sensors

MDPI

Article

Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3

Akwasi Adu-Kyere *, Ethiopia Nigussie and Jouni Isoaho

Department of Computing, University of Turku, Vesilinnatie 5, 20500 Turku, Finland
* Correspondence: akwasi.adu-kyere@utu.fi

Abstract: Autonomous "Things" is becoming the future trend as the role, and responsibility of IoT keep diversifying. Its applicability and deployment need to re-stand technological advancement. The versatile security interaction between IoTs in human-to-machine and machine-to-machine must also endure mathematical and computational cryptographic attack intricacies. Quantum cryptography uses the laws of quantum mechanics to generate a secure key by manipulating light properties for secure end-to-end communication. We present a proof-of-principle via a communication architecture model and implementation to simulate these laws of nature. The model relies on the BB84 quantum key distribution (QKD) protocol with two scenarios, without and with the presence of an eavesdropper via the interception-resend attack model from a theoretical, methodological, and practical perspective. The proposed simulation initiates communication over a quantum channel for polarized photon transmission after a pre-agreed configuration over a Classic Channel with parameters. Simulation implementation results confirm that the presence of an eavesdropper is detectable during key generation due to Heisenberg's uncertainty and no-cloning principles. An eavesdropper has a 0.5 probability of guessing transmission qubit and 0.25 for the polarization state. During simulation re-iterations, a base-mismatch process discarded about 50 percent of the total initial key bits with an Error threshold of 0.11 percent.

Keywords: quantum key distribution; quantum mechanics laws; cybersecurity; eavesdropper detection

check for updates

Citation: Adu-Kyere, A.; Nigussie, E.; Isoaho, J. Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3. *Sensors* **2022**, *22*, 6284. https://doi.org/10.3390/s22166284

Academic Editor: Sherali Zeadally

Received: 25 July 2022
Accepted: 18 August 2022
Published: 21 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

An increasing body of literature recognizes both the importance and emergence of quantum computers [1,2]. The quantum principles on which these future computers will rely have a crucial role in today's communication security and have received considerable attention recently [3]. These principles and properties are becoming a key instrument in how current security infrastructural design may need to adapt towards a post-quantum era. Different platforms and service categories utilize these diverse security infrastructures to secure communications and share data through cryptographic mechanisms. The purpose is to ensure information risk management despite attacks on communication protocol stacks. Both researchers and market analysts commonly suggest that quantum technologies such as QKD will be essential for a wide range of Internet communication technologies based on the current market demand [4]. This relationship between quantum and classic cryptography will likely influence several sectors in the coming years.

The Internet of Things (IoT) plays an increasing role in sectors such as cyber–physical systems and autonomous systems, which extend versatility to human-to-machine and machine-to-machine, vehicle-to-things, and vehicle-to-Internet (V2I) interactions [5]. Today, solving relevant and on-demand technological challenges such as data retrieval, automation, analysis, machine learning (ML), and monitoring processes in intelligent environments is achievable across multiple cloud platforms through several Internet services. These services include data collection and sharing supported by numerous hardware-to-service

nodes on heterogeneous devices over current classic communication channels. IoT security, challenges, and importance for these related service categories depend on cryptographic technologies that utilize symmetric and asymmetric algorithms. However, the current state-of-the-art key distribution and management processes face constraints and challenges such as managing numerous encryption keys, threats from malicious insiders and intruders, data accessibility by non-authorized users, governance, and application support, while dependent on the communication channels for communication secrecy. They depend on mathematical difficulty and computational complexities [6,7] compared to quantum technologies and cannot detect eavesdropping. This inability and dependency variation may allow malicious intruders and insiders to use clever and efficient ways to actively or passively manipulate and complicate secure secret key transmission and distribution. It can also influence the end-to-end trust in an ecosystem with differential security levels.

For example, a typical asymmetric (public key) cryptographic system has three components. These components are the message (plain-text) to be encrypted, denoted as M, the key used for the encryption K, and finally, the output (cipher-text), which is the encrypted message C, as shown in the figure below. Two keys are utilized for encryption and decryption [8]. One of the keys is public (encryption key), while the other is secret or private (decryption key). The publicly available is for anyone who wishes to communicate securely with the owner and holder of the private key.

The decryption of the cipher-text uses the second part of the key as $D_dB(m') = (x)$. Figure 1 illustrates this process by using two parties, A and B. Both Party A and B have a secret key and a private key (d_A, e_A) and (d_B, e_B), respectively. Assume Party A wants to send a message $M = (x)$ to Party B by using Party B's public key (e_B) for the encryption $(E_eB(x) = (m'))$. Public key infrastructures such as the Rivest–Shamir–Adleman (RSA) algorithms rely on the inability to factorize larger integers of the form $n = PQ$ effectively [9] in a realistic time (polynomial time) [10], hence applying computational complexity and mathematical difficulty to increase or decrease the security robustness [6,11–13].

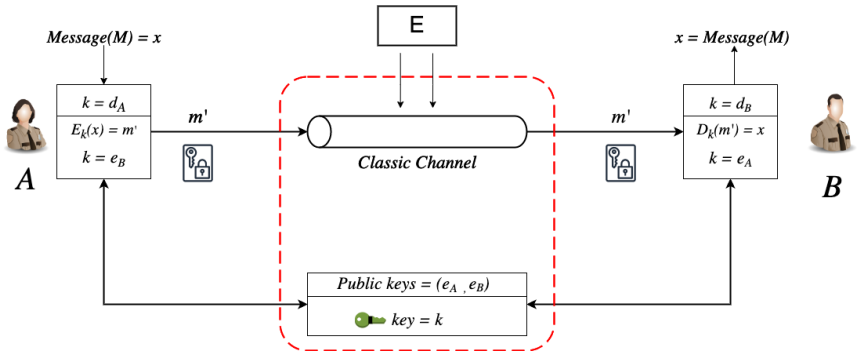

Figure 1. This figure represents a basic public key cryptosystem.

This work studies and demonstrates QKD use for secure cryptographic key distribution over a classic communication channel. It focuses on implementing a standard de facto BB84 protocol in a simulation model design. The contributions of this work are:

1. Design of a communication architecture model that takes advantage of quantum cryptography for enabling secure communication;
2. Implementation and simulation of the BB84 protocol in python3;
3. Analysis of QKD efficacy for secure communication.

The first section is a theoretical overview of quantum cryptography (QC) and commonly used terminologies in this paper. The next section describes the communication architecture model, followed by its implementation. Further characterization of the architectural model illustrates our simulation for the no-cloning theorem and uncertainty principle with and without an eavesdropper. Finally, the research findings focus on QKD's importance.

2. Overview of Quantum Cryptography

A century ago, Steve Wiesner's paper *Conjugate Coding* considerably ignited quantum cryptography's realization [14] after a series of contributing events. For example, Max Planck discovered Planck's constant by finding ways to explain his glowing light filament observation [15]. Einstein's 1905 prediction and Sir Isaac Newton interpreted light as a wave and not just an energy source with millions of elementary particles [16]. Each particle's discrete quantity of energy is proportional in magnitude to the source frequency emission and transformation of light. This development, later on, led to photons through Arthur Compton's work in 1923 [17]. However, the 20th Century [12] evidences these contributions in current quantum cryptographic popularity and the evolution of advancements in the reality of quantum principles and concepts.

Today, the *"science of secrets"* [18] as we now know through photon–quanta energy manipulation has benefited a wide range of technologies such as QKD. It is now among one of the fully developed and heaviest research focus areas in quantum informatics [19,20]. This advancement is partly due to the prospects of quantum computing and classic cryptographic systems' shortcomings benefiting QKD's trends. QKD's cryptosystem basis and construction reveal a guarantee of secrecy explicitly attributed to the laws of nature in quantum mechanics [21]. It is a mechanism for agreeing on secret shared keys between remote parties [22] to ensure tamper-proof shared keys via alerting the original parties if tampered with during transmission by an adversary.

Now, let us clarify a few necessary terms used throughout this paper. A *qubit* is a classic bit in a quantum system. Qubits in a quantum domain spin continuously in a direction dependent on the propagating source, as shown in Figure 2. This spinning property is the quantum state [13], referring to a condition of an entity being differentiable from others of its kind at a specific instance. Determining this state requires measurement, which could be through observation. However, measuring a quantum state introduces a disturbance that irretrievably changes the state, leading to our first core principle, *Heisenberg's uncertainty principle* [23]. It states that measuring a photon's quantum state is impossible without introducing a disturbance within a quantum system. This uncertainty principle implies that a change in a quantum state is the direction in which a qubit spins at any particular time, shown in Figure 2, prior to measurement. It refers to this behavior as an unknown state, which is also the superposition theorem [24]. It is a property of a qubit and entanglement, where two or more qubits correlatively spin in a direction within a quantum system [25]. If the spinning direction of a single qubit is known, then this spinning direction can help determine multiple qubits' directions. Hence, quantum bits for information transference from one point to another are restricted or induced to a defined pattern or direction for message encoding in polarization. They are horizontally or orthogonally biased before transmission over a protocol. A *protocol* is a systematic [26] and recommended set of procedures that officially govern how a specific activity's internal operation occurs for profitable utilization. Quantum protocols share basic foundational principles, even though some specific characteristics and properties are unique to some protocols.

Based on the previously mentioned uncertainty property and characteristics, there would be challenges whenever copying a polarized photon because the quantum state of that specific photon is unknown. This leads to our final core principle: the *No-Cloning theorem*. This theorem relies on Wootters and Zurek's no-cloning theorem in 1982, which states that the copying of a polarized photon is impossible due to the unknown quantum state of that specific photon [27]. Another aspect of this definition is that cloning a specific photon requires measurement parameters, including obtaining the quadrature component [28], which accurately represents the clone. However, this principle breaches the no-cloning theorem and is no longer a clone of that polarized photon.

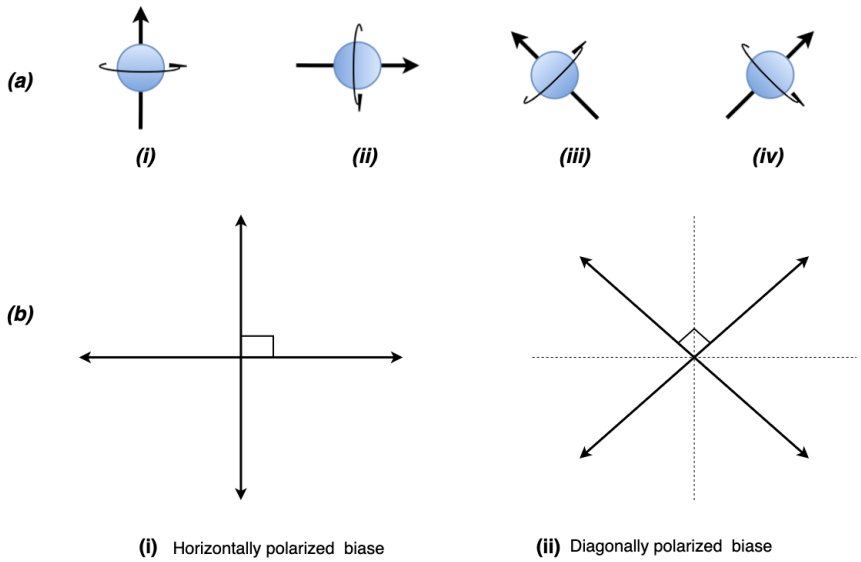

Figure 2. This is a figure representing the spinning direction of the qubit and its quantum states at a specific time: (**a**) Shows the four states of polarization qubits. (**b**) (i,ii) illustrate the two types of polarization for encoding purposes in quantum cryptography only detectable by the correct photon filter.

In light of the uncertainty theorem, an eavesdropper has a probability of 0.5 of guessing the currently encoded qubit and 1/n chances for the polarized quantum states, where n is the amount of the existing state in that quantum system. Figure 2b illustrates this by showing that at any point in time, a qubit could be horizontally biased or octagonally biased with the probability existing in Figure 2a. For example, in a typical quantum cryptographic communication, a polarized photon's direction of 0° and 45° may represent $|0\rangle$ as $0bit$ while 90° and 135° represent $|1\rangle$ as $1bit$. Only either horizontal or orthogonal bias is detectable by the correct photon filter. It is a one-way operation in quantum cryptography. Significantly, photons detected by the photon filter or detector upon impact are not reconstructable. Moreover, undetected photons also suffer the same fate. Therefore, assume a photon filter detecting three photons polarized in the following ways, (0° or 45°), (90° or 135°), (90° or 135°), or (0° or 45°), would be encoded in a classical bit equivalent of a 1001 bit representation.

Quantum Attacks

The principles of quantum cryptography relying on the laws of quantum mechanics for generating a secure key via manipulating light's properties for secure end-to-end communication is theoreticallysound [29–31]. The versatile security interaction between "Things", such as human-to-machine and machine-to-machine, currently benefits from this advancement worldwide through communication architectural quantum networks, a promise yet to spread across countless practical applications even with positive trends with technological evolutional advancements in their early stages. However, this promise and technological paradigm of this quantum regime have unprecedented challenges related to conceptualizing and interpreting quantum principles from theoretical to fully functional, practical quantum systems. These are noticeable technical imperfections, impeding physical barriers in coherent pulse generation, oscillators, interferometers, synchronizations, channel noise, and auto-compensating optical communication causalities. Even worse, these challenges cannot be generalized but have a moderate figure of merit on differentiable QKD vendor systems.

Quantum experimental hacking and exploitation attacks take advantage of the essential nature of light's property as a wave other than packets of energy quanta, which requires an indistinguishable phase difference via introducing instability or interference in

its hardware modeling nodes and devices. These practical non-uniformities attributed to attack causalities can also be extended to quantum protocol drawbacks and environmental influence. Today, quantum error rate (QBER) stemming from the error correction in a quantum key distribution systems (QKDs) has been a contributing factor as an attack vector for influencing the coherence photon state [32] source. Stimulated emission, which approximates perfect quantum cloning [33], parametric optical amplification, and the bunching properties of light fields [11] can be considered post-quantum polarization cloners in contrast to the no-cloning theorem. The process assumes a perfect cloning device capable of cloning and maintaining all the characteristics and properties of that specific polarized photon, even though they are affected by the fidelity of the equipment used. Relative attacks such as beam-splitting [34–36] have been a platform for daisy chaining other exploratory exploitations, such as calibration attacks [37,38], side-channel attacks [39–41], which extend wavelength manipulation [42,43] with a similar profile attack, such as detector-device-independent [44], denial of service attack [45,46], intercept-resend attack [47], and Trojan horse attack [48].

3. Related Work

The literature on the evolution of QKD has highlighted several advantages and disadvantages concerning possible attack scenarios and perceived weaknesses [49]. Different theories exist in the literature stemming from variations of the original BB84 protocol of Bennett–Brassard. More recently, attention has focused on the frameworks, algorithms, platforms, and software for simulating different experimental concepts and ideas [50–53].

Using the simulation approach, researchers can balance cost, convenience, and other factors that are complex to maneuver with hardware. A considerable amount of published literature has been on QKD simulation with this outcome. Some examples of these studies and research include Omer et al. [54], who simulated a QKD process based on the BB84 protocol. The core part of their simulation was written in Visual C sharp. Buhari et al. [55] used the OptiSystem platform. Antje Kohnle and Aluna Rizzoli [56] used either polarized photons or spin 1/2 particles as physical realizations. Chatterjee et al. [57] also simulated QKD based on the B92 protocol. Mogos [58] focused on two cases: with and without cyber-attacks using C plus-plus (C++). Shajahan, Rimitha, Nair, and Suchithra S. [59] explained how a networking scenario could exploit pure laws in physics through QKD simulation inside a classical communication channel. Khan et al. [7] presented an in-depth security analysis on QKD protocols encompassing theoretical assertions to practical implementation factors. Anuj Sethia and Anindita Banerjee [60] simulated a practical model implementation of differential phase shift (DPS) QKD with a toolkit based on Simulink and MATLAB. Kashyap and M. Ramachandra [61] and Mina Mihai-Zico and Simion Emil [62] simulated QKD in the Qiskit library of Python. Fan-Yuan et al. [63] simulated using a single-photon and Hong–Ou–Mandel interference optical units.

These works share key features that are consistent with the literature and the theoretical results. In contrast and as an extension to previous work, some analytical and simulation works did not clearly state the error threshold bound limit they were working with. There was an insufficient comparison between scenarios with and without the presence of an eavesdropper. In some instances, the simulations were by example rather than by modeling, making it complicated to compare the initial and final parameters.

4. Simulation Architectural Model and Implementation

Indeed, the possibility of intercepting a quantum transmission via a quantum channel is through disturbance. It is also clear that such activities are detectable via the quantum protocol's error rate and eavesdropper presence. With these already-established core principles, in combination with the mathematical proof that it is impossible to decode a random one-shot key with an equal key and message length [64], an efficient QKD secure key distribution guarantees absolute secrecy between parties. To establish our proof-of-concept on the above characteristics, the communication architecture model in Figure 3 illustrates

this in an overall conceptual simulation model with three main components called quantum blocks (QBs). The QBs represent the transmitter (Alice's QB), the receiver (Bob's QB), and the Eavesdropper block (Eve's QB) as non-authorized access to the quantum channel.

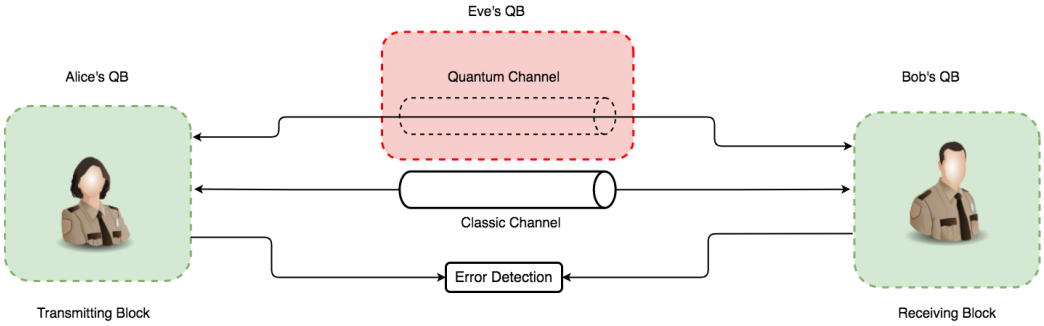

Figure 3. This is a figure representing the base overview of the simulation concept for subsequent simulation iterations.

The overall simulation procedure in Figure 4 describes photon detectors filtering a polarized photon transported in quantum transmission and then rectified by the transmitting parties through bit comparisons, the error detection rate, and error correction. The output is optimized to enhance the security, enabling the total quantum shared key to meet the exact security requirements through a series of privacy amplification processes.

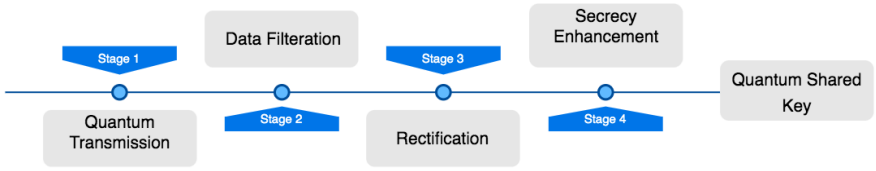

Figure 4. Main simulation procedure.

4.1. Architectural Model

The communication architecture model in Figures 5 and 6 consists of an independent component within each QB with specific code base functionalities. Each QB has a photon-based generator (PG_b) and photon-based encoder/decoder (PE/D_b) component. However, only Parties A and B have a key generator (KG_b) with an output. Two channels operate on different principles: a quantum channel (security based on the laws of nature) and a classic channel (security based on mathematical and computational complexity). The flow and pattern assume Eve's QB can intercept and re-transmit over the quantum channel via intercept-resend attack. This assumption only holds in discussing eavesdropping and its effect on the channel—the error between communicating parties handled via the error detection block. Because Eve's presence requires both a photon-based generator and a photon-based encoder/decoder to perform both re-sending and interception operations, the two arrows leading to the quantum channel in Figure 6 denote that. Bitstreams from Eve's operation can be sent to the receiver via the quantum channel, again with a major advantage for the comparison, effect, and verification of the principal concept that QKD can detect eavesdropping (Eve's quantum block) transmission tampering.

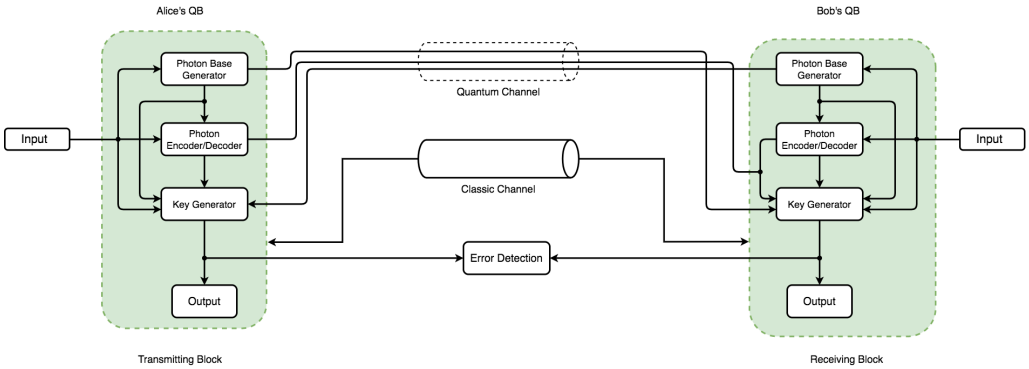

Figure 5. Simulation model design used for simulating an instance without the presence of eavesdropping (Eve's quantum block).

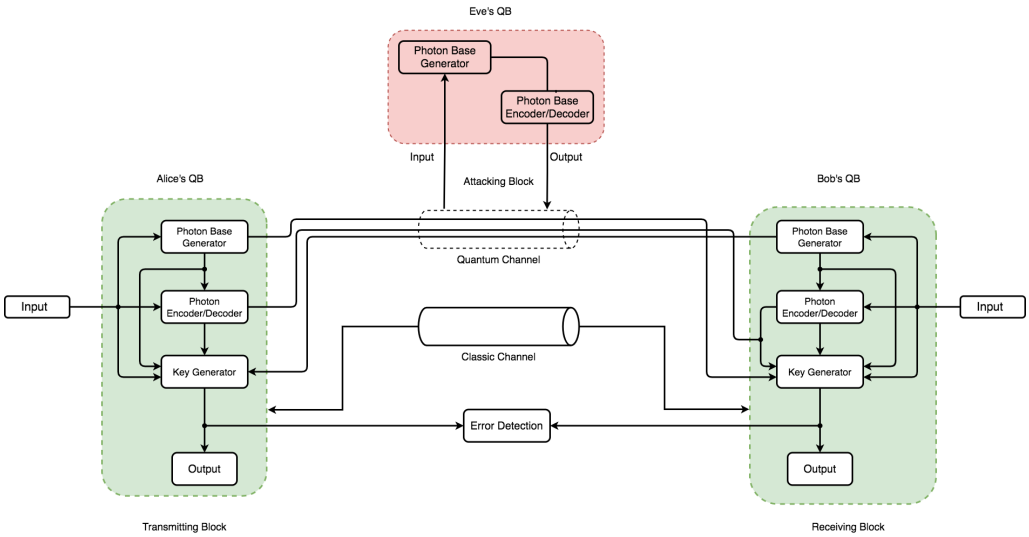

Figure 6. Simulation model design used for simulating an instance with the presence of eavesdropping (Eve's quantum block).

4.2. Implementation

This implementation uses a Linux environment with a significant advantage in its code base and implementation flexibility. It allows the utilization of open-source software libraries and modules. This simulation of the communication architecture model design uses a custom Python3 code base environment as shown in Figure 7. This figure represents the setup configuration of the simulation and development environment. It shows a stack of layers constituting our simulation requirements. The main language framework sits on top of the base operating system (OS) in the base library, while all external language core modules are base dependencies. The custom libraries and dependencies represent the simulation code for this implementation. Each code structure for the classes, functions, and packages follows the same naming convention used in both Figures 5 and 6 to ensure consistency in code flow. For example, a PG_b in Alice's QB would be a single class with subsequent operations divided into functions converted into a custom package. There were two distinct simulation approaches used. The first instance was run without Eve's block as the normal mode of operation in Figure 5, while the second instance in Figure 6 considered the presence of Eve's QB. The algorithms for this implementation are in Algorithm 1.

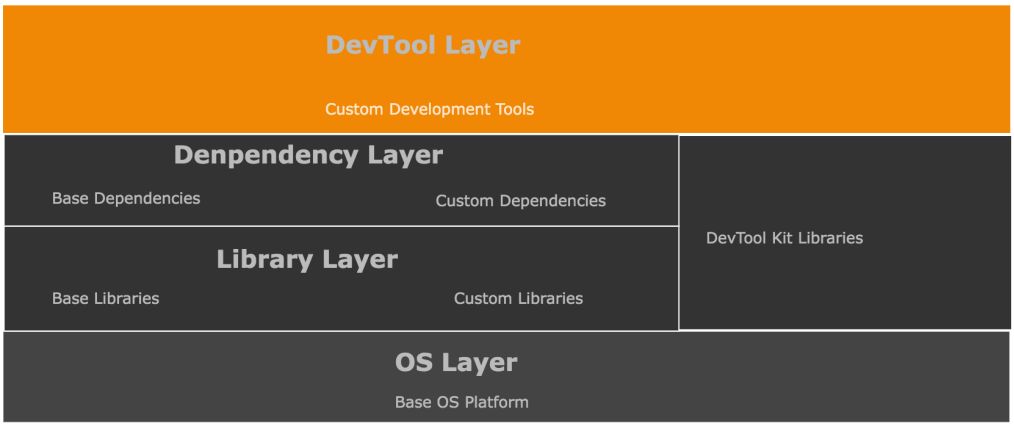

Figure 7. Simulation code base development environment.

Algorithm 1 Custom code simulation using the BB84 protocol.

procedure SIMULATION PROCEDURE
  label: *top*.
  LBR gen ← Lower bound range of bit *Random*
  HBR gen ← Higher bound range of bit *Random*
  Base ← Base *Base-MID gen* – $(0.5x10^{10})$
  if *Base* > *LBR gen* **then return** $|0\rangle$
  end if
  if *Base* < *HBR gen* **then return** $|1\rangle$
  end if
  Assign a polarization base for each iteration of bit
  Assign a polarization state for each iteration of bit
  Compare each parties' generated bit, polarization base, and polarization state
  Calculate mismatch rate, error correction rate, error detection rate, and total error rate
  if *Errorrate* > *error threshold* **then**
    goto *top*.
  else
    Strengthen the final shared key via privacy amplification
  end if
  Final shared key is ready
end procedure

The initial bitstream generation detection occurs during the simulation to know the exact amount of quantum bases for the encoding process. The generation of each bit sent to PG_b undergoes a series of steps. The first step is assessing and evaluating the feeds to know precisely the needed single-photon bases to generate. It randomly assigns a quantum base for each bit separately, either horizontally biased or orthogonally biased. This step is the set polarization base class, which calls a random choice selection on a list containing the quantum base. Each time the set polarization step runs, the bit present at that particular instance is randomly assigned a base. The second step stores output bases iteratively from the previous step in each instance because the results need to reach KG_b.

In the third step (random polarization), each polarized bit from the first step corresponds to a single and specific quantum state ($\uparrow \rightarrow \nwarrow \nearrow$) through a series of decision-making patterns. First, this step checks the polarization bases of the bit and the bit representation agreement between the communication parties beforehand. These parameters determine which quantum state needs assignment for each specific bit and polarization base. The results in this step stay in storage for replication and retrieval. However, the sender side uses PE_b, while the receiver uses the photon-based decoder (PD_b) and vice

versa. PG_b ensures the generation of the corresponding polarization base for the initial series of bits. PE_b continues the step by evaluating the quantum bases from PG_b to encode the bits. This stage checks if the polarization base matches the quantum state of each bit of generated information from Step 1 in PG_b and then outputs the corresponding bit accordingly. To ensure that the data PE_b utilized are precisely from the right source, the method responsible for this operation performs the length, data type, element validation, and assertions before and during code execution.

In a nutshell, the sender and receiver agree on bits that will represent the four quantum states. Afterward, Party A generates random streams of bits and feeds them to the QB to undergo quantum operations. The results are then sent to the receiver (Party B) in the initial stage using a quantum channel. The QB on Party B's side also performs certain quantum operations and outputs the results based on B's measurement criteria. B establishes communication on a classic channel, telling A the polarization bases of the measurement. Party A informs Party B on the same classic channel; the polarization bases are on the single-photon pulses sent. Both the sender and receiver share each other's information without revealing any sensitive information on the classic channel. The exact process can be conversely bi-directional, where the receiver becomes the sender and vice versa. Parties A and B compare the stream of bits with each other's information on the classic channel. The results then become the quantum key if both keys on both sides are equal. The process will start again if the bit error rate exceeds the acceptable threshold value for the QKD communication process.

The KG_b section of the code implementation takes care of the data filtration and rectification processes. KG_b's responsibility is to compare the sender and receiver data to generate the actual key in both halves after taking care of the data filtration and rectification processes. It compares the sender's and receiver's polarization base, measurement base, and stream of bits at each side along with the quantum states. The error detection component of this implementation evaluates the deviations within the streams of bits interchanged between the sender and the receiver. The process ensures the generation of the overall extraction of the quantum shared key. This component includes privacy amplification and other operations relating to the final quantum key.

5. Results and Discussions

The purpose of both simulation scenarios was to give a proof-of-concept of QKD based on the uncertainty and no-cloning principle, showing the advantages of using quantum cryptography for securing Internet communications, platforms, and infrastructures. The results are given in sections regarding the simulation steps and the processes involved. Each subsequent section presents the result in that simulation stage and discusses its significance.

5.1. Communication Phase Results

The simulation models in both Figures 5 and 6 illustrate two communication channels representing class objects. An agreement over a classic channel on the parameters in Table 1 between the sender and receiver occurs. The literature and theoretical study of QKD simulation in practice are affected by error correction [65] factors related to transmission errors, attacks, improper diode pulse configurations, time shifts, imperfect measurements, and other aspects of the overall quantum errors. As a result, the uncertainty accuracy in QKD research simulations ranges from 90 to 99 percent. However, in this work, even though the error threshold with Eve's presence exceeds the threshold, 0.11 was chosen as the error threshold, consistent with the theory and literature [7]. They both do so without revealing any important information. As a result, the sender generates bitstreams and the associated quantum base output in Figure 8 using lower (0.0) and upper (1.0) limits with a precision of ten digits with a bit probability of 0.5. This limit allows the generation of bitstreams for base generation of 50 percent probability of either $|0\rangle$ or $|1\rangle$ per sample instance.

Table 1. Initial parameter used in the simulation.

Parameters	Values
Qubit length (bits)	256
Sender's bit probability	0.5
Receiver's bit probability	0.5
Attacker's bit probability	0.5
Error threshold	0.11
Error detection sample length (bits)	128

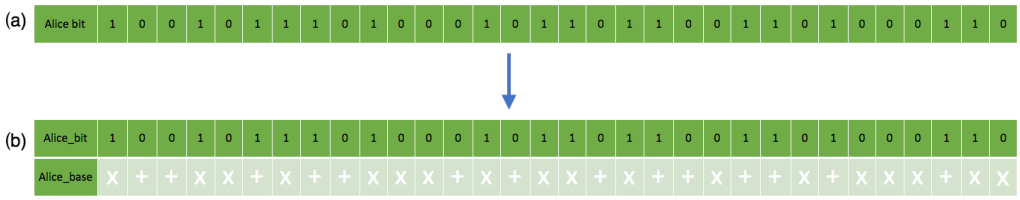

Figure 8. This figure shows bitstreams' generation in the simulation: (**a**) shows the sender's random bitstream. (**b**) shows the sender's random bitstream with the associated polarization states.

Figures 9 and 10 show the randomness of the sender's and receiver's QB qubit generation process for each bitstream, while Figure 11 shows the combination of both qubit generations. This approach mimics the condition in a real photon generator, which is modifiable to produce a desirable single photon. The initial base parameters and values influenced the operation and results of the custom code throughout the simulation.

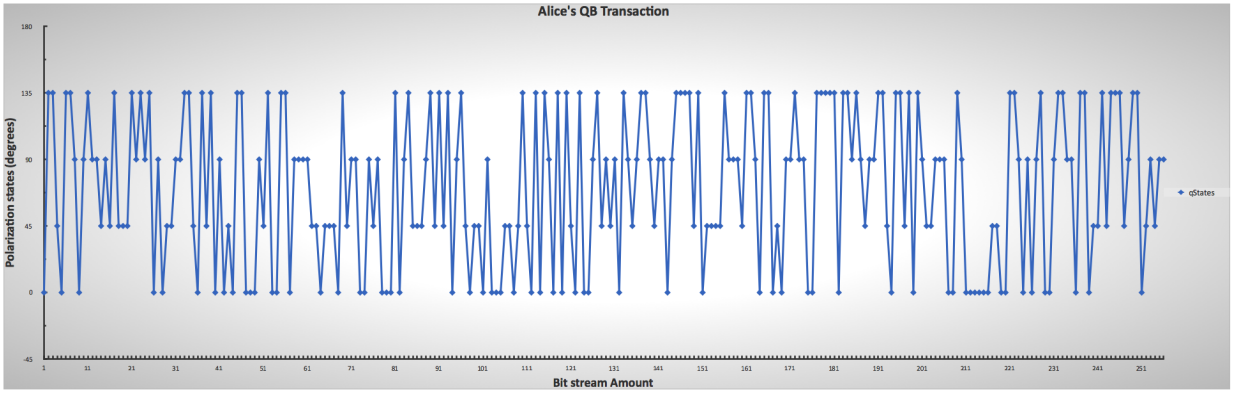

Figure 9. Sender's lower and upper limit ranges for mimicking the chosen photon encoding through polarization, indicating the randomness of Alice's choice.

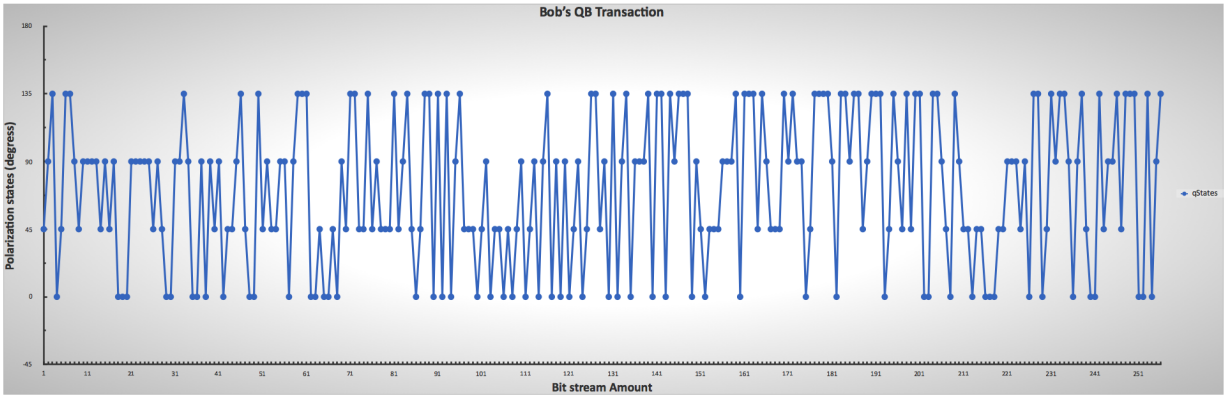

Figure 10. Receiver's lower and upper limit ranges for mimicking the chosen photon encoding through polarization, indicating the randomness of Bob's choice.

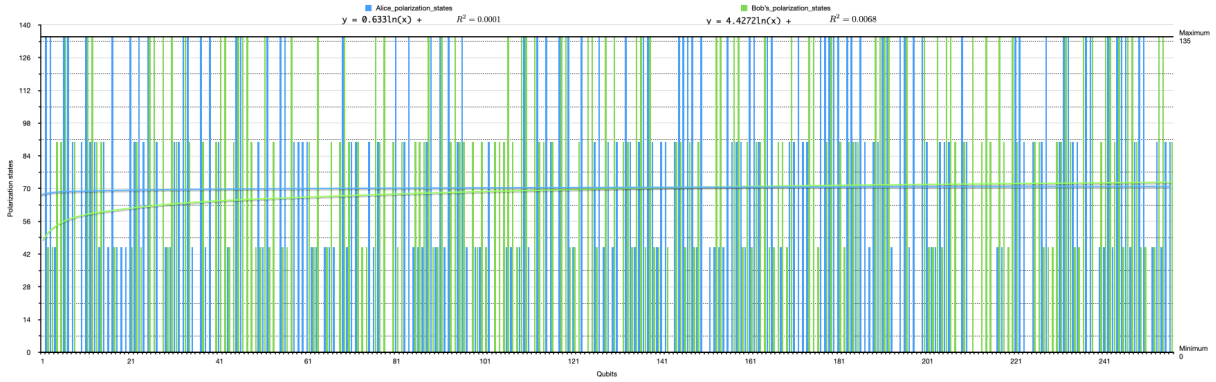

Figure 11. A histogram plot of the sender and receiver in the first simulation instance's (without the presence of Eve) polarization state, indicating the chosen and measured qubits' randomness.

On the receiver's side, the recorded bit and polarizations through measurement sent from the sender in Figure 12 also show their matching polarization states. Figure 12b does not match Figure 8 because of quantum mechanics principles (no-cloning and Heisenberg's uncertainty principle). The receiver measuring all single-photon pulses causes a disturbance, hence the changes in quantum states. The receiver also assumes a random quantum base and polarization quantum state, which reflect the bases below the bit in Figure 8b with the randomness in Figure 10.

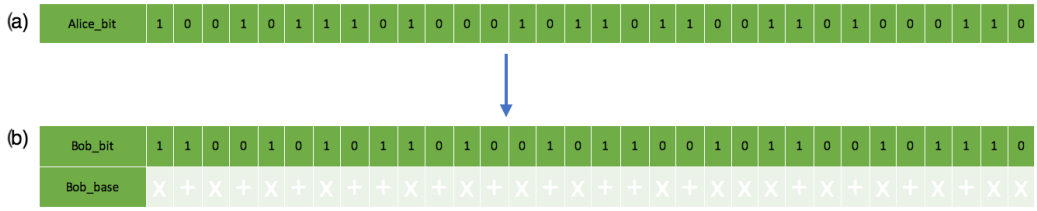

Figure 12. This is a figure showing the chosen bitstreams' comparison: (**a**) Description of the sender's chosen bitstreams. (**b**) Description of the receiver's measurement and chosen bitstream with the associated polarization states.

5.2. Reconciliation Phase Results

Comparing the implementation code and simulation result through the assertion technique ensures each node can identify channel-specific operations in multiple quantum nodes. The quantum measurement bases sent by both parties do not include their corresponding quantum states. The sender and receiver cross-check each other's measurements by eliminating non-matching bases to produce the final result, as shown in Figure 13. Both parties produced approximately 0.546875 mismatches based on base retrieval in the communication channel during the simulation with an eavesdropping rate of 0.04296875 with an error correction rate of 0.2421875. However, it made no significant difference in the simulation re-iterations to the final secret shared key. The total number of bits (shared key) present on both sides after the reconciliation process was 116 out of 256 initial qubits.

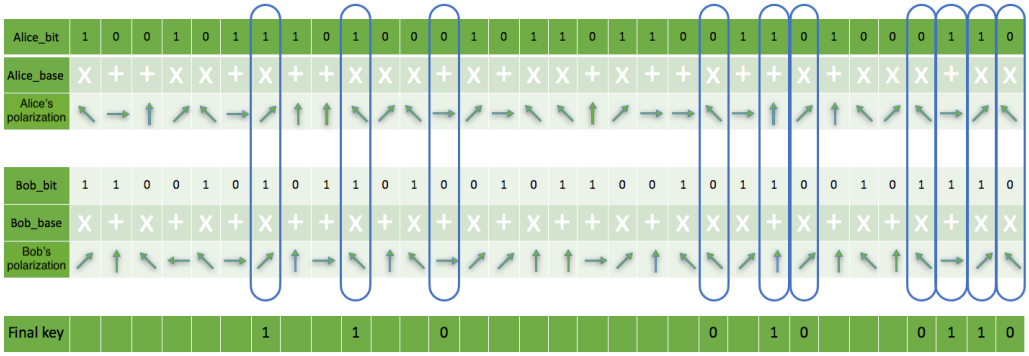

Figure 13. This is a figure showing a sample of the sender and receiver comparing each other's selected results.

5.3. Detection of Eavesdropper

Two types of error-checking operations took place during the simulation. The first error operation relates to each side's qubit error during transmission as transmission errors during communication due to transmission factors such as noise, heat, environmental conditions, and others. The second part of the error process detects eavesdropping on the communication between parties by comparing the sub-keys. It takes a random sample of a specific length selected from the shared keys. A checking process then occurs by comparing if the base matches the initial stream of bits and sent bases for error detection. However, the errors attributed in the simulation by eavesdropping and the transmission processes are considered the same. Therefore, the total errors cannot be greater than the error threshold in Table 1. Figure 14 also shows the randomness of Eve's guessing and chosen measurement during the transmission intercept-resend attack manipulation, while Figure 15 shows all combinations of all parties with the presence of Eve. The results show that an error correction rate of 0.265625 resulted in a variable shared key length out of the initial bits after a base-mismatch, as shown in Figure 16. There was a significant difference in the eavesdropper rate of 0.125 with a total key mismatch of a length of 36 after privacy amplification, shown in Figure 17. Table 2 lists some of the essential values relating to both simulations on the communication architectural model implementation.

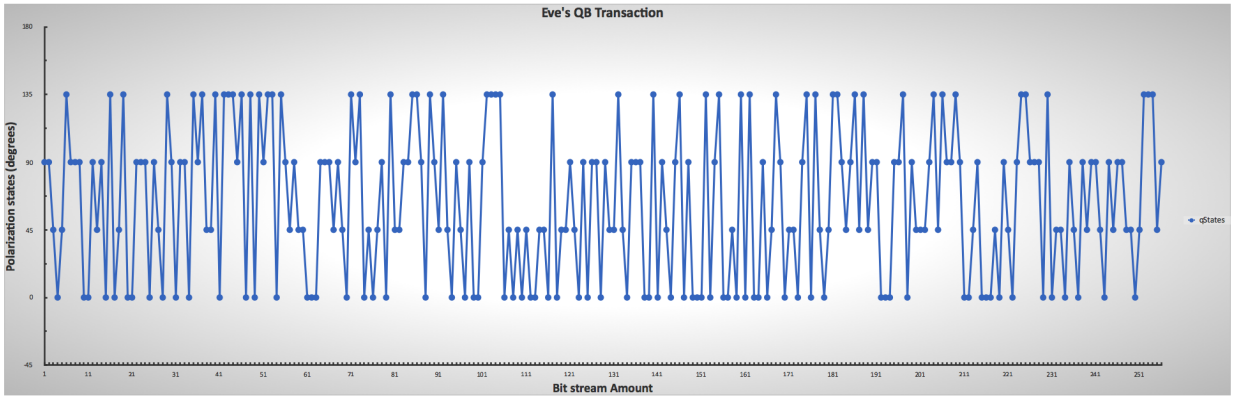

Figure 14. Eve's lower and upper limit ranges for mimicking photon measurement and chosen encoding through polarization, indicating the randomness of Eve's guesses.

Table 2. Comparison of base parameters used and obtained results from the two main simulation instances.

Parameters	Normal	Eavesdropping
Initial bits (bits)	256	256
Final key length (bits)	54	36
Error correction rate	0.2421875	0.265625
Eavesdropper rate	0.04296875	0.125
Party A, B bit probability	0.5	0.5
Eve bit probability	0.5	0.5
Base-mismatch (%)	0.546875	0.5234375

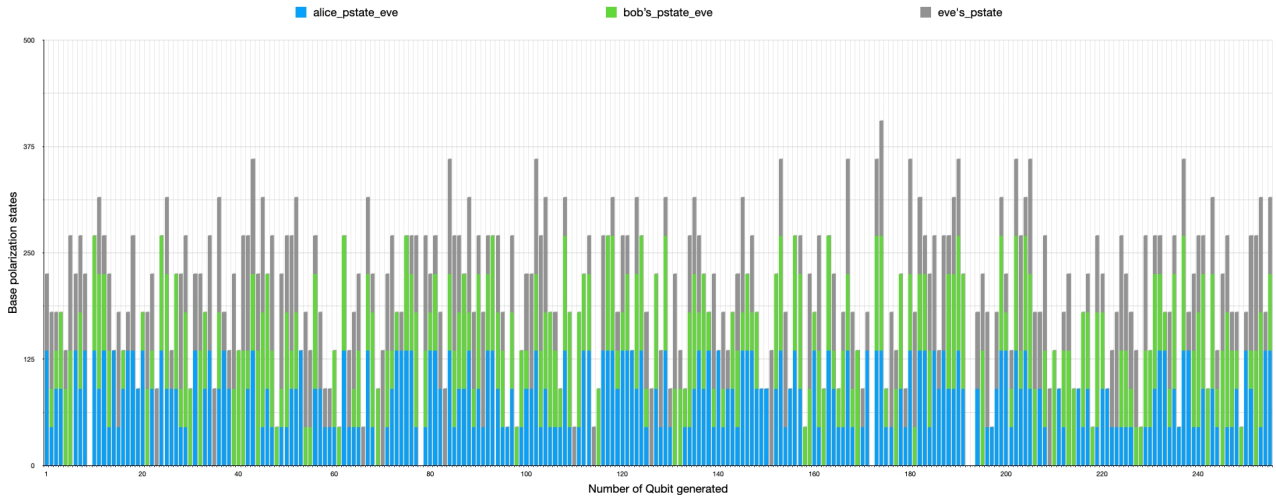

Figure 15. A 2D stacked bar chart with the sender's, receiver's, and Eve's polarization states in the second simulation instance (with the presence of Eve), indicating the chosen and measured qubit randomness.

Communicating Parties	Shared Secret Key
Alice_bit	0 1 0 0 1 1 0 0 1 0 0 0 1 0 0 1 1 0 0 0 0 1 0 1 0 1 0 1 1 1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 1 1 0 1 0 1 1 1 1 1 0 1 1 1 0 0 0 1 1 0 1 0 1 1 1 0 1 1 1 1 0 0 0 1 0 1 1 0 0 0 0
Bob_bit	1 1 1 0 0 0 1 0 1 0 1 0 0 1 1 1 1 0 1 1 0 1 0 0 0 0 1 1 1 0 1 1 0 1 1 1 0 1 1 0 0 0 0 0 0 0 0 0 1 1 0 1 0 0 1 1 0 1 1 0 0 1 0 1 1 0 0 0 1 1 0 0 1 1 1 1 0 1

Figure 16. Sender and receiver final shared key in the reconciliation phase with the eavesdropper's presence.

In Figure 16, the size/length of the two bitstreams is different before privacy amplification because of the presence of Eve. Eve is intercepting the qubit on the quantum channel via intercept-resend attack, either detectable or not, depending on the key length. In this re-iteration simulation, Eve's guess due to chance and probability was not favorable such that the altered and measured qubits by Bob influenced the initial shared key before privacy amplification, visible in the length/size.

Communicating Parties	Shared Secret Key
Alice_final	0 1 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 1 1 0 0 1 1 1 0 1 1 1 1 1 0 1 1 0 0 0
Bob_final	0 1 1 0 1 1 0 1 1 0 1 0 0 0 0 0 0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1 0 1 1 1

Figure 17. Sender and receiver final shared key mismatch with the eavesdropper's presence.

5.4. Privacy Amplification Operations

The operation continues from the detection stage, intending to clean up the information leakage over the channel during the communication operations. The presence of an eavesdropper in a channel attack ensures that the probability of Eve making the right guess is 1/4. Hence, a simple privacy amplification process takes two separate random bits for an XOR operation to reduce the probability. The total number of keys left after privacy amplification is 54 out of 80 in the detection operation. Both sides compare their results, and if their results are the same, the shared key from detection is left untouched; if not, the bit elimination occurs at that specific index.

6. Conclusions

In this work, the communication architecture model and implementation of QKD using the BB84 protocol were presented. This communication architecture focused on the key distribution in python and eavesdropper detection utilizing quantum cryptography to enable secure communication through a proof-of-principle on quantum mechanics laws. The implementation of the model was carried out by developing a python custom base code with its efficiency analyzed through a series of aggregative simulation re-iterations in two scenarios. The communication architecture extended our simulation via modeling to allow the comparison of the initial and final parameters and the overall simulation modeling effect. We then carried out base reconciliation, rectification, and error correction operations on photon transmissions, consistent with the literature and theoretical results.

The first scenario is without the presence of an eavesdropper. It produced an eavesdropper rate of 0.04296875 since all error attributions were cumulative (including transmission, imperfect measurement, and others), with an error correction rate of 0.2421875 and a qubit probability of 0.5. This significantly led to a 54 bit-length shared key.

The second is with the eavesdropper's presence through a methodological interception-resend attack from a practical perspective. Its results demonstrated the possibility of intercepting a quantum transmission via a quantum channel attack introducing a disturbance. However, such activities are detectable via the error rate attributed to transmission and eavesdropping. These rates resulted in a variable shared key length. Hence, the final shared key did not match due to an eavesdropper rate of 0.125 and an error correction rate of 0.265625, significantly more than the initial error threshold with a qubit probability of 0.5.

In some cases, the base-mismatch process discarded about 50 percent of the pre-initial shared key with an error threshold of 0.11 percent. However, it made no significant difference in the simulation re-iterations.

Future works can revolve around the power consumption analysis of the quantum cryptographic process and its deployment in resource-constrained devices without external QKD nodes, but embedded QKD nodes with a significantly improved error correction process.

Author Contributions: Conceptualization, A.A.-K.; formal analysis, A.A.-K.; investigation, A.A.-K.; methodology, A.A.-K.; supervision, E.N. and J.I.; validation, A.A.-K., E.N. and J.I.; visualization, A.A.-K.; writing—original draft, A.A.-K.; writing—review and editing, A.A.-K., E.N. and J.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
V2I	Vehicle-to-Internet
QKD	Quantum key distribution
BB84	Charles Bennett and Gilles Brassard's protocol
QB	Quantum box
PG_b	Photon-based generator
PE/D_b	Photon-based encoder/decoder
PE_b	Photon-based encoder
KG_b	Key-based generator
PD_b	Photon-based decoder

References

1. Dahlberg, A.; Skrzypczyk, M.; Coopmans, T.; Wubben, L.; Rozpundefineddek, F.; Pompili, M.; Stolk, A.; Pawełczak, P.; Knegjens, R.; de Oliveira Filho, J.; et al. A Link Layer Protocol for Quantum Networks Axel. In Proceedings of the SIGCOMM'19: Proceedings of the ACM Special Interest Group on Data Communication, Beijing, China, 19–23 August 2019; pp. 159–173. [CrossRef]
2. Wang, S.; Rohde, M.; Ali, A. Quantum Cryptography and Simulation: Tools and Techniques. In Proceedings of the ICCSP 2020: Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, Nanjing, China 10–12 January 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 36–41. [CrossRef]
3. Corcoles, A.D.; Kandala, A.; Javadi-Abhari, A.; McClure, D.T.; Cross, A.W.; Temme, K.; Nation, P.D.; Steffen, M.; Gambetta, J.M. Challenges and Opportunities of Near-Term Quantum Computing Systems. *Proc. IEEE* **2020**, *108*, 1338–1352. [CrossRef]
4. 360researchreports. Global Quantum Key Distribution Qkd Market and Industry Reports. 2020. Available online: https://www.360researchreports.com/global-quantum-key-distribution-qkd-market-15068633 (accessed on 24 July 2022).
5. Suresh, P.; Daniel, J.V.; Parthasarathy, V.; Aswathy, R.H. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In Proceedings of the 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, India, 27–29 November 2014; pp. 1–8. [CrossRef]
6. Porzio, A. Quantum cryptography: Approaching communication security from a quantum perspective. In Proceedings of the 2014 Fotonica AEIT Italian Conference on Photonics Technologies, Naples, Italy, 12–14 May 2014; pp. 1–4. [CrossRef]
7. Khan, E.; Meraj, S.; Khan, M.M. Security Analysis of QKD Protocols: Simulation and Comparison. In Proceedings of the 2020 17th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 14–18 January 2020; pp. 383–388. [CrossRef]
8. Mandal, B.; Chandra, S.; Alam, S.S.; Patra, S.S. A comparative and analytical study on symmetric key cryptography. In Proceedings of the 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, India, 17–18 November 2014; pp. 131–136. [CrossRef]
9. Wu, C.L.; Hu, C.H. Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application. In Proceedings of the 2012 Third International Conference on Innovations in Bio-Inspired Computing and Applications, Kaohsiung, Taiwan, 26–28 September 2012; pp. 307–311. [CrossRef]
10. Simion, E.; Constantinescu, N.S. Complexity computations in code cracking problems. In Proceedings of the 24th International Spring Seminar on Electronics Technology. Concurrent Engineering in Electronic Packaging. ISSE 2001. Conference Proceedings (Cat. No.01EX492), Calimanesti-Caciulata, Romania, 5–9 May 2001; pp. 225–232. [CrossRef]
11. Sharbaf, M.S. Quantum Cryptography: A New Generation of Information Technology Security System. In Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 27–29 April 2009; pp. 1644–1648. [CrossRef]
12. Sharma, A.; Ojha, V.; Lenka, S. Security of entanglement based version of BB84 protocol for Quantum Cryptography. In Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 9–11 July 2010; Volume 9; pp. 615–619. [CrossRef]
13. Chen, C.Y.; Zeng, G.J.; jhu Lin, F.; Chou, Y.H.; Chao, H.C. Quantum cryptography and its applications over the internet. *IEEE Netw.* **2015**, *29*, 64–69. [CrossRef]
14. Brassard, G. Brief history of quantum cryptography: a personal perspective . In Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Awaji Island, Japan, 16–19 October 2005; pp. 19–23. [CrossRef]
15. Coolman, R. What Is Quantum Mechanics? Scinerds. 2021. Available online: https://scinerds.tumblr.com/post/658075954562908161/what-is-quantum-mechanics-by-robert-coolman (accessed on 24 July 2022).
16. Chris, D. The Famous Physicist Who Discovered Photons. Sciencing. 2019. Available online: https://sciencing.com/famous-physicist-discovered-photons-16203.html (accessed on 24 July 2022).

17. Arthur, C. Famous Scientists. Arthur Compton–Biography, Facts and Pictures. 2018. Available online: https://www.famousscientists.org/arthur-compton (accessed on 24 July 2022).
18. Djellab, R.; Benmohammed, M. Securing Encryption Key Distribution in WLAN via QKD. In Proceedings of the 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Sanya, China, 10–12 October 2012; pp. 160–165. [CrossRef]
19. Shrivastava, A.; Singh, M. A security enhancement approach in quantum cryptography. In Proceedings of the 2012 5th International Conference on Computers and Devices for Communication (CODEC), Kolkata, India, 17–19 December 2012; pp. 1–4. [CrossRef]
20. Pirandola, S.; Andersen, U.L.; 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*, 1012. [CrossRef]
21. Kurochkin, V.L.; Neizvestny, I.G. Quantum cryptography. In Proceedings of the 2009 International Conference and Seminar on Micro/Nanotechnologies and Electron Devices, Novosibirsk, Russia, 1–6 July 2009; pp. 166–170. [CrossRef]
22. Qu, Z.; Ordjevic, I.B. High-speed free-space optical continuous variable-quantum key distribution based on Kramers-Kronig scheme. *IEEE Photonics J.* **2018**, *10*, 1–7. [CrossRef]
23. Sharma, R.D.; De, A. A new secure model for quantum key distribution protocol. In Proceedings of the 2011 6th International Conference on Industrial and Information Systems, Kandy, Sri Lanka, 16–19 August 2011; pp. 462–466. [CrossRef]
24. Gyongyosi, L.; Imre, S. A Survey on quantum computing technology. *Comput. Sci. Rev.* **2019**, *31*, 51–71. [CrossRef]
25. Oszmaniec, M.; Grudka, A.; Horodecki, M.; Wójcik, A. Creating a Superposition of Unknown Quantum States. *Phys. Rev. Lett.* **2016**, *116*, 110403. [CrossRef]
26. Moody, D.; Alagic, G.; Apon, D.C.; Cooper, D.A.; Dang, Q.H.; Kelsey, J.M.; Liu, Y.K.; Miller, C.A.; Peralta, R.C.; Perlner, R.A.; et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
27. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
28. Vignesh, R.S.; Sudharssun, S.; Kumar, K.J. Limitations of Quantum and the Versatility of Classical Cryptography: A Comparative Study. In Proceedings of the 2009 Second International Conference on Environmental and Computer Science, Dubai, United Arab Emirates, 28–30 December 2009; pp. 333–337. [CrossRef]
29. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 839–894. [CrossRef]
30. Shor, P.W.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
31. 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*, 1301–1350. [CrossRef]
32. El Allati, A.; El Baz, M. Quantum key distribution using optical coherent states via amplitude damping. *Opt. Quantum Electron.* **2015**, *47*, 1035–1046. [CrossRef]
33. Liu, S.; Lou, Y.; Chen, Y.; Jing, J. All-Optical Optimal N -to- M Quantum Cloning of Coherent States. *Phys. Rev. Lett.* **2021**, *126*, 60503. [CrossRef] [PubMed]
34. Walton, A.; Ghesquiere, A.; Brumpton, G.; Jennings, D.; Varcoe, B. Thermal state quantum key distribution. *J. Phys. B At. Mol. Opt. Phys.* **2021**, *54*, 185501. [CrossRef]
35. Phattaraworamet, T.; Youplao, P. Double Layers Quantum Key Distribution with Ability to Against PNS Attacks. In Proceedings of the 2019 2nd World Symposium on Communication Engineering, WSCE 2019, Nagoya, Japan, 20–23 December 2019; pp. 1–5. [CrossRef]
36. Miroshnichenko, G.P.; Kozubov, A.V.; Gaidash, A.A.; Gleim, A.V.; Horoshko, D.B. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack. *Opt. Express* **2018**, *26*, 11292. [CrossRef]
37. Fei, Y.Y.; Meng, X.D.; Gao, M.; Ma, Z.; Wang, H. Exploiting wavelength-dependent beam splitter to attack the calibration of practical quantum key distribution systems. *Optik* **2018**, *170*, 368–375. [CrossRef]
38. Pljonkin, A.; Petrov, D.; Sabantina, L.; Dakhkilgova, K. Nonclassical attack on a quantum keydistribution system. *Entropy* **2021**, *23*, 509. [CrossRef]
39. Arteaga-díaz, P.; Cano, D.; Fernandez, V. Practical side-channel attack on free-space QKD systems with misaligned sources and countermeasures. *IEEE Access* **2022**, *4*, 1–11. [CrossRef]
40. Jain, N.; Stiller, B.; Khan, I.; Elser, D.; Marquardt, C.; Leuchs, G. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemp. Phys.* **2016**, *57*, 366–387. [CrossRef]
41. Park, D.; Heo, D.; Kim, S.; Hong, S. Single Trace Attack on Key Reconciliation Process for Quantum Key Distribution. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 21–23 October 2020; Volume 2020-October, pp. 209–213. [CrossRef]
42. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A-At. Mol. Opt. Phys.* **2013**, *87*, 062329. [CrossRef]
43. Huang, J.Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A-At. Mol. Opt. Phys.* **2014**, *89*, 032304. [CrossRef]

44. Wei, K.; Liu, H.; Ma, H.; Yang, X.; Zhang, Y.; Sun, Y.; Xiao, J.; Ji, Y. Feasible attack on detector-device-independent quantum key distribution. *Sci. Rep.* **2017**, *7*, 449. [CrossRef] [PubMed]
45. Dervisevic, E.; Lauterbach, F.; Burdiak, P.; Rozhon, J.; Sl, M. Simulations of Denial of Service Attacks in Quantum Key Distribution Networks. In Proceedings of the 2022 XXVIII International Conference on Information, Communication and Automation Technologies (ICAT), Sarajevo, Bosnia and Herzegovina, 16–18 June 2022.
46. Al-Mohammed, H.A.; Al-Ali, A.; Yaacoub, E.; Abualsaud, K.; Khattab, T. Detecting Attackers during Quantum Key Distribution in IoT Networks using Neural Networks. In Proceedings of the 2021 IEEE Globecom Workshops, GC Wkshps 2021, Madrid, Spain, 7–11 December 2021. [CrossRef]
47. Zhao, W.; Shi, R.; Huang, D. Practical Security Analysis of Reference Pulses for Continuous-Variable Quantum Key Distribution. *Sci. Rep.* **2019**, *9*, 18155. [CrossRef] [PubMed]
48. Pan, Y.; Zhang, L.; Huang, D. Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution. *Appl. Sci.* **2020**, *10*, 7788. [CrossRef]
49. Nandal, R.; Nandal, A.; Joshi, K.; Rathee, A.K. A Survey and Comparison of Some of the Most Prominent QKD Protocols(January 19, 2021). . *SSRN Electron. J.* **2021**. [CrossRef]
50. Morris, J.D.; Hodson, D.D.; Grimaila, M.R.; Jacques, D.R.; Baumgartner, G. Towards the modeling and simulation of quantum key distribution systems. *Dep. Air Force Air Univ.* **2014**, *4*, 47.
51. Lardier, W.; Varo, Q.; Yan, J. Quantum-sim: An open-source co-simulation platform for quantum key distribution-based smart grid communications. In Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October 2019; pp. 1–6. [CrossRef]
52. Aji, A.; Jain, K.; Krishnan, P. A Survey of Quantum Key Distribution (QKD) Network Simulation Platforms. In Proceedings of the 2021 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 1–3 October 2021; Volume 16; pp. 1–8. [CrossRef]
53. Quantum Key Distribution. 2022. Available online: https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html (accessed on 24 July 2022).
54. Jasim, O.K.; Abbas, S.; El-Horbaty, E.S.M.; Salem, A.B.M. Quantum Key Distribution: Simulation and Characterizations. *Procedia Comput. Sci.* **2015**, *65*, 701–710. [CrossRef]
55. Buhari, A.; Zukarnain, Z.A.; Subramaniam, S.K.; Zainuddin, H.; Saharudin, S. An efficient modeling and simulation of quantum key distribution protocols using OptiSystem™. In Proceedings of the 2012 IEEE Symposium on Industrial Electronics and Applications, Bandung, Indonesia, 23–26 September 2012; pp. 84–89. [CrossRef]
56. Kohnle, A.; Rizzoli, A. Interactive simulations for quantum key distribution. *Eur. J. Phys.* **2017**, *38*, 35403. [CrossRef]
57. Chatterjee, R.; Joarder, K.; Chatterjee, S.; Sanders, B.C.; Sinha, U. Qkd S im, a simulation toolkit for quantum key distribution including imperfections: Performance analysis and demonstration of the B92 protocol using heralded photons. *Phys. Rev. Appl.* **2020**, *14*, 24036. [CrossRef]
58. Mogos, G. Quantum key distribution—QKD simulation. In Proceedings of the 18th Conference of Quantum Information Processing, Sydney, Australia, 10–16 January 2015.
59. Shajahan, R.; Nair, S.S. Simulation of BB84 Protocol over Classical Cryptography Channel for File Transfer. *Int. Res. J. Eng. Technol. IRJET* **2020**, *7*, 1029–1035.
60. Sethia, A.; Banerjee, A. A MATLAB-based modelling and simulation package for DPS-QKD. *J. Mod. Opt.* **2022**, *69*, 392–402. [CrossRef]
61. Kashyap, M.R. QKD Algorithm BB84 Protocol in Qiskit. *Int. Res. J. Eng. Technol.* **2020**, *7*, 2623–2626.
62. Mina, M.Z.; Simion, E. A Scalable Simulation of the BB84 Protocol Involving Eavesdropping. In *Innovative Security Solutions for Information Technology and Communications*; Springer: Cham, Switzerland, 2021; pp. 91–109. [CrossRef]
63. Fan-Yuan, G.J.; Chen, W.; Lu, F.Y.; Yin, Z.Q.; Wang, S.; Guo, G.C.; Han, Z.F. A universal simulating framework for quantum key distribution systems. *Sci. China Inf. Sci.* **2020**, *63*, 180504. [CrossRef]
64. Kurochkin, V.L. Protocols for quantum cryptography. In Proceedings of the 2011 International Conference and Seminar of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM), Erlagol, Altai, 30 June–4 July 2011; pp. 114–115. [CrossRef]
65. Swan, M.; Witte, F.; dos Santos, R.P. Quantum Information Science. *IEEE Internet Comput.* **2022**, *26*, 7–14. [CrossRef]