


Article

Beyond the Limits of Shannon's Information in Quantum Key Distribution

Luis Adrián Lizama-Pérez ^{1,*} , J. Mauricio López R. ² and Emmanuel H. Samperio ¹

¹ Dirección de Investigación, Innovación y Posgrado, Universidad Politécnica de Pachuca, Ex-Hacienda de Santa Bárbara, Zempoala, Hidalgo 43830, Mexico; esamperio593@micorreo.upp.edu.mx

² Cinvestav Querétaro, Libramiento Norponiente 2000, Real de Juriquilla, Santiago de Querétaro, Querétaro 76230, Mexico; jm.lopez@cinvestav.mx

* Correspondence: luislizama@upp.edu.mx

Abstract: We present a new post-processing method for Quantum Key Distribution (QKD) that raises cubically the secret key rate in the number of double matching detection events. In Shannon's communication model, information is prepared at Alice's side, and it is then intended to pass it over a noisy channel. In our approach, secret bits do not rely in Alice's transmitted quantum bits but in Bob's basis measurement choices. Therefore, measured bits are publicly revealed, while bases selections remain secret. Our method implements sifting, reconciliation, and amplification in a unique process, and it just requires a round iteration; no redundancy bits are sent, and there is no limit in the correctable error percentage. Moreover, this method can be implemented as a post-processing software into QKD technologies already in use.

Keywords: QKD; distillation; amplification; reconciliation



Citation: Lizama-Pérez, L.; López R., J.M.; Samperio, E.H. Beyond the Limits of Shannon's Information in Quantum Key Distribution. *Entropy* **2021**, *23*, 229. <https://doi.org/10.3390/e23020229>

Academic Editor: Ivan B. Djordjevic

Received: 18 December 2020

Accepted: 10 February 2021

Published: 16 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

To put it in historical context, fiber-optic telecommunications over long distances was not possible until manufacturing techniques that improved drastically its efficiency were developed. Fibers had been used to see inside the body, but they remained unusable for long-distance information transfer because too much light was lost along the way. However, in the 1960s, Charles Kao introduced a new disruptive approach based on pure glass fibers and laser technology with transcendent achievements [1].

In the quantum era, Quantum Key Distribution (QKD) is one of the most promising technologies to secure the information intended to cross data networks. However, the development of new techniques for the rapid establishment of secret key information using quantum pulses over long distances has become unpostponable [2–6].

Unfortunately, some factors prevent QKD of becoming a widely used technology as its inability to reach long-distances and produce large keys at high speed. The greatest weakness of QKD technology lies in its ability to gain useful information to establish a secret key despite the noise in the quantum channel [7,8]. On the one hand, noise provides the possibility for an attacker to disguise themselves, and, on the other hand, it imposes severe difficulties to correct errors produced during transmission in order to derive two identical cryptographic keys at both sides of the quantum link [9,10]. In the case of BB84 protocol, it has been estimated that a secure key can be distilled when the quantum bit error rate (QBER) is less than 11% [11].

In the few past years, we have developed a new scheme for QKD quantum called quantum flows [12–14] capable of resisting challenging attacks [15–25]. In quantum flows approach, Alice sends to Bob a pair of quantum states, parallel or non-orthogonal, which is chosen randomly. Bob measures the two quantum states with the same measurement basis, X or Z under active basis selection. If Bob obtains the same result, a single bit has been transmitted from Alice to Bob. Quantum flows have allowed us to formulate

a new method for QKD distillation based on binary structures called frames. Framed reconciliation integrates the regular QKD stages of sifting, reconciliation, and amplification in a unique process. This property makes our method unique in the context of QKD distillation; moreover, it accelerates convergence and produces a key that grows cubically in the number of double detection events.

In this work, we enhance the framed reconciliation method showed previously for 2×2 frames [14], and we discuss that framed reconciliation can surpass Shannon's information bounds for noisy channels. We strongly recommend that the reader consults our previous work on Quantum Key Distillation Using Binary Frames, so that we can keep the present article concise, as far as possible. Basic concepts comprise quantum flows, non-orthogonal quantum states, quantum photonic gains, binary frames, and matching results (MR). Having introduced 2×2 frames, which are the frames with the minimum size, we discuss here 3×2 frames. Throughout the article, we will compare both schemes.

2. Communication Model

Classical theory of communication, as it was established by Claude Shannon in 1948, defines a general communication system where Alice (the information source) prepares an information signal, that she sends over a noisy channel, but it corrupts at least in part due to the presence of noise in the channel [26,27]. At the other side, Bob receives this information signal, but Alice and Bob must implement a processing method to recover from the errors produced during transmission [28–32].

Shannon's theory imposes a limit to the highest transmission speed over a noisy channel because it can never surpass the channel capacity. The coding rate is computed as the number of message symbols divided by the number of transmitted signals. A higher coding rate means higher transmission speed. When the efficiency of the codes approximates to the channel capacity by increasing the number of transmitted signals, it is known that these codes approach to the Shannon limit. However, a coding rate too high makes it impossible to achieve a decoding error probability close to zero because the optimum channel capacity is achievable just by letting the number of transmitted signals reach infinity [33]. We claim our method goes beyond this limit because it does not require the number of transmitted signals to be increased. In fact, the coding rate reaches unity. The QKD protocol in Reference [34] exhibits a total efficiency of the communication to come up to 100%, but it does not define an error correction algorithm.

On the other side, if e is the probability that a transmitted 0 bit is received as a 1 and $1 - e$ is the probability to be received as a 0, Shannon theory implies that, in case that $e = 0.5$, one can never say anything about the original message [35,36] because the entropy is maximized when the two possible outcomes are equally probable. Since our method corrects errors when $e = 0.5$, we claim that it goes beyond the limits implied by Shannon's theory.

In our approach, we call active (or real) information that which is derived from Shannon's model viewpoint because information is first prepared by Alice, then transmitted through the (quantum) channel, and, finally, recovered by Bob after it has been measured and proven to be correct. Conversely, in our scheme, information is not enclosed in the transmitted quantum pulses but in the quantum bases (X or Z) that Bob chooses at the other side. In fact, measured bits are publicly announced but the measurement bases are never revealed. We designated reactive information to this communication paradigm that we introduced to the sifting QKD procedure.

Reactive bits are computed using Bob's measurement bases, so errors produced in the quantum channel are easily detected by Alice because such bits are publicly revealed by Bob. Remarkably, in the presence of the unit error rate, information can still be recovered since errors give reactive information by themselves. For the same reason, not all of Alice's information can be recovered, even in the absence of errors produced by the quantum channel.

Two reconciliation approaches have been conceived in QKD: direct and reverse reconciliation. In reverse reconciliation (RR), Alice must infer Bob's outcomes, rather than Bob guessing Alice's encodings, known as direct reconciliation (DR). Under this classification frame, reconciliation is RR, so let us briefly contrast our approach with RR which was introduced in the context of continuous variable QKD [31,37].

It has been demonstrated that RR reconciliation achieves longer distances even beyond the 3dB limit of previous CV-QKD works [38]. RR reconciliation has been implemented over LDPC basis [39], and it was shown that LDPC codes can reach within 0.0045 dB of the Shannon limit. Unfortunately, it requires large block lengths (10^7) [40]. Even more, decoding LDPC has larger computational and memory requirements than either Cascade or Winnow algorithms [41]. In contrast, our method does not require additional bits which reduces the coding rate. Our experimental simulations show complete efficiency in detecting/correcting errors. Moreover, the secret throughput grows cubically in the number of double detection events.

Before we introduce 3×2 frames, we will explain quantum communication based on frames through a simple example about our reconciliation method. To facilitate its exposition, we use 2×2 frames in this example. Then, to simplify exposition we discuss the role of auxiliary frames in the 2×2 case. In Section 3, we address the research methodology for 3×2 frames and then we detail the QKD distillation protocol. To make the discussion more effective, we have placed tables of 3×2 protocol in the Appendix A. Finally, in Section 4, we analyze the efficiency and the security of the 3×2 protocol against different attacks as the Intercept-Resend (IR) attack and the Photon Number Splitting (PNS) attack.

2.1. Quantum Communication

In the BB84 protocol [42–45], a quantum state $|i_X\rangle$ (or $|i_Z\rangle$), where i represents the encoded bit ($i = 0, 1$), is useful to be distilled whenever it has been measured in the proper (compatible) quantum basis, basis X for $|i_X\rangle$ (or Z for $|i_Z\rangle$). Otherwise, a non-compatible measurement is produced, the bit derived from this measurement is ambiguous, and it must be discarded. However, in the quantum flows scheme, ambiguous cases can still be used for the following reasons [14]:

- The states are grouped by non-orthogonal pairs ($|i_X\rangle, |i_Z\rangle$) or ($|i_X\rangle, |(i-1)_Z\rangle$), where $i = 0, 1$.
- A non-orthogonal pair is measured with the same quantum basis X or Z . Both measurements yield the same result half of the times, i.e., if measuring ($|i_X\rangle, |i_Z\rangle$) with X (or Z) gives i , or measuring ($|i_X\rangle, |(i-1)_Z\rangle$) with X (or Z) gives i or $1-i$, in both cases. We call those cases double matching detection event. Then, non-compatible measurements never occur.
- It implies that the bit encoded in the X or Z basis is transmitted from Alice to Bob. This communication model defines two communication channels, channel X and channel Z , because there are two bits enclosed in a non-orthogonal quantum pair: one bit over channel X and other bit in channel Z . Bob just chooses which channel he wants to use. Provided a double matching detection event is generated, both measurements are equally useful.

2.2. Example of Error Correction

In order to better introduce our communication model, let us illustrate it with a simple example to contrast it with Shannon's model. To see the effect of the errors instead of the losses in the channel, let us assume a conservative quantum channel. Table 1 shows an hypothetical QKD protocol possibly based on BB84, where Alice has sent 18 quantum states (in practical implementations, some sifted bits must be sacrificed to estimate the error rate of the channel). In this example, a 30% error rate (e) is produced; therefore, the QKD distillation process must be declined because prominent reconciliation algorithms, such as Cascade, Winnow, or LDPC, cannot work with this high error rate.

Table 1. In this example of a running Quantum Key Distribution (QKD), 6 errors (underlined at Bob’s column) among 18 measured quantum states are produced, so it gives an error rate of 30%. According to Shannon’s limit, it yields a transmission rate of 0.0817. It is known that, at 50%, there is no reconcilable information.

Alice	Bob
$ 0_X\rangle_2, 0_Z\rangle_1,$	$ 0_X\rangle_2, 0_Z\rangle_1,$
$ 1_X\rangle_4, 0_Z\rangle_3,$	$ 1_X\rangle_4, 1_Z\rangle_3,$
$ 1_X\rangle_6, 1_Z\rangle_5,$	$ 1_X\rangle_6, 1_Z\rangle_5,$
$ 0_X\rangle_8, 1_Z\rangle_7,$	<u>$1_X\rangle_8,$</u> $ 1_Z\rangle_7,$
$ 1_X\rangle_{10}, 0_Z\rangle_9,$	<u>$0_X\rangle_{10},$</u> $ 0_Z\rangle_9,$
$ 0_X\rangle_{12}, 1_Z\rangle_{11},$	<u>$0_X\rangle_{12},$</u> $ 0_Z\rangle_{11},$
$ 1_X\rangle_{14}, 1_Z\rangle_{13},$	$ 1_X\rangle_{14}, 1_Z\rangle_{13},$
$ 1_X\rangle_{16}, 0_Z\rangle_{15},$	<u>$0_X\rangle_{16},$</u> $ 0_Z\rangle_{15},$
$ 0_X\rangle_{18}, 1_Z\rangle_{17}$	<u>$1_X\rangle_{18},$</u> $ 1_Z\rangle_{17}$

Let us suppose that the same errors are produced using the framed reconciliation method as it is illustrated in Figure 1. In this example, we ignored the losses due to double detection events and the amplification gain produced by the amount of combinations between double matching detection events (we will discuss them later). The reconciliation based on frames can process this error rate; in fact, it can reconcile any error rate that e has in the channel, so there is no need to estimate e wasting bits for this purpose. To simplify the exposition, in this example, we used 2×2 frames, but we will discuss 3×2 frames in the Distillation Method section.

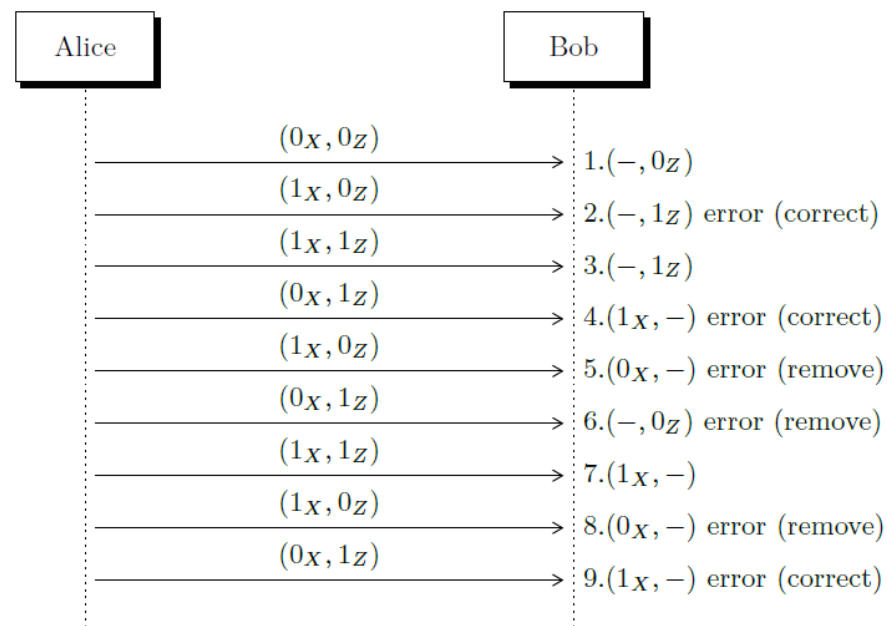


Figure 1. Using frame reconciliation, all errors are detected and corrected (or removed). Each double detection event has been enumerated to follow them into the frames (see Tables 2 and 3).

Table 2. Alice receives the Sifting String (SS) from Bob, which she knows belongs to $f_2, f_3,$ and $f_4,$ respectively, but they are ambiguous, so she uses the auxiliary frames $f_{10}, f_9,$ and $f_9,$ respectively, to identify the error and then correct it.

$f_2 \begin{matrix} \text{MR} = 01 \\ 2. \begin{pmatrix} - & 1_Z\rangle \\ 3. \begin{pmatrix} - & 1_Z\rangle \end{pmatrix} \\ \text{SS} = 00, 11 \end{matrix} \end{matrix}$	$f_{10} \begin{matrix} \text{MR} = 01 \\ 2. \begin{pmatrix} - & 1_Z\rangle \\ 1. \begin{pmatrix} - & 0_Z\rangle \end{pmatrix} \\ \text{SS} = 01, 10 \end{matrix} \end{matrix}$
$f_3 \begin{matrix} \text{MR} = 10 \\ 4. \begin{pmatrix} 1_X\rangle & - \\ 3. \begin{pmatrix} - & 1_Z\rangle \end{pmatrix} \\ \text{SS} = 11, 11 \end{matrix} \end{matrix}$	$f_9 \begin{matrix} \text{MR} = 10 \\ 4. \begin{pmatrix} 1_X\rangle & - \\ 1. \begin{pmatrix} - & 0_Z\rangle \end{pmatrix} \\ \text{SS} = 10, 10 \end{matrix} \end{matrix}$
$f_4 \begin{matrix} \text{MR} = 00 \\ 7. \begin{pmatrix} 1_X\rangle & - \\ 9. \begin{pmatrix} 1_X\rangle & - \end{pmatrix} \\ \text{SS} = 00, 11 \end{matrix} \end{matrix}$	$f_9 \begin{matrix} \text{MR} = 10 \\ 9. \begin{pmatrix} 1_X\rangle & - \\ 1. \begin{pmatrix} - & 0_Z\rangle \end{pmatrix} \\ \text{SS} = 10, 10 \end{matrix} \end{matrix}$

Table 3. After Alice receives these SS, she determines that the respective frames must be eliminated because ambiguity cannot be removed.

$f_2 \begin{matrix} \text{MR} = 10 \\ 5. \begin{pmatrix} 0_X\rangle & - \\ 3. \begin{pmatrix} - & 1_Z\rangle \end{pmatrix} \\ \text{SS} = 01, 01 \end{matrix} \end{matrix}$	$f_3 \begin{matrix} \text{MR} = 01 \\ 6. \begin{pmatrix} - & 0_Z\rangle \\ 3. \begin{pmatrix} - & 1_Z\rangle \end{pmatrix} \\ \text{SS} = 01, 01 \end{matrix} \end{matrix}$	$f_6 \begin{matrix} \text{MR} = 00 \\ 8. \begin{pmatrix} 0_X\rangle & - \\ 7. \begin{pmatrix} 1_X\rangle & - \end{pmatrix} \\ \text{SS} = 10, 01 \end{matrix} \end{matrix}$
---	---	---

2.3. Auxiliary Frames

A major component of the framed reconciliation method relies in the auxiliary frames. There are two types of auxiliary frames: zero frames and testing frames. Every quantum state of a zero frame is $|0_X\rangle$ or $|0_Z\rangle$. Identifying measurement errors in a zero frame is easy, as we will see later. A testing frame contains one row that is under evaluation because it presumably contains error, and the rest of the rows come from a zero verified frame.

To compute the sifting string (SS), we follow the next procedure: A sifting string is constructed concatenating the bits that result after the \oplus logical operation is applied to each column of the frame (a blank space is treated as a zero bit) and putting the measured bits that are produced by the optical detectors. The secret bits are derived from the code that is assigned to the arrangement of measurements inside the frame. We call measurement results (MR) to this arrangement. To see the role of auxiliary frames, let us assume that we intend to apply the framing algorithm to the Shannon’s model; thus, several zero bits are interleaved between the secret bits to be used as auxiliary correcting bits.

1. To achieve reconciliation in Shannon’s model, the first step is to ensure that auxiliary zero bits are error-free. However, Shannon’s 2×1 frames does not allow to identify errors in two consecutive zero bits (at least in one round iteration) as indicated by the following relations:

$$\begin{pmatrix} 0 \\ \oplus \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ \oplus \\ 1 \end{pmatrix} = 0 \text{ (SS)}.$$

In addition, when using 2×1 frames, there is a unique possible matching result (MR), that is written below; therefore, no secret information can be derived from MRs in Shannon’s model.

$$\begin{pmatrix} |\bullet\rangle \\ |\bullet\rangle \end{pmatrix}.$$

2. By contrast, using 2×2 frames, errors in the auxiliary frames can be easily identified. Here, we list the error-free zero frames:

$$\begin{pmatrix} |0_X\rangle & - \\ \oplus & \\ - & |0_Z\rangle \end{pmatrix} = \begin{pmatrix} - & |0_Z\rangle \\ \oplus & \\ |0_X\rangle & - \end{pmatrix} = \begin{pmatrix} |0_X\rangle & - \\ \oplus & \\ |0_X\rangle & - \end{pmatrix} = \begin{pmatrix} - & |0_Z\rangle \\ \oplus & \\ - & |0_Z\rangle \end{pmatrix} = 00,00 \text{ (SS)},$$

which can be compared, for illustrative purposes, to the erroneous cases:

$$\begin{pmatrix} |1_X\rangle & - \\ \oplus & \\ - & |1_Z\rangle \end{pmatrix} = \begin{pmatrix} - & |1_Z\rangle \\ \oplus & \\ |1_X\rangle & - \end{pmatrix} = 11,11 \text{ (SS)},$$

$$\begin{pmatrix} |1_X\rangle & - \\ \oplus & \\ |1_X\rangle & - \end{pmatrix} = \begin{pmatrix} - & |1_Z\rangle \\ \oplus & \\ - & |1_Z\rangle \end{pmatrix} = 00,11 \text{ (SS)}.$$

3. Ambiguous SS are produced in regular frames. For example, to the left, we indicate that Alice sends the frame f_2 to Bob, who measures it using $MR = 11$. However, when applying the Z measurement basis, the photo-detector yields an error reporting $|1_Z\rangle$ instead $|0_Z\rangle$; so, we have:

$$f_{2a} = \begin{pmatrix} |1_X\rangle & |0_Z\rangle \\ |1_X\rangle & |1_Z\rangle \end{pmatrix}, f_{2b} = \begin{pmatrix} - & |1_Z\rangle \\ \oplus & \\ |1_X\rangle & - \end{pmatrix} = 11,11 \text{ (SS)}.$$

When Alice receives the string $SS = 11,11$ which belongs to f_2 , she knows it implies two possibilities: either SS comes from the error-free string $SS_{24} = 11,11$ under $MR = 10$ in f_2 or an error is produced in the first measured bit that actually corresponds to the string $SS_{23} = 10,01$ under $MR = 11$ in f_2 . To disambiguate it, Alice uses the auxiliary frame f_{10} . Thus, she looks at a frame f_{10} where the ambiguous row $(-, |1_Z\rangle)$ is allocated. Remember that each row is combined with each other. Previously, the second row of f_{10} , i.e., $(|0_X\rangle, -)$, was verified as a zero frame. Then, suppose Alice finds the following f_{10} case:

$$f_{10} = \begin{pmatrix} - & |1_Z\rangle \\ \oplus & \\ |0_X\rangle & - \end{pmatrix} = 10,10.$$

The sifting string $10,10$ reveals that an error exists in the row that is under evaluation; therefore, Alice decides SS_{23} . Then, the pair (SS_{23}, f_2) determines Alice's secret bit. It must be highlighted that the sifting strings of auxiliary frames cannot be distinguished from other identical SS from regular frames, so privacy is guaranteed. In fact, it is ensured that each SS can proceed equally from each bit.

2.4. One-Time Pad XOR Equivalency

It is known that the XOR one-time pad encryption method is a perfect cryptosystem provided the crypto key achieves the same number of bits as the plaintext. Let us show that the framing method actually behaves as one-time encryption. First, in Table 4, we can see the logical XOR (\oplus) function. Each encrypted bit c could be produced by each key bit denoted as k .

Table 4. The logical XOR function.

c	$k \oplus b$
0	$0 \oplus 0$
	$1 \oplus 1$
1	$0 \oplus 1$
	$1 \oplus 0$

As specified in the framed reconciliation method [14], Bob must reveal the sifting bits along the measured bits. However, each SS maps two different MRs, as can be verified in Table 5. Since secret bits are enclosed in MRs, we proved that secret bits of the framing protocol are equivalent to the secret bits of the XOR one-time pad cryptosystem. The same analysis can be applied to the 3×2 frames.

Table 5. The XOR function for 2×2 frames; matching results (MR) is the measurement result, and sb denotes the final secret bit.

c	$k \oplus b$	MR	Frames	sb
00	$(0_X\rangle, -) \oplus (-, 0_Z\rangle)$	10	f_1	0
	$(-, 0_Z\rangle) \oplus (0_X\rangle, -)$	11	f_5	1
	$(1_X\rangle, -) \oplus (1_X\rangle, -)$	00	f_2, f_6	0
	$(-, 1_Z\rangle) \oplus (-, 1_Z\rangle)$	01	f_3, f_4	1
01	$(-, 1_Z\rangle) \oplus (-, 0_Z\rangle)$	01	f_1, f_6	0
	$(-, 1_Z\rangle) \oplus (0_X\rangle, -)$	11	f_4	1
	$(0_X\rangle, -) \oplus (-, 1_Z\rangle)$	10	f_3	0
	$(-, 0_Z\rangle) \oplus (-, 1_Z\rangle)$	01	f_2, f_5	1
10	$(1_X\rangle, -) \oplus (0_X\rangle, -)$	00	f_4, f_5	0
	$(1_X\rangle, -) \oplus (-, 0_Z\rangle)$	10	f_6	1
	$(0_X\rangle, -) \oplus (1_X\rangle, -)$	00	f_1, f_3	0
	$(-, 0_Z\rangle) \oplus (1_X\rangle, -)$	11	f_2	1
11	$(-, 1_Z\rangle) \oplus (1_X\rangle, -)$	11	f_1, f_3, f_6	0
	$(1_X\rangle, -) \oplus (-, 1_Z\rangle)$	10	f_2, f_4, f_5	1

3. Distillation Method with 3×2 Frames

Before we detail the steps of the distillation method for 3×2 frames, let us describe the research methodology we applied:

1. The 3×2 frames must be identified: there are $4^3 = 64$ binary 3×2 frames.
2. The measurement results (MR) must be specified: in 3×2 frames, there are 8 MR. Those MR are illustrated in Table A2 of Appendix A.
3. Frames are classified as usable and useless frames: a usable frame is a frame that produces a distinct SS under each MR. In 3×2 frames, there are 8 distinct SS per frame and 24 usable frames. Sifting bits are written in Table A4 of Appendix A. Remember that Sifting Strings (SS) are composed by the sifting bits and the measured bits: SS = 1st sifting bit || 2nd sifting bit || 3th sifting bit, 1st measured bit || 2nd measured bit || 3th measured bit. The 3th sifting bit is appended to achieve discrimination, and it can be considered as a parity sifting bit.
4. Auxiliary frames which are intended to catch errors produced in regular frames must be identified. In 3×2 frames, there are 3 auxiliary frames labeled as f_{25} , f_{26} , and f_{27} . The frame f_{25} is the zero frame and is used to verify the two (below) rows of the testing frames f_{26} and f_{27} . The upper row of f_{26} and f_{27} is the row that is being tested. In the end, Alice will include the auxiliary frames inside the set of frames that Bob must remove. Auxiliary frames are listed in Table A1 of Appendix A.
5. All usable frames under each MR must be expanded to analyze all possible errors through SS, from single to multiple errors. Then, ambiguous SS that can be corrected

under the auxiliary frames must be detected. In addition, all the SS that cannot be disambiguated must be identified and the corresponding frames must be removed. We show in Table A5 the cases that can be successfully disambiguated.

6. At Bob's side, each (SS, MR) pair defines a secret bit (sb). For Alice, the same secret bit results from the pair (SS, f_i) because she knows the frame that is behind each SS. It must be guaranteed that each SS can be produced equally by both bits. In addition, it must be ensured that each secret bit proceeds from the same number of frames, so that the bit probability of each SS is the same in order to reduce the eavesdropper's information gain (SS are publicly transmitted over the classical channel). This action may involve removing some extra SS. Alice sends to Bob the set of SS of all the frames that must be eliminated including auxiliary frames. Table A3 of Appendix A enlists SS, MR, frames, and sb.

Now, we can proceed to summarize the steps of the distillation method for 3×2 frames that comprises sifting, reconciliation, and privacy amplification. The overall steps of the process are indicated in Figure 2:

1. Alice sends some non-orthogonal quantum pairs either $(|i_X\rangle, |i_Z\rangle)$ or $(|i_X\rangle, |(1-i)_Z\rangle)$ where $i = 0, 1$. Although quantum non-orthogonal pairs can be mutually interleaved they are numbered, so each pair can be identified by Alice and Bob
2. Bob measures each quantum pair using the same measurement basis (X or Z) which is chosen randomly (under active basis measurement). Some double detection events are produced. Bob informs Alice the tag number of such quantum pairs.
3. Alice computes all usable frames including null frames and auxiliary frames. She communicates to Bob the frame arrangement information. We call this step privacy amplification.
4. Bob computes the Sifting String (SS) of each frame. He returns the set of Sifting Strings he obtained to Alice.
5. Alice analyzes the SS received from Bob:
 - She generates frames f_{25} to prepare the auxiliary frames.
 - Using auxiliary frames, Alice removes ambiguity. Alice gets the secret bits using the relation (SS, f_i) and Table A3 of Appendix A.
 - Alice informs Bob of the cases that must be eliminated (because they cannot be disambiguated).
6. Bob removes the frames identified by Alice to reach Alice's secret bit string. Bob's secret bits are derived from (SS, MR) and Table A3 of Appendix A.

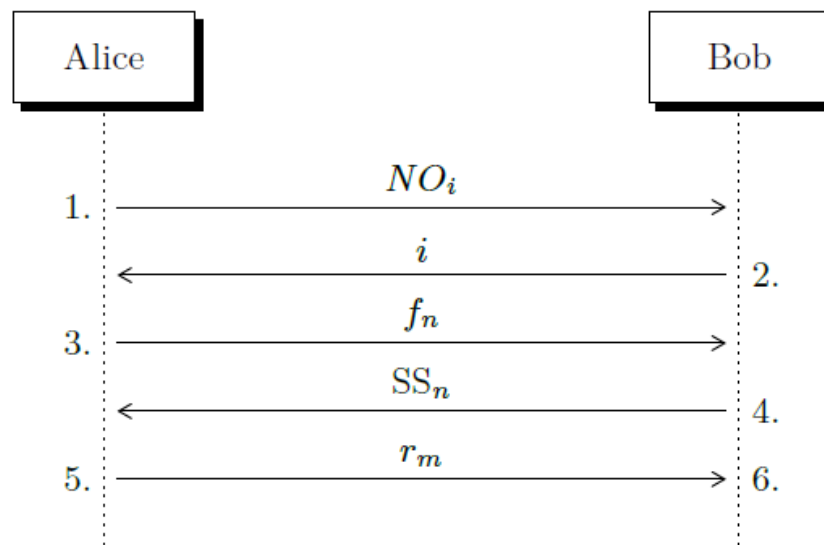


Figure 2. The frame distillation runs in one iteration: Alice sends pairs of non-orthogonal states (NO_i). Bob informs to Alice which cases produced double matching detection events (i). Alice generates all possible frames and sends to Bob the frame arrangement information (f_n). Bob returns back the sifting strings (SS_n). Finally, Alice tells Bob which cases he must delete (r_m). Step 1 is executed over the quantum channel, while steps 2 to 5 are completed using the classical channel.

4. Secret Rate

The secret rate of the framed reconciliation method can be derived directly from frames without recurring to quantum physics mathematical relations. First off, we must enlist the Sifting String (SS) generated by all the frames classified by Measurement Result (MR) and separate the error-free SS from the erroneous SS (single and multiple errors). According to the size of frames (2×2 or 3×2), the error could be in the first bit, second bit, third bit, two bits, two of three bits, and three bits simultaneously. Then, we proceed to identify ambiguous SS, (because they appear simultaneously as error-free SS and erroneous SS for a given frame). Then, we identify the SS that can still be used after they are inspected under auxiliary frames. We call those cases unequivocal SS cases.

We calculate the secret rate (in absence of eavesdropping) as the sum up of the information derived from the unequivocal error-free rate and the amount of information derived from the unequivocal erroneous rate (unequivocal error-free rate is obtained as the number of unequivocal error-free SS under the total number of error-free SS; conversely, the unequivocal error rate is obtained as the rate of unequivocal erroneous SS over the total erroneous SS cases). As mentioned earlier, unequivocal means that ambiguity can be removed using auxiliary frames. The bits from remaining SS must be eliminated since they do not contribute to the secret rate.

In Table 6, we detail the deduction of the secret rate. Each SS contributes with a single bit. In 2×2 frames, we have 4 usable frames, and each one generates 4 SS; to compute the unequivocal erroneous rate, we have 2 SS per frame that can be recovered from 12 SS per frame yields $\frac{1}{6}$. On the other hand, to derive the unequivocal error-free rate, we have 2 SS per frame that can be recovered from 4 SS per frame it yields $\frac{1}{2}$. The unequivocal erroneous rate in 3×2 frames yields $\frac{1}{3}$, and the unequivocal error-free rate gives $\frac{1}{21}$ (see Figure 3).

Table 6. The secret rate is indicated without taking the framing gain for each frame size. The secret rate is shown when $e = 0$ and $e = 1$.

$I_{ab_{(2 \times 2)}}$	$I_{ab_{(3 \times 2)}}$
$\frac{1}{2}(1 - e) + \frac{1}{6}e$	$\frac{1}{3}(1 - e) + \frac{1}{21}e$
$\frac{1}{2} - \frac{1}{3}e$	$\frac{1}{3} - \frac{2}{7}e$
$e = 0 \rightarrow I_{ab_{(2 \times 2)}} = \frac{1}{2}$	$e = 0 \rightarrow I_{ab_{(3 \times 2)}} = \frac{1}{3}$
$e = 1 \rightarrow I_{ab_{(2 \times 2)}} = \frac{1}{6}$	$e = 1 \rightarrow I_{ab_{(3 \times 2)}} = \frac{1}{21}$

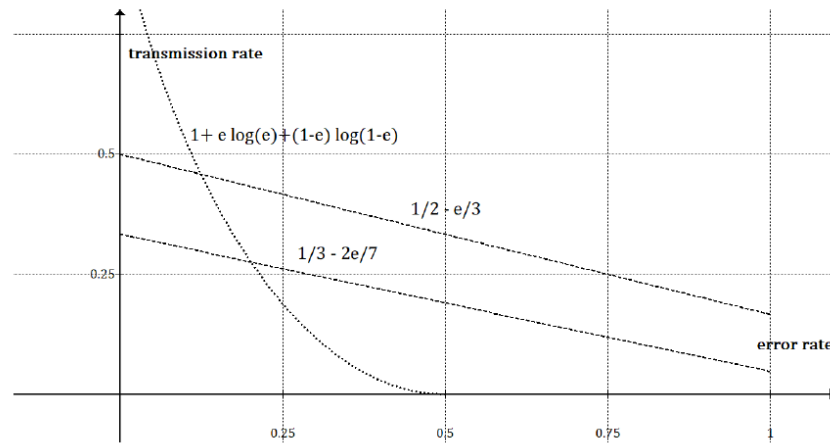


Figure 3. The theoretical transmission rate is plotted as a function of the quantum bit error rate (QBER) e ; we show the 2×2 and 3×2 lines and the Shannon’s reference function. When $e = 1$, the secret rate achieves 0.16 for 2×2 frames and 0.047 for 3×2 frames.

4.1. Secret Throughput

One of the main advantages of the reconciliation method based on frames is the total number of secret bits that results when the framing gain is applied. Remarkably, framing gain results from the amount of total combinations among double matching detection events. We call this process privacy pre-amplification (or amplification in short). Therefore, we compute the secret throughput multiplying the secret rate by the framing gain. In the case of 2×2 frames, we have 4 usable frames under 16 total frames, so the framing gain is $\frac{1}{4} \binom{n}{2}$. Conversely, in 3×2 frames, there are 24 over 64 frames, so the framing gain is $\frac{3}{8} \binom{n}{3}$. Equation (2) describes the secret throughput for each case.

$$\begin{aligned}
 I_{ab_{(2 \times 2)}} &= \frac{1}{4} \binom{n}{2} \left(\frac{1}{2} - \frac{1}{3}e \right) \\
 I_{ab_{(3 \times 2)}} &= \frac{3}{8} \binom{n}{3} \left(\frac{1}{3} - \frac{2}{7}e \right)
 \end{aligned}
 \tag{1}$$

Just to appreciate the growth rate of each frame size, we compute, in Table 7, some values of the secret throughput as a function of n and e . As it can be inferred, 3×2 frames have a visible advantage to produce secret bits, e.g., when $n = 10^3$, it raises the secret throughput to $n = 10^8$ bits.

Table 7. The theoretical secret throughput (bits) as a function of n and e for each frame size.

n	$e = 0$		$e = 0.5$		$e = 1$	
	$I_{ab(2 \times 2)}$	$I_{ab(3 \times 2)}$	$I_{ab(2 \times 2)}$	$I_{ab(3 \times 2)}$	$I_{ab(2 \times 2)}$	$I_{ab(3 \times 2)}$
100	618	20,212	412	11,550	206	2887
500	15,593	2,588,562	10,395	1,479,178	5197	369,794
1000	62,437	20,770,875	41,625	11,869,071	20,812	2,967,267

4.2. Rate Code

The rate code r_{ab} is the relation between the secret information and the total bits generated to achieve reconciliation. In the case of 2×2 frames, the total information is $4\binom{n}{2}$, while the total number is $6\binom{n}{3}$ in 3×2 frames. The rate code for each size of frame is written in Equation (2).

$$\begin{aligned} r_{ab(2 \times 2)} &= \frac{1}{16} \left(\frac{1}{2} - \frac{1}{3}e \right) \\ r_{ab(3 \times 2)} &= \frac{1}{16} \left(\frac{1}{3} - \frac{2}{7}e \right) \end{aligned} \quad (2)$$

4.3. Secret Key Rate

In the case of frame reconciliation, the eavesdropper has a great disadvantage since they do not know Bob's bases selection because they are not revealed over the classical channel. Even if the eavesdropper captures some copies of the quantum pulses, they must deal with the double detection events and the basis choices. Moreover, although the eavesdropper could replicate some double detection events, Alice performs all combinations between double detection events. As a consequence of the privacy amplification process, the eavesdropper's information reduces even more.

4.3.1. The Intercept and Resend Attack (IR)

In the Intercept and Resend (IR) attack, the eavesdropper first measures each pair of non-orthogonal quantum pulses in the quantum channel, and then they send another pair of quantum pulses to Bob prepared according to the same quantum states.

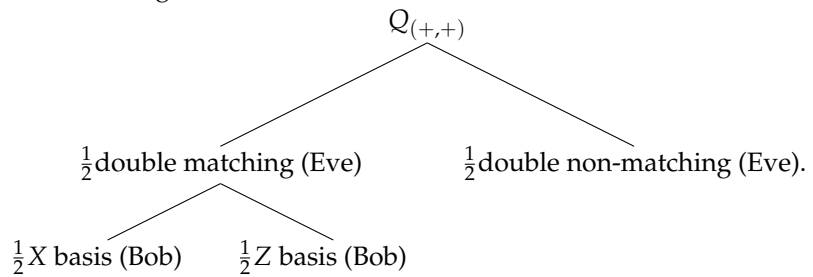
Since secret bits are derived only from double matching detection events, Eve must produce first a double matching detection event using the quantum states she intercepts in the quantum channel because no useful information could be extracted from double non-matching detection events nor even single detection events.

In addition, Eve must guarantee that both states she resends to Bob's station achieve his optical detectors, which imposes a severe difficulty because vacuum or single detection events are more probable than double detection events. However, suppose Eve forces both quantum states to arrive Bob's receiver station. We can derive the efficiency of the IR attack using the following example:

- Alice sends the non-orthogonal pair $(|0_X\rangle, |0_Z\rangle)$ to Bob over the quantum channel. Eve measures them using Z basis, and let us assume she obtains a double matching detection event, say $(|0_Z\rangle, |0_Z\rangle)$.
- Eve prepares and sends the quantum pair $(|0_Z\rangle, |0_Z\rangle)$ to Bob.
- Suppose Eve can force both quantum pulses to arrive to Bob's optical station. There are two quantum measurement bases (X or Z) and five possible outcomes:
 - $\frac{1}{2}$ due to Bob's Z basis: $(|0_Z\rangle, |0_Z\rangle)$.
 - $\frac{1}{2}$ due to Bob's X basis: $\{(|0_X\rangle, |0_X\rangle), (|1_X\rangle, |1_X\rangle), (|1_X\rangle, |0_X\rangle), (|0_X\rangle, |1_X\rangle)\}$.

To match Eve's double detection event $(|0_Z\rangle, |0_Z\rangle)$, Bob must choose the Z basis which occurs with $\frac{1}{2}$ probability, so Eve's final probability is $\frac{1}{4}$.

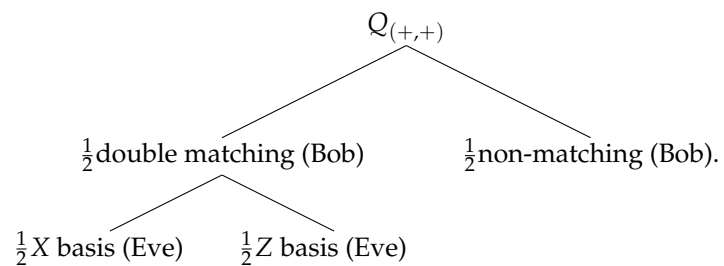
The overall scheme is depicted in the following diagram, where $Q_{(+,+)}$ represents Alice’s pairs of non-orthogonal states:



4.3.2. The Photon Number Splitting Attack (PNS)

The eavesdropper has a copy of all the quantum states that arrive to Bob’s station because Alice sends attenuated (multi-photon) quantum pulses, and the eavesdropper is equipped with a sufficiently large quantum memory. However, the eavesdropper’s probability of getting a double matching detection event is $\frac{1}{2}$. In addition, Eve must measure choosing between two different measurement basis (X or Z); thus, his final probability is $\frac{1}{4}$:

- $\frac{1}{2}$ because of the probability to get a double matching detection event.
- $\frac{1}{2}$ due to basis matching. Eve must measure choosing between two different measurement basis (X or Z).



4.3.3. The Bases Choice Attack (BC)

The eavesdropper would decide to apply another quantum measurement bases to gain more information, and then they use the measurement bases $X + Z$ or $X - Z$. First, consider that the eavesdropper chooses between the measurement bases ($X + Z$ or $X - Z$) with 0.5 probability. However, non-matching detection events are ambiguous for the eavesdropper, which occur with $\frac{6}{16}$ probability. In contrast, they get a double matching event with $\frac{9}{16}$ probability. As a result, the chance to get Bob’s information is $\frac{9}{32}$.

Equation (3) shows the relation to compute the secret key rate for each frame size. It is written as the secret information multiplied by the rate between the total frames produced by Alice and those the eavesdropper duplicates.

$$\begin{aligned} \Delta I_{(2X2)} &= \left[\frac{1}{2} - \frac{1}{3}e \right] \left[1 - \frac{\binom{R \cdot n}{2}}{\binom{n}{2}} \right] \\ \Delta I_{(3X2)} &= \left[\frac{1}{3} - \frac{2}{7}e \right] \left[1 - \frac{\binom{R \cdot n}{3}}{\binom{n}{3}} \right]. \end{aligned} \tag{3}$$

Table 8 shows the final secret key information for each attack: Intercept and Resend attack (IR), Photon Number Splitting attack (PNS), and Basis Choice attack (BC). In the case of 2×2 frames, we have ignored the linear term n that is generated in $\binom{n}{2}$ because the quadratic term n^2 is dominant. In the same way, we omitted the quadratic and linear terms produced by $\binom{n}{3}$ because of the high order of the cubic term.

Table 8. The secret key rate is computed as $\Delta I = I_{ab} - I_{ae}$ for each attack.

IR	PNS	BC
$\left(1 - \left(\frac{1}{4}\right)^2\right) \cdot I_{ab(2 \times 2)}$	$\left(1 - \left(\frac{1}{4}\right)^2\right) \cdot I_{ab(2 \times 2)}$	$\left(1 - \left(\frac{9}{32}\right)^2\right) \cdot I_{ab(2 \times 2)}$
$\left(1 - \left(\frac{1}{4}\right)^3\right) \cdot I_{ab(3 \times 2)}$	$\left(1 - \left(\frac{1}{4}\right)^3\right) \cdot I_{ab(3 \times 2)}$	$\left(1 - \left(\frac{9}{32}\right)^3\right) \cdot I_{ab(3 \times 2)}$

As it can be deduced from Table 8, the secret key rate is affected slightly by the eavesdropper's behavior. This new scenario opens the possibility to employ less attenuated pulses as in CV-QKD to achieve, on one hand, long-distances quantum links or, on the other, portable QKD in closed buildings [46].

5. Conclusions

We have discussed a new post-processing method for Quantum Key Distribution (QKD) that raises cubically the secret key rate in the number of double matching detection events. Secret bits are derived from reactive bits instead of Shannon information, so Bob's measured bits are publicly revealed, while bases selections remain secret. Our method implements sifting, reconciliation, and amplification in a unique process, and it just requires a round iteration; no redundancy bits are sent, and no limit in the correctable error percentage. Despite the fact that the reconciliation is performed with a unity error channel, the secret rate is kept, at least theoretically, in 16% using 2×2 frames and 4.7% when using 3×2 frames.

It is not difficult to evaluate the security of this method because it can be evaluated directly through the frames. There is no dependency on other security mechanism as hash functions.

The protocol works fast, at least theoretically, convergence is guaranteed, and it can be implemented as a post-processing software into QKD technologies.

Author Contributions: L.A.L.-P. conceived of the presented idea, he developed the theoretical formalism, J.M.L.R. supervised the project and contributed to the interpretation of the results and E.H.S. performed software and numerical simulations. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Council of Science and Technology of Mexico (CONACyT) and Center for Research and Advanced Studies of the National Polytechnic Institute of Mexico (Cinvestav-IPN).

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available within the article.

Conflicts of Interest: The authors declare no conflict of interest in this article.

Appendix A

This Appendix contains the relevant tables used for the framed methodology:

- Table A1 describes the complete set of 3×2 frames.
- MR are illustrated in Table A2.
- Table A3 enlists SS, MR, frames, and sb.
- Sifting bits are written in Table A4.
- Table A5 shows the cases that can be successfully disambiguated.

Table A1. There are 24 useful frames: f_i , where $i = 1, \dots, 24$ and 3 Auxiliary frames f_j , where $j = 25, \dots, 27$.

Useful Frames			Auxiliary Frames
$f_1 = \begin{pmatrix} 0_X\rangle & 0_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_2 = \begin{pmatrix} 1_X\rangle & 0_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_3 = \begin{pmatrix} 0_X\rangle & 0_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 0_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{25} = \begin{pmatrix} 0_X\rangle & 0_Z\rangle \\ 0_X\rangle & 0_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$
$f_4 = \begin{pmatrix} 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_5 = \begin{pmatrix} 1_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_6 = \begin{pmatrix} 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_{26} = \begin{pmatrix} 0_X\rangle & 1_Z\rangle \\ 0_X\rangle & 0_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$
$f_7 = \begin{pmatrix} 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_8 = \begin{pmatrix} 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_9 = \begin{pmatrix} 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 0_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{27} = \begin{pmatrix} 1_X\rangle & 1_Z\rangle \\ 0_X\rangle & 0_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$
$f_{10} = \begin{pmatrix} 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_{11} = \begin{pmatrix} 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_{12} = \begin{pmatrix} 0_X\rangle & 0_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \end{pmatrix}$	
$f_{13} = \begin{pmatrix} 0_X\rangle & 0_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{14} = \begin{pmatrix} 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \\ 0_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_{15} = \begin{pmatrix} 0_X\rangle & 0_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \end{pmatrix}$	
$f_{16} = \begin{pmatrix} 0_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \end{pmatrix}$	$f_{17} = \begin{pmatrix} 0_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{18} = \begin{pmatrix} 0_X\rangle & 0_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \end{pmatrix}$	
$f_{19} = \begin{pmatrix} 0_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{20} = \begin{pmatrix} 1_X\rangle & 0_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{21} = \begin{pmatrix} 1_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \end{pmatrix}$	
$f_{22} = \begin{pmatrix} 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 0_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{23} = \begin{pmatrix} 1_X\rangle & 0_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \end{pmatrix}$	$f_{24} = \begin{pmatrix} 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 1_Z\rangle \\ 1_X\rangle & 0_Z\rangle \end{pmatrix}$	

Table A2. There exist eight possible Matching Results (MR) for 3×2 frames. The bit produced by a double matching event is represented inside the key notation with the symbol \bullet . Additionally, each MR has been identified with a binary code left to each frame. After the sifting process, such MR code will become part of the secret key.

MR = 000 $\begin{pmatrix} \bullet X\rangle & - \\ \bullet X\rangle & - \\ \bullet X\rangle & - \end{pmatrix}$	MR = 100 $\begin{pmatrix} \bullet X\rangle & - \\ \bullet X\rangle & - \\ - & \bullet Z\rangle \end{pmatrix}$
MR = 001 $\begin{pmatrix} - & \bullet Z\rangle \\ - & \bullet Z\rangle \\ - & \bullet Z\rangle \end{pmatrix}$	MR = 101 $\begin{pmatrix} - & \bullet Z\rangle \\ - & \bullet Z\rangle \\ \bullet X\rangle & - \end{pmatrix}$
MR = 010 $\begin{pmatrix} \bullet X\rangle & - \\ - & \bullet Z\rangle \\ \bullet X\rangle & - \end{pmatrix}$	MR = 110 $\begin{pmatrix} \bullet X\rangle & - \\ - & \bullet Z\rangle \\ - & \bullet Z\rangle \end{pmatrix}$
MR = 011 $\begin{pmatrix} - & \bullet Z\rangle \\ \bullet X\rangle & - \\ - & \bullet Z\rangle \end{pmatrix}$	MR = 111 $\begin{pmatrix} - & \bullet Z\rangle \\ \bullet X\rangle & - \\ \bullet X\rangle & - \end{pmatrix}$

Table A3. Bob sends to Alice the Sifting Strings (SS) which are constructed with the sifting bits and the measured bits. Alice knows the frames behind each SS, so she can get the secret bit (sb). On his side, Bob uses the SS and the MR to achieve the same bit.

Sifting String		Bob's MR	Alice's Frame	sb	Bob's MR	sb	Alice's Frame
Measured	Sifting						
110	000	000	f_6, f_9, f_{14}, f_{22}	0	001	1	$f_5, f_{11}, f_{16}, f_{24}$
011	000	000	$f_8, f_{13}, f_{18}, f_{19}$	0	001	1	$f_{12}, f_{15}, f_{20}, f_{23}$
011	001	110	$f_{12}, f_{15}, f_{17}, f_{19}$	0	111	1	$f_4, f_{13}, f_{18}, f_{23}$
110	001	100	$f_6, f_{10}, f_{14}, f_{24}$	0	101	1	$f_5, f_{11}, f_{21}, f_{22}$
010	011	110	$f_1, f_{11}, f_{16}, f_{18}$	0	101	1	f_2, f_6, f_{12}, f_{20}
111	011	100	f_4, f_9, f_{22}, f_{23}	0	111	1	$f_8, f_{10}, f_{19}, f_{24}$
001	010	001	f_3, f_4, f_9, f_{13}	0	011	1	f_{15}, f_{20}
100	010	001	f_7, f_8, f_{10}, f_{14}	0	011	1	f_5, f_{16}
010	010	001	f_1, f_2, f_6, f_{18}	0	010	1	f_{11}, f_{12}
111	010	001	$f_{17}, f_{19}, f_{21}, f_{22}$	0	010	1	f_{23}, f_{24}
001	011	110	f_3, f_{13}	0	100	1	f_{15}, f_{17}
100	011	101	f_7, f_{14}	0	111	1	f_5, f_{21}
001	100	000	$f_1, f_{15}, f_{16}, f_{17}$	0	010	1	f_8, f_{13}
100	100	000	f_2, f_5, f_{20}, f_{21}	0	010	1	f_9, f_{14}
010	100	000	f_3, f_7, f_{11}, f_{12}	0	011	1	f_6, f_{18}
111	100	000	$f_4, f_{10}, f_{23}, f_{24}$	0	011	1	f_{19}, f_{22}
001	101	111	f_1, f_{15}	0	101	1	f_4, f_{13}
100	101	100	f_2, f_5	0	110	1	f_{10}, f_{14}
010	101	111	f_3, f_6, f_9, f_{12}	0	100	1	f_7, f_8, f_{11}, f_{18}
111	101	101	$f_{16}, f_{17}, f_{19}, f_{24}$	0	110	1	$f_{20}, f_{21}, f_{22}, f_{23}$
011	110	010	$f_1, f_{15}, f_{16}, f_{17}, f_{18}, f_{19}$	0	011	1	$f_3, f_4, f_9, f_{12}, f_{13}, f_{23}$
110	110	010	$f_2, f_5, f_6, f_{20}, f_{21}, f_{22}$	0	011	1	$f_7, f_8, f_{10}, f_{11}, f_{14}, f_{24}$
011	111	101	$f_1, f_{15}, f_{18}, f_{23}$	0	100	1	$f_3, f_{12}, f_{13}, f_{19}$
110	111	110	f_2, f_5, f_6, f_{24}	0	111	1	$f_7, f_{11}, f_{14}, f_{22}$

Table A5. We list the cases that can be successfully disambiguated. Zero cases refer to the error-free SS.

Frame	MR	SS	Disambiguated Bits
f_1	010	011,110	2nd & 3rd
	101	011,111	
f_2	010	110,110	1st & 2nd
	110	110,111	
f_3	011	011,110	2nd & 3rd
	100	011,111	
f_4	100	111,011	zero & 1st
f_5	001	110,000	zero & 2nd
	010	110,110	
	101	110,001	
	110	110,111	
f_6	000	110,000	zero & 1st
	010	110,110	
	100	110,001	
	110	110,111	
f_7	011	110,110	1st & 2nd
	111	110,111	
f_8	111	111,011	1st & 3rd
f_9	100	111,011	1st & 3rd
f_{10}	111	111,011	zero & 3rd
f_{11}	001	110,000	zero & 1st
	011	110,110	
	101	110,001	
	111	110,111	
f_{12}	001	011,000	zero & 3rd
	011	011,110	
	100	011,111	
	110	011,001	
f_{13}	000	011,000	zero & 2nd
	011	011,110	
	100	011,111	
	111	011,001	
f_{14}	000	110,000	zero & 2nd
	011	110,110	
	100	110,001	
	111	110,111	
f_{15}	001	011,000	zero & 2nd
	010	011,110	
	101	011,111	
	110	011,001	
f_{16}	101	111,101	1st & 3rd
f_{17}	101	111,101	zero & 1st

Table A5. Cont.

Frame	MR	SS	Disambiguated Bits
f_{18}	000	011,000	zero & 3rd
	010	011,110	
	101	011,111	
	111	011,001	
f_{19}	001	111,010	zero & 1st
	011	111,100	
	101	111,101	
	111	111,011	
f_{20}	110	111,101	1st & 3rd
f_{21}	110	111,101	zero & 3rd
f_{22}	001	111,010	zero & 3rd
	011	111,100	
	100	111,011	
	110	111,101	
f_{23}	000	111,100	zero & 1st
	010	111,010	
	100	111,011	
	110	111,101	
f_{24}	000	111,100	zero & 3rd
	010	111,010	
	101	111,101	
	111	111,011	

References

- Kao, K.C.; Hockham, G.A. Dielectric-fibre surface waveguides for optical frequencies. In *Proceedings of the Institution of Electrical Engineers*; IET: London, UK, 1966; Volume 113, pp. 1151–1158.
- Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [[CrossRef](#)]
- Xu, F.; Ma, X.; Zhang, Q.; Lo, H.; Pan, J. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [[CrossRef](#)]
- Mehic, M.; Niemiec, M.; Rass, S.; Ma, J.; Peev, M.; Aguado, A.; Martin, V.; Schauer, S.; Poppe, A.; Pacher, C.; et al. Quantum key distribution: A networking perspective. *ACM Comput. Surv. CSUR* **2020**, *53*, 1–41. [[CrossRef](#)]
- Lovic, V. Quantum key distribution: Advantages, challenges and policy. *Camb. J. Sci. Policy* **2020**, *1*, e8410270193. [[CrossRef](#)]
- Razavi, M.; Leverrier, A.; Ma, X.; Qi, B.; Yuan, Z. Quantum key distribution and beyond: Introduction. *JOSA B* **2019**, *36*, QKD1–QKD2. [[CrossRef](#)]
- Geihs, M.; Nikiforov, O.; Demirel, D.; Sauer, A.; Butin, D.; Günther, F.; Alber, G.; Walther, T.; Buchmann, J. The status of quantum-key-distribution-based long-term secure internet communication. *IEEE Trans. Sustain. Comput.* **2019**. [[CrossRef](#)]
- Kong, P. A review of quantum key distribution protocols in the perspective of smart grid communication security. *IEEE Syst. J.* **2020**. [[CrossRef](#)]
- Pearson, D. High-speed qkd reconciliation using forward error correction. In *AIP Conference Proceedings*; American Institute of Physics: Melville, NY, USA, 2004; Volume 734, pp. 299–302.
- Runser, R.J.; Chapuran, T.; Toliver, P.; Peters, N.A.; Goodman, M.S.; Kosloski, J.T.; Nweke, N.; McNown, S.R.; Hughes, R.J.; Rosenberg, D.; et al. Progress toward quantum communications networks: Opportunities and challenges. In *Optoelectronic Integrated Circuits IX*; International Society for Optics and Photonics: Red Hook, NY, USA, 2007; Volume 6476, p. 64760I.
- Lütkenhaus, N. Estimates for practical quantum cryptography. *Phys. Rev. A* **1999**, *59*, 3301. [[CrossRef](#)]
- Lizama-Pérez, L.A.; López, J.M.; Carlos-López, E.D.; Venegas-Andraca, S.E. Quantum flows for secret key distribution in the presence of the photon number splitting attack. *Entropy* **2014**, *16*, 3121–3135. [[CrossRef](#)]
- Lizama-Pérez, L.A.; López, J.M.; De Carlos López, E. Quantum key distribution in the presence of the intercept-resend with faked states attack. *Entropy* **2016**, *19*, 4. [[CrossRef](#)]
- Lizama-Pérez, L.A.; Lopez, M. Quantum key distillation using binary frames. *Symmetry* **2020**, *12*, 1053. [[CrossRef](#)]

15. Fung, C.H.F.; Qi, B.; Tamaki, K.; Lo, H.K. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **2007**, *75*, 032314. [CrossRef]
16. Xu, F.; Qi, B.; Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **2010**, *12*, 113026. [CrossRef]
17. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 691–705. [CrossRef]
18. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313. [CrossRef]
19. Makarov, V.; Skaar, J. Faked states attack using detector efficiency mismatch on sarg04, phase-time, dpsk, and ekert protocols. *Quantum Inf. Comput.* **2008**, *8*, 622–635.
20. Qi, B.; Fung, C.F.; Lo, H.; Ma, X. Time-shift attack in practical quantum cryptosystems. *arXiv* **2005**, arXiv:quant-ph/0512080.
21. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [CrossRef]
22. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2011**, *2*, 349. [CrossRef]
23. Wiechers, C.; Lydersen, L.; Wittmann, C.; Elser, D.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. After-gate attack on a quantum cryptosystem. *New J. Phys.* **2011**, *13*, 013043. [CrossRef]
24. Weier, H.; Krauss, H.; Rau, M.; Fuerst, M.; Nauerth, S.; Weinfurter, H. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. *New J. Phys.* **2011**, *13*, 073024. [CrossRef]
25. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef] [PubMed]
26. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
27. Verdu, S. Fifty years of shannon theory. *IEEE Trans. Inf. Theory* **1998**, *44*, 2057–2078. [CrossRef]
28. Kuritsyn, K. Modification of error reconciliation scheme for quantum cryptography. In *First International Symposium on Quantum Informatics*; International Society for Optics and Photonics: Red Hook, NY, USA, 2003; Volume 5128, pp. 91–94.
29. Brassard, G.; Salvail, L. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 410–423.
30. Buttler, W.T.; Lamoreaux, S.K.; Torgerson, J.R.; Nickel, G.H.; Donahue, C.H.; Peterson, C.G. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A* **2003**, *67*, 052303. [CrossRef]
31. Van Assche, G.; Cardinal, J.; Cerf, N.J. Reconciliation of a quantum-distributed gaussian key. *IEEE Trans. Inf. Theory* **2004**, *50*, 394–400. [CrossRef]
32. Bennett, C.H.; Brassard, G.; Crépeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **1995**, *41*, 1915–1923. [CrossRef]
33. Muramatsu, J. Transmission of messages to the efficiency limit—implementation of tractable channel code achieving the shannon limit. *NTT Tech. Rev.* **2019**, *17*, 34–39.
34. Yuan, H.; Song, J.; Han, L.; Hou, K.; Shi, S. Improving the total efficiency of quantum key distribution by comparing bell states. *Opt. Commun.* **2008**, *281*, 4803–4806. [CrossRef]
35. Abou Jaoude, A. The paradigm of complex probability and claude shannon’s information theory. *Syst. Sci. Control Eng.* **2017**, *5*, 380–425. [CrossRef]
36. Wagner, N.R. The Laws of Cryptography with Java Code. 2003. Available online: https://www.cssh.net/sites/default/files/_downloadable/crypto/laws_of_cryptography_with_java_code.pdf (accessed on 18 December 2020).
37. 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]
38. Grosshans, F.; Grangier, P. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv* **2002**, arXiv:quant-ph/0204127.
39. Wang, X.; Zhang, Y.; Yu, S.; Guo, H. High speed error correction for continuous-variable quantum key distribution with multi-edge type ldpc code. *Sci. Rep.* **2018**, *8*, 1–7. [CrossRef] [PubMed]
40. Chung, S.; Forney, G.D.; Richardson, T.J.; Urbanke, R. On the design of low-density parity-check codes within 0.0045 db of the shannon limit. *IEEE Commun. Lett.* **2001**, *5*, 58–60. [CrossRef]
41. Mehic, M.; Niemiec, M.; Siljak, H.; Voznak, M. Error reconciliation in quantum key distribution protocols. *Lect. Notes Comput. Sci.* **2020**, *12070*, 222–236.
42. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, Systems & Signal Processing*, Bangalore, India, 9–12 December 1984.
43. Van Assche, G. *Quantum Cryptography and Secret-Key Distillation*; Cambridge University Press: Cambridge, UK, 2006.
44. Hughes, R.; Nordholt, J.; Rarity, J. *Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography—A Quantum Information Science and Technology Roadmap*; United States Government: New York, NY, USA, 2004.
45. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
46. Kumar, V.V.; Karthikeyan, T.; Praveen Sundar, P.V.; Magesh, G.; Balajee, J.M. A quantum approach in lifi security using quantum key distribution. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 2345–2354.