Journal of Physics: Conference Series **3027** (2025) 012033 doi:10.1088/1742-6596/3027/1/012033

Indefinite Quantum Key Agreement code involving a third party extendable to several participants

Gilberto Juárez-Rangel[1], Carlos Latorre-Valdivia[1] and Francisco Delgado[1]

[1] Tecnologico de Monterrey, School of Engineering and Sciences, Mexico

E-mail: fdelgado@tec.mx

Abstract. Quantum Key Agreement (QKA) is a current research topic within quantum cryptography where two or more parties collaboratively generate a shared secret key, commonly without individual full control of it. This work proposes a QKA method involving a third party other than the transmitter and receiver. Based on an initial BB84 procedure as in the EBB84 protocol, participants create an indefinite key, which becomes strong against multiple intercept-resend attacks. The process does not need decoy photons as in many other QKA protocols. Security improvements against eavesdropping are observed as compared with the BB84 protocol. The proposal could be designed to reach eavesdropping failure probabilities of $\frac{5}{16}$ on average and fidelities lower than $\frac{1}{4}$ for the modified state during the attack. The simplicity of the proposed protocol allows its implementation for more than two participants with current technology for the protection of information. Overall, it gives an understanding of the process used to share secured information between several parties without a previous agreement.

1. Introduction

Cryptography is a methodology to protect information using secret codes to mask information between two o more parties, to which any other external participant cannot have not access. This methodology commonly employs cryptographic keys to transform the original information during the transmission, until it is read by the recipient who decodes it. One of the greatest problems with classical cryptography is the use of classical channels of transmission, together with the inability to break the code using traditional computing to perform complex calculations. Both problems could be tackled with the use of quantum systems and the use of quantum processing, thus raising quantum cryptography and post-quantum cryptography respectively.

Nowadays, the most widely used quantum encryption protocol is BB84 [1]. Nevertheless, currently, there are lots of variants exploiting the features of quantum systems, such as B92 and E91 protocols as an instance. All of the mentioned protocols use both, classical and quantum channels of communication and typically authenticated channels to improve security against eavesdropping. EBB84 is a protocol that eliminates the need for a classical communication channel, reducing the potential stealing of information there.

Another problem found in classical encryption is that it often requires the need for a previous or at least an ongoing agreement between parties for the generation of the encryption key. The Quantum Key Agreement (QKA) approach allows to multiple participants generate secret encryption keys without having a previous agreement.

2. Quantum protocols of cryptography

Quantum cryptography mainly exploits a method commonly used in classical cryptography, a randomly generated key distribution using quantum channels to share the created key. This key is paired to the binary-coded message and then summing module 2 them to encrypt it. The advantage of exploiting quantum mechanics to create a key is that the key is safe and the procedure can easily detect eavesdropping attempts by the sender and receiver.

2.1. Quantum cryptography and main protocols

In BB84, to generate keys, the sender Alice shares a series of randomly encoded photons in diagonal and horizontal bases with the receiver, Bob. Bob then randomly chooses a measurement basis for each photon and measures them. Alice and Bob finally share their bases list used through a classical channel. The encryption key is taken from those cases measured using the same bases, whose outcomes should match.

B92 protocol [2] is similar to BB84, but Alice randomly generates keys using just two types of non-orthogonal states, for instance, $|H\rangle$ for the key 0 and $|+\rangle$ for the key 1, then sharing them with Bob. He measures arbitrarily in both bases assigning 0 to all diagonally polarized photons where he gets $|-\rangle$ and 1 to vertically polarized photons where he gets $|V\rangle$, communicating the photons where any of two cases happen. With that, they can construct a shared key. E91 protocol [3] uses a source generating entangled pairs shared in parallel to Alice and Bob. Only the pairs measured with the same base are retained for the key, note in this case there is not a physical transmission of the photons.

2.2. Protocol EBB84

EBB84 is a protocol based on the BB84 but eliminates the need for a classical channel when comparing the outcomes of the measurement. They first run another traditional QKD protocol to get a first shared key $K = \{K^1, K^2, \ldots, K^n\}$ (for instance BB84, otherwise B92, or E91). This shared key is used to select the basis P_i. As instance, if $K^i = 0$, P^i is the diagonal basis, otherwise if $K^i = 1$, then P^i is the rectilinear basis. It eliminates the need for classical communication to agree on the correct measurement basis selection [4]. An example of this protocol is shown in Table 1.

Table 1. EBB84 protocol beginning with the BB84 protocol generating an agreed basis key to proceed with the secret key generation. NA (not apply) corresponds to the cases when the Alice and Bob bases do not match during the BB84 stage. EBB84 is not performed for those cases.

BB84	Alice's selected bits	0	0	1	1	1	0	0	...
	Alice's basis	+	×	×	+	+	×	+	...
	Alice's photon	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	...
	Bob's basis	+	+	×	+	+	×	×	...
	Bob's measurement	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	...
	Basis key	0	1	1	1	1	0	0	...
EBB84	Alice's secret key	1	NA	1	0	0	1	NA	...
	Alice's photons state	$\|-\rangle$	NA	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	NA	...
	Bob's measured state	$\|-\rangle$	NA	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	NA	...
	Bob's secret key	1	NA	1	0	0	1	NA	...

2.3. Quantum Key Agreement (QKA)

Quantum key agreement is a cryptographic paradigm within the realm of quantum cryptography. It addresses the critical need for secure and efficient multi-party key establishment protocols, allowing multiple participants to collectively generate secret cryptographic keys without prior knowledge [5]. By using the unique properties of quantum mechanics, QKA offers a promising avenue for achieving information-theoretic security without relying on computational assumptions.

A recent QKA protocol [6] proposes the use of two classical keys of $2n$ bits each, for Alice $K_A = (k_1^A, k_2^A, \ldots, k_n^A)$ and Bob $K_B = (k_1^B, k_2^B, \ldots, k_n^B)$ where $k_i^{A,B} \in \{00, 01, 10, 11\}$. For each pair, Alice prepares the states:

$$00 \quad \rightarrow \quad |++\rangle, \quad 01 \quad \rightarrow \quad |-+\rangle, \quad 10 \quad \rightarrow \quad |+-\rangle, \quad 11 \quad \rightarrow \quad |--\rangle \tag{1}$$

Creating a sequence of two-particle states $|S_A\rangle$ (e.g. $|S_A\rangle = |++\rangle|-+\rangle \ldots |++\rangle)$). Before sending this states to Bob, Alice inserts $2n$ decoy-qubits (in the states $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$) at random positions of the sequence $|S_A\rangle$, creating the complete sequence $|S'_A\rangle$. With the decoy qubits at random positions, Alice sends the complete sequence $|S'_A\rangle$ to Bob. When Bob receives the complete sequence, he announces his key K_B to Alice via a classical channel. With this information, Alice can construct the final key by computing $K_A \oplus K_B$.

Once Bob announces his part of the key, Alice indicates the positions and the states of the decoy qubits to Bob. Bob measures them on the basis indicated by Alice. By observing the measurements on that chain of decoy qubits and comparing them with the initial states of Alice, they can notice if there was an eavesdropper with a probability of $1 - (3/4)^{2n}$ (for large n, this gets close to 1). If no eavesdropper is detected, Bob can recover each key pair $k_i^A \oplus k_i^B$ from the remaining recovered chain $|S_A\rangle$ by applying the operators $U_s = 2|s\rangle\langle s| - \mathbf{1}$ and $U_\omega = \mathbf{1} - 2|\omega\rangle\langle\omega|$ to each pair of qubits, thus obtaining $U_\omega U_s |k_i^A\rangle$ [6] and then measuring the 2 qubits in the z basis obtaining $|k_i^A \oplus k_i^B\rangle$, the same final pair in the final key already in possession of Alice. There, $|s\rangle = |++\rangle$ and $|\omega\rangle = |k_i^B\rangle$. Nevertheless, this last step can be done shortly and with less error by measuring directly the incoming qubits in the x-basis and computing the key $k_i^A \oplus k_i^B$ classically.

2.4. An improved protocol combining EBB84 and QKA

A possible weakness in the last QKA protocol depicted is the fact that Alice always uses the x-basis to send her chain $|S_A\rangle$. Nevertheless, decoy qubits have been introduced using the x and z-basis. It is the key to the protocol's success, a more secure implementation could be introduced by merging some ideas with the EBB84 protocol.

If a first EBB84 procedure is performed between Alice and Bob, they can set an initial key of length $2n$, $K_{\mathrm{M}} = (k_1^M, k_2^M, \ldots, k_i^M)$, with each $k_i^M \equiv k_{i_a}^M k_{i_b}^M \in \{00, 01, 10, 11\}$. Such a key could be used by Alice to initially codify their photons in $|S_A\rangle$ (sending it in the z-basis instead of x one) and by Bob measuring the chain. If $k_{i_{a,b}} = 0$ implies the use of x-basis, otherwise z one, then it means that he instead applies $U_\omega U_s H_a^{k_{i_a}} \oplus H_b^{k_{i_b}} |k_i^A\rangle$ (or simply he measures in the correct basis as a function of the agreed basis in the initial BB84 procedure; in this strict sense, it is not necessary to send the code by pairs). An advantage of this procedure is that the key K_{M} could be used again without a high compromise for the final cryptographic key (not a one-time pad). In the next section, we will improve this strategy.

3. A quantum cryptographic protocol using an indefinite coding with three parties

In the current section, we modify the last procedure involving three parties. While the decoy qubits strategy becomes optional, the following only regards the code qubits.

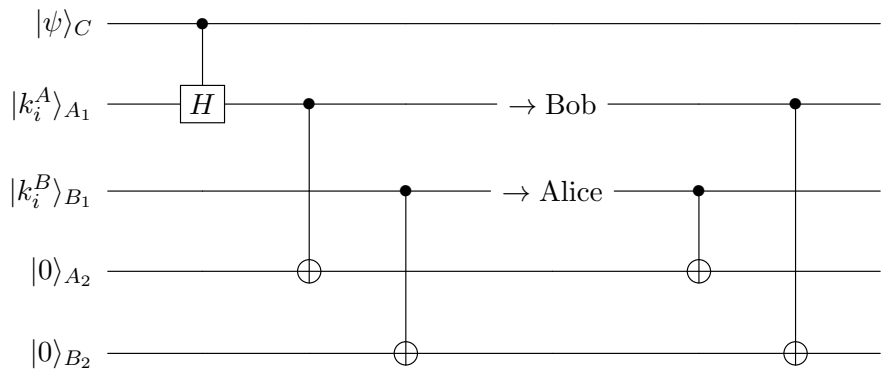


Figure 1. Circuit to generate a three-parties undefined QKA able to code simultaneously in two bases

Differently from the last procedure, a third party, Charlie (C), is a quantum system deciding the basis on which each qubit coming from Alice (A) to Bob (B) is used to codify the bit. Thus, if the state of C is $|0_C\rangle$ the basis (R) used will be the z one, instead, if it is $|1_C\rangle$ the the x-basis (D) will be used. Moreover, we will use a superposition of both states $|\psi\rangle_C = \alpha|0_C\rangle + \beta|1_C\rangle$. The procedure is depicted in the Figure 1. Note that two ancilla qubits have been added, each one in possession of A and B. They play the role of quantum registers for the final quantum agreed key. We depict the procedure for one qubit in the code.

Assuming that the qubit sent by A is $|k_i^A\rangle$ (the i-th qubit in the code), and similarly $|k_i^B\rangle$ is the Bob's qubit in the QKA chain (we are used concretely B_j as superscript in the key of Bob to denote a possible series of receivers $j = 1, 2, ..., m$ in the further development). Both qubits are being exchanged between A and B. Before A sends her qubit, C applies a Hadamard gate to code the qubit in the basis R or D, as previously depicted. Qubits have been labelled with proper subscripts C for Charlie, A_1, B_1 for the last key qubits used by Alice and Bob, and A_2, B_2 for the corresponding ancilla qubits previously mentioned. Then, the initial state is:

$$\Big(\alpha|0_C\rangle + \beta|1_C\rangle\Big)\otimes|{k_i^A}_{A_1}\rangle \otimes |{k_i}^{B_j}{}_{B_1}\rangle \otimes |0_{A_2}\rangle \otimes |0_{B_2}\rangle \tag{2}$$

after, by applying the controlled Hadamard gate $C-H$, we get:

$$\left(\alpha|0_C, {k_i^A}_{A_1}\rangle + \frac{\beta}{\sqrt{2}}|1_C\rangle\Big(|0_{A_1}\rangle + (-1)^{k_i^A}|1_{A_1}\rangle\Big)\right)|{k_i^{B_j}}_{B_1}\rangle|0_{A_2}\rangle|0_{B_2}\rangle \tag{3}$$

and then, applying the first pair of controlled-not gates $C^{A_1}NOT_{A_2}$ and $C^{B_1}NOT_{B_2}$ (between the qubits in their respective possession):

$$|\psi_{exch}\rangle = \left(\alpha|0_C\rangle|{k_i^A}_{A_1}, {k_i^A}_{A_2}\rangle + \frac{\beta}{\sqrt{2}}|1_C\rangle\Big(|0_{A_1}, 0_{A_2}\rangle + (-1)^{k_i^A}|1_{A_1}, 1_{A_2}\rangle\Big)\right)|{k_i^{B_j}}_{B_1}, {k_i^{B_j}}_{B_2}\rangle \tag{4}$$

At this point, the qubits A_1, B_1 are exchanged between A and B. Finally, another pair of controlled-not gates $C^{A_1}NOT_{B_2}$ and $C^{B_1}NOT_{A_2}$ are applied, again between the qubits in their current possession:

$$|\psi_{final}\rangle = \alpha|0_C, k_i^A{}_{A_1}\rangle|k_i^{B_j}{}_{B_1}\rangle|(k_i^A \oplus k_i^{B_j})_{A_2}\rangle|(k_i^A \oplus k_i^{B_j})_{B_2}\rangle + \tag{5}$$

$$\frac{\beta}{\sqrt{2}}\sum_{s=0}^{1}(-1)^{s\cdot k_i^A}|s_C, k_{A_1}\rangle|k_i^{B_j}{}_{B_1}\rangle|(s \oplus k_i^{B_j})_{A_2}\rangle|(s \oplus k_i^{B_j})_{B_2}\rangle$$

thus getting a notable outcome, a superposition (weighted by α, β) for the QKA code combining and sharing the cases $k_i^A \oplus k_i^{B_j}$, $0 \oplus k_i^{B_j}$, and $1 \oplus k_i^{B_j}$.

Thus, the three parties could take several alternative actions. For instance, because of the exact entanglement exhibited by (5), A or B could measure his qubits A_2, B_2 in the z-basis to get a defined shared key code, but they could use the undefined code in superposition to code and share a concrete message and still be able to decode in the other extreme. If they measure their exchanged qubits B_1, A_1 they still get an undefined code. Finally, if C measures his qubit, it still will produce the agreed code $k_i^A \oplus k_i^{B_j}$ (if he obtains $|0_C\rangle$) or still an undefined code (if he obtains $|1_C\rangle$).

Nevertheless, this procedure fails if an eavesdropper steals and replaces the qubits A_1 and B_1 during the exchange. If he measures them in the z basis, due to the entanglement, it conducts a perfect scheme for the eavesdropper: he obtains the code, and leaves the same code to Alice and Bob, so in a reconciliation process Eve goes unnoticed. To avoid this situation, we will use the idea behind of EBB84 protocol. A first BB84 procedure will be performed by Alice and Bob, thus getting a first shared chain $c_1, c_2, ...$ with $c_i \in \{0, 1\}$. These values will encode the exchange of A_1 and B_1 through the agreed selection of $U_{c_i} \in \{U_0, U_1\}$ between a pair of local operations. They will encode their qubits during the exchange, and decode them upon the reception, thus letting the procedure, but now having:

$$|\psi_{coded}\rangle = U_{c_i}^{A_1} \otimes U_{c_i}^{B_1} \cdot |\psi_{exch}\rangle \tag{6}$$

$|\psi_{final}\rangle$ will be recovered as $U_{c_i}^{A_1\dagger} \otimes U_{c_i}^{B_1\dagger} \cdot |\psi_{coded}\rangle$. In the following discussion, we have selected U_{c_i} as a pair of rotations around y given by:

$$U_{c_i} = R_y(\theta_{c_i}) = \cos\frac{\theta_{c_i}}{2}\sigma_0 + i\sin\frac{\theta_{c_i}}{2}\sigma_y, \quad \theta_{c_i} \in [0, \pi] \tag{7}$$

being σ_0 and $\sigma_i, i = x, y, z$, the identity and the Pauli operators. Still, a more complex process introducing teleportation to send those qubits is possible as in [7].

4. Security analysis under a multiple attack

In the current section, a security analysis is performed assuming that an eavesdropper does a multiple attack on the exchanged qubits by Alice and Bob following a stolen and replace scheme.

4.1. Quantum fidelity under multiple eavesdropping

Assuming that the eavesdropper Eve employs a stolen and replace scheme, then she should select the z basis to measure the stolen states in A_1, B_1, in the most efficient way during the exchange. If such measured states are $|k_{A_1}^a\rangle$ and $|k_{B_1}^b\rangle$, then the emerging state instead (4) becomes:

$$|\psi'_{coded}\rangle_{un} = |k_{B_1}^b\rangle\langle k_{B_1}^b| \cdot |k_{A_1}^a\rangle\langle k_{A_1}^a| \cdot |\psi_{coded}\rangle \tag{8}$$

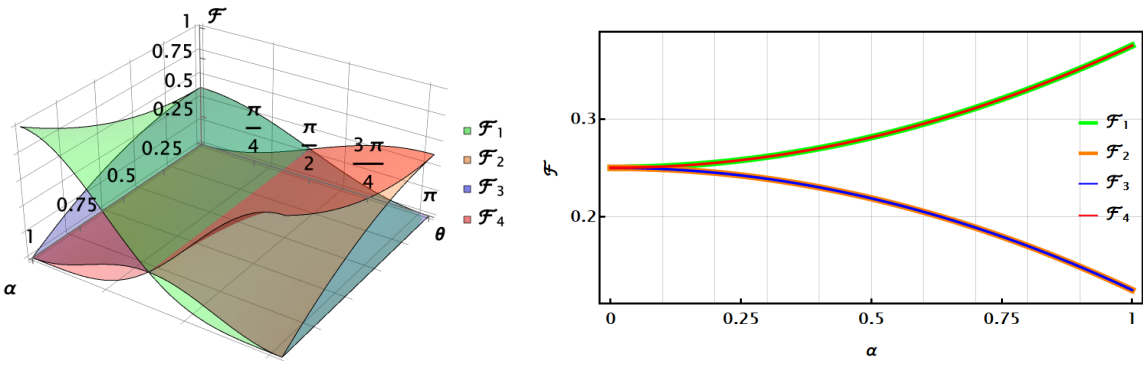
which becomes un-normalized. It should be normalized by calculating the success probability of Eve obtaining her outcomes $|k^a_{A_1}\rangle, |k^b_{B_1}\rangle$, which is simply $P_{meas} = \langle\psi'_{coded}|\psi'_{coded}\rangle_{un}$. Thus, the normalized state becomes $|\psi'_{coded}\rangle = |\psi'_{coded}\rangle_{un}/\sqrt{P_{meas}}$. Finally, upon the reception by Alice and Bob, they respectively apply first $U^{A_1\,\dagger}_{c_i}, U^{B_1\,\dagger}_{c_i}$, and then the two remaining controlled-not gates $C^{A_1}NOT_{B_2}$ and $C^{B_1}NOT_{A_2}$ to reach $|\psi'_{final}\rangle = C^{A_1}NOT_{B_2} \otimes C^{B_1}NOT_{A_2} \cdot U^{A_1\,\dagger}_{c_i} \otimes U^{B_1\,\dagger}_{c_i} \cdot |\psi'_{coded}\rangle$, a final state altered by Eve in the process. Here, we are interested in the fidelity of the process:

$$\mathcal{F} = |\langle\psi'_{final}|\psi_{final}\rangle|^2 \tag{9}$$

Table 2 summarizes the expressions obtained for the fidelities as function of $k^A_i, k^{B_j}_i, k^a_i, k^b_i$ values and α, θ. Note that the 4 cases can be seen as Eve obtaining k^a_i and k^b_i equal to Alice (k^A_i) and Bob ($k^{B_j}_i$), different from Bob's, different from Alice, or different from both. Those expressions were plotted in Figure 2a in colours. Note that only $\mathcal{F}_1$ reach 1 for $\alpha = 1$ and $\theta = 0, \pi$. Because the operations U_{c_i} will be selected by Alice and Bob in the agreement gained by the first BB84 process, two angles should selected as functions of the chain of $c_i = 0, 1$ values between θ_0, θ_1. Because the election of $\theta = 0$ is not convenient for Alice and Bob because Eve could effectively steal the code (at least one-half of the times in this procedure), then, we have selected the values $\theta = \frac{\pi}{4}, \frac{3\pi}{4}$. In such case, averaging each fidelity between two those values, $\overline{\mathcal{F}}_i = \frac{1}{2}(\mathcal{F}_i(\frac{\pi}{4}) + \mathcal{F}_i(\frac{3\pi}{4})), i = 1, ..., 4$, we get the plot in Figure 2b for each $\overline{\mathcal{F}}_i$ as function of α. Even if Eve knows those angles, she still will have difficulties because of the random selection decided by the initial BB84 procedure.

Table 2. Fidelity and eavesdropping failure probability expressions for each set of $k^A_i, k^{B_j}_i, k^a_i, k^b_i$ values.

k^A_i	$k^{B_j}_i$	k^a_i	k^b_i	$\mathcal{F}$	$\mathcal{P}$
0	0	0	0		
0	1	0	1	$\mathcal{F}_1 = \frac{1}{2}\cos^2\frac{\theta}{2}\left(1+\alpha^2\cos\theta\right)$	$\mathcal{P}_1 = 1 - \frac{\cos^2\frac{\theta}{2}\left(3+\cos 2\theta - 2\left(1-\alpha^2\right)\cos\theta\right)}{2(1+\alpha^2\cos\theta)}$
1	0	1	0		
1	1	1	1		
0	0	0	1		
0	1	0	0	$\mathcal{F}_2 = \frac{1}{2}\sin^2\frac{\theta}{2}\left(1+\alpha^2\cos\theta\right)$	$\mathcal{P}_2 = 1 - \frac{\sin^2\frac{\theta}{2}\left(3+\cos 2\theta + 2\left(1+\alpha^2\right)\cos\theta\right)}{2(1+\alpha^2\cos\theta)}$
1	0	1	1		
1	1	1	0		
0	0	1	0		
0	1	1	1	$\mathcal{F}_3 = \frac{1}{2}\cos^2\frac{\theta}{2}\left(1-\alpha^2\cos\theta\right)$	$\mathcal{P}_3 = 1 - \frac{\cos^2\frac{\theta}{2}\left(3+\cos 2\theta - 2\left(1+\alpha^2\right)\cos\theta\right)}{2(1-\alpha^2\cos\theta)}$
1	0	0	0		
1	1	0	1		
0	0	1	1		
0	1	1	0	$\mathcal{F}_4 = \frac{1}{2}\sin^2\frac{\theta}{2}\left(1-\alpha^2\cos\theta\right)$	$\mathcal{P}_4 = 1 - \frac{\sin^2\frac{\theta}{2}\left(3+\cos 2\theta + 2\left(1-\alpha^2\right)\cos\theta\right)}{2(1-\alpha^2\cos\theta)}$
1	0	0	1		
1	1	0	0		



a) b)

Figure 2. a) Fidelities $\mathcal{F}_i, i = 1, ..., 4$ as function of α, θ as depicted in Table 2; b) Average fidelities $\overline{\mathcal{F}}_i$ as function of α upon the uniform election of θ between $\frac{\pi}{4}$ and $\frac{3\pi}{4}$.

As seen in Figure 2a, to keep the process secure, the value of α should remain lower (as instance below than $\frac{1}{\sqrt{2}}$) as it increases Eve's chances of effectively stealing the code at least for a couple of fidelity cases. As consistently shown in Figure 2b, some of those fidelities increase when α is closer to 1, despite the average remaining 0.25. Even though the values of $\mathcal{F}_2$ and $\mathcal{F}_3$ decrease when α comes closer to 1, the values of $\mathcal{F}_1$ and $\mathcal{F}_4$ increase suggesting best outcomes for Eve. Because maintaining α on the same value could provide some advantage to the eavesdropper, an α variable could be more recommended. Otherwise, if θ is switched between two values, its range should still be taken into consideration to provide convenient values for $\mathcal{F}_i$ in the process.

$\mathcal{F}_i$ induced by Eve's measurement as compared with the final state expected by Bob and Alice is $\frac{1}{4}$ in average independently of α, θ. In fact, in agreement with the particular values selected for θ in Figure 2b, the election of α could become important if the values of $c_i = 0$ are not balanced. It is not possible for the BB84 initial procedure to at least a modification, for instance, the election of a different basis to measure some of the code outcomes (other than the x basis there as an instance). If such change is performed, then the more lower fidelity election could be induced.

Otherwise, when using lower values of α, the range of each $\mathcal{F}_i$ drops in general, becoming almost similar for both cases of θ, so the previous selection imposed by the BB84 bits will not have significant changes in the fidelity. Nevertheless, a lower fidelity does not provide complete security against eavesdropping, so we will need to quantify the failure probability for the eavesdropper.

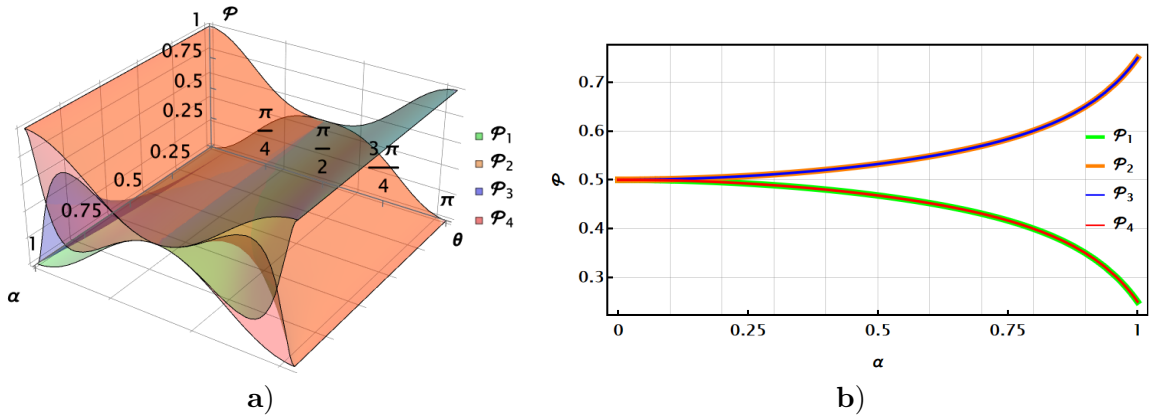
4.2. Eavesdropping effectivity under reconciliation

Under a reconciliation process, Alice and Bob will measure their pair of qubits to compare them. We will calculate the probability of failure of Eve by assuming that the last measures become equal, $|k_{A_2}\rangle, |k_{B_2}\rangle$ with $k = 0, 1$, then obtaining its complement, $\mathcal{P}$:

$$\begin{aligned} \mathcal{P} &= 1 - \sum_{k=0}^{1} |\langle \psi'_{k_{rec}} | \psi'_{k_{rec}} \rangle_{un}|^2 \\ &\text{with :} \quad |\psi'_{k_{rec}}\rangle_{un} = \langle k_{A_2} k_{B_2} | \psi'_{final} \rangle \end{aligned} \tag{10}$$

As in the previous section, and following the same methodology, we have constructed plots for $\mathcal{P}$ in Figure 3a for each set of $k_i^A, k_i^{B_j}, k_i^a, k_i^b$ values as function of α, θ (the corresponding

expressions were included in the last column of Table 2). Note that only two of those probabilities reach the values of zero, but just if the other two reach the value of 1, but restricted to $\alpha = 1$ and for $\theta = 0, \pi$. As before, we get the average failure probability upon the uniform selection of θ as $\frac{\pi}{4}$ and $\frac{3\pi}{4}$. Thus, $\overline{\mathcal{P}}_i = \frac{1}{2}(\mathcal{P}_i(\frac{\pi}{4}) + \mathcal{P}_i(\frac{3\pi}{4})), i = 1, ..., 4$ are shown in Figure 3b, being lower for low values of α as for $\overline{\mathcal{F}}_i$. Still, note that the average is α-independent and equal to $\frac{1}{2}$ for the case shown. In fact, for other selection of θ_0 and $\theta_1 = \theta_0 + \frac{\pi}{2}$, the average remains in $\frac{1}{2}$.



a) **b)**

Figure 3. a) Failure probabilities for Eve $\mathcal{P}_i, i = 1, ..., 4$ as function of α, θ as depicted in Table 2; b) Average $\overline{\mathcal{P}}_i, i = 1, ..., 4$ as function of α upon the uniform election of θ between $\frac{\pi}{4}$ and $\frac{3\pi}{4}$.

Moreover, given the probability functions of Eve's failure in Table 2, we can calculate the total probability of Eve's failure in the protocol in terms of α and θ. This quantity is obtained by considering the probability of occurrence of each case. As in Table 2 where the fidelity and probability of Eve's failure are the same for the cases shown, the probability of occurrence is also the same for the same cases. The probability of occurrence is equal to the fidelity. The total probability of Eve's failure results independent from the Charlie choice of α.

$$\mathcal{P}(\theta) = \sum_{i}^{4} \mathcal{F}_i(\theta)\mathcal{P}_i(\theta) \tag{11}$$

Considering different choices of θ_0 and θ_1, we still obtain $\overline{\mathcal{P}}(\theta_0, \theta_1) = \frac{1}{2}(\mathcal{P}(\theta_0) + \mathcal{P}(\theta_1))$, which is α-independent, thus it is shown in Figure 4a as a function of θ_0, θ_1. Such an election could be free, but certain selections appear more convenient. Thus, we show particular cases regarding $\Delta\theta = \theta_1 - \theta_0$ in Figure 4b, which provides some of the most convenient selections.

For the particular cases in Figure 4b, we can advise for $\Delta\theta \neq \pi/2$, the biggest Eve's failure probabilities $\overline{\mathcal{P}} \approx \frac{1}{2}$ are achieved (around $\theta_0 = \pi/2$). Nevertheless, for such a case, there exist lower probabilities around $\theta_0 = 0, \pi$. If we uniformly pick a random value of θ_0 in each bit constructed, the average probability of Eve's failure is the same for all cases. If Eve gets to know which θ_0 and θ_1 are Alice and Bob using, then, for Alice and Bob, it is natural to pick $\Delta\theta = \pi/2$, since this will give the maximum probability of Eve failure (as the case shown in Figure 3b). Note that the election $\Delta\theta \approx 0$ is few convenient because the operations U_{c_i} become practically identical, thus giving a certain advantage to Eve.

Moreover, if Alice and Bob could set a procedure to randomly select θ_0 and $\theta_1 = \theta_0 + \delta$ each time (either classically or quantumly), the average value for $\hat{\mathcal{P}}$ becomes $\delta-$independent:

$$\hat{\mathcal{P}} = \frac{1}{\pi}\int_0^{\pi} \overline{\mathcal{P}}(\theta_0, \theta_0 + \delta)d\theta_0 = \frac{5}{16} \tag{12}$$

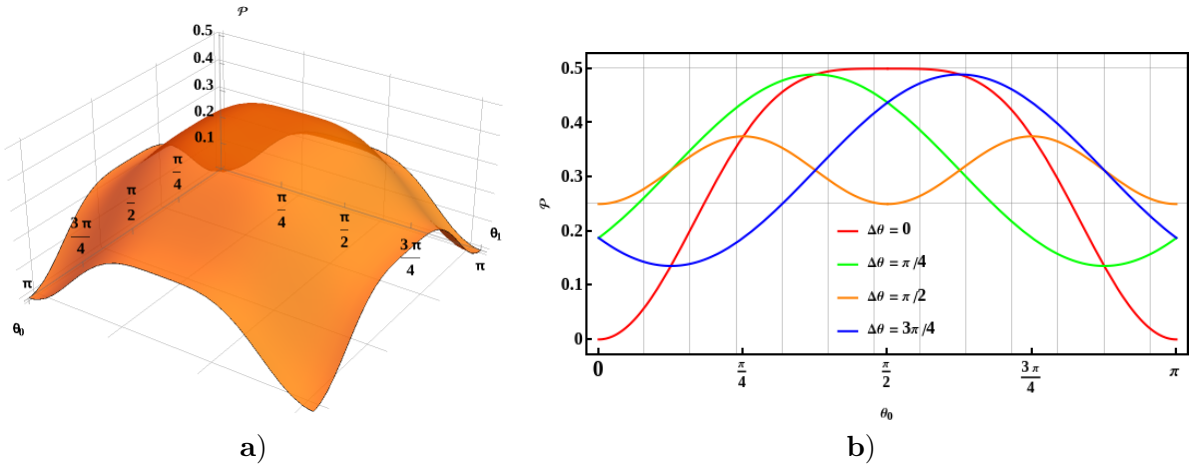


Figure 4. a) Failure probability of Eve for different values of θ_1 and θ_2; b) Failure probabilities for particular cases of $\Delta\theta$.

such a scheme provides lower probabilities of failure on average than fixing θ_0, θ_1, but otherwise introduces additional complexity for Eve guessing or deducting these values.

4.3. Generalizing the QKA protocol for several participants

The protocol can be generalized to $m+1$ participants, as instance, Alice and m receivers, $B_1, B_2, ..., B_m$. In fact, by circulating the key qubits $A_1, B_{11}, ..., B_{m1}$ between them, they can still agree on a shared key on their ancilla qubits $A_2, B_{12}, ..., B_{m1}$. It means, Alice sends her qubit to Bob_1, Bob_1 to Bob_2 and so on until Bob_m sends his qubit to Alice. This process is then repeated $m-1$ times more between the adjacent participants. In each step, each receiver applies a CNOT gate between the qubit received and their ancilla $A_2, B_{12}, ..., B_{m1}$.

To maintain security against eavesdropping, each participant must follow the procedure mentioned at the end of subsection 3 with each participant besides him (Bob_j with Bob_{j-1} and Bob_{j+1}, and so on). Note that the operations U_{c_i} could be maintained independently between each pair of participants during their exchange.

5. Conclusions

Further than Quantum Key Distribution, QKA exploits the post-quantum shared statement of a cryptographic key among several participants without single full control by any of them. In this work, we proposed an indefinite code serving efficiently as a key.

We explored how an attacker could attempt an intercept-resend attack. The indefinite code procedure shows a low fidelity between the eavesdropper-free and eavesdropper-intervened states. Because it first implements a based BB84 key as support, possibly is not as efficient as other known procedures, but still, it becomes much more secure in other aspects. It briefly explores also how multiparty communication could be performed as an extension.

Thus, the proposed code has shown robustness against multiple intercept-resend attacks by an eavesdropper, with less than 68.75% of undetected events during a reconciliation process, by each bit distributed. But it is just under the worst scenario for punctual values of the involved parameters, while under a typical alternate selection basis, this outcome dramatically drops below 50%. Due to the properties and efficiency of the model, it presents an intriguing avenue for future research, particularly in terms of time improvements and coherent attack analysis.

Acknowledgments
The authors would like to acknowledge the financial support from the School of Engineering and Sciences of Tecnologico de Monterrey in the production of this work.

References
[1] Bennett C H and Brassard G 1984 *IEEE Int. Conf. on Computers, Systems and Signal Proc.* 175-179
[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[4] Abdullah A A and Jassem Y H 2019 *JCNT* **16** (3) 1138
[5] Giuseppe A, Michael S and Gene T 2000 *IEEE J. Sel. Areas Commun.* **18** 628
[6] Xi H, Shi-Bin Z, Yan C, Chi Q, Dong-Mei L and Min H 2021 *Int J Theor Phys.* **60** 838-847
[7] Cardoso-Isidoro C and Delgado F 2022 *Symmetry.* **14** 713