symmetry

MDPI

Article

Shared Quantum Key Distribution Based on Asymmetric Double Quantum Teleportation

Carlos Cardoso-Isidoro [1,†] and Francisco Delgado [2,*,†]

[1] Tecnologico de Monterrey, School of Engineering and Sciences, Monterrey 64849, Mexico; ccardoso@tec.mx
[2] Tecnologico de Monterrey, School of Engineering and Sciences, Atizapán 52926, Mexico
* Correspondence: fdelgado@tec.mx
† These authors contributed equally to this work.

Abstract: Quantum cryptography is a well-stated field within quantum applications where quantum information is used to set secure communications, authentication, and secret keys. Now used in quantum devices with those purposes, particularly Quantum Key Distribution (QKD), which proposes a secret key between two parties free of effective eavesdropping, at least at a higher level than classical cryptography. The best-known quantum protocol to securely share a secret key is the BB84 one. Other protocols have been proposed as adaptations of it. Most of them are based on the quantum indeterminacy for non-orthogonal quantum states. Their security is commonly based on the large length of the key. In the current work, a BB84-like procedure for QKD based on double quantum teleportation allows the sharing of the key statement using several parties. Thus, the quantum bits of information are assembled among three parties via entanglement, instead of travelling through a unique quantum channel as in the traditional protocol. Asymmetry in the double teleportation plus post-measurement retains the secrecy in the process. Despite requiring more complex control and resources, the procedure dramatically reduces the probability of success for an eavesdropper under individual attacks, because of the ignorance of the processing times in the procedure. Quantum Bit Error Rate remains in the acceptable threshold and it becomes configurable. The article depicts the double quantum teleportation procedure, the associated control to introduce the QKD scheme, the analysis of individual attacks performed by an eavesdropper, and a brief comparison with other protocols.

Keywords: quantum information; quantum cryptography; Quantum Key Distribution; BB84 protocol; teleportation

Citation: Cardoso-Isidoro, C.; Delgado, F. Shared Quantum Key Distribution Based on Asymmetric Double Quantum Teleportation. *Symmetry* **2022**, *14*, 713. https://doi.org/10.3390/sym14040713

Academic Editors: Durdu Guney, David Petrosyan and Ignatios Antoniadis

Received: 9 February 2022
Accepted: 25 March 2022
Published: 1 April 2022

1. Introduction

With the development of quantum applications, particularly quantum cryptography [1], new cryptosystems intended to be unconditionally secure are being developed. Such cryptosystems are commonly composed of a sender and a receiver assuming to share an Encryption and a Decryption key [2]. Then, a message can be encrypted and transmitted from the sender's end to the receiver's end. Along the way, an eavesdropper can try to steal the key intended to be transmitted between them. For instance, experimental implementations are led using imperfect photon detectors, thus allowing the loss of some photons [3] and allowing an intruder to tamper these imperfect devices to obtain advantages against the security of the protocol [4,5]. Due to this feasibility, it is necessary to strengthen the security in all cryptosystems.

With this purpose, new research aiming to obtain better unbreakable ways of key distribution between two parties has been conducted. Such development has boosted technology implementing Quantum Key Distribution (QKD). There, two entities (sender and receiver) can communicate securely to set codification keys. The peculiarity of quantum cryptography is the use of fundamental aspects of quantum mechanics such as the

uncertainty principle [6], entanglement [7], and the quantum measurement theory [8] to provide a set of constraints on the communication channel to make it safer [9]. The generation of this quantum key can be distributed through many protocols developed for this purpose [10]. Some existing QKD protocols include BB84 [11], B92 [12], SARG04 [13], and E91 [14].

In this sense, quantum cryptography has become a leading development for the secure transmission of data [15]. After the last-mentioned QKD protocols, quantum cryptography has been refining its methods and complexity to keep off quantum hacking as a counterpart [16]. Thus, post-quantum cryptography pursues cryptography algorithms being secure against cryptanalytic attacks performed by quantum computers [17]. Otherwise, QKD can be made unconditionally secure over arbitrarily long distances against attacks by an eavesdropper [18]. Thus, quantum cryptography is requiring more complex procedures including quantum processing to enhance security.

In another trend, for the development of communications, quantum teleportation has played a central role in communication enhancements. Various approaches seeking experimental implementations of such algorithms soon emerged [19,20]. Since then, the great importance of the development of quantum teleportation has boosted applications in quantum communication to a large extent. Some of them include the creation of quantum networks [21], cryptography applications regarding quantum computing systems [22], settlement of photonic quantum computing [23], and particularly teleportation-based quantum cryptography protocols [24] as complementary scaffolding procedures improving its efficiency and security.

Improvements in the quality of teleportation involve new approaches. Some of them for long-distance quantum teleportation with the use of a fiber-delayed Bell state measurement (BSM) [25] and others using optical fiber to avoid using large-aperture optics and other complex techniques [26,27]. Teleportation is being combined with quantum strategies as a causal order [28] to remove some underlying noisy effects. Recently, an analysis for a double teleportation process for the same input state has been presented in [29,30]. In such a scenario, one main party (Alice) has prepared the input state and then shared two entangled resources with another two parties (here called Bob_0 and Bob_1) keeping one qubit of each pair. A central resource, in principle accessible for the three parties, works as a control to decide who of the Bob's will receive the teleported state. With such a scheme, cryptography protocols can be performed to set secure authentication methods [30].

This work presents a BB84-like shared protocol exploiting double teleportation to generate controlled correlated information to set a quantum key between two final parties. Despite BB84 being one of the first quantum cryptography protocols, it has remained as a heraldic one. Nowadays, variations of such protocol are still proposed to improve some of its features, thus remaining valid in the contemporary literature. While the traditional BB84 protocol employs a single quantum channel to transmit the key in the form of two-level states first settled on an unknown basis for the receiver, in the current proposal, non-local features of double teleportation combined with asymmetric post-processing allow us to assemble this key during it. It reduces the action time for an eavesdropper by reducing his rate of success while the key has still not been assembled. Some outstanding outcomes in this procedure are:

- A notable rate of success for the coincident basis scenario between the sender and the receiver closer to the ideal case in the original BB84 protocol;
- A dramatic reduction of success for an eavesdropper under individual attacks for the undetected scenario during a reconciliation step;
- A practical reduced time of action for an eavesdropper due to the non-local properties of the key assembling and the absence of a physical quantum channel;
- A configurable setup to adjust some quantitative working features in the procedure as the eavesdropper success ratio or the Quantum Bit Error Rate (QBER).

The structure of the article is as follows. The second section introduces the protocol in the contemporary scenario of quantum cryptography. The third section develops the

main lines to perform the double teleportation and the necessary post-processing for the task, together with some remarks about its non-locality features. Then, the control of such asymmetric post-processing to distribute quantum keys between those two parties is presented in the fourth section, setting the scenario for QKD. The fifth section first discusses the contemporary validity of the BB84 protocol in the literature; then, it properly analyses the QKD protocol departing from the previous development, as well as the inclusion of an eavesdropper in the process presented to quantify the vulnerability under individual attacks in terms of its success and detection. The sixth section includes brief discussions about benchmarking for the procedure, possible effects related to decoherence, and fidelity. Conclusions are settled in the last section.

2. Introductory Remarks for Contemporary Post-Quantum Cryptography

Quantum cryptography is the science that pretends to exploit any quantum mechanical feature to perform cryptography tasks, which means methods of encryption naturally using the properties of quantum mechanics to secure and transmit data without hacking. The economy in quantum cryptography has been pursued through the main original developments despite the contemporary technology at the time those works were published. Possibly, QKD is the most important contribution to quantum cryptography by promoting the fusion of classical and quantum approaches, setting a natural incubator in which to develop the field.

The first quantum protocol for QKD was the BB84 one [11] based on quantum conjugate variables. Such protocol states a procedure to state a key in the form of a chain of zeroes and ones without a direct transmission from the sender to the receiver. Instead, the key is codified through a series of quantum resources randomly prepared by the sender on one from two orthogonal agreed bases. Then, they are stochastically found by the receiver through random measurements on such bases. In the end, the bases used are shared by both parts to conserve the identical outcomes when the bases meet. Such a procedure allows us to detect eavesdropping when it intermediately alters the coincident bases and outcomes through a different basis measurement.

Thus, QKD protocols, as that mentioned before, first used quantum correlations to set a quantum key between two parties (another one similar is the B92 [12]). Soon, other protocols appeared exploiting the statistical nature of quantum systems involved, as in the SARG04 [13]. While alternative protocols such as the E91 [14] used entanglement pairs more than just the quantum nature of states in terms of orthogonal basis in a symmetrical treatment of information to construct the key together. Moreover, Quantum Key Agreement (QKA) protocols [31] introduced a shared decision generation for the key.

When quantum computers are introduced to break quantum codes of such developments, the scenario was moved to secure protocols including quantum computer-based attacks. It has raised the post-quantum cryptography terrain to set secure protocols against quantum computer attacks. Despite this, the roadmap is unclear because some of the most current classical symmetric cryptographic protocols are still considered to be relatively secure against quantum computer attacks [32], thus it is believed that classical approaches in theoretical cryptography could be combined with quantum cryptography trends [33].

The current development introduces some elements exploiting quantum processing together with extreme features of quantum information as double teleportation, non-local operations performed via entanglement, and controlled measurements by quantum machines. Some features of the protocol also combine QKA approaches. Thus, they allocate the current proposal in the terrain of post-quantum cryptography (or quantum-safe cryptography) to set a QKD procedure reducing the eavesdropper success.

Other technology concerns should be considered because of the growing complexity of the post-quantum protocols including more complex processing and finer theoretical cryptography considerations. Such aspects are similar to those premises considered in quantum processing: quality and reliability on state generation processes, development

of coherent quantum gates to preserve their supposed quantum nature, and faithfully quantum measurement. Those aspects are remarked through the development.

3. Double Teleportation as Superposition and Parallel Post-Processing

Multiple teleportation exploits the quantum linearity to extend the traditional teleportation procedure to perform virtual transference of states and processing. In the end, global states could be recovered for concrete tasks. Quantum states obtained by multiple teleportation exhibit interesting non-local properties [29] and they could be used with cryptography purposes [30]. In this section, we will describe the process only for double teleportation (DT) with additional post-processing (PP). Then, in Section 4, we deal with the control problem (TC) to share and transfer concrete quantum states to be used for QKD purposes (QKD) in Section 5. To ease the reading, we first account in Table 1 for the key symbols (states, operators, and related key quantities) through the entire development.

Table 1. States, Gates, and Parameters involved in the analysis through each step (DT, PP, TC, QKD) of the whole QKD protocol.

Symbol	Process	Description
$\|\psi_0\rangle$	DT	Original qubit state to be teleported
$\|\psi_C\rangle$	DT	Control state to manage the final receiver in double teleportation
p_i	DT	Superposition probabilities for each receiver in double teleportation
$\|\beta_{ij}\rangle$	DT	Entangled resources for teleportation in the for of Bell states
C_U, H_0	DT	Controlled C^aNOT_b and Hadamard gates to manage the double teleportation
$\|\psi\rangle, \|\psi'\rangle$	DT	Initial state and pre-measurement state during the double teleportation process
$\|\psi_{pm}\rangle, \|\psi_{teleported}\rangle$	DT	Post-measurement and corrected states at the end of double teleportation process
$\mathcal{U}_{i_k}$	PP	Local processing operators on the qubit k in possession of party i
ω_i	PP	Parametric continuous characterization of each local processing
$C_{\mathcal{U}}$	PP	Controlled operation to apply local processing $\mathcal{U}_{i_k}$ on each receiver
$\|\psi_0^i\rangle$	PP	Output state from the each local processing on $\|\psi'\rangle$
$\|\psi_{proc}\rangle, \|\psi_{final}\rangle$	PP	Local processing operators on the qubit k in possession of party i
β_i, ϕ_m	TC	Parameters for the basis measurement of the control state
P_i	TC	Success probability for each outcome of the control measurement
K, m, j	QKD	Key parameters in the QKD process
P	QKD	Absolute rate of the success eavesdropper without reconciliation
P_E	QKD	Relative rate of the success eavesdropper with reconciliation
$P_{QBER_{abs}}, P_{QBER_{rel}}$	QKD	Absolute and relative QBER

3.1. Double Teleportation Process as Superposition

Figure 1a synthetically depicts the process followed for double teleportation immersed in the context of QKD. In the current section, we develop the double teleportation process as it was originally presented [29]. As it was stated, one party (Alice) generates secretly an arbitrary state $|\psi_0\rangle$ (known or unknown) to then potentially transmit it in superposition by teleportation to other two parties (Bob_0 and Bob_1). The presence of an eavesdropper (Eve) acting on Bob_1 is possible, so it is shown in Figure 1a,b, but her action will be considered and depicted at the end. In this case, instead of the traditional algorithm, the process intends to virtually teleport such state to those two simultaneous receivers, Bob_0 and Bob_1 [29].

The process begins with the main qubit $|\psi_0\rangle$ to be teleported in possession of Alice, where $|\psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. In this work, the Bell states will be written: $|\beta_{ij}\rangle = \frac{1}{\sqrt{2}}(|0\ j\rangle + (-1)^i|1\ j \oplus 1\rangle)$. Then, a pair of Bell entangled resources $|\beta_{00}\rangle_{12}, |\beta_{00}\rangle_{34}$ are prepared to be shared with each one of both receivers to implement the teleportation process (subscripts state the numbering of the resources). In the process, a control state is required to rule the quantum transmission on a concrete receiver $|\psi_C\rangle = \sum_{i=0}^{1} \sqrt{p_i}|i\rangle_C$, with: $\sum_{i=0}^{1} p_i = 1$. Thus,

if control is settled in the state $|0\rangle_C$ then $|\psi_0\rangle$ is teleported to Bob_0, otherwise to Bob_1 if the control is $|1\rangle_C$. Then, the global initial state being considered becomes:

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_C\rangle \otimes |\beta_{00}\rangle_{12} \otimes |\beta_{00}\rangle_{34} \tag{1}$$

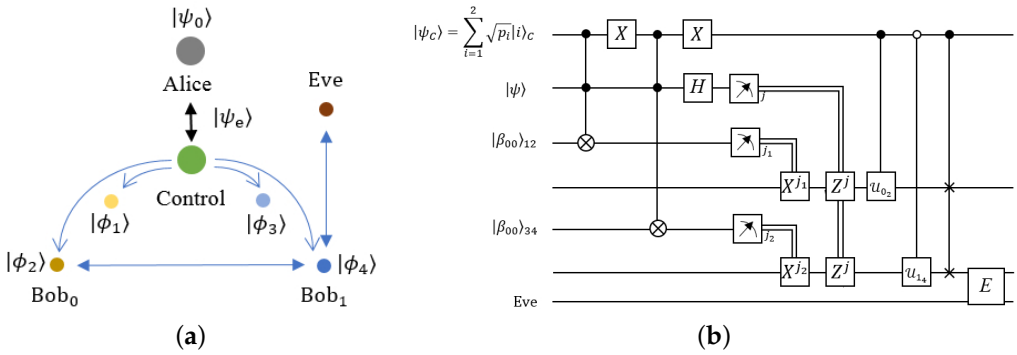

Figure 1. (**a**) Three main parties performing double controlled teleportation with a central control accessible for all of them; a possible eavesdropper is present; (**b**) Quantum circuit representing the main elements of the double teleportation process.

Then, the following controlled gate is applied: $C_U = |0\rangle_C\langle 0| \otimes C^0NOT_1 + |1\rangle_C\langle 1| \otimes C^0NOT_3$, which is clearly unitary [29]. In fact, this gate is basically a pair of Toffoli gates each one followed by another:

$$\begin{aligned} C_U &= \text{Toff}_{C,0,3} \cdot \mathbf{X}_C \cdot \text{Toff}_{C,0,1} \cdot \mathbf{X}_C \\ &= (|0\rangle_C\langle 0| \otimes \mathbf{1}_3 + |1\rangle_C\langle 1| \otimes C^0NOT_3) \cdot (|0\rangle_C\langle 0| \otimes C^0NOT_1 + |1\rangle_C\langle 1| \otimes \mathbf{1}_1) \end{aligned} \tag{2}$$

Then, remarking that $C^aNOT_b = |0\rangle_a\langle 0| \otimes \mathbf{1}_b + |1\rangle_a\langle 1| \otimes \mathbf{X}_b$ (there, $\mathbf{X}$ is the NOT gate), and considering that $\mathbf{X}_a|\beta_{00}\rangle_{ab} = |\beta_{01}\rangle_{ab}$, the double teleportation process follows by applying a Hadamard gate on the qubit to be teleported, $|\psi'\rangle = H_0 \cdot C_U|\psi\rangle$:

$$\begin{aligned} |\psi'\rangle &= \sqrt{p_0}|0\rangle_C[\alpha_0|+\rangle_0|\beta_{00}\rangle_{12} + \alpha_1|-\rangle_0|\beta_{01}\rangle_{12}]|\beta_{00}\rangle_{34} \\ &\quad + \sqrt{p_1}|1\rangle_C|\beta_{00}\rangle_{12}[\alpha_0|+\rangle_0|\beta_{00}\rangle_{34} + \alpha_1|-\rangle_0|\beta_{01}\rangle_{34}] \end{aligned} \tag{3}$$

$$\begin{aligned} &= \frac{|0\rangle_0}{2}\Big(\sqrt{p_0}|0\rangle_C(|0\rangle_1\mathbf{1}_2 + |1\rangle_1\mathbf{X}_2)|\psi_0\rangle_2|\beta_{00}\rangle_{34} \\ &\quad + \sqrt{p_1}|1\rangle_C(|0\rangle_3\mathbf{1}_4 + |1\rangle_3\mathbf{X}_4)|\psi_0\rangle_4|\beta_{00}\rangle_{12}\Big) \\ &\quad + \frac{|1\rangle_0}{2}\Big(\sqrt{p_0}|0\rangle_C(|0\rangle_1\mathbf{Z}_2 + |1\rangle_1\mathbf{X}_2\mathbf{Z}_2)|\psi_0\rangle_2|\beta_{00}\rangle_{34} \\ &\quad + \sqrt{p_1}|1\rangle_C(|0\rangle_3\mathbf{Z}_4 + |1\rangle_3\mathbf{X}_4\mathbf{Z}_4)|\psi_0\rangle_4|\beta_{00}\rangle_{12}\Big) \end{aligned} \tag{4}$$

dropping the tensor products for the sake of simplicity, remarking that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, and expanding some Bell states to express it in terms of $|\psi_0\rangle$ [29]. Clearly, those steps state an extension of the traditional teleportation algorithm [34] for qubits. Finally, performing measurements on the original qubit to teleportate, as well as the qubits 1 and 3 (being part of the entangled resources) with respective outcomes s_0, s_1 and s_3, we get the un-normalized post-measurement state:

$$|\psi_{pm}\rangle = \frac{|s_0\rangle_0|s_1\rangle_1|s_3\rangle_3}{2\sqrt{2}} \otimes \Big(\sqrt{p_0}|0\rangle_C|s_3\rangle_4\mathbf{X}_2^{s_1}\mathbf{Z}_2^{s_0}|\psi_0\rangle_2 + \sqrt{p_1}|1\rangle_C|s_1\rangle_2\mathbf{X}_4^{s_3}\mathbf{Z}_4^{s_0}|\psi_0\rangle_4\Big) \tag{5}$$

where if the exponent on an operator is zero, it implies that such operator is omitted. It is easy to notice that each one of the eight possible measurement outcomes occur with

probability of $\frac{1}{8}$. Thus, normalizing and finally, as a function of the outcomes, applying the generic correction $\mathbf{Z}_2^{s_0}\mathbf{X}_2^{s_1}\mathbf{Z}_4^{s_0}\mathbf{X}_4^{s_3}$ ($\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ are the Pauli operators), we obtain [29]:

$$|\psi_{teleported}\rangle = \sqrt{p_0}|0\rangle_C|\psi_0\rangle_2|0\rangle_4 + \sqrt{p_1}|1\rangle_C|0\rangle_2|\psi_0\rangle_4 \tag{6}$$

where we dropped the states for the qubits 1 and 3, as well as the original qubit for the sake of simplicity. This state represents the virtual teleportation to both Bob's. Figure 1b shows the quantum circuit of the process depicted, based on the traditional teleportation algorithm [34]. Black dots in the controlled operations are traditional controls C^aG_b, while white dots corresponds to negative controls: $\mathbf{X}_a \cdot C^aG_b \cdot \mathbf{X}_a$. The action of Eve is just indicative, we deal with the eavesdropping intervention below. In the next subsection, we will perform certain post-processing to introduce the necessary tasks to set QKD.

3.2. Post-Processing Following to Double Teleportation

In the last expression, each outcome still can be managed by the control state to perform different processing on each virtual teleported qubit. Applying the operator (see Figure 1b on the right in the form of a pair of controlled gates):

$$\begin{aligned} C_{\mathcal{U}} &= (|0\rangle_C\langle 0| \otimes \mathcal{U}_{0_2} + |1\rangle_C\langle 1| \otimes \mathbf{1}_2) \cdot (|0\rangle_C\langle 0| \otimes \mathbf{1}_4 + |1\rangle_C\langle 1| \otimes \mathcal{U}_{1_4}) \\ &= |0\rangle_C\langle 0| \otimes \mathcal{U}_{0_2} \otimes \mathbf{1}_4 + |1\rangle_C\langle 1| \otimes \mathbf{1}_2 \otimes \mathcal{U}_{1_4} \end{aligned} \tag{7}$$

Such asymmetric post-processing following to the double teleportation will set the successful secrecy for the QKD procedure. Thus, by defining $|\psi_0^{i-1}\rangle_{2i} = \alpha_0^i|0\rangle_{2i} + \alpha_1^i|1\rangle_{2i}$ (with $i = 1, 2$) as the output of each processing $\mathcal{U}_{(i-1)_{2i}}$, then we will get:

$$|\psi_{proc}\rangle = C_{\mathcal{U}}|\psi_{teleported}\rangle = \sqrt{p_0}|0\rangle_C \otimes \mathcal{U}_{0_2}|\psi_0\rangle_2 \otimes |0\rangle_4 + \sqrt{p_1}|1\rangle_C \otimes |0\rangle_2 \otimes \mathcal{U}_{1_4}|\psi_0\rangle_4 \tag{8}$$

$$= \sqrt{p_0}|0\rangle_C \otimes |\psi_0^0\rangle_2 \otimes |0\rangle_4 + \sqrt{p_1}|1\rangle_C \otimes |0\rangle_2 \otimes |\psi_0^1\rangle_4 \tag{9}$$

As a useful possibility for further applications, we consider the final transference of the state from Bob_0 to Bob_1 by applying a controlled *SWAP* to send the processed output state on the qubit 4: $C_{SWAP2,4} = |0\rangle_C\langle 0| \otimes SWAP_{2,4} + |1\rangle_C\langle 1| \otimes \mathbf{1_2} \otimes \mathbf{1_4}$ (see Figure 1b on the right).

Note operations $C_{\mathcal{U}}$ and $C_{SWAP2,4}$ are few practical because qubits $C, 2$ are far away from qubit 4. We show them in such last synthetic forms, but they can be equivalently achieved using additional entangled resources between Alice/Bob_0 and Bob_1. The details about the equivalence of such processes are given in the Appendices A and B. There, related techniques required are delayed measurements [35] and quantum controlled measurements [36,37]. In any case, it gives the following state settled on the qubit 4 in possession of Bob_1:

$$|0\rangle_2 \otimes |\psi_{final}\rangle \equiv C_{SWAP2,4}|\psi_{proc}\rangle = |0\rangle_2 \otimes (\sqrt{p_0}|0\rangle_C \otimes |\psi_0^0\rangle_4 + \sqrt{p_1}|1\rangle_C \otimes |\psi_0^1\rangle_4) \tag{10}$$

disregarding the separable qubit 2. In addition, Alice will decide to measure the control state on an eligible orthogonal basis $\{|b_0\rangle_C, |b_1\rangle_C\}$ given by $|0\rangle_C = \beta_0|b_0\rangle_C + e^{i\phi_m}\beta_1|b_1\rangle_C$, $|1\rangle_C = e^{-i\phi_m}\beta_1|b_0\rangle_C - \beta_0|b_1\rangle_C$, with $\phi_m, \beta_0, \beta_1 \in \mathbf{R}$, $\beta_0^2 + \beta_1^2 = 1$. It means, $|\psi_{final}\rangle$ can be written as:

$$|\psi_{final}\rangle = \sqrt{p_0}(\beta_0|b_0\rangle_C + e^{i\phi_m}\beta_1|b_1\rangle_C) \otimes |\psi_0^0\rangle_4 + \sqrt{p_1}(e^{-i\phi_m}\beta_1|b_0\rangle_C - \beta_0|b_1\rangle_C) \otimes |\psi_0^1\rangle_4 \tag{11}$$

to ease the identification of the measurement outcomes in such basis. In the following, we will commonly drop the labels C for the control and 4 for the qubit 4, which now become clear from the development.

3.3. Entanglement and Non-Locality Activation

The double teleportation plus post-processing process depicted at this point has been previously analysed in terms of generation of non-local properties [29]. In fact, after of the measurement of the control state on the basis $\{|b_0\rangle, |b_1\rangle\}$, a wide type of entangled states could be generated if each Bob introduces additional local resources. Using the concurrence as entanglement measurement, it was shown that they can range from separable states to maximally entangled ones. In addition, the Clauser-Horne-Shimony-Holt (CHSH) inequality has been used to demonstrate the non-locality activation through the involved quantity $S(|\psi\rangle, \theta) \equiv |E(S^A, S^B) + E(S^A, S^{B'}) + E(S^{A'}, S^B) - E(S^{A'}, S^{B'})|$ (there, $E(S^1, S^2)$ is the correlation between the measurements S^1, S^2). This quantity reaches the Tsirelson's bound in the process, indicating the non-locality activation. Such analysis dealt with the measurement basis settled by the operators $\{S^A = \mathbf{X}, S^{A'} = \mathbf{Z}\}$ and $\{S^B = \cos\theta\mathbf{X} + \sin\theta\mathbf{Z}, S^{B'} = -\sin\theta\mathbf{X} + \cos\theta\mathbf{Z}\}$ to get the correlations on a setup testing of the CHSH inequality. It means that the state transference depicted strongly undergoes through a non-local process generating non-locality correlations. Such non-local transference has been also demonstrated between a couple of semiconductor microcavities connected by optical fiber for solid-state physics [38,39] using geometric quantum discord and concurrence as main non-locality quantifiers. Despite the process presented in that article proposing entanglement to generate quantum states at distance, those works set a certain kind of alternative technology to share or generate quantum states in a second party using non-classical light.

3.4. Concrete Post-Processing and Information Transference via Post-Measurement

We will consider the asymmetric post-processing performed by Bob_0 and Bob_1 as:

$$\mathcal{U}_{i_{2i+2}} = \cos\omega_i\mathbf{1} + i\sin\omega_i\mathbf{Y}, \quad i = 0, 1 \tag{12}$$

characterized by the parameter ω_i. Thus, asymmetry is introduced by the differentiated parameter ω_i in each post-processing, together with the different value for the strength of the teleportation, p_i and the control measurement. By expressing $|\psi_0\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ in its Bloch representation, in such scenario, the probabilities to get the measurement outcome of $|b_0\rangle$ or $|b_1\rangle$ becomes [30]:

$$P_0 = \beta_0^2 p_0 + \beta_1^2 p_1 + 2\beta_0\beta_1\sqrt{p_0 p_1}\cos\phi_m(\cos\Delta^-\omega - \tan\phi_m\sin\Delta^-\omega\sin\theta\sin\phi) \tag{13}$$

$$P_1 = \beta_1^2 p_0 + \beta_0^2 p_1 - 2\beta_0\beta_1\sqrt{p_0 p_1}\cos\phi_m(\cos\Delta^-\omega - \tan\phi_m\sin\Delta^-\omega\sin\theta\sin\phi) \tag{14}$$

where $\Delta^\pm\omega \equiv \omega_0 \pm \omega_1$. Because $P_0 + P_1 = 1$, for such reason if $\omega_0 = \omega_1$, then the probability to get $|\psi_0^0\rangle = |\psi_0^1\rangle$ is one in any case. As we will see, we can use the previous process to generate and distribute quantum keys, if Alice works together with Bob_0 as a central computer performing part of the processing, while Bob_1 is an associated user.

4. Transference of Programmed Quantum States Using Double Teleportation

In the current section, we deal with the control problem for the transference to Bob_1 of a programmed state prepared by Alice/Bob_0. The post-processing in (12) is stated to introduce a public and classical authentication fingerprint ω_1. Then, we will assume this fingerprint could be known as an extreme case by an eavesdropper to emphasize the quantum features of the procedure. Without such authentication, the remaining state exchange will not work [30]. In addition, as we will note in the procedure to be presented, an advantage is that the state being transferred does not exist until it becomes assembled by the collaboration of the involved parts.

4.1. Generation of Quantum States as a Collaboration among Three Parties

Following the discussion in the last section, by inserting explicitly the action of (12) on $|\psi_0\rangle$:

$$|\psi_0^j\rangle = \cos\omega_j(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle) + \sin\omega_j(e^{i\phi}\sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle) \tag{15}$$

with $j = 0, 1$. We note that if $e^{i\phi} \in \mathbf{R}$, it means such parameter takes one of the two possible values $\phi_p = 0, \pi$ or $e^{i\phi_p} = (-1)^p$, $p = 0, 1$. In such case, the last expression naturally states an orthogonal basis defined by the couple of vectors:

$$|0\rangle_{\theta,p} = \cos\frac{\theta}{2}|0\rangle + (-1)^p\sin\frac{\theta}{2}|1\rangle \tag{16}$$

$$|1\rangle_{\theta,p} = (-1)^p\sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle \tag{17}$$

they could be selected through the initial election of $|\psi_0\rangle$ on the Bloch sphere meridian containing the states $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle$. It still leaves sufficient room to choose a quasi arbitrary state. Integrating those expressions in (11), we get:

$$\begin{aligned}|\psi_{final}\rangle = {} & e^{-i\phi_m}|b_0\rangle\left[(\sqrt{p_0}\beta_0\cos\omega_0 e^{i\phi_m} - \sqrt{p_1}\beta_1\cos\omega_1)|0\rangle_{\theta,p}\right.\\ & \left.+(\sqrt{p_0}\beta_0\sin\omega_0 e^{i\phi_m} - \sqrt{p_1}\beta_1\sin\omega_1)|1\rangle_{\theta,p}\right]\\ & +|b_1\rangle\left[(\sqrt{p_0}\beta_1\cos\omega_0 e^{i\phi_m} + \sqrt{p_1}\beta_0\cos\omega_1)|0\rangle_{\theta,p}\right.\\ & \left.+(\sqrt{p_0}\beta_1\sin\omega_0 e^{i\phi_m} + \sqrt{p_1}\beta_0\sin\omega_1)|1\rangle_{\theta,p}\right]\end{aligned} \tag{18}$$

For further applications, we will require certain coefficients of each pair $|0\rangle_{\theta,p}, |1\rangle_{\theta,p}$ in the previous expression become zero. It is only possible if $e^{i\phi_m} \in \mathbf{R}$, meaning that $\phi_m = 0, \pi$. Then, $e^{i\phi_m} = (-1)^m$, $m = 0, 1$. In such case, the probabilities (13) and (14) for the measurements on the control state are:

$$P_0 = \beta_0^2 p_0 + \beta_1^2 p_1 + 2\beta_0\beta_1\sqrt{p_0 p_1}(-1)^m\cos\Delta^-\omega \tag{19}$$

$$P_1 = \beta_1^2 p_0 + \beta_0^2 p_1 - 2\beta_0\beta_1\sqrt{p_0 p_1}(-1)^m\cos\Delta^-\omega \tag{20}$$

4.2. General Notation for the Control of Post-Selection Problem

In the current subsection, we are interested in the post-selection by Alice/Bob$_1$ of certain states as well as in the control and Bob$_1$ systems. With that purpose, we develop a general notation to solve the problem. First, by defining:

$$f_k(\omega) = \begin{cases}\cos\omega, & k = 0\\ \sin\omega, & k = 1\end{cases} \tag{21}$$

then, clearly $|\psi_0^j\rangle = \sum_{k=0}^{1} f_k(\omega_j)|k\rangle_{\theta,p}$. In those terms, $|\psi_{final}\rangle$ reads:

$$|\psi_{final}\rangle = \sum_{j=0,1}(-1)^{mj}|b_j\rangle\sum_{k=0,1}|k\rangle_{\theta,p}(\sqrt{p_0}\beta_{0\oplus j}f_k(\omega_0) - (-1)^{j+m}\sqrt{p_1}\beta_{1\oplus j}f_k(\omega_1)) \tag{22}$$

If then Alice/Bob$_0$ pretends to control the post-selection of $|b_j\rangle$ and $|k\oplus 1\rangle_{\theta,p}$, two conditions should be imposed. The first one is:

$$\sqrt{p_0}\beta_{0\oplus j}f_k(\omega_0) = (-1)^{j+m}\sqrt{p_1}\beta_{1\oplus j}f_k(\omega_1) \tag{23}$$

which post-selects one of $|k \oplus 1\rangle_{\theta,p}, k = 0, 1$ for certain j. It could be solved by demanding:

$$0 < K \equiv \frac{\sqrt{p_1}\beta_{1\oplus j}}{\sqrt{p_0}\beta_{0\oplus j}}, \quad K \in \mathbf{R}^+ \tag{24}$$

Such a condition states a possible asymmetric treatment ($K \neq 1$) to introduce the secrecy of the QKD procedure [29]. Such condition states an asymmetric treatment to introduce the secrecy of the QKD procedure because the transmitted state to Bob_1 remains uncertain. It immediately implies the fulfilling of:

$$f_k(\omega_0) = (-1)^{j+m} K f_k(\omega_1) \tag{25}$$

Equation (25) states the way to select ω_0 when ω_1 is first settled choosing certain value for K stating certain secret asymmetry in the election (together with j, m, all those parameters under the control of Alice/Bob_0). Figure 2a,b show such process for $k = 0$ and $k = 1$ respectively (remembering that the selected state for Bob_1 is $k \oplus 1$). If the restriction $\omega_1 \in [0, \frac{\pi}{2}]$ is settled (such condition it is not completely necessary but it eases some further expressions), upon the selection of $K > 0, j + m = 0$, then ω_0 could be selected as it is indicated by the green circles in both figures ($K > 1$ or $K < 1$); otherwise, if $K > 0, j + m = 1$, ω_0 could be selected as in the red circles ($K > 1$ or $K < 1$). There, we restrict $\omega_0 \in [0, \pi]$ for $k = 0$ and $\omega_0 \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ for $k = 1$. Note in any case that $f_{k\oplus 1}(\omega_0) > 0$ will fulfill. Consequently, the election of K stated by (24) relates p_0 with β_0. Those relations are shown in Figure 2c,d for $k = 0$ and $k = 1$ respectively. Each red curve corresponds to certain K value being selected. While $K > 0$, the darkest red curves show the lowest values for $K \approx 0$, and the lightest ones the largest values for $K \to \infty$.

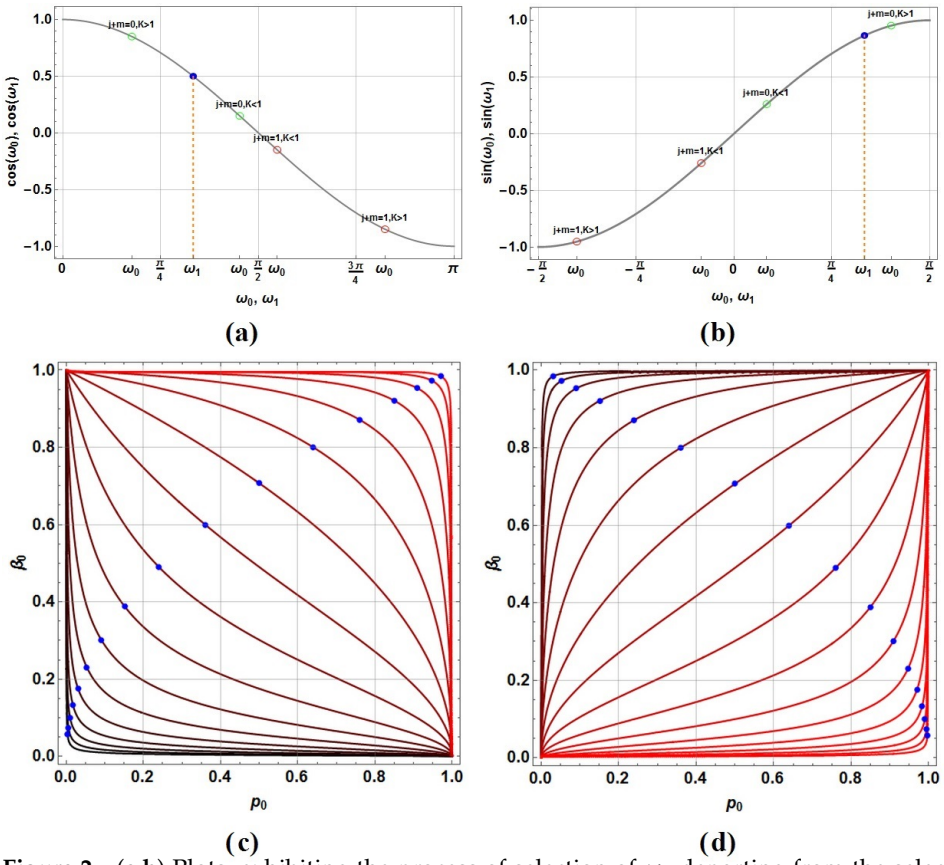

Figure 2. (**a**,**b**) Plots exhibiting the process of selection of ω_0 departing from the selection of ω_1 through the condition (25) for each case $k = 0$ (left) or $k = 1$ (right). (**c**,**d**) Possible values for the combination of p_0, β_0 upon the prior selection of K (each red curve) for each case $k = 0$ (left) or $k = 1$ (right); blue dots show the values of $p_0 = \frac{1}{1+K}$ maximizing P_j.

The second condition is obtained by substituting the first condition in the probability of success (13) or (14) for $|b_j\rangle$:

$$\begin{aligned} P_j &= p_0\beta_{0\oplus j}^2 + p_1\beta_{1\oplus j}^2 - 2\sqrt{p_0p_1}\beta_0\beta_1(-1)^{j+m}\cos\Delta_\omega^- \\ &= p_0\beta_{0\oplus j}^2(1+K^2-2K(-1)^{j+m}\cos\Delta_\omega^-) \end{aligned} \tag{26}$$

by choosing a high value for P_j (ideally $P_j = 1$). By defining $c_\omega^- = (-1)^{j+m}\cos\Delta_\omega^-$, we note that P_j depends from p_0, β_0, and c_ω^- in general, as Figure 3 shows. Figure 3a,b show the contours on which P_j become constant in agreement with the color scale on the right (for $j = 0, 1$ on the left and right respectively). Below, Figure 3c,d show the three dimensional version of Figure 2c,d with their K values shown in black in their top. In addition, each contour was additionally coloured in agreement with their P_j value in each point of the space (from the reddest for $P_j \approx 0$ to the bluest for $P_j \approx 1$, also in agreement with the color bar besides and with the previous plots). In fact, the solutions are first found by selecting K and then intersecting each lower plot with its corresponding upper plot (for the same j value). Despite, c_ω^- is not an independent parameter as the last intersection shows.

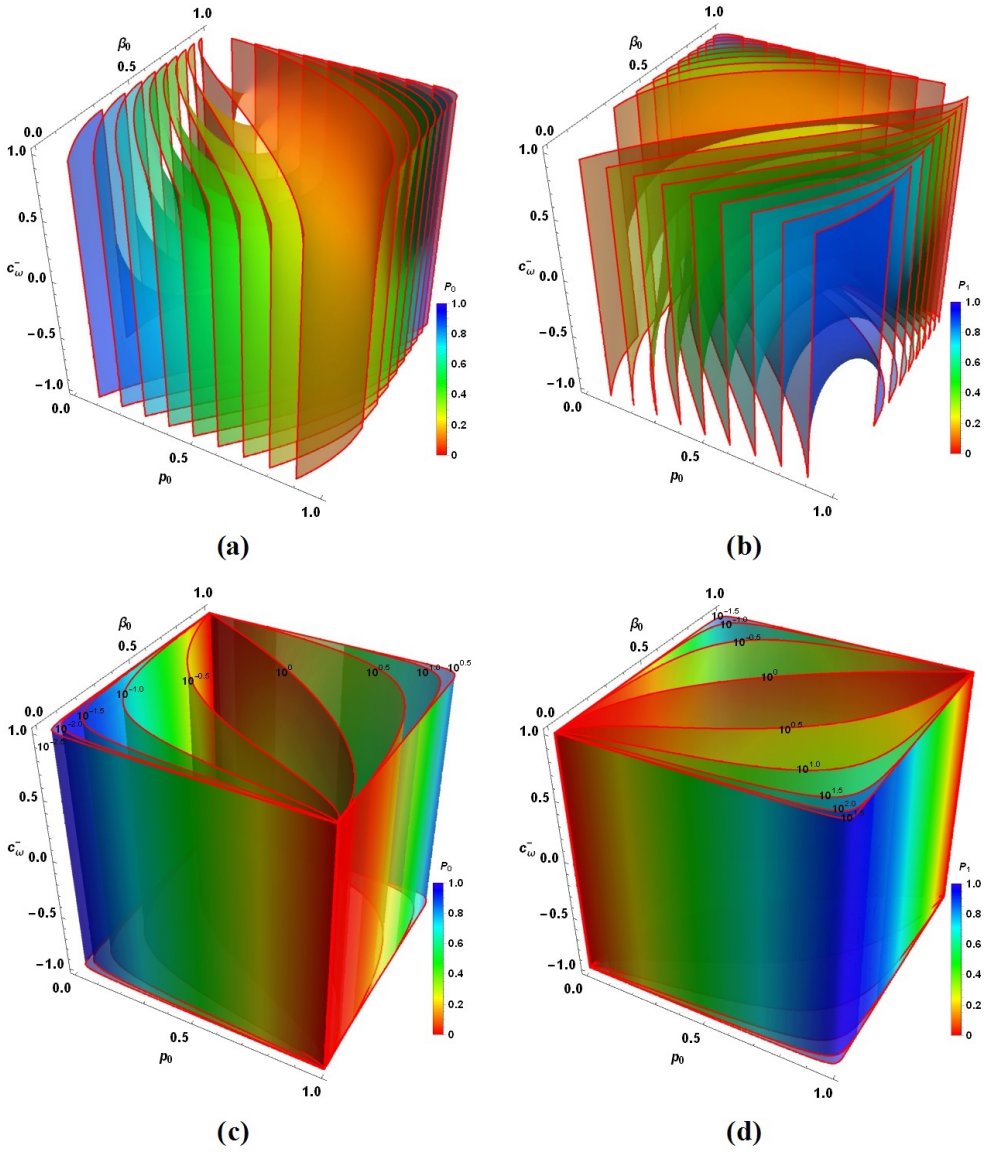

Figure 3. (**a**,**b**) Contour plots of P_j for $j = 0, 1$ respectively as function of p_0, β_0, and c_ω^-. (**c**,**d**) Three-dimensional version of plots in Figure 2c,d, now including c_ω^- and coloured from red ($P_j = 0$) to blue ($P_j = 1$) in agreement with P_j values through them for $j = 0, 1$ respectively.

4.3. Control Prescriptions for the Quantum State Transference

In fact, we can analyse c_ω^- in terms of k, ω_1 and K (using the fact $f_{k\oplus 1}(\omega_0) > 0$ with $\omega_1 \in [0, \frac{\pi}{2}]$):

$$\frac{c_\omega^-}{(-1)^{j+m}} = \cos\Delta_\omega^- = \cos(\omega_0 - \omega_1) = f_k^2(\omega_1)(-1)^{j+m}K + f_{k\oplus 1}(\omega_1)\sqrt{1 - K^2 f_k^2(\omega_1)} \quad (27)$$

Thus, when each upper contour intersects to their lower partner, it generates the affordable solutions. Such solutions are shown in the Figure 4 but in the variables to be selected, ω_1, K, j, k, m (remembering that the selected state for Bob_1 is $k \oplus 1$): (a) $k = 0, j + m = 0$, (b) $k = 0, j + m = 1$, (c) $k = 1, j + m = 0$, and (d) $k = 1, j + m = 1$ (in fact, $j \oplus m = 0, 1$, but we will maintain just those simpler expressions in the following). Curves in each plot show some affordable solutions (black region) for each c_ω^- value in color from red ($c_\omega^- = -1$) to blue ($c_\omega^- = 1$). We have plotted the region only in the more convenient interval for $\omega_1 \in [0, \frac{\pi}{2}]$ being congruent with the previous remark. $K > 0$ values are not restricted in their strength, but clearly $K > 1$ reduces the possible solutions.

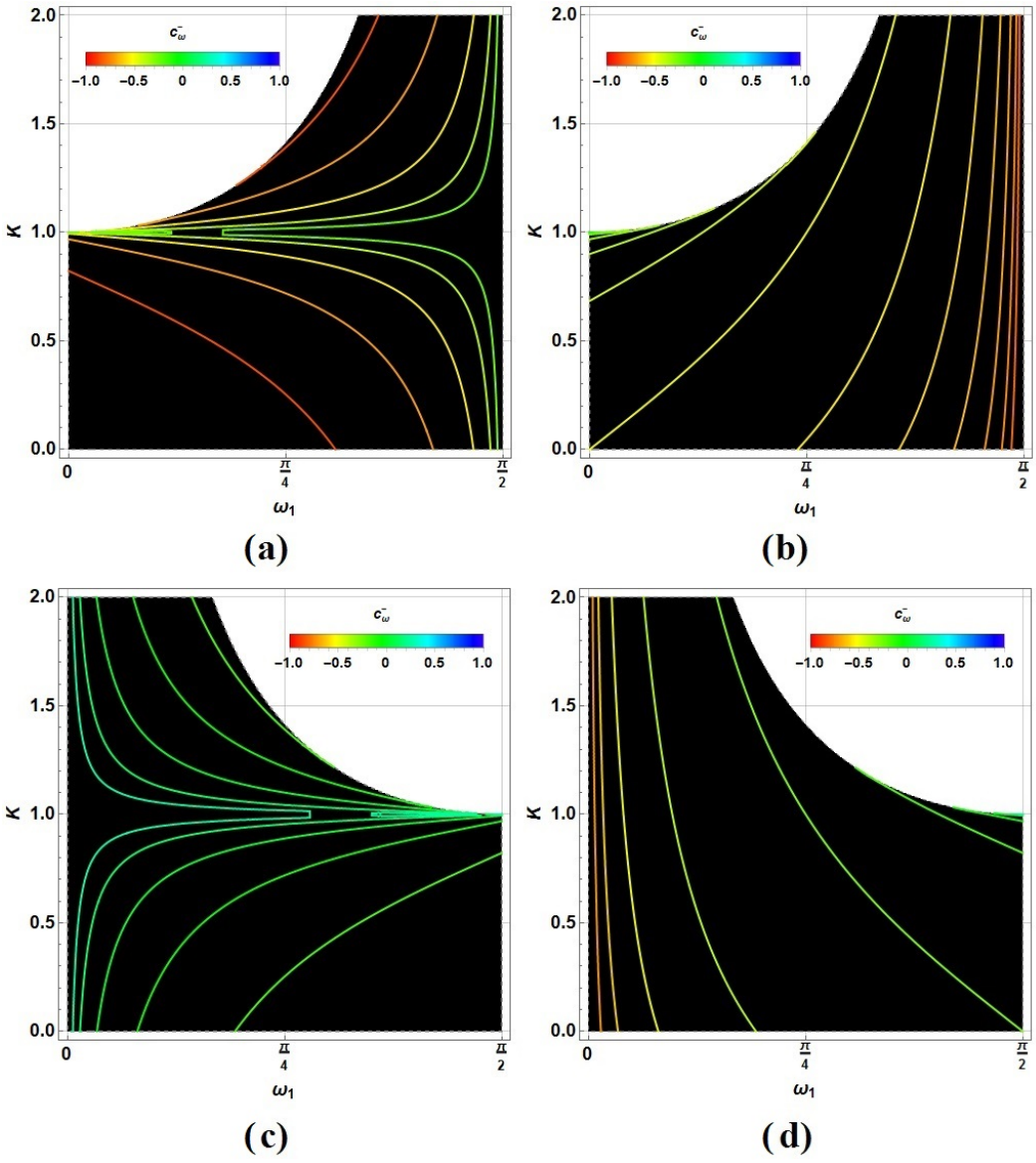

Figure 4. Solutions for c_ω^- as function of ω_1 and K in color (reddest for $c_\omega^- \approx -1$ and bluest for $c_\omega^- \approx 1$) for (**a**) $k = 0,\ j + m = 0$, (**b**) $k = 0,\ j + m = 1$, (**c**) $k = 1,\ j + m = 0$, and (**d**) $k = 1,\ j + m = 1$.

Solving (24) for $\beta^2_{0\oplus j}$ and introducing the overall restrictions in (26), we get the following expression for P_j:

$$P_j = \frac{p_0(1-p_0)}{1-p_0(1-K^2)}\left[1+K^2-2K(f_k^2(\omega_1)K-(-1)^{j+m}f_{k\oplus 1}(\omega_1)\sqrt{1-K^2f_k^2(\omega_1)}\right] \quad (28)$$

The coefficient there, $C_0(p_0,K) \equiv \frac{p_0(1-p_0)}{1-p_0(1-K^2)}$, depends only on p_0 and K. An easy analysis shows that such coefficient reaches its maximum for $p_{0_{max}} = \frac{1}{1+K}$ becoming $C_{0_{max}} = \frac{1}{(1+K)^2}$. Such optimal values are also shown for each K-curve in Figure 2c,d with blue dots. Because it is zero in their edges $p_0 = 0, 1$, then the values of such coefficient are folded in the intervals $p_0 \in [0, p_{0_{max}}]$ and $p_0 \in [p_{0_{max}}, 1]$.

Figure 5 depicts P_j for (a) $k = 0, j+m = 0$, (b) $k = 0, j+m = 1$, (d) $k = 1, j+m = 0$, and (e) $k = 1, j+m = 1$ (remembering that the selected state transmitted to Bob_1 is $k \oplus 1$). They are three-dimensional regions (transparent clear gray regions) under the main maximal surface plotted in dark gray, which corresponds to the two folded points generated vertically by $p_0 \in [0,1]$ (shown by the arrows in the Figure 5a,b,d,e). Figure 5c,f show the comparison between the corresponding maximum values in each case, (c) $k = 0$ and (f) $k = 1$ respectively, remarking the advantage for $j+m = 1$ (green) against $j+m = 0$ (red), thus it is better to choose m with a different parity of the selected j. In such cases, ω_1 could be selected almost openly, to then select those K values reaching P_j at least near from 1, thus controlling better the stochastic selection of $|b_j\rangle$. Note in the figures, that the regions have been maintained in $\omega_1 \in [0, \frac{\pi}{2}]$ as it was initially recommended in the procedure. In addition, we have not extended the interval for K further than $K = 1$, because plot regions there become restricted to narrower non-rectangular regions as it was shown in the Figure 4, becoming unpractical because of the restricted combinations of ω_1 and K values able to be selected. Still, in the practice, $K > 1$ also provides valuable solutions.

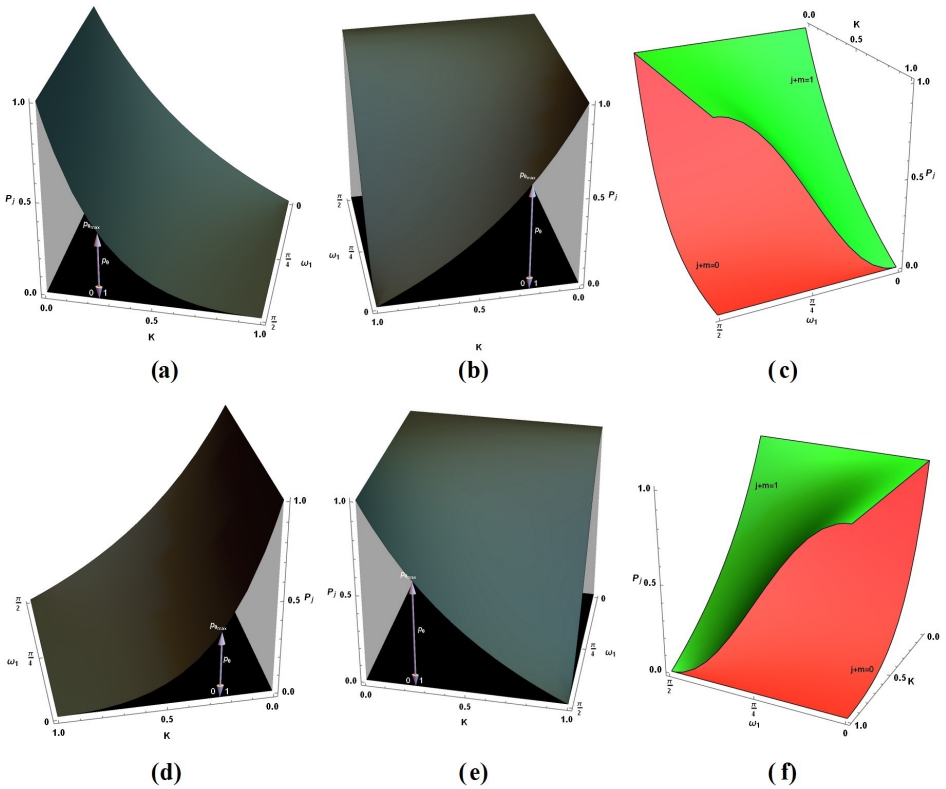

Figure 5. Plots for P_j in (28) as function of ω_1 and K for the cases (**a**) $k = 0$, $j+m = 0$, (**b**) $k = 0$, $j+m = 1$, (**c**) $k = 1$, $j+m = 0$, and (**d**) $k = 1$, $j+m = 1$. Comparisons for the cases (**e**) $k = 0$, and (**f**) $k = 1$ exhibiting the advantage for $j+m = 1$ to reach higher values for P_j.

Another important remark should be stated—Despite the election of $p_{0_{max}}$ is quite recommendable to maximize P_j. It implies that Alice should decide to prepare the control state determining K from the beginning. Instead, the election of K independently of p_0 opens the opportunity to not fix the form of the states until the application of $\mathcal{U}_{0_2}$ when ω_0 should be settled (at least around a certain neighborhood of $p_{0_{max}}$ to reach the higher values of P_j, still keeping the efficiency of the process).

5. A QKD Protocol Based on a Shared Collaboration among Three Parties

Despite many cryptography developments for QKD having emerged since 1984 after the BB84 protocol, most of them to a large extent are based on it. By proposing modifications or alternative approaches, they have improved the security or efficiency, together to prevent more sophisticated kinds of attack, particularly those possibly coming from a quantum computer. Thus, some of them have received names by their authors, as it occurs in the area. Thus, BB84 based protocols are completely valid nowadays. Among the BB84-like protocols for QKD, we can find the six-state protocol [40] which, rather than using two or four states as in the BB84, uses six states on three bases **X**, **Y** and **Z**, thus causing the eavesdropper to produce a higher rate of error. For the case of the SARG04 protocol [13], it shares the first step of photon transmission with BB84, but then, for the second step, Alice does not directly announce her bases, but a pair of non-orthogonal states instead, one of which is being used to encode her bit. Another protocol, the BBM92 [41] coincides with BB84 in the fact that if Alice possesses the source, then her measurement (which is led on a random basis) would prepare the state to be sent to Bob in one of the four possible states of those used in the BB84, and there is no way of knowing whether Alice first measured part of a Bell state or she prepared a qubit state using a random number generator. In [42], a simplified three-state BB84 protocol was presented. In this case, Alice sends three possible states to Bob, but he performs a simplified measurement with a basis-independent detection efficiency condition, thus limiting an eavesdropper to control the efficiency of detection, depending on Bob's basis choice. Another approach, based on the BB84, is the protocol presented in [43], where both, sender and receiver, select a random basis for modulation, encode on basis of random bits. Thus, both send the qubits over a quantum channel to each other. Then, both decode on basis of their random bits. Finally, both exchange their random basis and correct the positions of common bits. This process allows both, sender and receiver, to get two keys and a final key can be generated by combining them. Another protocol is presented in [44], which is identical to the BB84 protocol for the entire quantum mechanism, but the difference is that such protocol uses private reconciliation from a random seed and asymmetric cryptography for the classic procedures. In another trend, Quantum Key Agreement (QKA) protocols (those whereby two or more parties agree upon a key over insecure communication channels based on their exchanged messages) which are based on the BB84 protocol [45], but the outcome of the protocol is going to be influenced by both parties. Therefore, no one can determine the shared key alone and the protocol has 50% qubit efficiency after the random sampling discussion and it provides unconditional security.

In our current proposal, several parties meet to generate the quantum key but via teleportation, entanglement, and collaboration, thus reducing the rate of success for an individual eavesdropper. At this point in our development, we have shown the prescriptions to solve the control problem of post-selecting the states in the Alice/Bob_0 and Bob_1 subsystems. In such sense, Alice/Bob_0 pretends, after Bob_1 applies the transformation characterized by an agreed ω_1, to control the system configuration in possession of Bob_1 (the control and the Bob_1 subsystem inclusively) to secretly reach one of the states $|b_j\rangle$ in the control and to set one of the orthogonal states $|0\rangle_{\theta,p}$, $|1\rangle_{\theta,p}$ (note that this knowledge keeps unknown for him). In the following subsection, we will exploit this procedure to state the QKD scheme.

5.1. QKD Protocol Description Based on a Shared Generation

In this section, we will describe how to afford a QKD scheme with the previous procedure based on double teleportation. The process is partially based on the BB84 protocol [11], but there, any sensitive information is transmitted through a quantum channel directly. Instead, it is generated by post-measurement. BB84 protocol is based on the transmission of a series of unknown states by the receiver, to then compare the outcomes between two bases independently selected. Still, they should be communicated directly through a quantum channel, nevertheless, it is relatively secure. Other protocols, as the E91 [14], exploit the entangled properties of certain states to transmit no-communicated correlations to set the key. Similarly, as the BB84, the B92 protocol [12] uses the comparison between two non-orthogonal bases to shade part of the information to a possible eavesdropper, while previously agreed correlations allow us to set the key. Nevertheless, BB92 protocol still lets an eavesdropper gain more information [46] as compared with other protocols.

Thus, in this subsection, we use the previous procedure to set an improved BB84-like QKD protocol. First, Alice supported by Bob_0 (which could be assumed to be part of the same system) sets the double teleportation algorithm to virtually transmit a state just known by her. It is previously configured to be generated as one element of two different bases selected at a time by Alice, B_A. It is reached by selecting $\theta = 0, \frac{\pi}{2}$ and $\phi = 0$ (it implies $p = 0$), setting after the basis $H = \{|0\rangle, |1\rangle\}$ or $D = \{|-\rangle, |+\rangle\}$. K, p_0 should be selected at this point to define the control state (if the strategy is to increase the probability of success P_j in the stochastic step to choose the correct control state $|b_j\rangle$, otherwise it could be delayed after the processing of Bob_1).

Thus, through a public key statement dictating which ω_1 is applied by Bob_1 in a concrete time (see Figure 6a exhibiting a step pseudo-random function to generate ω_1 for instance), Alice can improve the election of the basis and the outcome for the QKD protocol. At the same time, she has settled, in advance, the future state in possession of Bob_1 upon the selection of the parameter ω_0 depending on K (then also β_0, related with the further measurement on the control, by using the maximal prescription $p_{0_{max}}$). In fact, in the process, K could be selected randomly but always secretly by a classical procedure.

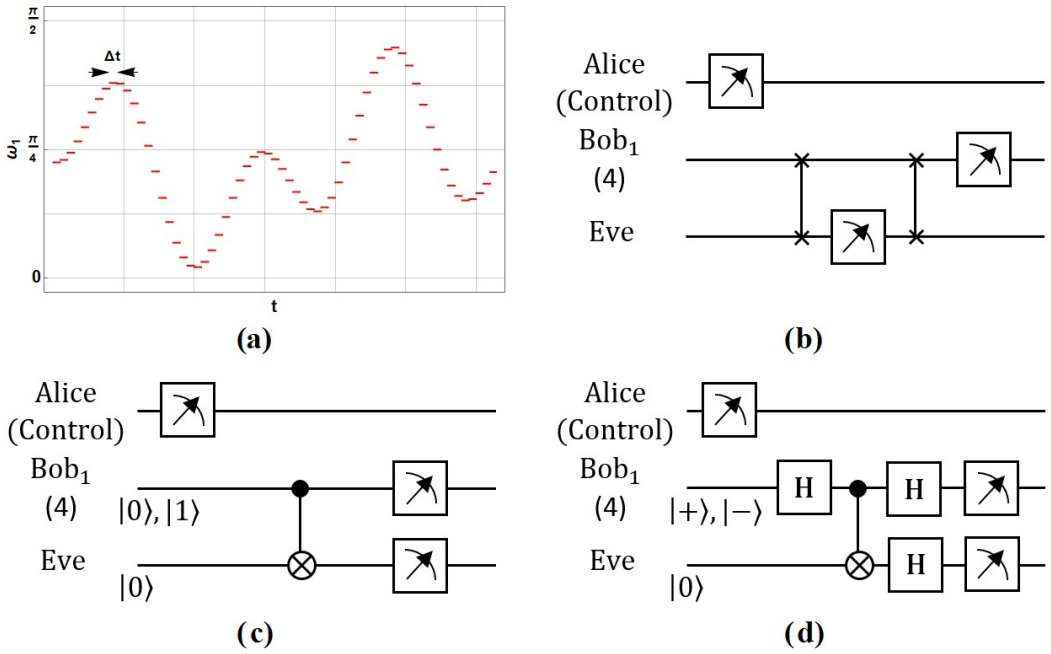

Figure 6. (**a**) Timely generation of ω_1 agreed between Alice and Bob_1 through a classical public channel, (**b**) *SWAP* gates used by Eve to stole and reinsert the state of Bob_1, (**c**,**d**) alternating *CNOT* gates to infer the Bob_1 state by Eve.

Then, through the controlled processing $\mathcal{U}_{0_2}$ and $\mathcal{U}_{1_4}$ by Bob_0 and Bob_1 respectively, we get the state (18), which is ready to begin the QKD protocol, still without transmitting any sensible information. Finally, all is decided by the control measurement performed by Alice. It is reached by settling an apparatus of measurement in agreement with the β_0 value (which indeed was already decided upon the selection of ω_1 and K), and the selection of j, m in agreement with $j + m = 1$ to get the maximum P_j (if that is the strategy being followed). Note that $0.5P_j$ represents the efficiency in the generation of a useful key, compared with 0.5 for the traditional BB84 protocol. Despite possibly lower, additional advantages against eavesdropping are present as it will be discussed below. Thus, when the control measurement stochastically fits with the selection of j, Alice has successfully transferred a qubit in one specific state from the respective set expanding the Hilbert space on the basis selected by Alice. Then, Bob_1 should measure his state by selecting one of the two agreed basis, $B_B \in \{H, D\}$. Thus, if Bob_1 selects the same basis H or D to measure his state (characterized by α instead θ in (16) or (17)), the outcome is already known previously by Alice, thus sharing secretly a common element of the key. It only happens if the control measurement fits with j and if both bases coincide ($\theta = \alpha$), precisely as the BB84 protocol works.

At this point, still they can infer the key until Alice publishes her basis (θ or B_A) also as Bob_1 (α or B_B). Still, Alice also should skip the failed control measurements (they are expected to be a minimum as she is closer to $P_j = 1$) but still communicate it to Bob_1 as a failed outcome. Table 2 shows an illustrative sequence of such procedure until the information sharing, thus getting the useful key using QKD based on double teleportation. It skips the technical details dealt with in the previous subsection.

Table 2. Example of a series of shared information bits to set the quantum secret key.

Setup		**Selection**			**Measurement**				**Sharing**		**Decision**	
Alice			Alice		Alice		Bob$_1$		Alice	Bob$_1$	Alice/Bob$_1$	
θ	B_A	j	m	$\lvert k \oplus 1\rangle_{\theta,p}$	$\lvert b_j\rangle$	α	B_B	$\lvert k \oplus 1\rangle_{\alpha,p}$	B_A	B_B	A/R	key
0	H	0	1	$\lvert 0\rangle_{0,0}$	$\lvert b_0\rangle$	0	H	$\lvert 0\rangle_{0,0}$	H	H	✓	0
$\frac{\pi}{2}$	D	1	0	$\lvert 0\rangle_{\frac{\pi}{2},0}$	$\lvert b_0\rangle$	$\frac{\pi}{2}$	D	$\lvert 0\rangle_{\frac{\pi}{2},0}$	$\times$	D	✗	-
0	H	1	0	$\lvert 0\rangle_{0,0}$	$\lvert b_1\rangle$	$\frac{\pi}{2}$	D	$\lvert 0\rangle_{\frac{\pi}{2},0}$	H	D	✗	-
$\frac{\pi}{2}$	D	1	0	$\lvert 1\rangle_{\frac{\pi}{2},0}$	$\lvert b_1\rangle$	$\frac{\pi}{2}$	D	$\lvert 1\rangle_{\frac{\pi}{2},0}$	D	D	✓	1
$\frac{\pi}{2}$	D	1	0	$\lvert 1\rangle_{\frac{\pi}{2},0}$	$\lvert b_0\rangle$	0	H	$\lvert 0\rangle_{0,0}$	$\times$	H	✗	-
0	H	0	1	$\lvert 1\rangle_{0,0}$	$\lvert b_0\rangle$	0	H	$\lvert 1\rangle_{0,0}$	H	H	✓	1
$\frac{\pi}{2}$	D	0	1	$\lvert 0\rangle_{\frac{\pi}{2},0}$	$\lvert b_0\rangle$	$\frac{\pi}{2}$	D	$\lvert 0\rangle_{0,0}$	D	D	✓	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

The first two columns state the θ value selected by Alice, thus implying the basis B_A selected, H or D, used to state the final transferred state. Third to fifth columns state the elections of Alice: j, m, and the $|k \otimes 1\rangle_{\theta,p}$ selected to be delivered to Bob_1. The following four columns state the related information regarding the measurement outcomes: $|b_j\rangle$ performed by Alice on the control; α or B_B the measurement basis selection of Bob_1, as well as the corresponding outcome $|k \oplus 1\rangle_{\alpha,p}$. The tenth and eleventh columns exhibit information sharing through a public channel. Note that Alice should report the failed events marked there with $\times$. Two last columns show the understood decisions of usefulness, acceptation, or rejection (A/R), of each event with ✓ (success) or ✗ (fail), as well as the useful bit keys: 0110.... Note that the key just arises with their non-communicated outcomes when the registers of bases coincide and the Alice measurement on the control succeeds her predictions.

As in the BB84 protocol, the key still should pass an error correction reconciliation by sharing and comparing part of the key to detect transmission errors, otherwise the presence of an eavesdropper through the quantification of the QBER. Another relevant

characteristic of this procedure is that Alice can switch the BB84 four-state protocol into a six-state protocol [40,47] adapting the post-processing (12) and selecting θ, ϕ conveniently.

5.2. Action and Impact of a Possible Eavesdropper under an Individual Attack

QKD schemes are subject to security attacks. In the analysis of quantum security, several types of attacks are normally considered. There, in the most simple level, individual attacks include quantum interactions with a single quantum channel carrying the information to be read as a single register under measurement (in this case the qubit of Bob_1). Other types of attacks consider collective attacks [48,49], where measurements are not individual, instead, they are allowed to be performed coherently together. Otherwise, coherent attacks [48,50] allow us to apply unitary transformations to the whole set of measurements in addition. While collective and coherent attacks are out of the scope of this work, in this subsection, we analyse a type of individual attack showing a certain advantage on the traditional BB84 protocol.

For the sifting of the Bob_1 state, Eve achieves it using an alternative pair of $SWAP$ gates exchanging the states between Bob_1 and Eve to thus steal and return it. In such a case, an intermediate measurement of the stolen state by Eve is then returned to Bob_1 before his measurement (see Figure 6b). The initial state in possession of Eve could be non-meaningful.

Otherwise, an alternative C^aNOT_b gate arrangement could be performed upon the election of the measurement basis (see Figure 6c,d). In this case, Eve first bets by the basis on which Alice has prepared the state. If she supposes the basis is H, then she should arrange the procedure presented in Figure 6c, just stating a C^aNOT_b gate between her qubit in the state $|0\rangle_E$ and controlled by the Bob_1 state; instead, if she bets for the basis D, she should implement the circuit in Figure 6d using complementary H gates to translate the Bob_1 states to the previous situation, but still returning him his original one. It is immediate to demonstrate that any of those circuits effectively copy the Bob_1 state if Eve hits the correct basis in which Alice has prepared the final state for Bob_1:

$$\begin{aligned} |i\rangle_{\text{Bob}_1} \in \{|0\rangle, |1\rangle\} \quad &\longrightarrow \quad C^{\text{Bob}_1}NOT_{\text{Eve}} \cdot |i\rangle_{\text{Bob}_1} \otimes |0\rangle_{\text{Eve}} = |i\rangle_{\text{Bob}_1} \otimes |i\rangle_{\text{Eve}} \\ |i\rangle_{\text{Bob}_1} \in \{|+\rangle, |-\rangle\} \quad &\longrightarrow \quad H_{\text{Eve}}H_{\text{Bob}_1}C^{\text{Bob}_1}NOT_{\text{Eve}}H_{\text{Bob}_1} \cdot |i\rangle_{\text{Bob}_1} \otimes |0\rangle_{\text{Eve}} = |i\rangle_{\text{Bob}_1} \otimes |i\rangle_{\text{Eve}} \end{aligned} \tag{29}$$

Otherwise, if Eve fails in the basis selection, then her outcomes are non-meaningful so they do not change the overall probabilistic distribution in the BB84 protocol with Eve using the $SWAP$ gate as before, thus giving the same outcomes previously discussed.

As it is well-known for the BB84 protocol, for the individual attacks on the qubits coming from Alice, Eve will have success in the 50% ($\frac{1}{4} / \frac{1}{2} = \frac{1}{2}$ in Table 3) of the useful key where she passes unnoticed. Table 3 classifies the possible cases. There, probability P is absolute concerning the entire cases, so it should be divided by $1/2$ to get the conditional probability for the useful cases. Class 1 in the first row corresponds to the previous situation where the three bases selected meet. In this case, Eve becomes unnoticed and in possession of a valuable key bit. Class 4 corresponds to the cases conducting to the non-useful key because Alice and Bob_1 do not meet in their basis if Eve does or not. Thus, only Classes 1 to 3 correspond with a possible useful key.

Table 3. Classification of basis selection and outcomes considering the presence of an eavesdropper for the traditional BB84 protocol.

Basis Selection and Outcomes Classes	**Alice**		**Eve**		**Bob$_1$**		P
	Basis	**Out**	**Basis**	**Out**	**Basis**	**Out**	
1: Basis selections completely meets	B_A	o_α	B_A	o_α	B_A	o_α	$\frac{1}{4}$
2: Eve basis fails but Bob_1 output not	B_A	o_α	$B_{E\neq A}$	o_ϵ	B_A	o_α	$\frac{1}{8}$
3: Bob_1 basis meets but output fails	B_A	o_α	$B_{E\neq A}$	o_ϵ	B_A	$o_{\beta\neq\alpha}$	$\frac{1}{8}$
4: Bob_1 basis and output fail	B_A	o_α	B_E	o_ϵ	$B_{B\neq A}$	o_β	$\frac{1}{2}$

If Alice and Bob_1 spend some part of the key, they could detect the Eve presence [11] by comparing their outcomes in a reconciliation procedure. Considering just the useful key (or part of it), 25% ($\frac{1}{8}/\frac{1}{2} = \frac{1}{4}$ in Table 3) of it corresponds to the QBER in the protocol (Class 3). QBER is due to the presence of an eavesdropper, or otherwise to the presence of noisy communication in the quantum channel. Finally, Class 2 corresponds to the cases where the presence of Eve is undetectable for Alice and Bob_1. Despite this, Eve has no certainty if their key is correct because her basis does not meet with that of them (assuming she has access to that information published in a public channel). In the following, we will assume that such a class is not successful for Eve.

For the scheme presented here, the situation runs identical if such attack is performed just before Bob_1 measures his state, but after to be assembled by Alice/Bob_0. In any case, this intervention assumes the possibility to steal the system and then be reintegrated ready for the Bob_1 measurement (otherwise gaining complete access to it, still being classically unnoticed, but no quantumly). In any case, it requires non-trivial interventions on the Bob_1 state as it was shown in the circuits in Figure 6b,c. Despite their technical complexity, note those procedures should be performed during the state transmission in the BB84 protocol, but in the current procedure, they should be performed after Alice measures their control state. Despite, if Eve pretends to perform the sifting of the Bob_1 state under the current protocol, then the probability of Class 1 (P_E in the following) and the only successful for Eve, changes dramatically. Then, we perform our analysis around this quantity and upon such assumptions.

Figure 7a exhibits the eavesdropper temporal action through the events in the protocol. Instead of remaining the quantum channel opened all time as in the BB84 original eavesdropping, in our case, Eve needs to sift the Bob_1 state during the entire process consisting of the stages shown in black. There, the action performed by Alice to define K (orange) determines the beginning of the assembling of the transmitted state to Bob_1. Such selection could be made since the beginning when she prepares the control state (particularly if she wants to maximize $C_0(p_0, K)$ by selecting ($p_0 = p_{0_{max}}$), or otherwise just before Bob_0 should perform his processing $\mathcal{U}_{0_2}$ if milder P_j values are allowed. Thus, Eve can perform several types of individual attacks during such a period. Type A, after Alice's control measurement, has been already discussed as equivalent to the traditional individual attack in the BB84 protocol. Despite this, such a possibility is not meaningful here because the information is not properly travelling through a quantum channel. Anyway, Bob_1 should avoid this possibility by using this resource rapidly after the assembling. In addition, if Eve has not to control the time assembling of the transmitted state, she can perform her attack just before Alice's control measurement (type C) or still before the $\mathcal{U}_{0_2}$ codification by Bob_0 (type B). Both attacks conduct to the same Eve's success probability outcome as it is seen in the Appendix C. Note this procedure is not equivalent to the BB84 one, so the success probability changes, despite it still requires the exchange methods depicted in Figure 6.

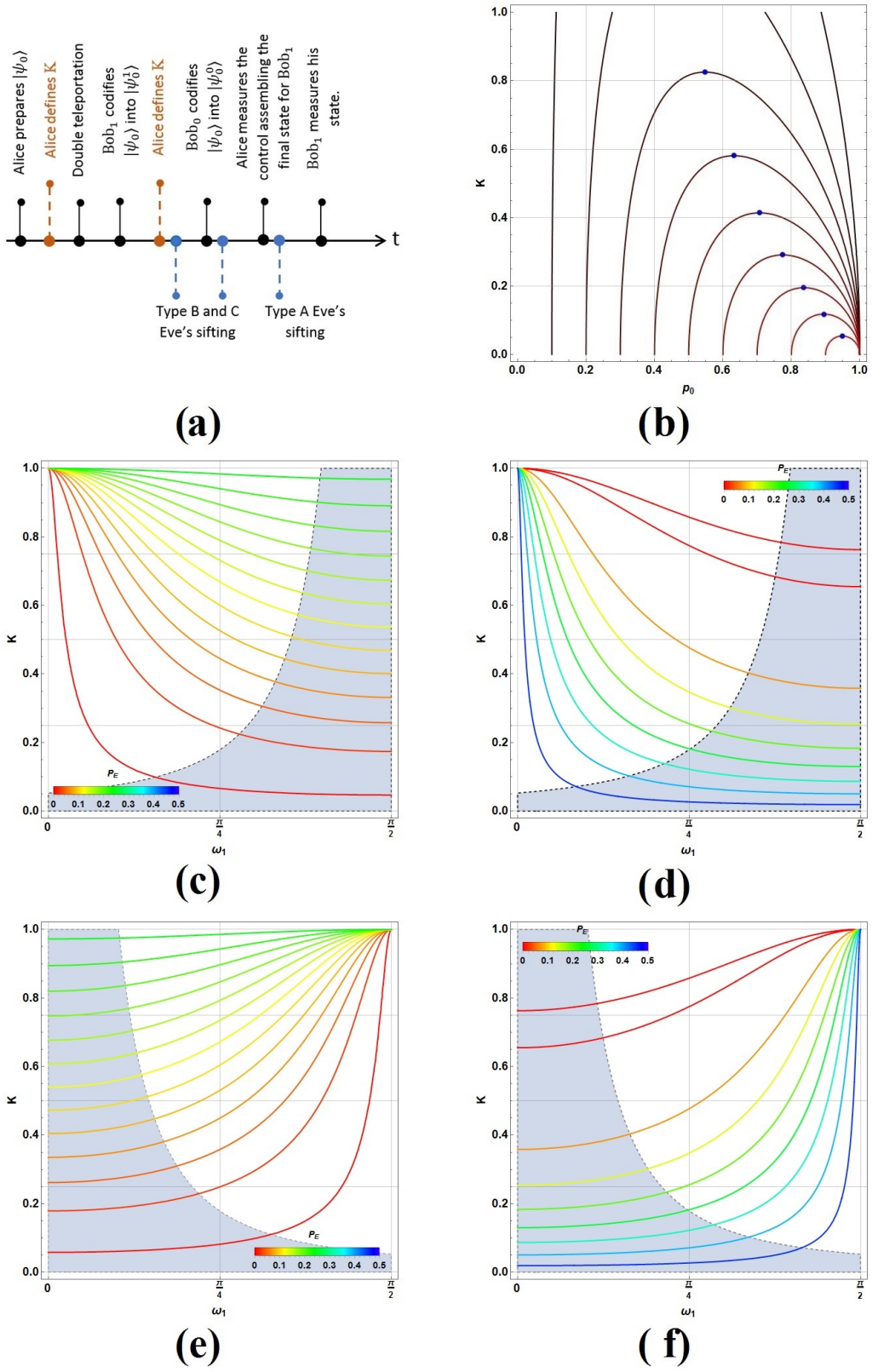

Figure 7. (**a**) Eavesdropping temporal action through the protocol; (**b**) contour lines of $C_0(p_0, K)$ as function of p_0 and K with their maximal values as blue dots; and contour lines for the conditional probability for the Eve success, P_E, as function of ω_1 and K in color for (**c**) $k = 0, \theta = 0$; (**d**) $k = 0, \theta = \frac{\pi}{2}$; (**e**) $k = 1, \theta = 0$; and (**f**) $k = 1, \theta = \frac{\pi}{2}$. $P_j \geq 0.9$ corresponds to the gray region.

In addition, the difference does not depend on the open selection of $C_0(p_0, K)$ (becoming better choosing $C_{0_{max}}$ to maximize P_j) as will be seen. For both cases (Type B and C), P_E is given by (see Appendix C):

$$P_E = \frac{P}{P_j} = \frac{C_0(p_0, K)}{P_j}(f_{k\oplus 1}(\frac{\theta}{2})\sqrt{1 - K^2 f_k^2(\omega_1)} - K f_{k\oplus 1}(\omega_1))^2 \quad (30)$$

then, an attempt to maximize P_j (the rate for the successful key) directly should raise the value of P, but not P_E. Figure 7b shows such dependence through contour lines. As function of p_0, K could be selected almost openly, despite only one value maximizes the value of $C_0(p_0, K)$ with p_0 fixed (blue dots in Figure 7b). The color of each point on the curves reflects the $C_0(p_0, K)$ value (darkest for the lowest values and brightest for the highest ones). Blue dots mark the value where the maximum of $C_0(p_0, K)$ is reached for a given p_0 or K. Nevertheless, many other values of K could still keep P_j in a higher value to maintain the performance of the key generation, but still to conveniently reduce P_E. In Figure 7c–f, the involved regions marked in gray with $P_j \geq 0.9$ (just for the $j + m = 1$ cases), remark certain criteria for the random election of K. In any case, the meaningful quantity to evaluate the performance of Eve is the conditional probability P_E which is independent of $C_0(p_0, K)$. It just accounts for the useful key cases when Alice reaches correctly her selection $|b_j\rangle$, as similarly the conditional probabilities for the Table 3 were calculated concerning the useful key outcomes. It is plotted as a function of ω_1 and K, and coloured in agreement with the color bar inside. Cases correspond to (c) $k = 0, \theta = 0$; (d) $k = 0, \theta = \frac{\pi}{2}$; (e) $k = 1, \theta = 0$; and (f) $k = 1, \theta = \frac{\pi}{2}$ (remembering that the selected state for Bob_1 is $k \oplus 1$). In any case, clearly, the strategy lets a notable lowering for the probabilities for the success of Eve to great extent. The reason is now evident, P has a wide distribution in the region where P_j is high, then it still lets the selection of low values for P. The last behavior is due to the election of basis by Eve before Alice did, thus modifying the global state and lowering the success notably in most cases. In fact, performing a numerical analysis based on a Monte Carlo simulation about the average value of P_E inside the gray region for the random selection of ω_1 and K defined by the threshold of $P_j \geq 0.9$, we get: $\overline{P}_{E_H} = 0.076$ for $\theta = 0$ and $\overline{P}_{E_D} = 0.173$ for $\theta = \frac{\pi}{2}$. It clearly shows a notable advantage against individual attacks of Types B and C. Such outcomes could increase only if Eve has strict control over the knowledge about the period when Alice already has performed her control measurement and only if Bob_1 maintains such resource without use.

5.3. Considerations for Complexity and Number of Resources in the Procedure

Secure communications remain safe against attacks, particularly by those performed by quantum computers. They require effective and strong protocols of QKD. In any case, even when the use of a minimum of resources has been mainly pursued in the original contributions to those protocols, extreme security only requires a sizable, but a finite number of resources and signals.

The BB84 protocol is the earliest QKD protocol [11]. It has inspired a variety of other similar slender protocols as the B92 protocol [12] but reducing the communication efficiency and the practicability. Still, the six-state protocol is a more secure extension of the BB84 protocol, despite raising the upper limit of the QBER. Otherwise, limited to the current single-photon source technology, it is not possible to obtain ideal single photons, instead of using multi-photon sources [13] as in the decoy-state [51], the most widely implemented QKD scheme. Such protocols anyway introduce higher complexity compared to the more theoretical QKD protocols being proposed. As well, single-photon QKD systems commonly include polarization and phase encoding, thus introducing a higher number of resources to the theoretical ideal approaches.

Thus, the BB84 protocol uses the fewest resources to produce each bit of the key, a single ideal qubit properly prepared on a certain basis and two signals, one travelling through a single quantum channel and a classical one to share the basis used by both main parties, after the receiver measures the incoming qubit. Compared with the procedure

being presented, the current protocol uses five qubits partially entangled by pairs. This number, as it was seen, increases to nine qubits for feasible implementations: two for performing the $C^C\mathcal{U}_{1_4}$ and two more for performing the $C_{SWAP_{24}}$ among the faraway qubits 2, 4. In addition, two more classical signals should be added in each case (see Appendices A and B). A more elaborated infrastructure is expected in terms of quantum gates and entanglement control. Despite this, the asymmetric processing combined with the shared assembling via teleportation allow for a strategy to lower the eavesdropping rate of success to a great extent. In any case, the number of resources grows linearly concerning the key block length.

More complex proposals have been considered in real scenarios to avoid environmental factors lowering the efficiency of quantum cryptography [52]. Other complex deployments currently consider more specialized quantum and optical resources in QKD protocols [53]. Thus, entangled resources and shared multipartite schemes as in the current proposal should be considered to set more secure procedures, particularly in the small block length regime [54]. Complexity is not equivalent to impossibility, until now, first approaches to QKD have arisen in parallel with our technological scope. Nevertheless, while more control is reached on quantum systems, more new audacious proposals are being tried combining full quantum resources to reach more outstanding outcomes.

Considering the outcomes for the success of Eve, $\overline{P}_{E_H} = 0.073$ for $\theta = 0$ (basis H) and $\overline{P}_{E_D} = 0.164$ for $\theta = \frac{\pi}{2}$ (basis D), we note she has a higher probability to guess outcomes in the last basis. The last outcomes are not the complete picture because still Alice should decide which θ will use (basis) and also the pair j, k to impose the adequate prescriptions. Thus, the global average success probability for Eve in a key of length $N = n_H + n_D$ (when Alice decides to use n_H times the basis H and n_D times the basis D) is:

$$\overline{P}_{E_{Total}} = (\frac{n_H}{N}\overline{P}_{E_H} + \frac{n_D}{N}\overline{P}_{E_D})^N = (\overline{P}_{E_H} + f_D(\overline{P}_{E_D} - \overline{P}_{E_H}))^N \tag{31}$$

where $f_D \equiv \frac{n_D}{N}$. Such formula goes into the continuous dominion for large N, but for small N is discrete. Figure 8 shows in color $\overline{P}_{E_{Total}}$ in agreement with the color bar inside on the left.

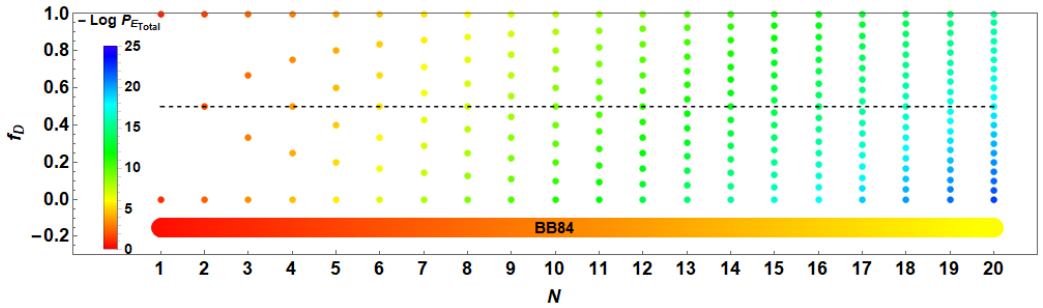

Figure 8. $\overline{P}_{E_{Total}}$ values for keys of small block length as function of f_D (Alice's proportion for choosing D) and their length N. Values are coloured as c in $\overline{P}_{E_{Total}} = 10^{-c}$. Red dashed line corresponds to the typical case $f_D = 0.5$ when Alice selects randomly the basis.

Note such bar refers to the exponent c for $\overline{P}_{E_{Total}} = 10^{-c}$. Then, blue corresponds to lowest $\overline{P}_{E_{Total}}$ values and red for the highest ones. A horizontal dashed black line shows the typical case where both cases are equally selected. As it could be expected, the case $f \to 0$ gives the lower advantage for Eve. Despite this, such an election is not the best because Eve could change her strategy by learning from the public sharing of basis. Thus, if as an extreme fact Eve knows Alice always selects the basis H, then the new conditional probability will become one because we add the sure knowledge of the basis by Eve, thus getting a sure outcome. If $f_D = 0.5$, it does not add new knowledge, thus the values of $\overline{P}_{E_{Total}}$ become as those on the dashed red line in Figure 8. In any case, the probability $\overline{P}_{E_{Total}}$ never exceeds 0.013 for $N \geq 2$. As a reference, we are included the coloured bar at the

bottom (using the same color pattern) which refers to the success probability for Eve using the BB84 protocol: 0.5^N. It shows an outstanding advantage for the current procedure.

6. Some Final Considerations about Benchmarking, Decoherence Effects, and Fidelity

Through the history of QKD developments since the BB84 protocol, many other approaches and different aspects in the key distribution have been tried. Of course, one of the main aspects is the security against eavesdropping, but others aspects sometimes go in different directions, for instance, the economy in the quantum resources or the robustness against quantum computer attacks. In the last case, the reduction of quantum resources in terms of not only efficiency but a feasible operation is important. Clearly, in the procedure being developed here, the economy has not been the focus, instead of the security, particularly based on the distributed tasks to set the key.

6.1. QBER and a Brief Comparison with Other Similar QKD Protocols

Thus, comparison between protocols is usually complicated because there are lots of elements to be performed. Moreover, some developments put more attention on certain variables to highlight the goodness of their approaches. In this subsection, we account for a review of similar BB84-like protocols in terms of some relative indicators for security. Despite the current development, the P_E is the outstanding feature because it measures the effective use of the sifting for Eve (when she gets the correct outcome without detection), the most common comparative reference is the QBER. Thus, we show in the Appendix D, that the conditional QBER (relative to the useful outcomes when the basis of Alice and Bob_1) becomes:

$$P_{QBER_{rel}} = \frac{C_0(p_0,K)}{P_j} K^2 \sum_{k'=0}^{1} \left[f_k(\omega_1) f_{k'}(\frac{\theta'}{2}) - (-1)^{k'(k+k')} f_k(\omega_1 + \frac{\Delta\theta}{2}) f_{k\oplus k'}(\frac{\Delta\theta}{2}) \right]^2 \quad (32)$$

Again, note the coefficient $C_0(p_0,K)$ is non-meaningful due P_j, but instead, $P_{QBER_{rel}}$ is proportional to K^2. In addition, note that $\theta' \neq \theta$, then $\theta' = \frac{\pi}{2} - \theta, \Delta\theta = \frac{\pi}{2} - 2\theta$. Figure 9 shows the contour plots for $P_{QBER_{rel}}$ as function of ω and K corresponding to (a) $k = 0, \theta = 0$; (b) $k = 0, \theta = \frac{\pi}{2}$; (c) $k = 1, \theta = 0$; and (d) $k = 1, \theta = \frac{\pi}{2}$ remarking the region with $P_j > 0.9$. Each contour value of $P_{QBER_{rel}}$ was coloured in agreement with the color bar besides.

Inside the region shown with $P_j \geq 0.9$ and $0 \leq K \leq 1$, the QBER drops in average around (a) 0.03, (b) 0.04, (c) 0.03, and (d) 0.02 relative to each figure. Despite, alternative elections with larger K and P_j values (as instance $0.8 \leq K \leq 20$ and $P_j > 0.95$) raises those values to (a) 0.09, (b) 0.12, (c) 0.11, and (d) 0.07 respectively, near of the threshold for the QBER in the BB84 protocol [55], and under the security bound of 0.25 [56]. This fact is interesting because the method is configurable by selecting the region where P_E and $P_{QBER_{rel}}$ are both satisfactory. Thus, if QBER is the main goal (the detection of eavesdropper more than its failure), then, regions with larger K values could be more practical. Still, some considerations should be analysed due to decoherence effects that could increase the QBER [57], thus reaching the security bound. It will be discussed in the next subsection.

As it was stated in Section 5, the trend of BB84-like protocols has continued by proposing new approaches mainly based on this protocol. Thus, the BBM92 protocol [12] reports for individual attacks a theoretical QBER of $\frac{1}{4}$ and a success probability of eavesdropping of $\frac{1}{4}$ as the BB84 one. The SSP98 protocol [40] has reported theoretical QBER values of $\frac{2}{3}$ and success probability of $\frac{1}{3}$. Nevertheless, practical implementations report QBER's of 0.110 and 0.126% [58] for BB84 and SSP98 respectively. The SARG04 protocol [13] has reported QBER from 0.968% and 0.271% for single-photon and double photon pulses respectively. In newer protocols based on BB84 as MKP16 protocol [43] the QBER range from 0.56 until 0.25 depending on the initial number of qubits generated. Thus, the development of QKD protocols is not uniformly developed going first on the proposal, the QBER or success probability analysis, the attack type to be considered in the analysis. Each one could have different complexity, requiring further developments for its analysis through those several

approaches highlighting their goodness. For the current procedure, the QBER is on the range of the BB84 protocols, despite, it exhibits outstanding properties in terms of the reduced Eve success probability, his possible configuration, and the existence of quantum correlations during the quantum key generation.

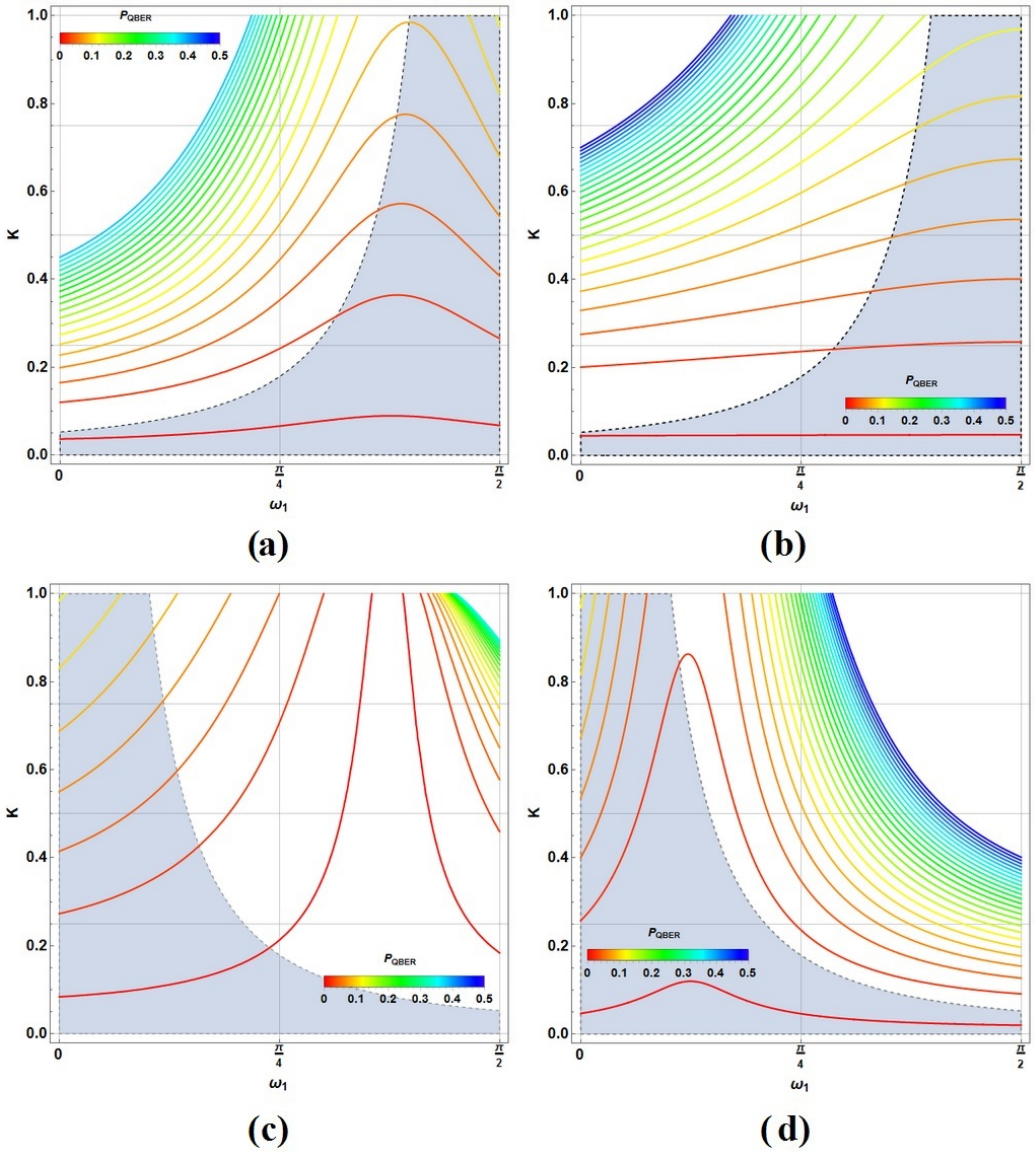

Figure 9. Contour lines for the conditional QBER, $P_{QBER_{rel}}$, as function of ω_1 and K in color for (**a**) $k = 0, \theta = 0$; (**b**) $k = 0, \theta = \frac{\pi}{2}$; (**c**) $k = 1, \theta = 0$; and (**d**) $k = 1, \theta = \frac{\pi}{2}$. $P_j \geq 0.9$ corresponds to the gray region.

6.2. Fidelity and Possible Decoherence Effects Due to the Environment

Technical implementations for security protocols involving quantum processing, as the current one, will depend strongly on the physical system where it pretends to be implemented. Quantum decoherence due to the interaction with the environment differently affects setups settled on photonic systems than matter systems. While photonic implementations are recommended whenever quantum information should not be stored. Despite quantum processing is commonly settled on gates models, all of them finally involve or reduce to physical interactions ruled by a Hamiltonian. For matter, the preferred approach to analyse such decoherence are the quantum open systems equations as Linblad or Redfield ones [59]. A simpler but none-less useful approach is the modelling of decoherence

through non-Hermitian Hamiltonians [60]. Still, both approaches can become complex if a large number of gates are involved.

Thus, quantum decoherence is the main challenge to reach scalability and reliability. In addition, it is known that decoherence effects (dephasing, amplitude, and depolarizing) increase harmfully the QBER to undesired effects near from the security bound [57]. A precise quantification about the fidelity of such systems is complex because it depends on the type and size of the gate and its architecture; also, on the number and kind of the quantum states involved, particularly those involving entanglement. For these reasons, together with the development of quantum information and its processing, this problem has been tackled through practical considerations for different implementations on matter and for the most typical gates [61]. While for photonic implementations decoherence becomes mild, it is not true for matter systems. Thus, gates as NOT, Hadamard, C^aNOT_b, Toffoli, and so forth, all of them involved in the current procedure, have been recently analysed for Nuclear Magnetic Resonance (NMR) using the Lindblad equation to give certain guidelines to quantum circuit designers about the decoherence for the most typical gates, thus reporting their fidelity behavior [62]. Such analysis shows as expected, that the decoherence process and the further loss of fidelity depend on the input state and the type of decoherence. By analyzing amplitude and phase damping as the most representative examples of noise, several aspects arise in the analysis: (a) deeper circuits (circuits with more gates) of course exhibit lower fidelity, (b) multiqubit gates do not necessarily show lower fidelity than single qubit ones, and (c) shorter time-scales to reach each gate still maintain fidelities near to one. For Noisy Intermediate Scale Quantum (NISQ) technologies, global coherence times are in the range of 50–100 μs. Dealing with fidelities routinely implemented above 0.99 for single qubits gates, but also many two qubits gates. While, individual operation times are in the order of nanoseconds, so large circuits can be addressed during the entire coherence times [63]. Thus, circuits containing tens of gates are currently able to be implemented. Table 4 accounts for the gates and their barely type arranged by process (DT for double teleportation and PP for post-processing) and the number of qubits involved. More than half are single qubits gates, showing that the implementation on matter-based technologies is in order.

Table 4. Depth and number of each type of gate involved through the different steps of the whole QKD protocol (DT and PP).

Process & Qubits	**1**			**2**			**3**	**Total**
	X	**Z**	**Hadamard**	C^aNOT_b	$SWAP_{ab}$	$C^a\mathcal{U}_{i_j}$	**Toffoli**	
DT	4	2	1	0	0	0	2	9
PP	4	1	1	1	1	10	1	19

6.3. Quantum Processing in QKD Developments and Post-Quantum Cryptography

The protocol proposed has implemented quantum processing to a great extent compared with the most traditional procedures. Because quantum cryptography promises unconditional security in data communication because it is currently pretended to be deployed for military and commercial applications, it should be secure. Despite QKD is being widely adopted, it still faces several important challenges regarding the rates for secret key settlement, communication distance and decoherence, deployment sizes, the effective cost in terms of quantum resources, maintenance, and security [64]. As it was stated through the development, quantum coherence is preferable mandatory to reach all the basic features provided by Quantum mechanics.

Quantum computers are believed to solve (at least via problem translation) any exponential problem in principle solvable by a classical computer but not in a finite time. Then, due to classical cryptography protocols are commonly breakable in an exponential time, they are susceptible to failure under such scenarios. Then, with the advent of quantum computers, the necessity to develop secure QKD protocols under their possible attacks is mandatory. Post-quantum cryptography (sometimes also referred as quantum-safe cryp-

tography) deals with cryptographic algorithms thought to be secure against cryptanalytic attacks performed by an ideal quantum computer in terms of coherence, prompt quantum resources, and speed-up [32].

While in conventional symmetric cryptography algorithms, the security in communication is solely related to the secrecy of the encryption key, other QKD protocols currently studied, exploit an asymmetry in their implementation, thus stating the state-of-the-art in their practical implementations [64]. In the post-quantum cryptography terrain, despite currently experimental quantum computers still lacking processing power to break any contemporary cryptographic algorithm, people working in the frontier of theoretical cryptography are preparing impressive protocols to prepare for a time when quantum computers become a real threat. It requires implementing mathematics, physics, and technology to a great extent.

Cryptography systems are commonly grouped in several cryptographic classes [17]. Despite linear, our procedure could be adapted to be asymmetrically non-linear in (24); together, authentication introduced by ω_i parameters could be specialized to introduce a Courtois, Finiasz and Sendrier Signature scheme [65], thus being able to fall in the Multivariate-quadratic-equations and the Code-based schemes. It suggests a fusion between the classical cryptography schemes with trends based on Quantum mechanics features.

7. Conclusions

The BB84 protocol is the most representative protocol in quantum cryptography. The protocol uses a single quantum channel to transfer quantum encoding states. Despite an outstanding security performance, it still allows the possibility to steal the key by interfering with the mentioned quantum channel under individual attacks by an eavesdropper. Since its development, many other BB84-like protocols have been developed, many of them called by specific names despite their clear similitude to the BB84 one. There is not a unique line of development, instead, they commonly attend to some improvements in the protocol such as economy, security, and so forth.

In the present work, a protocol for the settlement of QKD using double teleportation and quantum processing together has been proposed. The procedure generates an entangled multipartite system among three parties plus a control system. The involved entanglement, together with local control, still allows us to manipulate the global quantum state on different parts to those exerting it. The process involved in the double teleportation plus post-processing has been shown to have non-locality activation, thus stating quantum correlations. Thus, an asymmetric post-processing scheme is proposed to generate and assemble a quantum state on a selected basis (defined by the state to teleport) on one of those parts. Then, it is shaped under the proper control, finally setting the QKD protocol.

7.1. Summarizing and Featuring the Protocol

The QKD procedure presented is intended to generate sensitive secret information to transmit it to a second party but is still assembled by post-measurement during the process, instead of like previous QKD protocols, such as the BB84, where any sensible information is transmitted by a quantum channel directly, being affordable for eavesdroppers at all times. Thus, the protocol presented also considers the action of a possible eavesdropper performing an individual attack under time uncertainty. In fact, with the correct prescriptions, Alice can guarantee with the desired success threshold on her post-measurement, a faithful reproduction of the BB84 protocol. Nevertheless, the control complexity is increased, together with implementations of double teleportation and quantum processing, the success for the eavesdropper becomes notably reduced if the attack is performed before the assembling. QBER remains in the typical range and it could be configurable on the election region of the parameters. Thus, while the eavesdropper has in the BB84 protocol a theoretical 50% chance of success on the useful key, in the present protocol, the probability of success drops down to as low as between 7% and 17%, thus improving the security.

Due to the processing complexity involved, aspects regarding the decoherence demand attention. There is not a unique procedure to quantify the loss of fidelity for a trend of gates, mainly because it depends on their architecture, specific physical realization and, inclusively, on the input states being considered. Despite this, for technologies other than light (which reaches large decoherence times), such as NISQ ones, currently there is a good fidelity performance of around 0.9 for the range of tens of gates. Then, despite the reports stating an increase of QBER due to decoherence, it still could be controlled by reducing the operation times of the gates as in the NISQ technologies.

7.2. Future and Additional Research

Additional research of course should be extended to probe the effectiveness extent against collective and coherent eavesdropping attacks for this protocol using asymptotic formulas or numerical analytic approaches [66]. We have limited our analysis to individual attacks, assuming Eve only has access to public communication and the end of quantum edge of Bob_1 before the assembling of the key. However, for collective attacks, where Eve brings each quantum signal and hears all public communication between Alice and Bob [18], more decisive probes are needed.

Together, extensions for the current approach in the six-states protocol direction [40,47] should be tried with more general and complex processing to that established in (12), instead with the full form for two-qubit rotations: $\mathcal{U}_k = e^{i\omega_k \vec{n}_k \cdot \vec{\sigma}}$, with $\vec{\sigma} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$, thus introducing additional parameters for the basis selection. In that trend, deeper elements regarding the classical authentication ω_k and the mathematical relation stated by the parameter K could be oriented to well-stated methods in classical cryptography.

An optimality analysis should be performed to reach adequate prescriptions fixing affordable values for the QBER and the eavesdropper rate of success in terms of the configurable selection of the parameters on the region settled by the Figures 7 and 9.

Author Contributions: Conceptualization, F.D.; methodology, F.D.; software, C.C.-I. and F.D.; validation, C.C.-I. and F.D.; formal analysis, F.D.; investigation, C.C.-I.; resources, C.C.-I. and F.D.; data curation, C.C.-I.; writing—original draft preparation, C.C.-I. and F.D.; writing—review and editing, C.C.-I. and F.D.; visualization, C.C.-I. and F.D.; supervision, F.D.; project administration, C.C.-I. and F.D.; funding acquisition, C.C.-I. and F.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Authors acknowledge the economic support to publish this article to the School of Engineering and Science from Tecnologico de Monterrey. Carlos Cardoso-Isidoro and Francisco Delgado acknowledge the support of CONACYT.

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

Appendix A. Control on Faraway Non-Local Resources

Controlled operations on faraway non-local parties as that in the second factor of (7), $C^C\mathcal{U}_{1_4} = |0\rangle_C\langle 0| \otimes \mathbf{1}_4 + |1\rangle_C\langle 1| \otimes \mathcal{U}_{1_4}$, are not possible to be performed directly (assuming that the control and qubit 4 cannot be moved from their locations). Nevertheless, they can be achieved via LOCC with the support of an entangled pair $|\beta_{00}\rangle_{ab}$ where qubit a is in possession of Alice and b is sent to Bob_1:

$$|\psi\rangle \quad = \quad (\sqrt{p_0}|0\rangle_C|\phi_0\rangle_2|\psi_0\rangle_4 + \sqrt{p_1}|1\rangle_C|\phi_1\rangle_2|\psi_1\rangle_4) \otimes |\beta_{00}\rangle_{ab} \tag{A1}$$

A direct calculation shows that a such state can be written in the basis of the Bell states for the qubits C and a as:

$$|\psi\rangle = \frac{1}{2}\sum_{x,y\in\{0,1\}} |\beta_{xy}\rangle_{Ca}(\sqrt{p_0}|0\oplus y\rangle_b|\phi_0\rangle_2|\psi_0\rangle_4 + (-1)^x\sqrt{p_1}|1\oplus y\rangle_b|\phi_1\rangle_2|\psi_1\rangle_4) \quad (A2)$$

$$= \frac{1}{2}\sum_{x,y\in\{0,1\}} |\beta_{xy}\rangle_{Ca}\mathbf{Z}_b^x\mathbf{X}_b^y(\sqrt{p_0}|0\rangle_b|\phi_0\rangle_2|\psi_0\rangle_4 + \sqrt{p_1}|1\rangle_b|\phi_1\rangle_2|\psi_1\rangle_4) \quad (A3)$$

then, Alice applies the operation $H_C \cdot C^C NOT_a$ on her qubits, getting:

$$|\psi^{(1)}\rangle = \frac{1}{2}\sum_{x,y\in\{0,1\}} |xy\rangle_{Ca}\mathbf{Z}_b^x\mathbf{X}_b^y(\sqrt{p_0}|0\rangle_b|\phi_0\rangle_2|\psi_0\rangle_4 + \sqrt{p_1}|1\rangle_b|\phi_1\rangle_2|\psi_1\rangle_4) \quad (A4)$$

The following development could be achieved using delayed measurements [35] or still just controlled operations. Despite, they commonly require interactions between faraway resources, which implies some of them will be moved from their locations using extra classical communication operations. Instead, we will use projective measurements and corrections. Thus, Alice measures their qubits C, a obtaining the outcomes $|x\rangle_C$ and $|y\rangle_a$ respectively. Using classical communication, Alice shares those outcomes with Bob_1 who applies the controlled operation $C^C\mathbf{X}_b^y \cdot C^a\mathbf{Z}_b^x$. The outcome is:

$$|\psi^{(2)}\rangle = |xy\rangle_{Ca}(\sqrt{p_0}|0\rangle_b|\phi_0\rangle_2|\psi_0\rangle_4 + \sqrt{p_1}|1\rangle_b|\phi_1\rangle_2|\psi_1\rangle_4) \quad (A5)$$

thus, Bob_1 applies the controlled operation $C^b\mathcal{U}_{1_4}$:

$$|\psi^{(3)}\rangle = |xy\rangle_{Ca}(\sqrt{p_0}|0\rangle_b|\phi_0\rangle_2|\psi_0\rangle_4 + \sqrt{p_1}|1\rangle_b|\phi_1\rangle_2\mathcal{U}_{1_4}|\psi_1\rangle_4) \quad (A6)$$

Finally, qubit b is sent to Alice to perform the $SWAP_{Cb}$ operation:

$$|\psi^{(4)}\rangle = |yx\rangle_{ab}(\sqrt{p_0}|0\rangle_C|\phi_0\rangle_2|\psi_0\rangle_4 + \sqrt{p_1}|1\rangle_C|\phi_1\rangle_2\mathcal{U}_{1_4}|\psi_1\rangle_4) \quad (A7)$$

which, disregarding the qubits a and b, is the same state obtained by $C^C\mathcal{U}_{1_4}$.

Appendix B. *SWAP* Operations between Faraway Non-Local Parties

As in the Appendix A, we will show how to perform the $C_{SWAP_{2,4}}$ operation between the faraway parties 2, 4 (assuming they cannot be moved close together). Again, we will use the entangled resource $|\beta_{00}\rangle_{ab}$ where qubit a is in possession of Bob_0 and b is sent to Bob_1:

$$|\psi\rangle = (\sqrt{p_0}|0\rangle_C|\psi_0^0\rangle_2|0\rangle_4 + \sqrt{p_1}|1\rangle_C|0\rangle_2|\psi_0^1\rangle_4) \otimes |\beta_{00}\rangle_{ab} \quad (A8)$$

As before, by rearranging the qubits 2 and a in the first term of (A8), and expressing it in terms of Bell stats basis:

$$|\psi\rangle = \frac{\sqrt{p_0}}{2}|0\rangle_C|0\rangle_4\sum_{x,y\in\{0,1\}} |\beta_{xy}\rangle_{2a}\mathbf{Z}_b^x\mathbf{X}_b^y|\psi_0^0\rangle_b + \sqrt{p_1}|1\rangle_C|0\rangle_2|\psi_0^1\rangle_4|\beta_{00}\rangle_{ab} \quad (A9)$$

then, Alice and Bob_0 apply the controlled operation $\tilde{C}^C(H_2C^2NOT_a)$ on their qubits (where, $\tilde{C}^aG_b \equiv \mathbf{X}_a(C^aG_b)\mathbf{X}_a$). Then, it becomes:

$$|\psi^{(1)}\rangle = \frac{\sqrt{p_0}}{2}|0\rangle_C|0\rangle_4\sum_{x,y\in\{0,1\}} |xy\rangle_{2a}\mathbf{Z}_b^x\mathbf{X}_b^y|\psi_0^0\rangle_b + \sqrt{p_1}|1\rangle_C|0\rangle_2|\psi_0^1\rangle_4|\beta_{00}\rangle_{ab} \quad (A10)$$

then, Bob_0 measures qubits 2 and a if the control register is $|0\rangle_C$, getting $|x\rangle_2$ and $|y\rangle_a$ using controlled quantum measurements [36,37]. Thus:

$$|\psi^{(2)}\rangle = \sqrt{p_0}|0\rangle_C|0\rangle_4|xy\rangle_{2a}\mathbf{Z}_b^x\mathbf{X}_b^y|\psi_0^0\rangle_b + \sqrt{p_1}|1\rangle_C|0\rangle_2|\psi_0^1\rangle_4|\beta_{00}\rangle_{ab} \quad (A11)$$

Using controlled classical communication, the measurement outcomes are shared with Bob_1 just if the control register is $|0\rangle_C$ to perform the operation $\mathbf{X}_b^y \mathbf{Z}_b^x$ and then $SWAP_{4b}$, all of them on his qubits. Similarly, Bob_0 applies $\tilde{C}^C \mathbf{X}_2^x$ and $\tilde{C}^C \mathbf{X}_a^y$. It gives:

$$|\psi^{(3)}\rangle \quad = \quad |0\rangle_2(\sqrt{p_0}|0\rangle_C|\psi_0^0\rangle_4|00\rangle_{ab} + \sqrt{p_1}|1\rangle_C|\psi_0^1\rangle_4|\beta_{00}\rangle_{ab}) \tag{A12}$$

Finally, Bob_0 uses controlled quantum measurements again when the control register is $|1\rangle_C$ to measure the qubit a getting $|z\rangle_a$ as outcome. He performs $C^C \mathbf{X}_a^z$ and uses controlled classical communication to share the outcome to Bob_1 who performs $\mathbf{X}_b^z$. It gives the state:

$$|\psi^{(4)}\rangle \quad = \quad |000\rangle_{2ab}(\sqrt{p_0}|0\rangle_C|\psi_0^0\rangle_4 + \sqrt{p_1}|1\rangle_C|\psi_0^1\rangle_4) \tag{A13}$$

which, disregarding $|000\rangle_{2ab}$, fits with $|\psi_{final}\rangle$ in (10) upon the application of $C_{SWAP_{2,4}}$.

Appendix C. Conditional Probability for Eve Success in the Protocol

Departing from the double teleported state after of the Bob_1 processing but before to the Bob_0 processing and Alice's measurement of the control system:

$$|\psi_1\rangle \equiv \sqrt{p_0}|0\rangle_C \otimes |\psi_0\rangle_2 \otimes |0\rangle_4 + \sqrt{p_1}|1\rangle_C \otimes |0\rangle_2 \otimes |\psi_0^1\rangle_4 \tag{A14}$$

then, we consider the state $|k\rangle_{\theta,p}$ stated on the basis generated by the θ, p parameters:

$$|k\rangle_{\theta,p} \quad = \quad (-1)^{pk}(f_k(\frac{\theta}{2})|0\rangle + (-1)^{p+k} f_{1\oplus k}(\frac{\theta}{2})|1\rangle) \tag{A15}$$

so, we get the expressions for the following projections:

$$_{\theta,p}\langle k|0\rangle \quad = \quad (-1)^{pk} f_k(\frac{\theta}{2}) \tag{A16}$$

$$_{\theta,p}\langle k|\psi_0^1\rangle \quad = \quad (-1)^{pk} W_1 \tag{A17}$$

where we have defined the quantity:

$$W_i \quad \equiv \quad f_k(\frac{\theta}{2}) \cos\left(\omega_i - (-1)^p \frac{\theta}{2}\right) + (-1)^{p+k+1} f_{1\oplus k}(\frac{\theta}{2}) \sin\left(\omega_i - (-1)^p \frac{\theta}{2}\right) \tag{A18}$$

Then, Eve performs the sifting on the Bob_1 state measuring it and then returning it to Bob_1. In addition, Bob_0 processing is followed, which gives (omitting the tensor product for simplicity, but indicating the systems with a proper subscript):

$$|\psi_2\rangle \equiv C^C \mathcal{U}_{0_2} \cdot |k\rangle_{\theta,p_4}\langle k| \cdot |\psi_1\rangle = (-1)^{pk}|k\rangle_{\theta,p_4}\left[\sqrt{p_0} f_k(\frac{\theta}{2})|0\rangle_C|\psi_0^0\rangle_2 + \sqrt{p_1} W_1|1\rangle_C|0\rangle_2\right] \tag{A19}$$

where the previous expressions have been applied on the corresponding projections on the Bob_1 state. At this point, note that the Eve sifting could be performed equivalently before or after to the Bob_0 processing because measurement and the last processing works on different systems. It implies that Type B and C become equivalent for the current calculation as it was stated in Section 5.2. Thus, in any case Eve obtains $|k\rangle_{\theta,p}$ as outcome (after selecting the basis defined by θ, p).

In the following step, the $C_{SWAP_{2,4}} \equiv \mathbf{X}_C \cdot C^C_{SWAP_{2,4}} \cdot \mathbf{X}_C$ is applied between the Bob's, giving:

$$|\psi_3\rangle \equiv C_{SWAP_{2,4}} \cdot |\psi_2\rangle = (-1)^{pk}\left[\sqrt{p_0} f_k(\frac{\theta}{2})|0\rangle_C|k\rangle_{\theta,p_2}|\psi_0^0\rangle_4 + \sqrt{p_1} W_1|1\rangle_C|0\rangle_2|k\rangle_{\theta,p_4}\right] \tag{A20}$$

Then, Alice performs the measurement of the control state on the basis stated by the election of K. Here, she hits her selection $|b_j\rangle$ so the next measurement performed by Bob_1

could be performed equivalently after or before to the Alice's measurement for calculation purposes. Employing such property, we get first:

$$|\psi_4\rangle \equiv {}_{\theta,p_4}\langle k|\psi_3\rangle = (-1)^{pk}\left[\sqrt{p_0}f_k(\frac{\theta}{2})|0\rangle_C|k\rangle_{\theta,p_2}\ {}_{\theta,p_4}\langle k|\psi_0^0\rangle_4 + \sqrt{p_1}W_1|1\rangle_C|0\rangle_2\right] \quad \text{(A21)}$$

where it has been assumed that he hits on the same basis selection and outcome that Eve to then get the success probability of her. Then, finally performing the Alice's measurement with outcome $|b_j\rangle$:

$$\begin{aligned} |\psi_5\rangle &\equiv {}_C\langle b_j| \cdot {}_{\theta,p_4}\langle k|\psi_4\rangle \\ &= \sqrt{p_0}\beta_{0\oplus j}W_0 f_k(\frac{\theta}{2})e^{i\phi_m j}|k\rangle_{\theta,p_2} + (-1)^{j+pk}\sqrt{p_1}\beta_{1\oplus j}W_1 e^{-i\phi_m(1+j)}|0\rangle_2 \end{aligned} \quad \text{(A22)}$$

We will need to switch $k \to k \oplus 1$ as the outcome obtained by Eve and Bob_1 in the main text. In this way, by imposing the prescriptions to assemble the transmitted state from Alice to Bob_1 discussed in the text: $p = 0, j + m = 1, e^{i\phi_m} = (-1)^m$, as well as Formulas (24) and (25), we calculate the norm of the last state. It corresponds to the success probability for Eve, P, given when Eve and Bob_1 meet their outcomes and basis, while Alice succeeds in her planned $|b_j\rangle$ measurement:

$$\begin{aligned} P &= p_0\beta_{0\oplus j}^2\left[f_{k\oplus 1}(\omega_0)f_{k\oplus 1}(\frac{\theta}{2}) - Kf_{k\oplus 1}(\omega_1)\right]^2 \\ &= C_0(p_0,K)(f_{k\oplus 1}(\frac{\theta}{2})\sqrt{1-K^2f_k^2(\omega_1)} - Kf_{k\oplus 1}(\omega_1))^2 \end{aligned} \quad \text{(A23)}$$

where we have reduced $W_i = f_k(\omega_i)$ applying the prescriptions. Note this probability is referred to the entire process. To get the conditional or relative probability to the useful key cases, P_E, we will need to divide P by the corresponding P_j to restrict the universe to the successful control measurement outcome, because in fact, it implies that Alice, Eve, and Bob_1 meet their measurement basis and outcomes.

Appendix D. Conditional QBER in the Protocol

Similarly to the Eve success probability, taking the teleported state after of the Bob_1 processing but before to the Bob_0 processing and the Alice's measurement of the control system (A14), then we consider the sifting and measurement from Eve, reaching the outcome $|k'\rangle_{\theta',p}$, with $\theta' \neq \theta$, the basis planned by Alice. k' is also not necessarily equal to $k \oplus 1$ (the outcome finally obtained by Bob_1). Following the expressions (A15)–(A17): ${}_{\theta',p}\langle k'|0\rangle = (-1)^{pk'}f_{k'}(\frac{\theta}{2})$ and ${}_{\theta',p}\langle k'|\psi_0^1\rangle = (-1)^{pk'}W_1'$, where, in this case, we introduced the quantity:

$$W_i' \equiv f_{k'}(\frac{\theta'}{2})\cos\left(\omega_i - (-1)^p\frac{\theta}{2}\right) + (-1)^{p+k'+1}f_{1\oplus k'}(\frac{\theta'}{2})\sin\left(\omega_i - (-1)^p\frac{\theta}{2}\right) \quad \text{(A24)}$$

As before, Eve performs the sifting, measuring, and returning on the Bob_1 state. Then, Bob_0 processing is followed similarly as in (A19), giving:

$$|\psi_2'\rangle \equiv C^C\mathcal{U}_{0_2} \cdot |k'\rangle_{\theta',p_4}\langle k'| \cdot |\psi_1\rangle = (-1)^{pk'}|k'\rangle_{\theta',p_4}\left[\sqrt{p_0}f_{k'}(\frac{\theta'}{2})|0\rangle_C|\psi_0^0\rangle_2 + \sqrt{p_1}W_1'|1\rangle_C|0\rangle_2\right] \quad \text{(A25)}$$

Observe that, in any case, Eve obtains $|k'\rangle_{\theta',p}$ as the outcome (by selecting the basis defined by θ', p). Now, the $C_{SWAP_{2,4}} \equiv \mathbf{X}_C \cdot C^C_{SWAP_{2,4}} \cdot \mathbf{X}_C$ is applied between the Bob's, obtaining:

$$|\psi_3'\rangle \equiv C_{SWAP_{2,4}} \cdot |\psi_2'\rangle = (-1)^{pk'}\left[\sqrt{p_0}f_{k'}(\frac{\theta'}{2})|0\rangle_C|k'\rangle_{\theta',p_2}|\psi_0^0\rangle_4 + \sqrt{p_1}W_1'|1\rangle_C|0\rangle_2|k'\rangle_{\theta',p_4}\right] \quad \text{(A26)}$$

Now, Alice performs the measurement of the control state on the basis stated by K, hitting $|b_j\rangle$ and generating the state $|k''\rangle_{\theta,p}$ on qubit 4, thus:

$$\begin{aligned} |\psi_4'\rangle &\equiv {}_{\theta,p_4}\langle k''|\psi_3'\rangle \\ &= (-1)^{pk'}\left[\sqrt{p_0}f_{k'}(\frac{\theta'}{2})|0\rangle_C|k'\rangle_{\theta',p_2}\ {}_{\theta,p_4}\langle k''|\psi_0^0\rangle_4 + \sqrt{p_1}W_1'|1\rangle_C|0\rangle_2\ {}_{\theta,p_4}\langle k''|k'\rangle_{\theta',p_4}\right] \end{aligned} \quad \text{(A27)}$$

where it has been assumed that he hits on a different basis selection than Eve, and a different outcome, but still in the same basis than Alice planned. It will let, under the reconciliation, notice the presence of Eve. Then, finally performing Alice's measurement with outcome $|b_j\rangle$:

$$\begin{aligned} |\psi_5'\rangle \equiv {}_C\langle b_j|\cdot {}_{\theta,p_4}\langle k''|\psi_4'\rangle = (-1)^{p(k'+k'')}\Big[\sqrt{p_0}\beta_{0\oplus j}W_0 f_{k'}(\frac{\theta'}{2})e^{i\phi_m j}|k'\rangle_{\theta',p_2} \\ +(-1)^{j+pk'+k'(k'+k'')}\sqrt{p_1}\beta_{1\oplus j}W_1' f_{k'\oplus k''}(\frac{\Delta\theta}{2})e^{-i\phi_m(1+j)}|0\rangle_2\Big] \end{aligned} \quad \text{(A28)}$$

where W_0 is the same expression as in (A18) but changing k by k'' and $\Delta\theta = \frac{\theta-\theta'}{2}$. As in the Appendix C, we set the prescriptions there. With this, $W_0 = f_{k''}(\omega_0)$ and $W_1' = f_{k''}(\omega_1 + \frac{\Delta\theta}{2})$. Additionally, we note that if $k \oplus 1$ is the outcome planned by Alice to reach Bob_1 in absence of the Eve's intervention, then we will need set $k \oplus 1 \neq k'' \to k'' = k$. It implies that $f_k(\omega_0) = (-1)^{j+m}Kf_k(\omega_1) = -Kf_k(\omega_1)$. Finally, by obtaining the norm of (A28), then summing over $k' = 0, 1$, we get the absolute QBER (without disregarding the failures in the control measurement by Alice):

$$P_{QBER_{abs}} = C_0(p_0, K)K^2\sum_{k'=0}^{1}\left[f_k(\omega_1)f_{k'}(\frac{\theta'}{2}) - (-1)^{k'(k+k')}f_k(\omega_1+\frac{\Delta\theta}{2})f_{k\oplus k'}(\frac{\Delta\theta}{2})\right]^2 \quad \text{(A29)}$$

To get the conditional or relative QBER to the useful key cases, $P_{QBER_{rel}}$, we will need, as before, to divide $P_{QBER_{abs}}$ by the corresponding P_j to restrict the universe to the successful control measurement outcome.

References

1. Hong, K.W.; Foong, O.M.; Low, T.J. Challenges in Quantum Key Distribution: A Review. In *ICINS '16: Proceedings of the 4th International Conference on Information and Network Security;* Association for Computing Machinery: New York, NY, USA, 2016; pp. 29–33.
2. Ghosh, C.; Parag, A.; Datta, S. Different Vulnerabilities And Challenges Of Quantum Key Distribution Protocol: A Review. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 307–311. [CrossRef]
3. Ribeiro, J. Cryptography. In *Theoretical Advances in Practical Quantum Cryptography*; Delft University of Technology: Delft, The Netherlands, 2020; p. 32.
4. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313. [CrossRef]
5. Sajeed, S.; Radchenko, I.; Kaiser, S.; Bourgoin, J.P.; Pappa, A.; Monat, L.; Legré, M.; Makarov, V. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A* **2015**, *91*, 032326. [CrossRef]
6. Sen, D. The Uncertainty relations in quantum mechanics. *Curr. Sci.* **2014**, *107*, 203–218.
7. Miller, D.A.B. Entanglement. In *Quantum Mechanics for Scientists and Engineers*; Cambridge University Press: New York, NY, USA, 2008.
8. Gyongyosi, L.; Imre, S. Dense Quantum Measurement Theory. *Sci. Rep.* **2019**, *9*, 6755. [CrossRef]
9. Cao, W.-F.; Zhen, Y.-Z.; Zheng, Y.-L.; Chen, Z.-B.; Liu, N.-L.; Chen, K.; Pan, J.-W. Highly Efficient Quantum Key Distribution Immune to All Detector Attacks. *arXiv* **2014**, arXiv:1410.2928.
10. Singh, H.; Gupta, D.-L.; Singh, A.-K. Quantum Key Distribution Protocols: A Review. *IOSR J. Comput. Eng.* **2014**, *16*, 1–9. [CrossRef]
11. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the Computer System and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
12. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121. [CrossRef]
13. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef]

14. Ekert, A.-K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef]
15. Padmavathi, V.; Vishnu-Vardhan, B.; Krishna, A.-V.-N. Quantum Cryptography and Quantum Key Distribution Protocols: A Survey. In Proceedings of the IEEE 6th International Conference on Advanced Computing, Bhimavaram, India, 27–28 February 2016; pp. 556–562.
16. Hughes, R.; Nordholt, J. Refining Quantum Cryptography. *Science* **2011**, *333*, 1584–1586. [CrossRef] [PubMed]
17. Bernstein, D.J.; Lange, T. *Post-Quantum Cryptography: Dealing with the Fallout of Physics Success*; Cryptology ePrint Archive: Report 2017/314; TU/e: Eindhoven, Denmark, 2017.
18. Lo, H.K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
19. Bouwmeester, D.; Pan, J.; Mattle, K.; Eibl, M.; Weinfurter, H.; Zeilinger, A. Experimental quantum teleportation. *Nature* **1997**, *390*, 575–579. [CrossRef]
20. Kim, Y.-H.; Kulik, S.P.; Shih, Y. Quantum Teleportation of a Polarization State with a Complete Bell State Measurement. *Phys. Rev. Lett.* **2001**, *86*, 1370. [CrossRef]
21. Sun, Q.C.; Mao, Y.L.; Chen, S.J.; Zhang, W.; Jiang, Y.F.; Zhang, Y.B.; Zhang, W.J.; Miki, S.; Yamashita, T.; Terai, H.; et al. Quantum teleportation with independent sources and prior entanglement distribution over a network. *Nat. Photonics* **2016**, **10**, 671–675. [CrossRef]
22. Liu, Q. *Cryptography in the Age of Quantum Computers 2.0*; Princeton University: Princeton, NJ, USA, 2021.
23. Metcalf, B.J.; Spring, J.B.; Humphreys, P.C.; Thomas-Peter, N.; Barbieri, M.; Kolthammer, W.S.; Jin, X.M.; Langford, N.K.; Kundys, D.; Gates, J.C.; et al. Quantum teleportation on a photonic chip. *Nat. Photonics* **2014**, *8*, 770–774. [CrossRef]
24. Lima, D.; Rigolin, G. Asymptotic security analysis of teleportation-based quantum cryptography. *Quantum Inf. Process.* **2020**, *19*, 201. [CrossRef]
25. de Riedmatten, H.; Marcikic, I.; Tittel, W.; Zbinden, H.; Collins, D.; Gisin, N. Long Distance Quantum Teleportation in a Quantum Relay Configuration. *Phys. Rev. Let.* **2004**, *92*, 047904. [CrossRef]
26. Ursin, R.; Jennewein, T.; Aspelmeyer, M.; Kaltenbaek, R.; Lindenthal, M.; Walther, P.; Zeilinger, A. Quantum teleportation across the Danube. *Nature* **2004**, *430*, 849. [CrossRef]
27. Takesue, H.; Dyer, S.D.; Stevens, M.J.; Verma, V.; Mirin, R.P.; Nam, S.W. Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors. *Optica* **2015**, *2*, 832–835. [CrossRef]
28. Cardoso-Isidoro, C.; Delgado, F. Symmetries in Teleportation Assisted by N-Channels under Indefinite Causal Order and Post-Measurement. *Symmetry* **2020**, *12*, 1904. [CrossRef]
29. Cardoso-Isidoro, C.; Delgado, F. Post-selected double teleportation and the modelling of its related non-local properties. *J. Phys. Conf. Ser.* **2021**, *2090*, 012033.
30. Cardoso-Isidoro, C.; Delgado, F. Quantum authentication using double teleportation. *J. Phys. Conf. Ser.* 2021, *in press*.
31. Zhou, N.; Zeng, G.; Xiong, J. Quantum key agreement protocol. *Electron. Lett.* **2004**, *40*, 1149. [CrossRef]
32. Chen, L.; Jordan, S.; Liu, Y.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
33. Bernstein, D. Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*; Bernstein, D.J., Buchmann, J., Dahmen, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2009.
34. Bennett, C.H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wootters, W.K. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Phys. Rev. Lett.* **1993**, *70*, 1895. [CrossRef]
35. Cross, O.A. *Topics in Quantum Computing*; CreateSpace Independent Pub: Scotts Valley, CA, USA, 2012.
36. Dusek, M.; Buzek, V. Quantum-controlled measurement device for quantum-state discrimination. *Phys. Rev. A* **2002**, *66*, 022112. [CrossRef]
37. Fiurásek, J.; Dusek, M.; Filip, R. Universal measurement apparatus controlled by quantum software. *Phys. Rev. Lett.* **2002**, *89*, 190401. [CrossRef]
38. Mohamed, A.A.-B.; Eleuch, H.; Raymond-Ooi, C.-H. Non-locality Correlation in Two Driven Qubits Inside an Open Coherent Cavity: Trace Norm Distance and Maximum Bell Function. *Sci. Rep.* **2019**, *9*, 19632 . [CrossRef]
39. Mohamed, A.; Eleuch, H. Quantum correlation control for two semiconductor microcavities connected by an optical fiber. *Phys. Scr.* **2017**, *92*, 065101. [CrossRef]
40. Bruß, D. Optimal Eavesdropping in Quantum Cryptography with Six States. *Phys. Rev. Lett.* **1998**, *81*, 3018–3021. [CrossRef]
41. Bennett, C.-H.; Brassard, G.; Mermin, N.-D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557. [CrossRef] [PubMed]
42. Rusca, D.; Boaron, A.; Curty, M.; Martin, A.; Zbinden, H. Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol. *Phys. Rev. A* **2018**, *98*, 052336. [CrossRef]
43. Kalra, M.; Poonia, R.-C. Design a New Protocol and Compare with BB84 Protocol for Quantum Key Distribution. In *Soft Computing for Problem Solving Advances in Intelligent Systems and Computing*; Springer: Singapore, 2019.
44. Serna, E.-H. Quantum Key Distribution from a Random Seed. *arXiv* **2013**, arXiv:1311.1582v2.
45. Chong, S.-K.; Hwang, T. Quantum key agreement protocol based on BB84. *Opt. Commun.* **2010**, *283*, 1192–1195. [CrossRef]
46. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.; Tomamichel, M.; Werner, R. Erratum: Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **2014**, *112*, 019902. [CrossRef]

47. Bechmann-Pasquinucci, H.; Gisin, N. Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography. *Phys. Rev. A* **1999**, *59*, 4238. [CrossRef]
48. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in Quantum Cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
49. Boyer, M.; Liss, R.; Mor, T. Security Against Collective Attacks of a Modified BB84 QKD Protocol with Information only in One Basis. In Proceedings of the 2nd International Conference on Complexity, Future Information Systems and Risk, Porto, Portugal, 24–26 April 2017; Volume 1, pp. 23–29.
50. Nikolopoulos, G.M.; Khalique, A.; Alber, G. Provable entanglement and information cost for qubit-based quantum key-distribution protocols. *Eur. Phys. J. D* **2015**, *37*, 441–450. [CrossRef]
51. Lo, H.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
52. Zhao, B.; Zha, X.; Chen, Z.; Shi, R.; Wang, D.; Peng, T.; Yan, L. Performance Analysis of Quantum Key Distribution Technology for Power Business. *Appl. Sci.* **2020**, *10*, 2906. [CrossRef]
53. He, W.; Guha, S.; Shapiro, J.; Bash, B. Performance analysis of free-space quantum key distribution using multiple spatial modes. *Opt. Express* **2021**, *29*, 19305. [CrossRef] [PubMed]
54. Lim, C.; Xu, F.; Pan, J.; Ekert, A. Security Analysis of Quantum Key Distribution with Small Block Length and Its Application to Quantum Space Communications. *Phys. Rev. Lett.* **2021**, *126*, 100501. [CrossRef] [PubMed]
55. Gottesman, D.; Lo, H. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **2003**, *49*, 457–475. [CrossRef]
56. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 181–182. [CrossRef]
57. Sun, Y.; Wen, Q.; Gao, F.; Zhu, F. Robust variations of the Bennett-Brassard 1984 protocol against collective noise. *Phys. Rev. A* **2003**, *80*, 032321. [CrossRef]
58. Shu, H. Asymptotically Optimal Quantum Key Distribution Protocols. *arXiv* **2021**, arXiv:2110.01973v3.
59. Breuer, H.; Petruccione, F. *The Theory of Open Quantum Systems*; Oxford University Press: Oxford, UK, 2002.
60. Eleuch, H.; Rotter, I. Nearby states in non-Hermitian quantum systems I: Two states. *Eur. Phys. J. D* **2015**, *69*, 229. [CrossRef]
61. Scheel, S.; Pachos, J.; Hinds, E.; Knight, P. Quantum Gates and Decoherence. In *Quantum Coherence*; Springer: Singapore, 2006.
62. Ash Saki, A.; Alam, M.; Ghosh, S. Study of Decoherence in Quantum Computers: A Circuit-Design Perspective. *arXiv* **2019**, arXiv:1904.04323v1.
63. Kjaergaard, M.; Schwartz, M.; Braumüller, J.; Krantz, P.; Wang, J.; Gustavsson, S.; Oliver, W. Physics Superconducting Qubits: Current State of Play. *Annu. Rev. Condens. Matter* **2019**, *11*, 95.
64. Diamanti, E.; Lo, H.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
65. Courtois, N.; Finiaz, M.; Sendrier, N. How to achieve a McEliece-based Digital Signature Scheme. In *Advances in Cryptology—ASIACRYPT 2001. Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 2248, pp. 157–174.
66. Bunandar, D.; Govia, L.; Krovi, H.; Englund, D. Numerical finite-key analysis of quantum key distribution. *npj Quantum Inf.* **2020**, *6*, 104. [CrossRef]