Quantum Key Distribution Shared Protocol Using Teleportation and Delayed Measurement

Cinthya Hernández[1], Miriam Portillo[1], Erick Sánchez-Gaitán[1], Francisco Delgado[1] and Alan Anaya[2]

[1] Tecnologico de Monterrey, School of Engineering and Sciences, Mexico.
[2] Technical University of Denmark, Physics department, Denmark.

E-mail: `s222435@dtu.dk`

Abstract. With the rise of quantum computers, cryptographic protocols are being required to set secure communications. In the current study, a 3-party Quantum Key Distribution protocol is proposed to ensure safe communication considering ideas from BB84 and GR10 protocols against eavesdropping by using a parameterized partially entangled resource. The protocol is built so that the sender is the only one knowing the code key and the message encryption is made ongoing. Delayed measurements are applied just at the end of the protocol to decode the message effectively. The parameter of the entangled resource is used as a double control for the exchange rate of classical communications involved in the procedure. Finally, a security analysis is made, where multiple coordinated attacks could be a threat to this protocol.

1. Introduction

Nowadays, communication has evolved according to technological needs generating different trends to improve and increase the quality and security of communication. The creation of security methods and their implementation in quantum applications have led this field [1]. As representative novel alternative methods of implementation, quantum procedures have notably raised the security level of authentication and encryption by using specific combined states to be analyzed in a communication channel, thus also decreasing the probability of interception by multiple cyber-attacks [2]. To achieve that, it is possible to implement in addition to the features provided by quantum teleportation when they are applied to cryptography [1].

Together, quantum teleportation deals with the transmission of quantum information settled on qubits, from a sender (Alice) to a receiver (Bob). By using quantum entanglement channels, a distant communication between those two parties is allowed, to then transmit and obtain a message without the use of a material channel and without directly influencing the generation of the secret key [3]. This process is one of the most versatile protocols in quantum information due to its property of securely transmitting information, playing a decisive role in information science with different applications such as communications, quantum networks, the development of quantum technologies, and quantum processing [4].

Quantum cryptography is based on the use of different quantum features to guarantee the security of information against attacks. Based on established security protocols [5], one of the best known is the BB84 protocol [6]. It was the first used for Quantum Key Distribution (QKD) [6, 7]. This protocol begins with Alice sending qubits in 2 random different bases to Bob, who also performs their measurements on those random bases. Through public classical communication, Alice and Bob share the bases used in each share and measurement. Thus, they set the key with the never shared outcomes measured only on the coincident bases. The results obtained are still evaluated in a reconciliation process using part of the key. If they differ by a certain notable percentage (around 50% from the cases with common bases), it is confirmed that an eavesdropper was present, otherwise, the communication was safe [6].

In this paper, the GR10, as well as the BB84 protocols [8], are considered to build a quantum key. Among GR10's main features, it is established that the protocol works securely using partially entangled states to share classical bits of a secret key encoded in two orthogonal states to be teleported [8]. The additional use of quantum teleportation makes it possible to reduce the errors generated by the physical channels where the key is normally transmitted [8]. It allows for an increase in the fidelity of the cryptographic key being shared, which directly impacts the degree of security. On the other hand, the GR10 protocol, by using a partially entangled state, brings improvements to encryption security. In the current study, a QKD protocol is presented by combining the features of both protocols. Here, a third party is introduced acting as a control to secretively decide between the two bases codifying the key. In this case, neither the receiver nor the sender gets knowledge more than the information they provide.

The aim of the current work is to analyze a shared strategy in Quantum Key Distribution (QKD) to encrypt an ongoing message coming from the receptor of the key by following some combined ideas around BB84 and GR10 protocols, particularly using teleportation. The structure of the paper is as follows. Section 2 presents the general aspects of the protocol by analyzing its configurable functioning as BB84 or controlled BB84 protocol with delayed measurement. The third section generalizes the last procedure introducing non-maximal entangled resources during the teleportation. Conclusions are presented in the last section.

2. 3-party QKD using teleportation and delayed measurement

In the current procedure, a shared key is used, which remains unknown by two of the three parties involved in the process. As mentioned before, this approach has been considered similar to elements of the BB84 cryptographic protocol [6]. But it also implements some elements present in the GR10 protocol [8]. Together, it will be analyzed how those protocols determine the presence of the eavesdroppers threatening the QKD and reducing the success cracking probability of the encryption with respect to BB84 protocol.

A two-level state $|\psi\rangle_C$ was considered in possession of Charlie as a control system which is intended to select the basis to codify the random qubit sent by Alice:

$$|\psi\rangle_C = \sqrt{1-p_0}\,|0\rangle_C + \sqrt{p_0}\,|1\rangle_C \tag{1}$$

While, Alice qubit is randomly selected between $|0\rangle$ or $|1\rangle$ (in fact, by selecting θ as 0 or π). It will be analyzed as:

$$|\psi\rangle_A = \cos\frac{\theta}{2}\,|0\rangle_A + \sin\frac{\theta}{2}\,|1\rangle_A \tag{2}$$

The entangled resource used in the teleportation scheme is a generalized partially entangled state. Where if $\omega = \frac{\pi}{2}$ we get the Bell state $|\beta_{00}\rangle_{1,2} = \frac{1}{\sqrt{2}}(|0,0\rangle_{1,2} + |1,1\rangle_{1,2})$ corresponding to a maximally entangled state. The fact that ω can have other values other than $\frac{\pi}{2}$, gives the possibility to analyze both cases of entanglement in the procedure.

$$|B\rangle_{1,2} = \cos\frac{\omega}{2}\,|0,0\rangle_{B_1,B_2} + \sin\frac{\omega}{2}\,|1,1\rangle_{B_1,B_2} \tag{3}$$

As seen in Figure 1, the first step into the protocol consists of applying a control Hadamard gate, it allows the third party, Charlie, to decide the basis on which each qubit will be sent (Z basis, $\{|0\rangle, |1\rangle\}$; or X basis, $\{|+\rangle, |-\rangle\}$):

$$C^C H_A = |0\rangle \cdot \langle 0|_C\, \sigma_{0A} + |1\rangle \cdot \langle 1|_C\, H_A \tag{4}$$

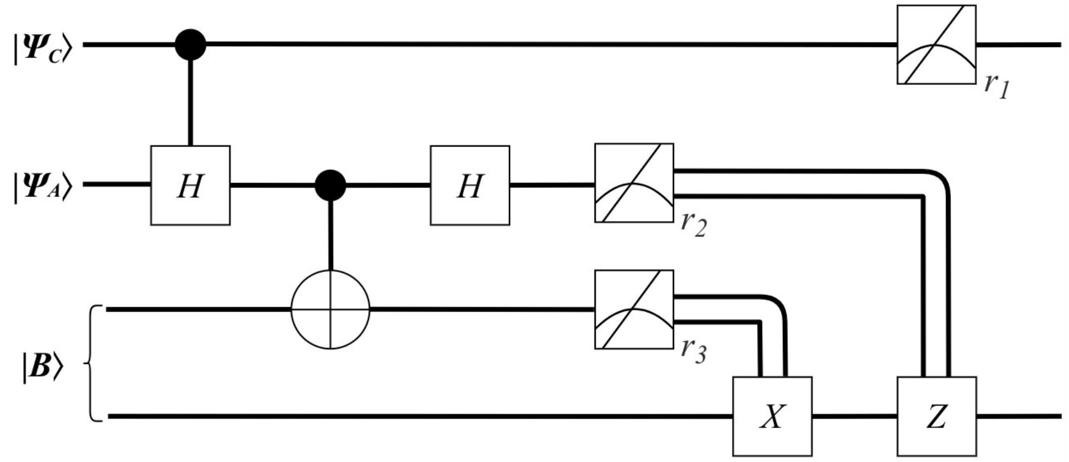


Figure 1. Quantum circuit comprising the entire procedure with the basis selection, teleportation, and a possible delayed post-measurement on the control.

Notice that, in contrast to the ordinary BB84 protocol, Alice will never know the basis selected by Charlie to send the message. After, quantum teleportation is used to transmit each qubit of the key (using $\omega = \frac{\pi}{2}$). It is worth mentioning that the entangled resource for this procedure corresponds to a maximally entangled state to demonstrate the BB84 protocol. The next step follows the same path as the teleportation algorithm by applying a C^ANOT_1 gate and a Hadamard gate H_A to Alice's qubits (A and 1). At this point, the state has been almost teleported to Bob but still measurements and corrections must be made to ensure the message becomes adequately teleported.

The measurements $\{M_{ij} = |i,j\rangle \cdot \langle i,j|_{A,B_1} \, |i,j = 0,1\}$ performed on the Alices' qubits with outcomes r_2, r_3 let to correct Bob's qubit by applying flip and phase operations to it, $X_{B_2}^{r_2}, Z_{B_2}^{r_3}$ (X and Z are the corresponding Pauli operators) in that order. The application of those phase operations is determined through classical communication from Alice to Bob. Finally, the complete settlement is obtained finishing with the qubit $|s\rangle_B$ received by Bob. Table 1 shows the different results obtained for $|s\rangle_B$ in the different cases where Charlie changes the base codification for Alice's qubit A (by just using $p_0 = 0,1$). It demonstrates this protocol works as a functional BB84 protocol using 3 parties instead of 2, Charlie decides the codifying basis.

Table 1. Algorithm functioning as a programmed BB84 protocol

Alice's qubit	Charlie's qubit	Bob's qubit
$\|0\rangle_A$	$\|0\rangle_C$	$\|0\rangle_B$
$\|0\rangle_A$	$\|1\rangle_C$	$\|+\rangle_B$
$\|1\rangle_A$	$\|0\rangle_C$	$\|1\rangle_B$
$\|1\rangle_A$	$\|1\rangle_C$	$\|-\rangle_B$

Table 2. Algorithm functioning as a BB84 protocol with delayed-measurement

Alice's	Bob qubit & Charlie's qubit
$\|0\rangle_A$	$\sqrt{1-p_0}\,\|0\rangle_B\,\|0\rangle_C + \sqrt{p_0}\,\|+\rangle_B\,\|1\rangle_C$
$\|1\rangle_A$	$\sqrt{1-p_0}\,\|1\rangle_B\,\|0\rangle_C + \sqrt{p_0}\,\|-\rangle_B\,\|1\rangle_C$

Alternatively, Table 2 shows the outcomes if Charlie has instead used a superposition control state as in (1). It clearly reduces to the previous outcomes when p_0 takes the values $0,1$. Otherwise, Charlie could decide it using a delayed retrospective post-measurement on his qubit C. Also, now it will be analyzed as a 3-party protocol for QKD using the superposition of the basis selection.

In this procedure, a series of time steps are performed departing from the sending of the codifying qubit by Alice (t_0) to the basis selection by Charlie (t_1) and finishing with the teleportation and Bob's reception of the code (t_2). Now, Bob will use the qubit received to encode an ongoing new qubit $m_k = t$ being part of a message chain built as $|m_1 m_2 ... m_n\rangle_M$, which he pretends to send back to Alice (t_3). Thus, the next step is to codify such message qubit from Bob to Alice using the state previously sent by Alice through the teleportation process. For practical purposes, in the next steps, only one qubit of the chain is analyzed, however, this could be easily repeated for any of the other qubits in Bob's message. It is important to clarify that each state of $|t\rangle_M$ only takes the values of 0 or 1.

The original Alice's qubit $|s\rangle_A$ received by Bob after the teleportation process could be written using the following general notation $|s_0\rangle \in \{|0\rangle, |1\rangle\}$ or $|s_1\rangle \in \{|+\rangle, |-\rangle\}$ as a superposition of choices made by Alice and the qubit of Charlie for the state and the basis respectively. This qubit will allow Bob to codify the new qubit message that now Bob attempts to send back to Alice by applying a $C^B NOT_M$ gate (t_3). The teleported qubit $|s\rangle_B = \alpha |s_0\rangle_B + \beta |s_1\rangle_B$ ($\alpha = \sqrt{1-p_0}, \beta = \sqrt{p_0}$) gives the following state for the messaging process (t_2):

$$\alpha |s_0\rangle_B |t\rangle_M |0\rangle_C + \beta |s_1\rangle_B |t\rangle_M |1\rangle_C \tag{5}$$

Then, the application of a $C^B NOT_M$ gate is made to the message qubit $|t\rangle_M$ controlled by the teleported state $|s\rangle_B$. A generalized superposition of codifications in each basis is shown in the equation below. When the basis corresponds to the Z basis, the message qubit is modified only if $|s_0\rangle_B = 1$. On the other hand, when the X basis is selected, the message qubit is modified to obtain an entangled state.

$$\alpha |s\rangle_B |t \oplus s\rangle_M |0\rangle_C + \frac{\beta}{\sqrt{2}} (|0\rangle_B |t\rangle_M + (-1)^s |1\rangle_B |t \oplus 1\rangle_M) |1\rangle_C \tag{6}$$

In fact, the generalized equation shows that the term with $|0\rangle_C$, then the initial state $|t\rangle_M$ in the message is directly recovered. Instead, terms with $|1\rangle_C$ become still codified with s as:

$$\alpha |s\rangle_B |t\rangle_M |0\rangle_C + \frac{\beta}{\sqrt{2}} (|0\rangle_B |t \oplus s\rangle_M + (-1)^s |1\rangle_B |t \oplus 1 \oplus s\rangle_M) |1\rangle_C \tag{7}$$

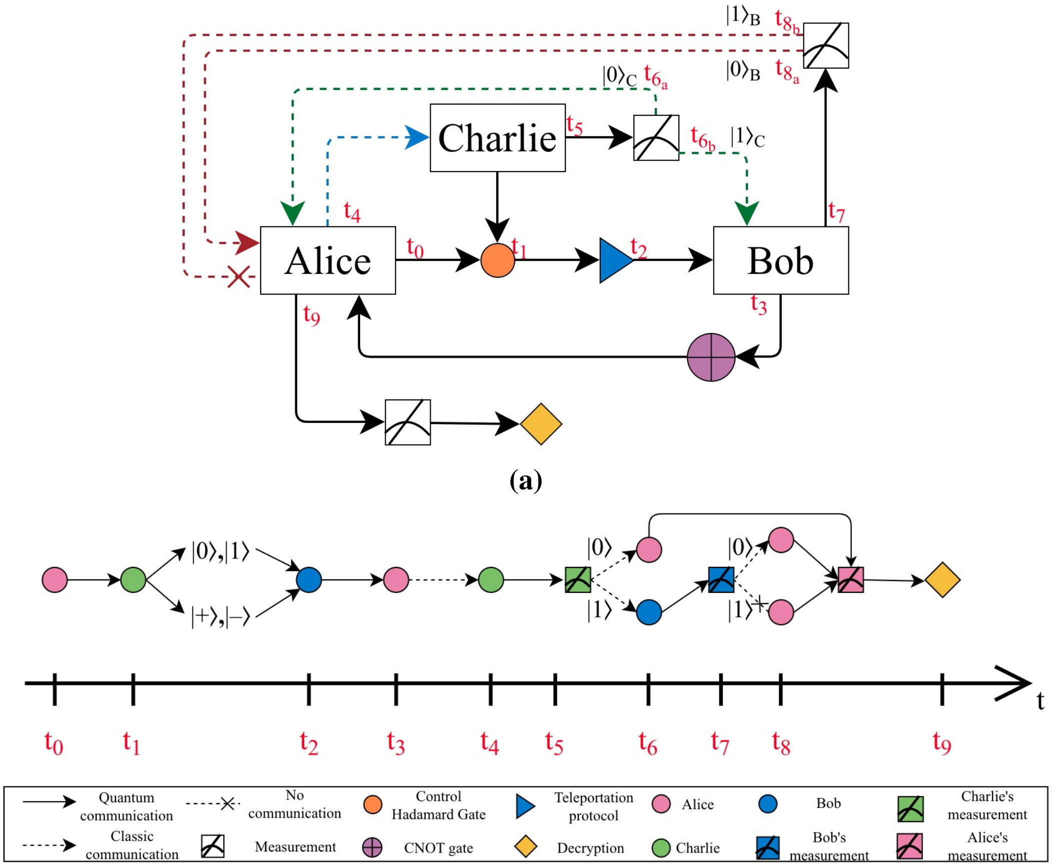
The last process has been illustrated in Figure 2a and b. While Figure 2a shows a flow chart of the process, Figure 2b shows an equivalent timeline of it. The common symbology used is shown at the bottom of Figure 2b. Steps comprising times from t_0 to t_4 have been already explained until the reception of the codified message from Bob to Alice.

The message qubit will be sent to Alice through a physical channel or again using teleportation. When the qubit arrives with Alice, she will try to decodify the message qubit (t_4). The most reasonable decodification process to be performed by Alice (without measurement) will consist of applying the operation X^s turning the information accessible to her just in case of Charlie was absent in the process. After the tentative decodification, she informs Charlie that the message was received through a classical communication channel. Charlie then measures his qubit (t_5) to set the basis finally encoding the message delayed. If he measures $|0\rangle_C$ ($r_1 = 0$) then he contacts Alice (scenario A), otherwise ($r_1 = 1$) he communicates with Bob classically (scenario B):

A. In each case where Alice receives the message from Charlie, the basis was not changed and Alice can start measuring the message (t_9).

B. Nevertheless, if instead, Charlie sends the message to Bob, he now must measure his qubits (t_7). He can obtain $|0\rangle_B$ or $|1\rangle_B$. After those measurements, Alice receives a message from Bob (scenario B.1), during a specific period if he measured a $|0\rangle_B$ (t_{8_a}). Instead, if during this time gap Alice has no information from Bob (t_{8_a}), she assumes Bob's result was the state $|1\rangle_B$ (scenario B.2). Then, Alice can start measuring the message (t_9).

As it can be seen from (7), with all this information in each case, Alice can decode and get the message sent by Bob using the operation X^s by regarding their original codifying qubit $|s\rangle_A$ (t_9). Such shared strategy lets Alice read each qubit coming from Bob, codified with a code defined delayed.



(a)

(b)

Figure 2. Ongoing codifying procedure using delayed measurement on the system selecting the code basis: (a) Flow chart of the entire procedure, and (b) Timeline version of the procedure with the common symbology in the bottom.

3. Protocol using a parameterized partial entangled state

If state $|B\rangle_{1,2}$ in (3) is generalized in terms of ω, then we define the states:

$$\left|\psi^{\pm}\right\rangle_B = \cos\frac{\omega}{2}\,|0\rangle_B \pm \sin\frac{\omega}{2}\,|1\rangle_B \tag{8}$$

$$\left|\phi^{\pm}\right\rangle_B = \sin\frac{\omega}{2}\,|0\rangle_B \pm \cos\frac{\omega}{2}\,|1\rangle_B \tag{9}$$

Note that states ${}_B\langle\psi^+|\phi^-\rangle_B = 0$ and ${}_B\langle\psi^-|\phi^+\rangle_B = 0$ are orthonormal. Then, Table 3 shows the outcomes for the protocol as a function of the Alice qubit being sent and the measurement r_3 performed on the first qubit of the entangled resource.

Notice that protocol presented at the end of the previous section could work similarly. In fact, if the message qubit $|t\rangle_B$ is considered, and $|s\rangle_A$ is the qubit originally sent by Alice, the overall states reported in Table 3 could be written, before Bob codifies the message qubit, as:

Table 3. Algorithm functioning as a BB84 protocol with delayed-measurement using a partially entangled state

Alice's qubit	Bob & Charlie's qubits	
	$r_3 = 0$	$r_3 = 1$
$\vert 0\rangle_A$	$\frac{\sqrt{2(1-p_0)}\cos\frac{\omega}{2}\vert 0\rangle_B\vert 0\rangle_C+\sqrt{p_0}\vert\psi^+\rangle_B\vert 1\rangle_C}{\sqrt{1+(1-p_0)\cos\omega}}$	$\frac{\sqrt{2(1-p_0)}\sin\frac{\omega}{2}\vert 0\rangle_B\vert 0\rangle_C+\sqrt{p_0}\vert\phi^+\rangle_B\vert 1\rangle_C}{\sqrt{1-(1-p_0)\cos\omega}}$
$\vert 1\rangle_A$	$\frac{\sqrt{2(1-p_0)}\sin\frac{\omega}{2}\vert 1\rangle_B\vert 0\rangle_C+\sqrt{p_0}\vert\psi^-\rangle_B\vert 1\rangle_C}{\sqrt{1-(1-p_0)\cos\omega}}$	$\frac{\sqrt{2(1-p_0)}\cos\frac{\omega}{2}\vert 1\rangle_B\vert 0\rangle_C+\sqrt{p_0}\vert\phi^-\rangle_B\vert 1\rangle_C}{\sqrt{1+(1-p_0)\cos\omega}}$

$$\frac{\sqrt{(1-p_0)(1+(-1)^{s\oplus r_3}\cos\omega)}\,|s\rangle_B\,|t\rangle_M\,|0\rangle_C+\sqrt{p_0}(\cos\frac{\omega}{2}\,|r_3\rangle_B+(-1)^s\sin\frac{\omega}{2}\,|r_3\oplus 1\rangle_B)\,|t\rangle_M\,|1\rangle_C}{\sqrt{1+(-1)^{s\oplus r_3}(1-p_0)\cos\omega}} \tag{10}$$

then, when Bob codifies the message with the received qubit from Alice, and also Alice decodifies the message qubit using her s value, the states becomes:

$$\sqrt{P_0}\,|s\rangle_B\,|t\rangle_M\,|0\rangle_C+\sqrt{P_1}(\cos\frac{\omega}{2}\,|r_3\rangle_B\,|t\oplus r_3\oplus s\rangle_M+(-1)^s\sin\frac{\omega}{2}\,|r_3\oplus 1\rangle_B\,|t\oplus r_3\oplus s\oplus 1\rangle_M)\,|1\rangle_C \tag{11}$$

$$\text{with}:\quad P_0=\frac{(1-p_0)(1+(-1)^{s\oplus r_3}\cos\omega)}{1+(-1)^{s\oplus r_3}(1-p_0)\cos\omega}$$

$$P_1=\frac{p_0}{1+(-1)^{s\oplus r_3}(1-p_0)\cos\omega}$$

Then, if Charlie measures his qubit obtaining $|0\rangle_C$, he can communicate with Alice as before, who measures the qubit M getting the bit message. This event occurs with probability P_0. Otherwise, if in the previous procedure Charlie gets $|1\rangle_C$ (with probability P_1), thus boosting Bob's measurement on his qubit (using the basis $|0\rangle_B, |1\rangle_B$), the procedure remains almost without changes, just varying the probabilities of each event as a function of ω, p_0. Despite this, note that in this case, Bob will call Alice if he obtains $|r_3\rangle_B$ ($r_1 = r_3$), while no call is performed to Alice if he obtains $|r_3 \oplus 1\rangle_B$ ($r_1 = r_3 \oplus 1$). Thus, Bob will call to Alice with probability $P_{1a} = P_1 \cos^2\frac{\omega}{2}$ and he will not call her with probability $P_{1b} = P_1 \sin^2\frac{\omega}{2}$. Note that under this procedure, Alice (and possibly Charlie) has control over the frequency of each one of the three scenarios that will happen. Thus, an eavesdropper cannot make predictions about it to gain an advantage in the procedure because Alice could change such frequencies in each bit message. Note that it is still possible due to the shared information among the three parties using orthogonal states. All three probabilities P_0, P_{1a}, P_{1b} are plotted on Figure 3a-c for the two cases $s \oplus r_3 = 0$ and in 3d-f $s \oplus r_3 = 0$.

Then, Figure 3 comprises all different probabilities to decode the message when Charlie makes a measurement on his qubit, thus post-selecting the base to encode the qubit: Charlie calls to Alice (P_0); Charlie calls to Bob, then Bob to Alice (P_{1a}); and Charlie call to Bob but Alice is not called (P_{1b}). Plots show the possible ways to choose different values for ω and p_0 to control such probabilities. The sum of the three probabilities will be one, and that feature is observed in every three corresponding plots (a-c) and (d-f). Probabilities also depend on the joint value of s and r_3. Alice and Bob have the knowledge of r_3, but note it was stochastic. While s is just exclusively known by Alice. Those facts help the security of the protocol, making it very difficult for a group of eavesdroppers to obtain that information.

With the selection or definition of those values ($p_0, \omega, s \oplus r_3$), the three parties can privilege the classical protocol communication and they can avoid the weakest communication channels by choosing proper values favoring some other the three cases. It limits the spies' interventions since there are random values with no predetermined rules. Note that $\omega = 0, \pi$ or 2π should be avoided because it does not

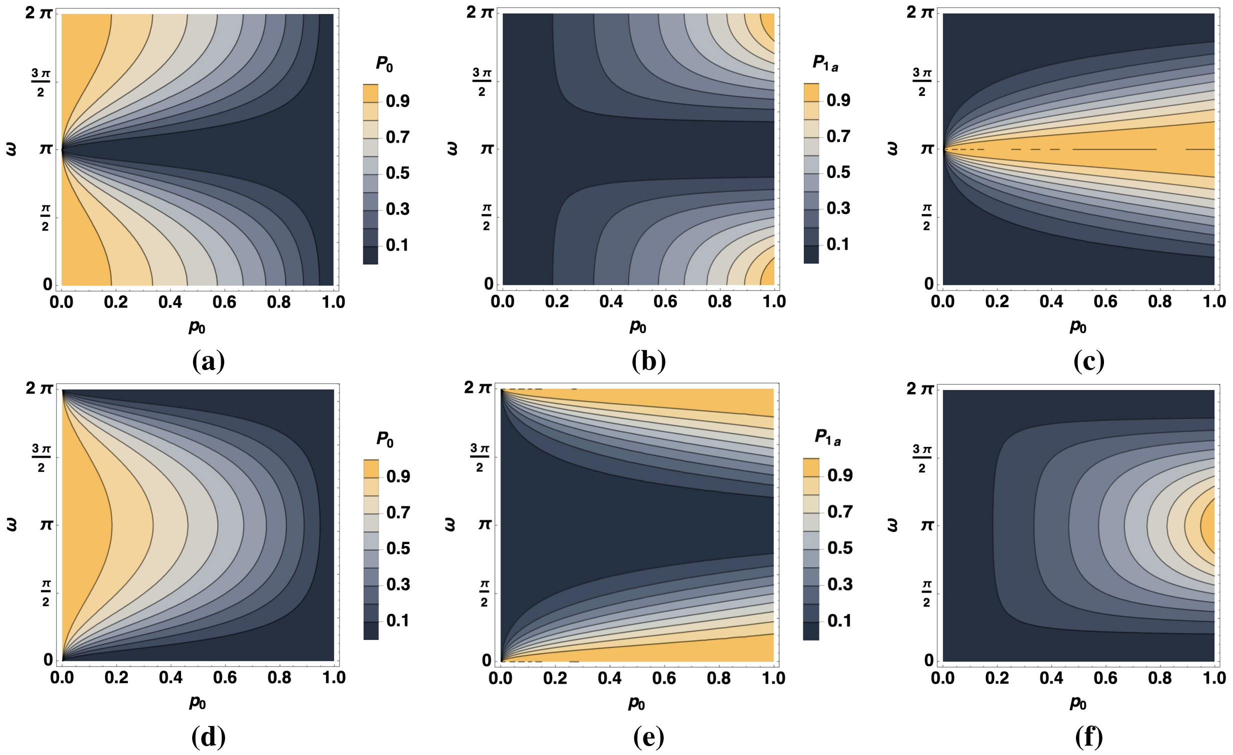


Figure 3. Contourplots for (a) $P_0, r_3 \oplus s = 0$ (b) $P_{1a}, r_3 \oplus s = 0$, (c) $P_{1b}, r_3 \oplus s = 0$, (d) $P_0, r_3 \oplus s = 1$, (e) $P_{1a}, r_3 \oplus s = 1$, and (f) $P_{1a}, r_3 \oplus s = 1$ as function of $p_0 \in [0,1]$ and $\omega \in [0, 2\pi]$.

generate the entanglement resource necessary for teleportation. Despite we will devote the following section to discussing eavesdropping, we close the current one with some examples about the elections.

For instance, if Alice chooses $\omega = \frac{\pi}{4}$ with the qubit $|s\rangle_A = 0$, Charlie selects p_0=0.2, together with the stochastic measurement $r_3 = 0$, then the case when Charlie calls Alice would have more probability of occurring as shown in Figure 3a. This can be also seen from Figure 3b and c, where those cases are unlikely to occur. In a second example, one of the most valuable cases corresponds to the equiprobable scenario where none of the three communications involved is favored: $P_0 = P_{1a} = P_{1b} = \frac{1}{3}$. Note that in the protocol of the second section it is advisable in 7 that if $p_0 = \sqrt{2/3}$ and $\omega = \frac{\pi}{2}$, all the cases will have the same probability of occurring. By superimposing the set of Figure 3a-c or 3d-f, it is found that there is a second solution with $\omega = \frac{3\pi}{2}, p_0 = \sqrt{2/3}$.

4. Multiple eavesdropping analysis and QISKIT implementation

Sharing information through classic channels rises the possibility to be stolen by an eavesdropper. While quantum key encryption ensures higher security against eavesdropping. Thus, in our last procedure, only Alice knows each key bit $|s\rangle_A$ to encode a tentative comeback message to be sent ongoing upon its reception. When teleportation is combined with the procedure, no material channels to be intercepted are present increasing security. The use of a partially entangled state for teleportation characterized by the ω parameter sets an additional control on the shared process. Such control changes the rules for the exchange rate of classical information in the process of hardening the task for eavesdroppers.

Despite this, for this protocol, a simultaneous attack can be implemented for each party involved through it: Alice, Charlie, and Bob. All of them can have possible eavesdroppers waiting to obtain the shared information. In the best case for an eavesdropper, all classical information could be considered public due to the weakness of the channels exchanging it. There, the control settled by ω plays an important task in regulating the preferred classical communication channels as a function of their security. Then, the clever information in the quantum process is centered on $|s\rangle_A$ and ω values (only known by Alice through the entire procedure), as well in the basis selection settled as a quantum superposition and the notable possibility to be settled through a delayed measurement. In fact, such a delayed measurement lets to decode the message only at the final stage when Alice has received and secured the encoded message with information only known by her.

The more critical knowledge of protocol is the information of $|s\rangle_A$ and of course $|t\rangle_M$. Then, it is assumed that neither the access to Alice's qubit ($|s\rangle_A$) since its creation until the teleportation (and their parties), nor the access to the message qubit ($|t\rangle_M$) before Bob's encoding, are achievable for none eavesdropper. Those parts should be extremely secure. Then, the weaker parts of the protocol are located on the theft of Charlie's qubit or the encoded message qubit before it arrives to Alice. We should remember that in an extreme analysis, all outputs of classical communications are available for a group of eavesdroppers under multiple attacks.

4.1. Charlie's qubit theft before or after the basis change

If an eavesdropper manages to steal Charlie's measurement results, the eavesdropper will know the codifying base used for each qubit in the codifying key. However, by choosing adequate values for ω and p_0, the X basis could be favored by probability reducing any possibility to effectively guessing the message for the eavesdropper. In fact, the X basis could cause more problems for the eavesdroppers to crack the code without collaboration of Bob, when they try to steal information from other sources.

If the eavesdropper steals the qubit sent by Charlie before the change of basis, (t_1), he can interfere with this process by establishing a unique basis by cheating on Charlie by exchanging his qubit with another in the state $|0\rangle$. In the end, even though they have interfered with the channel, the probability of decoding the message will correspond to the same as the BB84 protocol. If the eavesdropper steals information after the basis election (t_6), he should cheat Charlie by stealing and measuring his qubit and replacing it with another in the same outcome state obtained, $|0\rangle$ (the easier outcome where Charlie communicates with Alice, despite stochastic) or $|1\rangle$ (getting the Bob collaboration still becoming unnoticed, then boosting the planned Bob actions). It helps the eavesdropper to follow the natural sequence of events and, due to other accomplices collaborating with him in the classical public channels to follow the evolution of the message encoded.

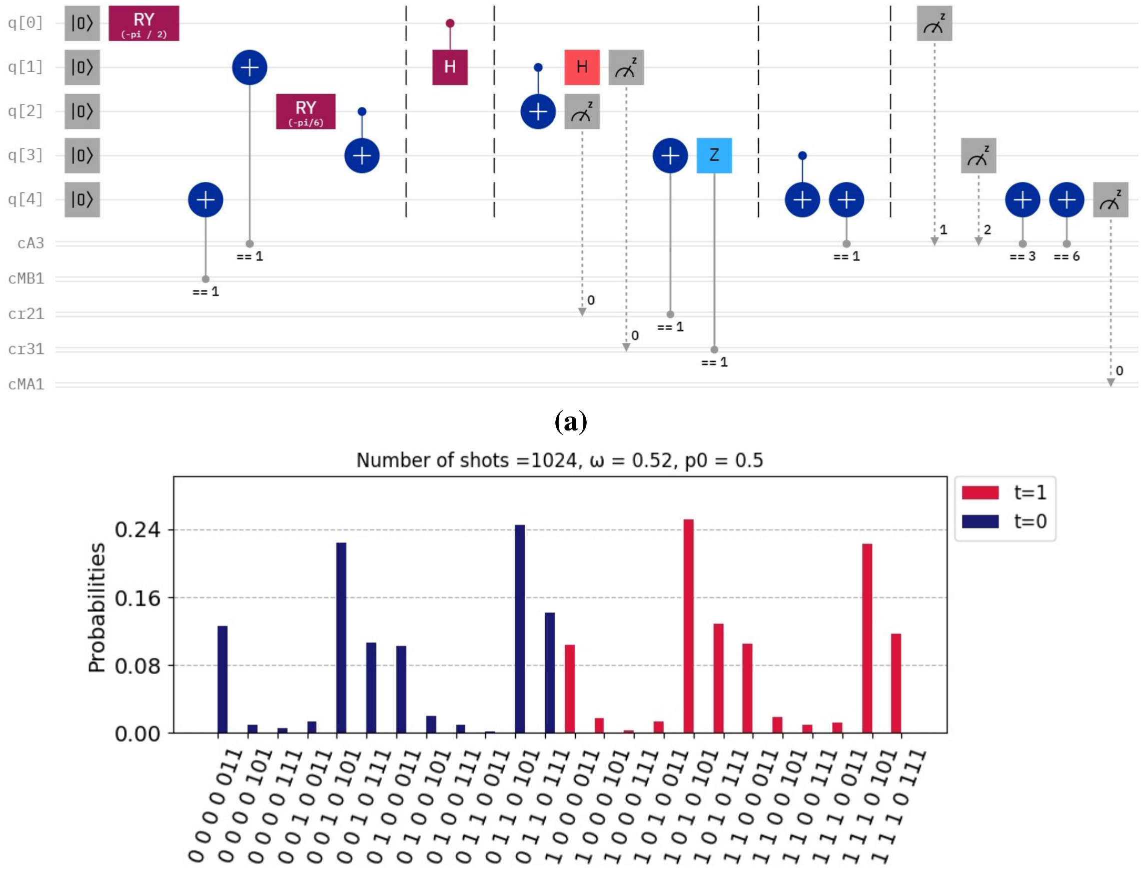
4.2. Message qubit theft before its arriving with Alice

In any case for the previous discussion, the eavesdropper will need the collaboration of another partner on Alice's side. By stealing the message qubit before it arrives to Alice, just the knowledge of the basis used to encode and the actions followed by the three parties (Alice, Bob, and Charlie), the group of eavesdroppers under such complex and improbable attack are in the same situation of Alice before the decoding. Nevertheless, only the knowledge of s will let them crack the encryption.

5. Conclusions

The protocol presented sets a scheme of ongoing quantum encryption shared among three parties and uses delayed measurement for decryption. It allows for maintaining the confidentiality of the encrypted message between the parties involved and it prevents the possible presence of several eavesdroppers working together in multiple attacks on the classical and quantum information being exchanged. In the protocol, in turn, both Alice and Bob act as receiver and sender, first sending the cryptography key, then exchanging an encoded message with that key. It is worth mentioning that Alice is the only one who knows the value of s in each qubit $|s\rangle_A$ conforming the cryptographic key, and additionally, she does not know the basis used to share the code. In our analysis, only if s is known, the eavesdroppers will have effective access to the message sent.

It has been demonstrated that the protocol can work properly as the BB84 protocol by selecting ω as $\pi/2$. On the other hand, different values for ω allow the introduction of a partially entangled state to perform the teleportation step. Also, p_0 helps increase or reduce the probability of encoding the key through two bases. While ω lets together to mix the encoding on several states and bases. This in turn means that Alice can take advantage of specific classical channels to become more secure, thus preventing information theft. The process depicted in the second section can be simulated using QISKIT as it is illustrated in Figure 4 in the dashboard composer.



(a)

(b)

Figure 4. (a) Protocol implementation on the QISKIT composer, and (b) Statistical outcomes for classical registers ($cA3$ -three-bit registers-, $cMB1$, $cr21$, $cr21$, and $cMA1$) using 1024 shots for each message value $t = 0$ (blue) and $t = 1$ (red), showing a perfect agreement between t and $cMA1$ (bottom value in the horizontal ticks).

In the implementation, $q[0] - q[4]$ quantum registers correspond to Charlie, Alice, first and second partially entangled qubits (Alice/Bob), and the Message. Classical registers with one bit are as follows: $cMB1$ is the bit of the message; $cr21$ and $cr31$ are the registers to store r_2 and r_3 respectively. While $cA3$ is a 3-bit register to store r_4 (the Bob measurement), r_1 (the Charlie measurement), and s (the bit of the state initially selected by Alice). There, r_4 is the most significant bit, and s is the least significant. From (7), we advise that if the message measurement m obtained at the end by Alice is related with t as $t = m \oplus r_1 \cdot (s + r_4)$. Then, if $cA3$ has stored $3(r_4 = 0, r_1 = 1, s = 1)$ or $6(r_4 = 1, r_1 = 1, s = 0)$, it means $r_1 \cdot (s + r_4) = 1$, then a NOT gate should be applied to the qubit message $q[4]$ to get correctly t when it is finally measured (see Figure 4a) and stored on $CMA1$.

The process has been divided by dashed lines in the following sections from left to right: states initialization, basis codification, teleportation, message encoding by Bob and decoding by Alice, and measurement process finishing with the message reading. Circuit is configurable for p_0 and ω through rotations $\mathrm{RY}(-\alpha)$ ($p_0 = \cos\frac{\alpha}{2}$) and $\mathrm{RY}(-\omega)$. In Figure 4b, the statistical outcomes of the classical registers are depicted. By using $\omega = \frac{\pi}{6}$ and $p_0 = 1/\sqrt{2}$, 1024 random shots on a quantum processor were performed by each possible value for $t = 0, 1$. Ticks in the horizontal axis correspond to the values in the classical registers (from the top to the bottom: $cA3$ -three-bit registers-, $cMB1$, $cr21$, $cr21$, and $cMA1$). Note that in each case, the value used for t meets with the value in $cMA1$, thus showing that protocol works.

Future work should be directed to the analysis of protocol under a coherent attack [9]. In this case, by tracking the Holevo information through the entire QKD and encoding process, it could be possible to have the maximum of available information to detect the weaker points of the entire protocol. It will help to secure such parts from a coherent attack.

Acknowledgments

The authors would like to acknowledge the financial support of NOVUS (Grant number: 214), Institute for the Future of Education, Tecnologico de Monterrey, Mexico, in the production of this work.

References

[1] Shu H 2022 Asymptotically optimal quantum key distribution protocols (*Preprint* `quant-ph/2110.01973`)
[2] Maitra A and Paul G 2013 *Information Processing Letters* **113**(12) 418–422
[3] Chen M C, Li R, Gan L, Zhu X, Yang G, Lu C Y and Pan J W 2019 *Phys. Rev. Lett.* **124** 080502
[4] Liu T 2020 *Journal of Physics: Conference Series* **1634**(1) 012089
[5] Adu-Kyere A, Nigussie E and Isoaho J 2022 *Sensors* **22**(16) 6284
[6] Bennet C H and Brassard G 1984 *International Conference on Computers, Systems & Signal Processing* **1** 175–179
[7] Lee C, IEEE M, Sohn I and Lee W 2022 *IEEE Transactions on Network* **19**(3) 2689–2701
[8] Lima D and Rigolin G 2020 *Quantum Information Processing* **19** 201
[9] Xiang-bin W 2002 On the role of coherent attacks in a type of strategic problem related to quantum key distribution (*Preprint* `quant-ph/0110089`)