future internet

MDPI

Article

Estimating Interception Density in the BB84 Protocol: A Study with a Noisy Quantum Simulator

Francesco Fiorini, Michele Pagano *, Rosario Giuseppe Garroppo and Antonio Osele

Department of Information Engineering, University of Pisa, Via G. Caruso, 16, 56122 Pisa, Italy; francesco.fiorini@phd.unipi.it (F.F.); rosario.garroppo@unipi.it (R.G.G.); a.osele@studenti.unipi.it (A.O.)
* Correspondence: michele.pagano@unipi.it

Abstract: Quantum computers have the potential to break the public-key cryptosystems widely used in key exchange and digital signature applications. To address this issue, quantum key distribution (QKD) offers a robust countermeasure against quantum computer attacks. Among various QKD schemes, BB84 is the most widely used and studied. However, BB84 implementations are inherently imperfect, resulting in quantum bit error rates (QBERs) even in the absence of eavesdroppers. Distinguishing between QBERs caused by eavesdropping and QBERs due to channel imperfections is fundamentally infeasible. In this context, this paper proposes and examines a practical method for detecting eavesdropping via partial intercept-and-resend attacks in the BB84 protocol. A key feature of the proposed method is its consideration of quantum system noise. The efficacy of this method is assessed by employing the Quantum Solver library in conjunction with backend simulators inspired by real quantum machines that model quantum system noise. The simulation outcomes demonstrate the method's capacity to accurately estimate the eavesdropper's interception density in the presence of system noise. Moreover, the results indicate that the estimation accuracy of the eavesdropper's interception density in the presence of system noise is dependent on both the actual interception density value and the key length.

Keywords: BB94; quantum key distribution (QDK); partial intercept-and-resend; interception density; quantum bit error rates (QBER)

Citation: Fiorini, F.; Pagano, M.; Garroppo, R.G.; Osele, A. Estimating Interception Density in the BB84 Protocol: A Study with a Noisy Quantum Simulator. *Future Internet* **2024**, *16*, 275. https://doi.org/10.3390/fi16080275

Academic Editors: Gianluigi Ferrari and Carlo Blundo

Received: 6 June 2024
Revised: 17 July 2024
Accepted: 30 July 2024
Published: 2 August 2024

1. Introduction

Quantum computers could render legacy cryptographic methods obsolete with their ability to solve complex mathematical problems exponentially faster than classical computers [1]. To counter this emerging threat, quantum key distribution (QKD) has been developed, leveraging the principles of quantum mechanics to ensure unconditionally secure communication, irrespective of advancements in computational power. Basically, QKD works by encoding binary information into the physical state of a particle (photon), transmitting this encoded state through the quantum channel, and then decoding it at the receiving end. The encoded physical state, a quantum bit or qubit, forms the cornerstone of this technology.

The first practical demonstration of QKD over 30 cm of free space using polarization coding [2] increased the interest in this new technology. Since then, a plethora of theoretical and experimental studies have led to the commercial availability of prototype QKD products. Various quantum cryptography protocols have been developed, with some demonstrating key transmission over tens of kilometers through both optical fiber and free space [3,4].

Recently funded research projects, such as SECOQC, have indicated a model for the development and operation of a point-to-point QKD network architecture with advanced protocols [5]. Additionally, GÉANT, an organization that connects National Research and Education Networks (NRENs) throughout Europe and beyond, is exploring the integration

of QKD services into its network, as well as the necessary hardware and software solutions for maintaining and monitoring a QKD-secured network. The growing interest in practical applications of QKD protocols in recent years is also evidenced by the establishment of the European Quantum Communication Infrastructure (EuroQCI) project [6]. This infrastructure will consist of a terrestrial fiber-optic segment and a satellite network connecting strategic sites nationally and across borders to safeguard the privacy of sensitive and critical data for governmental institutions, their data centers, hospitals, and more.

In the context of smart grid infrastructure security, the work [7] utilizes QKD secret keys over the MQTT protocol to support distributed energy resource (DER) communication. The practical implementation was tested in a real utility environment at the Electric Power Board (EPB) in Chattanooga, Tennessee, between a data center and an electrical substation connected via optical fiber.

In another recent work [8], the application of QKD is discussed for communication channels in hydropower facilities. This implementation encrypts and decrypts command/control communications, mitigating security risks while integrating with existing control interfaces.

Moreover, Ref. [9] demonstrates the implementation of quantum-safe 100 Gbps IPsec VPN tunnels over 46 km of fiber between two data centers, achieving a secret key rate of 7.4 kbps.

Another promising application is presented in [10], which showcases and tests a real-time implementation of a submarine QKD system based on the BB84 protocol using an FPGA as a photon counting module.

QKD enables the secure sharing of a secret key between two parties, traditionally referred to as Alice and Bob, over a quantum channel. An eavesdropper, Eve, may attempt to intercept the communication during this process.

Several QKD protocols have been proposed, with the Brassard–Bennett 1984 (BB84) protocol being the first and most widely adopted [11]. Due to its prominence and practical applications, this study focuses on the four-state BB84 protocol as the foundational model for QKD. The robustness of the protocol and its widespread use make BB84 an ideal candidate for investigating the effectiveness and security of QKD in real-world scenarios.

This paper advocates for a deeper investigation into the detectability of eavesdroppers, a non-trivial and unique feature of QKD. Indeed, the accurate detection of an eavesdropper would allow for more efficient use of the expensive quantum resources involved in QKD, ultimately enhancing the overall security and effectiveness of key-sharing processes.

The intercept-and-resend attack is widely recognized as a strategy employed by eavesdroppers within the BB84 protocol [12]. The study of this approach has led to a practical eavesdropping method known as a partial intercept-and-resend attack [13,14], where the eavesdropper intercepts a qubit with probability p (also referred to as the interception rate or density) and leaves it untouched with probability $(1 - p)$. Such an attack represents one of the simplest individual attacks by an eavesdropper. For simplicity and clarity in analyzing eavesdropper detectability in the QKD protocol, this paper assumes the partial intercept-and-resend attack as the sole strategy employed by the eavesdropper.

Previous studies have calculated the quantum bit error rate (QBER) under the partial intercept-and-resend attack with rate p in the BB84 protocol as $p/4$ [15]. This calculation considers the error due to eavesdropping independently of the error introduced via quantum system noise. This paper extends the previous analysis by examining the QBER of the partial intercept-and-resend attack in the BB84 protocol as a function of errors generated via quantum system noise. Therefore, this comprehensive analysis, in conjunction with the simulation validation, aims to provide a more realistic understanding of QBER behavior by incorporating the imperfections inherent in practical QKD systems.

Paper Contributions

The main contributions of the paper can be summarized as follows.

- A definition and statistical performance analysis of an intrusion detection system for partial intercept-and-resend attacks to BB84 scheme, also considering quantum system noise.
- An investigation of the role of the interception rate and key lengths on the BB84 security performances, which reflects its possible future application as a QKD scheme.
- A simulative implementation that exploits an open-source library able to model the noise of real quantum computers. This feature allows the analysis of the obtained results using backend simulators inspired by real quantum machines.

To the best of the authors' knowledge, all of these combined aspects have not been studied.

2. Related Works

A lot of work has been proposed to analyze the QKD in general and BB84 in particular.

The general unconditional security of the BB84 protocol has been demonstrated under ideal noise-free implementations [16,17]. Only specific studies have considered particular device imperfections [18,19], but they have typically employed an information theory-like approach to allow the extraction of a secure key. Conversely, the goal of this work is not to evaluate the security of the BB84 protocol but to develop an intrusion detection method for the partial intercept-and-resend attack on this protocol.

The simulation of the BB84 protocol has also been performed in several studies, such as [20–23]. They demonstrate its working principles, along with its limitations and the effects of noise in a quantum system.

There has been significant research on eavesdropper detection in the context of intercept-and-resend attacks within QKD protocols. Bennett and Brassard initially assumed that a communication could be considered free from eavesdropping activity if the measured QBER were zero [11]. Elboukhari et al. calculated that, in the four-state BB84 QKD protocol, an eavesdropper would go undetected with a probability of $(3/4)^K$, where K represents the number of qubits used to compute QBER [24]. Subramaniam and Parakh extended this analysis to the limit case of infinite-state BB84 and quantum Diffie–Hellman protocols, determining that the probability of an eavesdropper remaining undetected is, at minimum, $(1/2)^K$ [25]. Zamani and Verma proposed a two-way QKD protocol and calculated the probability of undetected eavesdropping in relation to both K and the number of key exchanges [26]. However, a common assumption across these studies is the consideration of an ideal quantum system, wherein any QBER greater than zero is solely attributed to eavesdropping. This idealized perspective does not account for quantum system noise, which can also contribute to QBER.

A few works have investigated the possibility of developing an intrusion detection system for the BB84 scheme. Among these, the most similar to the approach presented in this paper are [12,27]. They present satisfactory results, often with high detection accuracy in their considered conditions. However, they do not examine some details, either the noisy simulation of a real quantum computer or the possibility for the eavesdropper to intercept only a fraction of the qubits being sent.

3. Background

The distribution of secret keys over insecure networks plays a pivotal role in guaranteeing secure communications. This problem was first addressed in 1976 by the celebrated Diffie–Hellman algorithm, which considered the challenge of secret key agreement by relying on the classically difficult discrete logarithm problem. Unfortunately, this problem can, nowadays, be easily solved using quantum computers by leveraging Shor's algorithm [15].

3.1. Quantum Computer and Qubits

A quantum computer employs quantum mechanical phenomena to enable the calculation of some problems exponentially faster than classical computers. The fundamental unit of such a computer is the qubit, which differs from a classical bit in that it exists in a su-

perposition of two basis states The state of superposition implies that, upon measurement, the qubit will invariably assume one of two possible values, either 0 or 1, according to a probability law that is dependent on the relative weights of these two states [28].

For the sake of simplicity, from here on in the paper, it is assumed that polarization encoding is used to represent classical bits (0 s and 1 s), hence employing the polarization states of photons. In this case, each qubit can exist in one of two bases: a $+$ ("rectilinear") basis, with orthogonal states $|\uparrow\rangle$ and $|\rightarrow\rangle$, and an X ("diagonal") basis, with orthogonal states $|\nearrow\rangle$ and $|\nwarrow\rangle$. An example of mapping between classical bits and qubits is $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\rightarrow\rangle$ for the $+$ basis or $|0\rangle = |\nearrow\rangle$ and $|1\rangle = |\nwarrow\rangle$ for the X basis, as summarized in Table 1.

Table 1. Example of mapping classical bits to quantum states.

Classical Bit	$+$ Basis	X Basis
0	$\|\uparrow\rangle$	$\|\nearrow\rangle$
1	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$

A quantum computer employs quantum logic gates to manipulate the states of qubits. Of particular interest are the Pauli-X gate, denoted as `X`, which functions in a manner analogous to a NOT gate, and the Hadamard gate, denoted as `H`, which induces a rotation that changes the basis, e.g., from $+$ to X, and vice versa, since its functional matrix is hermetian and unitary. Both gates operate on individual qubits, allowing for transitions between different states and bases as desired [29]. The quantum indeterminacy principle precludes the possibility of distinguishing between the four states with absolute reliability, as they are not all orthogonal to each other. Rather, they can only be distinguished in pairs. Indeed, once the basis has been set, the measurement is only possible between the orthogonal states.

If you tried to measure a qubit with the wrong basis (i.e., different from the one used for encoding), the resulting reading would be random, either 0 or 1, with equal probability $\frac{1}{2}$. Conversely, if the measurement was conducted with the same basis, the output would always be the original state (of course, in the absence of external noise sources). In brief, one fundamental property of quantum mechanics is that the act of measurement itself alters the state of the observed object. Related to this property is the no-cloning theorem, which states that an arbitrary quantum state cannot be duplicated perfectly [30]. In other words, this theorem implies that creating an independent and identical copy of an unknown qubit is impossible.

These two properties form the basis of QKD protocols, as they prevent an adversary, referred to as Eve, from intercepting a stream of qubits, modifying them, and forwarding them without being visible.

One reason why quantum computation is so important today is the discovery, by Peter Shor, of a uniform family of quantum networks that solve the factoring problem. Shor's factoring algorithm has demonstrated that the security of many public cryptographic systems is compromised once a quantum computer is available. On a quantum computer, Shor's algorithm is capable of factoring an integer, N, in polynomial time. This means that the time taken is polynomial in $logN$, which is significantly faster than the most efficient known classical algorithm [31]. Shor's algorithm has indicated the necessity of the development of new protocols that can withstand the mainstream implementation of quantum computers. One potential solution is the use of QKD protocols as a secure alternative to classical public-key distribution schemes.

3.2. Background on BB84

QKD protocols represent a method of secure communication that implements a cryptographic protocol involving quantum mechanical components. The first QKD protocol was presented in 1984 by Bennett and Brassard, from which the BB84 protocol name derives: [11]. This protocol is provably secure when assuming a perfect implementation and two conditions:

1. Information can only be gained at the expense of disturbing the signal. If the no-cloning theorem is valid, the act of measurement required to obtain information about the quantum state disturbs the original state, preventing exact replication.
2. The use, in parallel, of an authenticated public classical channel.

BB84 or other analogous protocols permit the continued utilization of established symmetric encryption algorithms, such as Advanced Encryption Standard (AES) [32], since they are not as significantly affected by the advent of quantum computers, as instead, it affects public key algorithms, including Diffie–Hellman [33].

BB84 Scheme

The BB84 algorithm begins with Alice randomly selecting a set of n bits. Considering the polarization encoding, for each bit, it is necessary to establish the basis and the quantum states, using for example the mapping shown in Table 1. In this manner, Alice obtains n qubits that are subsequently transmitted to Bob through the quantum channel. Before reaching Bob, the eavesdropper Eve may attempt to intercept the qubits, decode them, and then, according to the read value, forward new qubits to Bob. Due to the no-cloning theorem, Eve is unable to copy the qubits unless she takes a measurement that inevitably disturbs the original state of that qubit half of the time if she chooses the wrong basis. Consequently, the only option for Eve is to randomly select the basis, measure and decode the intercepted qubit, regenerate the new one using the selected basis, and then forward it to Bob. Similarly, Bob is unable to ascertain in advance the set of bases used by Alice to generate the qubits. Thus, Bob can randomly select the set of n bases to measure the received qubits and decode the related bits. After the decoding of the n bits, Bob publicly announces he has received Alice's signals. Alice responds by sharing, on the public classical channel, the set of n bases used in the previous transmission. At this point, this operation is safe because the shared bases refer to the previous signal. Similarly, Bob communicates to Alice over the public channel the n bases he has randomly selected to decode the signal. Both Alice and Bob now compare the received n bases with those they have used, and they discard the bits corresponding to mismatches. The remaining bits measured with the same bases are instead retained. Assuming that the number of such bits is k, Alice selects a certain fraction of them (in our subsequent simulation analysis, for reasons of simplicity, we will assume the first $k/2$ bits). She then discloses her selection to Bob over the public channel. Subsequently, both Alice and Bob publicly announce the values of the selected bits and verify whether a predetermined number of them are identical. If this verification fails, the issue may be attributed to Eve, random noise, or a combination of both. In such cases, the algorithm must be restarted. Otherwise, the algorithm concludes, and both parties can proceed to generate a secret shared key with the remaining bits, as detailed in [34].

It is worth mentioning that *information reconciliation* and *privacy amplification* techniques [2] can be employed to create the secret shared key. In a nutshell, these techniques address discrepancies between keys, which can result from eavesdroppers or noise. Since it is impossible to distinguish in advance between these types of errors, they are necessary to ensure final key security. Accordingly, if the number of discrepancies (in the compared bits) falls below a certain threshold, these techniques can be used to correct erroneous bits and subsequently reduce Eve's knowledge of the key to an arbitrarily small value. More detail follows:

- Information reconciliation is a process of error correction performed between Alice and Bob's keys to ensure that both keys are identical.
- Privacy amplification is a method used to reduce and effectively eliminate Eve's partial information about Alice and Bob's key.

4. BB84 Simulation Model

This section describes the implementation of the BB84 simulation model within QuantumSolver (QS) [35], with a specific focus on its *Crypto* module. QS is a toolset developed

in Qiskit [36] that enables the simulation of QKD protocols, such as BB84, using IBM simulators and real quantum computers.

Figure 1 shows a simplified overview of the program's internal operations.

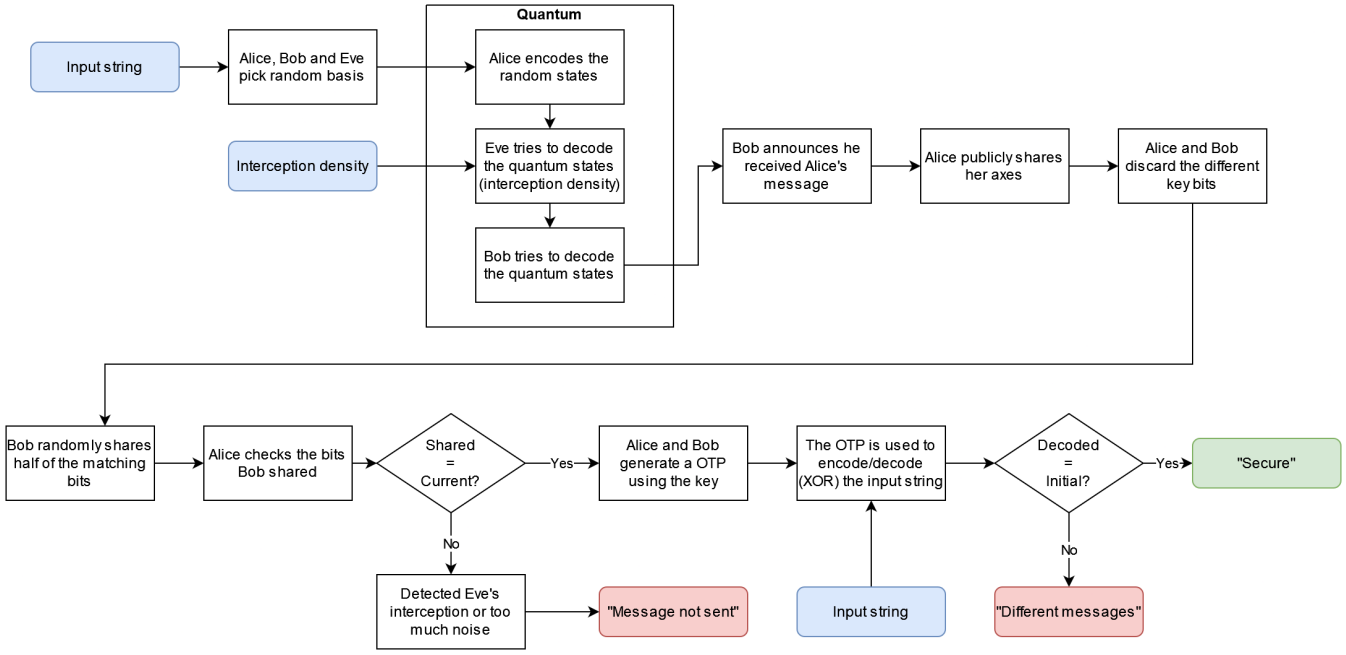

Figure 1. BB84 flowchart.

In more detail, the program flow can be divided into three distinct phases presented in the following subsections:

1. Key generation.
2. Key checking.
3. Validation.

4.1. Key Generation

The initial phase of the program, depicted in Figure 2, is responsible for generating the cryptographic key. When initiating the program, the available inputs that can be chosen include the following:

- Input string length: In our modified version of the simulator, this parameter exactly corresponds to n, the number of bits initially exchanged during the QKD process.
- Interception density: This refers to the percentage of qubits that Eve may intercept and forward to Bob. It quantifies Eve's ability to eavesdrop on the qubit transmission between Alice and Bob, hence influencing the overall security and effectiveness of the key distribution process.
- Backend: The IBM backend simulator to be used in receiving operations for decoding bits.

The program then initiates with Alice generating a binary array of length n, corresponding to the random transmission "axes" (i.e., bases). Additionally, she randomly generates the n bits to be exchanged with Bob to establish the secret key. For each bit, the associated quantum state is determined based on the corresponding random basis and the mapping strategy, as shown in Table 1 and as explained below.

The simulation of the qubit encryption process on quantum hardware begins by looping the number of times specified by the parameter n to encode each bit. Accordingly, if the qubit's state is 1, the `X` gate is applied. Otherwise, the qubit is skipped to the next step. Similarly, if the corresponding basis value is X (i.e., "diagonal"), the `H` gate is applied. Otherwise, no action is taken. Following this step, the qubit has been encrypted, and the

next one can begin the same encryption process. Once all the qubits from the Alice $n-$long array have been encrypted, they can be transmitted to Bob.

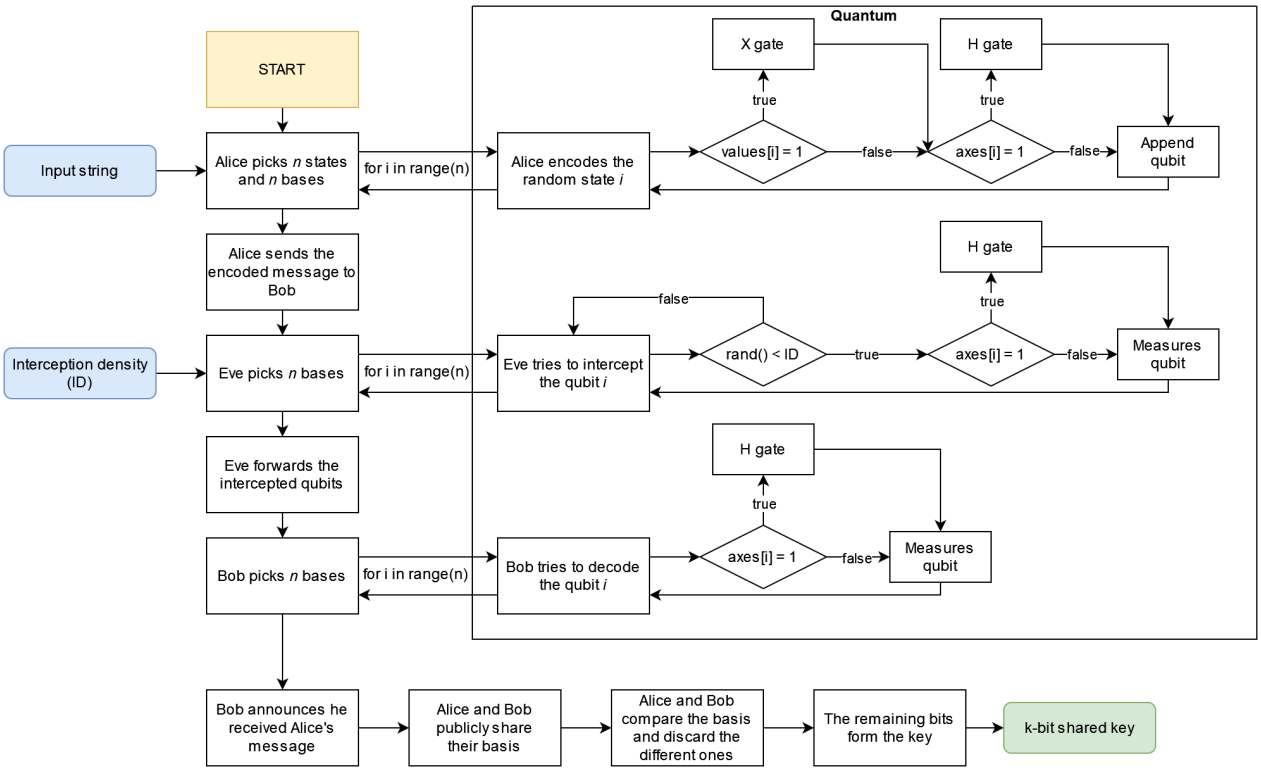

Figure 2. BB84 key generation.

Before reaching Bob, Eve may attempt to intercept the transmitted qubits. She is equipped with an array of n randomly generated bits, which serve as her basis values. As with Alice, she will loop n times and attempt to guess the received bit. More specifically, the program randomly generates a number between 0 and 1, and if it is smaller than the interception density chosen as input, then Eve is successful in intercepting the qubit. Subsequently, the qubit is eventually subjected to an `H` gate operation if the corresponding basis is the "diagonal" one, or otherwise, no other operation is performed. Now the process continues by effectively measuring the intercepted qubit (by performing the Qiskit `measure` operation) and by decoding the corresponding bit value through the readout operation of the backend simulator (selected at the start of the program). Once all the intercepted qubits have been processed, they are forwarded to Bob.

Bob's behavior is essentially identical to that of Eve, differing only in his interception density value, which is 1, since he intercepts all the qubits sent by Alice and Eve. Subsequently, Bob decodes the n received qubits by applying the same operations as Eve, based on the values of his random bases array. Upon completion, he publicly announces that Alice's message has been received.

Upon receipt of the message, both Bob and Alice can securely share their bases. By doing so, they can compare the bases and keep only the bit values in which the bases are the same. Such remaining k bits will be used to subsequently form the private key, which will be verified in the following step.

4.2. Key Checking

Figure 3 illustrates the flow chart of the key-checking procedure. This procedure determines whether Alice and Bob share a secure secret or whether it is necessary to restart the BB84 protocol due to Bob observing bit errors on the received key, which may be caused by Eve's interference and/or system noise. This is achieved by Bob publicly sharing the

first $m = k/2$ bits of the key with Alice. Subsequently, both parties compare these bits to ascertain any discrepancies. In such an event, the algorithm fails and necessitates a restart. Otherwise, if all the shared bits are identical, probably, the remaining, unshared bits will also be so. Subsequently, Alice and Bob discard the shared bits, as they have become public and cannot be utilized for the private key generation. The remaining bits then form the actual shared secret key, which can be used by both participants.

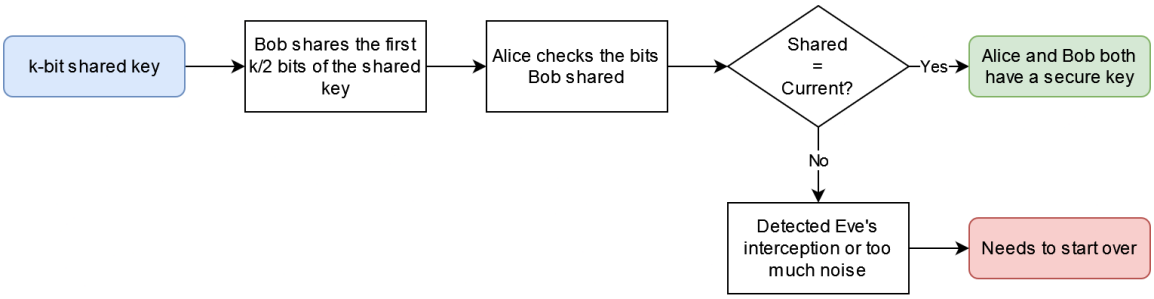

Figure 3. BB84 key checking.

It should be noted that QS does not perform information reconciliation and privacy amplification techniques because, firstly, they are not strictly part of the protocol and, secondly, the described implementation requires a perfect match (i.e., zero error rate) between the cases of Alice and Bob compared key bits, rendering these techniques less indispensable. In a real-world scenario, instead, both are typically employed, as commented upon in Section 3.2.

4.3. Validation

Finally, QS provides a potential subsequent step, namely a message exchange, as depicted in Figure 4. This is not a component of the BB84 algorithm; rather, it is a validation process to show that the generated key can be employed to transmit encrypted messages in a practical setting.

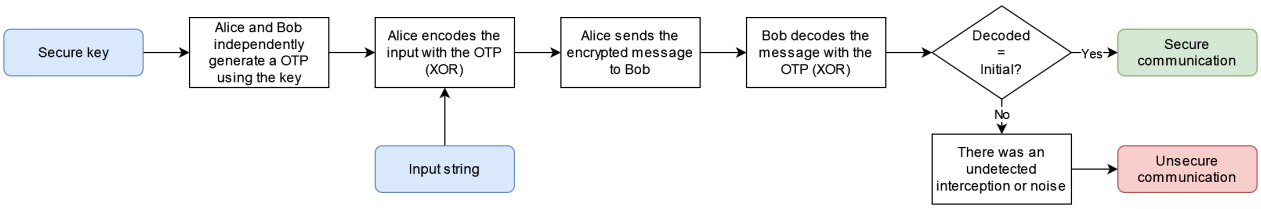

Figure 4. BB84 validation.

The newly created and verified shared secret key is used by both Alice and Bob to generate a One-Time Pad (OTP). Alice encodes the original input string by XOR-ing it with the OTP and sends the encrypted message to Bob. Bob XORs the message once more with his own OTP to obtain the decrypted message. The program then checks whether the message that Bob decrypted differs from the original that was sent by Alice. If Bob's resulting message differs from that originally sent by Alice, the cause may be the undetected interception of Eve or random noise. This step is feasible only in a testing-simulative scenario, as in the real world, Alice and Bob would have to publicly share the decrypted message to ascertain that they are equal.

5. Intrusion Detection Method

To define the intrusion detection method, it is necessary to analyze the details of some important aspects.

The first one is to evaluate the probability of detecting Eve, taking into account the conservative approach used with the QS in the checking phase. In particular, we recall that QS publicly shares half of the generated key to detect errors in the received bits caused by

Eve's action and/or system noise. In certain scenarios, this approach may be inefficient because each shared bit is subsequently discarded and cannot contribute to the final key. Furthermore, as the average probability of Bob correctly guessing Alice's basis is only 50%, the number of usable bits for the key will be reduced to around one-quarter of the initial number.

Table 2 summarizes the meaning of the symbols used in the remainder of the paper.

Table 2. Summary of the meanings of the symbols used.

Symbol	Meaning
EU	Event: Eve is undetected.
CB	Event: Bob selects the correct basis.
Sb	Event: Bob decodes the same bit transmitted by Alice.
p	Interception density.
n	Number of transmitted bits.
k	Number of key bits measured on the same basis between Alice and Bob.
m	Number of shared key bits publicly compared between Alice and Bob.
d	Number of erroneous bits detected at Bob's side in the shared key bits.
$\hat{QBER}$	Estimated QBER at Bob's side.
$QBER_{SN}$	QBER due to system noise.
$\hat{QBER}_{SN}$	Estimated QBER due to system noise.
$\hat{p}$	Estimated p.
MD	Event: missed Eve's detection.

5.1. Probability of Detecting Eve's Presence

Let us consider the situation in which it is known that Eve eavesdrops all qubits. When assuming the ideal scenario of a lack of system noise, the probability of each event can be easily determined, as follows.

- Case 1: Eve selects the same basis as Alice. The probability of this event is 0.5. In this case, the data are successfully exchanged between Alice and Bob, and Eve intercepts the bit without introducing any error.
- Case 2: Eve selects a basis that is different from Alice's. The probability of this event is 0.5. However, two different subcases can be defined, depending on whether Bob correctly receives the qubit transmitted by Alice or not. In the first subcase, Eve's interception is not detected, and Bob will successfully receive the bit sent by Alice. The second subcase considers the possibility that Bob fails to measure the qubit transmitted by Alice. This leads to an error in the qubit reception and, consequently, to the decoded bit. Both subcases have the same conditional probability, i.e., 0.5.

Considering all cases, the probability that Bob correctly receives the bit transmitted by Alice conditioned to the event that Eve intercepts all qubits is 0.75. This value is obtained by summing the probability of Case 1 (0.5) and the probability of Case 2 (0.5), multiplied by the corresponding conditional probability of the subcase 1 (0.5). In such an event, Alice and Bob are not aware of Eve's interception because Bob correctly decodes the qubit regenerated by Eve. However, Eve is present. This probability is, therefore, linked to the scenario where Eve remains undetected because Alice and Bob have no actionable information to detect Eve's presence.

This reasoning can be extended to determine the probability of Eve's non-detection when Alice and Bob use m bits for comparison. When assuming the statistical independence of Eve's interception process, the probability of the event EU (Eve's interception is undetected) is as follows:

$$\mathbb{P}\{EU\} = 0.75^m.$$

This equation demonstrates that the probability of detecting Eve's interception, equal to $1 - \mathbb{P}\{EU\}$, increases rapidly with the number of compared bits in the case where Eve intercepts all qubits. For instance, in the case of 15 bits, $\mathbb{P}\{EU\} = 0.013$ [36]. For longer keys, comparing half of the bits becomes unnecessary and merely wastes useful bits that could be retained for the final key. For this reason, there is a clear need for the development of a more effective approach for practical applications.

5.2. Model QBER vs. Eve's Interception Density

It is important to recall that the previous results are obtained with the assumption that Eve is present and intercepts all qubits. A general analysis instead should consider that the only information available is that Eve performs a partial intercept-and-resend attack. To analyze this scenario in detail, the two cases, with and without Eve's interception, must be considered separately.

5.2.1. Case 1: Without Eve's Interception

This analysis starts by considering the following example. Referring again to Table 1, we consider the case in which Alice encodes the bit 0 with the basis $+$, hence employing the $|\uparrow\rangle$ state. Indeed, we will carry out the subsequent statistical analysis by making such an assumption. Anyway, it is worth emphasizing that such a model does not preclude the generalization of the obtained results to the remaining cases, given the inherent symmetry of the problem (i.e., equiprobable random choice of bit values and bases). Moreover, throughout the remainder of this paper, quantum states will be explicitly represented only with their corresponding bit values, as each state is uniquely determined according to its associated bit once the basis has been defined. On Bob's side, the events and their associated probabilities are illustrated in Figure 5 and described as follows:

- Bob picks the correct basis, $+$, and hence, he always measures the correct state, 0, given the ideal communication channel.
- Bob picks the wrong basis, X, and then the measured state is random, 0 or 1, with each state having the same probability of 0.5.

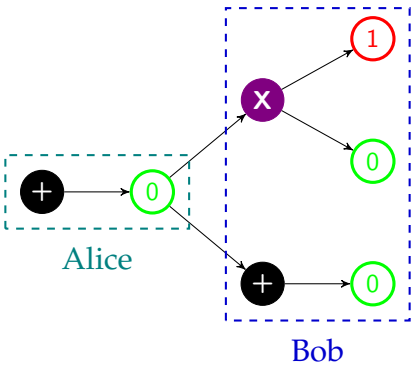

Figure 5. Case 1: without Eve.

The probability of the event "Bob selects the correct basis", shortly CB (i.e., the $+$ basis in Figure 5), can easily be determined:

$$\mathbb{P}\{CB\} = \frac{1}{2}. \tag{1}$$

With the assumption of an ideal communication channel and the properties of quantum mechanics, the probability of the event "Bob measures the same bit" of Alice, shortly Sb, conditioned to have selected the correct basis is $\mathbb{P}\{Sb|CB\} = 1$, as is evident from Figure 5. Therefore, in this scenario, if Bob chooses the correct basis (i.e., the same as Alice), he is sure about the correctness of the decoded bit.

Differently, the unconditioned probability of the event "Bob decodes the same bit transmitted by Alice" can be easily computed using the total probability theorem:

$$\mathbb{P}\{Sb\} = \mathbb{P}\{Sb|+\}\,\mathbb{P}(+) + \mathbb{P}\{Sb|X\}\,\mathbb{P}(X) = \mathbb{P}\{Sb|+\}, \tag{2}$$

since $\mathbb{P}(+) = \mathbb{P}(X) = 0.5$, and $\mathbb{P}\{Sb|+\} = \mathbb{P}\{Sb|X\}$ (for the symmetry of the formulation, as previously discussed). In the above Equation (2), the condition refers to the basis employed by Alice.

Applying the total probability theorem and also considering the assumption of the state (or bit, equivalently) transmitted by Alice, $\mathbb{P}\{Sb|+\}$ is given by the following:

$$\mathbb{P}\{Sb|+\} = \mathbb{P}\{Sb| + \bigcap 0\}\,\mathbb{P}\{0\} + \mathbb{P}\{Sb| + \bigcap 1\}\,\mathbb{P}\{1\} = \frac{3}{4}, \tag{3}$$

where $\mathbb{P}\{Sb| + \bigcap 0\} = \mathbb{P}\{Sb| + \bigcap 1\} = (\frac{1}{2} + \frac{1}{4})$, and $\mathbb{P}\{0\} = \mathbb{P}\{1\} = \frac{1}{2}$ (we recall that it is assumed that Alice encodes with equal random probability 0 or 1 bit values through qubits).

Again, the symmetry of the problem allows us to neglect the explicit computations for the other basis cases.

Therefore, Equation (3) shows that Bob measures the correct bit with a probability of 0.75. However, it is worth noting that the BB84 implementation discards the bits measured with the wrong basis, i.e., the edge X in the tree shown in Figure 5. Consequently, only around 50% of the received bits will be kept. Nevertheless, 100% of the set of measured bits with the correct bases will produce the transmitted bits without errors, as previously shown. The importance of this strategy is outlined by the successive discussion that describes the scenario where Eve's presence is assumed.

5.2.2. Case 2: With Eve

A more complex scenario occurs when Eve mimics Bob's behavior by attempting to intercept the bits transmitted by Alice. The discussion of this case considers an example similar to the previous case, i.e., Alice encodes the bit 0 with the basis $+$. The alternative events are illustrated in Figure 6 and described in the following.

- Eve picks the correct basis with a probability of 0.5, always measuring the bit 0. As illustrated in the lower edge of the tree shown in Figure 6, in this case, Bob is in the same situation as in the previous case; i.e., he receives a bit, "0", transmitted using the basis $+$ (i.e., state $|0\rangle$). Eve is transparent to Bob's reception performance. Therefore, Bob measures the bit "0" with a probability of 1 when the correct basis, $+$, is selected. Consequently, the global probability of measuring the bit "0" in this case is $\frac{1}{4}$. Another event that allows Bob to observe "0" is when he uses the wrong basis. In this case, the two alternative outputs, 0 and 1, can be observed with the same probability. Thus, the probability of observing 0 is obtained from the intersection of the following events: "Eve selects the correct basis", "Bob selects the wrong basis", and "on the wrong basis Bob measures 0". All of these events have the same probability, $\frac{1}{2}$. Thus, the probability of this global event is $\frac{1}{8}$.
- Eve picks the wrong basis with a probability of 0.5 and will equiprobabilly measure the two alternative bits, 0 and 1. From this point, Bob performs his measurement, which leads to two different scenarios:
  - Eve measured 0; Bob will measure 0 with a probability equal to 1 when picking the wrong basis (with respect to Alice and, hence, the same basis of Eve) and, randomly, 0 (with 50% probability) when picking the same basis as Alice. When taking into account the probability of Eve's choices, the global probabilities of the two events are $\frac{1}{8}$ and $\frac{1}{16}$, respectively.
  - If Eve measured 1, Bob will measure 1 with a probability equal to 1 when picking the wrong basis and, randomly, 0 (with, again, a 50% probability) when picking the same basis as Alice. In summary, Bob selects the correct state, 0, with probability $\frac{1}{16}$. This can be computed as the product of the probability of the following

events: "Eve picks the wrong basis", "Eve measures 1", "Eve picks the same basis as Alice", and "Bob measures 0". Indeed, all the above events are independent and have the same probability, $\frac{1}{2}$.

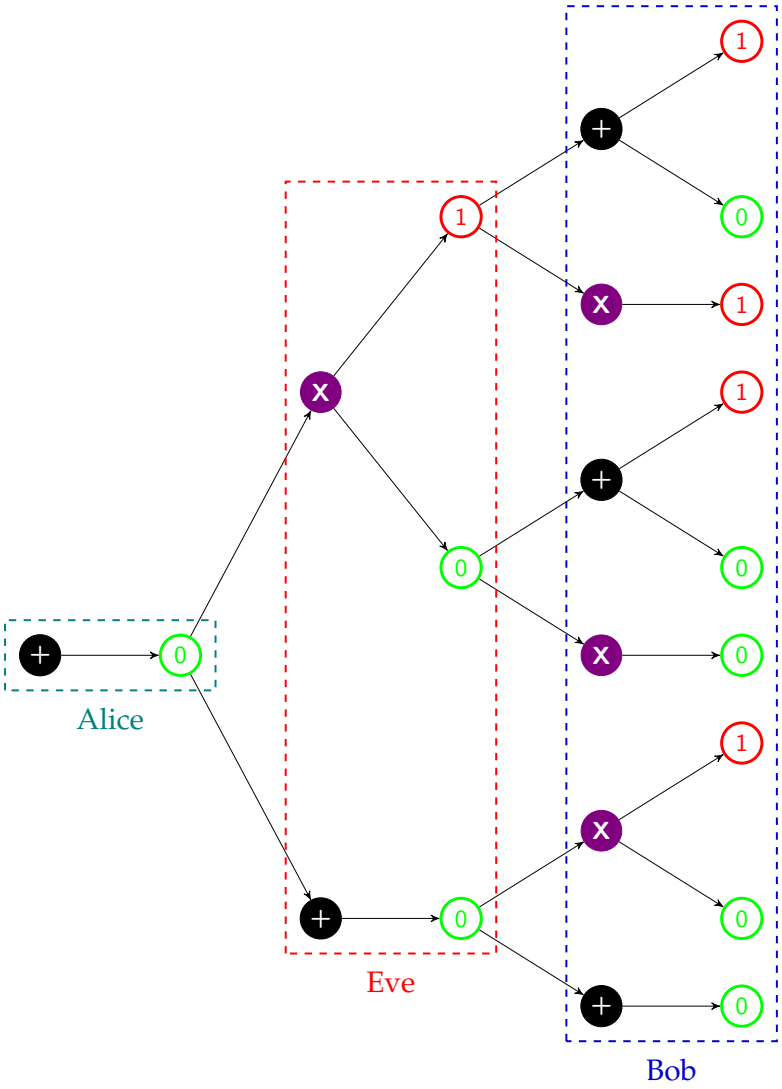

Figure 6. Case 2: with Eve.

Equation (2) allows $\mathbb{P}\{Sb\}$ to be obtained via the calculation of $\mathbb{P}\{Sb|+\}$. The detailed analysis presented above allows for the calculation of this probability as follows:

$$\begin{aligned}\mathbb{P}\{Sb|+\} &= \mathbb{P}\{Sb|+\bigcap 0\}\,\mathbb{P}\{0\} + \mathbb{P}\{Sb|+\bigcap 1\}\,\mathbb{P}\{1\} \\ &= 2\,\frac{1}{2}\,\mathbb{P}\{Sb|0\bigcap +\} = \mathbb{P}\{Sb|+\bigcap 0\}.\end{aligned} \tag{4}$$

$\mathbb{P}\{Sb|+\bigcap 0\}$ can be calculated by summing the probability of the different events leading Bob to measure state 0, as detailed above. Hence, referring to Figure 6, we get $\mathbb{P}\{Sb|0\bigcap +\} = \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{16} + \frac{1}{8} = \frac{5}{8}$. Consequently,

$$\mathbb{P}\{Sb\} = \mathbb{P}\{Sb|+\} = \frac{5}{8} = 0.625. \tag{5}$$

This result indicates that Eve's presence reduces $\mathbb{P}\{Sb\}$ from 0.75 to 0.625. It is worth noting again that, in the BB84 procedure, only the bits that Bob obtains using the same basis as Alice are considered. The others are rejected.

Consequently, it is also important to calculate $\mathbb{P}\{Sb|CB\}$:

$$\mathbb{P}\{Sb|CB\} = \frac{\mathbb{P}\{Sb \bigcap CB\}}{\mathbb{P}\{CB\}}, \tag{6}$$

where, again, $\mathbb{P}\{CB\} = \frac{1}{2}$, and

$$\begin{aligned} \mathbb{P}\{Sb \bigcap CB\} &= \mathbb{P}\{Sb \bigcap CB|0\}\,\mathbb{P}\{0\} + \mathbb{P}\{Sb \bigcap CB|1\}\,\mathbb{P}\{1\} \\ &= 2\,\frac{1}{2}\,\mathbb{P}\{Sb \bigcap CB|0\} = \mathbb{P}\{Sb \bigcap CB|0\}. \end{aligned} \tag{7}$$

The term $\mathbb{P}\{Sb \bigcap CB|0\}$ can be calculated by considering, again, the operations depicted in Figure 6, as follows:

$$\begin{aligned} \mathbb{P}\{Sb \bigcap CB|0\} &= \mathbb{P}\{Sb \bigcap CB|0 \bigcap +\}\,\mathbb{P}\{+\} + \mathbb{P}\{Sb \bigcap CB|0 \bigcap X\}\,\mathbb{P}\{X\} \\ &= 2\,\frac{1}{2}\,\mathbb{P}\{Sb \bigcap CB|0 \bigcap +\} = \frac{1}{4} + \frac{1}{16} + \frac{1}{16} = \frac{3}{8} = 0.375. \end{aligned} \tag{8}$$

Finally, we return to Equation (6). Given that $\mathbb{P}\{Sb \bigcap RB\} = \frac{3}{8}$, we get $\mathbb{P}\{Sb|RB\} = 2\,\frac{3}{8} = \frac{3}{4}$.

This result indicates that, even when Bob guesses the same basis as Alice, there is a probability of 0.25 that he measures the wrong state with respect to Alice due to Eve's intervention. This observation quantifies how much Eve negatively affects Bob's chances of measuring the correct value that Alice sent.

5.2.3. Impact of the Interception Density

The previous analysis considers the cases of knowing the presence or absence of Eve. The extension of the study is to evaluate the impact on the BB84 performance of the interception density parameter, indicated as p, which represents the percentage of qubits (and, hence, bits) that Eve intercepts. This parameter is considered in QS and can be set before starting the simulation, as was already highlighted in Section 4.1. If referring to the previous analysis, this parameter impacts the BB84, as described in Figure 7:

- With probability p, Eve intercepts the qubit; consequently, the BB84 performance can be computed following the analysis of Case 2 in this subsection.
- With probability $1 - p$, Eve does not intercept the qubit; i.e., the scenario is equivalent to Case 1 in this subsection.

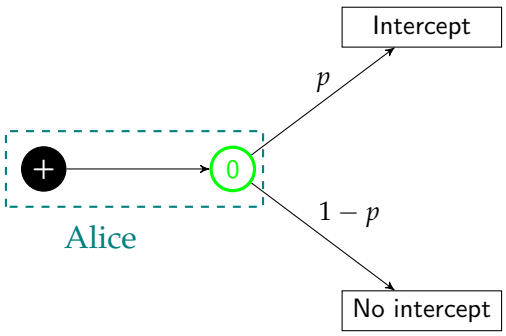

Figure 7. Scenario with interception density p.

With respect to the previous analysis, the introduction of p does not change Equation (1), i.e., $\mathbb{P}\{CB\} = \frac{1}{2}$, while it impacts the probability of some other events as follows.

Recall Equation (2), $\mathbb{P}\{Sb\} = \mathbb{P}\{Sb|+\}$, which can be calculated by considering Equations (3) and (5), weighted according to the conditioning probability $(1-p)$ and p, respectively:

$$\mathbb{P}\{Sb|+\} = \frac{3}{4}(1-p) + \frac{5}{8}p = \frac{3}{4} - \frac{1}{8}p. \tag{9}$$

$\mathbb{P}\{Sb|CB\}$ can be easily derived from Equation (6), taking into account that $\mathbb{P}\{Sb \bigcap CB\}$ is equal to $\frac{3}{8}$ or $\frac{1}{2}$ if Eve does or does not intercept the qubit, respectively:

$$\begin{aligned}\mathbb{P}\{Sb|CB\} &= 2\,\mathbb{P}\{Sb \bigcap CB\} \\ &= 2\left(\mathbb{P}\{Sb \bigcap CB|\text{No intercept}\}\,(1-p) + \mathbb{P}\{Sb \bigcap CB|\text{Intercept}\}\,p\right) \\ &= 2\left(\frac{1}{2}(1-p) + \frac{3}{8}p\right) = 1 - \frac{1}{4}p.\end{aligned} \tag{10}$$

This result allows for deriving a key relation between the computable (by Alice and Bob) $QBER$ and Eve's interception density, p, in the case of a partial intercept-and-resend attack:

$$QBER = 0.25\,p, \tag{11}$$

which confirms previous results [15] and represents the starting point of the proposed intrusion detection method. It is worth pointing out that Equation (11) is obtained when assuming ideal channel conditions, i.e., no system noise.

5.3. The Proposed Intrusion Detection Method

To generalize Equation (11), the assumption on the channel noise should be released. For this aim, four different cases can be defined, depending on the presence of Eve and noise. Each case has a different impact on the theoretical $QBER$, as described in the following:

1. **No system noise, no Eve**: $QBER = 0$,
2. **System noise, no Eve**: the $QBER$ can be derived once the amount of random noise is determined,
3. **No system noise, Eve**: $QBER = 0.25\,p$,
4. **System noise, Eve**: $QBER \geq 0.25\,p$.

Among these alternative scenarios, the latter (with interception density p) is the most interesting one. Considering a noisy scenario and Equation (11), in the case where the parameter p is known, the information that could be derived from the $QBER$ observation is that, if $QBER < 25\,p\%$, Eve has not intercepted the exchanged bits. On the contrary, no useful information is available when $QBER \geq 25\,p\%$ if no information on the noise is available. Of course, this is a probabilistic approach that may fail, as discussed below.

The $QBER$ can be estimated after establishing the number of bits used for testing the BB84 procedure (i.e., m), Therefore indicating with d the number of erroneous bits detected at Bob's side in the shared key:

$$\hat{QBER} = \frac{d}{m}. \tag{12}$$

When considering the above analysis and Equation (11), the *missed detection* (MD) event corresponds to the case that $d < 0.25pm$, but Eve is present, i.e., when the number of wrong bits in the shared key is less than the expected mean value.

More specifically, when considering the corresponding integer value and, hence, setting a threshold equal to $\lfloor 0.25pm \rfloor - 1$, the missed detection probability $\mathbb{P}\{MD\}$ can be calculated as follows:

$$\mathbb{P}\{MD\} = \sum_{i=0}^{\lfloor 0.25pm \rfloor - 1} \binom{m}{i} (0.25p)^i\,(1-0.25p)^{m-i}. \tag{13}$$

It is worth noting that the above Equation does not consider the noise; consequently, the actual $\mathbb{P}\{MD\}$ would be even smaller since the noise would increase the probability of a bit error on Bob's side. In other words, the proposed intrusion detection method incorporates errors on the bits due to system noise into Eve's intervention, thus following a conservative approach in evaluating the attack scenario.

6. Performance Evaluation

The performance evaluation of the proposed intrusion detection method was carried out with the QS, using different quantum backend simulators and simulation settings, as described in Sections 6.1 and 6.2, respectively. The key element of our approach, the estimation of the $QBER$, is discussed throughout all the remaining subsections.

6.1. Simulators of Quantum Communication

QS can be interfaced with a large amount of backend simulators, provided via IBM, and inspired by real quantum machines. These simulators mainly differ in terms of the following properties.

- The number of qubits available for computations to the quantum computer.
- The maximum number of shots. A shot is a single execution of a quantum algorithm; for example, a shot is a single pass through each stage of a complete quantum circuit. The maximum number of shots represents how many times an algorithm can be run for a single task, resulting in a probability distribution of results [37].
- The noise model, used to simulate the noisy operations of a real quantum computer.

After the analysis of all available backends (to take advantage of their inherent characteristics), our choice is to utilize the following two simulators: `aer_simulator` and `fake_brooklin`, both with the number of shots set to 1. Table 3 summarizes their main features.

More specifically, the `aer_simulator` was selected for two main reasons:

- The execution times are very low, enabling a high number of simulations in a short amount of time.
- It simulates an ideal, noise-free, quantum circuit, allowing for the isolation of the impact of Eve.

On the other hand, the selection of `fake_brooklin` was due to its ability to model the system noise, giving more accurate and realistic results.

Table 3. Summary of the main features and settings of the simulators used.

Parameters	`aer_simulator`	`fake_brooklin`
Number of qubits	29	65
Maximum shots	1,000,000	8192
Noise modeling	No	Yes

6.2. Settings of Simulation Analysis

The simulation study was carried out with different settings of p and n. In more detail, the values of Eve's interception density are as follows:

$$p = \{\ 0,\ 0.2,\ 0.4,\ 0.6,\ 0.8,\ 1\ \},$$

and for each of them, four different settings of n were considered:

$$n = \{\ 1024,\ 1536,\ 2048,\ 2048\}.$$

The first three values refer to scenarios where BB84 is used to generate a symmetric key with the same security level as today's standard symmetric key algorithms: AES-128,

AES-192, and AES-256, respectively [32]. Indeed, about half of the n bits are lost due to the random choice of the bases by Alice and Bob, and another half of the remaining bits must be discarded because of the key-checking procedure (see Section 4.2). Consequently, the average number of bits useful for the key is about $\frac{n}{4}$. Furthermore, once quantum computers can implement Grover's algorithm, the complexity of a symmetric key search will be reduced from $\mathcal{O}(2^n)$ to $\mathcal{O}(2^{\frac{n}{2}})$ [1]. This means that, to have an equivalent post-quantum security level, the key lengths must be multiplied by a factor of 2. In summary, for example, $n = 1024$ permits having the same security level of AES-128. Finally, the value $n = 4096$ was chosen to provide sufficient data to accurately model the noise of the simulator and analyze the evolution of the model's performance under increased safety requirements.

For each scenario characterized by the pair (p, n), 50 independent runswere conducted to estimate the average value and the corresponding 95% confidence interval (CI).

6.3. Results: Model Validation

The first set of results aimed to validate the accuracy of Equation (11). Two different scenarios were considered: without and with system noise. Clearly, the analysis of the first case exploits the `aer_simulator`, while the second one refers to `fake_brooklin`, under the assumption that the system noise is additive to Eve's interception, i.e.,

$$QBER = 0.25\, p + QBER_{SN}, \tag{14}$$

where $QBER_{SN}$ is the $QBER$ introduced via the system noise.

Figures 8 and 9 display the considered values of p on the x-axis, while the estimated $QBER$, $\hat{QBER}$, and its related 95% C.I. are shown on the y-axis. The dashed black line represents the best-fitting line (least squares error), based on the estimated mean $\hat{QBER}$ for each value of p.

More specifically, Figure 8 shows the results with the `aer_simulator` for $n = 1024$. The resulting slope of the best-fitting line is 0.2493, which is closely aligned with the theoretical predicted value of 0.25 p. As expected, the regression line passes through the origin, given that this simulator does not model noise.

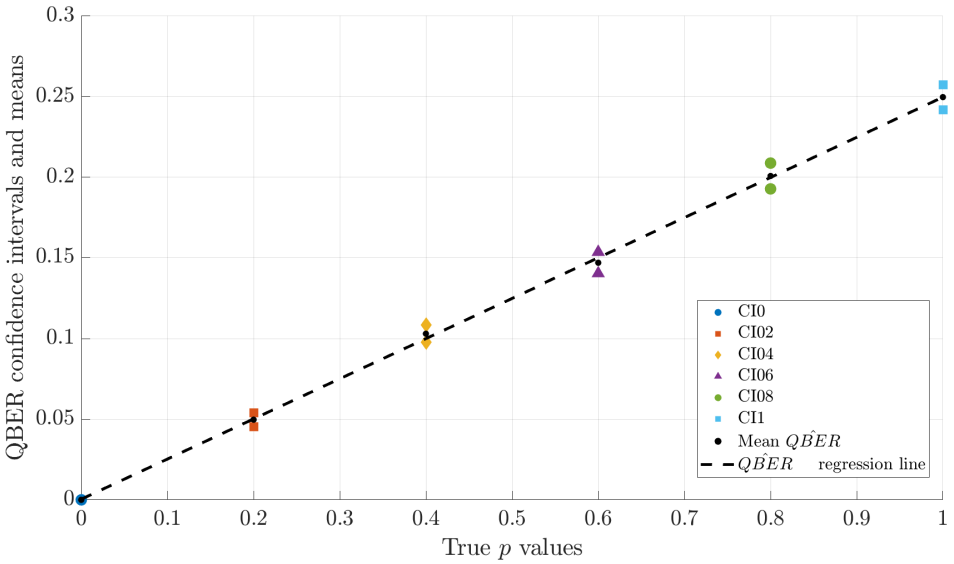

Figure 8. `aer_simulator` model, n = 1024.

Similar results were obtained for the other n settings. For simplicity, only the case $n = 4096$ is depicted in Figure 9, while the essential data required to validate the model of Equation (11) are summarized in Table 4 for all considered values of n.

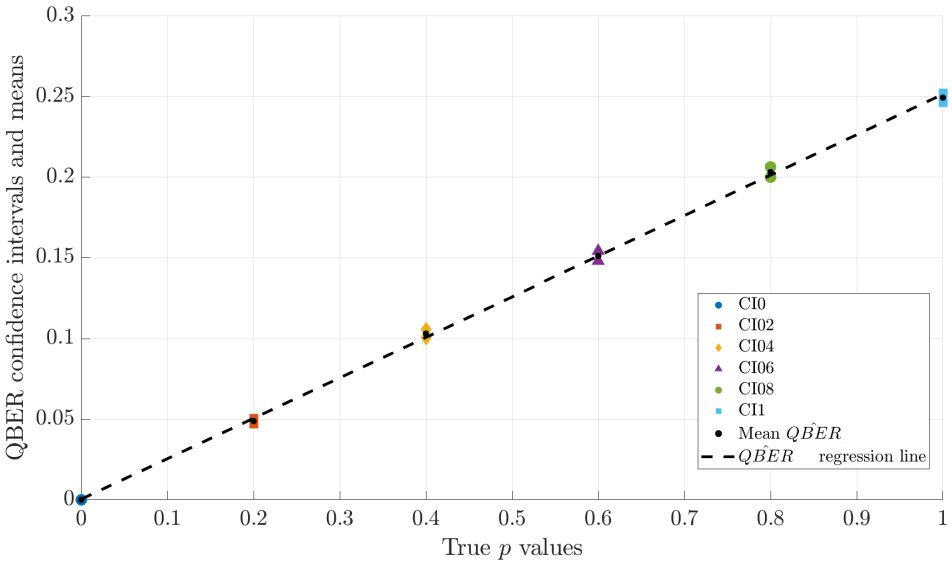

Figure 9. `aer_simulator` model, $n = 4096$.

Table 4. Results for the `aer_simulator` model.

n	Slope	$\hat{QBER}_{SN}$
1024	0.2493	0
1536	0.2533	0
2048	0.2476	0
4096	0.2511	0

Figures 10 and 11 refer to the `fake_brooklin` simulator. The main distinction from the previous results is the inclusion of system noise, which generates $QBER_{SN}$.

The best-fitting line in these figures suggests two conclusions. Firstly, $QBER_{SN}$ appears to be additive, as assumed in Equation (14). Indeed, the best-fitting line has a slope of around 0.25. Secondly, the estimation of $QBER_{SN}$ can be derived by evaluating $\hat{QBER}$ when $p = 0$. For instance, Figure 10 displays a slope of 0.237 and $\hat{QBER}_{SN} = 0.01835$.

The comparison between Figures 10 and 11 reveals a decrease in the size of the 95% CI as n increases. Additionally, the figures illustrate a trend of higher CI intervals as p increases.

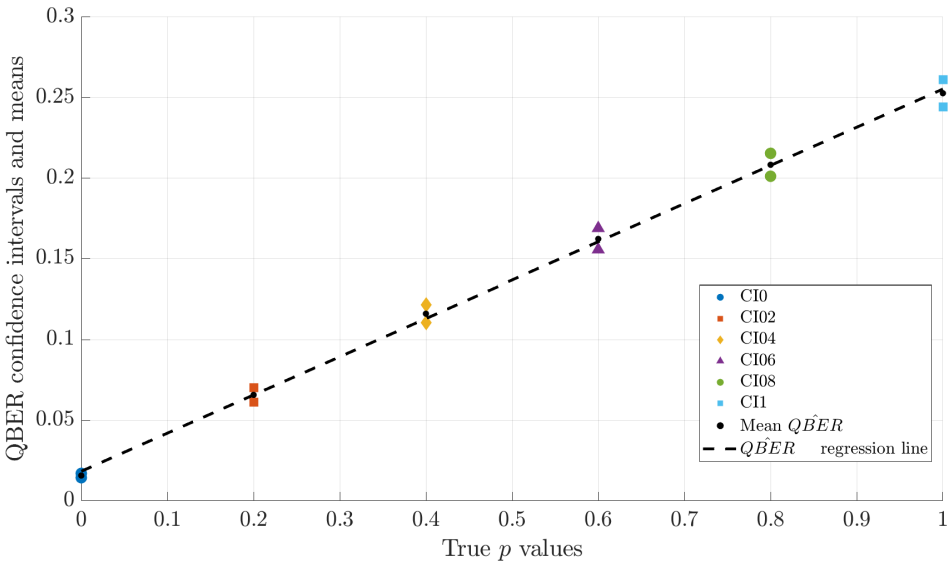

Figure 10. `fake_brooklin` simulator model, $n = 1024$.

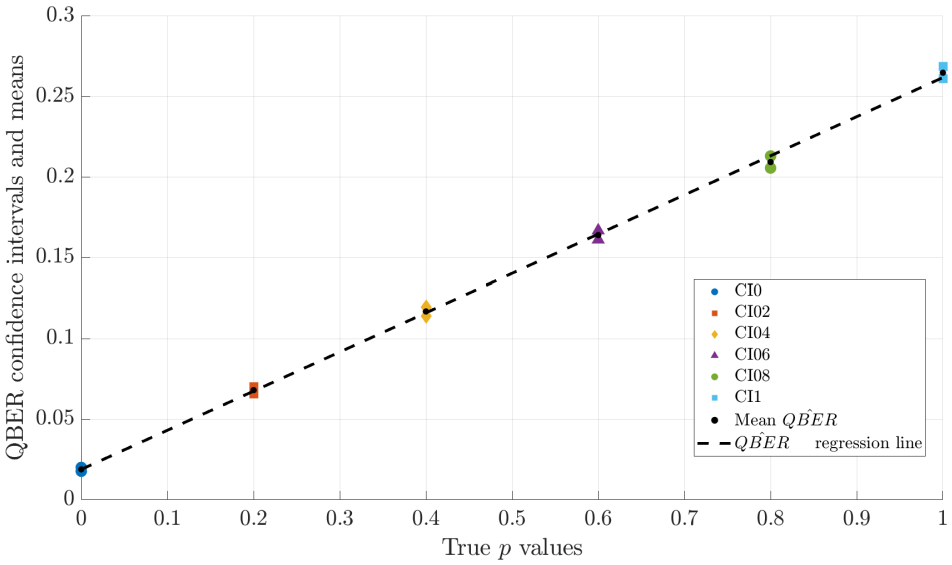

Figure 11. `fake_brooklin` simulator model, n = 4096.

Table 5 summarizes the quantitative results, highlighting the small variations in the estimated values of the slope and $\hat{QBER}_{SN}$.

Therefore, the results shown provide experimental evidence of the validity of Equation (14).

Table 5. Results for the `fake_brooklin` simulator model.

n	Slope	$\hat{QBER}_{SN}$
1024	0.237	0.01835
1536	0.247	0.01705
2048	0.244	0.01918
4096	0.243	0.0189

6.4. Results: Intrusion Detection

This analysis aims to evaluate the accuracy of the method used to estimate p on Bob's side. The assumption is that $QBER_{SN}$ is known, for example, through measurement campaigns, as previously discussed. The intrusion detection procedure involves calculating $\hat{QBER}$ on Bob's side and then, by inverting Equation (14), estimating $\hat{p}$, which provides Bob with information on the interception density. This information can help Bob decide whether the shared key can be considered secure or if the BB84 protocol needs to be rerun. This study only considered the `fake_brooklin` simulator because it is important to account for the effects of the system noise in the estimation process.

In this regard, the $QBER_{SN}$ value refers to the result obtained in the scenario with $n = 4096$, as shown in Table 5, i.e., $QBER_{SN} = 0.0189$. The rationale behind this choice is that the higher the value of n, the higher the accuracy of the $QBER$ estimate.

Figures 12 and 13 show the results for the cases $n = 1024$ and $n = 4096$, respectively. The figures display the set of points (p,$\hat{p}$) obtained for each of the 50 runs. The analysis of the figures suggests that the average estimate is close to the set p value. However, the different estimations are spread over a relatively wide interval. This interval widens further as p approaches 1.

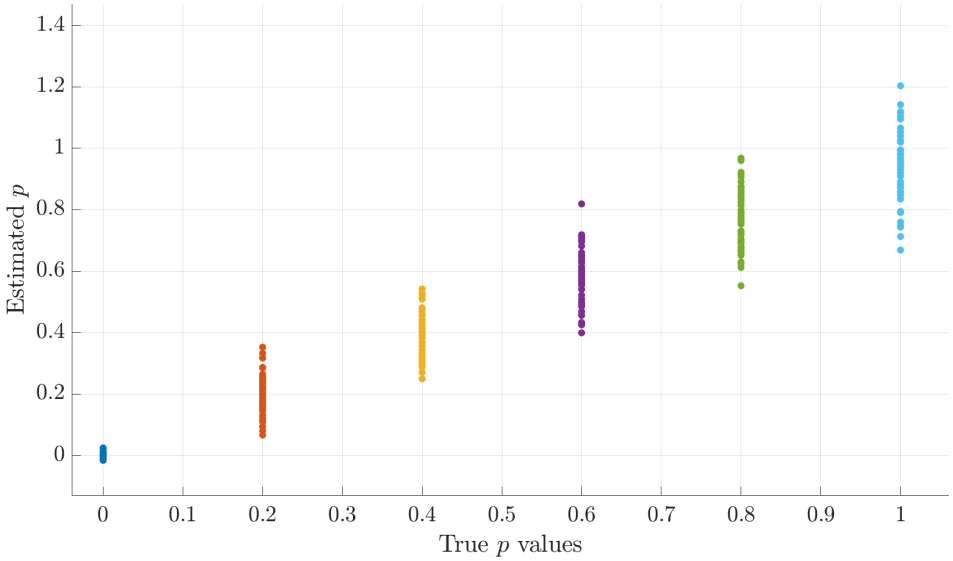

Figure 12. Estimated p with `fake_brooklin` simulator, $n = 1024$.

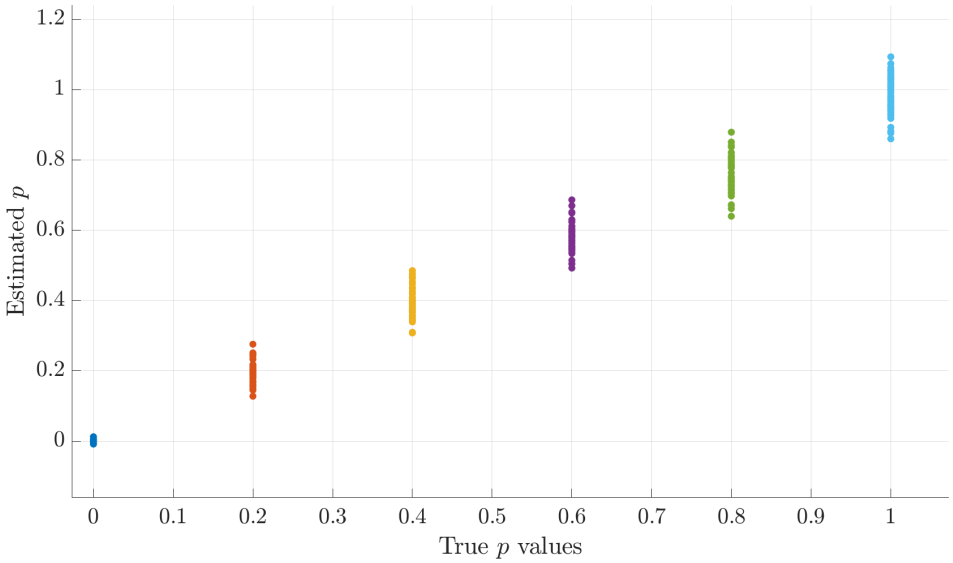

Figure 13. Estimated p with `fake_brooklin` simulator, $n = 4096$.

The comparison between Figures 12 and 13 reveals that, as n increases, $\hat{p}$ becomes progressively more accurate, and the spread of the estimation interval decreases. These conclusions were corroborated with the results for other values of n, namely $n = 1536, 2048$.

For the sake of brevity, only the quantitative results of the various scenarios are presented in Tables 6–9.

Table 6. Estimated p, $n = 1024$.

p	avg.	min.	max.	σ
0	−0.0110	−0.0622	0.0471	0.0200
0.2	0.1960	0.0839	0.3100	0.0490
0.4	0.3911	0.2880	0.5147	0.0548
0.6	0.5963	0.4641	0.7239	0.0600
0.8	0.7774	0.6120	0.9753	0.0742
1	0.9687	0.7628	1.1138	0.0762

Table 7. Estimated p, n = 1536.

p	avg.	min.	max.	σ
0	−0.0026	−0.0453	0.0455	0.0173
0.2	0.1964	0.1382	0.2699	0.0346
0.4	0.3868	0.3098	0.5016	0.0458
0.6	0.5988	0.4980	0.7080	0.0510
0.8	0.7982	0.6658	0.9057	0.0539
1	0.9953	0.8646	1.1436	0.0656

Table 8. Estimated p, n = 2048.

p	avg.	min.	max.	σ
0	−0.0059	−0.0375	0.0415	0.0141
0.2	0.1980	0.1355	0.2704	0.0300
0.4	0.4044	0.3076	0.4960	0.0387
0.6	0.6011	0.5135	0.7073	0.0387
0.8	0.8052	0.6809	0.9086	0.0534
1	0.9993	0.8376	1.1544	0.0624

Table 9. Estimated p, n = 4096.

p	avg.	min.	max.	σ
0	−0.0000	−0.0228	0.0259	0.0100
0.2	0.1999	0.1447	0.2593	0.0265
0.4	0.4035	0.3570	0.4691	0.0265
0.6	0.6016	0.5377	0.6645	0.0300
0.8	0.7938	0.7159	0.8605	0.0346
1	1.0040	0.9366	1.1059	0.0361

The analysis of these tables reveals that the estimation becomes progressively more accurate with the increase in n. Particularly, the last table, Table 9 provides almost perfect average estimations, with a mean standard deviation (σ in the tables) that is always less than 4% for all values of the interception density.

It is important to note that, while the accuracy of determining the real value of p is certainly valuable, in practical scenarios, simply knowing that $p > 0$ may indicate a high likelihood of Eve's presence. In summary, the method can detect Eve's action as long as information on $QBER_{SN}$ is available.

6.5. Additional Remarks

The results presented here assumed a noise-free environment, except for the intrinsic noise of the simulated quantum system. However, in real-world scenarios, noise could originate from various sources, including the communication channel. Excessive noise could potentially reduce the reliability of intrusion detection.

Moreover, this approach is inherently probabilistic, so if it were to be employed in a real-world application to detect an eavesdropper, an acceptance threshold would need to be established. If the estimated values were to fall above this threshold, the key exchange would be deemed insecure. To determine this threshold, all potential sources of noise would need to be considered, along with the number of errors that could be tolerated and corrected using error correction codes.

7. Conclusions

This paper has presented a method for intrusion detection within the BB84 QKD scheme with a partial intercept-and-resend attack. The proposed approach is based on a theoretical model that considers the $QBER$ induced via both eavesdropping (Eve's interception) and inherent quantum system noise. A performance evaluation, conducted using

a realistic quantum system simulator with noise, demonstrated the validity of the proposed method in estimating the interception density, which is crucial for detecting Eve's presence.

In more detail, the results obtained indicate that the system accuracy is influenced by the actual interception density and the initial key length, n. Specifically, lower interception densities and longer key lengths improve the precision of the detection mechanism.

Therefore, these findings suggest that the method could be effectively utilized in real-world scenarios to detect eavesdropping activities during the generation of a private shared key, thereby enhancing the security of quantum communication systems. Further work on this topic will include an examination of the viability of the proposed method in actual BB84 applications, such as those described in Section 1.

Author Contributions: Conceptualization, F.F., R.G.G. and M.P.; investigation, F.F.; simulation, A.O. and F.F.; writing—original draft preparation, R.G.G., F.F. and A.O.; writing—review and editing, R.G.G., M.P. and F.F.; supervision, R.G.G. and M.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the Italian Ministry of University and Research (MUR) in the framework of the FoReLab project (Departments of Excellence) and by the University of Pisa in the framework of the PRA_2022_64 "hOlistic Sustainable Management of distributed softWARE systems (OSMWARE)" project.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219. [CrossRef]
2. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
3. Hughes, R.J.; Nordholt, J.E.; Derkacs, D.; Peterson, C.G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.* **2002**, *4*, 43. [CrossRef]
4. Stucki, D.; Gisin, N.; Guinnard, O.; Ribordy, G.; Zbinden, H. Quantum key distribution over 67 km with a plug and play system. *New J. Phys.* **2002**, *4*, 41. [CrossRef]
5. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.; et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [CrossRef]
6. EUROQCI. The European Quantum Communication Infrastructure (EuroQCI) Initiative. Available online: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (accessed on 11 July 2024).
7. Alshowkan, M.; Evans, P.G.; Starke, M.; Earl, D.; Peters, N.A. Authentication of smart grid communications using quantum key distribution. *Sci. Rep.* **2022**, *12*, 12731. [CrossRef] [PubMed]
8. Green, A.; Lawrence, J.; Siopsis, G.; Peters, N.A.; Passian, A. Quantum Key Distribution for Critical Infrastructures: Towards Cyber-Physical Security for Hydropower and Dams. *Sensors* **2023**, *23*, 9818. [CrossRef] [PubMed]
9. Alia, O.; Huang, A.; Luo, H.; Amer, O.; Pistoia, M.; Lim, C. 100 Gbps Quantum-safe IPsec VPN Tunnels over 46 km Deployed Fiber. *arXiv* **2024**, arXiv:2405.04415
10. Kebapci, B.; Levent, V.E.; Ergin, S.; Mutlu, G.; Baglica, I.; Tosun, A.; Paglierani, P.; Pelekanakis, K.; Petroccia, R.; Alves, J.; et al. FPGA-Based Implementation of an Underwater Quantum Key Distribution System With BB84 Protocol. *IEEE Photonics J.* **2023**, *15*, 1–10. [CrossRef]
11. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
12. Lee, C.; Sohn, I.; Lee, W. Eavesdropping Detection in BB84 Quantum Key Distribution Protocols. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2689–2701. [CrossRef]
13. Inoue, K. Quantum key distribution technologies. *IEEE J. Sel. Top. Quantum Electron.* **2006**, *12*, 888–896. [CrossRef]
14. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
15. Rieffel, E.; Polak, W. Quantum Computing: A Gentle Introduction. In Scientific and Engineering Computation; The MIT Press: Cambridge, MA, USA, 2011.
16. Shor, P.W.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [PubMed]
17. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **2001**, *48*, 351–406. [CrossRef]

18. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *arXiv* **2004**, arXiv:quant-ph/quant-ph/0212066.
19. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
20. Biswas, S.; Goswami, R.S. Securing Quantum Communication: An IBM Quantum Lab Simulation Study of the Enhanced BB84 Protocol with Error Correction and Privacy Amplification. 2023, *in press*. Available online: https://www.researchsquare.com/article/rs-3035008/v1 (accessed on 5 June 2024). [CrossRef]
21. SujayKumar Reddy, M.; Chandra Mohan, B. Comprehensive Study of BB84, A Quantum Key Distribution Protocol. *arXiv* **2023**, arXiv:2312.05609. [CrossRef]
22. Pereira, M.; Currás-Lorenzo, G.; Navarrete, A.; Mizutani, A.; Kato, G.; Curty, M.; Tamaki, K. Modified BB84 quantum key distribution protocol robust to source imperfections. *Phys. Rev. Res.* **2023**, *5*, 023065. [CrossRef]
23. Anusuya Devi, V.; Kalaivani, V. Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. *Pers. Ubiquitous Comput.* **2023**, *27*, 875–885. [CrossRef]
24. Elboukhari, M.; Azizi, A.; Azizi, M. Quantum key distribution in practice: The state of art. In Proceedings of the 5th International Symposium On I/V Communications and Mobile Network, Rabat, Morocco, 30 September–2 October 2010; pp. 1–4.
25. Subramaniam, P.; Parakh, A. Limits on detecting eavesdropper in QKD protocols. In Proceedings of the 2014 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS), New Delhi, India, 14–17 December 2014; pp. 1–3. [CrossRef]
26. Zamani, F.; Verma, P.K. A QKD protocol with a two-way quantum channel. In Proceedings of the 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, India, 18–21 December 2011; pp. 1–6. [CrossRef]
27. Elboukhari, M.; Azizi, M.; Azizi, A. Analysis of the Security of BB84 by Model Checking. *arXiv* **2010**, arXiv:abs/1005.4504.
28. Dirac, P.A.M. The Principles of Quantum Mechanics. In *International Series of Monographs on Physics*; Clarendon Press: Oxford, England, 1981.
29. Contributors, W. Quantum Logic Gate. Available online: https://en.wikipedia.org/wiki/Quantum_logic_gate (accessed on 31 May 2024).
30. Qi, B.; Qian, L.; Lo, H.K. A brief introduction of quantum cryptography for engineers. *arXiv* **2010**, arXiv:1002.1237. [CrossRef]
31. Ekert, A.; Hayden, P.; Inamori, H. Basic concepts in quantum computation. In Proceedings of the Coherent Atomic Matter Waves, Les Houches, France, 27 July–27 August 1999; pp. 661–701.
32. Dworkin, M.; Barker, E.; Nechvatal, J.; Foti, J.; Bassham, L.; Roback, E.; Dray, J. Advanced Encryption Standard (AES). 2001. Available online: https://doi.org/10.6028/NIST.FIPS.197-upd1 (accessed on 5 June 2024). [CrossRef]
33. Escanez-Exposito, D.; Caballero-Gil, P.; Martín-Fer-nández, F. Interactive simulation of quantum key distribution protocols and application in Wi-Fi networks. *Wireless Networks* **2023**, *29*, 3781–3792. [CrossRef]
34. Pirandola, S.; Andersen, U.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 361502. [CrossRef]
35. Escanez-Exposito, D. QuantumSolver. Available online: https://github.com/jdanielescanez/quantum-solver (accessed on 31 May 2024).
36. IBM. Qiskit. Available online: https://www.ibm.com/quantum/qiskit (accessed on 31 May 2024).
37. Amazon. Amazon Braket Pricing. Available online: https://aws.amazon.com/braket/pricing/ (accessed on 31 May 2024).