 doi:10.20944/preprints202012.0523.v1

Beyond the limits of Shannon's information in quantum key distribution

Luis A. Lizama-Perez[1][0000−0001−5109−2927] and J. Mauricio López[2] and Emmanuel H. Samperio[1]

Sección de Posgrado de la Universidad Politécnica de Pachuca,
Ex-Hacienda de Santa Bárbara, 43830, México
luislizama@upp.edu.mx
esamperio593@micorreo.upp.edu.mx
Cinvestav Querétaro, Libramiento Norponiente 2000,
Real de Juriquilla, 76230, Santiago de Querétaro, Querétaro, México
jm.lopez@cinvestav.mx

Abstract. We present a new post-processing method for Quantum Key Distribution (QKD) that raise 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 then it is 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, it just require 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.

1 Introduction

To put it in historical context, fiber optic telecommunications over long distances was possible until manufacturing techniques were developed that improved drastically its efficiency. 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, it has become unpostponable the development of new techniques for the rapid establishment of secret key information using quantum pulses over long distances [2–4].

Unfortunately, some factors prevent QKD becomes 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 [5, 6]. On the one hand, noise provides the possibility for an attacker to disguise himself and on the other hand it imposes severe difficulties to correct the errors produced during transmission in order to derive two identical cryptographic keys at both sides of the quantum link [7, 8]. 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% [9].

 doi:10.20944/preprints202012.0523.v1

In the past years, we have developed a new scheme for quantum key distribution called quantum flows [10–12] capable to resist challenging attacks [13–23]. 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 has 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 unique our method in the context of QKD distillation, moreover it accelerates convergence and produces key that grows cubically in the number of double detection events.

In this work we enhance the framed reconciliation method showed previously for 2X2 frames [12] and we discuss that framed reconciliation can surpass Shannon's information bounds for noisy channels. We strongly recommend the reader consult our previous work on Quantum Key Distillation Using Binary Frames, so we can keep the present article being 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 2X2 frames, which are the frames with the minimum size, we discuss here 3X2 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 a information signal, that she sends over a noisy channel, but it corrupts or at least part of it due to the presence of noise in the channel [24, 25]. 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 [26–30]. Shannon theory implies that above 50% in the error rate of the channel is impossible that Bob recovers Alice's information. We call active (or real) information to the Shannon's model because it 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.

By contrast, in our approach, information is not enclosed in the transmitted quantum pulses but in the quantum bases that Bob chooses at the other side. As fact, measured bits are publicly announced but the measurement bases are never revealed. We designate reactive information to this kind of communication that we employ during the sifting QKD procedure.

Reactive bits are computed from Bob's measurement bases while errors produced in the Shannon's model are easily detected by Alice because such bits are publicly announced. Remarkably, in the presence of the unit error rate, information can still be recovered since errors gives reactive information by they self. For the same reason, not all Shannon's information can be recovered even in the absence of errors.

Before we introduce 3X2 frames we account for quantum communication through a simple example to explain our reconciliation method. To facilitate its exposition, we use 2X2 frames. Then, we discuss the role of auxiliary frames in the 2X2 case. In section 3 we address the research methodology for 3X2 frames and then we detail the QKD distillation protocol. To make the discussion more effective we have placed tables of 3X2 protocol in the Appendix A. Finally, in section 4 we analyze the efficiency and the security of the 3X2 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 [31–34] 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 measurement, 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 by the following reasons [12]:

- 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, that is 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 $1-i$ 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 want 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. Tab. 1 shows an hypothetical QKD protocol possibly based on BB84 where Alice has sent 18 quantum states (in practical implementations it must sacrificed some sifted bits to estimate the error rate of the channel). In this example a 30% error rate (e) is produced, so the QKD distillation process must be declined because prominent reconciliation algorithms as Cascade, Winnow or LDPC cannot work with this high error rate.

Table 1: In this example of a running 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 beyond 50% there is no reconcilable information.

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

 doi:10.20944/preprints202012.0523.v1

Suppose that the same errors are produced using the framed reconciliation method as it is illustrated in Fig. 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, as fact it can reconcile any error rate e in the channel so there is no need to estimate e wasting bits for this purpose. To simplify exposition in this example we used 2X2 frames but we will discuss 3X2 frames in the Distillation Method section.

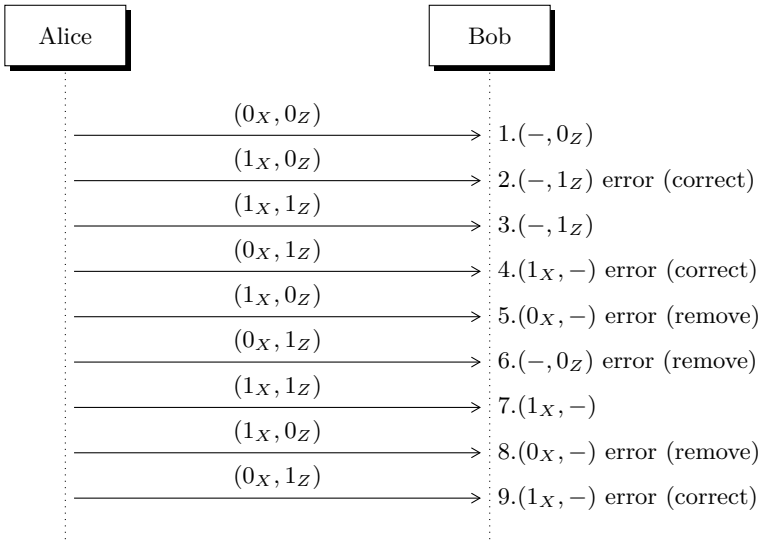


Fig. 1: Using frame reconciliation, all the errors are detected and corrected (or removed). Each double detection event has been enumerated to follow them into the frames (see Tabs. 2 and 3)

2.3 Auxiliary Frames

A major component of the framed reconciliation method relies in the auxiliary frames. Auxiliary frames are of two types: 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.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Table 2: Alice receives from Bob the SS which she knows that 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.

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

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

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

 doi:10.20944/preprints202012.0523.v1

1. To achieve reconciliation in Shannon's model, the first step is to ensure that auxiliary zero bits are error-free. However, Shannon's 2X1 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 2X1 frames there is a unique possible matching result (MR), that is written bellow, thus, no secret information can be derived from MRs in Shannon's model.

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

2. By contrast, using 2X2 frames, errors in the auxiliary frames can be easily identified. Here, we list the error-free zero frames:

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

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

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

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

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:

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

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

 doi:10.20944/preprints202012.0523.v1

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

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. As 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, we can see in Tab.4 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 [12], Bob must reveal the sifting bits along the measured bits. However, each SS maps two different MRs as it can be verified in Tab.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 3X2 frames.

3 Distillation Method with 3X2 frames

Before we detail the steps of the distillation method for 3X2 frames, let us describe the research methodology we applied:

1. It must be identified the 3X2 frames: there are $4^3 = 64$ binary 3X2 frames.
2. It must be specified the measurement results (MR): in 3X2 frames there are 8 MR. Those MR are illustrated in Tab. 10 of Appendix A.
3. Frames are classified as usable and useless frames: an usable frame is a frame that produce a distinct SS under each MR. In 3X2 frames there are 8 distinct SS per frame and 24 usable frames. Sifting bits are written in Tab. 12 of Appendix A. Remember that Sifting Strings (SS) are composed by the sifting bits and the measured bits: SS = 1^{st} sifting bit $||$ 2^{nd} sifting bit$||$ 3^{th} sifting bit, 1^{st} measured bit $||$ 2^{nd} measured bit$||$ 3^{th} measured bit.

 doi:10.20944/preprints202012.0523.v1

Table 5: The XOR function for 2X2 frames, 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

The 3^{th} sifting bit is appended to achieve discrimination, it can be considered as a parity sifting bit.

4. It must be identified auxiliary frames which are intended to catch errors produced in regular frames. In 3X2 frames there 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 (down) 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. At the final, Alice will include the auxiliary frames inside the set of frames that Bob must remove. Auxiliary frames are listed in Tab. 9 of Appendix A.
4. It must be expanded all usable frames under each MR and analyze errors through SS, from single to multiple errors. Then, it must be detected ambiguous SS that can be corrected under the auxiliary frames. Also, it can be identified all the SS that cannot be disambiguate and must be removed. We show in Tab. 13 the cases that can be successfully disambiguated.
5. 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. Also, 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 Eve'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. Tab. 11 of Appendix A enlists SS, MR, frames and sb.

Now, we can proceed to summarize the steps of the distillation method for 3X2 frames that comprises sifting, reconciliation and privacy amplification. The overall steps of the process are indicated in Fig.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 privacy amplification to this step.
4. Bob computes the Sifting String (SS) of each frame. He returns to Alice the set of Siting Strings he obtained.
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 Tab. 11 of Appendix A.
   – Alice informs Bob the cases that must be eliminated (because they cannot be disambiguate).
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 Tab. 11 of Appendix A.

4 Secret Rate

The secret rate of the framed reconciliation method can be derived directly from frames without recurring to quantum physics mathematical relations. Firstly, we must enlist the Sifting String (SS)

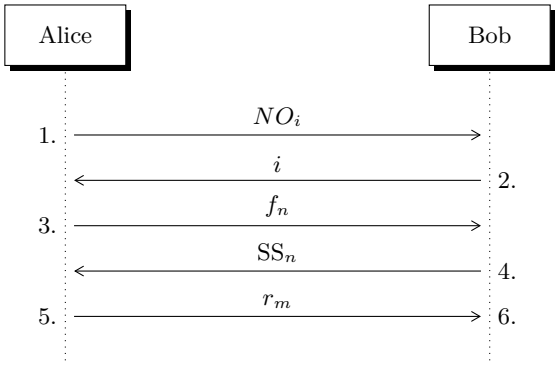


Fig. 2: The frame distillation runs in one iteration: Alice sends pairs of non-orthogonal states (NO_i). Bob informs to Alice which cases produced double matching detection events (i). Alice generates all possible frames and sends to Bob the frame arrangement information (f_n). Bob returns back the sifting 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.

generated by all the frames classified by Measurement Result (MR) and separating the error-free SS from the erroneous SS (single and multiple errors). According to the size of frames (2X2 or 3X2) the error could 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 Tab. 6 we detail the deduction of the secret rate. Each SS contributes with a single bit. In 2X2 frames we have 4 usable frames, 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 3X2 frames yields $\frac{1}{3}$ and the unequivocal error-free rate gives $\frac{1}{21}$.

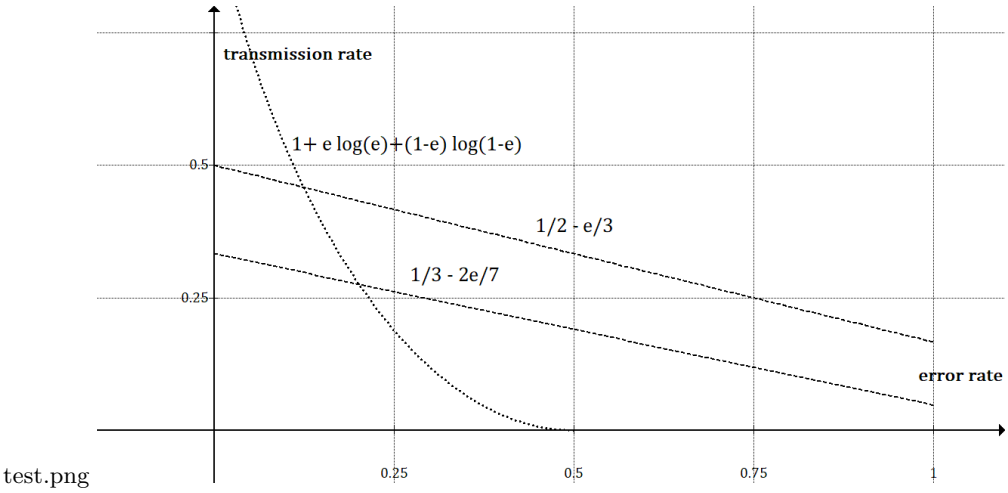
4.1 Secret Throughput

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 2X2 frames we have 4 usable frames

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

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

$I_{ab_{(2x2)}}$	$I_{ab_{(3x2)}}$
$\frac{1}{2}(1-e)+\frac{1}{6}e$	$\frac{1}{3}(1-e)+\frac{1}{21}e$
$\frac{1}{2}-\frac{1}{3}e$	$\frac{1}{3}-\frac{2}{7}e$
$e=0 \rightarrow I_{ab_{(2x2)}}=\frac{1}{2}$	$e=0 \rightarrow I_{ab_{(3x2)}}=\frac{1}{3}$
$e=1 \rightarrow I_{ab_{(2x2)}}=\frac{1}{6}$	$e=1 \rightarrow I_{ab_{(3x2)}}=\frac{1}{21}$



test.png

Fig. 3: The theoretical transmission rate is plotted as a function of the QBER e, we show the 2X2 and 3X2 graphs and the Shannon function. When $e = 1$ the secret rate achieves 0.16 for 2X2 frames and 0.047 for 3X2 frames.

 doi:10.20944/preprints202012.0523.v1

under 16 total frames, so the framing gain is $\frac{1}{4}\binom{n}{2}$. Conversely, the in 3X2 frames there are 24 over 64 frames, so the framing gain is $\frac{3}{8}\binom{n}{3}$. Eq. 2 describes the secret throughput for each case.

$$\begin{aligned} I_{ab_{(2x2)}} &= \frac{1}{4}\binom{n}{2}\left(\frac{1}{2}-\frac{1}{3}e\right) \\ I_{ab_{(3x2)}} &= \frac{3}{8}\binom{n}{3}\left(\frac{1}{3}-\frac{2}{7}e\right) \end{aligned} \tag{1}$$

Just to appreciate the growth rate of each frame size we compute in Tab. 7 some values of the secret throughput as a function of n and e. As it can be inferred, 3X2 frames has 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	$e=0$		$e=0.5$		$e=1$	
	$I_{ab_{(2x2)}}$	$I_{ab_{(3x2)}}$	$I_{ab_{(2x2)}}$	$I_{ab_{(3x2)}}$	$I_{ab_{(2x2)}}$	$I_{ab_{(3x2)}}$
100	618	20,212	412	11,550	206	2,887
500	15,593	2,588,562	10,395	1,479,178	5,197	369,794
1,000	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. For the case of 2X2 frames, the total information is $4\binom{n}{2}$ while the total number is $6\binom{n}{3}$ in 3X2 frames. The rate code for each size of frame is written in Eq. 2.

$$\begin{aligned} r_{ab_{(2x2)}} &= \frac{1}{16}\left(\frac{1}{2}-\frac{1}{3}e\right) \\ r_{ab_{(3x2)}} &= \frac{1}{16}\left(\frac{1}{3}-\frac{2}{7}e\right) \end{aligned} \tag{2}$$

4.3 Secret Key Rate

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

The Intercept and Resend Attack (IR). In the Intercept and Resend (IR) attack, Eve firstly measures each pair of non-orthogonal quantum pulses in the quantum channel, then she sends another pair of quantum pulses to Bob prepared according to the same quantum states. Since only one case matches Eve's double detection event, the probability to get the same result is $\frac{1}{5}$.

The Photon Number Splitting Attack (PNS). Eve has a copy of all the quantum states that arrives to Bob's station because Alice sends attenuated (multi-photon) quantum pulses and Eve is equipped with a sufficiently large quantum memory. However, Eve's probability to get a double matching detection event is 50%. In addition, Eve must measure choosing between two different measurement basis (X or Z) thus his final probability is $\frac{1}{4}$.

The Bases Choice Attack (BC). Eve would decide to apply another quantum measurement bases to gain more information, then she uses the measurement bases $X+Z$ or $X-Z$. First consider that Eve chooses between the measurement bases ($X+Z$ or $X-Z$) with 0.5 probability. However, non-matching detection events are ambiguous for Eve, which occur with $\frac{6}{16}$ probability. By contrast, she gets a double matching event with $\frac{9}{16}$ probability. As a result, the chance to get Bob's information is $\frac{9}{32}$.

Eq. 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 of Alice and those Eve can duplicate.

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

Tab. 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 2X2 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
$\left(1-(\frac{1}{5})^2\right)\cdot I_{ab_{(2x2)}}$	$\left(1-(\frac{1}{4})^2\right)\cdot I_{ab_{(2x2)}}$	$\left(1-(\frac{9}{32})^2\right)\cdot I_{ab_{(2x2)}}$
$\left(1-(\frac{1}{5})^3\right)\cdot I_{ab_{(3x2)}}$	$\left(1-(\frac{1}{4})^3\right)\cdot I_{ab_{(3x2)}}$	$\left(1-(\frac{9}{32})^3\right)\cdot I_{ab_{(3x2)}}$

As it can be deduced from Tab. 8 the secret key rate is affected slightly by Eves' 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 side, portable QKD in closed buildings [35].

5 Conclusions

We have discussed a new post-processing method for Quantum Key Distribution (QKD) that raise 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, it just require a round iteration, no redundancy bits are sent and no limit in the correctable error percentage. Despite the reconciliation is performed with a unity error channel the secret rate is kept in 16% using 2X2 frames and 4.7% when using 3X2 frames.

It is not difficult to evaluate the security of this method because it can be evaluated directly through the frames. There are 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.

A Appendix

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

- Tab. 9 describes the complete set of 3X2 frames.
- MR are illustrated in Tab. 10.
- Tab. 11 enlists SS, MR, frames and sb.
- Sifting bits are written in Tab. 12.
- Tab. 13 show the cases that can be successfully disambiguated.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Table 9: There are 24 useful frames: f_i, where $i = 1, \ldots, 24$ and 3 Auxiliary frames f_j, where $j = 25, \ldots, 27$.

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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Table 10: There exist eighth possible Matching Results (MR) for 3X2 frames. The bit produced by a double matching event is represented inside the ket notation with the symbol •. 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 $\begin{pmatrix} \vert\bullet_X\rangle & - \\ \vert\bullet_X\rangle & - \\ \vert\bullet_X\rangle & - \end{pmatrix}$	MR=100 $\begin{pmatrix} \vert\bullet_X\rangle & - \\ \vert\bullet_X\rangle & - \\ - & \vert\bullet_Z\rangle \end{pmatrix}$
MR=001 $\begin{pmatrix} - & \vert\bullet_Z\rangle \\ - & \vert\bullet_Z\rangle \\ - & \vert\bullet_Z\rangle \end{pmatrix}$	MR=101 $\begin{pmatrix} - & \vert\bullet_Z\rangle \\ - & \vert\bullet_Z\rangle \\ \vert\bullet_X\rangle & - \end{pmatrix}$
MR=010 $\begin{pmatrix} \vert\bullet_X\rangle & - \\ - & \vert\bullet_Z\rangle \\ \vert\bullet_X\rangle & - \end{pmatrix}$	MR=110 $\begin{pmatrix} \vert\bullet_X\rangle & - \\ - & \vert\bullet_Z\rangle \\ - & \vert\bullet_Z\rangle \end{pmatrix}$
MR=011 $\begin{pmatrix} - & \vert\bullet_Z\rangle \\ \vert\bullet_X\rangle & - \\ - & \vert\bullet_Z\rangle \end{pmatrix}$	MR=111 $\begin{pmatrix} - & \vert\bullet_Z\rangle \\ \vert\bullet_X\rangle & - \\ \vert\bullet_X\rangle & - \end{pmatrix}$

Table 12: We list the 24 frames that Alice uses during the distillation process. Bob computes the sifting bits applying the xor function to each column (they are written at the bottom of each frame) and appending an extra (required) sifting bit. The sifting bits define the set $\{000, 001, 010, 011, 100, 101, 110, 111\}$ that does not contain redundancy, so that Alice can identify without ambiguity Bob's Matching Results.

Alice	Bob
$f_1 = \begin{pmatrix} \vert 0_X\rangle & \vert 0_Z\rangle \\ \vert 0_X\rangle & \vert 1_Z\rangle \\ \vert 1_X\rangle & \vert 0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \vert 0_X\rangle & - \\ \vert 0_X\rangle & - \\ \vert 1_X\rangle & - \end{pmatrix}$ $1\ 0\ 0$ $\quad \begin{pmatrix} - & \vert 0_Z\rangle \\ - & \vert 1_Z\rangle \\ - & \vert 0_Z\rangle \end{pmatrix}$ $0\ 1\ 0$ $\quad \begin{pmatrix} \vert 0_X\rangle & - \\ - & \vert 1_Z\rangle \\ \vert 1_X\rangle & - \end{pmatrix}$ $1\ 1\ 0$ $\quad \begin{pmatrix} - & \vert 0_Z\rangle \\ \vert 0_X\rangle & - \\ - & \vert 0_Z\rangle \end{pmatrix}$ $0\ 0\ 0$ $\begin{pmatrix} \vert 0_X\rangle & - \\ \vert 0_X\rangle & - \\ - & \vert 0_Z\rangle \end{pmatrix}$ $0\ 0\ 1$ $\quad \begin{pmatrix} - & \vert 0_Z\rangle \\ - & \vert 1_Z\rangle \\ \vert 1_X\rangle & - \end{pmatrix}$ $1\ 1\ 1$ $\quad \begin{pmatrix} \vert 0_X\rangle & - \\ - & \vert 1_Z\rangle \\ - & \vert 0_Z\rangle \end{pmatrix}$ $0\ 1\ 1$ $\quad \begin{pmatrix} - & \vert 0_Z\rangle \\ \vert 0_X\rangle & - \\ \vert 1_X\rangle & - \end{pmatrix}$ $1\ 0\ 1$

Continued on the next page

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Alice	Bob			
$f_2 = \begin{pmatrix} \|1_X\rangle & \|0_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \\ \|0_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ $1\ 0\ \ 0$	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ $0\ 1\ \ 0$	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ $1\ 1\ \ 0$	$\begin{pmatrix} - & \|0_Z\rangle \\ \|0_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ $0\ 0\ \ 0$
	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ $1\ 0\ \ 1$	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ $0\ 1\ \ 1$	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ $1\ 1\ \ 1$	$\begin{pmatrix} - & \|0_Z\rangle \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ $0\ 0\ \ 1$
$f_3 = \begin{pmatrix} \|0_X\rangle & \|0_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ $1\ 0\ \ 0$	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|0_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ $0\ 1\ \ 0$	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ $0\ 0\ \ 0$	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ $1\ 1\ \ 0$
	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ $1\ 1\ \ 1$	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ $0\ 0\ \ 1$	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|0_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ $0\ 1\ \ 1$	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ $1\ 0\ \ 1$
$f_4 = \begin{pmatrix} \|1_X\rangle & \|0_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ $1\ 0\ \ 0$	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|0_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ $0\ 1\ \ 0$	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|0_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ $0\ 0\ \ 0$	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ $1\ 1\ \ 0$
	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ $0\ 1\ \ 1$	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|0_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ $1\ 0\ \ 1$	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|0_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ $1\ 1\ \ 1$	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ $0\ 0\ \ 1$
$f_5 = \begin{pmatrix} \|1_X\rangle & \|1_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \\ \|0_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ $1\ 0\ \ 0$	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ $0\ 0\ \ 0$	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ $1\ 1\ \ 0$	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ $0\ 1\ \ 0$
	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ $1\ 0\ \ 1$	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ $0\ 0\ \ 1$	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ $1\ 1\ \ 1$	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ $0\ 1\ \ 1$

Continued on the next page

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Alice	Bob			
$f_6 = \begin{pmatrix} \|1_X\rangle & \|0_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \\ \|0_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 0 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 1 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 1 1 1	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 0 1
$f_7 = \begin{pmatrix} \|0_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \\ \|0_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|0_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 1 0
	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 1 1	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|0_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 1 1
$f_8 = \begin{pmatrix} \|0_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|0_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|0_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 1 0
	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|0_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 1	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|0_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 1 1
$f_9 = \begin{pmatrix} \|1_X\rangle & \|0_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|0_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 1 1 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 1	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|0_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 1 1 1	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 0 1

Continued on the next page

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Alice	Bob			
$f_{10} = \begin{pmatrix} \lvert 1_X\rangle & \lvert 1_Z\rangle \\ \lvert 1_X\rangle & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & \lvert 0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \lvert 1_X\rangle & - \\ \lvert 1_X\rangle & - \\ \lvert 1_X\rangle & - \end{pmatrix}$ $1\ \ 0\ \ 0$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ - & \lvert 0_Z\rangle \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $0\ \ 1\ \ 0$	$\begin{pmatrix} \lvert 1_X\rangle & - \\ - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \end{pmatrix}$ $0\ \ 0\ \ 0$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ \lvert 1_X\rangle & - \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $1\ \ 1\ \ 0$
	$\begin{pmatrix} \lvert 1_X\rangle & - \\ \lvert 1_X\rangle & - \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $0\ \ 0\ \ 1$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \end{pmatrix}$ $1\ \ 1\ \ 1$	$\begin{pmatrix} \lvert 1_X\rangle & - \\ - & \lvert 0_Z\rangle \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $1\ \ 0\ \ 1$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ \lvert 1_X\rangle & - \\ \lvert 1_X\rangle & - \end{pmatrix}$ $0\ \ 1\ \ 1$
$f_{11} = \begin{pmatrix} \lvert 0_X\rangle & \lvert 1_Z\rangle \\ \lvert 1_X\rangle & \lvert 1_Z\rangle \\ \lvert 0_X\rangle & \lvert 0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ \lvert 1_X\rangle & - \\ \lvert 0_X\rangle & - \end{pmatrix}$ $1\ \ 0\ \ 0$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ - & \lvert 1_Z\rangle \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $0\ \ 1\ \ 0$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ - & \lvert 1_Z\rangle \\ \lvert 0_X\rangle & - \end{pmatrix}$ $0\ \ 1\ \ 0$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ \lvert 1_X\rangle & - \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $1\ \ 1\ \ 0$
	$\begin{pmatrix} \lvert 0_X\rangle & - \\ \lvert 1_X\rangle & - \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $1\ \ 0\ \ 1$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ - & \lvert 1_Z\rangle \\ \lvert 0_X\rangle & - \end{pmatrix}$ $0\ \ 0\ \ 1$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ - & \lvert 1_Z\rangle \\ - & \lvert 0_Z\rangle \end{pmatrix}$ $0\ \ 1\ \ 1$	$\begin{pmatrix} - & \lvert 1_Z\rangle \\ \lvert 1_X\rangle & - \\ \lvert 0_X\rangle & - \end{pmatrix}$ $1\ \ 1\ \ 1$
$f_{12} = \begin{pmatrix} \lvert 0_X\rangle & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & \lvert 1_Z\rangle \\ \lvert 0_X\rangle & \lvert 1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ \lvert 1_X\rangle & - \\ \lvert 0_X\rangle & - \end{pmatrix}$ $1\ \ 0\ \ 0$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ - & \lvert 1_Z\rangle \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $0\ \ 0\ \ 0$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ - & \lvert 1_Z\rangle \\ \lvert 0_X\rangle & - \end{pmatrix}$ $0\ \ 1\ \ 0$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $1\ \ 1\ \ 0$
	$\begin{pmatrix} \lvert 0_X\rangle & - \\ \lvert 1_X\rangle & - \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $1\ \ 1\ \ 1$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ - & \lvert 1_Z\rangle \\ \lvert 0_X\rangle & - \end{pmatrix}$ $0\ \ 1\ \ 1$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ - & \lvert 1_Z\rangle \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $0\ \ 0\ \ 1$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \\ \lvert 0_X\rangle & - \end{pmatrix}$ $1\ \ 0\ \ 1$
$f_{13} = \begin{pmatrix} \lvert 0_X\rangle & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & \lvert 1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ \lvert 1_X\rangle & - \\ \lvert 1_X\rangle & - \end{pmatrix}$ $0\ \ 0\ \ 0$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ - & \lvert 0_Z\rangle \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $0\ \ 1\ \ 0$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \end{pmatrix}$ $1\ \ 0\ \ 0$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $1\ \ 1\ \ 0$
	$\begin{pmatrix} \lvert 0_X\rangle & - \\ \lvert 1_X\rangle & - \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $1\ \ 1\ \ 1$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \end{pmatrix}$ $1\ \ 0\ \ 1$	$\begin{pmatrix} \lvert 0_X\rangle & - \\ - & \lvert 0_Z\rangle \\ - & \lvert 1_Z\rangle \end{pmatrix}$ $0\ \ 1\ \ 1$	$\begin{pmatrix} - & \lvert 0_Z\rangle \\ \lvert 1_X\rangle & - \\ \lvert 1_X\rangle & - \end{pmatrix}$ $0\ \ 0\ \ 1$

Continued on the next page

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Alice	Bob			
$f_{14} = \begin{pmatrix} \|1_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \\ \|0_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|0_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 1 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|0_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 1 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|0_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 1 1
$f_{15} = \begin{pmatrix} \|0_X\rangle & \|0_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|0_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 0	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|0_Z\rangle \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 0
	$\begin{pmatrix} \|0_X\rangle & - \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 1	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 1	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|0_Z\rangle \\ \|0_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 1
$f_{16} = \begin{pmatrix} \|0_X\rangle & \|1_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|0_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 0	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 0
	$\begin{pmatrix} \|0_X\rangle & - \\ \|0_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 1	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 1
$f_{17} = \begin{pmatrix} \|0_X\rangle & \|1_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|0_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 0
	$\begin{pmatrix} \|0_X\rangle & - \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 1	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 1

Continued on the next page

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2020 doi:10.20944/preprints202012.0523.v1

Alice	Bob			
$f_{18} = \begin{pmatrix} \|0_X\rangle\ \|0_Z\rangle \\ \|1_X\rangle\ \|1_Z\rangle \\ \|1_X\rangle\ \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 0 0
	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 1	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 1 1	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 0 1
$f_{19} = \begin{pmatrix} \|0_X\rangle\ \|1_Z\rangle \\ \|1_X\rangle\ \|1_Z\rangle \\ \|1_X\rangle\ \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 1 0 0
	$\begin{pmatrix} \|0_X\rangle & - \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 1 1 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 1	$\begin{pmatrix} \|0_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 1 1
$f_{20} = \begin{pmatrix} \|1_X\rangle\ \|0_Z\rangle \\ \|0_X\rangle\ \|1_Z\rangle \\ \|0_X\rangle\ \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|0_Z\rangle \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 1 1 1	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 1 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|0_Z\rangle \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 1
$f_{21} = \begin{pmatrix} \|1_X\rangle\ \|1_Z\rangle \\ \|0_X\rangle\ \|1_Z\rangle \\ \|0_X\rangle\ \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|0_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 1 1 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|0_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 0 1 1

Continued on the next page

Alice	Bob			
$f_{22} = \begin{pmatrix} \|1_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \\ \|0_X\rangle & \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 1 1 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 1 0 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ \|0_X\rangle & - \end{pmatrix}$ 0 0 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ \|0_X\rangle & - \end{pmatrix}$ 1 1 1
$f_{23} = \begin{pmatrix} \|1_X\rangle & \|0_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 0 0 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 0 1 0	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 1 1 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ - & \|1_Z\rangle \end{pmatrix}$ 0 1 1	$\begin{pmatrix} - & \|0_Z\rangle \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 1 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|1_Z\rangle \end{pmatrix}$ 1 0 1	$\begin{pmatrix} - & \|0_Z\rangle \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 0 1
$f_{24} = \begin{pmatrix} \|1_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|1_Z\rangle \\ \|1_X\rangle & \|0_Z\rangle \end{pmatrix}$	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 0	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 0	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 0 1 0	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 1 1 0
	$\begin{pmatrix} \|1_X\rangle & - \\ \|1_X\rangle & - \\ - & \|0_Z\rangle \end{pmatrix}$ 0 0 1	$\begin{pmatrix} - & \|1_Z\rangle \\ - & \|1_Z\rangle \\ \|1_X\rangle & - \end{pmatrix}$ 1 0 1	$\begin{pmatrix} \|1_X\rangle & - \\ - & \|1_Z\rangle \\ - & \|0_Z\rangle \end{pmatrix}$ 1 1 1	$\begin{pmatrix} - & \|1_Z\rangle \\ \|1_X\rangle & - \\ \|1_X\rangle & - \end{pmatrix}$ 0 1 1

Table 11: 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 hand 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}

 doi:10.20944/preprints202012.0523.v1

Table 13: We list the cases that can be successfully disambiguated. Zero cases refer to the error-free SS.

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

Continued on the next page

Frame	MR	SS	Erroneous bits
	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
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

1. K. C. Kao and G. A. Hockham, "Dielectric-fibre surface waveguides for optical frequencies," in *Proceedings of the Institution of Electrical Engineers*, vol. 113, pp. 1151–1158, IET, 1966.
2. M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, *et al.*, "Quantum key distribution: A networking perspective," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.
3. V. Lovic, "Quantum key distribution: Advantages, challenges and policy," 2020.
4. M. Razavi, A. Leverrier, X. Ma, B. Qi, and Z. Yuan, "Quantum key distribution and beyond: introduction," *JOSA B*, vol. 36, no. 3, pp. QKD1–QKD2, 2019.

5. M. Geihs, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, F. Günther, G. Alber, T. Walther, and J. Buchmann, "The status of quantum-key-distribution-based long-term secure internet communication," *IEEE Transactions on Sustainable Computing*, 2019.
6. P.-Y. Kong, "A review of quantum key distribution protocols in the perspective of smart grid communication security," *IEEE Systems Journal*, 2020.
7. D. Pearson, "High-speed qkd reconciliation using forward error correction," in *AIP Conference Proceedings*, vol. 734, pp. 299–302, American Institute of Physics, 2004.
8. R. J. Runser, T. Chapuran, P. Toliver, N. A. Peters, M. S. Goodman, J. T. Kosloski, N. Nweke, S. R. McNown, R. J. Hughes, D. Rosenberg, *et al.*, "Progress toward quantum communications networks: opportunities and challenges," in *Optoelectronic Integrated Circuits IX*, vol. 6476, p. 64760I, International Society for Optics and Photonics, 2007.
9. N. Lütkenhaus, "Estimates for practical quantum cryptography," *Physical Review A*, vol. 59, no. 5, p. 3301, 1999.
10. 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.
11. 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.
12. L. A. Lizama-Pérez and M. Lopez, "Quantum key distillation using binary frames," *Symmetry*, vol. 12, no. 6, p. 1053, 2020.
13. 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.
14. 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.
15. V. Makarov* and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
25. S. Verdu, "Fifty years of shannon theory," *IEEE Transactions on information theory*, vol. 44, no. 6, pp. 2057–2078, 1998.

26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. C. Bennett and G. Brassard, "Proc. of int. conf. on computers, systems, and signal processing," 1984.
32. G. Van Assche, *Quantum cryptography and secret-key distillation*. Cambridge University Press, 2006.
33. R. Hughes, J. Nordholt, and J. Rarity, "Summary of implementation schemes for quantum key distribution and quantum cryptography—a quantum information science and technology roadmap."
34. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.
35. V. Vinoth Kumar, T. Karthikeyan, P. Praveen Sundar, G. Magesh, and J. Balajee, "A quantum approach in lifi security using quantum key distribution," *International Journal of Advanced Science and Technology*, vol. 29, pp. 2345–2354, 2020.