symmetry

IMPACT FACTOR 2.940

CITESCORE 4.3

Article

Reverse Reconciliation for Optimal Error Correction in Quantum Key Distribution

Luis Adrián Lizama-Perez

MDPI

https://doi.org/10.3390/sym15030710

symmetry

MDPI

Article

Reverse Reconciliation for Optimal Error Correction in Quantum Key Distribution

Luis Adrián Lizama-Perez

Departamento de Electrónica, Universidad Técnica Federico Santa María, Campus San Joaquín. Av. Vicuña Mackenna 3939, San Joaquín, Santiago 8940897, Chile; luis.lizamap@usm.cl

Abstract: In this work, we introduce a new method for the establishment of a symmetric secret key through the reconciliation process in QKD systems that, we claim, is immune to the error rate of the quantum channel and, therefore, has an efficiency of 100% since it does not present losses during the distillation of secret keys. Furthermore, the secret rate is scaled to the square of the number of pulses on the destination side. The method only requires a single data exchange from Bob over the classic channel. We affirmed that our results constitute a milestone in the field of QKD and error correction methods at a crucial moment in the development of classical and quantum cryptanalytic algorithms. We believe that the properties of our method can be evaluated directly since it does not require the use of complex formal-theoretical techniques. For this purpose, we provide a detailed description of the reconciliation algorithm. The strength of the method against PNS and IR attacks is discussed. Furthermore, we define a method to analyze the security of the reconciliation approach based on frames that are binary arrays of 2×2. As a result, we came to the conclusion that the conjugate approach can no longer be considered secure, while we came up with a way to increase the secret gain of the method with measured bits.

Keywords: QKD; distillation; reconciliation; sifting

Citation: Lizama-Pérez, L.A. Reverse Reconciliation for Optimal Error Correction in Quantum Key Distribution. *Symmetry* **2023**, *15*, 710. https://doi.org/10.3390/sym15030710

Academic Editor: Christos Volos

Received: 6 February 2023
Revised: 28 February 2023
Accepted: 8 March 2023
Published: 12 March 2023

1. Introduction

In the era of quantum technologies, cryptography based on the quantum cryptographic key distribution (QKD) emerges as one of the most-promising methods for establishing secret symmetric keys to achieve the confidentiality of communications [1–3]. The QKD stands out, together with post-quantum cryptography [4], as one of the most-secure schemes to face the threat posed by quantum computers capable of executing cryptanalytic algorithms such as the algorithm of Shor for integer factorization of large primes [5,6].

As research results indicate [7,8], the QKD reconciliation protocols do not tolerate high noise rates in the quantum channel, which will have a negative impact on the link distance of the QKD system. This is explained by the fact that the reconciliation methods used by the QKD have not shown error correction beyond 25% [9–12]. Discrete reconciliation has been achieved by BBBSS [13], Cascade [14], Winnow [15], Liu [12], polar codes [16,17], and frame reconciliation [18]. Unfortunately, interactive protocols requires a high number of message exchanges [19,20], and worse still, they do not guarantee the complete elimination of errors. The QKD also uses other reconciliation techniques developed in the field of telecommunication technologies, among which LDPC [21,22] stands out; however, its computational complexity is very demanding and requires transmitting redundant information [23]. Consider the following two scenarios:

1. Alice prepares and sends a message to Bob adding redundant information. Then, with the help of the auxiliary information, he seeks to recover the original message by identifying and correcting the errors in the message. This is the approach of correction methods used in telecommunications such as turbo codes and LDPC.

2. Alice seeks to establish a key of random bits with Bob, i.e., there is no predefined message, then Alice must identify the bits that Bob has obtained after quantum pulses were transferred over the quantum channel and errors have occurred.

In the Cascade algorithm, Bob reveals some bits and sends them to Alice, who evaluates the results, then tells Bob what to do with the remaining bits. If necessary, Alice and Bob use and sacrifice other bits until they obtain the same set of bits.

By contrast, in our approach, Bob computes some sifting bits over small binary information structures called frames that he sends to Alice, who determines the bits on Bob's side. It is not necessary to send more bits: all the errors are corrected, and all the pulses received by Bob are used, that is there is no loss of bits. How can this be possible? Shannon's limit establishes that, when the probability of error in a channel denoted as e reaches 0.5, information transfer cannot be established.

First of all, our reconciliation approach constitutes a reverse reconciliation method, so it does not correct errors; instead, Alice identifies them and, together with Bob, builds the key based on Bob's final results, which include the errors produced in the channel and the optical detection system [24,25]. Second, in our approach, we used 2×2 frames, and in particular, we used as the starting point those in which the probability of error is e^2. By evaluating the results that most of these instances produce, we can run the entire error correction process. In our previous works, we handled the following frame-based schemes:

1. Distill the key by means of the frames in which errors are detectable using the sifting bits and adding the bits obtained from the measurements [18,26].
2. To avoid the waste of frames, the inverse of the measured bits is used instead of the measured bits, that is the conjugated bits [27].
3. In this new approach, we only used the sifting bits of those frames that produce unitary results, since, as we will see, they are more visible from Alice's point of view.

Before discussing the new approach (Section 3), in the next section (Section 2), we present a way to evaluate the security of these methods and discuss the results obtained. As a result of this analysis, we found a method to increase the secret rate in the approach that uses the measured bits, and these results are presented in the Appendix A. Therefore, we analyzed the security and performance of the new method. However, let us continue by providing a brief explanation of the BB84 protocol followed by a discussion of pairs of quantum states.

1.1. BB84

Historically, the first protocol for the quantum cryptographic key distribution (QKD) was conceived of by Bennett and Brassard in 1984; hence, it is known as BB84 [28]. The BB84 protocol encodes a bit in a pair of non-orthogonal states, so it uses four quantum states, as shown in Figure 1, where $\mathbf{i}$ is the bit ($\mathbf{i} = \mathbf{0}, \mathbf{1}$) encoded in the pair of non-orthogonal states represented by $\mathbf{i_X}$ and $\mathbf{i_Z}$.

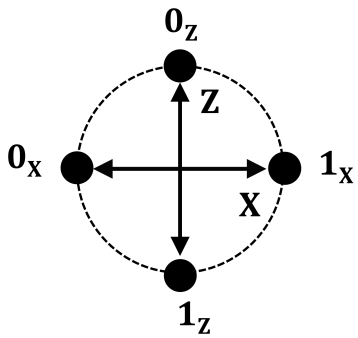

Figure 1. The quantum states of the BB84 protocol and the two measurement bases **X** and **Z** are represented through the bi-dimensional Bloch sphere. A bit is encoded by means of a pair of non-orthogonal states.

In BB84, the bits are transmitted by individual photons or quantum multiphotonic pulses, which upon arrival at the receiving station, are measured in one of the bases **X** or **Z**, which Bob chooses randomly. If the measurement basis matches the quantum state of the photon, for example if Bob measures $\mathbf{1_X}$ with the basis **X**, the result is predictable and useful for establishing a shared secret key. Otherwise, if Bob measures $\mathbf{1_X}$ with the **Z** basis, the result is ambiguous and should be discarded.

BB84 is vulnerable to the PNS attack in which the attacker separates and stores the photons coming from the multiphotonic quantum pulses that traverse the channel. Then, once Bob publishes the bases used in his measurements, Eve applies those bases, and from here, she is capable of deriving the secret key.

1.2. Pairs of Quantum States

The frame-based schemes that we have previously published are based on the following scheme: Alice sends pairs of non-orthogonal quantum states to Bob, who measures both states by applying the same measurement basis **X** or **Z** that he actively chooses. Suppose Alice sends the pair of states ($\mathbf{0_X}$, $\mathbf{0_Z}$). Bob measures the first state $\mathbf{0_X}$ with **X**, which produces $\mathbf{0_X}$. He then measures the second state $\mathbf{0_Z}$ with **X**, but produces $\mathbf{0_X}$. Although the basis does not match the quantum state, the event is useful because it produces the same result as the previous measurement.

However, in particular, if a double-matching detection event occurs in the other basis **Z**, the result can also be exploited. This implies that we have two communication channels: along the **X** basis and another through the **Z** basis, which gives us an additional advantage for the transmission of information through pairs of non-orthogonal states: they always produce a double-matching detection event. On the other hand, if the results of the two measurements are different, the result is ambiguous and cannot be used in the production of secret bits.

Figure 2 shows us the three categories that pairs of quantum states can fall into: orthogonal, non-orthogonal, and parallel. However, for the first time in the context of frame-based reconciliation, we now also took advantage of not only non-orthogonal state pairs, but also pairs of parallel states. Furthermore, as we will see in Section 3, to carry out the reconciliation, we are only interested in double-matching detection events, regardless of their origin: non-orthogonal states, parallel states, or error states, which may include orthogonal states. The only thing that really matters is that the double-matching event occurs; it does not matter whether it comes from the measurement of two erroneous states or the erroneous measurement of the states.

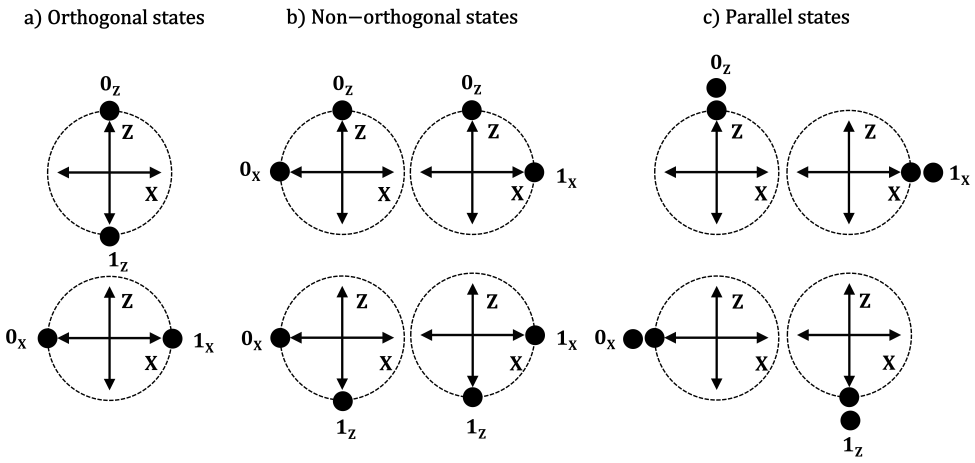

Figure 2. The pairs of quantum states are separated as orthogonal, non-orthogonal, and parallel states.

As a final remark, frame-based reconciliation does not reveal the bases used in Bob's measurements. Therefore, if Eve has copies of the sent quantum states, she must perform

measurements on both bases hoping to obtain double-matching detection events on both bases, which is not guaranteed if Eve has only a few copies of the states.

2. Security of Frame-Based Reconciliation Methods

2.1. Clarifications about the Symbology Used

With the aim of being clearer in the exposition of the later sections, let us introduce here some examples of the symbology that we used:

— $\mathbf{0_X}^i$, $\mathbf{0_Z}^j$, $\mathbf{1_X}^k$, and $\mathbf{1_Z}^l$ are examples of quantum states where the upper index i, j, k, l denotes the sequence number in which it was transmitted from Alice to Bob. As can be seen, we did not use the quantum ket notation, but rather, bold letters, in order to facilitate the discussion about the reconciliation methods. When necessary, we changed the numerical label, representing it as follows $i \to 0_{X_i}, j \to 0_{Z_j}, k \to 1_{X_k}, l \to 1_{Z_i}$, so states look like $\mathbf{0_X}^{0_{X_i}}$, $\mathbf{0_Z}^{0_{Z_j}}$, $\mathbf{1_X}^{1_{X_k}}$, and $\mathbf{1_Z}^{1_{Z_l}}$. At Bob's side, the received states, also called the detection events, are written as $\mathbf{0_X}^{\varepsilon_i}$, $\mathbf{0_Z}^{\varpi_j}$, $\mathbf{1_X}^{\epsilon_k}$, and $\mathbf{1_Z}^{\pi_l}$. Furthermore, depending on the specific context, the upper index could be omitted (in the case that the index would not be strictly necessary), or it could consist of two sequence numbers to refer to a double-matching detection event.

— $\left(-, \mathbf{1_Z}^{\pi_{l1},\pi_{l2}}\right)$ is a double-matching detection event at Bob's side: in this example, two detection events with the **Z** basis that produced $\mathbf{1_Z}$. We write between rectangular brackets the sequential numerical indices of such events, which in this case are $[\pi_{l1}, \pi_{l2}]$, where the position of the labels π_{l1}, π_{l2} between brackets $[\pi_{l1}, \pi_{l2}]$ does not matter. However, in a double-matching detection event, we write the **X** basis to the left as $(\mathbf{1_X}^{\epsilon_{k1},\epsilon_{k2}}, -)$ and the **Z** basis to the right as $\left(-, \mathbf{1_Z}^{\pi_{l1},\pi_{l2}}\right)$.

— $\{(\mathbf{1_X}^{1_{X_k}}, \mathbf{0_Z}^{0_{Z_j}}), (\mathbf{0_X}^{0_{X_i}}, \mathbf{1_Z}^{1_{Z_l}})\}$ is a frame at Alice's side. In fact, it corresponds to the frame f_5, one of the 16 possible 2×2 frames (for the complete list of frames, please see [27]). We commonly represent the frames in the form of a matrix, with the purpose of facilitating the visualization of the sifting bits (SSs) or the measurement results (MRs). However, when it comes to discussing the reconciliation methods, we used the notation introduced here. For a useful reference, consider that $f_1 = \{(\mathbf{0_X}^{0_{X_i}}, \mathbf{1_Z}^{1_{Z_l}}), (\mathbf{1_X}^{1_{X_k}}, \mathbf{0_Z}^{0_{Z_j}})\}$ because f_1 and f_5 are symmetrically equivalent.

— $\{(\mathbf{1_X}^{\epsilon_{k1},\epsilon_{k2}}, -), (-, \mathbf{1_Z}^{\pi_{l1},\pi_{l2}})\}$ is a frame at Bob's side (also referred to as an instance) denoting two double-matching detection events, where $[\epsilon_{k1}, \epsilon_{k2}]$ and $[\pi_{l1}, \pi_{l2}]$ are the corresponding sequential numerical indices of such events. Provided this frame comes from Alice's f_5, it implies that $1_{X_k} = \epsilon_{k1}$, $0_{Z_j} = \epsilon_{k2}$, $0_{X_i} = \pi_{l1}$, and $1_{Z_l} = \pi_{l2}$. From the numerical labels, we could establish that Alice sends $[1_{X_k}, 0_{Z_j}]$; Bob measures them as $[\epsilon_{k1}, \epsilon_{k2}]$; then, during reconciliation, Alice represents them as $[1_{X_k}, *]$. The last expression makes sense, because as we will see later, our algorithms focus on bits equal to one.

2.2. The Sifting String

The sifting string (SS) is a bit string prepared by Bob consisting of the sifting bits and the correction bits. In the absence of errors in the quantum channel, the sifting bits are enough to derive the secret key. However, when the channel or the optical detection system produces errors, then the correction bits are required to derive an identical key on both sides of the communication link.

To derive the sifting string (SS), the XOR logical function $\oplus$ between the bits of the columns of Bob's frame must be computed, where the symbol $-$ represents the vacuum state and is computed as a zero bit. The different bit configurations within Bob's frames are shown below: above each frame, we write the bits corresponding to the measurement result (MR), and at the bottom of each frame is the sifting bits, where $||$ denotes concatenation.

00	01	10	11

$$\begin{pmatrix} b_{11} & - \\ b_{21} & - \end{pmatrix}, \quad \begin{pmatrix} - & b_{12} \\ - & b_{22} \end{pmatrix}, \quad \begin{pmatrix} b_{11} & - \\ - & b_{22} \end{pmatrix}, \quad \begin{pmatrix} - & b_{12} \\ b_{21} & - \end{pmatrix}$$

$$b_{11} \oplus b_{21} \,||\, 0 \qquad 0 \,||\, b_{12} \oplus b_{22} \qquad b_{11} b_{22} \qquad b_{21} b_{12}$$

To perform error detection and depending on the approach used, some bits must be added: the measured bits or the conjugate bits:

— Measured bits: The bits detected at Bob's optical station must be appended, so SS= sifting bits || measured bits. It should be noted that the secret bits are derived from the geometric arrangement (MR) of the bits within Bob's frame, rather than the bits themselves obtained from the detection bases.
— Conjugate bits: The inverted bits of the measured bits are added, so SS= sifting bits || conjugate bits. The purpose of the conjugate bits is to detect errors where $\mathbf{1_X}$ is detected as $\mathbf{0_X}$ or $\mathbf{1_Z}$ as $\mathbf{0_Z}$, which cannot be detected using the measured bits.
— XOR bits: This will be detailed in this work and does not require additional bits.

2.3. Problem Statement

The bits that go into the secret key are derived from the double-matching detection events. The rate of such events has a squared decay with respect to the photon mean of the source quantum states. Furthermore, there are inherent challenges in the optical detection of two consecutive quantum states. Due to the above, we proposed in previous works that the states should not be transmitted consecutively from Alice to Bob, but interleaved between the states of other pairs. Therefore, we suggested a fixed window time between the two non-orthogonal states.

We established the research problem by questioning whether it will be possible to develop a QKD reconciliation algorithm using only the sifting bits, which is the minimum, string since it is built only with the sifting bits. We claim that the answer is affirmative, so in the new scheme we are proposing here, Alice sends a collection of quantum states defined as $\mathbf{S_a} = \bigcup_{i=1}^{a} \mathbf{0_X}^{0_{X_i}}, \bigcup_{j=1}^{b} \mathbf{0_Z}^{0_{Z_j}}, \bigcup_{k=1}^{c} \mathbf{1_X}^{1_{X_k}}, \bigcup_{l=1}^{d} \mathbf{1_Z}^{1_{Z_l}}$ in any order, with no predefined conditions or restrictions, except to send a similar amount of each of the four types of quantum states, in order to obtain a uniform distribution between them, so $a \sim b \sim c \sim d$. At the other side, Bob obtains a distribution of measurements that can be specified as $\mathbf{S_b} = \bigcup_{i=1}^{a'} \mathbf{0_X}^{\varepsilon_i}, \bigcup_{j=1}^{b'} \mathbf{0_Z}^{\omega_j}, \bigcup_{k=1}^{c'} \mathbf{1_X}^{\epsilon_k}, \bigcup_{l=1}^{d'} \mathbf{1_Z}^{\pi_l}$. Due to losses in the quantum channel $a > a'$, $b > b'$, $c > c'$, $d > d'$, it is still lossless and error free $a \neq a'$, $b \neq b'$, $c \neq c'$, and $d \neq d'$ because the results of Bob's quantum measurements depend on the quantum basis he chooses to use, which is performed actively.

Now, Bob groups the results $\mathbf{1_X}$ into pairs; similarly, he groups the results $\mathbf{1_Z}$ into pairs; symbolically, this is written as $\bigcup_{k=1}^{r} \left(-, \mathbf{1_X}^{\epsilon_{k1}, \epsilon_{k2}}\right), \bigcup_{l=1}^{s} \left(-, \mathbf{1_Z}^{\pi_{l1}, \pi_{l2}}\right)$ provided there are r pairs of $\mathbf{1_X}$ and s pairs of $\mathbf{1_Z}$. After Bob sends the necessary information to Alice and she identifies the errors in the transmitted states, they repeat the process with the remaining events, but changing $\left(\mathbf{0_X}^{\varepsilon_{i1}, \varepsilon_{i2}}, -\right)$ and $\left(-, \mathbf{0_Z}^{\omega_{j1}, \omega_{j2}}\right)$ to $\left(\mathbf{1_X}^{\epsilon_{k1}, \epsilon_{k2}}, -\right)$ and $\left(-, \mathbf{1_Z}^{\pi_{l1}, \pi_{l2}}\right)$, respectively. The protocol will be described in detail in Section 3. It is worth mentioning that, in frame-based error correction schemes, Alice identifies the errors produced during the transmission, and she adapts herself to what Bob received; that is why this constitutes a reverse reconciliation scheme [24,25].

As shown in Figure 3, there are ten types of sifting strings SS_i, so $i = 1 \ldots 10$, which are computed at Bob's side taking two double-matching detection events as their input. Table 1 shows the resulting sifting string (SS) for each frame-based reconciliation scheme: XOR bits, conjugate bits [27], and measured bits [18,26].

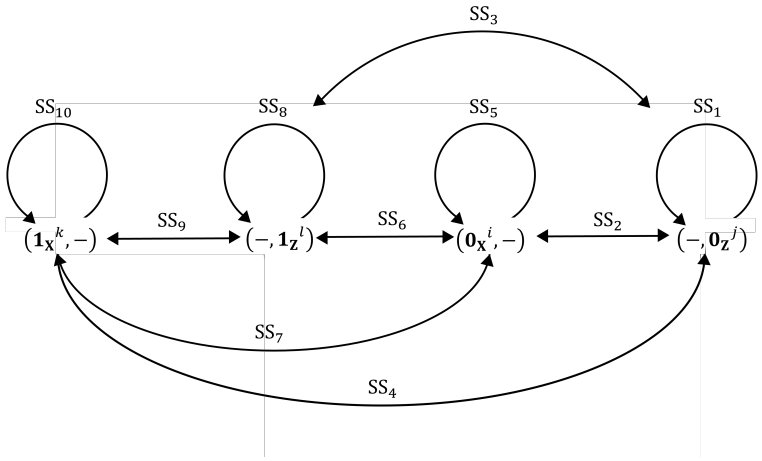

Figure 3. The diagram shows the sifting strings (SSs) for the different instances at Bob's side, which are represented as SS_i labels with $i = 1 \ldots 10$. The resulting labels depend on the specific approach that is used, and they are shown in Table 1.

Table 1. The list shows the sifting string (SS) for each frame-based reconciliation method. As previously indicated, the first two bits of the SS are the sifting bits, while the last two bits are the correction bits: measured or conjugated. Measured bits can produce different SSs depending on the ordering position of the double-matching detection events taken, as can be seen below when $i = 3, 4, 6, 7$.

$\mathbf{SS}_i$	XOR	Conjugate	Measured
SS_1	00	0000	0000
SS_2	00	0011	0000
SS_3	01	0101	0110, 0101
SS_4	10	1001	1010, 1001
SS_5	00	0000	0000
SS_6	01	0110	0110, 0101
SS_7	10	1010	1010, 1001
SS_8	00	0000	0011
SS_9	11	1100	1111
SS_{10}	00	0000	0011

The reconciliation information (SS) that Bob publicly shares with Alice remains in the hands of the spy Eve, so in the following subsections, we analyze whether, given the information in Eve's possession, she is capable of breaking the secret of the frames, that is if she can derive the MR of each frame. Then, in the next section, we describe in detail the new reconciliation method based on the XOR function and provide a description of its security. Finally, in the Conclusions, we compare the results obtained. In advance, we can claim that the new method is safe and more efficient than the previous ones.

2.4. Security of the Measured-Bit Approach

By using measured bits as correction bits, there are seven types of SSs that Bob can send to Alice (see Table 2). Item 7 of the list shows that Eve knows that, behind $SS_9 = 1111$ instances, there is an event $(\mathbf{1_X}^t, -)$ or $(-, \mathbf{1_Z}^t)$ in one of her rows. However, Items 2, 3, 4, and 5 of Table 2 show that this information does not allow Eve to infer the location of $\mathbf{0_X}^i$ or $\mathbf{0_Z}^j$ in the other row of the frame because it appears to both sides (left/right) under the same SS.

From the above analysis, we can conclude that the measured bits approach remains secure against this eavesdropping strategy. In our previous work [27], we derived a total secret gain reaching $\binom{n}{2}\left(\frac{2}{16} - \frac{1}{12}e'\right)$ taking the gain of the frame classes f_2, f_3, f_4, and f_6, where e' is the error rate of the frames computed as the number of erroneous frames over the amount of total frames at Bob's side. However, by taking the error rate e of the quantum

channel, then the probability of two errors in a frame is e^2, then we obtain a gain that amounts to $\binom{n}{2}\left(\frac{2}{16}-\frac{1}{16}e\right)$. Moreover, in the Appendix, we show that is possible to enhance such gain adding the frames f_i, where $i = 1,2,5,9,10,13,14,15,16$, thus increasing the secret gain up to $\binom{n}{2}\left(\frac{1}{16}+\frac{1}{16}e^2\right)$.

Table 2. Security test of the measured bits approach. Suppose Eve intercepts instances where $SS_9 = 1111$, but she knows that they are composed by the events $(\mathbf{1_X}^t, -)$ and $(-, \mathbf{1_Z}^t)$. The cases presented below show that, although Eve is provided with this information, she cannot identify other outcomes. For example, Case 2 demonstrates that Eve cannot differentiate between $(\mathbf{0_X}^i, -)$ and $(-, \mathbf{0_Z}^j)$ since they both produce the same $SS_{4,7} = 1001$, so this eavesdropping strategy becomes useless for Eve.

#	SS_i	i	Bob's Instances
1	0000	1,2,5	$\{(\mathbf{0_X}^t, -), (\mathbf{0_X}^i, -)\}, \{(\mathbf{0_X}^t, -), (-, \mathbf{0_Z}^j)\}$ $\{(-, \mathbf{0_Z}^t), (\mathbf{0_X}^i, -)\}, \{(-, \mathbf{0_Z}^t), (-, \mathbf{0_Z}^j)\}$
2	1001	4,7	$\{(\mathbf{0_X}^i, -), (\mathbf{1_X}^t, -)\}, \{(-, \mathbf{0_Z}^j), (\mathbf{1_X}^t, -)\}$
3	0101	3,6	$\{(\mathbf{0_X}^i, -), (-, \mathbf{1_Z}^t)\}, \{(-, \mathbf{0_Z}^j), (-, \mathbf{1_Z}^t)\}$
4	1010	4,7	$\{(\mathbf{1_X}^t, -), (\mathbf{0_X}^i, -)\}, \{(\mathbf{1_X}^t, -), (-, \mathbf{0_Z}^j)\}$
5	0110	3,6	$\{(-, \mathbf{1_Z}^t), (\mathbf{0_X}^i, -)\}, \{(-, \mathbf{1_Z}^t), (-, \mathbf{0_Z}^j)\}$
6	0011	8,10	$\{(\mathbf{1_X}^t, -), (\mathbf{1_X}^k, -)\}, \{(-, \mathbf{1_Z}^t), (-, \mathbf{1_Z}^l)\}$
7	1111	9	$\{(\mathbf{1_X}^t, -), (-, \mathbf{1_Z}^l)\}, \{(-, \mathbf{1_Z}^t), (\mathbf{1_X}^k, -)\}$

2.5. Security of the Conjugate Bit Approach

By using conjugate bits as correction bits, there are seven types of SS that Bob can send to Alice (see Table 3). Item 7 of this list shows that Eve knows that, behind $SS_9 = 1100$ instances, there is an event $(\mathbf{1_X}^t, -)$ or $(-, \mathbf{1_Z}^t)$ in one of her rows. Unfortunately, Items 2, 3, 4, and 5 of Table 3 show that this fact allows Eve to infer the location of $\mathbf{0_X}^i$ or $\mathbf{0_Z}^j$ in the other row of the frame because it appears at the same side (left/right) under the same SS.

Table 3. Security test of the conjugate bits approach. Suppose Eve intercepts instances where $SS_9 = 1100$, but she knows that they are composed by the events $(\mathbf{1_X}^t, -)$ and $(-, \mathbf{1_Z}^t)$. Using conjugated bits, such events allow Eve to identify other outcomes. Case $SS_7 = 1010$ (a) and case $SS_6 = 0110$ (a) show that $(\mathbf{0_X}^i, -)$ can be located. Case $SS_3 = 0101$ (a) and case $SS_4 = 1001$ (a) show that $(-, \mathbf{0_Z}^j)$ can be located. Case $SS_7 = 1010$ (b) and case $SS_4 = 1001$ (b) show that $(\mathbf{1_X}^k, -)$ can be located. Case $SS_6 = 0110$ (b) and case $SS_3 = 0101$ (b) show that $(-, \mathbf{1_Z}^l)$ can be located.

#	SS_i	i	Case	Bob's Instances
1	0000	1,5,8,10	(a)	$\{(\mathbf{0_X}^i, -), (\mathbf{0_X}^t, -)\}, \{(-, \mathbf{0_Z}^j), (-, \mathbf{0_Z}^t)\}$
			(b)	$\{(\mathbf{1_X}^k, -), (\mathbf{1_X}^t, -)\}, \{(-, \mathbf{1_Z}^l), (-, \mathbf{1_Z}^t)\}$
2	1010	7	(a)	$\{(\mathbf{0_X}^i, -), (\mathbf{1_X}^t, -)\}$
			(b)	$\{(\mathbf{1_X}^k, -), (\mathbf{0_X}^t, -)\}$
3	0110	6	(a)	$\{(\mathbf{0_X}^i, -), (-, \mathbf{1_Z}^t)\}$
			(b)	$\{(-, \mathbf{1_Z}^l), (\mathbf{0_X}^t, -)\}$
4	0101	3	(a)	$\{(-, \mathbf{0_Z}^j), (-, \mathbf{1_Z}^t)\}$
			(b)	$\{(-, \mathbf{1_Z}^l), (-, \mathbf{0_Z}^t)\}$
5	1001	4	(a)	$\{(-, \mathbf{0_Z}^j), (\mathbf{1_X}^t, -)\}$
			(b)	$\{(\mathbf{1_X}^k, -), (-, \mathbf{0_Z}^t)\}$
6	0011	2	(a)	$\{(-, \mathbf{0_Z}^j), (\mathbf{0_X}^t, -)\}, \{(\mathbf{0_X}^i, -), (-, \mathbf{0_Z}^t)\}$
7	1100	9	(a)	$\{(\mathbf{1_X}^k, -), (-, \mathbf{1_Z}^t)\}, \{(-, \mathbf{1_Z}^l), (\mathbf{1_X}^t, -)\}$

Given the results obtained in the previous analysis, we must state that this conjugated bits approach cannot be considered secure as a reconciliation method.

3. Frame Reconciliation with XOR Bits

In this section, we provide a detailed explanation of the new reconciliation method that uses only the sifting bits without the need for the correction bits. For a more fluent explanation, we present first the general method (see Figure 4), which includes the quantum transmission stage and the distillation process by means of the classical channel, leaving separately the additional algorithms that are required for error detection.

3.1. General QKD Protocol

The main idea behind this protocol is to first take advantage of the fact that the MRs behind SS = 11 are well hidden (see Section 3.5). Second, within those frames, it is possible to synthesize an algorithm for error identification by testing the combinations of events that should produce SS = 00 (see Test T.1). Third, there are fewer errors in f_1 frames because it takes two errors in a frame f_1 to produce an erroneous SS = 11; in fact, the error rate for them reduces to e^2 (see Section 3.3). This becomes relevant to evaluate what establishes the majority of the results computed in Algorithm A.2.

In this protocol, it is assumed that the optical stations of Alice and Bob are synchronized and that they have a quantum channel (air or fiber optic), and they also use a classical communication channel.

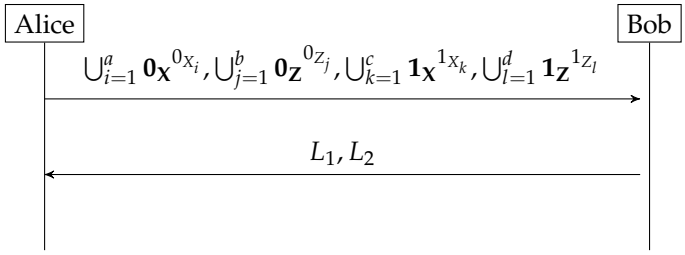

Figure 4. General QKD protocol based on XOR bits. The final step is for Alice and Bob to confirm that they have both set the same secret key because Alice sends the hash code of the distilled key to Bob and obtains a positive confirmation from him.

1. Alice sends the collection of quantum states $\bigcup_{i=1}^{a} \mathbf{0_X}^{0_{X_i}}, \bigcup_{j=1}^{b} \mathbf{0_Z}^{0_{Z_j}}, \bigcup_{k=1}^{c} \mathbf{1_X}^{1_{X_k}}, \bigcup_{l=1}^{d} \mathbf{1_Z}^{1_{Z_l}}$ to Bob, where the bold symbols $\mathbf{0_X}, \mathbf{0_Z}, \mathbf{1_X}, \mathbf{1_Z}$ denote the quantum states, while $0_{X_i}, 0_{Z_j}$, $1_{X_k}, 1_{Z_l}$ are Alice's sequential numerical indices of the transmitted quantum states, whose record is kept at her side. Of course, due to the noise and losses of the quantum channel, of the states sent, not all the states arrive at Bob's station and not all the ones that arrive are free of error.
2. Bob measures each received state applying randomly the quantum basis **X** or **Z**. Bob obtains the distribution $\bigcup_{i=1}^{a'} \mathbf{0_X}^{\varepsilon_i}, \bigcup_{j=1}^{b'} \mathbf{0_Z}^{\omega_j}, \bigcup_{k=1}^{c'} \mathbf{1_X}^{\epsilon_k}, \bigcup_{l=1}^{d'} \mathbf{1_Z}^{\pi_l}$, where $\varepsilon_i, \omega_j, \epsilon_k, \pi_l$ are the sequential numerical indices of the quantum measurements at Bob's side. We write $[\epsilon_{k1}, \epsilon_{k2}]$ to denote Bob's sequential numerical indices of two states measured by him with the **X** basis in which both measurements yield $\mathbf{1_X}$, then we represent it symbolically as the event $[\epsilon_{k1}, \epsilon_{k2}] \rightarrow \left(\mathbf{1_X}^{\epsilon_{k1}, \epsilon_{k2}}, -\right)$, where $k = 1 \ldots r$. In addition, we define the event of two quantum **Z** measurements that produces $\mathbf{1_Z}$ as $[\pi_{l1}, \pi_{l2}] \rightarrow \left(-, \mathbf{1_Z}^{\pi_{l1}, \pi_{l2}}\right)$, where $[\pi_{l1}, \pi_{l2}]$ are the sequential numerical indices of the two measurements and $l = 1 \ldots s$.
   A double-matching detection event as described before can be generated from a pair of non-orthogonal states, a pair of parallel states, or as a result of one or two errors in the channel and/or optical detection system. Furthermore, the double-matching detection events are chosen after performing the measurements, that is a posteriori, so the rate of those events is linear and not quadratic, as was the case in our previous works. As a result, there is no fixed time window separating the two quantum states. For the purposes of this protocol and the identification of the errors produced, the origin of those events is not relevant. Now, going back to the algorithm, Bob sends two lists L_1 and L_2 to Alice, which can be specified as follows:

$$L_1 = \bigcup_{k=1,l=1}^{k=r,l=s} \{[\epsilon_{k1}, \epsilon_{k2}], [\pi_{l1}, \pi_{l2}]\},$$
$$L_2 = \bigcup_{k=1,k'>k}^{k,k'=r} \{[\epsilon_{k1}, \epsilon_{k2}], [\epsilon_{k'1}, \epsilon_{k'2}]\}, \bigcup_{l=1,l'>l}^{l,l'=s} \{[\pi_{l1}, \pi_{l2}], [\pi_{l'1}, \pi_{l'2}]\}$$

The list L_1 allows two instances: (1) $\{[\epsilon_{k1}, \epsilon_{k2}], [\pi_{l1}, \pi_{l2}]\}$ or (2) $\{[\pi_{l1}, \pi_{l2}], [\epsilon_{k1}, \epsilon_{k2}]\}$. The instance is randomly chosen by Bob; see the example of Table 4. The specific instance (1) or (2) will determine the shared secret bit (see T.2 below). For this reason, an instance contains two specific pairs of events that cannot be applied more than once to an instance. L_2 is an auxiliary list that does not contribute secret bits, but contains auxiliary information that allows Alice to detect errors. The ordering between $\{[\epsilon_{k1}, \epsilon_{k2}], [\epsilon_{k'1}, \epsilon_{k'2}]\}$ and $\{[\pi_{l1}, \pi_{l2}], [\pi_{l'1}, \pi_{l'2}]\}$ in L_2 is randomly performed by Bob. As a result of the above description, L_1 contains the frames where SS = 11, while L_2 has those where SS = 00. The pairing process is performed on an even number of events, which may require the removal of an event. An example of these lists in the frame notation can be seen in Figure 5 and Table 4:

3. After Alice receives L_1 and L_2, she performs the following algorithms:

   A.1 to choose from L_1 the ones that belong to the frame class f_1 (or equivalently to f_5).
   A.2 to detect the errors in L_{1a}.
   A.3 to detect the remaining errors in L_1, which includes T.2, to determine the secret bits. Note that Bob obtains the secret bits by direct application of T.2.

4. Bob inverts the results of $(\mathbf{0_X}^{\varepsilon_{i1},\varepsilon_{i2}}, -)$ and $(-, \mathbf{0_Z}^{\omega_{j1},\omega_{j2}})$ to $(\mathbf{1_X}^{\epsilon_{k1},\epsilon_{k2}}, -)$ and $(-, \mathbf{1_Z}^{\pi_{l1},\pi_{l2}})$, respectively. Post-processing is then repeated: Step 2 (without quantum measurement) and Step 3.

$$L_1 = \begin{pmatrix} \mathbf{1_X}^{\epsilon_{11},\epsilon_{12}} & - \\ - & \mathbf{1_Z}^{\pi_{11},\pi_{12}} \end{pmatrix}, \begin{pmatrix} - & \mathbf{1_Z}^{\pi_{21},\pi_{22}} \\ \mathbf{1_X}^{\epsilon_{21},\epsilon_{22}} & - \end{pmatrix},$$
XOR bits: 1 1 1 1

$$L_2 = \begin{pmatrix} \mathbf{1_X}^{\epsilon_{11},\epsilon_{12}} & - \\ \mathbf{1_X}^{\epsilon_{21},\epsilon_{22}} & - \end{pmatrix}, \begin{pmatrix} - & \mathbf{1_Z}^{\pi_{11},\pi_{12}} \\ - & \mathbf{1_Z}^{\pi_{21},\pi_{22}} \end{pmatrix}$$
XOR bits: 0 0 0 0

Figure 5. An example of the labels contained in the lists $L_1 = \{[\epsilon_{11}, \epsilon_{12}], [\pi_{11}, \pi_{12}]\}, \{[\pi_{21}, \pi_{22}], [\epsilon_{21}, \epsilon_{22}]\}$ and $L_2 = \{[\epsilon_{11}, \epsilon_{12}], [\epsilon_{21}, \epsilon_{22}]\}, \{[\pi_{11}, \pi_{12}], [\pi_{21}, \pi_{22}]\}$. At the bottom of each frame, we have written the XOR bits.

Table 4. A portion of the quantum states (QS) sent by Alice is illustrated. At the receiving station, Bob randomly chooses the measurement basis **X** or **Z** to perform each measurement. Then, he groups the obtained results into randomly chosen pairs: $[\epsilon_{11}, \epsilon_{12}], [\epsilon_{21}, \epsilon_{22}], [\pi_{11}, \pi_{12}], [\pi_{21}, \pi_{22}]$. It should be noted that $\{[\epsilon_{11}, \epsilon_{12}], [\pi_{11}, \pi_{12}]\}$ is an f_5 frame, while $\{[\pi_{21}, \pi_{22}], [\epsilon_{21}, \epsilon_{22}]\}$ is an f_1 frame. Bob obtains the shared bits by the direct application of T.2, which in this example, produces $\{[\epsilon_{11}, \epsilon_{12}], [\pi_{11}, \pi_{12}]\} \to 1, \{[\pi_{21}, \pi_{22}], [\epsilon_{21}, \epsilon_{22}]\} \to 0$.

User	**Task**		**XOR Bit QKD Protocol**							
Alice	Time Slot	...	8	7	6	5	4	3	2	1
	QS		$\mathbf{0_X}$	$\mathbf{0_Z}$	$\mathbf{1_Z}$	$\mathbf{1_Z}$	$\mathbf{0_X}$	$\mathbf{0_Z}$	$\mathbf{1_X}$	$\mathbf{1_X}$
Bob	Basis		**Z**	**X**	**Z**	**Z**	**Z**	**X**	**X**	**X**
	Result	...	$\mathbf{1_Z}$	$\mathbf{1_X}$	$\mathbf{1_Z}$	$\mathbf{1_Z}$	$\mathbf{1_Z}$	$\mathbf{1_X}$	$\mathbf{1_X}$	$\mathbf{1_X}$
	Label		π_{22}	ϵ_{12}	π_{12}	π_{21}	π_{11}	ϵ_{22}	ϵ_{21}	ϵ_{11}

Of course, Step 4 can be performed within Step 2, but we prioritized the simplest explanation of the protocol. Using T.2, Alice and Bob derive the secret key bits from the MRs of all the frames that are built. Let us look at this more carefully in Section 3.2. The final task of the protocol would require a successful confirmation from Bob once Alice sends the hash code (from a secure cryptographic hash family, e.g., SHA-256) of the distilled key to ensure that both have established the same key.

At this point, we can highlight the following observation: in the previously published protocols (measured bits and conjugate bits), Alice defines the pairs of non-orthogonal quantum states a priori (using a time window between the non-orthogonal states). On the contrary, in the current scheme, it is Bob who determines, a posteriori, the pairs of states (by pairing the measurements that return a bit of 1), so a temporary separation between the states is not required, which implies that Alice chooses the quantum states to be sent randomly and without time separation constraints. On the other side, Bob measures, one by one, as they arrive, sequentially, the quantum states using a quantum basis that he chooses at random.

3.2. Auxiliary Algorithms

3.2.1. Algorithm A.1

For each element in L_1, identify the ones that belong to the frames f_1 (or equivalently to f_5):

1. If $\{[\pi_{l1}, \pi_{l2}], [\epsilon_{k1}, \epsilon_{k2}]\} == \{[0_{X_i}, 1_{Z_l}], [1_{X_k}, 0_{Z_j}]\}$, then it belongs to f_1; thus, write it in L_{1a}. Similarly, if $\{[\epsilon_{k1}, \epsilon_{k2}], [\pi_{l1}, \pi_{l2}]\} == \{[1_{X_k}, 0_{Z_j}], [0_{X_i}, 1_{Z_l}]\}$, then it belongs to f_5; thus, write it in L_{1a}. Additionally, store each $[\epsilon_{k1}, \epsilon_{k2}]$ as F_i in the list F and each $[\pi_{l1}, \pi_{l2}]$ as G_j in the list G.
2. Find which of the Cartesian elements $F_i \times F_j$, $F_i \times G_j$, and $G_i \times G_j$ are in L_1 or L_2, where $i \neq j$. The symbol $F_i \times G_j$ does not imply a specific ordering between the two sets, so it must be equally taken $G_j \times F_i$. Write the identified cases in the auxiliary list L_{2a}. Informally speaking, we can say that this list contains the results of the self-references $[\epsilon_{k1}, \epsilon_{k2}]$ and $[\pi_{l1}, \pi_{l2}]$, which will be useful in A.2.

We denote $\{[\epsilon_{k1}, \epsilon_{k2}], [\pi_{l1}, \pi_{l2}]\}$ as $\{[1_{X_k}, *], [*, 1_{Z_l}]\}$, where 1_{X_k} is the sequential numerical index that is in the **X** basis, and 1_{Z_l} is the sequential numerical index along the **Z** basis. The symbol $*$ represents the other sequential index, which we are not interested in focusing on. Conventionally, we write to the left-hand side the **X** basis numerical index, while the **Z** basis numerical index to the right-hind side. Furthermore, we refer to $\{[\pi_{l1}, \pi_{l2}], [\epsilon_{k1}, \epsilon_{k2}]\}$ as $\{[*, 1_{Z_l}], [1_{X_k}, *]\}$. To distinguish between two different 1_{X_k} events, we used the overdot symbol, so we write $1_{\dot{X}_k}$. For the same purpose, we write 1_{Z_l} and $1_{\dot{Z}_l}$.

3.2.2. Algorithm A.2

Let us write L_{1a} as $L_{1a} = \bigcup_{i=1}^{r'} \{[1_{X_k}, *], [*, 1_{Z_l}]\}_i$: 11. Take the instances $\{[1_{X_k}, *], [*, 1_{Z_l}]\}_i$ and $\{[*, 1_{Z_l}], [1_{X_k}, *]\}_j$. For $j = 1 \ldots r'$ and $i \neq j$, apply T_1 using L_{2a}. In the cases described below, the symbol $< i, j >$ denotes the evaluation of the instances sub-indexed as i, j under the rule T_1. The symbol $\uparrow$ means compliance with T_1, while the symbol $\downarrow$ is used to denote that it is not fulfilled. Finally, the symbol $| \, |$ denotes cardinality:

(a) $| < i, j >: \downarrow | \gg | < i, j >: \uparrow |$, then all i, j instances in $< i, j >: \uparrow$ are inverted; thus, correct them in L_{1a}.
(b) $| < i, j >: \downarrow | \ll | < i, j >: \uparrow |$, then all j instances in $< i, j >: \downarrow$ are inverted; thus, correct them in L_{1a}.

In simple words, what establishes Case (a) is that, if the majority says that you are wrong, while the minority says that you are right, in attention to the majority, you and the minority are wrong. Case (b) establishes that, if the majority says that you are right, while the minority says that you are wrong, in attention to the majority, then those who say that you are wrong are wrong.

3.2.3. Algorithm A.3

Let us write L_1 as $L_1 = \bigcup_{k=1,l=1}^{k=r,l=s} \{[\epsilon_{k1}, \epsilon_{k2}], [\pi_{l1}, \pi_{l2}]\}$:

1. From L_{1a}, choose a pivot, say $[1_{X_k}, *]$:
   - If $\{([1_{X_k}, *], [\epsilon_{k1}, \epsilon_{k2}]\} : 11$, then write $[*, 1_{Z_l}]$ for $[\epsilon_{k1}, \epsilon_{k2}]$ and $[1_{X_k}, *]$ for $[\pi_{l1}, \pi_{l2}]$.
   - If $\{([1_{X_k}, *], [\epsilon_{k1}, \epsilon_{k2}]\} : 00$, then write $[1_{X_k}, *]$ for $[\epsilon_{k1}, \epsilon_{k2}]$ and $[*, 1_{Z_l}]$ for $[\pi_{l1}, \pi_{l2}]$.
2. Use T.2 to determine the MR of all the elements of L_1.

3.2.4. Test T.1

There are four configurations for this rule, which are illustrated in Figure 6. The rule establishes the following implications:

(a) $\{[1_{X_k}, *], [*, 1_{Z_l}]\}, \{[1_{X_i}, *], [*, 1_{Z_j}]\} : 11$ implies $\{[1_{X_k}, *], [1_{X_i}, *]\}, \{[*, 1_{Z_l}], [*, 1_{Z_j}]\} : 00$ and $\{[1_{X_k}, *], [*, 1_{Z_j}]\}, \{[*, 1_{Z_l}], [1_{X_k}, *]\} : 11$.

(b) $\{[1_{X_k}, *], [*, 1_{Z_l}]\}, \{[*, 1_{Z_j}], [1_{X_i}, *]\} : 11$ implies $\{[1_{X_k}, *], [*, 1_{Z_j}]\}, \{[*, 1_{Z_l}], [1_{X_i}, *]\} : 11$ and $\{[1_{X_k}, *], [1_{X_i}, *]\}, \{[*, 1_{Z_l}], [*, 1_{Z_j}]\} : 00$.

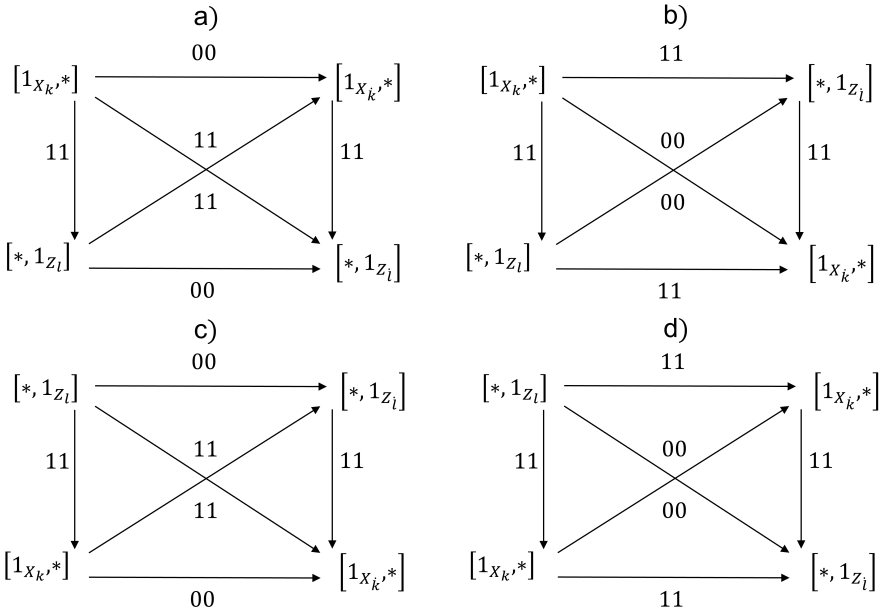

Figure 6. There are four configurations for T.1: the inputs are written in the left-hand corners (**top**, **bottom**), while the test cases appear in the right-hand corners. The implicit SSs are written above the arrows. The (**c**,**d**) configurations are just the reflection of the (**a**,**b**) ones, respectively.

3.2.5. Test T.2

The rule that is represented in Table 5 is used for the so-called measurement result (MR) code, according to which Alice and Bob derive the bits of the shared secret key.

Table 5. Secret bits are obtained as follows. Each frame contributes one bit to the secret key.

Frame	Alice	Bob	Secret Bit
f_1	$\{[*, 1_{Z_l}], [1_{X_k}, *]\}$	$\{[\pi_{l1}, \pi_{l2}], [\epsilon_{k1}, \epsilon_{k2}]\}$	0
f_5	$\{[1_{X_k}, *], [*, 1_{Z_l}]\}$	$\{[\epsilon_{k1}, \epsilon_{k2}], [\pi_{l1}, \pi_{l2}]\}$	1

3.3. The Error Probability in the Quantum Channel

In the general QKD algorithm of Section 3.1, we used $f_1 = \{(\mathbf{0_X}^{0_{X_i}}, \mathbf{1_Z}^{1_{Z_l}}), (\mathbf{1_X}^{1_{X_k}}, \mathbf{0_Z}^{0_{Z_j}})\}$ and $f_5 = \{(\mathbf{1_X}^{1_{X_k}}, \mathbf{0_Z}^{0_{Z_j}}), (\mathbf{0_X}^{0_{X_i}}, \mathbf{1_Z}^{1_{Z_l}})\}$, which produced MR = 11. Here are two possibilities about what happened: the error-free instance $f_1 = [*, 1_{Z_l}], [1_{X_k}, *]\}$ (or $f_5 = \{[1_{X_k}, *], [*, 1_{Z_l}]\}$,

respectively) was produced. The other explanation is that the erroneous instance $f_5 = \{[1_{X_k}, *], [*, 1_{Z_l}]\}$ instead of f_1 was produced (or $f_1 = \{[*, 1_{Z_l}], [1_{X_k}, *]\}$ instead of f_5, respectively). In the last case, two errors occurred. Let us see the f_1 case:

— $\mathbf{0_X}^{0_{X_i}}$ is erroneously detected as $\mathbf{1_X}^{1_{X_k}}$, while $\mathbf{1_Z}^{1_{Z_l}}$ is (error-free) measured as $\mathbf{1_Z}^{1_{Z_i}}$.
— $\mathbf{1_X}^{1_{X_k}}$ is (error-free) measured as $\mathbf{1_X}^{1_{X_k}}$, but $\mathbf{0_Z}^{0_{Z_j}}$ is erroneously detected as $\mathbf{1_Z}^{1_{Z_i}}$.

This is similar for f_5. However, what happens when the error probability in the quantum channel reaches values of 50% or more? When $e = 0.5$, the error rate in the frames f_1 is e^2, that is 0.25. In this case, there is an error-free majority, since most of the events are correct and the minority are incorrect. However, when $e = \frac{1}{\sqrt{2}} \sim 0.7$, then the number of correct instances grows to 50%, equaling the number of incorrect instances. In this situation, we cannot identify the errors in the frames f_1 and f_5. To overcome this drawback, the pair of frames (f_2, f_6) or the pair (f_3, f_4) can be used. We list such pairs:

— $f_2 = \{(\mathbf{1_X}^{1_{X_k}}, \mathbf{0_Z}^{0_{Z_j}}), (\mathbf{1_X}^{1_{X_k}}, \mathbf{1_Z}^{1_{Z_l}})\}$, $f_6 = \{(\mathbf{1_X}^{1_{X_k}}, \mathbf{1_Z}^{1_{Z_l}}), (\mathbf{1_X}^{1_{X_k}}, \mathbf{0_Z}^{0_{Z_j}})\}$.
— $f_3 = \{(\mathbf{0_Z}^{0_{Z_j}}, \mathbf{1_X}^{1_{X_k}}), (\mathbf{1_X}^{1_{X_k}}, \mathbf{1_Z}^{1_{Z_l}})\}$, $f_4 = \{(\mathbf{1_X}^{1_{X_k}}, \mathbf{1_Z}^{1_{Z_l}}), (\mathbf{0_Z}^{0_{Z_j}}, \mathbf{1_X}^{1_{X_k}})\}$.

Because, in order to produce MR = 11, such frames require either no error or only one error that occurred when $\mathbf{0_Z}^{0_{Z_j}}$ is detected as $\mathbf{1_Z}^{1_{Z_i}}$, now, the error rate is e and not e^2, most of the cases are incorrect, and the fewest cases are correct, so the errors can be identified. Of course, for this to work, it is necessary to invert the majority rule A.2. Therefore, if during the execution of the reconciliation algorithm it is detected that there is no majority in the results, it must be changed to use the pair (f_2, f_6) instead of (f_1, f_5).

3.4. Privacy Amplification Performance

Assuming that the attacker Eve can somehow obtain the bits of some of the double-matching detection events, then the rate of such information will be reduced when Alice and Bob proceed to derive the bits of all the frames that can be constructed. In this context, we call this process privacy amplification.

If Alice and Bob derive the secret bits from the double-execution of Step 3 of the general QKD algorithm, with say m and n instances (or frames), respectively, they obtain $\binom{m}{2} + \binom{n}{2} = \frac{m^2+n^2-m-n}{2}$ bits. However, they can increase the number of secret bits by combining the instances of those rounds.

Let $[\alpha_1^s, \omega_1^s] = [1_{X_k}, *]^s \parallel [*, 1_{Z_l}]^s$, where $s = 0$ is related to the first round and $s = 1$ to the second round of Step 3 of the QKD protocol. Then, Alice and Bob perform the combinations indicated in the matrix below:

$$\begin{bmatrix} [\alpha_{11}^{01}, \omega_{11}^{01}] & [\alpha_{12}^{01}, \omega_{12}^{01}] & \dots & [\alpha_{1n}^{01}, \omega_{1n}^{01}] \\ [\alpha_{21}^{01}, \omega_{21}^{01}] & [\alpha_{22}^{01}, \omega_{22}^{01}] & \dots & [\alpha_{2n}^{01}, \omega_{2n}^{01}] \\ \vdots & & & \\ [\alpha_{m1}^{01}, \omega_{m1}^{01}] & [\alpha_{m2}^{01}, \omega_{m2}^{01}] & \dots & [\alpha_{mn}^{01}, \omega_{mn}^{01}] \end{bmatrix}$$

As a result, the number of bits is increased until reaching $\binom{m+n}{2} = \frac{(m+n)(m+n-1)}{2}$. However, $\binom{m+n}{2} = \binom{m}{2} + \binom{n}{2} + mn$; thus, the added gain is mn.

Now, let us compute the size (in the number of events) of L_1 and L_2:

$$|L_1| = r \cdot s,$$
$$|L_2| = \binom{r}{2} + \binom{s}{2}$$

The size of the key is $|L_1|$, while the amount of information sent by Bob amounts to $|L_1| + |L_2|$, so the ratio between them is $\frac{|L_1|}{|L_1|+|L_2|} \sim 1 + \frac{1}{2}(\frac{r}{s} + \frac{s}{r}) = 2$ provided $r = s$ and neglecting the linear terms. Therefore, the amount of data transmitted over the classical channel tends to be twice the size of the secret key.

3.5. Security of the XOR Bit Approach

Contrary to the measured bit and the conjugate bit approaches, by using the XOR bit approach, there are only two types of SS that Bob sends to Alice: $SS_1 = 00$, which comes from the instances $\{(\mathbf{1_X}^k, -), (\mathbf{1_X}^k, -)\}, \{-, \mathbf{1_Z}^l), (-, \mathbf{1_Z}^l)\}$, and $SS_2 = 11$, which comes from $\{(\mathbf{1_X}^k, -), (-, \mathbf{1_Z}^l)\}, \{(-, \mathbf{1_Z}^l), (\mathbf{1_X}^k, -)\}$. Item 2 of Table 6 shows that Eve knows that, behind $SS_2 = 11$ instances, there is an event $(\mathbf{1_X}^t, -)$ or $(-, \mathbf{1_Z}^t)$ in one of her rows. However, Item 1 of Table 6 shows that this information does not allow Eve to infer the location of $\mathbf{1_X}^k$ or $\mathbf{1_Z}^l$ in the other row of the frame because it appears to both sides (left/right) under $SS_1 = 00$.

Table 6. Security test of the XOR bit approach. Suppose Eve intercepts instances where $SS_2 = 11$, but she knows that they are composed by the events $(\mathbf{1_X}^t, -)$ and $(-, \mathbf{1_Z}^t)$. Although Eve is provided with this information, she cannot differentiate between $(\mathbf{1_X}^k, -)$ and $(-, \mathbf{1_Z}^l)$, since they both produce the same $SS_1 = 00$; therefore, it does not reveal to Eve the MR of Bob.

#	SS	Bob's Instances
1	00	$\{(\mathbf{1_X}^k, -), (\mathbf{1_X}^t, -)\}, \{(-, \mathbf{1_Z}^l), (-, \mathbf{1_Z}^t)\}$
2	11	$\{(-, \mathbf{1_Z}^l), (\mathbf{1_X}^t, -)\}, \{(\mathbf{1_X}^k, -), (-, \mathbf{1_Z}^t)\}$

3.6. Strength of the System against Attacks

Let us discuss the strength of the protocol against PNS and IR attacks. For this, consider that, in addition to the quantum channel, Bob's optical detection system also produces errors when performing the measurements of the states sent by Alice. Security is based on two facts: (a) The key is distilled towards Bob's errors. (b) The bases with which Bob performs the measurements are not revealed, only the sifting bits:

1. The photon number splitting attack (PNS): Eve cannot obtain a copy of the key for two reasons:
   - Although Eve captures some of the photons contained in the multiphotonic pulses, nothing guarantees she can produce the required double-matching detection events.
   - Alice and Bob distill the key according to the errors produced in the channel and the optical detection system, but Eve is unable to reproduce the errors of Bob's detection system.
2. The intercept and resend attack (IR): Eve's behavior can be seen as noise in the quantum channel (measure/resend), which alters the quantum state of half of the states sent by Alice because Eve's basis is correct 50% of the time:
   - However, Alice and Bob obtain the key according to the final results obtained by Bob, which Eve cannot replicate. As long as the reconciliation process is confidential, Eve will not be able to derive the secret key.

One of the potentially most-relevant consequences of this strength is that it would allow the use of higher power quantum pulses and extend the total link distance of the QKD system.

3.7. Properties of the XOR Bit Approach

To close Section 3, in this subsection, we list the main advantages of the QKD distillation protocol based on XOR bits:

- It has no losses and exhibits 100% efficiency.
- It is immune to the error rate of the quantum channel; in other words, it is invariant with respect to the noise in the quantum channel.
- It requires just one data exchange between Alice and Bob through the classical channel.
- The secret key rate is $\frac{w^2-w}{2}$, where w is the number of double-matching detection events and amounts to half of the pulses received at Bob's station.

— Security against the photon number splitting attack (PNS) and intercept and resend (IR) attack is guaranteed.
— No bits of the shared (raw) key are revealed, just the sifting XOR bits.

It should be emphasized here that the secret rate scales up to the square of the number of pulses received by Bob (actually, half of them). In previous publications, the secret rate amounted to the square of the number of double-matching detection events, which decays quadratically with respect to the mean photon emission of the laser source.

4. Conclusions

We presented a new reverse reconciliation method for QKD systems that, at least theoretically, is immune to quantum channel errors, does not present losses at the time of key distillation, and therefore, has 100% efficiency. The analysis of the previous properties was achieved without high formal-theoretical resources, so it can be evaluated without difficulty. It only requires a single reconciliation data transfer by Bob over the classical channel, while the secret rate scales to the square of the number of pulses at the receiving station.

We analyzed the resistance of the method to PNS and IR attacks, but we will seek to demonstrate the resistance of the protocol to other attacks in future works; for now, we focused on the detailed description of the reconciliation algorithms.

On the other hand, after performing the security analysis of the frame-based reconciliation methods, we concluded that reconciliation by means of the XOR bits and the measured bits preserve security, while the conjugated bits can no longer be assumed as secure. Furthermore, as a result of this research, we found a way to enhance the secret gain of the method using the measured bits to a total value that depends on the square of the quantum channel error rate.

Funding: This research received no external funding.

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

Appendix A. Secret Gain with Measured Bits

In Tables A2–A9 of Appendix B, we derive the secret gain of frames with measured bits. Then, in Equation (A1), we sum up the gain of each frame where the subindex i denotes the frame class, so c_i refers to f_i. Here, e denotes the error rate of the quantum channel, while in Table A1, we refer to the error rate of frames as e'.

$$\begin{aligned} c_i &= \frac{1}{2}(1-e) + \frac{1}{2}e + \frac{1}{2}e^2 \text{ for } i = 1, 5, 15, 16 \\ c_j &= \frac{1}{2}e + e^2 \text{ for } j = 9, 10, 13, 14 \\ c_k &= (1-e) + \frac{1}{2}e \text{ for } k = 2, 3, 4, 6 \\ \sum_{i=1}^{16} c_i &= 1 + e^2, \text{ where } i \neq 7, 8, 11, 12 \\ g &= \frac{1}{16}\binom{n}{2}(1+e^2) \end{aligned} \tag{A1}$$

Table A1 shows a comparison of the secret gain computed applying the error rate of the frames e' and summing the gains c_i, where $i = 2, 3, 4, 6$, then summing those gains, but with the error rate of the quantum channel e, and finally, summing the gains when $i = 1, \ldots 16$, but $i \neq 7, 8, 11, 12$.

Table A1. We deduced the partial gain $g_p = \frac{1}{16}\binom{n}{2}c_i$, where $i = 2, 3, 4, 6$. The total gain is computed under the same formula $i = 1, \ldots 16$, but $i \neq 7, 8, 11, 12$.

g	g_p	[18]
$\binom{n}{2}\left(\frac{1}{16} + \frac{1}{16}e^2\right)$	$\binom{n}{2}\left(\frac{2}{16} - \frac{1}{16}e\right)$	$\binom{n}{2}\left(\frac{2}{16} - \frac{1}{12}e'\right)$

Appendix B. Secret Gain of the Frames

We derived the secret gain of all the frames where security is preserved. The results showed us that $c_1 = c_5 = c_{15} = c_{16} = \frac{1}{2}(1-e) + \frac{1}{2}e + \frac{1}{2}e^2$. Furthermore, we derived the gains $c_9 = c_{10} = c_{13} = c_{14} = \frac{1}{2}e + e^2$. In addition, $c_2 = c_6 = c_3 = c_4 = (1-e) + \frac{1}{2}e$.

Table A2. Secret gain of the frames $f_1 = \{(\mathbf{0_X}, \mathbf{1_Z}), (\mathbf{1_X}, \mathbf{0_Z})\}$ and $f_5 = \{(\mathbf{1_X}, \mathbf{0_Z}), (\mathbf{0_X}, \mathbf{1_Z})\}$, which are symmetrically equivalent, against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). Detectable cases {(MR, error), (MR', error')} are {(00-01),(01-10)} and {(10-11),(11-00)}. The secret gain is $\frac{1}{4}(1-e) + \frac{1}{4}e + \frac{1}{4}e^2$.

MR	**00**	**01**	**10**	**11**
00	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$
01	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$
10	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$
11	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$

Table A3. Secret gain of the frames $f_{15} = \{(\mathbf{0_X}, \mathbf{1_Z}), (\mathbf{0_X}, \mathbf{1_Z})\}$ and $f_{16} = \{(\mathbf{1_X}, \mathbf{0_Z}), (\mathbf{1_X}, \mathbf{0_Z})\}$, which are symmetrically equivalent, against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). Detectable cases {(MR, error), (MR', error')} are {(00-11),(01-00)} and {(10-01),(11-10)}. The secret gain is $\frac{1}{4}(1-e) + \frac{1}{4}e + \frac{1}{4}e^2$.

MR	**00**	**01**	**10**	**11**
00	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$
01	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$
10	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$
11	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$

Table A4. Secret gain of the frames $f_9 = \{(\mathbf{0_X}, \mathbf{1_Z}), (\mathbf{0_X}, \mathbf{0_Z})\}$ and $f_{10} = \{(\mathbf{1_X}, \mathbf{0_Z}), (\mathbf{0_X}, \mathbf{0_Z})\}$, which are symmetrically equivalent, against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). Detectable cases {(MR, error), (MR', error')} are {(00-11),(01-10)} and {(10-11),(11-10)}. The secret gain is $\frac{1}{2}e + \frac{1}{2}e^2$.

MR	**00**	**01**	**10**	**11**
00	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$
01	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$
10	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$
11	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$

Table A5. Secret gain of the frames $f_3 = \{(\mathbf{0_X}, \mathbf{1_Z}), (\mathbf{1_X}, \mathbf{1_Z})\}$ and $f_4 = \{(\mathbf{1_X}, \mathbf{1_Z}), (\mathbf{0_X}, \mathbf{1_Z})\}$, which are symmetrically equivalent, against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). Detectable cases {(MR, error), (MR', error')} are {(00-01),(01-00)} and {(10-01),(11-00)}. The secret gain is $\frac{1}{2}(1-e)+\frac{1}{2}e$.

MR	00	01	10	11
00	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$
01	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$
10	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$
11	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$

Table A6. Secret gain of the frames $f_2 = \{(\mathbf{1_X}, \mathbf{0_Z}), (\mathbf{1_X}, \mathbf{1_Z})\}$ and $f_6 = \{(\mathbf{1_X}, \mathbf{1_Z}), (\mathbf{1_X}, \mathbf{0_Z})\}$, which are symmetrically equivalent, against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). Detectable cases {(MR, error), (MR', error')} are {(00-00),(01-01)} and {(10-00),(11-01)}. The secret gain is $\frac{1}{2}(1-e)+\frac{1}{2}e$.

MR	00	01	10	11
00	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$
01	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$
10	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$
11	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$

Table A7. Secret gain of the frames $f_8 = \{(\mathbf{0_X}, \mathbf{0_Z}), (\mathbf{1_X}, \mathbf{1_Z})\}$ and $f_{12} = \{(\mathbf{1_X}, \mathbf{1_Z}), (\mathbf{0_X}, \mathbf{0_Z})\}$, which are symmetrically equivalent, against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). There are no detectable cases.

MR	00	01	10	11
00	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$
01	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$
10	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$
11	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$

Table A8. Secret gain of the frames $f_7 = \{(\mathbf{0_X}, \mathbf{0_Z}), (\mathbf{0_X}, \mathbf{0_Z})\}$ against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). There are no detectable cases.

MR	00	01	10	11
00	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$
01	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$
10	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$
11	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$

Table A9. Secret gain of the frames $f_{11} = \{(\mathbf{1_X}, \mathbf{1_Z}), (\mathbf{1_X}, \mathbf{1_Z})\}$ against the position error: 0 errors = 00, 1 error (first = 01/second bit = 10), 2 errors (both bits = 11). There are no detectable cases.

MR	00	01	10	11
00	$\{(\mathbf{1_X}, -), (\mathbf{1_X}, -)\} : 0011$	$\{(\mathbf{0_X}, -), (\mathbf{1_X}, -)\} : 1001$	$\{(\mathbf{1_X}, -), (\mathbf{0_X}, -)\} : 1010$	$\{(\mathbf{0_X}, -), (\mathbf{0_X}, -)\} : 0000$
01	$\{(-, \mathbf{1_Z}), (-, \mathbf{1_Z})\} : 0011$	$\{(-, \mathbf{0_Z}), (-, \mathbf{1_Z})\} : 0101$	$\{(-, \mathbf{1_Z}), (-, \mathbf{0_Z})\} : 0110$	$\{(-, \mathbf{0_Z}), (-, \mathbf{0_Z})\} : 0000$
10	$\{(\mathbf{1_X}, -), (-, \mathbf{1_Z})\} : 1111$	$\{(\mathbf{0_X}, -), (-, \mathbf{1_Z})\} : 0101$	$\{(\mathbf{1_X}, -), (-, \mathbf{0_Z})\} : 1010$	$\{(\mathbf{0_X}, -), (-, \mathbf{0_Z})\} : 0000$
11	$\{(-, \mathbf{1_Z}), (\mathbf{1_X}, -)\} : 1111$	$\{(-, \mathbf{0_Z}), (\mathbf{1_X}, -)\} : 1001$	$\{(-, \mathbf{1_Z}), (\mathbf{0_X}, -)\} : 0110$	$\{(-, \mathbf{0_Z}), (\mathbf{0_X}, -)\} : 0000$

References

1. Alléaume, R.; Branciard, C.; Bouda, J.; Debuisschert, T.; Dianati, M.; Gisin, N.; Godfrey, M.; Grangier, P.; Länger, T.; Lütkenhaus, N.; et al. Using quantum key distribution for cryptographic purposes: A survey. *Theor. Comput. Sci.* **2014**, *560*, 62–81. [CrossRef]

2. Hong, K.W.; Foong, O.M.; Low, T.J. Challenges in quantum key distribution: A review. In Proceedings of the 4th International Conference on Information and Network Security, Kuala Lumpur, Malaysia, 28–31 December 2016; pp. 29–33.
3. Bacco, D.; Da Lio, B.; Cozzolino, D.; Da Ros, F.; Guo, X.; Ding, Y.; Sasaki, Y.; Aikawa, K.; Miki, S.; Terai, H.; et al. Boosting the secret key rate in a shared quantum and classical fibre communication system. *Commun. Phys.* **2019**, *2*, 140. [CrossRef]
4. Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Miller, C.; Moody, D.; Peralta, R.; et al. *Status Report on the Third Round of the Nist Post-Quantum Cryptography Standardization Process*; US Department of Commerce, NIST: Washington, DC, USA, 2022.
5. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
6. Yan, B.; Tan, Z.; Wei, S.; Jiang, H.; Wang, W.; Wang, H.; Luo, L.; Duan, Q.; Liu, Y.; Shi, W.; et al. Factoring integers with sublinear resources on a superconducting quantum processor. *arXiv* **2022**, arXiv:2212.12372.
7. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 1–12. [CrossRef]
8. Sasaki, T.; Yamamoto, Y.; Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **2014**, *509*, 475–478. [CrossRef] [PubMed]
9. Mehic, M.; Niemiec, M.; Siljak, H.; Voznak, M. Error Reconciliation in Quantum Key Distribution Protocols. In *Reversible Computation: Extending Horizons of Computing*; Springer International Publishing: Cham, Switzerland, 2020; pp. 222–236.
10. Mink, A.; Nakassis, A. LDPC error correction for Gbit/s QKD. In Proceedings of the Quantum Information and Computation XII, Baltimore, MD, USA, 5–9 May 2014; Volume 9123, pp. 19–31.
11. Yan, H.; Ren, T.; Peng, X.; Lin, X.; Jiang, W.; Liu, T.; Guo, H. Information reconciliation protocol in quantum key distribution system. In Proceedings of the 2008 Fourth International Conference on Natural Computation, Jinan, China, 18–20 October 2008; Volume 3, pp. 637–641.
12. Liu, S.; Van Tilborg, H.C.; Van Dijk, M. A practical protocol for advantage distillation and information reconciliation. *Des. Codes Cryptogr.* **2003**, *30*, 39–62. [CrossRef]
13. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
14. Brassard, G.; Salvail, L. Secret-key reconciliation by public discussion. In *Advances in Cryptology—EUROCRYPT'93, Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, 23–27 May 1993*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 410–423.
15. Buttler, W.T.; Lamoreaux, S.K.; Torgerson, J.R.; Nickel, G.; Donahue, C.; Peterson, C.G. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A* **2003**, *67*, 052303. [CrossRef]
16. Jouguet, P.; Kunz-Jacques, S. High performance error correction for quantum key distribution using polar codes. *arXiv* **2012**, arXiv:1204.5882.
17. Arikan, E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 3051–3073. [CrossRef]
18. Lizama-Perez, L.A.; López, J.M. Quantum key distillation using binary frames. *Symmetry* **2020**, *12*, 1053. [CrossRef]
19. Limei, G.; Qi, R.; Di, J.; Duan, H. Qkd iterative information reconciliation based on ldpc codes. *Int. J. Theor. Phys.* **2020**, *59*, 1717–1729. [CrossRef]
20. Johnson, J.S.; Grimaila, M.R.; Humphries, J.W.; Baumgartner, G.B. An analysis of error reconciliation protocols used in quantum key distribution systems. *J. Def. Model. Simul.* **2015**, *12*, 217–227. [CrossRef]
21. Gallager, R.G. Low-density parity-check codes. *Inf. Theory Ire Trans.* **1962**, *8*, 21–28. [CrossRef]
22. Mink, A.; Nakassis, A. LDPC for QKD reconciliation. *arXiv* **2012**, arXiv:1205.4977.
23. Johnson, J.S. An Analysis of Error Reconciliation Protocols for Use in Quantum Key Distribution. Master's Thesis, Air Force Institute of Technology, Montgomery County, OH, USA, 2012.
24. Grosshans, F.; Grangier, P. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv* **2002**, arXiv:0204127.
25. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef] [PubMed]
26. Lizama-Pérez, L.A.; López R., J.M.; Samperio, E.H. Beyond the limits of Shannon's information in quantum key distribution. *Entropy* **2021**, *23*, 229. [CrossRef] [PubMed]
27. Lizama-Pérez, L.A.; López-Romero, J.M. Perfect Reconciliation in Quantum Key Distribution with Order-Two Frames. *Symmetry* **2021**, *13*, 1672. [CrossRef]
28. Bennett, C.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computer System and Signal Processing, Bangalore, India, 10–19 December 1984.