Comparative Analysis of BB84 and E91 Quantum Cryptography Protocols

Murat BAYRAM[1*], Elif Ilgaz ÇAĞLAYAN[2]

[1] *Department of Mathematics, Bilecik Şeyh Edebali University, Bilecik, Turkey,* ***ORCID:*** *0009-0000-0296-7125*
[2] *Department of Mathematics, Bilecik Şeyh Edebali University, Bilecik, Turkey,* ***ORCID:*** *0000-0002-4202-6570*

Article Info

Oral Presentation

Doi: 10.5281/zenodo.14316751

Keywords

Quantum Cryptography
Quantum Key Distribution Protocols
BB84 Protocol
E91 Protocol
Bell's Inequality
Entanglement

Abstract

In this study, the BB84 and E91 quantum cryptography protocols are comparatively analyzed. The BB84 protocol, based on the fundamental principles of quantum mechanics, enables secure key exchange and is more widely used in practice due to its simpler implementation requirements. The E91 protocol, on the other hand, theoretically provides superior security by employing the violation of Bell's inequality and entanglement, but it faces practical challenges, such as maintaining entangled states over long distances. The paper presents a mathematical analysis of both protocols, comparing factors such as error rates, key generation rates, and security conditions. In conclusion, it is noted that while BB84 is more feasible in practical applications, E91 provides stronger theoretical security.

Introduction

Quantum Key Distribution (QKD) is an innovative technique developed in the field of quantum cryptography, aiming for higher security compared to traditional cryptographic methods. Conventional cryptographic protocols rely on the complexity of solving difficult mathematical problems to ensure security; an example of this is the factorization of large prime numbers. Although these problems are considered unsolvable with classical computers, advancements in quantum computing pose a threat to the security of these traditional methods.

In contrast, the security foundation of QKD is based on the fundamental principles of quantum mechanics. Heisenberg's Uncertainty Principle and the no-cloning theorem of quantum states are the primary security-guaranteeing principles in this domain. Specifically, these principles ensure that, during the quantum key distribution process, any attempt by an eavesdropper (commonly referred to as Eve) to extract information from the system can be detected. This is due to the fact that, according to the principles of quantum mechanics, any attempt to measure the state of a qubit inevitably disturbs that state and disturbance that can be observed by both parties in communication (Alice and Bob).

One of the most well-known QKD protocols, the BB84 protocol, was proposed by Bennett and Brassard in 1984 [1]. This protocol is based on encoding quantum bits across four different quantum states, chosen from two different bases. Consequently, since a potential eavesdropper would not know which basis to measure in, any intrusion attempt can be detected. Another significant QKD protocol, the Ekert91 (E91) protocol, was developed by Ekert in 1991 [6]. The E91 protocol uses the principle of quantum entanglement, based on Bell's theorem, to enable key distribution. While offering a more complex structure compared to BB84, this protocol provides a stronger security infrastructure due to the inherent verification mechanisms found in quantum entanglement.

Both theoretical and practical applications of QKD are realized by integrating it with cryptographic methods such as one-time pad encryption and hashing schemes. The one-time pad, mathematically proven to provide unconditional security, maximizes the security level, as each key generated through QKD is used only once. This integration contributes to the superiority of quantum cryptography over classical cryptography in terms of both security and practicality.

I. Theoretical Framework

With advancing technology, increased computational power and newly discovered vulnerabilities, some well-known traditional cryptographic algorithms have lost their reliability. For instance, the Data Encryption Standard (DES), a symmetric key encryption algorithm, was once widely used. However,

* Corresponding Author: murat.bayram.1@ogr.iu.edu.tr
Tel.: +90 530 392 96 11

due to its short 56-bit key length, it was vulnerable to brute-force attacks. In 1999, the Electronic Frontier Foundation (EFF) developed a machine called Deep Crack that could break DES in less than a day. MD5 was a widely used cryptographic hash function, but in 2004, it was demonstrated to be vulnerable to collision attacks [18]. Similarly, SHA-1 is another cryptographic hash function that was broken through collision attacks. In 2017, Google and CWI Amsterdam announced the first practical collision attack on SHA-1 [16]. In 2020, the factorization of RSA-250 was reported [3]. Although the security of these algorithms has been compromised, the computational power required remains high. For example, the factorization of RSA-250, broken in 2020, was achieved using approximately 2700 CPU core-years, with a 2.1 GHz Intel Xeon Gold 6130 CPU used as a reference [3].

Today, over 50 companies are developing six different types of quantum computers. **Table 1** shows eight of the leading companies and the types of quantum computers they are developing.

Superconducting Qubits: Made from superconducting materials that operate at extremely low temperatures, these qubits exhibit nearly zero electrical resistance. This property allows them to produce highly precise electrical currents and microwaves, thereby enabling the encoding of quantum states [5]. Superconducting qubits offer high precision, fast processing times, scalability with a large number of qubits, good error tolerance, and robust quantum operations. However, the need for complex cooling systems and technical challenges are considered drawbacks.

Ion Trap: Ion trap technology uses a system in which positively charged atomic ions are trapped using electromagnets and lasers [8]. These ions act as qubits for the quantum computer. The energy levels of the ions are controlled by laser beams, and these energy levels represent quantum information. Ion traps offer high error tolerance, long quantum coherence times, and high accuracy. However, the need for appropriate laser systems for interactions between qubits, along with the complexity and large-scale nature of the equipment, are considered disadvantages.

Quantum Annealing: Quantum annealing is a quantum computing method designed to solve optimization problems by minimizing energy levels to find solutions [7]. Quantum annealers achieve problem-solving by utilizing quantum effects such as superposition and tunneling. They are especially suited for optimization problems and can be effective in certain industrial applications; however, their general quantum computing capabilities are limited.

Topological Qubits: Topological qubits aim to provide error tolerance for quantum computers. These qubits encode quantum information in topologically protected states, preserving specific quantum states against local disturbances within the system. They have the potential for high error tolerance and long coherence times; however, as they are still in the developmental phase [11], practical applications remain limited.

Photonic Qubits: Photonic quantum computers transmit quantum information through light photons [15]. The quantum states of photons are encoded using the properties of light waves. Photonic qubits, typically generated with lasers, are suitable for long-distance quantum communication and can process information at high speeds. However, their production processes are challenging, and maintaining the quantum states of photons poses difficulties.

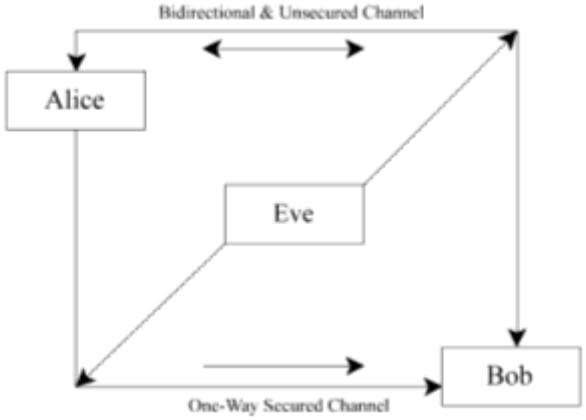
Table 1. Companies and types of computers developed

Company	Computer Type
IBM	Superconducting Qubits
Google	Superconducting Qubits
Microsoft	Topological Qubits
Rigetti Computing	Superconducting Qubits
D-Wave Systems	Quantum Annealing
IonQ	Ion Trap
Alibaba	Superconducting Qubits and Ion Trap
Honeywell	Ion Trap

II. Quantum Key Distribution Protocols

Quantum cryptography has three main entities: Alice (sender), Bob (receiver), and Eve (eavesdropper). Their communication structure is generally shown in **Figure 1**.

Figure 1. BB84 protocol communication table example



Through a bidirectional, unsecured channel, Alice and Bob share the bases they use. Alice sends a message to Bob over a one-way secured channel, with Eve's goal being to intercept the messages without Alice or Bob's knowledge. Quantum cryptographic protocols leverage certain fundamental principles of quantum mechanics, namely:

Superposition Principle: In quantum mechanics, a system can exist in multiple states simultaneously. For example, a

qubit can be in both |0⟩ and |1⟩ states at once. The superposition of a qubit is represented as shown in Eq. 2.1

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad 2.1$$

where α and β are complex numbers that satisfy the condition:

$$|\alpha|^2 + |\beta|^2 = 1 \qquad 2.2$$

Measurement Principle: When a quantum system is measured, it loses its superposition and collapses to a specific state. Measuring a qubit forces it to assume one of the states between |0⟩ and |1⟩.

Entanglement Principle: Two or more quantum systems can become entangled, at which point they cannot be treated independently. Entanglement is essential for ensuring the security of quantum cryptographic protocols.

III. BB84 Protocol

This protocol, introduced by Charles Bennett and Gilles Brassard in 1984, was the first quantum key distribution (QKD) protocol.

The BB84 protocol uses single photons to transmit a secret key composed of random bits. Each photon is polarized in one of four possible states, corresponding to one of two conjugate bases. These bases are defined as the linear basis for vertical and horizontal polarization and the diagonal basis for +45° and -45° polarization. The quantum states used in the BB84 protocol are represented in Dirac notation as follows:

Linear Basis:	$\|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad \|1\rangle = \begin{pmatrix}0\\1\end{pmatrix},$	3.1
Diagonal Basis:	$\|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad \|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	3.2

The BB84 protocol proceeds in the following steps:

1. Alice selects a bit string composed of 0s and 1s. For example, let her select the sequence: 0, 1, 1, 0, 0, 1, 0, 1.
2. For each bit, Alice randomly selects a basis. For the linear basis, 0 and 1 bits are polarized as horizontal |0⟩ and vertical |1⟩, respectively. Similarly, for the diagonal basis, 0 and 1 bits are polarized as +45° |+⟩ and -45° |−⟩ let her basis choices be: +, ×, +, ×, +, ×, +, ×, +.
3. Alice encodes each bit in the selected basis and sends the resulting quantum states to Bob.
4. For each photon received from Alice, Bob randomly selects a basis. Let his basis choices be: +, +, +, ×, ×, +, +, ×.
5. Bob measures each photon in his chosen basis and records the bit values obtained. If Bob's basis matches Alice's, he measures the correct bit value.
6. Alice and Bob share their basis choices over a secure channel, but they do not share the bit values.
7. Alice and Bob retain only those bits for which they used the same basis; these bits form the secure key.

Table 2. BB84 Protocol Communication Table example

	1	2	3	4	5	6	7	8
Alice's Bases	+	×	+	×	+	×	+	×
Alice's Bits	|0⟩	|−⟩	|1⟩	|+⟩	|0⟩	|−⟩	|0⟩	|−⟩
Bob's Bases	+	+	+	×	×	+	+	×
Bob's Bits	|0⟩	|0⟩	|1⟩	|+⟩	|−⟩	|1⟩	|0⟩	|−⟩
Protect Bits	Yes	No	Yes	Yes	No	No	Yes	Yes
Protected Bits	0		1	0			0	1

Measurements made with different bases are discarded since they produce random results due to the quantum superposition principle. Qubits measured with the same basis, on the other hand, form the building blocks of the secure key. The security stems from the "measurement disturbance" principle, which is a fundamental principle of quantum mechanics. When a third party, Eve, attempts to monitor the qubits, it changes the quantum states of the qubits, leading to an error that Alice and Bob can detect. In this way, the BB84 protocol provides a significantly higher level of security from an information-theoretic perspective compared to classical encryption methods, mathematically guaranteeing communication privacy based on the principles of quantum mechanics [2].

One of the most critical metrics of security in the BB84 protocol is a parameter known as the Quantum Bit Error Rate (QBER).

$$QBER = \frac{N_{error}}{N_{total}} \qquad 3.3$$

Here, N_{error} represents the number of errors, N_{total} denotes the total number of qubits. QBER measures the discrepancy between sent and received qubits, where a lower QBER indicates a higher security of the key. Factors affecting QBER include noise in quantum channels, imperfections in physical devices, and eavesdropping attempts by potential adversaries.

Studies have shown that the BB84 protocol is considered secure with a QBER of up to 11% [19]. However, if the error rate exceeds 25% [11] (this limit can be reduced to 19.7% through certain methods [20]), it is assumed that the protocol's security is compromised. A QBER of 25% or higher implies that an eavesdropper (Eve) has interfered with the quantum channels, successfully intercepting or manipulating a significant portion of the qubits.

The key generation rate (or key rate) of the BB84 protocol determines the amount of secure data the system can generate. This rate is directly related to the error rate and other difficulties in the channel. Mathematically, the secure key rate is often expressed by the following formula:

$$R = Q \cdot [1 - h(e)] \quad 3.4$$

Where R represents the secure key rate, Q is the transmission rate of qubits, and e denotes the error rate. The term h is a function associated with Shannon entropy and is defined as:

$$h(e) = -e\log_2(e) - (1-e)\log_2(1-e) \quad 3.5$$

This formula illustrates that as the error rate increases, the secure key rate decreases [12].

For the security of the BB84 protocol, achieving a low QBER and, accordingly, a high secure key rate is essential.

IV. E91 Protocol

The E91 protocol, proposed by Artur Ekert in 1991, is a quantum key distribution (QKD) protocol based on the fundamental principles of quantum mechanics [6]. Unlike previous protocols like BB84, it relies on quantum entanglement and Bell's theorem. Alice and Bob use entangled pairs to generate a secure key. These entangled pairs typically exist in specific quantum superposition states known as Bell states. The four Bell states are defined as follows:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad 4.1$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad 4.2$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad 4.3$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad 4.4$$

These four Bell states indicate that two qubits are entangled, with the differences depending on whether the qubits are in the same or opposite states. In the E91 protocol, the state $|\psi^-\rangle$ is typically used, though other Bell states can also be utilized based on similar principles. In classical systems, the Bell parameter S has a maximum value of 2. However, in quantum entangled states, this parameter can reach up to $2\sqrt{2}$

The Bell parameter S is calculated as follows:

$$S = E(\theta_A, \theta_B) - E(\theta_A, \theta'_B) + E(\theta'_A, \theta_B)E(\theta'_A, \theta'_B) \quad 4.5$$

Here, $E(\theta_A, \theta_B)$ represents the correlation of Alice's and Bob's measurements at angles θ_A and θ_B, defined as:

$$E(\theta_A, \theta_B) = P(\text{Alice} = \text{Bob}|\theta_A, \theta_B) - P(\text{Alice} \neq \text{Bob}|\theta_A, \theta_B) \quad 4.6$$

Where $P(\text{Alice} = \text{Bob}|\theta_A, \theta_B)$ represents the probability that Alice and Bob obtain the same result, and $P(\text{Alice} \neq \text{Bob}|\theta_A, \theta_B)$represents the probability of obtaining different results. According to quantum mechanics, the value of the Bell parameter S lies within the range:

$$2 < |S| \leq 2\sqrt{2} \quad 4.7$$

This range indicates the presence of quantum entanglement and implies that a classical eavesdropper (Eve) cannot passively monitor the protocol [6].

In the E91 protocol, communication proceeds as follows:

1. Alice and Bob receive pairs of entangled qubits tosend to each other. These entangled qubits are typically in Bell states. When Alice's qubit takes on a particular state, Bob's qubit will correspondingly take a determined state.
2. Alice and Bob randomly select bases to measure the qubits. The bases are defined as:

$$|0\rangle_Z = |0\rangle, \quad |1\rangle_Z = |1\rangle \quad 4.8$$

$$|+\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad 4.9$$

3. Alice and Bob perform measurements in the selected bases. If they choose the same basis, the qubit measurement results will be fully correlated. For example, if Alice measures $|0\rangle$, then Bob will measure $|1\rangle$. The correlation function is defined in Eq 4.6.
4. Alice and Bob compare their basis choices via a classical communication channel. During this step, they share only the bases they used—not the state of the qubits. If they chose the same basis, the measurement results are kept; if different, those results are discarded.
5. They calculate the security parameter S Equa 3.1 to test whether the protocol is secure.
6. They combine the secure measurement results to form a raw key. These bits, derived from same-basis measurements, comprise the raw key. Due to quantum channel

noise, unnoticed errors, or Eve's possible tampering, error correction is required.

7. Error Correction and Privacy Amplification are then applied to reduce Eve's possible information and increase the security of the raw key. Privacy amplification uses an universal hash function to make the key shorter but secure. For a raw key of length n, if Eve's information is estimated to be m bits, Alice and Bob extract a secure key of length n – m [13].

An universal hash function h(x) can be expressed as:

$$h(x) = \left(h_1(x), h_2(x), \dots, h_k(x)\right) \qquad 4.10$$

8. After Privacy Amplification, Alice and Bob obtain a final secure key, which can be used in various cryptographic applications, such as One-Time Pads (OTP) or symmetric encryption algorithms like AES or DES.
9. If a sufficiently long and secure key is not obtained in the first round, Alice and Bob repeat the protocol as needed. This repetition depends on noise levels and error rates in the quantum channel. With each protocol iteration, the length of the final secure key grows.

Each of these steps ensures the security of the E91 protocol, which builds on quantum mechanics principles beyond classical cryptography.

Similar to the BB84 protocol, the quantum bit error rate (QBER) for the E91 protocol is a critical parameter. Unlike BB84, it considers coincidence events from the simultaneous triggering of two detectors, which includes both real coincidences and false coincidences.

The coincidence probability, P_c, is divided into:

P_t = the probability of true coincidences from entangled photon pairs.
P_f = the probability of false coincidences from factors like single photon detections or dark counts.

The total coincidence probability is given by:

$$P_c = P_t + P_f \qquad 4.11$$

QBER is then expressed as [17]:

$$QBER = \frac{(P_f / 2 + \mu P_t)}{P_c} \qquad 4.12$$

A critical aspect of the E91 protocol is the secure key generation rate. This rate determines how much secure data the protocol can produce and is directly related to the QBER (Quantum Bit Error Rate). Mathematically, the secure key generation rate can be expressed as:

$$R = S \times (1 - 2 \times QBER) \qquad 4.12$$

Here, R represents the secure key rate, and S denotes the efficiency derived from the violation of Bell's inequality. This rate indicates that as the error rate increases, the secure key generation rate decreases. However, effective testing of Bell inequalities and management of error rates allow the E91 protocol to function securely.

V. Conclusion and Future Work

The BB84 and E91 protocols provide high levels of security in the field of quantum cryptography, proven mathematically. The BB84 protocol facilitates secure key distribution by using the polarization states of qubits based on the principles of quantum superposition and measurement disturbance. The polarization bases and Dirac notation employed in the protocol are fundamental for accurately measuring quantum states and detecting eavesdropping attempts. The E91 protocol, on the other hand, offers a more complex but highly secure key distribution method using Bell inequalities and entangled qubit pairs. This protocol achieves a higher level of security than classical systems through the Bell parameter S. Mathematically, a Bell parameter in the range $2 <| S |\leqslant 2\sqrt{2}$ demonstrates the existence of quantum entanglement and guarantees security theoretically. While both protocols provide high security, BB84 is simpler and more suitable for widespread use. E91 may be better suited for entanglement-based applications.

Future research could explore the performance of these protocols under various quantum attack scenarios and in more complex quantum networks, providing a deeper understanding of quantum cryptographic technologies.

It is essential to study the security performance of the BB84 and E91 protocols in noisy quantum channels and under different error rates [4]. In particular, integrating these protocols with quantum error correction algorithms and modeling these processes mathematically is crucial for evaluating security and efficiency. Quantum information theory and entropy-based security analyses play a critical role in this context.

Additionally, it is necessary to assess the security of both

protocols against emerging quantum computing technologies mathematically [14]. Specifically, the impact of quantum algorithms such as Shor's and Grover's algorithms should be analyzed by integrating these effects into the security structures of the protocols. The focus of future research should include the design of new protocols that are more resilient against such attacks and their mathematical validation [9].

Declaration of Ethical Standards

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission

VI. Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

VII. Acknowledgements

This study is supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) 2210-A Program and constitutes part of a master's thesis.

VIII. References

[1] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, *560*, 7-11.
[2] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, *85*(2), 441.
[3] Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., & Zimmermann, P. (2020). Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II 40* (pp. 62-91). Springer International 19Publishing.
[4] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner
Rev. Mod. Phys. 86, 419 – Published 18 April 2014; Erratum Rev. Mod. Phys. 86, 839 (2014)
[5] Devoret, M. H., & Schoelkopf, R. J. (2013). Superconducting circuits for quantum information: an outlook. *Science*, *339*(6124), 1169-1174.
[6] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67*(6), 661-663.
[7] Farhi, E., & Gutmann, S. (1998). Quantum annealing in the transverse Ising model. *Physical Review E*, *58*(5), 5355-5363.
[8] Kielpinski, D., Monroe, C., & Wineland, D. J. (2002). Architecture for a large-scale ion-trap quantum computer. Nature, 417, 709-711.
[9] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38–41.
[10] Nayak, C., Simon, S. H., Stern, A., Freedman, M., & Das Sarma, S. (2008). Non-Abelian anyons and topological quantum computation. *Reviews of Modern Physics*, *80*(3), 1083–1159.
[11] Gottesman, D., Lo, H. K., Lütkenhaus, N., & Preskill, J. (2004). Robustness of the BB84 quantum key distribution protocol against general coherent attacks. *arXiv preprint* arXiv /0403148.
[12] Vaitiekėnas, S., Winkler, G., Karzig, T., & von Oppen, F. (2021). Protocol to identify a topological superconducting phase in a three-terminal device. *arXiv preprint* arXiv:2103.12217
[13] Lim, C. C. W., Curty, M., Walenta, N., Xu, F., & Zbinden, H. (2010). Secure key rate of the BB84 protocol using finite sample bits. *Journal of Physics A: Mathematical and Theoretical*, *43*(49), 495302.
[14] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, *81*(3), 1301–1350
[15] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, *85*(2), 441–444
[16] O'Brien, J. L., Furusawa, A., & Vučković, J. (2019). Photonic quantum information processing: A concise review. *Applied Physics Reviews*.
[17] Stevens, M., Karpman, P., & Peyrin, T. (2017). The first collision for full SHA-1. In *Advances in Cryptology – CRYPTO 2017* (pp. 570–596). Springer.
[18] Bennink, R. S., Bentley, S. J., & Boyd, R. W. (2002). Security of quantum key distribution with entangled photons against individual attacks. *Physical Review A*, *65*(5), 052310.
[19] Qi, B., Lamas-Linares, A., & Lo, H. K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*,
[20] Wang, X., Yin, Z. Q., & Zhou, Z. (2004). Collisions for hash functions MD4, MD5, HAVAL-128, and RIPEMD. In *CRYPTO'04* (pp. 575-592). Springer.
[21] Qi, B., Lamas-Linares, A., & Lo, H. K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, *12*(11), 113026