Quantum Key Distribution with BB84: Breidbart-Based Eavesdropping and Channel Noise Effects

Author: Mª Lourdes Simón Codina
email: msimonco45@alumnes.ub.edu
Facultat de Física, Universitat de Barcelona, Diagonal 645, 08028 Barcelona, Spain.

Tutor: Bruno Juliá Díaz, Advisor: Artur Garcia Saez

Abstract: This work presents a security analysis of the BB84 quantum key distribution protocol, focusing on intercept-and-resend attacks and the effects of channel noise. We study two eavesdropping strategies—naive and Breidbart-based—and evaluate the probabilities of Eve (the spy) correctly measuring Alice's (the sender) bit and Bob (the receiver) measuring an incorrect one. We analyze the impact of bit-flip, phase-flip, and combined noise, derive theoretical expressions, and identify optimal attack parameters. A cost function is introduced to balance Eve's information gain and detectability. Finally, simulations carried out confirm the theoretical predictions. The results offer insight into the robustness of BB84 under both ideal and noisy conditions and confirm its security against intercept-and-resend attacks.
Keywords: Quantum Key Distribution, BB84 Protocol, Eavesdropping, Pauli Errors, Quantum Bit Error Rate, Quantum Simulation.
SDGs: This work is related to sustainable-development goals (SDGs) 4, 9 and 16 (see page 6).

I. INTRODUCTION

For decades, one of humanity's main concerns has been the ability to transmit information securely through a communication channel. The rise of quantum technologies has revolutionized this goal, providing a level of security that is fundamentally unattainable by classical means. This advantage relies on two key principles: Heisenberg's uncertainty principle and the no-cloning theorem [1].

A classical bit can be encoded in any quantum system with at least two accessible and distinguishable states, i.e., a qubit. Examples include the ground and excited states of a trapped ion, the spin-up and spin-down states of an electron, or the two polarization states of a photon. Among these, polarization-encoded single photons are the most commonly used in Quantum Key Distribution (QKD), transmitted via optical fibers or free space [2].

In practice, implementation devices are not perfect and may introduce errors. For example, quantum channels may suffer from losses or noise — where noise refers to any disturbance that alters the quantum state during transmission [1]. This can lead to discrepancies between the sent key and the one measured by the receiver. Such discrepancies are quantified by the Quantum Bit Error Rate (QBER), defined as the ratio between the erroneous bits and the total bits received [2].

This project aims to explore the security of the QKD BB84 protocol when facing realistic conditions. We compare naive and optimized attacks, introduce a cost function to quantify the trade-off between Eve's information gain and detectability, and evaluate the impact of different noise models. The theoretical predictions are supported by simulations run with Qiskit framework, including a test on a real quantum backend. The results demonstrate the robustness of the BB84 protocol's security.

The work is structured as follows: in Section II, we describe the BB84 protocol and the principles that ensure its security. Section III introduces the main threat to quantum key distribution—eavesdropping—and presents two intercept-and-resend strategies: the naive method and a more advanced one using the Breidbart basis. In Section IV, we analyze the effect of different types of quantum noise on the protocol and on Eve's performance. Section V presents the simulations performed and compares the results with theoretical predictions. Finally, Section VI contains the main conclusions of the work.

II. THE BB84 QUANTUM PROTOCOL

We consider a sender (Alice), a receiver (Bob), and an intruder (Eve). Alice and Bob communicate via a public classical channel and a quantum channel. Through the classical channel, they agree on two bases used to encode the qubits. Each basis is orthonormal within itself, but not mutually orthogonal. They are defined as:

- Computational basis (Z basis):

$|Z_0\rangle = |0\rangle, \quad |Z_1\rangle = |1\rangle.$

- Diagonal basis (X basis):

$|X_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |X_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$

Note that

$$|\langle Z_i|X_j\rangle|^2 = \frac{1}{2}, \tag{1}$$

since

$$\langle Z_i|Z_j\rangle = \delta_{ij}, \qquad \langle X_i|X_j\rangle = \delta_{ij},$$

where δ_{ij} is the Kronecker delta. Therefore, the conjugate observables are those whose eigenstates define the computational and diagonal bases. Specifically, they correspond to the Pauli matrices Z and X:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

These observables do not commute: $[X, Z] = 2iY$, where Y denotes the Pauli matrix associated with the Y-axis. As a consequence of the uncertainty principle, if a third party measures an unknown quantum state in a basis different from the one in which it was prepared, the state is inevitably disturbed. This fundamental property ensures that any unauthorized attempt to access the quantum information introduces detectable anomalies.

Another cornerstone of QKD security is the no-cloning theorem [3]. It states that if $|\Psi\rangle$ is an arbitrary unknown quantum state, there is no unitary operator that can produce a second identical and independent copy of $|\Psi\rangle$, due to the linearity of quantum mechanics. As a result, a third party cannot create a perfect copy of a qubit and forward the original.

The purpose of the BB84 protocol is to allow Alice and Bob to generate a shared secret key while being able to detect any unauthorized access on the quantum channel. To achieve this, they rely on random choices, two encoding bases, and the fundamental principles previously described. The protocol proceeds as follows [1, 5]:

1. Alice generates two random n-bit strings, a and b. The first string, a, contains the bits of the key she intends to send. The second string, b, determines the basis used to encode each qubit.

2. Alice encodes the qubits according to the following rule:

   - $a_i b_i = 00 \rightarrow |Z_0\rangle$
   - $a_i b_i = 01 \rightarrow |X_0\rangle$
   - $a_i b_i = 10 \rightarrow |Z_1\rangle$
   - $a_i b_i = 11 \rightarrow |X_1\rangle$

   Then, she sends the qubits to Bob through the quantum channel.

3. Bob generates a random n-bit string, c, which indicates the basis he will use to measure each qubit. He performs the measurements accordingly and obtains a bit string, which we denote by key.

4. Next, Alice and Bob publicly exchange the strings b and c and discard the bits in a and key where their bases differ, since Eq. (1) implies a 50% error probability for mismatched bases. This step is known as *sifting*. As a result, they obtain the shortened strings a' and key', which are approximately half the length of n.

5. They then randomly select a subset of bits from a' and key' and compare them over the public channel. Since these bits were encoded and measured using the same basis, they are expected to have the same values. However, if the quantum channel is noisy or Eve has interfered, some bits may not match. From this comparison, they compute the observed QBER.

6. If QBER exceeds a predefined threshold, the protocol is aborted and restarted. Otherwise, they remove the revealed bits from a' and key', as those bits are no longer secret, to obtain the final strings a'' and key''. The threshold value depends on the desired level of security and the expected noise in the quantum channel.

7. Finally, Alice and Bob apply classical error correction protocols, as key'' may still differ from a'' due to channel imperfections.

III. SECURITY THREATS IN QKD

The main threat to QKD protocols is the presence of someone who attempts to intercept the transmitted quantum information. This type of intrusion, known as *eavesdropping*, forms the basis for most security analyses in QKD.

Some attack strategies exploit flaws in the experimental setup, while others target the protocol itself, often under idealized conditions. A classification of different attack types can be found in [4]. In this analysis, we focus on one category: *Intercept-and-Resend attacks*, in which Eve intercepts and measures Alice's qubits, then sends replacements to Bob based on her results. The following subsections describe the two strategies studied.

A. Naive Intercept and Resend

This is the first eavesdropping strategy that comes to mind. To begin with, let us assume an ideal quantum channel, that is, one completely noiseless and without losses. In this approach, Eve intercepts and measures each of Alice's qubits by randomly selecting one of the two possible bases, which she knows in advance, as they have been publicly agreed upon through the classical channel. Consequently, she has a 50% chance of selecting the correct basis for each qubit. After performing the measurements, Eve obtains a bit string, which she uses to prepare and resend new qubits to Bob. She encodes each bit using the same basis she employed during the measurement process [5]. An example of this situation is illustrated in Figure 1. If Alice sends a bit 0 (in this case $|Z_0\rangle$), Eve correctly measures a bit 0 with probability: $0,5 \cdot 1 + 0,5 \cdot 0,5 = 0,75$. The same reasoning applies to the remaining three states Alice could send.

Let us now examine the error Eve introduces in Bob's measurement outcomes. We only consider the cases where Bob's measurement basis matches Alice's, since the protocol discards all bits where their bases differ. If

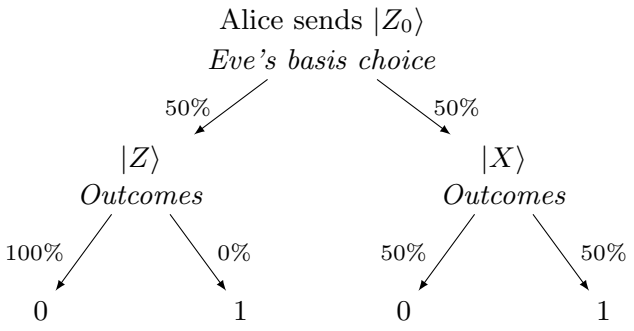

FIG. 1: Probabilities tree for intercept and resend attack when Alice sends $|Z_0\rangle$.

Eve happens to choose the right basis, she reproduces Alice's qubit, so Bob's measurement is always correct. However, if she selects the wrong basis, Bob will obtain the correct result with only 50% probability, as given by Eq. (1).

In summary, this naive intercept-resend method allows Eve to recover the correct bit value with a 75% probability, but at the cost of introducing a 25% QBER in Bob's measurements.

If the subset of bits compared in step 5 of the protocol contains $\widetilde{n}$ bits, the probability of detecting Eve is given by

$$P_d = 1 - \left(\frac{3}{4}\right)^{\widetilde{n}}. \tag{2}$$

Again, we assume an ideal quantum channel, meaning that any single bit mismatch is enough to detect the presence of Eve. In other words, the threshold in step 6 is set to zero.

B. Intercept and Resend in the Breidbart Basis

Once again, let us assume an ideal quantum channel. In this scenario, instead of using the two publicly agreed bases, Eve performs her measurements using a single orthonormal basis of the following form:

$$|b_0\rangle = \cos(\theta)|0\rangle - \sin(\theta)|1\rangle,$$
$$|b_1\rangle = \sin(\theta)|0\rangle + \cos(\theta)|1\rangle.$$

Afterwards, she proceeds as in the naive attack, preparing new qubits using the basis she used for the measurement ($|b\rangle$) and encoding them according to the bit string obtained [6]. Since Eve knows the computational and diagonal bases used by Alice and Bob ($|Z\rangle$, $|X\rangle$), she can compute both her probability of measuring the correct outcome, P_c, and the probability that Bob obtains an incorrect result, P_{err}.

By calculating P_c we obtain the following:

$$P_c(\theta) = \frac{1}{2} + \frac{1}{4}\left(\cos(2\theta) - \sin(2\theta)\right). \tag{3}$$

If we now optimize this probability with respect to the angle θ, we obtain:

$$\frac{dP_c(\theta)}{d\theta} = 0 \quad \rightarrow \quad \theta_B = -\frac{\pi}{8}. \tag{4}$$

The measurement basis $|b\rangle$ defined by the angle θ_B is known as the Breidbart basis. Nevertheless, we will refer to $|b\rangle$ as the Breidbart basis, regardless of the angle. For θ_B, the probability of Eve obtaining the correct bit is $P_c(\theta_B) = 0,85355\ldots \approx 0,85$, while the probability of Bob obtaining an incorrect result is $P_{err}(\theta_B) = 0,25$. Compared to the naive attack, Eve has increased her chances of guessing the correct bit without increasing her probability of being detected, which remains determined by Eq. (2).

IV. NON-IDEAL QUANTUM CHANNEL

Now suppose the quantum channel is no longer ideal. In this work, we focus on three fundamental noise models, each associated with a Pauli operator. In all cases, P_c and P_{err} could depend not only on the angle θ, but also on the corresponding error probability (p, q, or g). The detailed calculations for each noise model are provided in the Appendix.

- **Bit-flip error (X gate) with probability p:** Flips $|0\rangle \leftrightarrow |1\rangle$. It affects the computational basis but not the diagonal basis (up to a global phase). Optimizing $P_c(\theta, p)$ yields:

$$\theta(p) = \frac{1}{2}\arctan\left(\frac{-1}{1-2p}\right).$$

- **Phase-flip error (Z gate) with probability q:** Applies a relative phase, $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$. It affects the diagonal basis but not the computational basis (up to a global phase). Optimizing $P_c(\theta, q)$ yields:

$$\theta(q) = \frac{1}{2}\arctan\left(2q-1\right).$$

Since these two types of errors affect only one of the two bases, in the absence of eavesdropping, the QBER would be equal to half the error probability, i.e., $\frac{p}{2}$ or $\frac{q}{2}$.

- **Bit and phase-flip error (Y gate) with probability g:** A combination of both types of error, $Y|0\rangle = i|1\rangle$, $Y|1\rangle = -i|0\rangle$. It affects both bases.

In Figure 2, we observe a periodic behavior of P_c as a function of the measurement basis angle θ. Only one period is shown. The black curve corresponds to the ideal (noiseless) case, where P_c reaches its maximum at θ_B, as expected. Interestingly, both types of noise exhibit a symmetric distortion with respect to the ideal case. In the presence of bit-flip errors, the maximum of P_c shifts to the left and decreases in value as the error probability

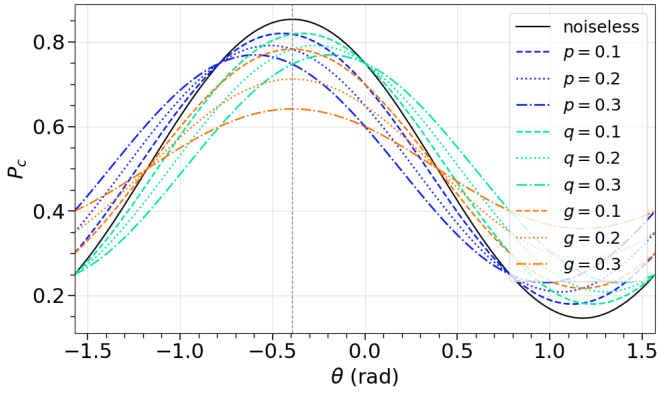

FIG. 2: Probability of Eve correctly measuring the bit P_c as a function of her basis angle θ. The noiseless case is shown in black, bit-flip, phase-flip and combined errors are shown in blue, turquoise and orange, respectively. The angle $-\frac{\pi}{8}$ is marked in gray.

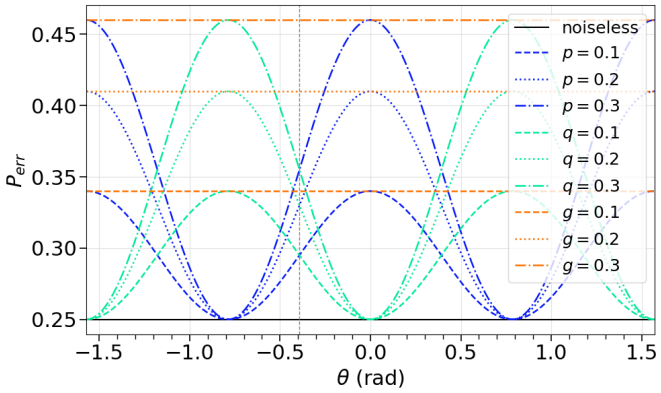

FIG. 3: Probability of Bob measuring the wrong bit P_{err} as a function of Eve's measurement basis angle θ. The noiseless case is shown in black, bit-flip, phase-flip and combined errors are shown in blue, turquoise and orange, respectively. The angle $-\frac{\pi}{8}$ is marked in gray.

increases. Phase-flip errors display the same behavior, but with the maximum shifting to the right. As a result, for the same values of p and q, the maximum value of P_c is identical for both types of error.

The behavior of P_{err}, the probability that Bob obtains an incorrect result, is shown in Figure 3. We also observe a periodic behavior, though with a shorter period. The functions are mirror images of each other with respect to θ_B, which implies that for equal values of p and q, the corresponding values of P_{err} coincide when evaluated at the angle that maximizes P_c.

If we now study the case where both bit-flip and phase-flip errors occur simultaneously, we observe that the P_c maximum remains at the Breidbart angle $\theta_B = -\pi/8$. As expected, its value decreases as the error probability g increases. In contrast, P_{err} becomes constant with respect to θ. Interestingly, for $p = q = g$ it satisfies the relation:

$$P_{\text{err}}^{Y} = P_{\text{err}}^{X}(\theta) + P_{\text{err}}^{Z}(\theta) - P_{\text{err}}^{noiseless}(\theta).$$

This implies that the disturbance caused by the combined bit-flip and phase-flip noise (Y) equals the total disturbance from the individual error types (X and Z), with the ideal contribution subtracted once to avoid double-counting.

Another possible strategy for Eve is to not only maximize P_c, but also to minimize P_{err}, in order to reduce her probability of being detected. This can be done by minimizing a cost function:

$$f(\theta, j) = -\alpha P_c(\theta, j) + \beta P_{err}(\theta, j),$$

where α and β are weight parameters chosen by Eve according to the importance she assigns to gaining information versus minimizing disturbance. The parameter $j \in \{p, q\}$, since in both the noiseless and Y-error cases P_{err} is constant, making its minimization meaningless. The negative sign reflects the goal of maximizing P_c. Some theoretical values are shown in Table I, located in the Appendix.

In all cases studied, the results show that the probability of detecting Eve is high, since the threshold chosen by Alice and Bob would typically be $\frac{p}{2}$, $\frac{q}{2}$, or g, and the value of P_{err} is always greater than these thresholds. Therefore, the protocol is secure against this type of attack.

However, if Eve were to interfere with the system calibration —during which Alice and Bob estimate the channel noise— she could cause them to overestimate the actual noise level. As a result, the detection threshold would be set too high, increasing her chances of going undetected and successfully extracting information.

V. SIMULATIONS

To study the BB84 protocol and the eavesdropping strategies mentioned, several simulations have been carried out with the Qiskit framework developed by IBM. Here we present the results.

In these simulations, we consider n qubits under the assumption that Alice and Bob have chosen the same basis for each qubit ($b = c$). This is justified because qubits measured in mismatched bases are discarded during the sifting process and do not contribute to the final key. Therefore, generating an effective key of length n would require Alice to initially send $2n$ qubits in a real case.

Following the authors' suggestion in [1], the subset compared in step 5 consists of approximately one third of the bits remaining after shifting; in this case, $round(\frac{n}{3})$ where $round$ returns the nearest integer.

To perform a statistical analysis of the probabilities, s simulations are carried out and the average over all runs is computed. For the Intercept and Resend in the Breidbart Basis attack and under ideal conditions, $s = 300$ simulations have been performed using AerSimulator, a backend for simulating quantum circuits on classical

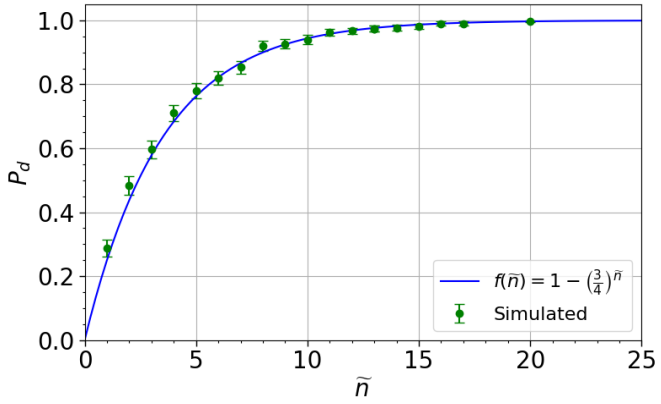

FIG. 4: Probability of detecting Eve as a function of the number of compared bits $\widetilde{n}$ with Intercept and Resend in the Breidbart Basis. The discrete points with error bars represent simulation results, the solid line corresponds to the theoretical prediction.

hardware, for 18 different values of n, all multiples of 3. The resulting data are shown in Figure 4.

We observe that the simulated points closely follow the theoretical curve determined by Eq. (2), and that the statistical uncertainty decreases as the number of qubits increases. The probability of detecting Eve increases rapidly with the number of qubits used. With an initial count of at least 120 qubits, this probability is already close to 1. Therefore, the protocol is secure against this type of eavesdropping.

To complement the simulations, an execution of the BB84 protocol has been implemented on IBM's real quantum backend *ibm_brisbane* (which employs superconducting transmon qubits), using $n = 500$ qubits and a quantum channel subject to Y-type noise with probability $g = 0, 2$. For step 7, the CASCADE error correction protocol is applied [7]. The code used for the simulations is available at [8]. After comparing a subset of 167 bits, the observed QBER was 0.1976, as expected, since this type of error affects both measurement bases. Following this, a final key of 500-167=333 bits was distilled through error correction. No discrepancies were found in the final shared key; however, the CASCADE protocol does not guarantee the correction of all errors. The results are shown in Table II in the Appendix.

VI. CONCLUSIONS

We have studied the security of the BB84 quantum key distribution protocol under intercept-and-resend attacks, both in ideal conditions and in the presence of noise. Two eavesdropping strategies were examined: the naive attack provides Eve with a 75% success rate while introducing a 25% QBER; when using the Breidbart basis, Eve increases her success probability to approximately 85% without increasing the QBER.

The analysis was extended by considering three noise models: bit-flip (X), phase-flip (Z), and combined bit- and phase-flip (Y). Analytical expressions were derived for the optimal attack angle in each case. Additionally, a cost function was introduced to capture the trade-off between information gain and detectability.

The theoretical predictions were validated through simulations using IBM's Qiskit framework. In particular, it was shown how the number of compared bits affects Eve's detectability. Furthermore, an execution of the BB84 protocol was carried out on the *ibm_brisbane* real quantum backend with $n = 500$ qubits and simulating Y-type noise. After applying the CASCADE error correction protocol, a final key of 333 bits was distilled with no remaining discrepancies.

Overall, the results confirm the theoretical security of the BB84 protocol under intercept-and-resend attacks, even in the presence of noise, while emphasizing the importance of setting appropriate error thresholds.

Acknowledgments

I would like to thank Bruno Juliá Díaz and Artur Garcia Saez for their guidance and valuable advice throughout the development of this work. I am also grateful to my family and friends for their support during this final stage of my degree.

[1] C.H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 175–179 (1984).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum Cryptography*, Rev. Mod. Phys. **74**, 145–195 (2002).

[3] W.K. Wootters and W.H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802–803 (1982).

[4] Rahul Aggarwal, Heeren Sharma, and Deepak Gupta, *Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol*, International Journal of Computer Applications,Volume 20– No.8, 28–31 (2011).

[5] C. Kollmitzer and M. Pivk (Eds.), *Applied Quantum Cryptography*, Lecture Notes in Physics, Vol. 797 (Springer, Berlin Heidelberg, 2010).

[6] D. Liu, C. Pei, D. Quan, B. Han, and N. Zhao, *A new attack strategy for BB84 protocol based on Breidbart basis*, in *Proceedings of the IEEE International Conference on Communications Technology and Applications (ICCTA)*, Xidian University, China, 2008.

[7] Bruno Rijsman, *CASCADE Protocol — Cascade 1.0.0 Documentation*, `https://cascade-python.readthedocs.io/en/latest/protocol.html`,

[8] Lourdes Simón Codina. *Code for BB84 simulations.* `https://github.com/lourdessico/QKD-BB84-Simulations--TFG`.

Distribució Quàntica de Claus amb BB84: Espionatge amb Base de Breidbart i Efectes del Soroll al Canal

Author: Mª Lourdes Simón Codina
email: msimonco45@alumnes.ub.edu
Facultat de Física, Universitat de Barcelona, Diagonal 645, 08028 Barcelona, Spain.

Tutor: Bruno Juliá Díaz, Advisor: Artur Garcia Saez

Resum: Aquest treball presenta una anàlisi de la seguretat del protocol de distribució quàntica de claus BB84, centrant-se en els atacs d'intercepció i reenviament i en els efectes del soroll al canal. S'estudien dues estratègies d'espionatge —una de tipus naïf i una altra basada en la base de Breidbart—, i s'avaluen les probabilitats que l'Eva (espia) mesuri correctament el bit enviat per Alice (remitent) i que en Bob (receptor) en mesuri un d'erroni. S'analitza l'impacte del soroll de tipus bit-flip, phase-flip i combinat, es deriven expressions teòriques i s'identifiquen els paràmetres òptims per a l'atac. També s'introdueix una funció de cost per equilibrar el guany d'informació de l'Eva i la seva probabilitat de ser detectada. Finalment, les simulacions realitzades confirmen les prediccions teòriques. Els resultats ofereixen una visió fonamentada de la robustesa del protocol BB84 tant en condicions ideals com sorolloses, i confirmen la seva seguretat davant d'atacs d'intercepció i reenviament.
Paraules clau: Distribució Quàntica de Claus, Protocol BB84, Espionatge, Errors de Pauli, Taxa d'Error de Bit Quàntic, Simulació Quàntica.

Objectius de Desenvolupament Sostenible (ODSs o SDGs)

1. Fi de les desigualtats		10. Reducció de les desigualtats	
2. Fam zero		11. Ciutats i comunitats sostenibles	
3. Salut i benestar		12. Consum i producció responsables	
4. Educació de qualitat	X	13. Acció climàtica	
5. Igualtat de gènere		14. Vida submarina	
6. Aigua neta i sanejament		15. Vida terrestre	
7. Energia neta i sostenible		16. Pau, justícia i institucions sòlides	X
8. Treball digne i creixement econòmic		17. Aliança pels objectius	
9. Indústria, innovació, infraestructures	X		

El contingut d'aquest TFG, part d'un grau universitari de Física, es relaciona amb diversos Objectius de Desenvolupament Sostenible. En particular, s'alinea amb l'ODS 4, i concretament amb la fita 4.4, ja que contribueix a l'educació universitària en l'àmbit de les tecnologies quàntiques i la confidencialitat de les comunicacions, potenciant les competències tècniques i científiques dels estudiants. També es vincula amb l'ODS 9, fita 9.5, promovent la recerca científica i el desenvolupament tecnològic en un camp estratègic com és la criptografia quàntica. Finalment, aquest treball també contribueix a l'ODS 16, en abordar la seguretat de la informació i la protecció contra espionatge, essencial per a institucions democràtiques i justes.

Appendix A: SUPPLEMENTARY MATERIAL

Theoretical Analysis of Probabilities in a Noisy Channel

TABLE I: Theoretical probabilities of Eve measuring the correct bit (P_c) and Bob measuring the wrong bit (P_{err}) for different values of α and β, under each type of noise. We present the results for three different error probabilities $p = q \equiv j \in \{0.1,\ 0.2,\ 0.3\}$.

$j = 0.1$		X		Z	
α	β	P_c	P_{err}	P_c	P_{err}
1	0	0.82015621	0.28512195	0.82015621	0.28512181
2	1	0.81763837	0.27452756	0.81763844	0.27452769
1	1	0.81224729	0.26716911	0.81224690	0.26716872
0	1	0.25000000	0.25000000	0.25000000	0.25000000

$j = 0.2$		X		Z	
α	β	P_c	P_{err}	P_c	P_{err}
1	0	0.79154759	0.29235296	0.79154759	0.29235310
2	1	0.78675932	0.26974304	0.78675927	0.26974293
1	1	0.78033077	0.26074440	0.78033086	0.26074449
0	1	0.75000000	0.25000000	0.25000000	0.25000000

$j = 0.3$		X		Z	
α	β	P_c	P_{err}	P_c	P_{err}
1	0	0.76925824	0.27896552	0.76925824	0.27896579
2	1	0.76563583	0.25967181	0.76563590	0.25967196
1	1	0.76208613	0.25463899	0.76208606	0.25463893
0	1	0.25000000	0.25000000	0.25000000	0.25000000

Notice how the values for the same parameters across the two different types of error are very similar, but not exactly identical — small differences appear in the last decimal places. For the noiseless and the Y-type noise cases, the value of P_{err} remains constant. Therefore, it does not make sense to search for the angle that minimizes P_{err}, and these results are not presented.

Real Backend BB84 Protocol Execution Results

TABLE II: Bit strings involved in the BB84 protocol execution implemented on IBM's real quantum backend *ibm_brisbane*, with a $g = 0.2$ probability of Y-type errors. **a.** Alice's initial key. **b.** Bob's raw key after measurement. **c.** Alice's key after comparing subsets. **d.** Bob's key after comparing subsets. **e.** Bob's key after error correction using the CASCADE protocol. Red bits indicate discrepancies between Bob's and Alice's keys.

a	1110001101110010100001110101101100110011010110100001111010110101100001000110101000101110110100001010 11100111110000110000110001010011110000001100110001010011001011100101110011000101110011010110100101101 1001001010001110000011001111011101111000111010110001100110010000100010001100011011011000000101101011110 0110000110011010011011111011110010000100101011111000110110100111111100010000011100111100100011100110 0010011011001000001011000101011110100100000001101010010100000010100011111001011111111101011101111110
b	111010110011001010011111101011111100010011110110101011111101111101001000010000101010001011100111101001010 1111010111011011011001000101000011001001000110001101000101010100001110011000101110110011111110101101 1001000011101111000110011010011101000001001011100100011001001111001000111001001101100011111000011010 0110000110001000011011010011110010000100001001111000110100100101111110000110001101011100100001110111 0011011011001000001011010100011010110100000001101110011101111010110111111011111011110101001101111110
c	0011010011011011110110100110010000100011010100011010001101100011001100011001010000100110011100111001 0001100110110001011011001010100011001001111110011110010110100001000110011011000010110010001100101011 01110100000001001111001111010011110000011100111110011101100011011001000010110001011110100100000101000 10100101000111100111111010111110
d	10010101110111011111110100111010000100001010100011011001110101011010100001010010001010001011100111001 0001101011111101011011001000111011001001101010001010000110100111000111010011001100110010001100100010 01110100000000011100111001000111001000110101111100011011100110110010000101101010110101101000001011001 11110110111110111011111010111110
e	0011010011011011110110100110010000100011010100011010001101100011001100011001010000100110011100111001 0001100110110001011011001010100011001001111110011110010110100001000110011011000010110010001100101011 01110100000001001111001111010011110000011100111110011101100011011001000010110001011110100100000101000 10100101000111100111111010111110

Probability Calculations

In this section, we present the analytical derivations of the different probabilities analyzed throughout the project. We consider the following projection probabilities:

$$
\begin{aligned}
|\langle b_0|0\rangle|^2 = |\langle b_1|1\rangle|^2 &= \cos^2\theta, \qquad |\langle b_0|+\rangle|^2 = |\langle b_1|-\rangle|^2 = \left(\tfrac{1}{2} - \sin\theta\cos\theta\right), \\
|\langle b_0|1\rangle|^2 = |\langle b_1|0\rangle|^2 &= \sin^2\theta, \qquad |\langle b_0|-\rangle|^2 = |\langle b_1|+\rangle|^2 = \left(\tfrac{1}{2} + \sin\theta\cos\theta\right).
\end{aligned}
$$

where the notation used for the computational basis and the diagonal basis is:

$$
|Z_0\rangle = |0\rangle, \qquad |X_0\rangle = |+\rangle,
$$
$$
|Z_1\rangle = |1\rangle, \qquad |X_1\rangle = |-\rangle.
$$

We use the following double-angle identities:

$$
\begin{cases}
\cos(2\theta) = \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1 \\
\sin(2\theta) = 2\sin\theta\cos\theta
\end{cases}
$$

- **Probability that Eve measures the correct result under ideal conditions.** The factor $1/4$ corresponds to the probability that Alice sends one of the four possible states.

$$\begin{aligned}
P_c(\theta) &= \frac{1}{4}\left[|\langle 0|b_0\rangle|^2 + |\langle +|b_0\rangle|^2 + |\langle 1|b_1\rangle|^2 + |\langle -|b_1\rangle|^2\right] \\
&= \frac{1}{4}\left[\cos^2\theta + \frac{1}{2}(\cos^2\theta - 2\cos\theta\sin\theta + \sin^2\theta) + \cos^2\theta + \frac{1}{2}(\cos^2\theta - 2\cos\theta\sin\theta + \sin^2\theta)\right] \\
&= \frac{1}{4}\left[2\cos^2\theta + (1 - 2\cos\theta\sin\theta)\right] \\
&= \frac{1}{4}\left[\cos(2\theta) + 1 + 1 - \sin(2\theta)\right] \\
&= \frac{1}{2} + \frac{1}{4}\left(\cos(2\theta) - \sin(2\theta)\right)
\end{aligned}$$

To find the angle θ that maximizes Eve's probability of correctly guessing the state, we compute the derivative of $P_c(\theta)$ and set it to zero:

$$\begin{aligned}
\frac{dP_c(\theta)}{d\theta} = 0 &= \frac{1}{4}\left(-2\sin(2\theta) - 2\cos(2\theta)\right) = 0 \\
&\Rightarrow \sin(2\theta) + \cos(2\theta) = 0 \\
&\Rightarrow \boxed{\theta_B = -\frac{\pi}{8}}
\end{aligned}$$

- **Probability that Eve measures the correct result when the quantum channel is affected by a bit-flip error with probability p.** This type of noise only affects the computational basis states, i.e., $|0\rangle$ and $|1\rangle$, while the diagonal basis states $|+\rangle$ and $|-\rangle$ remain unaffected (except for an overall global phase, which has no physical consequences).

$$\begin{aligned}
P_c(\theta, p) &= \frac{1}{4}\left[(1-p)|\langle 0|b_0\rangle|^2 + p|\langle 1|b_0\rangle|^2 + (1-p)|\langle 1|b_1\rangle|^2 + p|\langle 0|b_1\rangle|^2 + |\langle +|b_0\rangle|^2 + |\langle -|b_1\rangle|^2\right] \\
&= \frac{1}{4}\left[(1-p)\cos^2\theta + p\sin^2\theta + (1-p)\cos^2\theta + p\sin^2\theta + 2\left(\frac{1}{2} - \sin\theta\cos\theta\right)\right] \\
&= \frac{1}{4}\left[2(1-p)\cos^2\theta + 2p\sin^2\theta + 2\left(\frac{1}{2} - \sin\theta\cos\theta\right)\right] \\
&= \frac{1}{2}\left[(1-p)\cos^2\theta + p\sin^2\theta + \frac{1}{2} - \frac{1}{2}\sin(2\theta)\right] \\
&= \frac{1}{2}\left[\cos(2\theta)\left(\frac{1}{2} - p\right) + 1 - \frac{1}{2}\sin(2\theta)\right]
\end{aligned}$$

To find the angle θ that maximizes Eve's probability of correctly guessing the state, we compute the derivative of $P_c(\theta, p)$ and set it to zero:

$$\begin{aligned}
\frac{dP_c(\theta,p)}{d\theta} &= -\sin(2\theta)\left(\frac{1}{2} - p\right) - \frac{1}{2}\cos(2\theta) = 0 \\
&\Rightarrow \sin(2\theta)(1-2p) + \cos(2\theta) = 0 \\
&\Rightarrow \tan(2\theta) = \frac{-1}{1-2p} \\
&\Rightarrow \boxed{\theta = \frac{1}{2}\arctan\left(\frac{-1}{1-2p}\right)}
\end{aligned}$$

- **Probability that Eve measures the correct result when the quantum channel is affected by a phase-flip error with probability q.** This type of noise only affects the diagonal basis states, i.e., $|+\rangle$ and

$|-\rangle$, while the computational basis states $|0\rangle$ and $|1\rangle$ remain unaffected (except for an overall global phase which has no physical consequences).

$$\begin{aligned}
P_c(\theta,q) &= \frac{1}{4}\Big[(1-q)|\langle+|b_0\rangle|^2 + q|\langle-|b_0\rangle|^2 + (1-q)|\langle-|b_1\rangle|^2 + q|\langle+|b_1\rangle|^2 + |\langle 0|b_0\rangle|^2 + |\langle 1|b_0\rangle|^2\Big] \\
&= \frac{1}{4}\Big[(1-q)\left(\frac{1}{2} - \cos\theta\sin\theta\right) + q\left(\frac{1}{2} + \cos\theta\sin\theta\right) \\
&\qquad\qquad + (1-q)\left(\frac{1}{2} - \cos\theta\sin\theta\right) + q\left(\frac{1}{2} + \cos\theta\sin\theta\right) + 2\cos^2\theta\Big] \\
&= \frac{1}{4}\Big[2(1-q)\left(\frac{1}{2} - \cos\theta\sin\theta\right) + 2q\left(\frac{1}{2} + \cos\theta\sin\theta\right) + 2\cos^2\theta\Big] \\
&= \frac{1}{4}\left[2\left(\frac{1}{2} - \cos\theta\sin\theta\right) + 4q\cos\theta\sin\theta + 2\cos^2\theta\right] \\
&= \frac{1}{2}\left[\left(\frac{1}{2} - \cos\theta\sin\theta\right) + 2q\cos\theta\sin\theta + \cos^2\theta\right] \\
&= \frac{1}{2}\left[\frac{1}{2} + (2q-1)\cos\theta\sin\theta + \cos^2\theta\right]
\end{aligned}$$

To find the angle θ that maximizes Eve's probability of correctly guessing the state, we compute the derivative of $P_c(\theta, q)$ and set it to zero:

$$\begin{aligned}
\frac{dP_c(\theta,q)}{d\theta} &= \frac{1}{2}\left[(2q-1)(\cos^2\theta - \sin^2\theta) - 2\cos\theta\sin\theta\right] = 0 \\
&\Rightarrow (2q-1)\cos(2\theta) - \sin(2\theta) = 0 \\
&\Rightarrow (2q-1)\cos(2\theta) = \sin(2\theta) \\
&\Rightarrow \tan(2\theta) = 2q-1 \\
&\Rightarrow \boxed{\theta = \frac{1}{2}\arctan(2q-1)}
\end{aligned}$$

- **Probability that Eve measures the correct result when the quantum channel is affected by a bit-flip + phase-flip error with probability** g. This type of noise affects both bases.

$$\begin{aligned}
P_c(\theta,g) &= \frac{1}{4}\Big[(1-g)|\langle 0|b_0\rangle|^2 + g|\langle 1|b_0\rangle|^2 + (1-g)|\langle 1|b_1\rangle|^2 + g|\langle 0|b_1\rangle|^2 + (1-g)|\langle+|b_0\rangle|^2 + g|\langle-|b_0\rangle|^2 \\
&\quad + (1-g)|\langle-|b_1\rangle|^2 + g|\langle+|b_1\rangle|^2\Big] \\
&= \frac{1}{2}\left[(1-g)\cos^2\theta + g\sin^2\theta + (1-g)\left(\frac{1}{2} - \sin\theta\cos\theta\right) + g\left(\frac{1}{2} + \sin\theta\cos\theta\right)\right] \\
&= \frac{1}{2}\left[\cos^2\theta - g\cos^2\theta + g\sin^2\theta + \left(\frac{1}{2} - \sin\theta\cos\theta\right) - g\left(\frac{1}{2} - \sin\theta\cos\theta\right) + g\left(\frac{1}{2} + \sin\theta\cos\theta\right)\right] \\
&= \frac{1}{2}\left[\cos^2\theta - g\cos(2\theta) + \left(\frac{1}{2} - \sin\theta\cos\theta\right) + 2g\sin\theta\cos\theta\right] \\
&= \frac{1}{2}\left[\cos^2\theta - g\cos(2\theta) + \left(\frac{1}{2} - \frac{1}{2}\sin(2\theta)\right) + g\sin(2\theta)\right] \\
&= \frac{1}{2}\left[\cos^2\theta - g\cos(2\theta) + \frac{1}{2} + \left(g - \frac{1}{2}\right)\sin(2\theta)\right]
\end{aligned}$$

- **Probability that Bob measures the wrong result under ideal conditions.** For each possible input state, we compute the probability that Eve measures the correct result and Bob measures the wrong one, plus the

probability that Eve measures the wrong result and Bob measures the correct one. This accounts for the total probability that Bob obtains an incorrect outcome after Eve's intervention.

$$\begin{aligned}
P_{err}(\theta) &= \frac{1}{4}\Big(|\langle b_0|0\rangle|^2 \cdot |\langle b_0|1\rangle|^2 + |\langle b_1|0\rangle|^2 \cdot |\langle b_1|1\rangle|^2\Big) + \frac{1}{4}\Big(|\langle b_1|1\rangle|^2 \cdot |\langle b_1|0\rangle|^2 + |\langle b_0|1\rangle|^2 \cdot |\langle b_0|0\rangle|^2\Big) \\
&\quad + \frac{1}{4}\Big(|\langle b_0|+\rangle|^2 \cdot |\langle b_0|-\rangle|^2 + |\langle b_1|+\rangle|^2 \cdot |\langle b_1|-\rangle|^2\Big) + \frac{1}{4}\Big(|\langle b_1|-\rangle|^2 \cdot |\langle b_1|+\rangle|^2 + |\langle b_0|-\rangle|^2 \cdot |\langle b_0|+\rangle|^2\Big) \\
&= \frac{1}{2}\Big[|\langle b_0|0\rangle|^2 \cdot |\langle b_0|1\rangle|^2 + |\langle b_1|0\rangle|^2 \cdot |\langle b_1|1\rangle|^2 + |\langle b_0|+\rangle|^2 \cdot |\langle b_0|-\rangle|^2 + |\langle b_1|+\rangle|^2 \cdot |\langle b_1|-\rangle|^2\Big] \\
&= \frac{1}{2}\Big[\cos^2\theta\,|\langle b_0|1\rangle|^2 + \sin^2\theta\,|\langle b_1|1\rangle|^2 + \left(\frac{1}{2} - \cos\theta\sin\theta\right)|\langle b_0|-\rangle|^2 + \left(\frac{1}{2} + \cos\theta\sin\theta\right)|\langle b_1|-\rangle|^2\Big] \\
&= \frac{1}{2}\Big[2\cos^2\theta\,\sin^2\theta + 2\left(\frac{1}{2} - \cos\theta\sin\theta\right)\left(\frac{1}{2} + \cos\theta\sin\theta\right)\Big]
\end{aligned}$$

Taking into account that, for the angle θ_B, the following identities hold:

$$\begin{cases} \dfrac{1}{2} + \sin\theta_B\cos\theta_B = \sin^2\theta_B \\ \dfrac{1}{2} - \sin\theta_B\cos\theta_B = \cos^2\theta_B \end{cases}$$

we obtain for θ_B

$$P_{err}(\theta_B) = 2\cos^2\theta_B\sin^2\theta_B \quad \Rightarrow \boxed{P_{err}(\theta_B) = 0,25}$$

- When **noise is present in the quantum channel**, the states received by Eve and Bob are no longer pure, but rather mixed states described by a density matrix. To compute the **probability that Bob obtains an incorrect result**, we evaluate

$$P_{\text{err}} = \frac{1}{4}\left(P_0 + P_1 + P_+ + P_-\right),$$

where P_i denotes the probability that Bob measures the wrong result given that Alice sent state i. We recall that only those bits for which Alice's and Bob's bases match are considered, since all others are discarded.

We analyze three types of channel noise: bit-flip (X), phase-flip (Z), and combined bit- and phase-flip (Y), each occurring with respective probabilities p, q, and g.

In general, the state received by Eve is a mixed state of the form:

$$\rho_i = (1-j)\,|i\rangle\langle i| + j\,J|i\rangle\langle i|J,$$

where $|i\rangle$ is the state sent by Alice ($i = 0, 1, +, -$), $j \in \{p, q, g\}$ is the noise probability, and $J \in \{X, Z, Y\}$ is the corresponding quantum error operator.

The state received by Bob, after potential intervention by Eve, is given by:

$$\rho_i' = (1-j)\,|b_i\rangle\langle b_i| + j\,J|b_i\rangle\langle b_i|J,$$

where $|b_i\rangle$ denotes the state prepared by Eve, and here $i = 0, 1$ since Eve employs a single measurement basis throughout the protocol.

With this, we find:

$$\begin{aligned}
P_0 &= \langle b_0|\rho_0|b_0\rangle\langle 1|\rho_0'|1\rangle + \langle b_1|\rho_0|b_1\rangle\langle 1|\rho_1'|1\rangle && \text{(Alice sends } |0\rangle\text{, Bob gets } |1\rangle) \\
P_1 &= \langle b_0|\rho_1|b_0\rangle\langle 0|\rho_0'|0\rangle + \langle b_1|\rho_1|b_1\rangle\langle 0|\rho_1'|0\rangle && \text{(Alice sends } |1\rangle\text{, Bob gets } |0\rangle) \\
P_+ &= \langle b_0|\rho_+|b_0\rangle\langle -|\rho_0'|-\rangle + \langle b_1|\rho_+|b_1\rangle\langle -|\rho_1'|-\rangle && \text{(Alice sends } |+\rangle\text{, Bob gets } |-\rangle) \\
P_- &= \langle b_0|\rho_-|b_0\rangle\langle +|\rho_0'|+\rangle + \langle b_1|\rho_-|b_1\rangle\langle +|\rho_1'|+\rangle && \text{(Alice sends } |-\rangle\text{, Bob gets } |+\rangle)
\end{aligned}$$

By symmetry, we have $P_0 = P_1$ and $P_+ = P_-$. Therefore, we finally obtain:

$$P_{\text{err}}^X = \frac{1}{2}\Big[2(1-p)^2\sin^2\theta\cos^2\theta + 2(1-p)p\sin^4\theta + 2(1-p)p\cos^4\theta + 2p^2\sin^2\theta\cos^2\theta + 2\left(\frac{1}{4} - \sin^2\theta\cos^2\theta\right)\Big]$$

$$P_{\text{err}}^Z = \frac{1}{2}\Big[2(1-q)q\left(\frac{1}{2} + 2\sin^2\theta\cos^2\theta\right) + 2\left(\frac{1}{4} - \sin^2\theta\cos^2\theta\right)((1-q)^2 + q^2) + 2\sin^2\theta\cos^2\theta\Big]$$

$$P_{\text{err}}^Y = \frac{1}{2}\Big[2g(1-g)(\sin^4\theta + \cos^4\theta) + 2\sin^2\theta\cos^2\theta((1-g)^2 + g^2) + 2(1-g)g\left(\left(\frac{1}{2} - \sin\theta\cos\theta\right)^2 + \left(\frac{1}{2} + \sin\theta\cos\theta\right)^2\right) + 2((1-g)^2 + g^2)\left(\frac{1}{4} - \sin^2\theta\cos^2\theta\right)\Big] = g(1-g) + \frac{1}{4}$$

Some expressions may admit further simplification.