security architecture of the quantum system over the conventional classical cryptographic systems. According to the authors, QKD products have been commercialized publicly for over a decade and are valued at $50-500 million annually.

In [39], the authors provided a comprehensive insight into quantum science and cryptography. They started with the origins of cryptography and quantum communications, showed the experimental state of advanced quantum

communication with entangled photons, quantum logic using linear optics and quantum state sharing. They also explained further the intrigues of free-space quantum cryptography and then how noise-immune quantum key distribution works.

The authors in [40] experimented on the effect of turbulence on an underwater quantum channel using twisted photons. The aim was to show the feasibility of high-dimensional encoding schemes in comparison with different quantum protocols in an underwater quantum channel. The researchers sent a Gaussian laser beam over a 3m underwater link at a wavelength of 635nm. The result showed that they successfully achieved a positive secret key rate with a 2- and 3-dimensional QKD BB84 protocol.

3. CLASSICAL CRYPTOGRAPHY VS. QUANTUM CRYPTOGRAPHY

Using mathematical methods with large prime numbers, classical cryptographic techniques are almost impossible for classical computers of today to crack. In theory, the security architecture of classical encryption will fail when tested on future quantum computers due to the anticipated speed and superposition feature of these computers, which is a direct result of the assumption that classical cryptography's prime numbers are indecipherable. se.

On the other hand, quantum cryptography systems are secure because they use photons to convey information at the atomic level, which is protected by the principles of quantum physics [41].

Conventional transmission mediums cannot reproduce the unique cryptographic phenomena guaranteed by the uncertainty principle in primitive quantum systems. Due to the high-probability of disruption when it meets any external interference while transmitting, it is theoretically impossible to eavesdrop inside a quantum communications channel without being noticed [35].

Additionally, the following characteristics allow for a comparison of classical and quantum cryptography:

a) Technical aspects: 50 km is the sweet spot for quantum communication systems when it comes to data transmission efficiency [42]. Classical cryptography, on the other hand, allows for communication distances that may reach several million kilometers. With that said, real-time secure keys transmitting continuously at rates surpassing 10 Mb/s have set a new bitrate record for quantum communication using QKD [43]. In traditional cryptography, the processing capacity is the primary determinant of the bit rate.

b) Cost considerations: Quantum cryptography is prohibitively costly and only works for direct connections at the moment [44]. Conversely, customers may almost pay nothing to have traditional cryptography implemented in software.

c) Features of the application: A digital signature verifies the validity of digital data for traditional cryptography. The receiver may be certain that the communication was unaltered in transit thanks to a digital signature. conveyance [32]. Generation of keys, signing of keys, and verification of keys are the three primary algorithms. However, due to the usage of quantum mechanisms in quantum cryptography, algorithms are not simply implementable.

d) Baseline: In principle, it is possible to observe any traditional private channel without the parties involved knowing. However, due to the photons' inherent volatility, this becomes more challenging in quantum systems [23].

4. SHOR'S ALGORITHM

Prime numbers are, by definition, divisible only by themselves (or the number 1). They are the foundation of the number system. So, when asked the prime factors, or multipliers, for the number 15, almost every student with basic mathematical background knows the answer to be; 3 and 5 by memory. However, a larger number, such as 91, might call for some pen and paper before one could solve it. Also, a larger number, like 232, can (and has) taken scientists two full years to factor, even with hundreds of high-speed classical computers operating in parallel. Most encryption schemes like credit cards, state secrets, and other confidential data are based on the difficulty in factoring these numbers [45]. For example, in 2016 the RSA-220 which is 220 digits long was factored with significant computer resources [46]. Theoretically, a single qubit computer can easily crack this problem, by using hundreds of atoms, in parallel, to quickly factor the RSA-220 and other huge numbers.

Peter Shor, in 1994, came up with a quantum algorithm that was able to compute with a high-level of efficiency the prime factors of huge numbers that previously impossible for any classical supercomputer [47].

The basic idea of Shor's algorithm is the process of period-finding using the Quantum Fourier Transform (QFT). The QFT takes some function f(x) and figures out the period of the function [48].

Shor's algorithm is given as follows:

1. First, a random positive integer $m < n$ is chosen, then the gcd(m, n) is calculated in polynomial time using the Euclidean algorithm. If gcd(m, n) $\neq 1$, the prime factor of n has been found, and the problem is done. But, if gcd(m, n) = 1, then proceed to step 2.
2. A quantum computer is then used to get the unknown period P of the sequence and is given as follow; x mod n, x2 mod n, x3 mod n, x4 mod n, ... 4.
3. To proceed, if P is found to be an odd integer, step 1 is repeated. But, if P is an even integer, we proceed to step 4. Since the period P is even, $(m^{P/2}-1)(m^{P/2}-1)=m^{P}-1=0$ mod n
4. The next step is to check if $m^{P/2} + 1 = 0$ mod n, and if so, step 1 is repeated. However, if $m^{P/2} + 1 \neq 0$, then proceed to step 5.
5. Finally, *to compute* d = gcd($m^{P/2}$ - 1, n), we use the Euclidean algorithm, and since $m^{P/2} + 1 \neq 0$ mod n was proven in step 4 above, we can also show that d is a significant prime factor of n.

An example to illustrate Shor's algorithm is as follows:

Below is an example of how $n = 91(=7*13)$ can be factorized using Shor's algorithm:

1. A random positive integer $m = 3$ is chosen since gcd (91,3) =1
2. The period P is given by:
$$f(a)=3a \bmod 91$$

Shor's algorithm is used to find the period P, on a quantum computer, i.e., $P = 6$. Since the period P is even, we proceed to step 4.

3. Since the equation does not equal 0 mod 91, we proceed to step 5.
$3^{P/2}+1=33+1=28\neq 0 \bmod 91$
4. See below:
$d=gcd(3^{P/2}-1, 91)=gcd(33-1, 91)=gcd(26,91)=13$

Through careful calculation and the use of a quantum computer, the significant prime factor of $d = 13$ was found of $n = 91$ [49].

Note: So far, many researchers in quantum science have tried to implement Shor's algorithm with quantum systems; however, none have been successful in a scalable way with more than a few quantum bits [50].

5. AREAS OF APPLICATION OF QUANTUM CRYPTOGRAPHY

The capabilities and capabilities of quantum computers to do complex tasks have been covered in this study. However, is it presently sold in stores? "No," is the simplest way to put it; it is far from finished. In addition, a hybrid platform that securely employs both conventional and quantum computing in the cloud may be necessary for the effective deployment of various application areas [51]. Consequently, below are a few domains where quantum cryptography might be useful:

1) Chemistry with Computers: Solving many challenges in material science becomes easy when the correct catalyst is discovered for effectively improving current materials or creating new ones. So far, chemical interaction simulations have relied on conventional computers; nevertheless, there are situations where this approach may not be enough. Richard Feynman investigated the potential applications of a quantum computer in modeling quantum mechanical processes [51]. Here are a few key issues that, if addressed, might have a significant influence:

i) Ammonia, a key ingredient in fertilizers, requires the present Haber process

ii) Discovering innovative and sustainable materials is crucial if we are to reach room-temperature superconductors.

iii) Discovering a catalyst that enhances carbon sequestration efficiency.

iv) Novel battery chemistry is required for enhanced performance, since current lithium-ion batteries are in dire need of improvement [52].

Software, Hardware, and Circuit Fault Simulation: Creating a large piece of software often necessitates the use of Application-Specific Integrated Circuit (ASIC) devices with billions of transistors or millions of lines of code. It is often exceedingly difficult and costly to use a classical computer to check for accuracy in this situation. It is critical to identify and control errors. When it comes to saving lives or money, mistakes may have devastating consequences. Quantum computing has the ability to speed up these simulations and provide far greater coverage [52].

2) The Chinese and Austrian academies of sciences were the first to showcase the concept of the quantum internet. A secure video conference between the two universities was the intended goal of the intercontinental quantum communications experiments. They were able to successfully transmit the first photon packets 1,200 km to the Chinese Micius satellite. The packets were transmitted to Europe as the satellite sped past China. This accomplished the remarkable feat of laying down a secure fiber optic communication route spanning 7,600 kilometers between China and Austria. A future quantum internet may be traced back to this [13].

2) Swiss Secure Ballotting: The rollout of online voting in Switzerland was an early innovation. When it came to securing their electronic votes, the Swiss were the first to utilize a quantum cryptography system. Their central voting station's connection to government data centers via fiber-optic links was encrypted using a quantum cryptography method. The encryption boxes secured point-to-point connections using Triple-DES and used quantum cryptography for secret key exchange. A 1Gbps encryption bit rate was available on the device. One major drawback is that the encryption protons started to weaken after a transmission distance of 50 km [53].

6. DISCUSSION

Classical and quantum cryptography, as well as the fundamental ideas behind them, have been introduced and simplified in this study. We took a look back at some important studies conducted in conventional and quantum cryptography. The goal of the study is to provide a solid groundwork for newcomers to quantum cryptography and to encourage them to pursue further studies in the subject.

7. CONCLUSION

The incidence of data breaches in government and corporate databases throughout the globe has increased the need for privacy and data security to an all-time high. Modern cryptography systems face an even greater threat from quantum computers and Shor's Algorithm. The need for solutions to ensure the security of data has piqued the attention of experts in quantum cryptology.

REFERENCES

[1] Ed. Urie, "Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union. By Stephen Budiansky. New York, NY. Borzoi Book, Published by Alfred A. Knopf, Penguin Random House, New York, 2016.." Journal of Strategic Security 10, no.3 (2017):94-95. DOI: http://doi.org/10.5038/1944-0472.10.3.1641 Accessed on: Aug. 23, 2019. [Online] Available at: http://scholarcommons.usf.edu/jss/vol10/iss3/7

[2] R. De Wolf, "The potential impact of quantum computers on society." Ethics Inf Technol 19, 271–276, 2017. Accessed on: Aug. 23, 2019. [Online] Available at: https://doi.org/10.1007/s10676-017-9439-z

[3] D. Maslov, Y. Nam, & J. Kim, "An outlook for quantum computing [point of view]." Proceedings of the IEEE, 2018, 107(1), 5-10.

[4] J. P. Aumasson, "The impact of quantum computing on cryptography." Computer Fraud & Security, 2017(6), 8-11.

[5] A. Bhalla, E. Kenneth, and H. Matthew. "Quantum Computing, Shor's Algorithm, and Parallelism." Accessed on: Aug. 23, 2019. [Online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.1823&rep=rep1&type=pdf

[6] JF. Biasse., G. Micheli, E. Persichetti, P. Santini "LESS is More: Code-Based Signatures Without Syndromes. In: Nitaj A., Youssef A. (eds) Progress in Cryptology - AFRICACRYPT 2020. AFRICACRYPT 2020." Lecture Notes in Computer Science, 2020, Vol. 12174. Springer, Cham

[7] S. Huzaifa "A Brief History of Cryptography," Jan. 2, 2019, Accessed on: May. 13, 2019. [Online]. Available: https://access.redhat.com/blogs/766093/posts/1976023

[8] Mavroeidis, Vasileios, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. "The Impact of Quantum Computing on Present Cryptography," International Journal of Advanced Computer Science and Applications, 2018, Vol. 9, No. 3.

[9] J. Norman. Formulation of Shor's Algorithm for Quantum Computers, Apr. 30, 2020, Accessed on: June. 13, 2020. [Online]. Available: http://www.historyofinformation.com/detail.php?id=3877

[10] J. Buchmann, J. Braun, D. Demirel, M. Geihs. "Quantum cryptography: a view from classical cryptography." Quantum Science and Technology. 2017 May 25;2(2):020502.

[11] W. Diffie, M.E. Hellman. "Privacy and Authentication: An Introduction to Cryptography," in Proc. IEEE, Vol. 67(3) Mar 1979, pp 397-427

[12] T. Li, & Z. Q.Yin. "Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator." Science Bulletin, 2016, 61(2), 163-171.

[13] Nils Jacob Sand. "Introduction to Quantum Cryptography," Nov. 23, 2018. Accessed on: May. 13, 2019. [Online]. Available: https://www.norwegiancreations.com/2018/11/introduction-to-quantum-cryptography/

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

[15] M. Ekerå. "Revisiting Shor's quantum algorithm for computing general discrete logarithms." Accessed on: Aug. 13, 2019. [Online]. Available: arXiv preprint arXiv:1905.09084

[16] V. Mavroeidis, K. Vishi, M.D. Zych, & A. Jøsang. "The impact of quantum computing on present cryptography." Accessed on: May. 13, 2019. [Online]. Available: arXiv preprint arXiv:1804.00200

[17] S. Bone and M. Castro. "A Brief History of Quantum Computing," Surveys and Presentations in Information Systems Engineering (SURPRISE), vol. 4, no. 3, pp. 20–45, Accessed on: Aug. 13, 2019. [Online]. Available: http://www.doc.ic.ac.uk/~nd/surprise 97/journal/vol4/spb3/

[18] L. Andrew. "Breaking Germany's Enigma Code." April 2011; Accessed on: July. 13, 2020. [Online]. Available: http://www.storytellingworld.com/33669/EnigmaMachineWWIIShtr.pdf

[19] J. CLARK. "How Quantum Cryptology Works," Oct. 23, 2007. Accessed on: May. 13, 2019. [Online]. Available: https://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology1.htm

[20] C. E Shannan. "Communication Theory of Secrecy Systems," Bell System Technical Journal, Oct. 1949, Vol. 28-4, pp. 656-715,

[21] Shashank. "What is Cryptography? – An Introduction to Cryptographic Algorithms," May, 2020. Accessed on: July. 13, 2020. [Online]. Available: https://www.edureka.co/blog/what-is-cryptography/

[22] I.B. Djordjevic. "Conventional Cryptography Fundamentals." In: Physical-Layer Security and Quantum Key Distribution. Springer, Cham. 2019, pp 65-91.

[23] Patil, Pooja Anil, and Renuka Boda. "Analysis of Cryptography: Classical versus Quantum Cryptography." International Research Journal of Engineering and Technology (IRJET) 2016, Vol. 3, no. 05.

[24] G. O'Regan. "Cryptography. In: Guide to Discrete Mathematics." Texts in Computer Science. Springer, Cham, Accessed on: Aug. 13, 2019. [Online]. Available: https://doi.org/10.1007/978-3-319-44561-8_10

[25] C. Paar, J. Pelzl. "Introduction to Cryptography and Data Security." In: Understanding Cryptography. Springer, Berlin, Heidelberg; Accessed on: Aug. 13, 2019. [Online]. Available: https://doi.org/10.1007/978-3-642-04101-3_1

[26] U.H. Rao, U. Nayak, "Cryptography." In: The InfoSec Handbook. Apress, Berkeley, CA; Accessed on: Aug. 13, 2019. [Online]. Available: https://doi.org/10.1007/978-1-4302-6383-8_8

[27] M. Abadi, & D. G. Andersen. "Learning to protect communications with adversarial neural cryptography." Accessed on: Aug. 13, 2019. [Online]. Available: arXiv preprint arXiv:1610.06918

[28]M. Brooks. "Quantum computing and communications;" Springer-Verlag London Limited, 1999, PP. 87-93.

[29] T. B. Tentrup, T. Hummel, T. A. Wolterink, R. Uppu, A. P. Mosk, & P. W. Pinkse, "Transmitting more than 10 bit with a single photon." Optics express, 2017, 25(3), 2826-2833.

[30] E. Kania, and J. Costello. "QUANTUM HEGEMONY?: China's Ambitions and the Challenge to U.S. Innovation Leadership," The Second Quantum Revolution. Center for a New American Security, 2018, pp. 3–5, Accessed 16 July, 2020. [Online]. Available: www.jstor.org/stable/resrep20450.5.

[31] K. Crane, L. Joneckis, H. Acheson-Field, I. Boyd, B. Corbin, X. Han, & R. Rozansky. "Assessment of the Future Economic Impact of Quantum Information Science". Institute for Defense Analyses. (pp. 33-42, Rep.) Accessed 16 July, 2020. [Online]. Available: doi:10.2307/resrep22837.6

[32] T.Y. Wang, X.Q. Cai, Y.L. Ren, R.L. Zhang. "Security of quantum digital signatures for classical messages." *Scientific reports* 5 (2015): 9231.

[33] Quantum-Safe Security Working Group. What is Quantum Key Distribution? Accessed on: May. 13, 2019. [Online]. Available: https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf

[34] J-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens. "Robust polarization-based quantum key distribution over a collective-noise channel." *Physical review letters* 92.1 (2004): 017901.

[35] C.H. Bennett, G. Brassard. "Quantum cryptography: Public Key Distribution and coin tossing," Theoretical Computer Science 560. 2014, P. 7-11.

[36] Sophia Antipolis. "BB84 PROTOCOL," May. 2, 2015, Accessed on: May. 13, 2019. [Online]. Available: http://physique.unice.fr/sem6/2014-2015/PagesWeb/PT/Tomographie/?page=bb84

[37] Broadbent, Anne, and C. Schaffner. "Quantum cryptography beyond quantum key distribution." Designs, Codes and Cryptography 78, 2016, no. 1: 351-382.

[38] Crane, Keith W. "Quantum Communications." Institute for Defense Analyses, Assessment of the Future Economic Impact of Quantum Information Science, 2017, pp. 33–42, Accessed 16 July, 2020 Available: www.jstor.org/stable/resrep22837.6

[39] V. Sergienko Alexander. "Quantum communications and cryptography." CRC press, 2018.

[40] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, E. Karimi. "Quantum cryptography with twisted photons through an outdoor underwater channel," Opt. Express 26, 2018, 22563-22573.

[41] Qi Bing, Qian Li, Lo Hoi-Kwong. "A brief introduction of quantum cryptography for engineers," Book Chapter, Publisher: arXiv 2010.

[42] M. Lucamarini, Z. L. Yuan, J. F. Dynes. "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters." *Nature* 557, (2018) 400–403. Accessed on: July. 13, 2020. [Online]. Available: https://doi.org/10.1038/s41586-018-0066-6

[43] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes. A. Murakami, M. Kujiraoka. "10-Mb/s quantum key distribution." Journal of Lightwave Technology. 2018 Aug 15;36(16):3427-33.

[44] K. Azuma, K. Tamaki, W.J. Munro. "All-photonic intercity quantum key distribution." Nature communications. 2015 Dec 16;6(1):1-6.

[45] "Quantum cryptography and the future of security," Oct. 8, 2018, Accessed on: May. 13, 2019. [Online]. Available: https://www.wired.co.uk/article/quantum-cryptography-and-the-future-of-security

[46] Z. Bernard. "*A First Introduction to Quantum Computing and Information*." Springer International Publishing, 2018.

[47] J. BARCAN. "Quantum code cracking creeps closer." IEEE SPECTRUM (2000).

[48] P. Gokhale. "How does Shor's algorithm work in layman's terms?" Nov. 16, 2015, Accessed on: May. 13, 2019. [Online]. Available: https://www.quora.com/How-does-Shors-algorithm-work-in-laymans-terms

[49] D. Krambeck, "Fundamentals of Quantum Computing" Aug. 06, 2015, Accessed on: May. 13, 2019. [Online]. Available: https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing/

[50] T. Monz, D. Nigg, E.A. Martinez, M.F. Brandl, P. Schindler, R. Rines, S.X. Wang, I.L. Chuang, and R. Blatt. "Realization of a scalable Shor algorithm." *Science*, 2016, *351*(6277), pp.1068-1070.

[51] R.P. Feynman. "Simulating physics with computers." Int J Theor Phys 21, 1982, 467–488. Accessed on: Aug. 19, 2019. [Online]. Available: https://doi.org/10.1007/BF02650179

[52] "The Best Applications for Quantum Computing," Accessed on: May. 13, 2019. [Online]. Available: https://quantumcomputingreport.com/the-best-applications-for-quantum-computing/

[53] Lester Houston III. "Secure Ballots Using Quantum Cryptography," *Dec. 2, 2007*, Accessed on: May. 13, 2019. [Online]. Available at: https://www.cse.wustl.edu/~jain/cse571-07/ftp/ballots/index.html