Simulating the BB84 QKD Protocol: A QuTiP-Based Study in Ideal Quantum Channels

Henrique Sobrinho Ghizoni[1*], Anderson R. C. Buarque[1]
[1]QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC; Salvador, Bahia, Brazil

This work presents a simulation of the BB84 Quantum Key Distribution (QKD) protocol using QuTiP, an open-source Python framework for quantum system modeling. The protocol is implemented in an ideal noise-free quantum channel, enabling a clear analysis of its fundamental stages, including state preparation, basis selection, key sifting, error estimation, and privacy amplification. The simulation reproduces the expected behavior of BB84 and allows the investigation of eavesdropping effects through the Quantum Bit Error Rate (QBER) and mutual information between communicating parties. Results show that increasing the eavesdropping interception rate reduces the mutual information shared between Alice and Bob while increasing the information available to Eve. The analysis indicates that both quantities become comparable at approximately EIR ≈ 0.59, providing a quantitative criterion for assessing the impact of eavesdropping on BB84 security. In addition, computational performance measurements demonstrate that the proposed implementation can be executed efficiently on conventional personal computers, reinforcing its suitability for educational and research applications. The results highlight the potential of QuTiP-based simulations as an accessible and reproducible framework for studying the security principles underlying quantum key distribution.

Keywords: Quantum Key Distribution (QKD). BB84 Protocol. Quantum Cryptography. QuTiP. Quantum Education.

Abbreviations: QKD, Quantum Key Distribution. P&M, Prepare and Measure. HWP, Half-Wave Plate. PBS, Polarized Beam Splitter. RNG, Random Number Generation. SP, Single Photon. PP, Post-Processing. RKL, Raw Key Length. kB, Kilobytes. B, Bytes. ms, milliseconds. s, seconds.

Classical cryptography relies on the computational difficulty of efficiently solving problems such as integer factorization or discrete logarithms and underpins widely used protocols such as RSA and Diffie–Hellman. The advancement of quantum computing and the existence of algorithms such as Shor's threaten this traditional framework, making it urgent to seek solutions based on physical principles [2].

In this context, quantum cryptography emerges as a secure alternative. The BB84 protocol, conceived by Bennett and Brassard in 1984 [1], introduces a paradigm that exploits non-orthogonal quantum states distributed in conjugate bases to share secret keys. The protocol relies on two fundamental principles of quantum mechanics: the no-cloning theorem, which prevents copying unknown quantum states, and the unavoidable disturbance caused by any measurement, which introduces detectable errors. This approach grants BB84 physical security and enables the detection of intrusions that cannot be concealed, an advantage that classical cryptography does not offer.

This work presents simulations performed with QuTiP, a Python library dedicated to modeling quantum systems, which enables the step-by-step implementation of the BB84 protocol. The implementation was carried out over an ideal, noise-free quantum channel, in order to clearly observe each stage of the protocol, from preparation and measurement to post-processing. This controlled setting not only facilitates a detailed analysis of BB84's operation but also makes it a valuable tool for educational purposes, supporting the teaching and understanding of fundamental concepts in quantum cryptography. Finally, the work investigates how eavesdropping on the quantum channel can be detected through the estimation of the QBER parameter and/or the

Received on 7 June 2026; revised 24 September 2026.
Address for correspondence: Henrique Sobrinho Ghizoni. Av. Orlando Gomes, 1845 Piatã, Salvador - BA. Salvador, Bahia, Brazil. ZIP code: 41650-810. E-mail: hsghizoni@gmail.com.

J Bioeng. Tech. Health 2026;9(10):1040-1046
© 2026 by SENAI CIMATEC University. All rights reserved.

analysis of the mutual information between the parties involved in the protocol.

Quantum Key Distribution-BB84

The BB84 protocol, proposed by Charles Bennett and Gilles Brassard in 1984 [1], is the first and most well-known QKD protocol. It enables two parties, traditionally named Alice (sender) and Bob (receiver), to establish a shared secret key with security guaranteed by the laws of quantum mechanics. The protocol leverages fundamental quantum principles such as the no-cloning theorem and the fact that quantum measurements disturb the system, thereby making any eavesdropping attempt detectable [2,7].

To implement these principles in practice, BB84 relies on two types of communication channels: a quantum channel, inherently vulnerable to eavesdropping, used for transmitting quantum states, and a classical public channel that, despite being unsecured, requires authentication to prevent attacks.

While the quantum channel ensures the uniqueness and non-replicability of the transmitted qubits, the classical channel is used for basis reconciliation and error correction. By monitoring the quantum bit error rate, the protocol allows the detection of potential eavesdropping attempts, thereby ensuring the integrity and confidentiality of the final secret key.

BB84: Protocol Essential Parts

The protocol operationalizes three essential needs: a quantum channel for transmitting qubits encoded in photon polarization states; an authenticated classical channel for public communication; and trust in the validity of quantum mechanical postulates, especially the no-cloning theorem, superposition, and measurement-induced collapse.

In practical implementations, BB84 uses the polarization states of single photons to encode information [2]. The protocol employs two conjugate bases. The rectilinear basis, $\boldsymbol{B_z}$, consists of the horizontal (0°), $|\boldsymbol{H}\rangle$, and vertical (90°), $|\boldsymbol{V}\rangle$, polarization states,

$$\boldsymbol{B_z} = \{|\boldsymbol{H}\rangle, |\boldsymbol{V}\rangle\}, \quad (1)$$

while the diagonal basis, $\boldsymbol{B_x}$, consists of the diagonal (45°), $|\boldsymbol{D}\rangle$, and the anti-diagonal (-45°) polarization states,

$$\boldsymbol{B_x} = \{|\boldsymbol{D}\rangle, |\boldsymbol{A}\rangle\} \quad (2)$$

where

$$|\boldsymbol{D}\rangle = \frac{|\boldsymbol{H}\rangle+|\boldsymbol{V}\rangle}{\sqrt{2}}, \quad (3)$$

$$|\boldsymbol{A}\rangle = \frac{|\boldsymbol{H}\rangle-|\boldsymbol{V}\rangle}{\sqrt{2}} \quad (4)$$

Shannon entropy [6] quantifies the uncertainty associated with a random variable and is given by

$$\boldsymbol{H(X)} = -\sum_i \boldsymbol{p(x_i) log_2[p(x_i)]}, \quad (5)$$

where $\boldsymbol{p(x_i)}$ represents the probability of occurrence of event $\boldsymbol{x_i}$. In the context of quantum key distribution, entropy measures the unpredictability of the generated keys and serves as a key parameter for assessing security and the rate of useful information transmitted.

Closely related to this concept is mutual information, defined between two random variables $\boldsymbol{X}$ and $\boldsymbol{Y}$ as

$$\boldsymbol{I(X:Y) = H(X) + H(Y) - H(X,Y)}, \quad (6)$$

where $\boldsymbol{H(X,Y)}$ is the joint entropy between the X and Y variables [6]. The mutual information, $\boldsymbol{I(X:Y)}$, quantifies how much information is shared between the random variables X and Y. In the context of quantum key distribution, mutual information is used to quantify the information shared between the legitimate users (Alice and Bob) and compare it with the information potentially accessible to an eavesdropper (Eve).

Prepare and Measure

The P&M operation of the BB84 protocol can be divided into a few main steps:

P&M-I. Alice generates two uniformly random bit strings:

$$a = (a_1, \ldots, a_{4n}), \quad (7)$$

$$b = (b_1, \ldots, b_{4n}), \quad (8)$$

where $a_i \in \{0,1\}$ denotes the bit value and $b_i \in \{0,1\}$ determines the basis ($0: B_z, 1: B_x$). The use of an oversized block (e.g., 4n) anticipates the need for sifting and error estimation.

For each pair (a_i, b_i) Alice prepares a qubit:

$$|\psi_i\rangle = \begin{cases} |\mathrm{H}\rangle, & a_i = 0,\ b_i = 0; \\ |\mathrm{V}\rangle, & a_i = 1,\ b_i = 0; \\ |A\rangle, & a_i = 0,\ b_i = 1; \\ |D\rangle, & a_i = 1,\ b_i = 1. \end{cases} \quad (9)$$

She then sends the sequence of 4n qubits to Bob via the quantum channel. The no-cloning theorem ensures that any attempt by Eve to duplicate these states will fail [2-3].

P&M-II. Bob independently chooses a random basis string, given by

$$b' = (b'_1, \ldots, b'_{4n}) \quad (10)$$

and measures each incoming qubit in the corresponding basis. He records the outcomes a_i. If $b_i = b'_i$, then Bob retrieves a_i with certainty (ignoring noise); otherwise, the outcome is statistically uncorrelated with a_i.

Post-Processing

The post-processing operation of the BB84 protocol can be divided into a few main steps:

PP-I. Alice divulges her basis string b_i over the authenticated classical channel. Bob compares with his b'_i and retains only those indices where $b_i = b'_i$. The remaining bits, roughly 2n in number, form the sifted key. As shown by [2], the expected matching probability is 0.5 due to the uniform random choice of bases.

PP-II. Alice and Bob publicly sample a subset of the sifted key to estimate the Quantum Bit Error Rate (QBER):

$$QBER = {}^{N_b}/_{L_{Sk}}, \quad (11)$$

where N_b is the number of bit mismatches observed in the subset of sifted-key bits, and L_{Sk} is the size of this subset, used to estimate the QBER. An intercept-resend attack introduces a theoretical QBER of 25%, since Eve's random basis choice leads to a 50% error rate half the time [2-3].

PP-III. Provided the QBER is below a critical threshold (typically $\sim 11\%$ for individual attacks) [5], Alice and Bob engage in an error correction protocol (e.g., Cascade or LDPC codes) to reconcile discrepancies in their sifted keys.

PP-IV. To remove any partial knowledge Eve may have acquired, Alice and Bob apply a privacy amplification procedure, compressing the reconciled key into a shorter string of length L_{Rk}. A simplified estimate of the secret key fraction can be expressed as:

$$r = 1 - H(QBER) - I(A:E), \quad (12)$$

where $H(p)$ is the binary entropy function and $I(A:E)$ is Eve's estimated mutual information. This ensures a secure final key under general attacks.

Eve's Attack

There are different types of attacks [2,7] that Eve can perform against the BB84 protocol, including Intercept-Resend (IR), Photon Number Splitting (PNS), and Blinding Attacks. In the intercept-resend attack, Eve intercepts the quantum states transmitted through the quantum channel between Alice and Bob, randomly chooses a basis to measure each qubit, b''_i, and then prepares and retransmits a new quantum state to Bob according to the measurement outcome. Because Eve does not know the basis originally selected by Alice, her measurements inevitably introduce detectable errors into the key generation process, which can be quantified during the parameter estimation stage through metrics such as the Quantum Bit Error Rate (QBER). The objective of this attack is to acquire as much information as possible about the secret key while remaining undetected. As one of the most fundamental and pedagogically relevant attacks in quantum key distribution, the Intercept-Resend strategy is adopted in this work as the primary model for eavesdropping analysis.

There are more sophisticated attacks, such as the Photon Number Splitting (PNS) attack [2,7], in which Eve exploits multi-photon pulses emitted by a non-ideal photon source. By selectively splitting and storing one of the photons in a quantum memory while allowing the remaining photons to continue

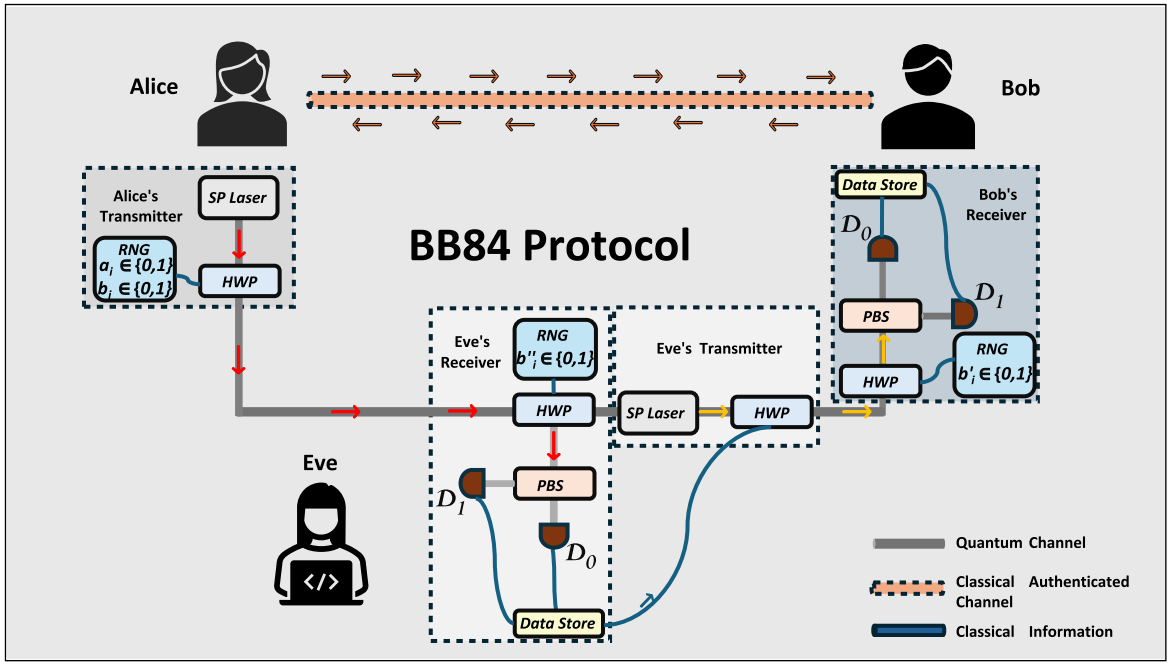
to Bob, Eve can postpone her measurement until basis information becomes available during the classical communication stage. Another well-known attack is the Blinding Attack [2,7], which exploits vulnerabilities in avalanche photodiode (APD) detectors. In this attack, Eve manipulates Bob's detector behavior using bright light pulses, allowing her to influence detection events and potentially gain information without introducing a significant increase in the QBER.

Implementation

The BB84 protocol was designed to be implemented in photonic systems, ideally operating in the Single-Photon (SP) regime. Figure 1 illustrates a possible implementation of the protocol, where the quantum channel may be established through free-space links or optical fibers. The Classical Authenticated Channel (CAC) may be public and fully observable by Eve, provided that authentication mechanisms prevent message forgery and message tampering.

In the context of BB84, the presence of an eavesdropper, conventionally called Eve, must always be considered. In this work, we focus on the Intercept-Resend attack, in which Eve can access all information disclosed through the classical channel, without being able to modify it. Additionally, Eve intercepts the quantum channel, measures the quantum state transmitted by Alice, $|\psi_A\rangle$, and then prepares and retransmits to Bob a new quantum state, $|\psi_E\rangle$, consistent with the measurement outcome. It is worth noting that, due to the no-cloning theorem [2], Eve cannot create a perfect copy of Alice's quantum state.

Figure 1. (Color online) Schematic representation of one possible implementation of the BB84 protocol. Alice randomly selects a basis and a bit value to prepare a quantum state by encoding the polarization of a laser-generated photon using a Half-Wave Plate (HWP). The encoded state is then transmitted to Bob through the quantum channel. Bob independently and randomly selects a measurement basis and configures his receiver accordingly. A Polarizing Beam Splitter (PBS) maps the photon's polarization onto distinct propagation paths, which are associated with detectors D_0 and D_1, corresponding to the binary outcomes 0 and 1. In the Intercept-Resend attack model considered in this work, Eve employs the same measurement apparatus as Bob and the same state-preparation apparatus as Alice, allowing her to intercept, measure, prepare, and retransmit quantum states through the channel.



As shown in Figure 1, Alice prepares the state using three main components: a random number generator (RNG), used to generate the bit to be sent a_i, and the basis chosen to encrypt the bit, b_i; a single-photon laser; and a Half-Wave Plate (HWP), responsible for generating polarization in the photon, which can be 0°, 90°, -45°, or 45°. Alice prepares the state $|\psi_A\rangle$ using these tools and sends it to Bob through the quantum channel.

Bob's and Eve's measurements rely on essentially the same optical components: a Random Number Generator (RNG) to select the measurement basis, a Polarizing Beam Splitter (PBS) to map the photon's polarization onto distinct propagation paths, two detectors, D_0 and D_1, associated with the binary outcomes 0 and 1, and a memory unit to store the measurement results. While Bob performs measurements as part of the legitimate protocol execution, Eve uses the same measurement procedure during the Intercept-Resend attack. After measuring Alice's transmitted quantum state, Eve prepares a new quantum state, $|\psi_E\rangle$, consistent with the measurement outcome and retransmits it to Bob through the quantum channel. This strategy allows Eve to gain information about the key while inevitably introducing errors that may reveal her presence.

Simulation Methodology

The primary objective of the BB84 protocol is to establish a secure key between Alice and Bob while enabling the detection of potential eavesdropping attempts. If Eve intercepts the quantum channel, her presence can be detected during the post-processing stage, particularly in the parameter estimation and privacy amplification steps, through the estimation of the Quantum Bit Error Rate (QBER) and the subsequent decision to either continue or abort the protocol. To simulate the BB84 protocol depicted in Figure 1, this work employs QuTiP [4], a Python framework for quantum system simulation and analysis.

Two complementary analyses are performed in this work. The first investigates the impact of Eve's interception on protocol reliability by considering fixed Eavesdropping Interception Rates (EIRs) of 0.5 and 1.0 over different numbers of protocol rounds. This analysis focuses on the relationship between the Quantum Bit Error Rate (QBER) and the size of the generated raw key. The second analysis evaluates how different EIR values affect the information shared among the communicating parties by examining the mutual information between Alice and Bob, $I(A:B)$, the mutual information between Alice and Eve, $I(A:E)$, and the difference between these quantities, defined as $\Delta I = I(A:B) - I(A:E)$.

Results

The Quantum Bit Error Rate (QBER) is a key metric in the BB84 protocol, as it enables the detection of potential eavesdropping attempts during protocol execution. Figure 2 contains the QBER results for 20 independent protocol executions for three Raw Key Length (RKL) values, namely 64 B, 0.25 kB, and 16 kB, and for two Eavesdropping Interception Rates (EIRs), 0.5 and 1.0, corresponding to 50% and 100% interception of the transmitted quantum states, respectively. The results reveal a clear relationship between the size of the generated raw key and the statistical stability of the QBER estimation. As the RKL increases, fluctuations in the estimated QBER decrease, leading to more stable and accurate measurements. This behavior indicates that larger key sizes improve the reliability of parameter estimation and, consequently, the effectiveness of eavesdropping detection, which is particularly relevant for practical QKD implementations.

The mutual information between Alice and Bob, $I(A:B)$, quantifies the amount of information shared between the legitimate users and therefore provides a useful metric for evaluating the effectiveness of a QKD protocol. Similarly, the mutual information between Alice and Eve, $I(A:E)$, represents the amount of information potentially accessible to the eavesdropper and can be used to assess the effectiveness of an attack.

Figure 2. (Color online) The QBER rate vs round in the BB84 protocol simulation using QuTiP. The orange, red, and light blue curves correspond to EIR = 1.0, for three key sizes, 64 B, 0.25 kB, and 16 kB, respectively. The green, dark blue and black curves correspond to EIR = 0.5, for three key sizes, 64 B, 0.25 kB, and 16 kB, respectively. The larger the key size, the smaller the variation in the QBER value.

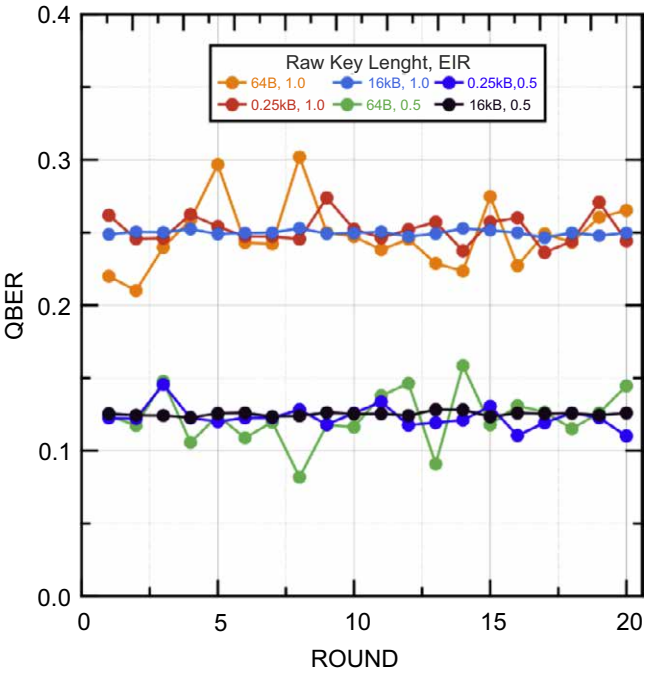


Figure 3 presents the relationship between the Eve Interception Rate (EIR) and the mutual-information quantities $\boldsymbol{I(A:B)}$, $\boldsymbol{I(A:E)}$ and $\boldsymbol{\Delta I}$, considering a Raw Key Length (RKL) of 64 kB. The results reveal a strong dependence of these quantities on the interception rate. As EIR increases, $\boldsymbol{I(A:B)}$ and $\boldsymbol{\Delta I}$ decrease, while $\boldsymbol{I(A:E)}$ increases approximately linearly. This behavior reflects the gradual transfer of information advantage from the legitimate users to the eavesdropper as the interception rate grows. A particularly important result is observed at approximately $\boldsymbol{EIR \approx 0.59}$, where $\boldsymbol{(A:B) \approx I(A:E)}$. At this point, Eve acquires an amount of information comparable to that shared between Alice and Bob, indicating a significant reduction in protocol security. This observation reinforces the importance of parameter estimation and QBER monitoring as mechanisms for detecting eavesdropping and deciding whether the protocol should proceed or be aborted.

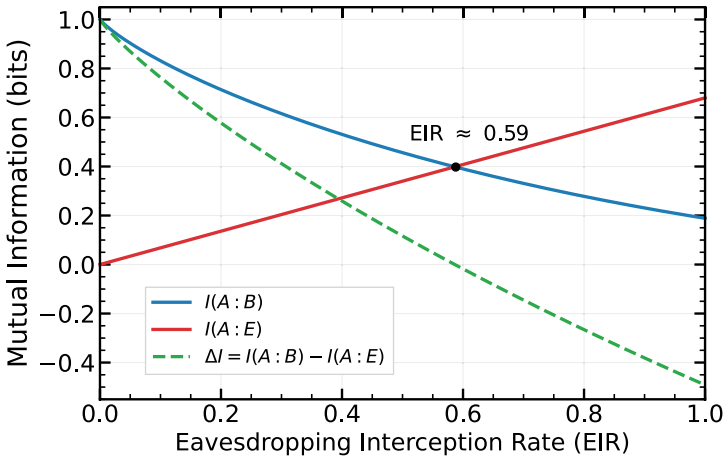
As shown in Figure 2, for $\boldsymbol{EIR = 1.0}$, the average QBER value is approximately $\boldsymbol{25\%}$, which corresponds to the theoretical value expected for an Intercept-Resend attack in an ideal quantum channel. For $\boldsymbol{EIR = 0.5}$, the average QBER is approximately $\boldsymbol{12.5\%}$, representing a warning region that is already close to the point where Eve's information becomes comparable to Bob's information about Alice's key.

In terms of performance, for the data obtained in Figure 2, the average execution times obtained for $\boldsymbol{EIR = 1.0}$ were $\boldsymbol{137.6\,ms}$, $\boldsymbol{423.3\,ms}$, and $\boldsymbol{24.67s}$ for RKL of 64 B, 0.25 kB, and 16 kB, respectively. For $\boldsymbol{EIR = 0.5}$, the average values obtained were $\boldsymbol{110.43\,ms}$, $\boldsymbol{349.4\,ms}$ and $\boldsymbol{19.7\,s}$, respectively, such that simulations with $\boldsymbol{EIR = 0.5}$ take on average approximately $\boldsymbol{81\%}$ of the execution time for cases with $\boldsymbol{EIR = 1.0}$ (values obtained with a notebook with an i7-9750H processor). These execution times demonstrate that the proposed framework can be efficiently executed on conventional personal computers, reinforcing its suitability for educational activities and introductory studies in quantum cryptography.

Conclusions

This work presented a QuTiP-based implementation of the BB84 protocol, enabling the investigation of key security metrics such as the Quantum Bit Error Rate (QBER) and mutual information under different eavesdropping scenarios. The results are consistent with the theoretical behavior of the BB84 protocol and demonstrate the effectiveness of QBER-based parameter estimation for detecting eavesdropping attempts. Furthermore, the mutual-information analysis revealed a progressive reduction in the information advantage shared between Alice and Bob as the Eve Interception Rate (EIR) increased. In particular, the point at which $\boldsymbol{I(A:B)}$ becomes comparable to $\boldsymbol{I(A:E)}$, observed at approximately

Figure 3. (Color online) Mutual information as a function of the Eve Interception Rate (EIR). As the interception rate increases, the mutual information shared between Alice and Bob, $I(A:B)$, decreases, while the mutual information available to Eve, $I(A:E)$, increases. The information advantage, ΔI, decreases accordingly and approaches zero at approximately $EIR \approx 0.59$, indicating the point at which Eve obtains an amount of information comparable to that shared between the legitimate users [2].



$EIR \approx 0.59$, highlights the security implications of the Intercept-Resend attack and reinforces the importance of protocol-abort criteria based on security monitoring. From a computational perspective, the measured execution times demonstrate that the proposed implementation can be efficiently executed on conventional personal computers, making it suitable for educational activities, classroom demonstrations, and introductory studies in quantum cryptography. The results obtained reinforce the value of simulation-based approaches for understanding and teaching quantum communication protocols while providing practical insights into the operation and security of BB84. Future work may extend the proposed framework by incorporating realistic quantum-channel impairments, detector non-idealities, and more advanced attack strategies, such as Photon Number Splitting (PNS) and detector-blinding attacks, enabling closer comparisons between simulated and experimental QKD implementations.

Acknowledgement

This work has been fully funded by the project "Circuito formativo em Tecnologias Quânticas-QIN-FCRH-2025-2-1-1" and was supported by QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPII.

References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560(7).
2. Wolf R. Quantum key distribution protocols. In: Wolf R. Quantum key distribution: an introduction with exercises. Cham: Springer Nature Switzerland; 2021. p. 93-98.
3. Nielsen MA, Chuang IL. Quantum computation and quantum information. Cambridge: Cambridge University Press; 2010. p. 587-589.
4. Johansson JR, Nation PD, Nori F. QuTiP: an open-source Python framework for the dynamics of open quantum systems. Comput Phys Commun. 2012;183(8):1760-1772. doi:10.1016/j.cpc.2012.02.021
5. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett. 2000;85(2):441-444.
6. Cover TM, Thomas JA. Elements of information theory. 2nd ed. Hoboken: Wiley; 2006.
7. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81(3):1301-1350.