Journal of Physics: Conference Series **2980** (2025) 012038 doi:10.1088/1742-6596/2980/1/012038

# Development of Quantum Key Distribution (QKD) with E91 Protocol for Future Secure Quantum Networks

**Muhammad Fajri Zulfa and Khoirul Anwar**

[1] The University Center of Excellence for Advanced Intelligent Communications (AICOMS), Telkom University, Bandung, Indonesia
[2] Research Collaboration Center for Quantum Technology 2.0 (PKR Kuantum 2.0), Labtek V, ITB, Bandung, Indonesia

E-mail: mfajrizulfa@student.telkomuniversity.ac.id, anwarkhoirul@telkomuniversity.ac.id

**Abstract.** This paper investigates practical performances of the Ekert 91 protocol (E91) for future secure quantum networks. To seek future possible improvement, we investigate the important different principles of E91 and Bennet-Brasard (BB84) protocols. We perform a series of computer simulations to evaluate the performances of them and investigate the practical parameters. Furthermore, we simulate the E91 protocol using real-world practical scenarios involving eavesdropping and quantum channel errors. We present two scenarios: (1) the performance with eavesdropper interception under a perfect channel and (2) the performances with eavesdropper interception combined with channel errors. We found that: (i) the E91 protocol produces fewer keys compared to the BB84 protocol but does not require verification between two parties, (ii) the E91 protocol enhances security due to the utilization of Clauser, Horne, Shimony, and Holt (CHSH) inequality, and (iii) both eavesdropper and channel errors can impact the less production of keys obtained during the keys production.

## 1. Introduction

Questions about cyber security and consumer privacy have become critical with the emergence of communications systems [1]. All of the communications systems require highly advanced security. Failure in the system could cause serious disruptions to essential service at any time. Classical cryptography is widely used in today's telecommunication systems, but it faces new threats from quantum computers, which are still rapidly developing. The RSA algorithm, currently used in practice, can be broken by quantum algorithms [2]. On the 5G and 6G future communications, quantum is one of the focusing study to give everything services with fast speed [3–5]. Quantum communications provides higher capacity, greater security, and lower latency, requiring quantum cryptography to support these needs [6]. Quantum cryptography is grounded in the principles of quantum mechanics and relies on the laws of physics to ensure secure communications. The main aim of quantum cryptography is to achieve information security and figure out any eavesdroppers in the communications channel.

Quantum Key Distribution (QKD) addresses security challenges for future applications in the sixth generation of telecommunications (6G) 2030 by leveraging entanglement and quantum teleportation. The E91 protocol, based on entanglement, is one such QKD method. Entanglement swapping, a fascinating

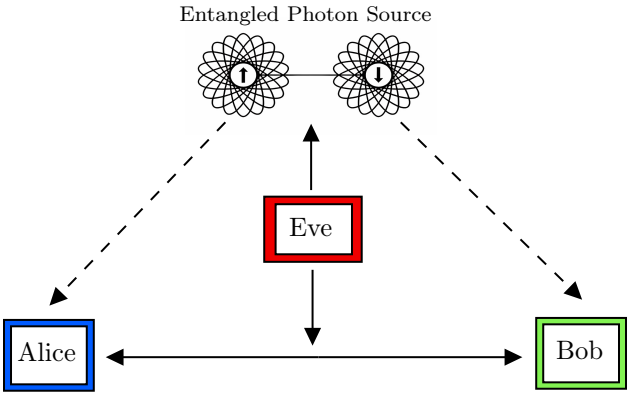



Fig. 1. QKD based on entanglement in quantum communications systems.

phenomenon in quantum mechanics, involves manipulating entangled particles like Einstein-Podolsky-Rosen (EPR) pairs [7], which can generate sequences of random bits in two remote locations. QKD uses this concept for key exchange, ensuring secure communications between distant nodes. The E91 protocol exemplifies that how quantum entanglement and measurement can enhance security in communications. Fig. 1 shows that how QKD serves as a key for secure communications through quantum mechanics. The E91 protocol, devised by Artur Ekert in 1991, is a notable quantum key distribution method that utilizes quantum entanglement and measurements to ensure the secure exchange of cryptographic keys. This protocol is particularly robust against attacks, guaranteeing a high level of security.

Several developments of E91 protocols have been conducted and reported. Authors in [8] developed E91 protocol for long distances communications. Authors in [9] explore a generalization of Ekert quantum cryptographic protocol, where qubits are substituted with qudits, which are systems of $N$- or $d$-dimensions. Authors in [10] developed E91 protocol with generated on demand by a quantum dot. Authors in [11] reviews security of E91 protocol with several attacking strategies. Authors in [12] proposed two new protocol inspired from E91 protocol for improving efficiency key exchange. Authors in [13] investigated of strength of E91 QKD protocol. In securities issue era, several developments for developing E91 QKD protocol have been developed to solve classical cryptography problem and security for entanglement communications. In the era of securities issues, several advancements have been made to develop the E91 QKD protocol to address the challenges of classical cryptography and enhance security for entanglement-based communications. In addition to these efforts, Authors in [14] proposed the utilization of quantum cryptography with two non-orthogonal states, while Authors in [15] introduced the concepts of anonymous-key quantum cryptography and unconditionally secure quantum bit commitment.

This paper investigates the impact of practical performance factors on the keys production in the E91 protocol. Our analysis evaluates more real-world scenario, providing insights into how practical challenges. On the other hand, this paper also clarifies the final key of keys productions process in the E91 protocol and BB84 in [16], and elaborates on the differences between them. We also develop E91 protocol to detailed investigation of the E91 protocol performance in the presence of eavesdropper interception and erroneus channels. Therefore, in this paper, we focus on the performance evaluation to the real-world scenario of the E91 protocol by doing a series computer sumulation. We also analyze the impact of eavesdropper interception and erroneus channels, which is widely regarded as the most adverse case in QKD or quantum communications.

## 2. Method and Scenario

Quantum cryptography in the E91 protocol is based on Bell theorem and entanglement. Introduced by Artur Ekert in 1991, this protocol employs the concept of entangled quantum particles to detect eavesdropping attempts. This approach makes E91 a highly secure QKD method, with the strength of its security rooted in the non-locality properties of quantum mechanics.

### *2.1. Quantum Gates*

Quantum gates are the basic components of quantum circuits. Quantum bits or qubits, can be in a superposition of states, unlike classical bits. In this study, We utilize several quantum gates expressed

Table 1. Bell States in E91 protocol.

| In | Out |
|---|---|
| $\|00\rangle$ | $(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$ |
| $\|01\rangle$ | $(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$ |
| $\|00\rangle$ | $(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$ |
| $\|00\rangle$ | $(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$ |

mathematically as

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathbf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{1}$$

The Hadamard gate, represented by $\mathbf{H}$ in (1), is an essential single-qubit gate in quantum computing. It converts the basis states $|0\rangle$ and $|1\rangle$ into equal superpositions. The CNOT gate in (1) performs a NOT operation on the target qubit (qubit 2) only when the control qubit (qubit 1) is in state $|1\rangle$. It is pivotal for creating entanglement and implementing conditional operations in quantum circuits. Other utilize gates in this paper are Pauli matrices, which are expressed as

$$\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{2}$$

The Gate $\mathbf{Z}$, also called the Pauli-$Z$ gate in (2), applies a phase flip by altering the sign of the second qubit state. Specifically, it leaves the state $|0\rangle$ intact and changes the sign of $|1\rangle$, converting it to $-|1\rangle$. The Gate $\mathbf{X}$ or the Pauli-$X$ gate performs a bit flip by swapping the states $|0\rangle$ and $|1\rangle$. It acts like a classical NOT gate flipping the qubit state.

The Gate $\mathbf{Y}$ or the Pauli-$Y$ gate combines a flip in the bit and a flip in the phase. The Pauli-$Y$ adds a complex phase factor. It maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$, where $i$ is the imaginary unit. Alice and Bob measurement bases are linear combinations of the Pauli matrices $\mathbf{X}$ and $\mathbf{Z}$ normalized by $\frac{1}{\sqrt{2}}$ expressed mathematically as

$$\mathbf{W} = \frac{\mathbf{X} + \mathbf{Z}}{\sqrt{2}}, \quad \mathbf{V} = \frac{-\mathbf{X} + \mathbf{Z}}{\sqrt{2}}. \tag{3}$$

In the E91 protocol, these gates are used to define the measurement bases and simulate the erroneus channels for real-world E91 protocol scenarios.

### *2.2. Bell States or EPR Pair*

Entanglement is a situation where two objects influence each other no matter how far the distance between the two objects. In mathematical, the states are entangled when if there is no factorization as expressed as

$$\alpha|10\rangle + \beta|11\rangle = |1\rangle(\alpha|0\rangle + \beta|1\rangle) \text{ (not entangled);} \tag{4}$$

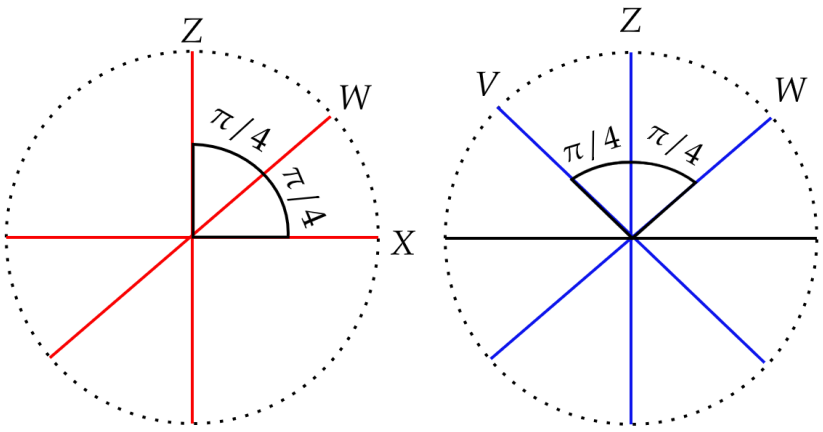
$$\alpha|00\rangle + \beta|11\rangle \text{ (entangled).} \tag{5}$$

These Bell States can be generated using quantum circuits and are represented as shown in Table 1.

### *2.3. CHSH Inequality*

John Stewart Bell, in his groundbreaking work [17], introduced a mathematical framework to differentiate the forecasts of quantum mechanics from local hidden variable theories, encapsulated in Bell inequality. The measurement results for two particles are given by $A(\vec{a}, \lambda) = \pm 1$ and $B(\vec{b}, \lambda) = \pm 1$, where $A$ for particle 1 is independent of the setting $\vec{b}$ for particle 2, and the reverse. The expectation value of the product of the two measurements is

$$P(\vec{a}, \vec{b}) = \int d\lambda \, \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda), \tag{6}$$




(a) (b)

Fig. 2. The use of (a) Alice measurement angle $\phi_a^i = \{0, \frac{1}{4}\pi, \frac{1}{2}\pi\}$ and (b) Bob measurement angle $\phi_b^j = \{\frac{1}{4}\pi, \frac{1}{2}\pi, \frac{3}{4}\pi\}$.

where $\rho(\lambda)$ defines the probability distribution of the hidden variable $\lambda$.

The CHSH inequality is a specific formulation of bell inequality, developed by John Clauser, Michael Horne, Abner Shimony, and Richard Holt (CHSH). It provides a way to test the predictions of quantum mechanics in the context of entangled particles. The CHSH inequality is expressed as

$$\langle S\rangle = |E(A_1B_1) + E(A_1B_2) + E(A_2B_1) - E(A_2B_2)| \leq 2, \tag{7}$$

where $A_i$ and $B_j$ represent measurement settings chosen by two observers (Alice and Bob) and $E(A_iB_j)$ represents the expectation value of the product of measurements taken along settings $A_i$ and $B_j$. Specifically, $E(A_iB_j)$ describes the average value of the product of outcomes from Alice measurement at setting $A_i$ and Bob's measurement at setting $B_j$. We use $E$ because the outcomes of the measurements are discrete rather than continuous as assumed in (6). For any classical system governed by local hidden variables, this inequality sets an upper bound of 2 for the combined correlation. However, quantum mechanics, due to the phenomenon of entanglement, allows for the maximal violation of this inequality. Specifically, for the quantum mechanical scenario, the $\langle S\rangle$ value is calculated as

$$\langle S\rangle = \langle \mathbf{Z}\otimes\mathbf{W}\rangle + \langle \mathbf{Z}\otimes\mathbf{V}\rangle + \langle \mathbf{X}\otimes\mathbf{W}\rangle - \langle \mathbf{X}\otimes\mathbf{V}\rangle = 2\sqrt{2}. \tag{8}$$

Thus, we obtain $\langle S\rangle = 2\sqrt{2}$, which clearly violates the CHSH version of bell inequality in (7).

Violation in (8) benefit for security of the E91 protocol to detect an eavesdropper. The security of the E91 protocol is deeply rooted in CHSH inequality. If an adversary like Eve attempts to gain knowledge of the keys by performing measurements on the entangled particles, her intervention would inevitably disturb the quantum system, leading to a drop in the CHSH value to below the quantum bound of $2\sqrt{2}$. Thus, the CHSH inequality acts as an additional safeguard, ensuring the security of keys production.

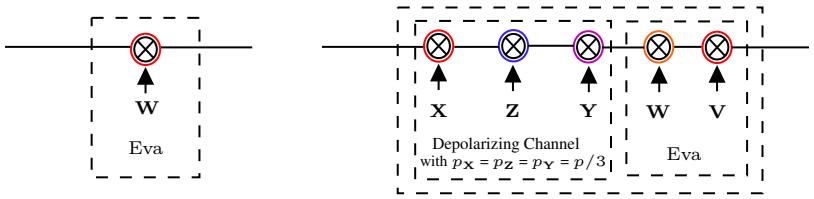
### *2.4. The E91 Protocol*

In this section, we provide a summary on how the E91 protocol works. Bases in this protocol refers to quantum gates for generate quantum state. The gates are uses is **Z**, **X**, **W** and **V**. These gates are used for bases measurement. Steps for constructing a simple E91 protocol are as follows:

- The E91 protocol uses entangled states, where in this paper, we use singlet state of

$$|\Phi^+\rangle = \frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}}. \tag{9}$$

- A trustful source generates pairs of $\frac{1}{2}$-spin particles in a singlet or an entangled state and sends them to Alice and Bob.




(a) (b)

Fig. 3. Channel simulations scenario for (a) the performance with eavesdropper interception under a perfect channel and (b) the performances with eavesdropper interception under the erroneus channels.

- Of each particle, Alice and Bob measure an observable, chosen randomly and independently from each other from a set of complementary attributes.
- Alice measures with angles $\phi_a^i = \{0, \frac{1}{4}\pi, \frac{1}{2}\pi\}$ or similar to $\{\mathbf{X}, \mathbf{W}, \mathbf{Z}\}$ as shown in Fig. 2(a), while Bob measures with $\phi_b^j = \{\frac{1}{4}\pi, \frac{1}{2}\pi, \frac{3}{4}\pi\}$ or similar to $\{\mathbf{W}, \mathbf{Z}, \mathbf{V}\}$ as shown in Fig. 2(b).
- Each random measurements can result in a spin state of +1 (spin up) or -1 (spin down), whereby they show an correlation coefficient E of a certain observable to have a certain value calculated by

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j). \tag{10}$$

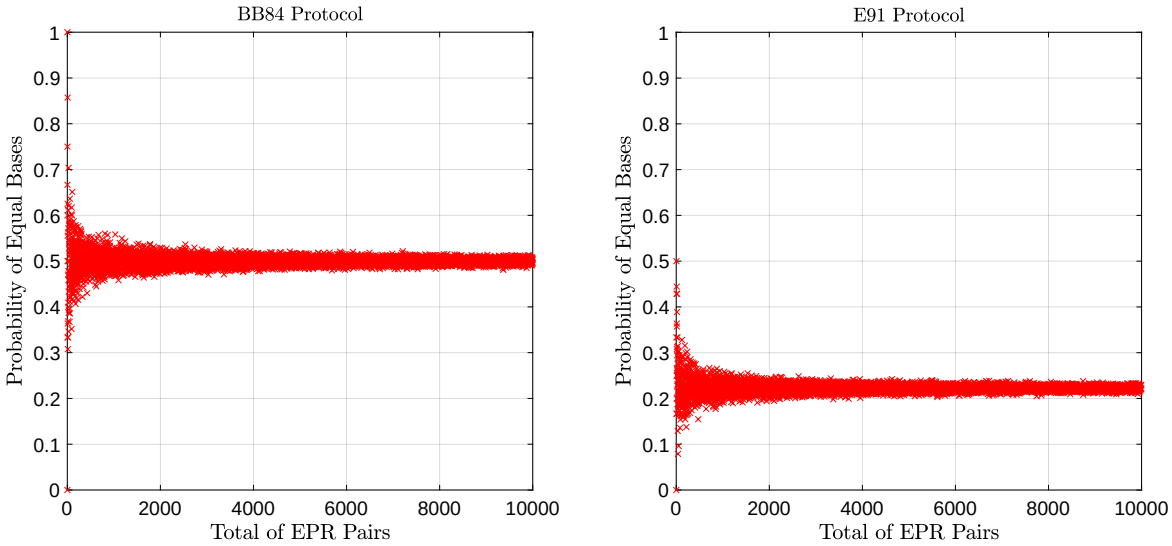
- After that, they exchange the bases of their measurement over the public channel and divide the results in two groups:
  - one with according bases
  - one with disaccording bases
- The ones with according bases determine the key as they are perfectly correlated (which means they have the exact value) due to their entangled state expressed as

$$E(a_2, b_1) = E(a_3, b_2) = 1. \tag{11}$$

- The disaccording particles can still be used to test either Eve listens to the qubits on the quantum channel or not.
- The Bell inequality is able to test the presence of an eavesdropper.
- The protocol uses a variant in [18] to test the presence of an eavesdropper.
- Alice and Bob can now exchange the disaccording particles openly (over the public channel), since they do not participate in the composition of the key.
- These values determine whether or not $S$ is fulfilled.
  - if so, an entangled state is present and the key derived from the group of corresponding result is legitimate
  - if not, Eve may have altered some or all of the particles and the key is not secure.

*2.5. Scenario of E91 Protocol with Eavesdropper under Erroneous Channels*

In this subsection, we explore two scenarios of practical parameters in potential vulnerabilities in the E91 protocol as shown in Figs. 3(a) for perfect channels and 3(b) for erroneous channels. These scenarios examine the impacts of eavesdropping and channel errors on secure communications. The E91 protocol relies on entangled quantum states to facilitate secure key exchange between Alice and Bob. However, these entangled states are susceptible to interference from eavesdroppers and simultaneously can be disrupted by errors in the communication channel. Here, we discuss how these vulnerabilities affect the reliability of keys production and compromise the security of the exchange process.




(a) (b)

Fig. 4. Probability of resulted keys from: (a) BB84 protocol and (b) E91 protocol.

*2.5.1. Scenario with Eavesdropper Interception under Perfect Channels*
In this scenario, we consider the E91 protocol in the involvement of an eavesdropper. The E91 protocol is simulated with a perfect channel, where no transmission errors occur. A trusted source generates 10,000 blocks of entangled qubits. Each blocks contains 100 pairs represented as $L$. The total number of keys production per set for E91 protocol is expected to be $3L$ assuming that 1 EPR pair represent 1 classical bit.[1] Eve is intercepting the communications channel between Alice and Bob. The initial steps for constructing the protocol remain the same as described in the previous subsection. A trustfull source generates entangled states and one qubit from each entangled pair is sends to Alice while the other is sends to Bob. However, in this scenario, Eve intercepts the qubits being sent to Alice as shown in Fig. 3(a). After intercepting, Eve measures the qubits and then sends her own qubits to Alice, attempting to remain undetected. Despite Eve interception, Alice and Bob proceed with the protocol as usual, they measure their qubits using randomly chosen measurement bases and subsequently share their measurement results over a public channel. To detect the presence of Eve, Alice and Bob compare a subset of their bases measurement results. in this results, we analyze a deviations from the key production due to the eve interception.

*2.5.2. Scenario with Eavesdropper Interception Combined under the Erroneus Channels*
In this scenario, we extend the E91 protocol to account for both the involvement of an eavesdropper and the emergence of depolarizing errors within the communications channels between Alice and Bob, as shown in Fig. 3(b). The same entangled state parameters are used: 10,000 blocks, 100 pairs per block, and a total of 300 keys per set. The initial steps for constructing the protocol remain consistent with the previous subsections. A trusfull source generates entangled states. From each pair, one qubit is directed to Alice and the other to Bob. During the transmission, the channel is considered the worst-case scenario because $p_X = p_Z = p_Y = \frac{p}{3}$, representing equal error probabilities for all axes. Simultaneously, Eve intercepts the qubits on both channels, measures them, and resends them in an attempt to remain undetected. Intercept and error can happen on either or both. Despite these challenges, Alice and Bob proceed with the protocol as usual. They measure their qubits using randomly chosen measurement bases

[1]The standard ASCII system uses 7 bits per character. However, in practice, ASCII typically employs 8 bits (1 byte) for simplicity and compatibility. For example, a password consisting of 8 characters would require 8 bytes. Using 8 bits per character, the total size for such a password would be 64 bits. In this simulation, each EPR pair represents 1 classical bit. Given that the E91 protocol achieves a success rate of 22 %, a block of 100 pairs yields approximately 22 bits. Consequently, to generate a password requiring 64 bits, at least 3 blocks are needed, calculated as $64/22 = 2.9$, which is rounded up to 3 blocks.

Table 2. The differences of E91 and BB84 protocols.

| BB84 | E91 |
|---|---|
| Polarization state of a single photon | Polarization state of two entangled photons |
| Need to verify between two parties | No need to verify between two parties |
| Probability of same basis of resulted key much more than E91 | Probability of same basis of resulted key is very small |
| Unable to detect unauthorized interception | Capable to detect unauthorized interception |
| Lower than E91 for high security and much more time consumption than E91 | Maintaining security and minimizing time consumption. |
| BB84 use single particle but vulnerable of a few attack (like Photons Number Splitting) | E91 leverages the CHSH inequality to offer extra layer security. |
| The implementation of BB84 protocol more viable | E91 protocol faces technological difficulties of computing resources. |

and then publicly share a subset of their measurement results. By analyzing these results, we can detect deviations from the key production due to both the channel errors and Eve interception.

## 3. Simulation Results and Analysis

In this section, we demonstrate and analyze the findings from the simulation. We begin by demonstrating a computer simulations of the keys production process in the E91 protocol. Then we delve into a comparative analysis of the E91 and BB84 protocols. We also highlight their respective strengths and weaknesses as well as the resulted keys from each. Finally, we explore the effects of eavesdropping and channel errors on the E91 protocol. Beside that, we also provide insights into how these challenging communications conditions influence key distribution and the overall robustness of the system.

### *3.1. Resulted Key*

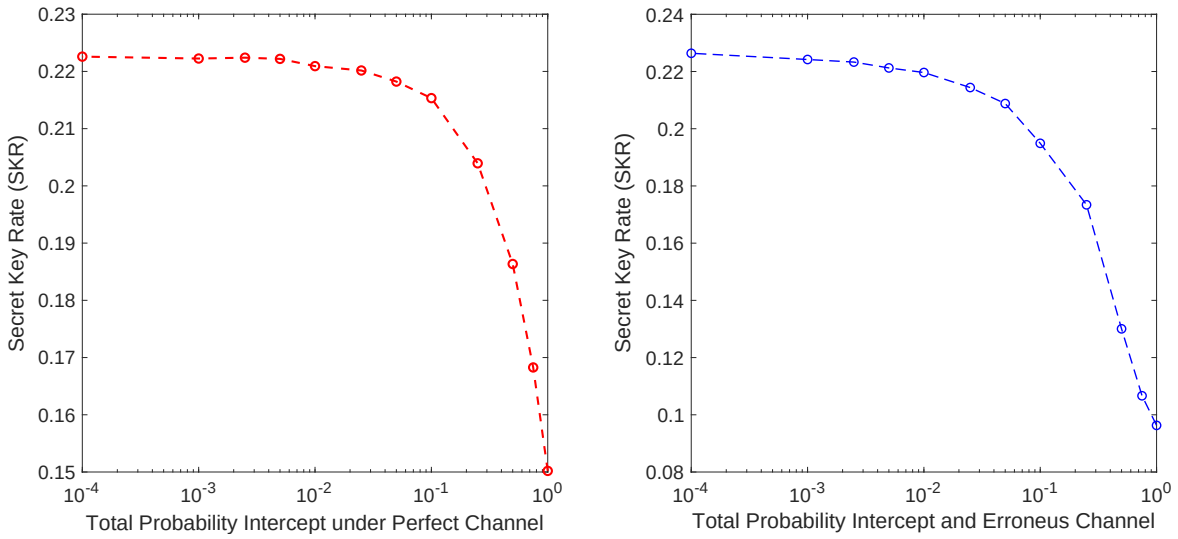
A notable difference is the final key rate for the E91 protocol as depicted in Fig. 4(b). This result indicates a probability of around $\frac{2}{9}$ for choosing equal measurement bases. This reflects thorough verification steps that enhance security by detecting eavesdropping through entangled states, albeit at the cost of a lower resultant key. Conversely, the BB84 protocol shown in Fig. 4(a) stabilizes at a probability of $\frac{1}{2}$ for equal measurement bases. This sign give a more straightforward and efficient resultant key. However, this simplicity makes BB84 slightly less robust against eavesdropper interception compared to E91. These parameters underscore the importance of selecting the appropriate protocol based on specific communications needs and balancing the requirements for security, speed, and final key efficiency.

### *3.2. Comparison of The BB84 and E91 Protocols*

the E91 and BB84 protocols exhibit notable differences in their approach to security and efficiency. One of the key distinctions is the type of quantum states employed. The E91 protocol leverages the entangled states of particles, which inherently provide stronger security features due to their sensitivity to external disturbances. In contrast, BB84 uses single-particle polarization states, which, while easier to implement, offer less robustness in revealing the presence of an eavesdropper.

A significant advantage of the E91 protocol lies in its ability to detect eavesdropping through quantum entanglement correlations. The protocol applies the CHSH inequality to test for deviations from the expected quantum correlations between the entangled particles. Any violation of these correlations serves as a direct indicator of tampering, making E91 highly effective in identifying potential threats. This contrasts with BB84, which requires statistical post-processing to infer the likelihood of an eavesdropper's presence, leading to potential delays and higher risks of undetected intrusion during transmission.

An important aspect to highlight is that the E91 protocol does not require verification between two parties, contributing to reduced time for practical implementations. However, this efficiency comes at a cost. Unlike E91, the BB84 protocol cannot inherently detect the presence of an eavesdropper and relies on statistical post-processing to infer whether communications have been compromised. BB84 involves the exchange of verification information, adding to the overhead of the key exchange process. However, this efficiency in E91 comes with the tradeoff of a lower probability of basis alignment for keys production




(a) (b)

Fig. 5. The performances of secret key rate to total probability of (a) intercept under perfect channel and (b) both interception and erroneus channels.

due to the randomness of entanglement measurements, which could lead to delays and a higher risk if an eavesdropper is manipulating the transmission.

The E91 protocol has a lower probability of measurement basis alignment in keys production due to the use of the CHSH inequality. Its reliance on entanglement and the CHSH inequality provides stronger protection against eavesdropping compared to the BB84 protocol, where bases are chosen independently, resulting in higher alignment and efficiency. Additionally, the BB84 protocol is particularly susceptible to Photon Number Splitting (PNS) attacks. This vulnerability arises because, in BB84, an eavesdropper can leverage multi-photon signals to gather partial knowledge about the keys without revealing their presence. In contrast, the quantum correlations in the E91 protocol make such attacks more difficult to perform without detection, enhancing the protocol's overall security.

However, practical implementation of the E91 protocol in real-world scenarios presents certain challenges. One of the primary constraints is the hardware requirement. Quantum entanglement-based systems, like those needed for E91, require more advanced and sensitive equipment, such as entanglement sources and detectors with high precision and low noise. These systems are more expensive and complex than those used for BB84, which can rely on relatively simpler single-photon detectors. Furthermore, E91's reliance on entanglement makes it more susceptible to environmental noise, such as photon loss and decoherence over long distances, which can significantly degrade the quality of the entangled states and compromise the security of the transmission. To address these issues, potential practical applications include the use of integrated photonic circuits to simplify hardware [19], superconducting nanowire detectors to enhance detection efficiency [20], polarization-maintaining fibers to mitigate environmental interference [21], and error correction algorithms [22]. Furthermore, investing in scalable sources of entangled photons, leveraging shared research infrastructure, and developing hybrid protocols that integrate quantum and classical systems can optimize practicality and scalability [23].

In summary, the E91 protocol offers enhanced security due to its reliance on quantum entanglement and the CHSH inequality, providing more robust detection of eavesdropping compared to BB84. While BB84 may be more efficient in terms of basis alignment and practical for a broader range of applications, it lacks the inherent security advantages of E91, especially in real-time eavesdropping detection. The choice between E91 and BB84 ultimately depends on the specific priorities of the application, whether the focus is on maximizing security or optimizing time and computational resources. Additionally, hardware requirements and environmental noise tolerance are critical factors in determining the practical viability of the E91 protocol in real-world networks.

### *3.3. The Performances of Secret Key Rate to Total Probability of Intercept under Perfect Channel*

The secret key rate (SKR) performance is strongly influenced by the probability of interception, which reflects the likelihood of a successful eavesdropping attempt on the quantum communication channel. In Fig. 5(a), the x-axis represents the total probability of interception under ideal (perfect) channel conditions, while the y-axis shows the resulted SKR. This figure reveals that at low intercept probabilities (approximately $10^{-4}$ to $10^{-2}$), the SKR remains consistently high at around 0.22, indicating that the protocol is resilient to minor interceptions. However, once the probability of interception rises above $10^{-2}$, the SKR starts to decline noticeably. This sharp decline highlights the balance between maintaining a high SKR and tolerating higher interception probabilities. At intercept probabilities nearing 1, the SKR decreases significantly to around 0.15, underscoring how high intercept levels can severely compromise the protocol's efficiency in generating secure keys. This relationship emphasizes the need to minimize interception probability to preserve a robust SKR and ensure protocol effectiveness.

### *3.4. The Performances of Secret Key Rate to Total Probability of Eavesropper Interception and Erroneus Channels*

The combined impact of interception probability and channel errors is crucial in assessing the overall performance of the QKD protocol. Minimizing both factors is essential to maintain the integrity and security of keys production in practical applications. In Fig. 5(b), the x-axis represents the combined probability of interception and channel errors, while the y-axis displays the corresponding SKR. At low combined probabilities (approximately $10^{-4}$ to $10^{-2}$), the SKR is stable and high, around 0.22, suggesting that the protocol can withstand minor errors and interceptions with minimal performance loss. However, as the probability of combined interception and error surpasses $10^{-2}$, the SKR declines more steeply than in the perfect channel scenario, indicating that errors further degrade protocol performance. As this probability approaches 1, the SKR drops to approximately 0.09, demonstrating that both interception and channel errors critically reduce the protocol's effectiveness in generating secure keys. This finding underlines the importance of controlling both interception and error rates to maintain a high SKR, essential for effective protocol performance in real-world conditions.

## 4. Conclusion

In this paper, we have investigated and compared the E91 and BB84 protocols to evaluate their practical performances for future secure quantum networks. We have demonstrated a series of computer simulations of: (1) probability of resulted keys from E91 and BB84 protocol and (2) the performance of secret key rate to total probability of: (a) intercept under perfect channel and (b) both interception and erroneus channels. The key findings from our study are: (i) the E91 protocol produced fewer keys with small probability compared to the BB84 protocol, which had a keys production probability of higher. However, the E91 protocol does not require verification between the communicating parties, (ii) the E91 protocol enhances security due to its utilization of the CHSH inequality, which provides a stronger basis for detecting eavesdropping, and (iii) both eavesdropper interception and quantum channel errors significantly impact keys generation when the error probability exceeds certain value. The combination of eavesdropper interception and channel errors exacerbates the reduction in keys production compared to a perfect channel, emphasized the need for robust error correction mechanisms to improve the performance of the SKR to enhance the security of future quantum networks. Our simulations offer insights into keys production under various real-world scenarios, underscoring the importance of selecting between E91 and BB84 based on specific security needs and technological capabilities. Advancements in the E91 protocol, particularly its enhanced resilience to eavesdropping, have significant implications for future networks like 6G. As the next generation communication systems increasingly rely on quantum technologies for enhanced security, the integration of E91 could provide stronger defenses against interception and improve overall network security, even in the presence of errors. These findings highlight the protocol's potential to play a key role in the development of quantum-secure 6G networks and beyond.

## 5. Acknowledgment

This research is partially supported by The B5.5G Laboratory.

## References

[1] Mehic M, *et al.* Quantum cryptography in 5g networks: A comprehensive overview. *IEEE Commun Surveys Tut.* 2023:302-46.

[2] Geddada VJ, Lakshmi PV. Distance Based Security using Quantum Entanglement:a survey. *Int Conf Comput Commun Netw Technol (ICCCNT).* 2022.

[3] Zhang Z, *et al.* 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. *IEEE Veh Technol Mag.* 2019;**14**:28-41.

[4] Ahadiansyah D, Anwar K, Budiman G. Investigation on Shor Codes as Degenerate Codes but Correct All Single Quantum Errors. *IEEE Symp Future Telecommun Technol (SOFTT).* 2022.

[5] Anwar K, Ramadhan M. The Smallest Perfect Quantum Accumulate Codes. *IEEE Asia-Pac Conf Commun (APCC).* 2021.

[6] Basudewa MI, Anwar K, Meylani L. Study on the Design of Simple Quantum Communications Based on Orbital Angular Momentum. *2022 IEEE Symp Future Telecommun Technol (SOFTT).* 2022:8-14.

[7] Einstein A, Podolsky B, Rosen N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys Rev.* 1935;**47**:777-80.

[8] Geddada VJ, Lakshmi PV. Distance Based Security using Quantum Entanglement:a survey. *Int Conf Comput Commun Netw Technol (ICCCNT).* 2022.

[9] Durt T, Kaszlikowski D, Chen JL, Kwek LC. Security of quantum key distributions with entangled qudits. *Phys Rev.* 2004;**69**.

[10] Basset B, *et al* . Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci Adv.* 2021;**7**.

[11] Madaan A, Raj G. Analysis of Quantum Key Distribution using Key Distribution and Attacking Strategies over Security Protocol. *Int Conf Cloud Comput, Data Sci Eng (Confluence).* 2018.

[12] Parakh A, Verma P. Improving the Efficiency of Entanglement Based Quantum Key Exchange. *Int Conf Comput Commun Netw (ICCCN).* 2014.

[13] Begimbayeva Y, Zhaxalykov T, Ussatova O. Investigation of Strength of E91 Quantum Key Distribution Protocol. *Int Asian Sch-Seminar Optim Complex Syst (OPCS).* 2023.

[14] Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett.* 1992 May;**68**:3121-4.

[15] Yuen HP. Anonymous-Key Quantum Cryptography and Unconditionally Secure Quantum Bit Commitment. In: Quantum Communication, Computing, and Measurement 3. Springer; 2002. p. 285-93.

[16] Bennett H, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Int Conf Comput, Syst Signal Process.* 1984;**1**.

[17] Bell JS. On the Einstein Podolsky Rosen Paradox. *Phys Physiq.* 1964;**1**(3):195-200.

[18] Clauser JF, Horne MA, Shimony A, Holt RA. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys Rev Lett.* 1969 Oct;**23**:880-4.

[19] Ning S, Zhu H, Feng C, Gu J, Jiang Z, Ying Z, et al. Photonic-Electronic Integrated Circuits for High-Performance Computing and AI Accelerators. Journal of Lightwave Technology. 2024;42(22):7834-59.

[20] Wang Q, Renema JJ, Engel A, de Dood MJA. Design of NbN Superconducting Nanowire Single-Photon Detectors with Enhanced Infrared Detection Efficiency. Phys Rev Appl. 2017 Sep;8:034004.

[21] Yu Z, Yang J, Lin C, Zhang X, Dang F, Yuan Y, et al. Distributed Polarization Measurement for Fiber Sensing Coils: A Review. Journal of Lightwave Technology. 2021;39(12):3699-710.

[22] Ginting MB, Anwar K, Maryopi D. Constructing Quantum Surface Codes for Arbitrary Surface Forms. In: 2021 IEEE Symposium On Future Telecommunication Technologies (SOFTT); 2021. p. 75-80.

[23] Hevia JL, Peterssen G, Piattini M. Dynamic integration for hybrid quantum/Classical software systems. Journal of Systems and Software. 2024;214:112061.