Quantum Key Distillation using Binary Frames

Luis A. Lizama-Perez[1] [0000−0001−5109−2927] and José Mauricio López Romero[2]

Sección de Posgrado de la Universidad Politécnica de Pachuca,
Ex-Hacienda de Santa Bárbara, 43830, México
luislizama@upp.edu.mx
Cinvestav Querétaro, Libramiento Norponiente 2000,
Real de Juriquilla, 76230, Santiago de Querétaro, Querétaro, México
jm.lopez@cinvestav.mx

Abstract. We introduce a new integral method for Quantum Key Distribution to perform sifting, reconciliation and amplification processes to establish a cryptographic key through the use of binary structures called frames which are capable to increase quadratically the secret key rate. The method can be implemented with the usual optical Bennett-Brassard ($BB84$) equipment allowing strong pulses in the quantum regime.

Keywords: frame · distillation · QKD.

1 Introduction

Quantum cryptography has emerged as a promissory theoretical and technological paradigm for the quantum computing era. This is so because the presence of an eavesdropper in QKD protocols produces a detectable disturbance on the quantum communication. Unfortunately, some technological loopholes have been found in the photo-detection system which have imposed new challenges to QKD systems.

Due to those technological loopholes most of the QKD systems have failed to be secure against some of the most challenging attacks: the Intercept-Resend with Faked States (IRFS) attack [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] and the Photon Number Splitting (PNS) attack [11]. $IRFS$ attack can be partially solved by monitoring the photo intensity at the receiver.

Previously, we have introduced the $ack-state$ protocol in [12, 13]. In addition, the $nack-state$ protocol was first discussed in [14]. Such protocols constitute a generalization of the $BB84$ to resist the PNS attack [13] and the $IRFS$ attack [14], respectively. Both methods are conceived under the basis of a new theoretical approach called quantum flows, denoted by Q [13, 15].

In this work, we extend the Q approach to introduce a new distillation method based on binary structures called frames. It is known that the distillation process generate a few secret bits after a high number of quantum pulses are transmitted from Alice (the sender) to Bob (the receiver).

Several algorithms are applied during the distillation process: sifting, error correction and privacy amplification among others. However, some of them have been developed from other research fields to attend specific requirements. Error correction algorithms are described in [16, 17, 18, 19] and privacy amplification is analyzed in [20]. Up to our knowledge there is no an integral method capable to perform the QKD distillation in a single process.

We will introduce here the frame distillation as an integral method for QKD to perform sifting, error correction and privacy amplification just in one process. Surprisingly, we have found that at least theoretically, this technique increases quadratically the size of the secret key allowing to raise up the secret key rate.

2 Related work

We will describe briefly some other reconciliation methods used in QKD:

1. Binary [16] is a reconciliation protocol that find and correct errors after the transmission of quantum pulses caused by the noise in the channel and possibly from the eavesdropper. After Alice and Bob obtain an error estimation based on a portion of their sifted key, they determine whether the error failure threshold has been breached. If the error rate is in excess of the fail threshold, Alice and Bob begin the raw key step again. If the estimated error rate is acceptable, Alice and Bob begin the first of a number of passes and use a predetermined random permutation, applying it to the sifted key bits.
2. Cascade [17] is a reconciliation method that has become the de-facto standard for all QKD practical implementations. After a number of passes, permutations, and cascades, the protocol finishes with low probability that errors still remain [21]. However, large communication overhead have raised methods based on error correcting codes which are more practical.
3. The Winnow algorithm [18] is a reconciliation method based on Hamming codes which introduces additional errors because the Hamming algorithm can only reveal one single error in each block.
4. LDPC [19] is a linear error correcting code that uses iterative decoding using the sum product soft decision decoder to correct transmission errors.

We conclude this section pointing out some of the challenges of interactive methods that could be summarized from [21] as follows:

. Cascade exhibits great efficiency at low error rates but is still robust up to 18% error rate if required.
. Effective estimation of the error rate in the quantum channel.
. Interactivity could be high intensive in the number of passes to check parity.
. The number of required permutations of the shared bits could demand a persistent computational effort.

3 Quantum Pulses

In the quantum flows approach [13, 14], Alice prepares n quantum states, parallel or non-orthogonal which are randomly interleaved to produce a photonic gain at each quantum flow. On the other side, Bob measures the n quantum states with the same measurement basis, X or Z. Fig. 1 shows the quantum states and measurement bases of BB84 and Fig. 2 the quantum states and measurement bases used in quantum flows.

3.1 Quantum information

The basic mechanism to transfer information from Alice to Bob is that one bit is codified at Alice's photonic source through a pair of non-orthogonal quantum states. On the other side, the bit is received successfully if a double matching detection event is produced at Bob's detectors.

Since the two states prepared by Alice are non-orthogonal and Bob uses the same basis to measurement them, it is produced one compatible measurement (the measurement basis matches

Table 1: Comparison of reconciliation methods as presented in [22].

Reconciliation	Method	Advantages	Disadvantages
Interactive	Binary [16]	Easy and simple	Large communication overhead
	Cascade [17]	Easy and simple Strong ability of error correction	
Code based	Winnow [18]	Communication time depending on the rate	Additional errors (Hamming) Great Efficiency
	LDPC [19]	Correction of errors as Cascade Improvement of the safety of the protocol	

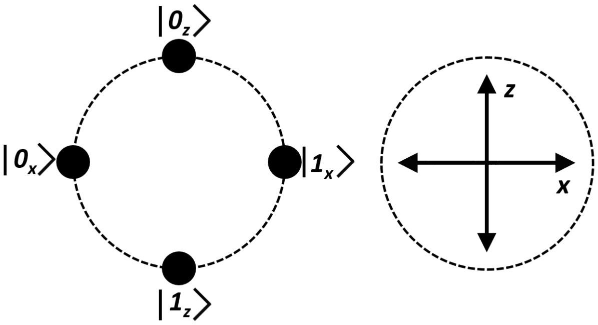

Fig. 1: BB84 pulses. The quantum states prepared by Alice (left): $|0_X\rangle$, $|1_X\rangle$, $|0_Z\rangle$, $|1_Z\rangle$ and the measurement bases applied by Bob (right): X and Z.

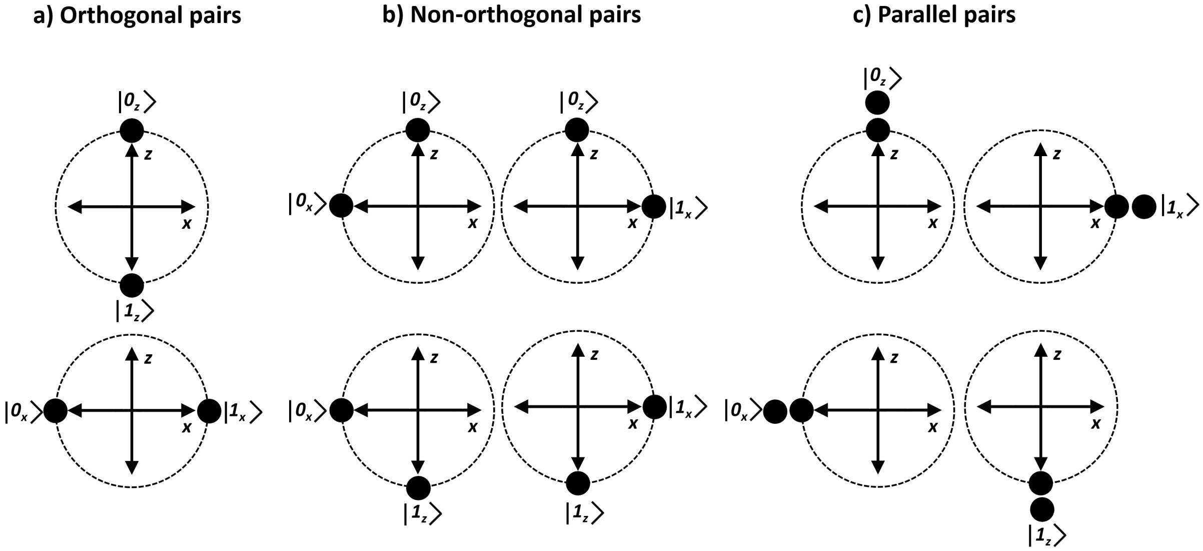

Fig. 2: We represent pairs of quantum states: a) orthogonal pairs ($|0_Z\rangle$, $|1_Z\rangle$) and ($|0_X\rangle$, $|1_X\rangle$), b) non-orthogonal pairs ($|0_X\rangle$, $|0_Z\rangle$), ($|1_X\rangle$, $|0_Z\rangle$), ($|0_X\rangle$, $|1_Z\rangle$) and ($|1_X\rangle$, $|1_Z\rangle$) and c) parallel pairs ($|0_Z\rangle$, $|0_Z\rangle$), ($|1_X\rangle$, $|1_X\rangle$),($|0_X\rangle$, $|0_X\rangle$) and ($|1_Z\rangle$,$|1_Z\rangle$).

one of the quantum states) and one non-compatible measurement (with 50% chance to be detected at the same detector). Therefore, if the quantum states are detected at the same detector, the transferred bit comes from the compatible measurement. As long as a double matching event is produced at Bob's station, the order between the compatible and the non-compatible measurement is irrelevant for our purposes.

Consider Alice sends to Bob some pairs of non-orthogonal states which are depicted in Fig. 2: ($|0_X\rangle$, $|0_Z\rangle$), ($|0_X\rangle$, $|1_Z\rangle$), ($|1_X\rangle$, $|0_Z\rangle$), ($|1_X\rangle$, $|1_Z\rangle$). One of the following detection events can be registered at Bob's optical system:

1. Single detection: One of two the pulses is detected at Bob's station. They could be processed as usual $BB84$ quantum pulses. However, in our context, they have not be included as part of the distillation process.
2. Double detection: The two non-orthogonal states are detected at Bob's station.
   – In the matching case both states are detected at the same photo-detector. In the current protocol this unique case will be exploited to derive secret bits.
   – In the non-matching case the states are registered at different detectors. These results are ambiguous and they are not useful to derive secret bits.
3. No detection: No pulse is registered.

In the BB84 protocol, when a single matching detection event is produced at Bob's station, the information is derived from the compatible quantum measurement cases, otherwise results are ambiguous and must be discarded, see Tab.2.

doi:10.20944/preprints202004.0222.v1

Table 2: Possible results after a single detection event. In BB84, compatible measurements are usable to derive secret bits.

Alice's non-orthogonal pairs	Single detection	Bob's basis measurement	
		X	Z
$(\|0_X\rangle, \|0_Z\rangle)$	$(\|0_X\rangle$, -) (-, $\|0_Z\rangle)$	$(\|0_X\rangle$, -) (-, $\|0_X\rangle)$ or (-, $\|1_X\rangle)$	$(\|0_Z\rangle$, -) or $(\|1_Z\rangle$, -) (-, $\|0_Z\rangle)$
$(\|0_X\rangle, \|1_Z\rangle)$	$(\|0_X\rangle$, -) (-, $\|1_Z\rangle)$	$(\|0_X\rangle$, -) (-, $\|0_X\rangle)$ or (-, $\|1_X\rangle)$	$(\|0_Z\rangle$, -) or $(\|1_Z\rangle$, -) (-, $\|1_Z\rangle)$
$(\|1_X\rangle, \|0_Z\rangle)$	$(\|1_X\rangle$, -) (-, $\|0_Z\rangle)$	$(\|1_X\rangle$, -) (-, $\|0_X\rangle)$ or (-, $\|1_X\rangle)$	$(\|0_Z\rangle$, -) or $(\|1_Z\rangle$, -) (-, $\|0_Z\rangle)$
$(\|1_X\rangle, \|1_Z\rangle)$	$(\|1_X\rangle$, -) (-, $\|1_Z\rangle)$	$(\|1_X\rangle$, -) (-, $\|0_X\rangle)$ or (-, $\|1_X\rangle)$	$(\|0_Z\rangle$, -) or $(\|1_Z\rangle$, -) (-, $\|1_Z\rangle)$

On the other hand, if a double detection event is produced at Bob's station, the information is also derived from the matching cases (see Tab.3). In this case, non-matching results are ambiguous and not usable to distill secret bits.

Table 3: Possible results after a double detection event (matching and non-matching). In case of a double matching detection event one secret bit is derived. The bit comes from the compatible measurement.

Alice's non-orthogonal pairs	Bob's basis measurement			
	Matching event		Non-matching event	
	X	Z	X	Z
$(\|0_X\rangle, \|0_Z\rangle)$	$(\|0_X\rangle, \|0_X\rangle)$	$(\|0_Z\rangle, \|0_Z\rangle)$	$(\|0_X\rangle, \|1_X\rangle)$	$(\|1_Z\rangle, \|0_Z\rangle)$
$(\|0_X\rangle, \|1_Z\rangle)$	$(\|0_X\rangle, \|0_X\rangle)$	$(\|1_Z\rangle, \|1_Z\rangle)$	$(\|0_X\rangle, \|1_X\rangle)$	$(\|0_Z\rangle, \|1_Z\rangle)$
$(\|1_X\rangle, \|0_Z\rangle)$	$(\|1_X\rangle, \|1_X\rangle)$	$(\|0_Z\rangle, \|0_Z\rangle)$	$(\|1_X\rangle, \|0_X\rangle)$	$(\|1_Z\rangle, \|0_Z\rangle)$
$(\|1_X\rangle, \|1_Z\rangle)$	$(\|1_X\rangle, \|1_X\rangle)$	$(\|1_Z\rangle, \|1_Z\rangle)$	$(\|1_X\rangle, \|0_X\rangle)$	$(\|0_Z\rangle, \|1_Z\rangle)$

3.2 Quantum photonic gains

Not taking into account losses in the quantum channel and the efficiency of optical detection system we can compute the gains of double pulses. In this context, $Q_{(+,+)}$ represents the photonic gain of two non-empty pulses, $Q_{(\pm,\mp)}$ is the gain of the pulses in which is produced a non-empty pulse and one vacuum pulse (whatever the order between them) and $Q_{(-,-)}$ is the gain of two consecutive vacuum pulses [15]. Since the gains follow a Poisson's distribution we can write them as:

$$\begin{aligned} Q_{(+,+)} &= (1-e^{-\mu})^2 \\ Q_{(\pm,\mp)} &= 2e^{-\mu}(1-e^{-\mu}) \\ Q_{(-,-)} &= e^{-2\mu} \end{aligned}$$

For example, for $\mu = 0.1$ we have $Q_{(-,-)} = 0.8187$, $Q_{(\pm,\mp)} = 0.1722$ and $Q_{(+,+)} = 0.01$. So the gain of double pulses reduces considerably. Increasing μ to 0.5 raises $Q_{(+,+)}$ to 0.15. However, the detection system sometimes requires a recuperation time after it can register another detection event, so the probability to get two consecutively pulses reduces even more. Fortunately, quantum states inside a pair of non-orthogonal states can be sent temporally separated as it is represented in Fig. 3 (for details see section 4.2 of [14])

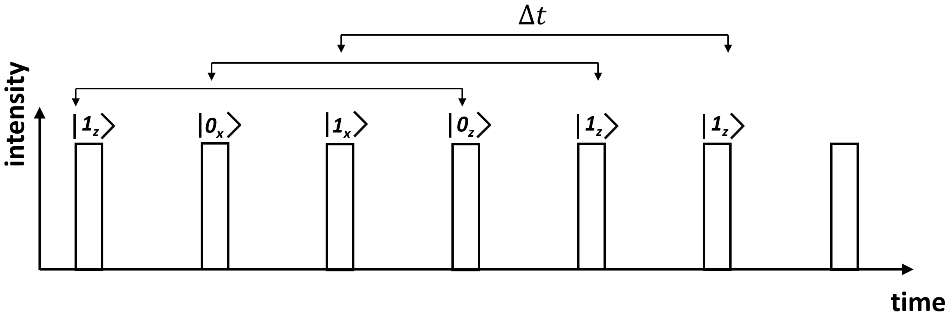

Fig. 3: Quantum states are separated temporally to avoid losses due to consecutive detection events. The order between two non-orthogonal states is not relevant for the present discussion.

3.3 Non-orthogonal measurement

Consider the following scenario: Alice prepares two non-orthogonal states (of those depicted in Fig. 2) and transmits them to Bob. Let us assume that a double matching detection has been produced in Bob's optical system (as stated before, a double matching detection event actives the same detector at the optical receiver system).

For example, Fig. 4 shows that Alice prepares and sends to Bob the pair of non-orthogonal states $(|0_X\rangle, |0_Z\rangle)$. He chooses randomly to measure both pulses with the X basis (or Z). The double detection event could be $|0_X\rangle$ or $|0_Z\rangle$ as can be seen in the bottom of Fig. 4. The four possible results $(|0_X\rangle, |0_Z\rangle)$, $(|0_X\rangle, |1_Z\rangle)$, $(|1_X\rangle, |0_Z\rangle)$ and $(|1_X, 1_Z\rangle)$ are shown in Figs. 4 to 7.

This is equivalent to say that exists one bit codified at each quantum basis. This kind of quantum measurement is just feasible in the case of non-orthogonal states since measurement of parallel states produces ambiguity. For example, consider that Alice sends $(|0_X\rangle, |0_X\rangle)$ to Bob. If he measures them with the (incompatible) Z basis and he obtains a double matching detection event, Bob would register $|0_Z\rangle$ or $|1_Z\rangle$ with the same probability.

4 Non-orthogonal distillation

To explain the distillation process for non-orthogonal states we must introduce a new concept based on binary structures called frames.

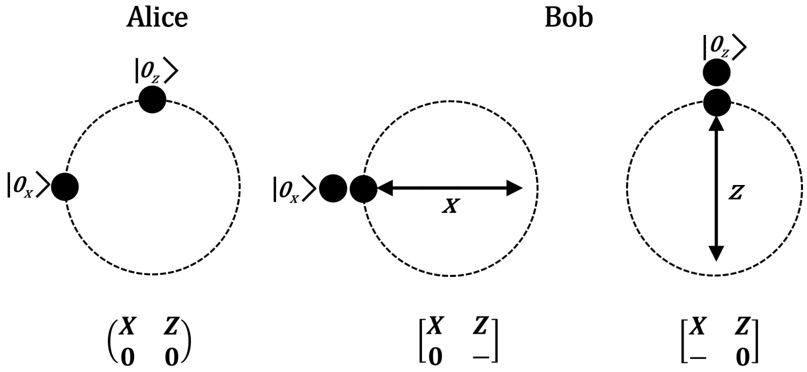

Fig. 4: Alice sends the non-orthogonal pair $|0_X\rangle$, $|0_Z\rangle$ to Bob. After a double matching detection event is produced, Bob's optical system could register $|0_X\rangle$ or $|0_Z\rangle$.

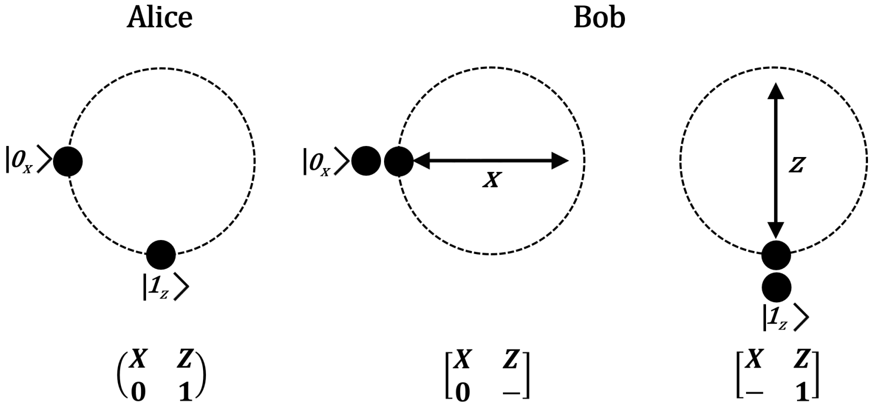

Fig. 5: Alice sends $(|0_X\rangle\,, |1_Z\rangle)$ to Bob. After a double matching detection event is produced, Bob's optical system could register $|0_X\rangle$ or $|1_Z\rangle$.

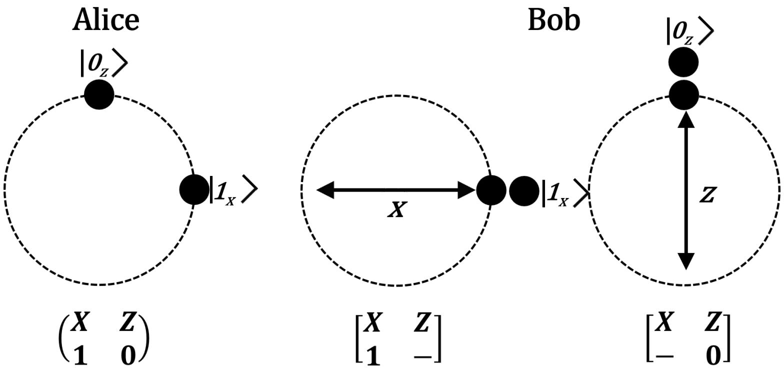

Fig. 6: Alice sends $(|1_X\rangle, |0_Z\rangle)$ to Bob. After a double matching detection event is produced, Bob's optical system could register $|1_X\rangle$ or $|0_Z\rangle$.

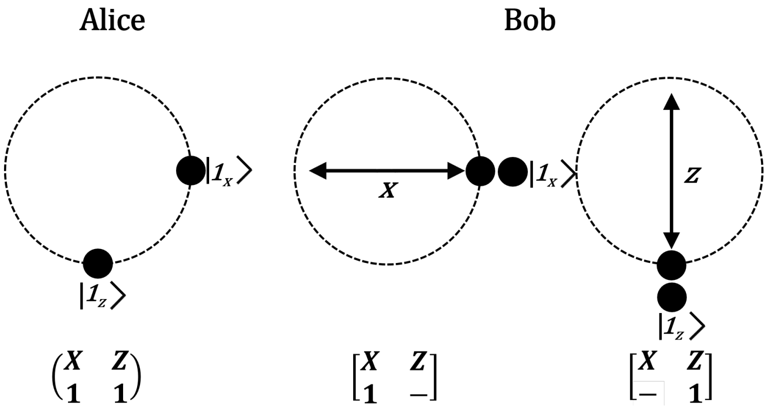

Fig. 7: Alice sends $(|1_X\rangle, |1_Z\rangle)$ to Bob. After a double matching detection event is produced, Bob's optical system could register $|1_X\rangle$ or $|1_Z\rangle$.

4.1 Frames

Binary frames or simply frames, are binary structures conceived to implement the sifting, error correction and amplification processes for non-orthogonal based QKD. We introduced the set of 2×2 frames enumerated from 1 to 6 in Tab. 4.

Each row of a frame contains the bits that could be registered at each basis (X or Z) after a double matching detection event is produced at Bob's station (basis X at the left, basis Z at the right) as it is shown in Tab. 4. Briefly, we can say that each row corresponds to a pair of Alice's non-orthogonal states. The same row represents a double detection event at Bob's side.

Table 4: There are 6 valid frames: f_i, where $i = 1, \ldots, 6$ and 8 invalid frames f_j, where $j = 7, \ldots, 14$.

valid frames		invalid frames	
$f_1 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$	$f_2 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$	$f_7 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$	$f_{11} \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 1 & 1 \end{pmatrix}$
$f_3 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$	$f_4 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$	$f_8 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$	$f_{12} \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 0 & 0 \end{pmatrix}$
$f_5 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$	$f_6 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$	$f_9 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$	$f_{13} \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$
		$f_{10} \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 0 \\ 0 & 0 \end{pmatrix}$	$f_{14} \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$

As can be deduced, Bob can obtain just one bit per row, the row that corresponds to the basis that Bob chose to measure the two non-orthogonal states sent by Alice. Just to be clearer, Fig. 8 show (at left) how are related the non-orthogonal states sent by Alice to the corresponding frame. At the right of Fig. 8 it is represented the four possible Matching Results (MR) at Bob's station.

4.2 Matching Results (MR)

Now, we will define the Matching Results, denoted as MR produced at Bob's station which are required for the sifting process. Tab. 5 illustrate the possible Matching Results for 2×2 frames. After Bob obtains a Matching Result a bit will replace the symbol $\bullet$ in Tab. 5.

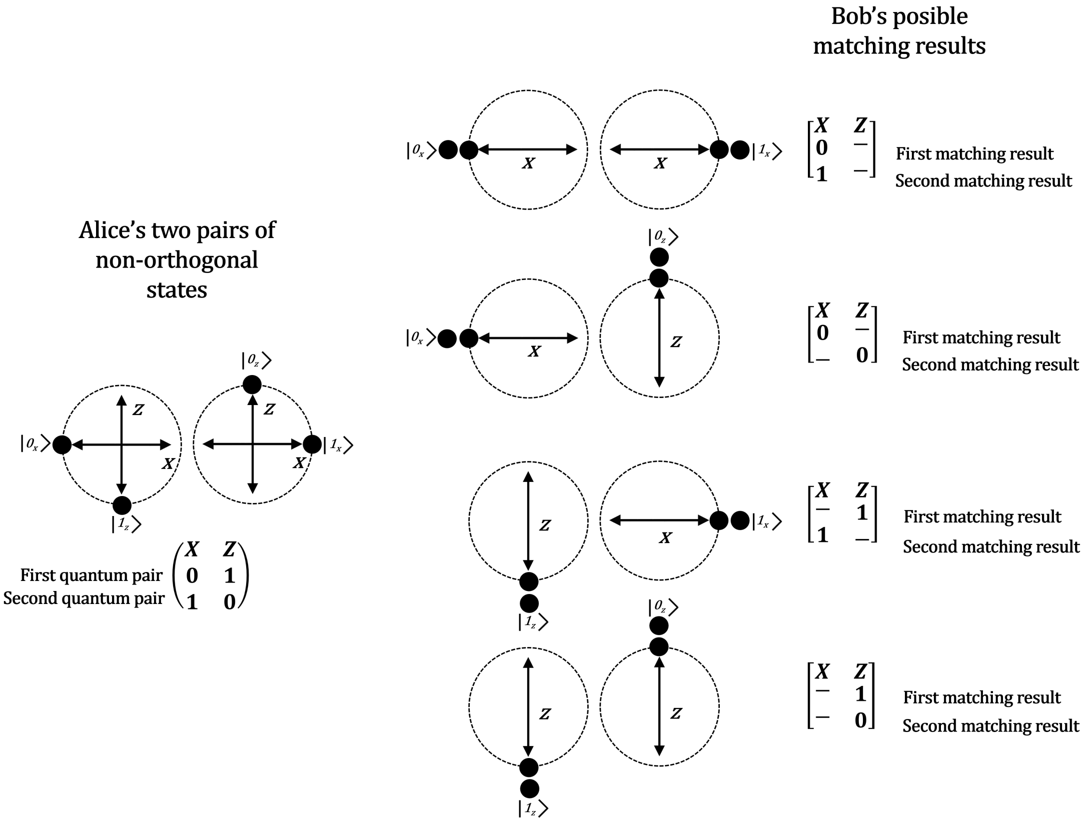

Fig. 8: We see (at left) the states prepared by Alice (two pairs of non-orthogonal states $(|0_X\rangle, |1_Z\rangle)$ and $(|1_X\rangle, |0_Z\rangle)$). After a double matching detection event is produced at Bob's side (in this example two double detection events) the possible matching results are exhibited at the right.

Each matching case has been identified with a binary code written at the top of each frame. The purpose of the sifting process is that Alice will realize Bob's Matching Results, so that they will share the corresponding binary code as secret bits.

Table 5: There exist four possible Matching Results (MR) for 2 × 2 frames. The double matching event is represented inside the frame with the symbol •. Additionally, each case has been identified with a binary code left to each frame. After the sifting process such code will become part of the secret key.

MR=00	$\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ \bullet & \\ \bullet & \end{pmatrix}$	MR=10	$\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ \bullet & \\ & \bullet \end{pmatrix}$
MR=01	$\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ & \bullet \\ & \bullet \end{pmatrix}$	MR=11	$\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ & \bullet \\ \bullet & \end{pmatrix}$

Now, let us enumerate the first steps of the sifting process which is based on frames:

1. Alice prepares a number of non-orthogonal states $(0_X, 0_Z)$, $(0_X, 1_Z)$, $(1_X, 0_Z)$ and $(1_X, 1_Z)$ and send them to Bob over the quantum channel (it was indicated that the pairs of quantum states are temporally separated each other, so users must agree previously the separating window).
2. Using a classical channel, Bob announces to Alice the double matching detection events.

4.3 Sifting bits based in the xor function

To complete the sifting process we will define the sifting bits as they are written at the bottom of each matching result (MR) in Tab. 7. To compute the sifting bits it must be applied the usual xor function to the vertical bits inside each column of the frame, taking a vacuum state as a zero bit. A simple example about the execution of the framed distillation can be found in the Appendix of this article.

The most important property of the sifting bits is that they cannot be derived from two distinct Matching Results as can be verified in Tab. 7. In other words, the sifting bits defines a complete set (without collisions) over the xor function.

At this point, it must result logical that not all the 2×2 frames can be used to establish a sifting process. Actually there are just 6 valid frames which are shown in Tab. 4. Now, we can complete the sifting process:

1. Alice prepares a number of non-orthogonal states $(0_X, 0_Z)$, $(0_X, 1_Z)$, $(1_X, 0_Z)$ and $(1_X, 1_Z)$ and send them to Bob over the quantum channel.
2. Using a classical channel, Bob announces to Alice the cases of double matching detection events.

3. Through the classical channel Bob reveals the sifting bits of each frame to Alice who derive the code of the Matching Result using Tab. 7 and Tab. 5. Since the sifting bits conform a complete binary set $\{00, 01, 10, 11\}$ Alice is allowed to identify Bob's Matching Results.
4. The secret bits they share are the bits that identify each matching result (according to Tab. 5).

5 Security of the sifting bits

For security reasons, the sifting bits cannot be correlated with a unique matching result. This property must be achieved to avoid an attacker derives the secret bits. The security property is demonstrated in Tab. 6.

Table 6: The sifting bits obtained by Bob (written at the bottom of each frame) must be produced from at least two different Matching Results. At the right of each frame we have indicated the corresponding original Alice's frame. Here, FMR stands for First Matching Result and SMR for Second Matching Result.

$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & 0 & - \\ \text{SMR} & - & 0 \\ \hline \text{sifting} & 0 & 0 \end{array}\ f_1$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & - & 0 \\ \text{SMR} & 0 & - \\ \hline \text{sifting} & 0 & 0 \end{array}\ f_5$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & 1 & - \\ \text{SMR} & 1 & - \\ \hline \text{sifting} & 0 & 0 \end{array}\ f_2, f_6$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & - & 1 \\ \text{SMR} & - & 1 \\ \hline \text{sifting} & 0 & 0 \end{array}\ f_3, f_4$
$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & - & 1 \\ \text{SMR} & - & 0 \\ \hline \text{sifting} & 0 & 1 \end{array}\ f_1, f_6$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & 0 & - \\ \text{SMR} & - & 1 \\ \hline \text{sifting} & 0 & 1 \end{array}\ f_3$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & - & 0 \\ \text{SMR} & - & 1 \\ \hline \text{sifting} & 0 & 1 \end{array}\ f_2, f_5$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & - & 1 \\ \text{SMR} & 0 & - \\ \hline \text{sifting} & 0 & 1 \end{array}\ f_4$
$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & 1 & - \\ \text{SMR} & 0 & - \\ \hline \text{sifting} & 1 & 0 \end{array}\ f_4, f_5$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & 0 & - \\ \text{SMR} & 1 & - \\ \hline \text{sifting} & 1 & 0 \end{array}\ f_1, f_3$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & - & 0 \\ \text{SMR} & 1 & - \\ \hline \text{sifting} & 0 & 1 \end{array}\ f_2$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & 1 & - \\ \text{SMR} & - & 0 \\ \hline \text{sifting} & 0 & 1 \end{array}\ f_6$
$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & - & 1 \\ \text{SMR} & 1 & - \\ \hline \text{sifting} & 1 & 1 \end{array}\ f_1, f_3, f_6$	$\begin{array}{lcc} & \mathbf{X} & \mathbf{Z} \\ \text{FMR} & 1 & - \\ \text{SMR} & - & 1 \\ \hline \text{sifting} & 1 & 1 \end{array}\ f_2, f_4, f_5$		

Table 7: To the left we see the 6 valid frames that Alice can prepare to be sent over the quantum channel. Provided Bob obtains the two (required) Matching Results he computes the sifting bits applying the xor function to each column (they are written at the bottom of each frame). The sifting bits which are publicly announced, conform a complete binary set $\{00, 01, 10, 11\}$ so that Alice can identify Bob's Matching Results. Here, FMR stands for First Matching Result and SMR means Second Matching Result.

Alice	Bob			
$\begin{array}{l}\text{First pair}\\ \text{Second pair}\end{array}\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\0&1\\1&0\end{pmatrix}\ f_1$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\0&-\\1&-\\ \hline 1&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\-&0\\ \hline 0&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\1&-\\ \hline 1&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\0&-\\-&0\\ \hline 0&0\end{bmatrix}$
$\begin{array}{l}\text{First pair}\\ \text{Second pair}\end{array}\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\1&0\\1&1\end{pmatrix}\ f_2$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\1&-\\ \hline 0&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&0\\-&1\\ \hline 0&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&0\\1&-\\ \hline 1&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\-&1\\ \hline 1&1\end{bmatrix}$
$\begin{array}{l}\text{First pair}\\ \text{Second pair}\end{array}\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\0&1\\1&1\end{pmatrix}\ f_3$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\0&-\\1&-\\ \hline 1&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\-&1\\ \hline 0&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\1&-\\ \hline 1&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\0&-\\-&1\\ \hline 0&1\end{bmatrix}$
$\begin{array}{l}\text{First pair}\\ \text{Second pair}\end{array}\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\1&1\\0&1\end{pmatrix}\ f_4$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\0&-\\ \hline 1&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\-&1\\ \hline 0&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\0&-\\ \hline 0&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\-&1\\ \hline 1&1\end{bmatrix}$
$\begin{array}{l}\text{First pair}\\ \text{Second pair}\end{array}\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\1&0\\0&1\end{pmatrix}\ f_5$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\0&-\\ \hline 1&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&0\\-&1\\ \hline 0&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&0\\0&-\\ \hline 0&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\-&1\\ \hline 1&1\end{bmatrix}$
$\begin{array}{l}\text{First pair}\\ \text{Second pair}\end{array}\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\1&1\\1&0\end{pmatrix}\ f_6$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\1&-\\ \hline 0&0\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\-&0\\ \hline 0&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\-&1\\1&-\\ \hline 1&1\end{bmatrix}$	$\begin{array}{l}\text{FMR}\\ \text{SMR}\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X}&\mathbf{Z}\\1&-\\-&0\\ \hline 1&0\end{bmatrix}$

The required exchange of messages of the (error-free) framing-based protocol is illustrated in Fig.9.

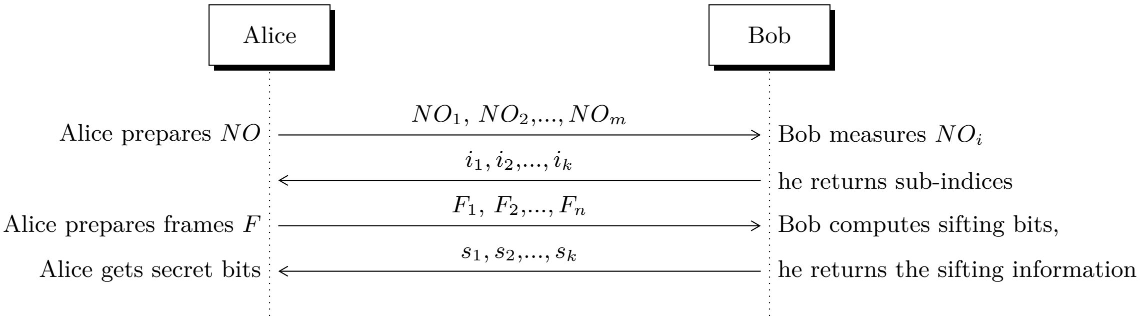

Fig. 9: The exchange of messages assuming an error free protocol. Here, NO represents the pairs of non-orthogonal states, the sub-indices i correspond to the measured pairs that arrive to Bob's station, F represents the frame arrangement information generated by Alice and s represents the sifting bits computed by Bob. To derive the secret bits Bob uses the codes listed in Tab.5 while Alice uses the received sifting bits.

6 Error correction

The method discussed so far does not allow error detection to discard erroneous transmissions produced in the quantum channel or the optical detection system. To make the frame distillation capable to identify erroneous detections we will proceed in the following manner: In addition to the sifting bits, Bob will reveal to Alice the measured bits obtained from the optical measurement system.

We define the Sifting String (SS) as a binary string composed by the sifting bits and the measured bits. A Sifting String SS is constructed as follows: SS= 1^{st} sifting bit || 2^{nd} sifting bit, 1^{st} measured bit || 2^{nd} measured bit.

As commented before, to preserve security, the Sifting String must be correlated to two Matching Results (MR). Then, a secret bit (denoted as sb) can be assigned to each MR as represented in Tab. 8. For example, consider that Bob announces the Sifting String (00,00), then the eavesdropper knows that there are two possible MR: 10 and 11. We have sb=0 for the first case and sb=1 for the second one (see Tab. 8).

The Sifting String allows Alice to detect the erroneous bits because SS reveals the sifting bits but also the measured bits. Provided Alice has sent an specific frame to Bob, he returns the SS which must be one of the listed in Tab. 9, otherwise an error is detected. However, some errors keep undetected because the SS falls within the set of valid SS. In the following section we will demonstrate an strategy to detect and correct all the errors produced in the channel and detection system.

As a final comment, double errors can be taken as single errors since, as we discuss next, every double detection event is combined with the rest of events.

Table 8: The Sifting String (SS) which is publicly announced is constructed with the sifting bits and the measured bits. To achieve a secret bit (sb) each SS must be correlated at least to two Matching Results (MR).

SS		MR	Frame	sb	MR	Frame	sb
sifting	measured	(see Tab. 5)	(see Tab. 4)		(see Tab. 5)	(see Tab. 4)	
00	00	10	f_1	0	11	f_5	1
00	11	00	f_2, f_6	0	01	f_3, f_4	1
01	10	01	f_1, f_6	0	11	f_4	1
01	01	10	f_3	0	01	f_2, f_5	1
10	01	00	f_1, f_3	0	11	f_2	1
10	10	00	f_4, f_5	0	10	f_6	1
11	11	11	f_1, f_3, f_6	0	10	f_2, f_4, f_5	1

Table 9: We list the set of valid Sifting String (SS) for each frame f_i. Provided Alice has sent an specific frame to Bob, he returns the SS which must be one of the listed here, otherwise an error is detected. We analyze if an error is detectable when occurs in the 1^{st} (or 2^{nd}) measured bit.

frame	Valid Sifting Strings (SS)	MR	1^{st} bit	detection	2^{nd} bit	detection	1^{st} and 2^{nd} bits	detection
f_1	$SS_{11} = 00, 00$	10	10,10	yes	01,01	yes	11,11	no
	$SS_{12} = 01, 10$	01	00,00	no	00,11	yes	01,01	yes
	$SS_{13} = 10, 01$	00	00,11	yes	00,00	no	10,10	yes
	$SS_{14} = 11, 11$	11	10,01	no	01,10	no	00,00	no
f_2	$SS_{21} = 00, 11$	00	10,01	no	10,10	yes	00,00	yes
	$SS_{22} = 01, 01$	01	00,11	no	00,00	yes	01,10	yes
	$SS_{23} = 10, 01$	11	11,11	no	00,00	yes	01,10	yes
	$SS_{24} = 11, 11$	10	01,01	no	10,10	yes	00,00	yes
f_3	$SS_{31} = 00, 11$	01	01,01	no	01,10	yes	00,00	yes
	$SS_{32} = 01, 01$	10	11,11	no	00,00	yes	10,10	yes
	$SS_{33} = 10, 01$	00	00,11	no	00,00	yes	10,10	yes
	$SS_{34} = 11, 11$	11	10,01	no	01,10	yes	00,00	yes
f_4	$SS_{41} = 00, 11$	01	01,01	yes	01,10	no	00,00	yes
	$SS_{42} = 01, 10$	11	00,00	yes	11,11	no	10,01	yes
	$SS_{43} = 10, 10$	00	00,00	yes	00,11	no	10,01	yes
	$SS_{44} = 11, 11$	10	01,01	yes	10,10	no	00,00	yes
f_5	$SS_{51} = 00, 00$	11	01,10	yes	10,01	yes	11,11	no
	$SS_{52} = 01, 01$	01	00,11	yes	00,00	no	01,10	yes
	$SS_{53} = 10, 10$	00	00,00	no	00,11	yes	10,01	yes
	$SS_{54} = 11, 11$	10	01,01	no	10,10	no	00,00	no
f_6	$SS_{61} = 00, 11$	00	10,01	yes	10,10	no	00,00	yes
	$SS_{62} = 01, 10$	01	00,00	yes	00,11	no	01,01	yes
	$SS_{63} = 10, 10$	10	00,00	yes	11,11	no	01,01	yes
	$SS_{64} = 11, 11$	11	10,01	yes	01,10	no	00,00	yes

doi:10.20944/preprints202004.0222.v1

6.1 Picking up undetected errors

Consider the undetected errors in Tab. 9 where the error is produced when 0_X is detected as 1_X or 0_Z as 1_Z. We describe here a method to identify them using an auxiliary quantum pair. We use for this purpose the auxiliary quantum pair $(0_X, 0_Z)$ that we call null quantum pair. Suppose Alice sends several pairs of null quantum pairs to Bob. After she receives the information about double matching detection events she can take advantage from the frames f_i where $i = 8, 9, 10$ and $i = 12, 13, 14$ of Tab. 4.

Consider the instances $(0_X, 1_Z)$, $(1_X, 0_Z)$, if measurement of 0_X yields error, it can be easily detected using the auxiliary null pair $(0_X, 0_Z)$. For the $(0_X, 1_Z)$ Alice finds the error if Bob responds SS=10,10 while the error in $(1_X, 0_Z)$ is identified with SS=01,10. The result is consistent as long as the null pair has been correctly measured by Bob which can be easily verified by Alice using several others null pairs. A convenient method to remove errors in null pairs instances is to use frames f_7 (see Tab. 4) that always yield SS=00,00 otherwise such null pairs are useless and must be discarded. On the other hand, if after measurement of 1_Z in $(0_X, 1_Z)$ or $(1_X, 0_Z)$ yields error, it does not alter the explained method because in such cases we have SS=00,00 that does not produce any conflict (see Tab. 10).

As a final remark, instances where the error is produced when 1_X is detected as 0_X or 1_Z is measured as 0_Z cannot be detected and must be eliminated along with the null pairs. In the following section we synthesize the error correction model.

7 Error-correction security model

Since not all undetected errors in Tab. 8 are detectable as it is shown in Tab. 11 and Tab. 12 we define the error-correction security model as the method capable to correct all the errors while it preserves the security property: frames are only known by Alice and MRs known by Bob, while Bob's SS is assigned a bit 0 or 1.

- To distill secret bits, Alice will use only 4 frames which are listed in Tab. 13. To verify errors she will use 4 frames: f_7, f_8, f_9, f_{10} so we have that $\frac{1}{2}$ of the frames will be useful to be distilled.
- In case of errors, SS are correctable as demonstrated in Tab. 11 and Tab. 12. As implied from tables, half of the SS must be removed. So, after Alice informs to Bob which cases must be removed, those that come from SS $= (10, 01), (01, 01), (01, 10), (10, 10)$, they keep $\frac{1}{4}$ of the total frames (considering that $\frac{1}{2}$ of frames are usable). Also, frames f_j where $j = 7, \ldots, 10$ must be discarded because they are used to detect errors in the null quantum pairs and they do not add up secret bits.
- Since each SS comes from two different frames it can be related to one secret bit, this property is demonstrated in Tab. 14.

8 Privacy pre-amplification

If Bob informs Alice the positions of N double matching detection events she can construct $\binom{N}{2}$ frames. Since $\binom{N}{2} = \frac{N(N-1)}{2}$, it implies that the secret information hidden in the double matching detection events grows quadratically with the number of double detection events N. Enhancing the number of secret bits by exploiting this property is what we call privacy pre-amplification since it is

Table 10: If an error exists in 0_X when measuring the quantum pair $(0_X, 1_Z)$ or 0_Z in $(1_X, 0_Z)$ it can be easily detected using the auxiliary pair $(0_X, 0_Z)$. The first and third rows represent the error-free scenario (frames f_9 and f_{10}). The second and fourth rows show the erroneous behavior (the error occurs in the bit underlined).

Alice	Bob			
$f_9 \begin{pmatrix}\mathbf{X} & \mathbf{Z}\\ 0 & 1\\ 0 & 0\end{pmatrix}$	FMR SMR sifting $\mathrm{SS} = 00, 00$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 0 & -\\ 0 & -\\ \hline 0 & 0\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 01, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 1\\ - & 0\\ \hline 0 & 1\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 01, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 1\\ 0 & -\\ \hline 0 & 1\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 00, 00$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 0 & -\\ - & 0\\ \hline 0 & 0\end{array}\right]$
$f_9 \begin{pmatrix}\mathbf{X} & \mathbf{Z}\\ \underline{0} & 1\\ 0 & 0\end{pmatrix}$	FMR SMR sifting $\mathrm{SS} = 10, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ 0 & -\\ \hline 1 & 0\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 01, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 1\\ - & 0\\ \hline 0 & 1\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 01, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 1\\ 0 & -\\ \hline 0 & 1\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 10, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ - & 0\\ \hline 1 & 0\end{array}\right]$
$f_{10} \begin{pmatrix}\mathbf{X} & \mathbf{Z}\\ 1 & 0\\ 0 & 0\end{pmatrix}$	FMR SMR sifting $\mathrm{SS} = 10, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ 0 & -\\ \hline 1 & 0\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 00, 00$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 0\\ - & 0\\ \hline 0 & 0\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 00, 00$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 0\\ 0 & -\\ \hline 0 & 0\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 10, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ - & 0\\ \hline 1 & 0\end{array}\right]$
$f_{10} \begin{pmatrix}\mathbf{X} & \mathbf{Z}\\ 1 & \underline{0}\\ 0 & 0\end{pmatrix}$	FMR SMR sifting $\mathrm{SS} = 10, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ 0 & -\\ \hline 1 & 0\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 01, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 1\\ - & 0\\ \hline 0 & 1\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 01, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ - & 1\\ 0 & -\\ \hline 0 & 1\end{array}\right]$	FMR SMR sifting $\mathrm{SS} = 10, 10$ $\left[\begin{array}{cc}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ - & 0\\ \hline 1 & 0\end{array}\right]$

Table 11: Error correction map for undetected errors. From Tab. 9 we list all erroneous cases that keep undetected. In case an error is detected, the correcting code is represented. If no detection is found the item must be removed. As defined in the security model, the frame f_1 is useless and will not be computed.

frame	quantum pair i^{th}	Sifting String (SS)	detection	Sifting String (SS)	error-bit	correction code
f_1	$\begin{pmatrix} X & Z \\ 0 & \underline{1} \end{pmatrix}$	00,00 10,01	-	-	1^{st}	remove
	$\begin{pmatrix} X & Z \\ \underline{1} & 0 \end{pmatrix}$	00,00 01,10	-	-	2^{nd}	remove
f_2	$\begin{pmatrix} X & Z \\ \underline{1} & 0 \end{pmatrix}$	10,01 01,01	-	-	1^{st}	remove
	$\begin{pmatrix} X & Z \\ 1 & \underline{0} \end{pmatrix}$	00,11 11,11	f_0	01,10	1^{st}	SS_{22} SS_{23}
f_3	$\begin{pmatrix} X & Z \\ 0 & \underline{1} \end{pmatrix}$	01,01 10,01	-	-	1^{st}	remove
	$\begin{pmatrix} X & Z \\ \underline{0} & 1 \end{pmatrix}$	11,11 00,11	f_0	10,10	1^{st}	SS_{32} SS_{33}

Table 12: Error correction map for undetected errors (cont). Frame f_5 will be discarded by Alice.

frame	quantum pair i^{th}	Sifting String (SS)	detection	Sifting String (SS)	error-bit	correction
f_4	$\begin{pmatrix} X & Z \\ 0 & \underline{1} \end{pmatrix}$	01,10 10,10	-	-	2^{nd}	remove
	$\begin{pmatrix} X & Z \\ \underline{0} & 1 \end{pmatrix}$	11,11 00,11	f_0	10,10	2^{nd}	SS_{42} SS_{43}
f_5	$\begin{pmatrix} X & Z \\ \underline{1} & 0 \end{pmatrix}$	00,00 01,01	-	-	1^{st}	remove
	$\begin{pmatrix} X & Z \\ 0 & \underline{1} \end{pmatrix}$	00,00 10,10	-	-	2^{nd}	remove
f_6	$\begin{pmatrix} X & Z \\ 1 & \underline{0} \end{pmatrix}$	00,11 11,11	f_0	01,10	2^{nd}	SS_{62} SS_{63}
	$\begin{pmatrix} X & Z \\ \underline{1} & 0 \end{pmatrix}$	10,10 01,10	-	-	2^{nd}	remove

Table 13: Usable (4) frames, it must be included (4) frames f_7, f_8, f_9 and f_{10} to verify errors in the null quantum pairs.

usable frames			
$f_2 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$	$f_3 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$	$f_4 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$	$f_6 \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$

Table 14: If an error is detected using Tab. 10 (inside f_0), then Alice corrects the error according to Tab. 11 and Tab. 12. If no error is found Alice use the secret bits listed here.

SS	MR	Frame	sb	MR	Frame	sb
$\mathrm{SS}_{21} = \mathrm{SS}_{31} = \mathrm{SS}_{41} = \mathrm{SS}_{61} = 00, 11$	00	f_2, f_6	0	01	f_3, f_4	1
$\mathrm{SS}_{24} = \mathrm{SS}_{34} = \mathrm{SS}_{44} = \mathrm{SS}_{64} = 11, 11$	11	f_3, f_6	0	10	f_2, f_4	1
$\mathrm{SS}_{42} = \mathrm{SS}_{62} = 01, 10$	01	f_6	0	11	f_4	1
$\mathrm{SS}_{22} = \mathrm{SS}_{32} = 01, 01$	10	f_3	0	01	f_2	1
$\mathrm{SS}_{23} = \mathrm{SS}_{33} = 10, 01$	00	f_3	0	11	f_2	1
$\mathrm{SS}_{43} = \mathrm{SS}_{63} = 10, 10$	00	f_4	0	10	f_6	1

computed during the reconciliation phase of the distillation process. Normally, amplification occurs as a separated stage after sifting and reconciliation have been performed.

In the next section we will derive the secret key rate but before, let us introduce some important properties of the frame-based reconciliation protocol:

Throughput. The throughput of the framed reconciliation can be computed as $\binom{N}{2} = \frac{N(N-1)}{2}$ the throughput of the protocol varies quadratically $O(N^2)$ with the number of the double matching detection vents N.

Effective throughput speed. We have $\frac{1}{2}$ of the frames are usable and $\frac{1}{2}$ is the correction gain. Therefore, the number of secret bits is $\frac{1}{4}\binom{N}{2} = \frac{1}{8}N(N-1) \sim N^2$. A running example of the framed reconciliation is shown in Appendix A. If $N = 1000$, the number of secret bits is around 10^5. Since the errors can be removed in no more than tens of milliseconds, the throughput speed achieves 10^6 bps. Such speed can be further enhanced applying a bigger N and using more computational resources as shown in Tab. 15.

Efficiency. The minimum number of required bits to reconcile the shared frames is $2(n^2 - n)$ bits (because there are four reveled bits per frame), but also the total number of revealed bits is $2(n^2 - n)$, so the efficiency of the protocol achieves unity.

Round trips. Although this protocol is an interactive reconciliation protocol, it only requires four rounds to be completed. Just a single transmission (from Alice to Bob) is needed for correction bits (the indices of events that must removed and those of the erroneous detection events). No redundant information is required. Other protocols require tens of parity check passes [21]. No extra permutation or interleaving is required to achieve reconciliation.

QBER. As we will show in the security analysis section, the protocol remains secure although the eavesdropper could be equipped with unlimited quantum memory and multiple copies of Bob's quantum states. It is known that the photon number splitting attack (PNS) can be detected when the QBER of the channel is beyond 25% due to Eve's erroneous basis selection. By contrast, the security of the framed reconciliation method is invariant despite the number of copies that Eve obtains from the quantum channel therefore immune to the PNS attack. In this case, no estimation of the QBER from the quantum channel is needed. Remarkably, we do not see any limit in the QBER of the channel because a single auxiliary null quantum pair is enough to detect all the errors. Remember that each double detection event is combined with each other.

Since the matching basis of frames f_7 is $\frac{1}{2}$, in order to detect erroneous f_7 we have $(1-e)\frac{N}{2} \geq 1$ where e is the error rate and N is the number of frames f_7. Therefore, detection of erroneous null quantum pairs is possible if $e \leq 1 - \frac{2}{N}$. Suppose $N = 10$, then errors can be detected if $e \leq 0.8$.

9 The Photon Number Splitting Attack

Suppose Eve has a copy of all the quantum states that arrives to Bob's station. We realize that Eve can achieve just 25% of secret information. This is so because, from the captured pulses Eve

Table 15: Simulation of the protocol when have been registered 1000 double matching detection events. Tests were performed in an Intel Core i7-8750H 2.2 GHz, 12GB RAM.

QBER	time (ms)	secret bits	Throughput (Kbps)
5%	54.0146	59,873.7	1108.90435
10%	57.6022	58,911.2	1025.13229
15%	54.0614	52,630.1	972.532054
20%	55.6709	48,830.9	877.799205
25%	60.9381	46,706.4	773.520113
30%	78.4297	45,488.9	600.767144

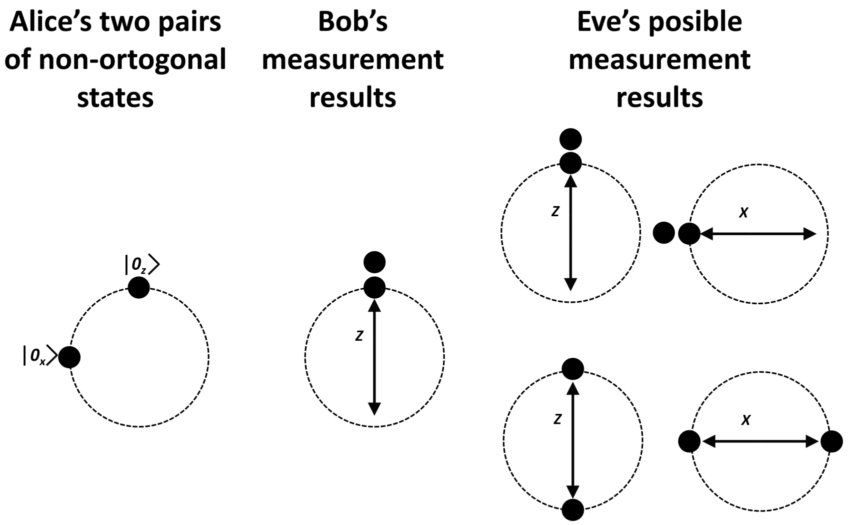
Alice's two pairs of non-ortogonal states
Bob's measurement results
Eve's posible measurement results
$|0_z\rangle$
$|0_x\rangle$
z
z
x
z
x

Fig. 10: Alice sends a pair of non-orthogonal states to Bob who obtains a double matching detection at his optical detectors. Eve has a copy of such states, however he has a 0.5 chance to choose the correct measurement basis. Furthermore, she has a 0.5 probability to get a double matching detection event. So, Eve's probability to get Bob's result is just 0.25.

must guess first the correct measurement basis which occur half of the times (see Fig. 10). Next, Eve must produce the corresponding double matching detection event.

For example, consider the eighth double detection events produced by Bob's station which are shown in Tab. 16 of Appendix A. Eve can produce just half of the double detection events, in this case four double detections. Then, due to basis matching she can derive only two successful results. In other words, Eve can capture just 25% of Alice and Bob secret information.

9.1 Optimal quantum measurement attack

Suppose Eve decide to measure looking for an optimal quantum measurement then she uses the measurement bases $X+Z$ or $X-Z$ as depicted at right in Fig. 11. Assuming Bob has registered a double matching detection event and Eve has a copy of those states sent by Alice, she can capture that information with 0.28125 probability. To see that, first consider that Eve choose the optimal measurement basis ($X+Z$ or $X-Z$) with 0.5 probability. Then, as shown in Fig.11 non-matching detection events are ambiguous for Eve, which occur with 0.375 probability. By contrast, she gets a double matching event with 0.5625 probability. As a result, the chance to get Bob's information is 0.28125.

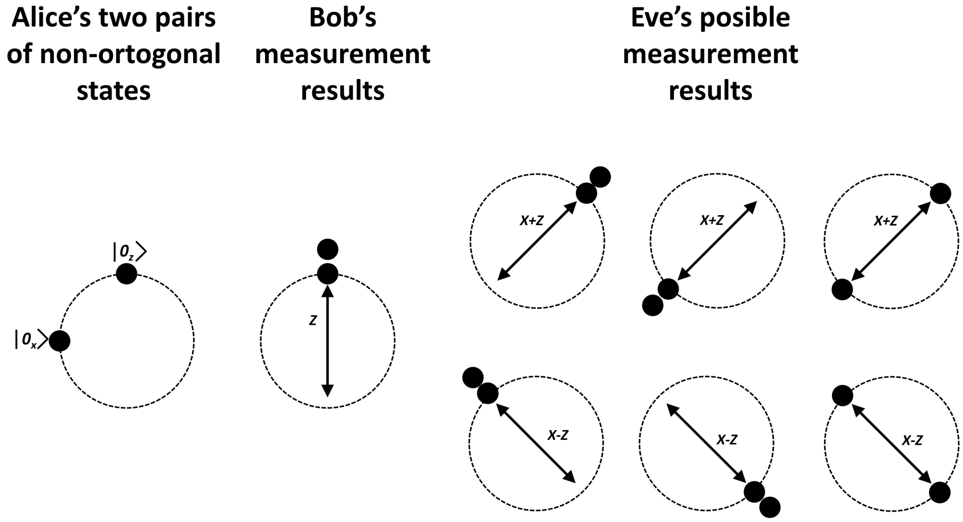
Alice's two pairs of non-ortogonal states
Bob's measurement results
Eve's posible measurement results
$|0_z\rangle$
$|0_x\rangle$
z
X+Z
X+Z
X+Z
X-Z
X-Z
X-Z

Fig. 11: Alice sends a pair of non-orthogonal states to Bob who obtains a double matching detection at his optical detectors. Eve has a copy of such states, however he has a 0.5 chance to choose the optimal measurement basis, in this case the $X-Z$ basis. Despite Eve choose the optimal quantum measurement basis, the chance to guess Bob's result is $\frac{9}{16}=0.5625$ while she obtains an inconclusive result with $\frac{6}{16}=0.375$. So the probability for Eve to get Bob's result is 0.28125.

Although is not our purpose to discuss here other possible optimal quantum attacks, this specific case shows that Eve's information increase is just residual.

10 The Secret Key Rate

In this section we will derive the mathematical relation to compute the secret bits gained by Alice and Bob in the presence of an attacker with unlimited quantum memory capacity.

The framed protocol involves measuring two pairs of $non-orthogonal$ states because frames has two rows. However, since the sifting process does not involve reveling bases Eve does not know Bob's measurement bases. So, the factors that affects unfavorably to Eve are:

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

Therefore, the total matching ratio for Bob is $\frac{1}{2}$ and $\frac{1}{4}$ for Eve. Suppose Eve obtains a copy of each state capturing the multi-photon pulses emitted by Alice equipped with a photonic source that follows a Poisson distribution. Eve behaves according to the following strategy:

- Eve uses the announced information about Bob's pairs, therefore she arranges her states in the corresponding pairs, say $Q_{(i,j)}$.
- Assume that Eve has at least one copy of all Bob's pairs so that $\sum Q_{(i,j)} = \frac{1}{2}Q_{(+,+)}$.
- Eve measures her quantum pairs to produce double matching events. However, as indicated before Eve's matching ratio is $\frac{1}{4}$.

Let Δi_{ab} be the secret key rate between Alice and Bob, so we deduced the relation of Eq. 1.

$$\Delta i_{ab} = \frac{1}{2}Q_{(+,+)} - \frac{1}{4}\sum Q_{(i,j)} \tag{1}$$

To ensure secrecy of the shared bits it must full filed $\Delta i > 0$, in Eq. 2 we have indicated such condition:

$$\Delta i_{ab} = 1 - \frac{1}{4} = \frac{3}{4} \tag{2}$$

Which indicates that Eve subtracts 25% of the shared information. In view of this result, we deduced that the eavesdropper cannot implement the PNS attack, then she could opt for a channel substitution attack. Thus, it could be better to implement this method across a wireless transmission medium. Up to our knowledge this the first QKD protocol capable to distill secret bits applying less attenuated quantum pulses between the two remote stations. An interesting opportunity for this scheme is to use quantum continuous variables (CV-QKD) because it does no require multiple matching detection events.

10.1 Secret throughput speed

Let us represent the shared information between Alice and Bob after they executed privacy preamplification as $I_{ab} = \frac{1}{4}\binom{N}{2} = \frac{1}{8}N(N-1)$ where N is the number of double matching detection events. As discussed in the previous section, Eve can obtain 25% of the shared secret information, so Eve can distill $I_{ae} = \frac{1}{4}\binom{\frac{N}{4}}{2} = \frac{1}{8}\left(\frac{N}{4}\left(\frac{N}{4}-1\right)\right)$, now we can derive the secret throughput speed $\Delta I_{ab} = I_{ab} - I_{ae}$ as indicated by Eq. 3.

$$\Delta I_{ab} = \frac{1}{8}\left(1 - \frac{1}{16}\right)N^2 - \frac{1}{8}\left(1 - \frac{1}{4}\right)N \tag{3}$$

10.2 Throughput speed with optimal quantum measurement

We know that the information shared between Alice and Bob is $I_{ab} = \frac{1}{4}\binom{N}{2} = \frac{1}{8}N(N-1)$. If we consider the optimal quantum measurement case as discussed previously, Eve can extract $\frac{9}{32}$ of double matching events represented as N, so $I_{ae} = \frac{1}{8}\binom{\frac{9N}{32}}{2} = \frac{1}{8}\left(\frac{9N}{32}\left(\frac{9N}{32}-1\right)\right)$. Therefore, we can compute the secret throughput speed $\varDelta I_{ab}$ as written in Eq. 4.

$$\varDelta I_{ab} = \frac{1}{8}\left(1-\left(\frac{9}{32}\right)^2\right)N^2 - \frac{1}{8}\left(1-\frac{9}{32}\right)N \qquad (4)$$

11 Conclusions

We have introduced a new method for QKD distillation. The framed reconciliation approach integrates the sifting, reconciliation and amplification stages in a unique process. The method can be implemented as a software level over the usual optical equipment of a BB84 system.

The protocol produces fast the secret bits, convergence of the method is guaranteed, the method works under any QBER in the channel while the key is distilled secretly.

So far functionality of the method has been demonstrated computationally. The key grows quadratically in the number of the double detection events. The method does not require additional bits to estimate channel's parameters. Our analysis indicates that the protocol is not vulnerable to the PNS attack. Moreover, it opens the possibility to use less attenuated quantum pulses in the context of continuous variable QKD.

A Appendix

In this appendix we demonstrate a running example of framed reconciliation using 2×2 frames. For this simple example we assume that after measuring the quantum states that Alice sent to Bob, he has gotten 8 double matching events (enumerated from i_1 to i_8 in Tab. 16).

Alice proceeds to compute the total 28 combinations. Alice identifies just 10 valid frames (see Tab. 17). Then, she communicates to Bob the arrangement information to construct such frames. Now, Bob computes and returns the Sifting Strings, which contains the sifting bits and the measured bits (see Tab. 18). We show the resulting secret bits in Tab. 19. The secret bit (sb) of each Sifting String is derived according to Tab. 8.

Let us introduce an error in the detection event i_1. Alice must verify the presence of errors in the shared bits. When she evaluates i_1 with Tab. 10 Alice detects SS=10,10 which indicates that i_1 has been measured with error. Alice corrects the error according to Tab. 11 and she communicates to Bob the erroneous event.

Table 16: Bob announces to Alice eighth double matching detection events N=8 (enumerated from i_1 to i_8).

Bob's detection	Bob's public announcement	Alice's original pair
$\begin{bmatrix} X & Z \\ 0 & - \end{bmatrix}$	i_1	$\begin{pmatrix} X & Z \\ 0 & 1 \end{pmatrix}$
$\begin{bmatrix} X & Z \\ - & 0 \end{bmatrix}$	i_2	$\begin{pmatrix} X & Z \\ 0 & 0 \end{pmatrix}$
$\begin{bmatrix} X & Z \\ - & 1 \end{bmatrix}$	i_3	$\begin{pmatrix} X & Z \\ 0 & 1 \end{pmatrix}$
$\begin{bmatrix} X & Z \\ 1 & - \end{bmatrix}$	i_4	$\begin{pmatrix} X & Z \\ 1 & 1 \end{pmatrix}$
$\begin{bmatrix} X & Z \\ - & 0 \end{bmatrix}$	i_5	$\begin{pmatrix} X & Z \\ 1 & 0 \end{pmatrix}$
$\begin{bmatrix} X & Z \\ - & 1 \end{bmatrix}$	i_6	$\begin{pmatrix} X & Z \\ 1 & 1 \end{pmatrix}$
$\begin{bmatrix} X & Z \\ 0 & - \end{bmatrix}$	i_7	$\begin{pmatrix} X & Z \\ 0 & 1 \end{pmatrix}$
$\begin{bmatrix} X & Z \\ 1 & - \end{bmatrix}$	i_8	$\begin{pmatrix} X & Z \\ 1 & 0 \end{pmatrix}$

Table 17: Alice constructs the set of valid frames, and she informs Bob the frame arrangement information: $\{1.f_3 = (i_1, i_4), 2.f_3 = (i_1, i_6), 3.f_3 = (i_3, i_4), 4.f_3 = (i_3, i_6),$ $5.f_6 = (i_4, i_5), 6.f_4 = (i_4, i_7), 7.f_6 = (i_4, i_8), 8.f_2 = (i_5, i_6), 9.f_4 = (i_6, i_7), 10.f_6 = (i_6, i_8)\}$.

i - frame	i - frame	i - frame	i - frame
1. $\begin{array}{c} \\ i_1 \\ i_4 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 1 & 1 \end{pmatrix} f_3$	3. $\begin{array}{c} \\ i_3 \\ i_4 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 1 & 1 \end{pmatrix} f_3$	5. $\begin{array}{c} \\ i_4 \\ i_5 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 1 & 0 \end{pmatrix} f_6$	
		6. $\begin{array}{c} \\ i_4 \\ i_7 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 0 & 1 \end{pmatrix} f_4$	9. $\begin{array}{c} \\ i_6 \\ i_7 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 0 & 1 \end{pmatrix} f_4$
2. $\begin{array}{c} \\ i_1 \\ i_6 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 1 & 1 \end{pmatrix} f_3$	4. $\begin{array}{c} \\ i_3 \\ i_6 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 0 & 1 \\ 1 & 1 \end{pmatrix} f_3$	7. $\begin{array}{c} \\ i_4 \\ i_8 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 1 & 0 \end{pmatrix} f_6$	10. $\begin{array}{c} \\ i_6 \\ i_8 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 1 \\ 1 & 0 \end{pmatrix} f_6$
		8. $\begin{array}{c} \\ i_5 \\ i_6 \end{array}\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ 1 & 0 \\ 1 & 1 \end{pmatrix} f_2$	

Table 18: Bob publishes the Sifting String that contains the sifting bits and the measured bits. Alice deduces MR and associates the corresponding secret bit (sb) (see also Tab. 8).

1. $\begin{array}{c}\text{MR=00}\\ i_1\\ i_4\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ 0 & -\\ 1 & -\\ \hline 1 & 0\end{bmatrix} f_3$	3. $\begin{array}{c}\text{MR=11}\\ i_3\\ i_4\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ - & 1\\ 1 & -\\ \hline 1 & 1\end{bmatrix} f_3$	5. $\begin{array}{c}\text{MR=10}\\ i_4\\ i_5\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ - & 0\\ \hline 1 & 0\end{bmatrix} f_6$	
		6. $\begin{array}{c}\text{MR=00}\\ i_4\\ i_7\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ 0 & -\\ \hline 1 & 0\end{bmatrix} f_4$	9. $\begin{array}{c}\text{MR=11}\\ i_6\\ i_7\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ - & 1\\ 0 & -\\ \hline 0 & 1\end{bmatrix} f_4$
2. $\begin{array}{c}\text{MR=10}\\ i_1\\ i_6\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ 0 & -\\ - & 1\\ \hline 0 & 1\end{bmatrix} f_3$	4. $\begin{array}{c}\text{MR=01}\\ i_3\\ i_6\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ - & 1\\ - & 1\\ \hline 0 & 0\end{bmatrix} f_3$	7. $\begin{array}{c}\text{MR=00}\\ i_4\\ i_8\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ 1 & -\\ 1 & -\\ \hline 0 & 0\end{bmatrix} f_6$	10. $\begin{array}{c}\text{MR=11}\\ i_6\\ i_8\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ - & 1\\ 1 & -\\ \hline 1 & 1\end{bmatrix} f_6$
		8. $\begin{array}{c}\text{MR=01}\\ i_5\\ i_6\\ \text{sifting}\end{array}\begin{bmatrix}\mathbf{X} & \mathbf{Z}\\ - & 0\\ - & 1\\ \hline 0 & 1\end{bmatrix} f_2$	

Table 19: Alice and Bob derive the secret bits according to Tab. 8. In is this example the number of secret bits is 5 which is consistent with the relation $\frac{1}{4}\binom{8}{2} = 7$.

item	SS	Alice's frame	Bob's MR	sb
1.	$\text{SS}_{33} = 10, 01$	f_3	00	remove
2.	$\text{SS}_{32} = 01, 01$	f_3	10	remove
3.	$\text{SS}_{34} = 11, 11$	f_3	11	0
4.	$\text{SS}_{31} = 00, 11$	f_3	01	1
5.	$\text{SS}_{63} = 10, 10$	f_6	10	remove
6.	$\text{SS}_{43} = 10, 10$	f_4	00	0
7.	$\text{SS}_{61} = 00, 11$	f_6	00	0
8.	$\text{SS}_{22} = 01, 01$	f_2	01	remove
9.	$\text{SS}_{42} = 01, 10$	f_4	11	remove
10.	$\text{SS}_{64} = 11, 11$	f_6	11	0

Table 20: In this example i_1 is erroneous. Alice found the error evaluating i_1 inside f_0 as indicated in Tab. 10. Then, Alice corrects the error using Tab. 11.

item	events	error-free SS	frame	erroneous SS	Operation to be implemented
1.	(i_1, i_4)	$\mathrm{SS}_{33} = 10, 01$	f_3	00,11	correct applying SS_{33}
2.	(i_1, i_6)	$\mathrm{SS}_{32} = 01, 01$	f_3	11,11	correct applying SS_{32}

Bibliography

[1] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A*, vol. 75, no. 3, p. 032314, 2007.

[2] F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," *New Journal of Physics*, vol. 12, no. 11, p. 113026, 2010.

[3] V. Makarov* and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005.

[4] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A*, vol. 74, no. 2, p. 022313, 2006.

[5] V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on sarg04, phase-time, dpsk, and ekert protocols," *Quantum Information & Computation*, vol. 8, no. 6, pp. 622–635, 2008.

[6] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *arXiv preprint quant-ph/0512080*, 2005.

[7] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[8] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature communications*, vol. 2, p. 349, 2011.

[9] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, no. 1, p. 013043, 2011.

[10] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, no. 7, p. 073024, 2011.

[11] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, no. 5, p. 057901, 2004.

[12] L. Lizama, J. M. Lopez, E. D. C. López, and S. E. Venegas-Andraca, "Enhancing quantum key distribution (qkd) to address quantum hacking," *Procedia Technology*, vol. 3, pp. 80–88, 2012.

[13] L. A. Lizama-Pérez, J. M. López, E. De Carlos-López, and S. E. Venegas-Andraca, "Quantum flows for secret key distribution in the presence of the photon number splitting attack," *Entropy*, vol. 16, no. 6, pp. 3121–3135, 2014.

[14] L. A. Lizama-Pérez, J. M. López, and E. De Carlos López, "Quantum key distribution in the presence of the intercept-resend with faked states attack," *Entropy*, vol. 19, no. 1, p. 4, 2016.

[15] L. A. Lizama-Pérez and J. M. López, "Quantum flows for secret key distribution," *Advanced Technologies of Quantum Key Distribution*, p. 37, 2018.

[16] K. Kuritsyn, "Modification of error reconciliation scheme for quantum cryptography," in *First International Symposium on Quantum Informatics*, vol. 5128, pp. 91–94, International Society for Optics and Photonics, 2003.

[17] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 410–423, Springer, 1993.

[18] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. Nickel, C. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A*, vol. 67, no. 5, p. 052303, 2003.

[19] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed gaussian key," *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 394–400, 2004.

[20] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *Information Theory, IEEE Transactions on*, vol. 41, no. 6, pp. 1915–1923, 1995.

[21] T. I. Calver, "An empirical analysis of the cascade secret key reconciliation protocol for quantum key distribution," 2011.

[22] N. Benletaief, H. Rezig, and A. Bouallegue, "Toward efficient quantum key distribution reconciliation," *arXiv preprint arXiv:2002.04887*, 2020.