Improving communication security Against Quantum Algorithms Impact

Hicham Amellal *
LabSIV, Department of Computer Science
Faculty of Sciences Agadir, Ibnou Zohr University
Agadir, Morocco.

Abstract

In this paper, we explore the impact of quantum algorithms on classical network security. Our analysis focuses on Shor's algorithm, which excels in factorizing large prime numbers, presenting a significant threat to classical cryptographic protocols. We conduct an in-depth analysis of Shor's algorithm's potential effects on HTTPS to highlight its disruptive capabilities. Moreover, to fortify classical cryptographic protocols against quantum threats, we introduce a novel Quantum Intrusion Prevention System (QIPS) scheme. Leveraging basic components like beam splitters and detectors, this solution serves as a dedicated hardware interface between the classical network and external quantum networks. Our proposed QIPS scheme offers enhanced resilience to classical cryptographic protocols, mitigating the vulnerabilities posed by quantum algorithms and reinforcing network security in the face of evolving threats.

Key Words:Quantum algorithms, Network security, Quantum IPS, HTTPS, RSA, Shor's algorithm.

1 Introduction

Quantum information, which relies on certain phenomena of quantum mechanics, is considered one of the most powerful solutions proposed for information processing in recent years, at least theoretically. Unlike classical computing, which utilizes bits to represent information as either 0 or 1, quantum computing operates on quantum bits or qubits, which have the ability to exist in superposition states. This means that a qubit can represent both 0 and 1 simultaneously, enabling quantum computers to perform certain computations exponentially faster than classical computers [1, 2]. Quantum computing has the potential to revolutionize a wide range of industries, including finance, logistics, drug discovery, and materials science. This is due to the different algorithms that can reduce the time required to solve complex mathematical problems.

One of the most important fields in information security is classical cryptography, which is a type of encryption that is based on the complexity of mathematical calculations. In classical cryptography, plaintext is transformed into ciphertext using a cryptographic algorithm and a secret key. The goal of encryption is to make it difficult for unauthorized parties to read the plaintext without the secret key. Classical cryptography algorithms include symmetric key algorithms, such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES), and asymmetric key algorithms, such as the Rivest-Shamir-Adleman (RSA) algorithm. These algorithms rely on the computational complexity of mathematical problems, such as factoring large numbers or solving the discrete logarithm problem, to provide security.

However, with advances in computing power and new cryptographic attacks, many classical cryptography algorithms are no longer considered secure. The emergence of this threads has spurred the creation of innovative cryptographic algorithms and protocols that are designed to be resistant to attacks by quantum attacks strategies, which are expected to be able to break many classical cryptographic algorithms.

The paper is structured as follows: Section 2 provides an introduction to Shor's algorithm. Section 3 discus some classical protocols based on cryptography. Section 4 introduces the proposal quantum intrusion prevention system schema (QIPS). Section 5 analyzes the performance of the proposed "QIPS", followed by the conclusion in the final section of the paper.

2 Exploring Shor's Algorithm

The algorithm was developed by mathematician Peter Shor in 1994. He demonstrated that a quantum computer could efficiently factor large integers exponentially faster than any known classical algorithm [3]. The algorithm works by exploiting the properties of quantum mechanics, such as superposition and entanglement, to perform the factorization of an integer into its prime factors. Specifically, the algorithm utilizes a quantum Fourier transform in conjunction with a subroutine designed for efficient identification of the periodicity, allowing for the swift determination of the factors of an integer.

The algorithm's performance is measured by its asymptotic running time, which is polynomial in the size of the input,

*LabSIV, Department of Computer Science, Faculty of Sciences Agadir. Email: hi.amellal@uiz.ac.ma

whereas the best known classical algorithms for factoring are exponential in the size of the input. This means that for sufficiently large integers, Shor's algorithm can factor them in a reasonable amount of time on a quantum computer, while classical algorithms become infeasible. Shor's algorithm has important implications for cryptography, as many modern cryptographic protocols rely on the assumption that factoring large integers is computationally infeasible for classical computers. However, the development of a large-scale, error-corrected quantum computer capable of running Shor's algorithm remains a significant challenge.

We can summarize the key steps used by Shor's algorithm as follows:

- Quantum Fourier transform: The first step of Shor's algorithm is to apply a quantum Fourier transform to a superposition of possible solutions to the factoring problem. This transform effectively measures the frequency of the period of the integer being factored.
- Period-finding subroutine: The next step is to use a period-finding subroutine to determine the period of the function that maps a value to its modular exponentiation with the number to be factored. This step is critical for the success of the algorithm, as it allows us to find the factors of the number being factored.
- Continued fractions: Once the period of the function has been found, it can be used to construct a continued fraction approximation of the ratio of the two factors of the number being factored.
- Finally, the greatest common divisor of the original number and the factors obtained from the continued fraction approximation is computed to obtain the prime factors of the number.

Therfore, the algorithm consists of 2 parts:

- The classical segment of this algorithm is employed to transform the task of integer factorization into the quest for determining the period of a specific function. This period can be efficiently computed using a classical computer.
  In the first stage of Shor's algorithm, a number a is randomly selected from the interval between 1 and $N-1$, ensuring that it is relatively prime to N. It then computes the period r of the function $f(x) = a^x \bmod N$. The period r can be found efficiently using the quantum part of Shor's algorithm. Once the period r is known, Shor's algorithm uses classical methods to compute the factors of N. Specifically, if r is even and $a^{(\frac{r}{2})}$ is not equal to $-1 \bmod N$, Subsequently, the factors of N can be derived as: $gcd(a^{\frac{r}{2}}+1, N)$ and $gcd(a^{\frac{r}{2}}-1, N)$. If r is odd or $a^{\frac{r}{2}}$ is equal to $-1 \bmod N$, then a new random number a must be selected and the process repeated.
- Quantum part used to find the period using the Quantum Fourier Transform (QFT).
  The quantum part of Shor's algorithm is used to efficiently find the period r of the function $f(x) = a^x \bmod N$, where a is a randomly chosen integer between 1 and $N-1$, and N is the number to be factored. The quantum part of the algorithm utilizes a quantum computer and the utilization of the "QFT" enables the algorithm to effectively ascertain the period denoted as "r" of the function f(x) with remarkable efficiency. The "QFT" is a quantum analogue of the classical Fourier Transform, which is a mathematical tool used to analyze signals and identify their frequencies. To use the QFT in Shor's algorithm, we first initialize two quantum registers: one to store the input values of the function f(x), and the other to store the output values of the QFT. The input register is prepared in a uniform superposition of all possible input values, and the output register is initialized to a state of all zeros. Afterwards, a sequence of quantum gates, including the modular exponentiation gate, is applied to accomplish the intended task., to the input register to create a superposition of all possible values of f(x). Next, we apply the QFT to the input register to transform this superposition into a superposition of all possible periods r. Finally, we measure the output register to obtain a period r with high probability. If the measured period is even and $a^{\frac{r}{2}}$ is not equal to $-1 \bmod N$, then we can use the classical part of the algorithm to obtain the factors of N.

Overall, the classical part of Shor's algorithm is essential in obtaining the final factorization of the composite number N, but the quantum part is crucial in finding the period r efficiently. In addition, the quantum part of Shor's algorithm is crucial in efficiently finding the period r using the QFT, which is exponentially faster than classical methods.

Utilizing Shor's Algorithm in Practical Applications

Suppose we want to factor the number $N = 35$, which is the product of two prime numbers 7 and 5.

- In the first step we choose a arbitrary number a among 1 and $N-1$. Let's choose $a = 3$.
- In the second step we use the quantum part of Shor's algorithm to find the period r of the function $f(x) = a^x \bmod N$. This is done by applying the Quantum Fourier Transform (QFT) to a superposition of states $|\alpha\rangle$, where x ranges from 0 to $N-1$, and measuring the result. The probability of measuring a state corresponding to a period r is given by:
  $$QFT \ \frac{1}{N}\sum x = 0^{N-1} |a^x \bmod N\rangle \ ^2.$$
  In this case, we get the result $r = 4$ with high probability (around 50%for $N = 35$).
- Check if r is even and if $a^{\frac{r}{2}}+1$ and $a^{\frac{r}{2}}-1$ are not multiples of N. If they are not multiples of N, we can find the prime factors of N as $gcd(a^{\frac{r}{2}}+1, N)$ and $gcd(a^{\frac{r}{2}}-1, N)$.
  In this case, we have $a^{\frac{r}{2}}+1 = 3^2+1 = 10$ and $a^{\frac{r}{2}} = 3^2 - 1 = 8$, which have common factors with $N = 35$. Therefore, we need to try again with a different value of a until we get

a period r such that $a^{\frac{r}{2}}+1$ and $a^{\frac{r}{2}}+1$ are not multiples of N.

- Repeat steps 1-3 until we find the prime factors of N. In practice, this can take many iterations and may require a large number of qubits and quantum gates.

In practice, using Shor's algorithm to factor large numbers on a quantum computer requires a large number of qubits and quantum gates, which are not yet available on current quantum computers. Therefore, factoring a number like $p = 15592110483128760 63$ using Shor's algorithm is not yet possible with current technology. Note that Shor's algorithm is only efficient for factoring large numbers on a quantum computer. For small numbers, classical algorithms are faster and more efficient.

3 Cryptographic Algorithm-Based Security Protocols

There are several web protocols related for secure the communication on the internet, and it is used by millions of websites worldwide to protect their users data. The most well-known and widely used ones is SSL (Secure Sockets Layer), TLS (Transport Layer Security), HTTPS (Hypertext Transfer Protocol Secure), , DNSSEC (Domain Name System Security Extensions) and SSH (Secure Shell). hese protocols are essential for protecting user's data and ensuring the security of web applications and services.

3.1 The Working Principle of Secure Sockets Layer (SSL)

SSL (Secure Sockets Layer) is a protocol that provides secure communication between two parties over the internet. It is used to establish an encrypted connection between a web server and a client (such as a web browser) to ensure that any data transmitted over the connection is protected and cannot be read by anyone who intercepts it [4]. The principle of work of SSL involves a series of steps that occur during the establishment of the encrypted connection:

- The client sends a request to the server to initiate an SSL connection.
- The server responds by sending a digital certificate to the client, which contains the server's public key and other information
- The client checks the certificate to ensure that it is valid and issued by a trusted authority.
- If the certificate is valid, the client generates a random symmetric key and encrypts it with the server's public key. This key is used to encrypt and decrypt data during the SSL session.
- The client sends the encrypted symmetric key to the server.
- The server decrypts the symmetric key using its private key.
- The server sends a message to the client, indicating that the SSL session has been established and encrypted communication can begin.
- The client and server can now exchange encrypted data over the SSL connection.

During the SSL session, all data transmitted between the client and server is encrypted using the symmetric key that was exchanged during the initial SSL handshake. This ensures that any data intercepted by an attacker is unreadable without the symmetric key.

Overall, the principle of work of SSL involves the exchange of digital certificates and symmetric keys to establish an encrypted connection between a client and server, ensuring secure communication over the internet (see Figure.1).

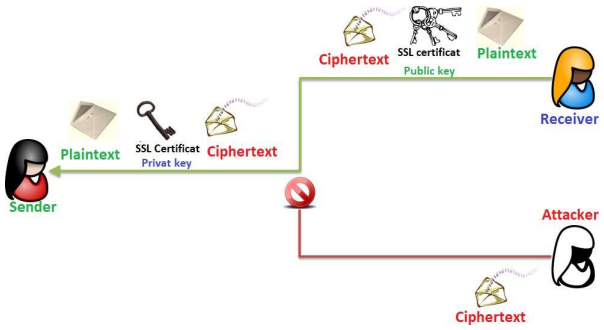

Figure 1: Principle of work of SSL

3.2 The Mechanism Behind the HTTPS Protocol

HTTPS is the secure version of HTTP, the protocol used for transferring data between a web browser and a website. It uses encryption to protect the data being transmitted, making it more difficult for attackers to intercept and steal sensitive information such as passwords, credit card numbers, and personal data. HTTPS uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to establish an encrypted connection between the web server and the client (the web browser). The encryption ensures that any data transmitted over the connection is protected and cannot be read by anyone who intercepts it. In summary, HTTPS is a vital web protocol for secure communication on the internet, and it is used by millions of websites to protect their user's data [5].

3.2.1 Cryptographic Algorithms Employed by HTTPS

HTTPS is a protocol that uses a combination of different cryptographic algorithms to provide secure communication over the internet. The main cryptographic algorithms used in HTTPS are:

- Symmetric-key encryption: HTTPS uses symmetric-key encryption to encrypt the data being transmitted between the client and server. The most commonly used symmetric-key encryption algorithms in HTTPS are AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard)

- Public-key encryption: HTTPS uses public-key encryption to establish a secure connection between the client and server. This is done through the use of digital certificates, which contain a public key that is used to encrypt data and a private key that is used to decrypt data. The most commonly used public-key encryption algorithm in HTTPS is RSA (Rivest-Shamir-Adleman).
- Hash functions: HTTPS uses hash functions to ensure data integrity and authenticity. Hash functions generate a unique digital fingerprint, or hash, of the data being transmitted, which is used to ensure that the data has not been tampered with or altered during transmission. The most commonly used hash functions in HTTPS are SHA (Secure Hash Algorithm) and MD5 (Message Digest 5).

Overall, HTTPS uses a combination of symmetric-key encryption, public-key encryption, and hash functions to provide secure communication over the internet, ensuring that data transmitted between the client and server is protected and cannot be read or altered by anyone who intercepts it. In this paper, we focus on the public-key encryption step, which is based on the RSA algorithm as mentioned below.

3.2.2 The Operational Principle of RSA Encryption

RSA (Rivest-Shamir-Adleman) stands as a renowned public-key encryption algorithm that plays a vital role in ensuring secure data transmission across the internet. Its inception dates back to 1977 when it was jointly developed by Ron Rivest, Adi Shamir, and Leonard Adleman. Even today, RSA remains one of the most widely utilized encryption algorithms. This cryptographic scheme relies on the principles of modular arithmetic and the challenge of factoring large composite numbers. By leveraging two large prime numbers, RSA generates a public key and a private key. The public key serves the purpose of encrypting data, while the private key is employed for decrypting the data.[6].
The process of generating a public key and a private key in RSA is as follows:

- Choose two large prime numbers, p and q.
- Calculate $n = p \times q$
- Calculate $\varphi(n) = (p-1) \times (q-1)$.
- Choose an integer e such that $1 < e < \varphi(n)$ and e is coprime with $\varphi(n)$. e is the public key exponent.
- Calculate d such that $d \times e \equiv 1 \pmod{\varphi(n)}$. d is the private key exponent.

The public key is then (n, e), and the private key is (n, d).

To encrypt a message using RSA, the sender uses the recipient's public key to encrypt the message. The encryption process involves converting the message into a numerical value, raising it to the power of the recipient's public key, and then taking the result mod n. The resulting number is the encrypted message.

To decrypt the encrypted message, the recipient uses their private key to perform the reverse calculation. They raise the encrypted message to the power of their private key and then take the result mod$n$. The resulting number is the original message.

The security of RSA is based on the fact that it is computationally infeasible to factor large composite numbers into their prime factors. The public key in RSA consists of two large prime numbers, and it is difficult to determine these prime numbers from the public key alone. This makes it difficult for an attacker to decrypt the encrypted message without the private key. Overall, RSA provides a secure way to encrypt and decrypt data, making it an important tool for secure data transmission over the internet(see Figure.2).

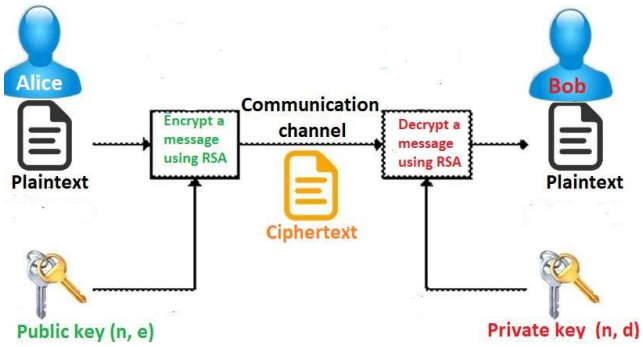

Figure 2: Principle of work of RSA algorithms

3.3 Security Analysis of HTTPS in Light of Shor's Algorithm

In section 3.2, we discussed that the security of HTTPS based on different cryptographic algorithms. Also, we mentioned that RSA is a widely used algorithm in HTTPS for public key generation, and any vulnerabilities or attacks that can compromise RSA could potentially weaken the security of HTTPS.

RSA is founded on the computational complexity of factoring large composite numbers into their prime factors. Shor's algorithm is a quantum algorithm that can efficiently factor large numbers, which could potentially break the security of RSA.

In the context of security analysis of RSA against Shor's algorithm, there are two main aspects to consider: the vulnerability of RSA to Shor's algorithm and the impact of this vulnerability on the security of systems that use RSA.

On the first aspect, it has been shown that Shor's algorithm can efficiently factor large numbers using a quantum computer, which means that RSA could be vulnerable to quantum attacks[7, 8, 9, 10]. However, it is important to note that building a large-scale quantum computer capable of running Shor's algorithm is still a challenging task, and there are still many technical and practical limitations that need to be overcome. On the second aspect, the impact of RSA's vulnerability to Shor's algorithm on the security of systems that use RSA depends on

various factors, such as the size of the key used in RSA, the sensitivity of the information being protected, and the available resources of the attacker. Theoretically, the RSA algorithm is vulnerable to attacks using Shor's algorithm. This means that if a large enough quantum computer were built, it could be used to break RSA encryption.

To secure RSA against attacks using Shor's algorithm, several post-quantum cryptographic schemes have been proposed. These schemes use mathematical problems that are believed to be hard for quantum computers to solve, such as the learning with errors (LWE) problem and the code-based McEliece cryptosystem. There are also efforts underway to develop quantum-resistant versions of RSA itself, which would involve modifying the RSA algorithm to make it resistant to attacks using quantum computers. However, this is still an area of active research, and it remains to be seen whether quantum-resistant versions of RSA can be developed that are as efficient and practical as the current version.

In the context of enhancing the security level of RSA against quantum attacks, we propose in this paper a quantum IPS that may help to secure RSA.

4 Description of the proposed quantum intrusion prevention system (QIPS)

In order to perform a quantum attack on a cryptographic system like RSA, a quantum computer alone is not enough. The attacker also needs to establish a secure communication channel with the target system using a quantum communication protocol, such as the BB84 protocol, in order to exchange information securely.

In a quantum communication system, information is encoded in quantum states, such as the polarization of photons [11]. These quantum states are then transmitted over a physical channel, such as an optical fiber, and measured at the receiving end. By using the principles of quantum mechanics, it's possible to detect any attempts to intercept or eavesdrop on the communication, as any observation of a quantum state changes its state.

Therefore, using a secure quantum communication protocol like BB84 can help to ensure the security of the communication channel, which is essential for performing a quantum attack on a cryptographic system like RSA.

4.1 Reviewing the Quantum Key Distribution Protocol: BB84

The BB84 protocol, formulated by Charles Bennett and Gilles Brassard in 1984, is considered as the most known quantum key distribution (QKD) protocol[12, 13]. The protocol is designed to allow two parties, traditionally named Alice and Bob, to establish a secure shared secret key over an insecure communication channel.

The protocol uses the properties of quantum mechanics to ensure the security of the key distribution process[14, 15]. The sender and the receiver both have access to a source of single photons that can be in one of four possible states, represented by two non-orthogonal bases. The sender randomly chooses one of the two bases to encode each photon, and sends the resulting sequence of photons to the receiver over the insecure communication channel. The receiver also randomly chooses one of the two bases to measure each photon upon reception.

Due to the non-orthogonality of the bases, the receiver's measurements are not always guaranteed to be correct. However, if the sender and the receiver choose their bases independently and at random for each photon, they can identify the presence of a malicious interceptor, traditionally named Eve, by comparing a subset of their measurement results. If the attacker has intercepted any of the photons to measure them, her presence will cause errors in the receiver's measurements, which the sender and the receiver can detect by comparing a subset of their results. They can then discard the corresponding key bits and establish a shorter, secure shared key from the remaining bits.

The BB84 protocol provides information-theoretic security, meaning that it is secure against any amount of computational power that the attacker may have. The protocol has been implemented experimentally and is widely considered to be a significant milestone in the field of quantum cryptography

- The sender transmits a sequence of random bits to the receiver by choosing either the "Horizontal/Vertical" or "Diagonal/Antidiagonal" bases to encode each bit
- The receiver randomly selects either the "Horizontal/Vertical" or "Diagonal/Antidiagonal"' basis to measure the states received from the sender,
- After transmitting the quantum states, the sender and the receiver communicate classically to exchange the bases they used for encoding and measuring the states. They then discard any bits in their shared key for which they used different bases during transmission.
- To improve the security of the shared key, the sender and the receiver publicly communicate a subset of the remaining bits.

The BB84 protocol utilizes single qubits to transmit key bits from the sender to the receiver. Each qubit is encoded in one of two orthonormal bases, which are conjugate to each other. When the sender uses the H/V bases, the signal states take on the following form:

$$\begin{aligned} |Horizontal\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle) \\ |Vertical\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle - |1_Z\rangle). \end{aligned} \quad (1)$$

When the sender utilizes the "Diagonal/Antidiagonal" bases, The signal states exhibit a varied form:

$$\begin{aligned} |Diagonal\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle + i|1_Z\rangle) \\ |Antidiagonal\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle - i|1_Z\rangle). \end{aligned} \quad (2)$$

4.2 Description of Unambiguous state discrimination (USD)

The subject of "USD" (Unambiguous State Discrimination) exhibits a strong connection to both QKD protocols and entanglement swapping protocols. It proves particularly useful in the realm of quantum communication, specifically when two signal states, which have yet to be implemented in solid-state systems, become non-orthogonal after traversing a channel. In the domain of quantum state discrimination, the primary goal is to design a measurement technique that effectively distinguishes a specified set of states. While the minimum-error measurement, known as the Helstrom measurement, is employed to differentiate between two equiprobable non-orthogonal states through a projective measurement, the optimal USD (Unambiguous State Discrimination) measurement is achieved through a generalized measurement known as the Ivanovic-Dieks-Peres (IDP) measurement. [16].

Suppose we have the simple example of comparing two coherent states that are different from each other: $|\alpha\rangle$ and $|\varphi\rangle$. A coherent state is a state for which $\hat{x}|\varphi\rangle = \varphi|\varphi\rangle$, where $\hat{x}$ is the annihilation operator. In this case, we have no knowledge of the phase or amplitude of $|\varphi\rangle$ and $|\lambda\rangle$, only that the states are coherent. To compare the two states, we can use a 50%/50% beam splitter, as shown in Figure.3.

$$\hat{x}_{result} = \frac{1}{\sqrt{2}}(\hat{x}_{initial} + \hat{y}_{initial}) \tag{3}$$

$$\hat{y}_{result} = \frac{1}{\sqrt{2}}(\hat{y}_{initial} - \hat{y}_{initial}) \tag{4}$$

After performing some calculations, we found that $|\alpha\rangle$ and $|\beta\rangle$ transforms in the following way:

$$|\varphi\rangle_{,}^{x\ initial} \otimes |\lambda\rangle_{,}^{y\ initial} \Longrightarrow \frac{\varphi+\lambda}{\sqrt{2}}_{x,result} \otimes \frac{\varphi-\lambda}{\sqrt{2}}_{y,result} \tag{5}$$

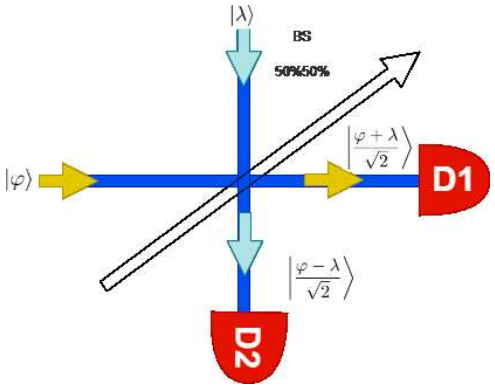

Figure 3: The beam splitter mixes the two input fields

- In the absence of dark counts in the detectors and when the values of φ and λ are equal, the result mode y will solely consist of vacuum. Accordingly, the presence of any signal detected in result y confirms the non-identity of the phase and amplitude of φ and λ.
- In the case when $P_{dark-counts} \neq 0$ in the detectors, we can no longer definitively confirm that $\varphi = \lambda$ in this scenario.
- The detector's efficiency against dark counts is not flawless, resulting in a decrease in its effectiveness and causing a probability of detecting a distinction between φ and λ that is less reliable.

The success probability to detect a variation between φ and λ is equal to the probability of detecting at one or more qubit in result mode y, where the coherent state $\frac{\varphi-\lambda}{\sqrt{2}}$ is present. Since the probability of detecting no qubits in this mode is given by: $p(0) = \exp\left(-\frac{1}{2}|\varphi-\lambda|^2\right)$, the success probability can be expressed as follows:

$$Probability_{-success} = P(0) = 1 - e^{-(1/2)|\varphi-\lambda|^2} \tag{6}$$

4.3 Designing the Quantum Intrusion Prevention System (QIPS)

In theory, the sender use one of the four possible states at random to transmit a key bit. The receiver measures the received qubit in both the "Horizontal/Vertical" and "Diagonal/Antidiagonal" bases, which are selected with equal probability. Subsequently, They establish key reconciliation by utilizing a classical channel and selectively preserving the key bits where matching bases were employed. The resultant key is then amplified. However, in practical implementation, the sender utilizes Dim-Laser pulses for transmitting the states via an optical fiber. In this investigation, we analyze the sender's origin states to prevent unauthorized signal propagation across the quantum channel. Furthermore, we express one of the four states by employing a photon mode pair, denoted by the annihilation operators a_R and a_S.

$$\begin{aligned}
|Horizontal\rangle &= e^{-|\varphi|^2} e^{\varphi\left(a_R^\dagger + a_S^\dagger\right)} |Vac\rangle_R \otimes |Vac\rangle_S = |\varphi\rangle_R \otimes |\varphi\rangle_S \\
|Vertical\rangle &= e^{-|\varphi|^2} e^{\varphi\left(a_R^\dagger - a_S^\dagger\right)} |Vac\rangle_R \otimes |Vac\rangle_S = |\varphi\rangle_R \otimes |-\varphi\rangle_S \\
|Diagonal\rangle &= e^{-|\varphi|^2} e^{\varphi\left(a_R^\dagger + i a_S^\dagger\right)} |Vac\rangle_R \otimes |Vac\rangle_S = |\varphi\rangle_R \otimes |i\varphi\rangle_S \\
|Antidiagonal\rangle &= e^{-|\varphi|^2} e^{\varphi\left(a_R^\dagger - i a_S^\dagger\right)} |Vac\rangle_R \otimes |Vac\rangle_S = |\varphi\rangle_R \otimes |-i\varphi\rangle_S
\end{aligned}$$

In this study, we focus on mode S, which is considered the "signal" pulse and used to encode the sender's information. We will examine a transmission scenario where a signal state $|\chi\rangle$ passes through our proposed device. When the incoming signal is received, certain detectors will click while others won't, depending on the state of the signal. In the following paragraph, we will describe various transmission scenarios and clarify how the quantum IPS either permits or blocks the input signal based on the detectors behavio (see Figure.4).

In the processing stage of the "QIPS" system, the original signal denoted as $|\chi\rangle$ is divided into 2 parts. The first part, $|\frac{\chi}{\sqrt{2}}\rangle$, undergoes analysis through the "QIPS", while the second part $|\frac{\chi}{\sqrt{2}}\rangle$, depending on the filtering rules, is either transmitted to detectors of received or rejected [17, 18]. During the processing stage, the initial portion is divided into four sub-fractions using beam splitters. The initial modes $|\frac{\chi}{2\sqrt{2}}\rangle$ are combined with

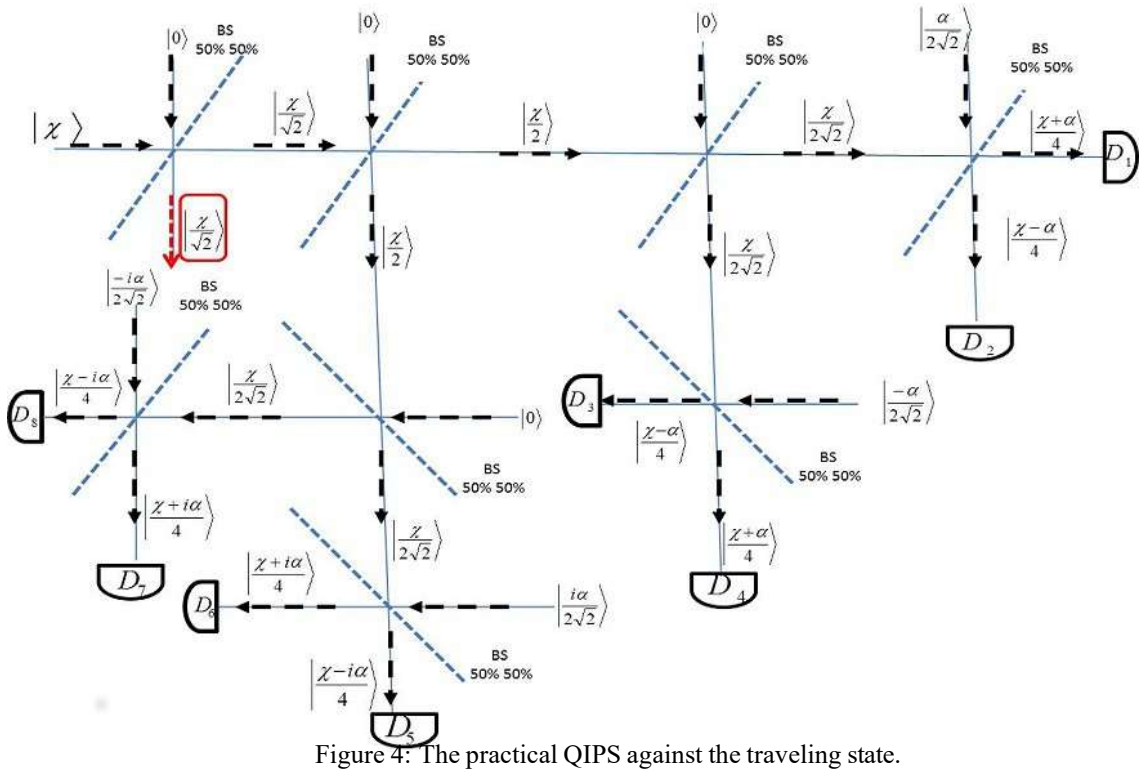

Figure 4: The practical QIPS against the traveling state.

special pulses such as $|_2\frac{\alpha}{2}\rangle$, $|-\frac{\alpha}{2\sqrt{2}}\rangle$, $|i_2\frac{\alpha}{2}\rangle$, and $|-i_2\frac{\alpha}{2}\rangle$ as the second beam-splitter input modes. The resulting output modes are $|\frac{\chi+\alpha}{4}\rangle$, $|\frac{\chi-\alpha}{4}\rangle$, $|\frac{\chi+i\alpha}{4}\rangle$, and $|\frac{\chi-i\alpha}{4}\rangle$, which are then directed to detectors D_i (where $i \in 1, 8$) to measure the incoming signal amplitude.

4.4 Description of the 'QIPS' device

In the processing stage of the "QIPS" system, the original signal denoted as $|\chi\rangle$ is divided into 2 parts. The first part, $|\frac{\chi}{2}\rangle$, undergoes analysis through the "QIPS", while the second part $|\frac{\chi}{2}\rangle$, depending on the filtering rules, is either transmitted to detectors of received or rejected [17, 18]. During the processing stage, the initial portion is divided into four sub-fractions using beam splitters. The initial modes $|\frac{\chi}{2\sqrt{2}}\rangle$ are combined with special pulses such as $|_2\frac{\alpha}{2}\rangle$, $|-\frac{\alpha}{2\sqrt{2}}\rangle$, $|i_2\frac{\alpha}{2}\rangle$, and $|-i_2\frac{\alpha}{2}\rangle$ as the second beam-splitter input modes. The resulting output modes are $|\frac{\chi+\alpha}{4}\rangle$, $|\frac{\chi-\alpha}{4}\rangle$, $|\frac{\chi+i\alpha}{4}\rangle$ and $|\frac{\chi-i\alpha}{4}\rangle$ which are then directed to detectors D_i (where $i \in 1, 8$) to measure the incoming signal amplitude. The detectors will either produce a click or not, depending on the output states. In this case, there are two possibilities:

- If certain detectors fail to click, it can be inferred that the input state originates from a legitimate sender, and as a result, the second part can be permitted to proceed through the receiver's measuring devices.
- In the event that all detectors click, it can be inferred that the input signal may have been intercepted by a spy. As a result, the second part of the split signal will be rejected. The receiver can quickly detect the presence of an eavesdropper using this method.

Suppose that the incoming signal to be analyzed using the proposed "QIPS" is $|\alpha\rangle$. In this case, only detectors 1, 4, 5, 6, 7, and 8 will click, while detectors 2 and 3 will remain silent, as shown in Figure.5. This clearly indicates the presence of an eavesdropper trying to intercept the transmission, enabling the receiver to detect their presence easily. We can summarize these simple rules in the following table:

5 Security analysis of the 'QIPS' system

In this section, we examine the impact of the proposed"QIPS" on various incoming signals. To simulate a real quantum communication scenario, we assume that the receiver cannot determine the source of the incoming signal (see Figure.5). This situation can be represented by three different scenarios:

- The first scenario involves the sender's signal source, which represents a typical communication between two legitimate correspondents. In this case, the sender transmits information using the four states mentioned earlier: $|\alpha\rangle$, $|-\alpha\rangle$, $|i\alpha\rangle$, and $|-i\alpha\rangle$.
- The second scenario involves the attacker's signal source in the context of a quantum attack. In this situation, the attacker creates pulses based on her measurements to send

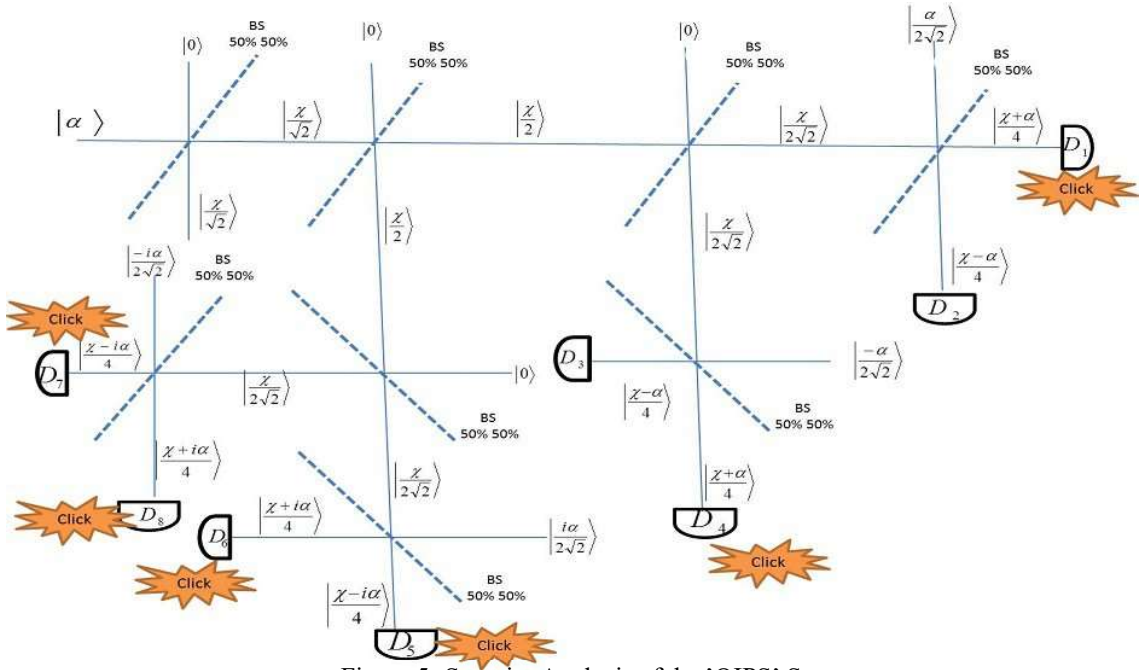

Figure 5: Security Analysis of the 'QIPS' System.

Table 1: Detector Responses Under Quantum IPS Operation.

Incoming signal	Detectors that will click	Quiet detectors	The source of the signal
$\|\alpha\rangle$	D_1, D_3, D_5, D_6, D_7, and D_8	D_2 and D_4	Legitimate sender
$\|-\alpha\rangle$	D_2, D_4, D_5, D_6, D_7, and D_8	D_1 and D_3	Legitimate sender
$\|i\alpha\rangle$	D_1, D_2, D_3, D_4, D_6, and D_8	D_5 and D_7	Legitimate sender
$\|-i\alpha\rangle$	D_1, D_2, D_3, D_4, D_5, and D_7	D_6 and D_8	Legitimate sender
$\|\beta\rangle / = \{\|\pm\alpha\rangle, \pm i\alpha\rangle\}$	all detectors	—	Illegitimate sender

to detectors of the receiver. As a result, the attacker can potentially select the same signal amplitude as sender's.

- The third scenario involves the attacker's source signal for blinding the receiver's detectors. To carry out the quantum attack, the attacker must blind the receiver's detectors by using a special signal. This involves shining continuous light into receiver's detectors and manipulating the pulse strength or amplitude to control when they click. The attacker can also use this technique to prevent the receiver's detectors from detecting the legitimate input signals.

Based on the aforementioned scenarios, we will now analyze the behavior of the proposed 'QIPS' incoming pulses. We will consider each case individually based on the source of signal, and observe:

- In the first scenario, the sender's will use one of the following states to create a confidential key with the receiver based on the BB84 protocol Π $|\pm\sqrt{2}\alpha\rangle, |\pm i\sqrt{2}\alpha\rangle$ (see Figure.6).

Once the sender has prepared the random key, he sends the bit value corresponding to her chosen bases. As the signal travels,

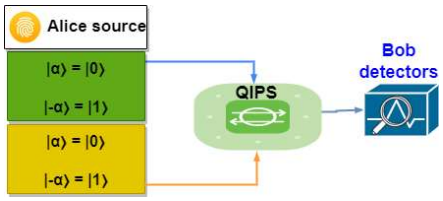

Figure 6: The normal use of the QIPS in a BB84 communication scheme.

it will be transformed by the "QIPS" process analysis (see Figure.7). From this analysis, we can conclude that the quantum state prepared by the sender passes the proposed 'QIPS' test and can then be measured in the receiver's devices according to the BB84 protocol.

In the first case, we consider the scenario in which the attacker attempts a quantum attack to obtain the secret key that the sender intends to share with the receiver. To carry out this attack, the attacker must first clone the architecture of both the sender and the receiver, as shown in the Figure.8:

In the second scenario, the attacker attempts to perform a

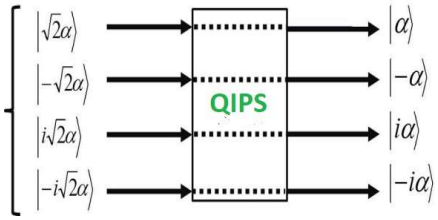

Figure 7: The evolution of the traveling qubits under the 'QIPS'.

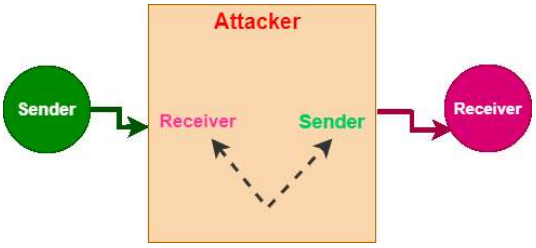

Figure 8: A simple scheme of quantum Attack.

quantum attack to obtain the secret key that the sender wants to share with the receiver. To achieve this, he clones the sender's and receiver's architecture and measures the intercepted states to prepare special pulses that will be sent to the receiver. The attacker may also clone the sender's states with the same amplitude, $|\pm\sqrt{2}\alpha\rangle, |\pm i\sqrt{2}\alpha\rangle$, in the first stage of the attack. In the next stage, she tries to blind the receiver's detectors using another light pulse, $|\beta\rangle$, that renders the blinded devices working in a linear mode. However, this state cannot bypass the proposed "QIPS" device and reach the target, as described earlier. Therefore, the receiver's attempt to blind the receiver's detectors will fail, and this attack will be ineffective in the presence of the proposed quantum device.

In the final scenario, we assume that the attacker prepares his states differently from sender's states. Analogously to the second case, it can be concluded that the attacker's states will also be blocked in the first attack stage before the blinding step, demonstrating the effectiveness of the proposed quantum IPS against such attacks.

From the results provided above, it is clear that the proposed Quantum IPS can distinguish between legitimate and illegitimate quantum signals. Additionally, we demonstrated that in order to use quantum computing to attack classical networks, a quantum network must be utilized first to initiate the attack. Therefore, if we can secure the quantum network against attack strategies based on quantum computing, we will also secure the classical network. As a simple implementation of the proposed "QIPS," we will deploy it between the classical and quantum networks, as depicted in the following figure (see Figure.9).

In the description of Shor's algorithm, we demonstrated that it consists of both classical and quantum steps to factorize a prime number. However, our analysis focuses on the quantum steps. The quantum part of Shor's algorithm begins by preparing

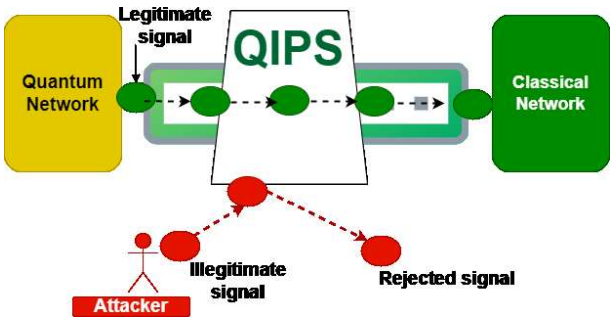

Figure 9: A Simple Scheme for Implementing Quantum Intrusion Prevention System (QIPS).

a quantum superposition of states using qubits. This is achieved by applying Hadamard gates to create a uniform superposition. The key quantum step in Shor's algorithm is the modular exponentiation, where repeated modular multiplications are performed using a controlled unitary operation to compute the values of a^x mod N. This step utilizes quantum gates. Following the modular exponentiation, a quantum Fourier transform is applied to the output qubits to measure the periodicity encoded in the quantum state. The final step involves measuring the quantum state, resulting in a superposition of possible period values.

It is evident that Shor's algorithm, based on quantum computing, is capable of factorizing prime numbers and compromising the security of classical algorithms like RSA. To address this, the use of the Quantum Intrusion Prevention System (QIPS) can effectively detect the utilization of Shor's algorithm and reject the corresponding signals, thereby enhancing the security of classical networks.

6 Conclusion

In this study, we introduced a Quantum Intrusion Prevention System (QIPS) employing a superposition of elementary devices such as detectors and beam-splitters. To perform a thorough security analysis, we present diverse scenarios involving different sender sources. The objective is to assess the capabilities and limitations of the proposed 'QIPS' under challenging conditions and in hostile environments.

We delved into the security aspects of our proposed system against quantum attacks. We showed how the eavesdropping pulses are rejected during transmission and are detected by the receiver. Furthermore, our proposed communication method using the "QIPS" outperforms the standard protocol, providing an ideal balance between secure transmission and the simplicity of the physical setup. In conclusion, we have proposed a practical quantum IPS scheme that can contribute to preserving confidentiality and reducing the risk of eavesdropping by quantum algorithms.

References

[1] P.A.M.Dirac, The Principles of Quantum Mechanics, 3rd ed.Oxford: Clarendon Press (1947).

[2] Kollmitzer.c, Pivk.M, Applied quantum cryptogtraphy, Lect.Not.Phys 797,ISBN 978-3-642-04829-6, Springer (2010).

[3] Peter W. Shor , SIAM J.Sci.Statist.Comput. 26,1480 (1997).

[4] Dierks, Tim and Eric Rescorla (2002). The TLS Protocol Version 1.1; IETF Internet-Draft.

[5] Mohamed G. Gouda, Elements of Network Protocol Design 1st Edition, Kindle Edition, 2008.

[6] Bleichenbacher, Daniel (1998). "Chosen ciphertext attacks against protocols based on RSA encryption standard PKCS#1." Advances in Cryptology—CRYPTO'98, Lecture Notes in Computer Science, vol. 1462, ed. H. Krawczyk. Springer-Verlag, Berlin.

[7] B.Qi, Fung.C.-H.F, Lo.H.-K and Ma.X, Time-shift attack in practical quantum cryptosystems. Quant.Inf.Comp. 7, 73,2 (2007).

[8] Lu¨N.tkenhaus, Security against individual attacks for realistic quantum key distribution. Phys.Rev.A 61, 052304 (2000).

[9] V.Scarani, A.Acin, G.Ribordy and N.Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys.Rev.Lett. 92, 057901 (2004).

[10] Y.Zhao, C.-H.FFung, B.Qi, C.Chen and H.-K.Lo, Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key- distribution systems. Phys. Rev. A 78, 042333 (2008).

[11] W.Y.Hwang, Quantum key distribution with high loss:Toward global secure communication. Phys.Rev.Lett. 91, 057901 (2003).

[12] C.H.Bennett, G.Brassard, In International Conference of Computers in Systems and Signal Processing, Bangalore, India (IEEE, New York 1984) 175 (1984).

[13] C.H.Bennett, G.Brassard and N.D.Mermin Phys. Rev. Lett. 68 (1992).

[14] A.Meslouhi, H.Amellal, Y.Hassouni, and A.El Allati, A Secure Quantum Communication via Deformed Tripartite Coherent States Journal of Russian Laser Research,35, pages369–382 (2014).

[15] P.W.Shor, and J.Preskill, simple proof of security of the BB84 quantum key distribution protocol. Phys.Rev.Lett 85, 441, 44 (2000).

[16] H.Amellal, A.Meslouhi, Y.Hassouni et M. El Baz. A quantum optical firewall based on simple quantum devices. Quantum Inf Process 14, 2617–2633 (2015).

[17] V.Makarov, Controlling passively quenched single photon detectors by bright light. New J. Phys. 11, 065003 (2009).

[18] V.Makarov, Anisimov.A and Skaar, J, Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys. Rev. A 74, 022313 (2006).