entropy

Article

Quantum Key Distribution in the Presence of the Intercept-Resend with Faked States Attack

Luis Adrian Lizama-Pérez [1,*], José Mauricio López [2] and Eduardo De Carlos López [3]

[1] Graduate Department, Universidad Politécnica de Pachuca, Carretera Pachuca-Cd. Sahagún, Km. 20, Ex-Hacienda de Santa Bárbara, Municipio de Zempoala, Hidalgo 43830, Mexico
[2] General Management, Cinvestav Querétaro, Libramiento Norponiente 2000, Real de Juriquilla, Santiago de Querétaro, Querétaro 76230, Mexico; jm.lopez@cinvestav.mx
[3] Time and Frequency Laboratory, Centro Nacional De Metrología, Carretera a Los Cués Km. 4.5, El Marqués, Santiago de Querétaro, Querétaro 76246, Mexico; edlopez@cenam.mx
* Correspondence: luislizama@upp.edu.mx; Tel.: +52-771-547-7510

Academic Editor: James J. Park
Received: 3 November 2016; Accepted: 19 December 2016; Published: 23 December 2016

Abstract: Despite the unconditionally secure theory of the Quantum Key Distribution (QKD), several attacks have been successfully implemented against commercial QKD systems. Those systems have exhibited some flaws, as the secret key rate of corresponding protocols remains unaltered, while the eavesdropper obtains the entire secret key. We propose the negative acknowledgment state quantum key distribution protocol as a novel protocol capable of detecting the eavesdropping activity of the Intercept Resend with Faked Sates ($IRFS$) attack without requiring additional optical components different from the $BB84$ protocol because the system can be implemented as a high software module. In this approach, the transmitter interleaves pairs of quantum states, referred to here as parallel and orthogonal states, while the receiver uses active basis selection.

Keywords: biqubit; double matching; single compatible; detection event

1. Introduction

Quantum Key Distribution (QKD) represents a new cryptographic method to distribute a key between two remote users, usually called Alice and Bob [1]. QKD systems require legitimate users to authenticate each other through a public channel. The purpose of a QKD system is to generate secret bits that can be used to encrypt plaintext messages according to a simple xor function between the message and the secret key.

If an eavesdropper, commonly called Eve, tries to intercept the quantum channel to get the key, she will be detected. In such a case, Alice and Bob will discard the process before a key could be established. However, if they do not detect any eavesdropping activity, the quantum measurements can be used to derive the secret key [2]. After the transmission, Alice and Bob can compare a fraction of the exchanged key to see if there are any transmission errors caused by eavesdropping. QKD systems have been carried out experimentally through dedicated optical fibers, across free space, weak laser pulses or single photons, entangled photon pairs or continuous variables [3].

Ideally, the security of QKD protocols is supported by the properties of quantum mechanics, which make eavesdropping in the middle of the quantum channel detectable [1,4]. However, serious concerns arise at the technological level. Unfortunately, most of the promising QKD systems are vulnerable to quantum hacking due to loopholes in the optical detection system [5–15]. Under this scenario, new QKD methods must be developed to resist attacks related to such vulnerabilities as the Photon Number Splitting (PNS) and the Intercept and Resend with Faked States ($IRFS$) attacks [16,17].

In [18], we introduced a novel *QKD* protocol that uses weak coherent states and active basis measurement, capable of detecting the *PNS* eavesdropping activity. The strengths of the *ack state* (in [18] referred to as *ack QKD*) against *PNS* attack were discussed in [19]. In this paper, we extend the *ack state* protocol to the dual protocol *nack state* protocol to analyze its security against *IRFS* attack. One of the main advantages of the proposed protocol is that it protects against *IRFS* attack without requiring any changes in the hardware; only software changes are required. We do not discuss other attacks nor pretend to perform a general formal demonstration of its security.

2. Quantum Hacking in *QKD* Systems

A variety of attacks have been conceived of as exploiting the security of *BB*84-based systems, either theoretically or technologically. The Photon Number Splitting (*PNS*) attack can be included in the first category. In the second class, commonly referred to as quantum hacking, the Intercept Resend with Faked States (*IRFS*) attack can be mentioned, which exploits loopholes in the Avalanche Photo Diodes (*APD*s) of the electronic detection system. In the following section, we will describe the Intercept Resend (*IR*) attack and the Intercept-Resend with Faked States (*IRFS*).

(a) Intercept Resend (*IR*) attack

In the intercept resend attack, the eavesdropper measures each photon pulse sent by Alice, which she replaces with another pulse prepared in the quantum state that she has already measured. Eve is successful 50% of the time in measuring the pulse in the correct measurement basis, while Bob chooses half of the times the same basis as her; thus over time, she generates a Quantum Bit Error Rate (*QBER*) of $50\% \times 50\% = 25\%$ (see Figure 1 and [4]).

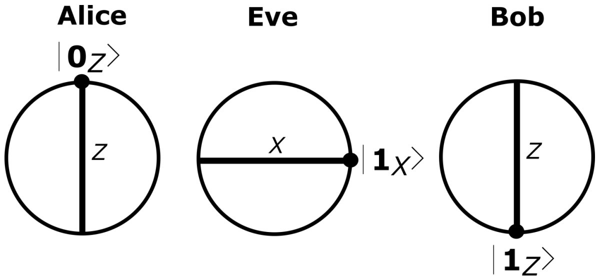

Figure 1. The Intercept Resend (*IR*) attack against the *BB*84 produces a detectable Quantum Bit Error Rate (*QBER*) of 25%. In the figure, Alice sends a $|0_Z\rangle$ state to Bob. However, Eve is in the middle of the quantum channel, and she applies the X basis measurement getting $|1_X\rangle$. Thus, she prepares a copy of such a state, and she resends it to Bob, who obtains $|1_Z\rangle$ because he used the Z basis measurement. This introduces a secret bit error because Alice expects that Bob obtained $|0_Z\rangle$.

(b) Intercept Resend with Faked States (*IRFS*) attack

In the Intercept Resend with Faked States (*IRFS*) attack, the eavesdropper is not interested in reconstructing the original states, but in producing instead pulses of that light that can be detected by Bob in a way that is controlled by her while she passes unnoticed in the quantum channel. The eavesdropper exploits imperfections of their optical system, so that Alice and Bob can assume that they are detecting the original quantum states while they are in fact detecting light pulses generated by Eve. These light pulses are called faked states [7]. To mount an *IRFS* attack, Eve can exploit some weaknesses of Bob's detector, such as time shift [8–10] or quantum blinding [7–9].

The quantum blinding attack is an *IRFS* attack where the *QKD* system is controlled by an eavesdropper using bright photon pulses during the linear mode operation of the *APD*s. In such attacks, Eve can eavesdrop on the full secret key without increasing the *QBER* of the protocol. In order to achieve this, the eavesdropper sends bright pulses to Bob's station that will be detected by the APD, which would operate like a classical photo diode, instead of operating in Geiger mode. Eve now can use the $IRFS$ attack to obtain the key [11,12].

As a result, as depicted in Figure 2a, if Bob chooses the same measurement basis as Eve, he gets a detection event in the corresponding APD detector. Otherwise, if Bob measures with the opposite basis as shown in Figure 2b, the optical power is distributed over the two detectors, and no event is detected. Thus, Eve blinds Bob's APDs detectors to make them operate as classical photo diodes. At the final stage of the protocol, Eve exploits the announcements revealed by Bob over the public channel to perform the classical post-processing, getting the same secret bits as Alice and Bob.

A simple countermeasure that can be applied in the electronic detection system is a watchdog detector that detects bright faked states [13]. The intercept-resend with faked states attack and quantum blinding were first implemented over a commercial QKD system at the University of Singapore [12].

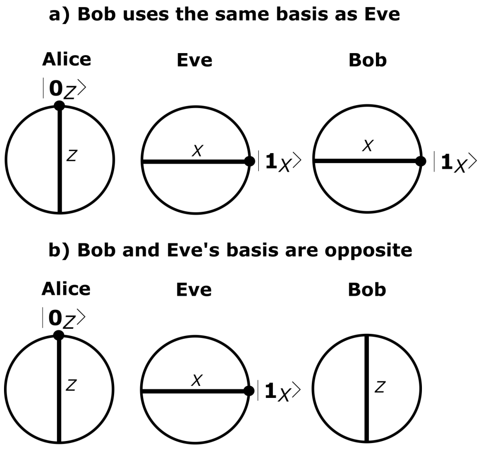
a) Bob uses the same basis as Eve
Alice
Eve
Bob
|0Z⟩
Z
X
|1X⟩
X
|1X⟩
b) Bob and Eve's basis are opposite
Alice
Eve
Bob
|0Z⟩
Z
X
|1X⟩
Z

Figure 2. In the quantum blinding Intercept Resend with Faked States ($IRFS$) attack, Eve uses the same optical receiver unit as Bob to detect Alice's states in a random basis. Then, she prepares those quantum states, but she sends her results to Bob as bright light pulses instead of quantum pulses. (**a**) Bob uses the same basis as Eve; (**b**) Bob and Eve's basis are opposite.

To conclude this section, we emphasize that the $IRFS$ attack works successfully on widely-used QKD protocols, namely $BB84$, $SARG04$, Differential Phase Shift ($DPSK$), Coherent One Way (COW), Ekert [9] and the *decoy state* method, as pointed out in [13,20]. The attack exhibits an extra 3 dB loss because of the basis mismatch between Eve and Bob. This is easily compensated in practice by Eve, since she may use better detector efficiencies and surpass loss in the channel. Blinding attacks over detectors have been demonstrated in two commercially available QKD systems [11]. It has been reported that Eve obtains the entire secret key while she remains undetected by the legitimate parties [12]. Finally, we remark that control detector attacks with active basis selection cause the gain from Eve to Bob be reduced by a half compared to the gain from Alice to Bob (see Figure 2 and Table A1 of Appendix A), according to the following rules [13]:

(i) For Bob's basis choice matching Eve's, the detector clicks deterministically;
(ii) For Bob's basis choice not matching Eve's, the faked state is not detected.

3. The *Nack State* Protocol

The *nack state* protocol is the dual version of the *ack state* protocol discussed in [19]. Both of them constitute a generalization of the well-known $BB84$. The *nack state* protocol uses pairs of parallel and orthogonal states instead of only single non-orthogonal state used in the $BB84$. This simple difference makes the *nack state* resilient to the $IRFS$ attack, as we will show later on. We chose the *nack* prefix to denote that provided Alice sends two quantum states to Bob, the second measurement acts as the negative acknowledgment (*nack*) of the previous one, because it yields the opposite bit result. In the rest of this section, we describe the *nack state* protocol, and in Section 4, we discuss how the *nack state* protocol is capable of detecting the $IRFS$ attack.

We refer to the pair of quantum states as a biqubit. To be more specific, the following biqubits are defined in the *nack state* protocol: four parallel biqubits $(|0_X\rangle, |0_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_X\rangle, |1_X\rangle)$, $(|1_Z\rangle, |1_Z\rangle)$ and two orthogonal biqubits $(|0_X\rangle, |1_X\rangle), (|0_Z\rangle, |1_Z\rangle)$. The parallel and orthogonal biqubits are randomly interleaved by Alice. The order of the quantum states within the biqubit does not affect the behavior of the protocol (see Figure 3). On the other side of the quantum channel, Bob measures two incoming states of a biqubit using the same measurement basis (X or Z). The *nack state* protocol can be described according to the following steps:

1. Alice is equipped with a photon source with an expected photon number μ that exhibits a Poisson distribution. Alice randomly chooses between a parallel or an orthogonal biqubit, and she prepares the biqubit to send it to Bob through the quantum channel;
2. Bob measures the biqubit (two incoming pulses) using the same measurement basis X (or Z) that he chooses randomly (in Section 4.2, we discuss that the consecutiveness of states can be avoided if Alice sends a burst of the first states of each pair, followed by a burst of the second states of each pair);
3. Bob announces publicly his measurement basis choices;
4. To share secret bits, Alice and Bob perform sifting using single compatible events and double compatible matching detection events (from parallel states). Similarly, they apply sifting to the double detection events that contain a single compatible detection event. For this purpose, Bob indicates if the single detection is the first or the second inside the biqubit;
5. Finally, they use an error correction algorithm and a privacy amplification method usually used in $BB84$-based protocols.

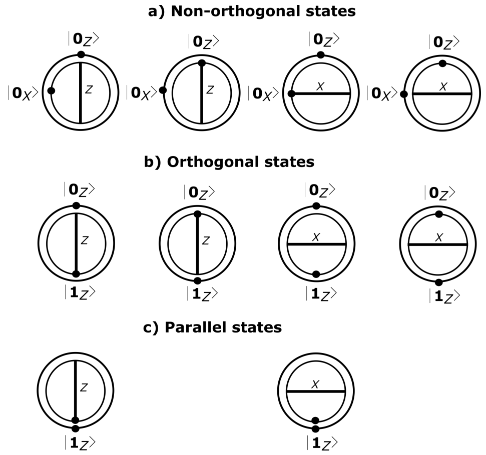

Figure 3. We represent the quantum states as black dots in a simplified Bloch sphere over two dimensions. The quantum measurement bases X and Z are illustrated here as a horizontal and a vertical line, respectively. In this representation, two concentric circles define the order in which the states are prepared and sent. Accordingly, the inner circle state contains the state that is first sent, and the outer circle state is prepared and transmitted. As discussed in [19], the non-orthogonal states are useful to detect the Photon Number Splitting (PNS) attack; an example is shown in (**a**). In the *nack state* protocol, Alice chooses randomly two consecutive parallel states as the case depicted in (**c**) $(|1_Z\rangle, |1_Z\rangle)$. They produce a compatible measurement if Bob chooses, X for $|i_X\rangle$ or Z for $|i_Z\rangle$ where $i = 0, 1$. We sketch in (**b**) the case of quantum orthogonal states. Two cases are possible here $\{(|0_X\rangle, |1_X\rangle), (|0_Z\rangle, |1_Z\rangle)\}$.

Table 1 shows an example of the *nack state* protocol. Here, Alice sends two biqubits to Bob. The first biqubit is the orthogonal pair $(|0_X\rangle, |1_X\rangle)$, and the second biqubit is the parallel pair $(|1_Z\rangle, |1_Z\rangle)$. If the two states sent by Alice arrive at Bob's detection system without any error, a double detection event is produced. If only one of the two states of the biqubit arrives at Bob's station, he obtains a single detection event.

Table 1. We show the *nack state* protocol running in absence of errors at the quantum channel, all of the possible measurement results at Bob's detectors. We assume that Alice sends the biqubits $(|0_X\rangle, |1_X\rangle)$ and $(|1_Z\rangle, |1_Z\rangle)$; then, all of the possible measurement results at Bob's detectors are written. According to Bob's basis selection, we show the detection event and Bob's corresponding advertisement over the public channel. Notice that Bob announces publicly the number of the single detections inside the biqubit, first or second.

Alice's Biqubit	Bob's Basis	Detection Event	Public Disclosure	Description
$(\lvert 0_X\rangle, \lvert 1_X\rangle)$	X	$(\lvert 0_X\rangle, \lvert 1_X\rangle)$	X, $(2nM)$	compatible double non-matching, useful as two compatible single detection events
	X	$(\lvert 0_X\rangle, -)$	X, (S_1)	compatible single matching, useful
	X	$(-, \lvert 1_X\rangle)$	X, (S_2)	compatible single matching, useful
	X	$(-, -)$	X, Lost	biqubit lost
	Z	$(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$	Z, $(2M)$	non-compatible double matching, useless
	Z	$(\lvert 1_Z\rangle, \lvert 1_Z\rangle)$	Z, $(2M)$	non-compatible double matching, useless
	Z	$(\lvert 0_Z\rangle, \lvert 1_Z\rangle)$	Z, $(2nM)$	non-compatible double non-matching, useless
	Z	$(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$	Z, $(2nM)$	non-compatible double non-matching, useless
	Z	$(\lvert 0_Z\rangle, -)$	Z, (S_1)	non-compatible single matching, useless
	Z	$(\lvert 1_Z\rangle, -)$	Z, (S_1)	non-compatible single matching, useless
	Z	$(-, \lvert 0_Z\rangle)$	Z, (S_2)	non-compatible single matching, useless
	Z	$(-, \lvert 1_Z\rangle)$	Z, (S_2)	non-compatible single matching, useless
	Z	$(-, -)$	Z, Lost	biqubit lost
$(\lvert 1_Z\rangle, \lvert 1_Z\rangle)$	Z	$(\lvert 1_Z\rangle, \lvert 1_Z\rangle)$	Z, $(2M)$	compatible double matching, useful
	Z	$(\lvert 1_Z\rangle, -)$	Z, (S_1)	compatible single matching, useful
	Z	$(-, \lvert 1_Z\rangle)$	Z, (S_2)	compatible single matching, useful
	Z	$(-, -)$	Z, Lost	biqubit lost
	X	$(\lvert 0_X\rangle, \lvert 0_X\rangle)$	X, $(2M)$	non-compatible double matching, useless
	X	$(\lvert 1_X\rangle, \lvert 1_X\rangle)$	X, $(2M)$	non-compatible double matching, useless
	X	$(\lvert 0_X\rangle, \lvert 1_X\rangle)$	X, $(2nM)$	non-compatible double non-matching, useless
	X	$(\lvert 1_X\rangle, \lvert 0_X\rangle)$	X, $(2nM)$	non-compatible double non-matching, useless
	X	$(\lvert 0_X\rangle, -)$	X, (S_1)	non-compatible single matching, useless
	X	$(\lvert 1_X\rangle, -)$	X, (S_1)	non-compatible single matching, useless
	X	$(-, \lvert 0_X\rangle)$	X, (S_2)	non-compatible single matching, useless
	X	$(-, \lvert 1_X\rangle)$	X, (S_2)	non-compatible single matching, useless
	X	$(-, -)$	X, Lost	biqubit lost

The *nack state* protocol has been conceived of to use the same optical hardware of the *BB*84 protocol; thus, it can be configured in most *QKD* systems as a software module application. However, two additional tasks must be implemented: the random computation of biqubits before preparing and sending the quantum states and the sifting stage of the protocol, which must include (1) sifting of single matching (compatible or non-compatible), where Bob announces the number of the single detections inside the biqubit; and (2) sifting of double detection, matching or non-matching, from parallel or orthogonal states. The error correction and privacy amplification stages of the *QKD* protocol do not require changes.

Until now, we have a protocol that behaves similarly to *BB*84. In the *nack state* protocol, most of the biqubits pulses sent by Alice arrive at Bob's station as single pulses that behave like *BB*84 signal pulses. However, we will see that in the presence of the *IRFS* attack, the eavesdropper unbalances the gain of the single and double detection events, which is useful to detect her presence in the middle of the quantum channel.

For the moment, we can say that the gain of single and double detection events can be properly computed by Alice as discussed in Appendix A. As a matter of fact, the double detection gain decreases quadratically with the transmittance of the channel, but Alice can verify the gain of the double detection events from parallel and from orthogonal states. It should be noted that in order to detect the $IRFS$, before using the $QBER$ of the protocol, instead, we will verify, as the first step, the gain of the single and the double detection events.

4. Detecting the *IRFS* Attack

What should Alice and Bob expect from the absence of the $IRFS$ attack? They expect a distribution of detection events according to the gains of Table A1 in Appendix A: for illustrative purposes, consider the case where $\mu = 0.2$, $\eta_{BT} = 0.8$, which is the overall efficiency between Alice and Bob and zero dark counts ($Y_0 = 0$). Thus, the great majority of the total biqubits that Alice sends finishes at Bob's station as lost biqubits (∼72.61%); single detection events are ∼25.2% and only ∼0.0219% of the measurement cases are double detection events. Although the double detection gain is small, it should not be considered negligible, because the number of pulses that Alice sends is high (10^{11}–10^{13} [21]), and the transmission interval can be properly enhanced. However, for practical purposes, we will assume that the secret bits in the *nack state* protocol are produced by single detection events, and the key rate is at most the $BB84$ key rate. Nevertheless, we argue that double detection events can be used to detect the $IRFS$ attack, so in this section, we discuss the security of the protocol despite Eve's efforts to improve her attack.

4.1. The IRFS Attack with Blinding Pulses and Quantum Channel Substitution

In the presence of the $IRFS$ attack with blinding pulses, Eve is in the middle of the quantum channel using an optical detection system similar to Bob's station. The challenge for Eve is to reproduce the gains of single and double detection events at Bob's side to pass unnoticed in the quantum channel. However, the gain of the single detection events decreases linearly with the channel efficiency, but the double detection gain drops quadratically. In Appendix B, we show that, for practical parameters of the quantum channel, the eavesdropper cannot adjust the two gains simultaneously. Eve cannot control the two gains because:

1. The eavesdropper can adjust the transmittance of the channel to a unique value, either to adjust the single or the double detection gain.
2. Alice's optical pulses arrive at Eve's station sequentially. Thus, once the eavesdropper station has detected a pulse, she cannot know whether the next pulse will be also detected or lost. That is, Eve does not know when a single or a double detection event will occur.

Eve could adjust the efficiency of the quantum channel to the gain of the double detection events. Therefore, in order to remove the excess of the single detection gain, Eve could eliminate pulses according to some probability (e.g., 0.5). However, due to the second point stated before, the eavesdropper looses double detection pulses (a quarter in this example). Eve could be more selective removing only single detection events where the detection occurs in the second pulse. Using this strategy, Eve keeps the double detection gain unaltered. However, since Bob announces publicly the number of single detections inside the biqubit, first or second (see Table 1), the presence of Eve becomes noticeable.

Eve could combine the two strategies increasing the efficiency of the channel to produce an excess of the double, but also the single detection gain. The problem for Eve is that once she chooses a strategy to remove pulses, it affects equally the single and the double detection gains. As discussed in Appendix A, such gains obey different rates: while the first decreases linearly, the second varies quadratically with the transmittance of the channel. In addition, at the receiver station, the single and double detection events are registered as random interleaved events.

In Appendix B.1, we discuss a convenient method to compute the photon gain deviation caused by the $IRFS$ attack at a practical level.

4.2. The Non-Structured Nack State Protocol

The argument of Point 2 implies that Eve uses only a single station, but this is not a practical restriction. Eve could use two stations, one close to Alice to detect and one close to Bob to generate fake pulses. If the quantum channel uses optical fibers (the most common practical channel for ground-based QKD), all Eve would need is a radio link between her two stations to "catch up" with the quantum link. Even if we assume a low source rate of 1 MHz, the time delay between pulses is only one microsecond, which can be compensated using a 600-m link (traveling in free space takes two microseconds; travel in fiber takes three microseconds). Any practical QKD system will operate over distances greater than 600 m, making it entirely feasible for Eve to detect both pulses of a pair before sending her fake state to Bob using a second station.

However, there is no reason why each pair has to be sent in a consecutive manner. We call this protocol the non-structured *nack state*. If Alice were to send a burst of the first states of each pair, followed by a burst of the second states of each pair, she would create a separation between the pairs equal to the length of the bursts without reducing the pulse rate. Consider a 100-km fiber optic link; Alice could send the first states of each pair for 500 microseconds, followed by the second state of each pair for the next 500 microseconds, with Bob re-choosing the same basis for both 500-microsecond bursts. Because the 500-microsecond delay is at least the full travel time in the quantum channel, Eve would always be forced to fake the first state of each pair before receiving the second. If there is no issue with this approach, the authors can use it to justify Point 2, which in turn justifies Point 1.

4.3. Faking Double Detection Events

Another scenario for the eavesdropper is to fake double detection events. After all, we might ask why Eve cannot fake double detection events while she remains hidden in the channel. First of all, let us recall that Alice knows which biqubits contain parallel or orthogonal states. Second, consider the cases depicted in Table 2. Suppose Alice has sent the $(|0_Z\rangle, |0_Z\rangle)$ biqubit to Bob. The first pulse reaches Eve's station, who measures it with the X (or Z) basis, but the second pulse arrives as a vacuum state either by the effect of the quantum channel, the detection system or the photon source. As a result, Eve gets a single detection event. Now, Eve decides to fake the second state, but she realizes that there are six possibilities to fake the $(|0_Z\rangle, |0_Z\rangle)$ biqubit; such cases are listed in Table 2. Additionally, one of those cases is erroneous because no orthogonal measurement can be derived from parallel states. In this example, $(|1_Z\rangle, |0_Z\rangle)$ cannot be obtained from $(|0_Z\rangle, |0_Z\rangle)$. Similarly, $(|0_Z\rangle, |0_Z\rangle)$ cannot be derived from $(|1_Z\rangle, |0_Z\rangle)$. As a consequence, if Eve tries to fake a double detection event, she will produce a bit error of $\frac{1}{6}$. In this case, a bit error is produced when Bob announces a double matching event, but Alice expects a double non-matching event or vice versa.

Table 2. After Eve detects the first state of a biqubit, she tries to fake the second state. However, there exist six possible states, but one of them is erroneous, so she introduces an error probability of $\frac{1}{6}$. Here, we show the six choices for $(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$ and $(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$ biqubits.

Alice's Biqubit	Eve's Basis	Eve's Detection	Forwarded Dates	Eve's Result
$(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$	Z	$(-, \lvert 0_Z\rangle)$	$(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$	hidden
			$(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$	detected
	X	$(-, \lvert 0_X\rangle)$	$(\lvert 0_X\rangle, \lvert 0_X\rangle)$	hidden
			$(\lvert 1_X\rangle, \lvert 0_X\rangle)$	hidden
		$(-, \lvert 1_X\rangle)$	$(\lvert 0_X\rangle, \lvert 1_X\rangle)$	hidden
			$(\lvert 1_X\rangle, \lvert 1_X\rangle)$	hidden
$(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$	Z	$(-, \lvert 0_Z\rangle)$	$(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$	detected
			$(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$	hidden
	X	$(-, \lvert 0_X\rangle)$	$(\lvert 0_X\rangle, \lvert 0_X\rangle)$	hidden
			$(\lvert 1_X\rangle, \lvert 0_X\rangle)$	hidden
		$(-, \lvert 1_X\rangle)$	$(\lvert 0_X\rangle, \lvert 1_X\rangle)$	hidden
			$(\lvert 1_X\rangle, \lvert 1_X\rangle)$	hidden

According to [22], Bob's visibility of Alice's quantum state is computed as $V_{AB} = \frac{P(signal)}{P(total)}$ where $P(signal) = T_{AB} \times \eta \times V_{opt}$ and $P(total) = T_{AB} \times \eta + (1 - T_{AB} \times \eta) \times 2 \times Y_0$. Here, V_{opt} is the optical visibility with a perfect source and detectors; η is the probability of detecting the photon when it arrives; T_{AB} is the transmittance between Alice and Bob; and Y_0 is the background noise. For realistic experimental parameters: $\alpha = 0.25$ dB·km^{-1}, $\eta = 0.3$, $Y_0 = 10^{-4}$ and $V_{opt} = 0.99$. Figure 4 shows the visibility as a function of the distance.

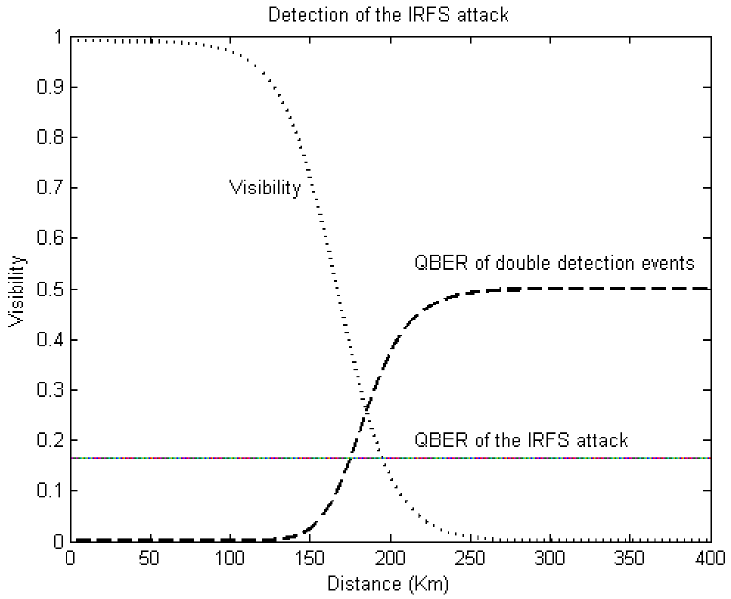

Figure 4. The error rate of double detection events caused by the *IRFS* attack is $\frac{1}{6}$. If it is compared against the *QBER* of the quantum channel, the maximum secure distance to detect the *IRFS* attack is 176 km. In the presence of the *IRFS* attack, perfect visibility and zero dark counts are assumed in the link between Alice and Eve and from her to Bob.

On the other hand, the *QBER* in *BB*84 can be computed as $QBER = \frac{pe}{pe+pc}$, where pc (pe) is the probability to get, correctly or erroneously, the quantum bit sent by Alice, respectively. If we write such probabilities as a function of the optical visibility V, we have $pc = (1 + V)/2$ and $pe = (1 - V)/2$.

We discussed pc (pe) for double detection events in Appendix C. Therefore, $pc = \frac{p_c^2}{p_c^2+p_e^2}$ and $pe = \frac{p_e^2}{p_c^2+p_e^2}$, and we derived the $QBER$ of the parallel and orthogonal states as $QBER = \frac{(1-V)^2}{(1-V)^2+(1+V)^2}$.

If we compare the $QBER$ of double detection events produced by the quantum channel against the $\frac{1}{6}$ error rate caused by the eavesdropper, we find that the maximum secure distance for detecting the $IRFS$ attack when the eavesdropper fakes double detection events is 176 km, which is within the range of the $BB84$ key rate, as is shown in Figure 4.

5. Discussion

5.1. Decoy State and the Nack State Protocol

At first glance, the *nack state* protocol seems to be similar to the *decoy state* protocol. However, they differ due to some main issues. For example, the states of the *decoy state* protocol are $BB84$ non-orthogonal states, which produce two photon distributions that differ from each other with respect to the expected photon number of the source ($\mu_1 \neq \mu_2$).

Thus, in the *decoy state* protocol, single detection events come from non-orthogonal states. As described by Hoi-Kwong Lo, if Eve lets an abnormally high fraction of multiphotons reach Bob's station, then decoy states, which have a high weight of multiphotons, will have an abnormally high transmission probability [23]. Unfortunately, *decoy state* QKD is vulnerable to the $IRFS$ attack [13,20]. On the other hand, in the *nack state* protocol, Alice interleaves randomly parallel and orthogonal quantum states. Unlike the *decoy state* protocol, in the *nack state*, the photon source uses a unique μ value. However, single and double detection events come from parallel and orthogonal states randomly.

5.2. Measurement Device-Independent QKD

In [17], a QKD system that is intended to be an independent measurement device has been introduced. Implementations of this approach have been demonstrated in [24,25]. However, [24] requires several additional optical components different from the $BB84$ protocol, and [25] relies on decoy states. Since QKD must be as device independent as possible, adding hardware to the system may aggravate it. In contrast, the *nack state* protocol relies on the hardware of the original $BB84$ protocol, which has been extensively studied.

Other protocols have been designed to resist the $IRFS$ attack: varying randomly the efficiency of the detectors [26], monitoring a rate of coincidence detection at a pair of single photon detectors [27] or simply adding watchdogs detectors [28]. However, the *nack state* protocol exhibits two main advantages:

1. The protocol uses the same optical equipment as the $BB84$. It does not use any other extra hardware;
2. The protocol or its dual protocol, the *ack QKD*, could be used to detect other attacks, such as the Photon Number Splitting attack (PNS) [19].

Thus, the *nack state* protocol would be useful to design a more secure and efficient QKD protocol.

6. Conclusions

The Intercept Resend with Faked (blinding) States ($IRFS$) attack is detected by the *nack state* protocol using the gain of single and double detection events. The protocol uses the same optical hardware of the $BB84$ protocol, and it can be implemented in most QKD systems as a software module application.

Although double detection events represent a small fraction of the total detection events, they are useful to detect the $IRFS$ attack. In addition, the smaller $QBER$ can be useful in future implementations to distill secret bits at longer distances.

Author Contributions: All authors contributed equally to this work. Luis Adrian Lizama-Pérez conceived the *nack state* protocol. José Mauricio López analyzed, discussed and improved the protocol. Eduardo De Carlos López analyzed the protocol and contributed with discussion to the work presented in this paper. All authors discussed the results and implications and commented on the manuscript at all stages. All authors have read and approved the final manuscript.

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

Appendix A. The Gain of Detection Events

In Table A1 (upper part), the symbol $Q_{(+)}$ represents the gain of the single detection events. According to [15], the gain of detection events is obtained from two parts: the photon source and the quantum channel. The photon source has an expected photon number μ, and it follows a Poisson distribution. On the other hand, the quantum channel presents a distribution that is computed for each i photons' state (where i is the number of photons in each pulse) that is called yield. The gain Q_i of i photons' state is the product of the probability of Alice sending an i photons' state (that follows a Poisson distribution) and the yield of i photons' state (and background states). It will produce a gain at Bob's side caused by the detection of events according to the relation $Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}$ where Y_i is the yield of i photons' state.

Table A1. The gain of the single (non-empty) and empty pulses, $Q_{(+)}$ and $Q_{(-)}$, respectively, where μ is the expected photon number of the source and Y_0 is the background noise. Here, η_{BT} and η_{ET} are the overall efficiency of Bob and Eve, respectively. In the *IRFS* attack, Eve remains undetected provided she meets the condition $\eta_{ET} \geq \frac{\ln(2e^{-\mu\eta_{BT}} - Y_0 - 1)}{-\mu}$. At the bottom, we show the gain of the double $(+,+)$ detection events, which is written as $Q_{(+,+)}$, and the gain of single $(\pm,\mp)$ detection events is represented as $Q_{(\pm,\mp)}$. In the *IRFS* attack, half of Eve's biqubits can be effectively forwarded to Bob's detectors. The "$\cdot$" symbol denotes multiplication inside the $Q_{(\pm,\mp)}$ relation. The factor of 1/2 is a result of Bob using an active basis choice, forcing Eve to blind his detector when his basis differs from her own (half the time), and since each pair of pulses is detected in the same basis, Eve will always blind Bob for both pulses or neither pulses, resulting in the same factor 1/2 for both single and double detection events.

Gain	*Alice*	*Alice − Bob*	*Eve − Bob*
$Q_{(-)}$	$e^{-\mu}$	$e^{-\mu\eta_{BT}} - Y_0$	-
$Q_{(+)}$	$1 - e^{-\mu}$	$Y_0 + 1 - e^{-\mu\eta_{BT}}$	$\frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})$
$Q_{(-,-)}$	$e^{-2\mu}$	$(e^{-\mu\eta_{BT}} - Y_0)^2$	-
$Q_{(\pm,\mp)}$	$2e^{-\mu}\cdot$ $(1 - e^{-\mu})$	$2(e^{-\mu\eta_{BT}} - Y_0)\cdot$ $(Y_0 + 1 - e^{-\mu\eta_{BT}})$	$(e^{-\mu\eta_{ET}} - Y_0)\cdot$ $(Y_0 + 1 - e^{-\mu\eta_{ET}})$
$Q_{(+,+)}$	$(1 - e^{-\mu})^2$	$(Y_0 + 1 - e^{-\mu\eta_{BT}})^2$	$\frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})^2$

The yield Y_i is computed across the following steps:

1. The fiber channel transmittance between Alice and Bob is written as $T_{AB} = 10^{-\frac{\alpha l}{10}}$ where α is the loss coefficient measured in dB/km, and the length l is measured in km. Furthermore, the local transmittance at Bob's side η_B is written as $t_B \cdot \eta_D$ where t_B is the internal transmittance of optical components and η_D is the quantum efficiency of Bob's detectors. Then, the overall transmission and detection efficiency at Bob's side η_{BT} is computed as $\eta_{BT} = t_B \cdot \eta_D \cdot T_{AB}$ and typically η_{BT} ranges 10^{-3} [15];
2. The transmittance η_i of i photons' state at Bob's, that is $\eta_{BTi} = 1 - (1 - \eta_{BT})^i$ for $i = 0, 1, ...,$ assuming independence between the i photons of the i photons' state;

3. The yield Y_i of the i photons' state is obtained from two sources, the background noise (Y_0) and the true signal. Assuming that the background counts are independent from the signal photon detection, Y_i is given by $Y_i = Y_0 + \eta_{BTi} - Y_0\eta_{BTi}$. However, assuming Y_0 small (around 10^{-5}) and $\eta_{BT} \sim 10^{-3}$, the above equation can be reduced to $Y_i \sim Y_0 + \eta_{BTi}$.

The overall gain $Q_{(+)}$ is the summation of each Q_i contribution, thus $Q_{(+)} = \sum_{i=1}^{\infty} Q_i = \sum_{i=1}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}$, which leads to the relation $Y_0 + 1 - e^{-\mu\eta_{BT}}$. Finally, the Quantum Bit Error Rate ($QBER$) between Alice and Bob has been derived in [15] through the relation $QBER_{AB} = \frac{0.5Y_0 + e_d(1-e^{-\mu\eta_{BT}})}{Y_0+1-e^{-\mu\eta_{BT}}}$, where e_d is the error probability of the detector ($e_d \sim 10^{-2}$).

In order to obtain the gain of double detection events $Q_{(-,-)}$, $Q_{(\pm,\mp)}$ and $Q_{(+,+)}$, we assume that each gain is independent of the other, that is $Q_{(-,-)} = Q_{(-)} \times Q_{(-)}$, $Q_{(+,-)} = Q_{(+)} \times Q_{(-)}$, $Q_{(+,-)} \sim Q_{(-,+)}$ and $Q_{(+,+)} = Q_{(+)} \times Q_{(+)}$. From the previous discussion, we have that the gain of the double detection events decreases quadratically $Q_{(+,+)} \sim Q^2_{(+)}$. In practical implementations of QKD, the single-matching events have the order of 10^{-5}, while the double matching events reach the order of 10^{-10}.

Appendix B. The *IRFS* Attack and Quantum Channel Substitution

The eavesdropper would try to adjust the two gains, from single and double detection events applying a quantum channel substitution and adjusting it to a specific transmittance. We define the Quantum Photon Error Gain ($QPEG$ or simply ΔQ) as the deviation from the reference gain that is caused by Eve's apparatus at Bob's receiver station when she performs the $IRFS$ attack. In normal conditions, it is expected that $\Delta Q \sim 0$, ideally for the single and the double detection events.

We represent the $QPEG$ of double $(+,+)$ detection events as $\Delta Q_{(+,+)}$, while the $QPEG$ of single $(\pm,\mp)$ detection events is written as $\Delta Q_{(\pm,\mp)}$. $\Delta Q_{(+,+)}$ is computed as the difference $Q_{(+,+)_{AB}} - Q_{(+,+)_{EB}}$ where the symbol $(+,+)_{AB}$ defines the reference gain of the double detection events and $(+,+)_{EB}$ denotes the gain of the double detection events at Bob's side, but in the presence of Eve. Similarly, $\Delta Q_{(\pm,\mp)}$ as $Q_{(\pm,\mp)_{AB}} - Q_{(\pm,\mp)_{EB}}$, where we use the sub-index of $(\pm,\mp)_{AB}$ and $(\pm,\mp)_{EB}$ with the same purpose.

Using the relations of Table A1, it is possible to establish if the eavesdropper can fulfill simultaneously the conditions $\Delta Q_{(+,+)} = 0$ and $\Delta Q_{(\pm,\mp)} = 0$. Let the eavesdropper adjust freely η_{BT} and η_{ET}. Thus, Eve's goal is to make $\Delta Q_{(+,+)_{AB}} = \Delta Q_{(+,+)_{EB}}$ and $\Delta Q_{(\pm,\mp)_{AB}} = \Delta Q_{(\pm,\mp)_{EB}}$. We get the following equation system:

$$2(e^{-\mu\eta_{BT}} - Y_0)(Y_0 + 1 - e^{-\mu\eta_{BT}}) = (e^{-\mu\eta_{ET}} - Y_0)(Y_0 + 1 - e^{-\mu\eta_{ET}}) \tag{B1}$$

$$(Y_0 + 1 - e^{-\mu\eta_{BT}})^2 = \frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})^2 \tag{B2}$$

Solving the system for η_{ET}, we obtain $\frac{\ln Y_0}{-\mu}$ and $\frac{\ln(1+Y_0)}{-\mu}$, which cannot be satisfied in practice. This is true because the second relation yields η_{ET} negative, and the first relation cannot be fulfilled for typical parameters, e.g., $Y_0 = 10^{-5}$, $\mu = 0.1$ produces $\eta_{ET} = 1.15$. Consider also the cases depicted in Figure B1.

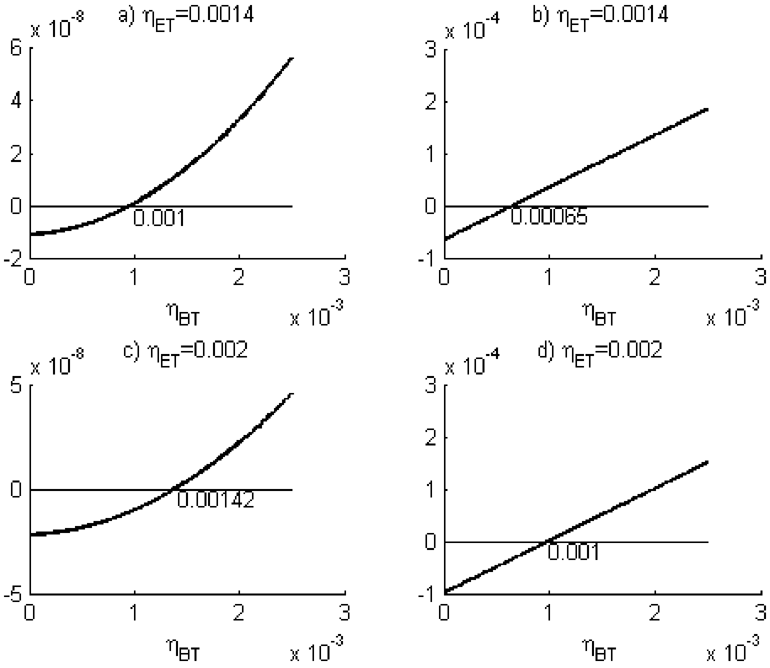

Figure B1. The y-axis shows the deviation from the reference gain. The upper and bottom left graphs correspond to double detections, while the right graphs represent single detections. Assuming that $\eta_{BT} = 0.001$ and Eve uses $\eta_{ET} = 0.0014$, she achieves in (**a**), $\Delta Q_{(+,+)} = 0$, however, in (**b**), $\Delta Q_{(\pm,\mp)} \neq 0$. Conversely, if Eve adjusts $\eta_{ET} = 0.002$, she gets in (**d**) $\Delta Q_{(\pm,\mp)} = 0$, but in (**c**), she causes simultaneously that $\Delta Q_{(+,+)} \neq 0$.

Appendix B.1. The Photon and the Vacuum Ratios

In this section, we will introduce a convenient method to detect the presence of the eavesdropper without requiring one to compute deviations from the reference gain, that is $\Delta Q(+,+) = 0$ or $\Delta Q(\pm,\mp) = 0$. For this purpose, let us define the photon ratio R as the relation between the gains $\frac{Q_{EB}}{Q_{AB}}$ where the subscript EB denotes the presence of the eavesdropper and AB indicates its absence. For double detection events, we represent R as $\frac{Q(+,+)_{EB}}{Q(+,+)_{AB}}$, while $\frac{Q(\pm,\mp)_{EB}}{Q(\pm,\mp)_{AB}}$ for single detection events. In addition, we will define the vacuum ratio r as $\frac{e^{-\mu\eta_{ET}} - Y_0}{e^{-\mu\eta_{BT}} - Y_0}$.

If the eavesdropper adjusts the channel to achieve $Q(+,+)_{AB} = Q(+,+)_{EB}$, then Equation (B2) is satisfied. We get that $R_{(\pm,\mp)} = \frac{r}{\sqrt{2}}$, but $r = \frac{e^{-\mu\eta_{ET}} - Y_0}{e^{-\mu\eta_{BT}} - Y_0}$ and $\eta_{ET} \geq \eta_{BT}$; thus, $r \leq 1$ and $R_{(\pm,\mp)} \leq \frac{1}{\sqrt{2}}$. To discard Eve's presence, we do not need to check that $\Delta Q(\pm,\mp) = 0$, but it must be verified that $R_{(\pm,\mp)} > \frac{1}{\sqrt{2}}$. Conversely, if Eve modifies the channel to achieve $Q(\pm,\mp)_{AB} = Q(\pm,\mp)_{EB}$, we get that $R_{(+,+)} = \frac{2}{r^2}$. Since, $r \leq 1$, we have that the $IRFS$ attack causes that $R_{(+,+)} \geq 2$. To be sure that the system is safe against the $IRFS$ attack, we do not need to check that $\Delta Q(+,+) = 0$, but it is equivalent to verify that $R_{(+,+)} < 2$.

Appendix C. The *QBER* of One-Photon States

As mentioned before, in the *nack state* protocol, the great majority of the pulses that Alice sends to Bob behave as $BB84$ signal pulses. Each time Bob applies a compatible basis measurement, the result, either from single detection or double detection, is useful as in $BB84$. Thus, for practical purposes, the *nack state* protocol has an efficiency comparable to the $BB84$. Nevertheless, we must expect a partial reduction of the bit rate, because Alice reduces the optical pulse rate to avoid the eavesdropper to register double detection events. In this manner, Eve is detected if she waits for double detection events before she can forward them.

The rate of the double detection event is small because it decreases quadratically. However, at the same time, it is very remarkable that the $QBER$ of the double matching detection events from parallel and orthogonal states also decreases quadratically. To see this, let us recall that in the $BB84$ protocol, the probability to get the correct bit is $pc = (1+V)/2$, and the probability to obtain an erroneous bit is $pe = (1-V)/2$, where V is the visibility of the optical system. To calculate the $QBER$ of the one-photon states, the relation $QBER = pe/(pe+pc)$ is applied [29].

Now, suppose Alice sends the two parallel states $(|1_Z\rangle, |1_Z\rangle)$ to Bob who measures them using the Z basis. Those states are depicted in Figure C1a. The probability to get the two states $(|1_Z\rangle, |1_Z\rangle)$ is p_c^2, and the probability to get the opposite values $(|0_Z\rangle, |0_Z\rangle)$ is p_e^2, Case II of Figure C1a. Since the measurement cases $(|0_Z\rangle, |1_Z\rangle)$ and $(|1_Z\rangle, |0_Z\rangle)$, Cases III and IV of Figure C1a, are always discarded because they are non-matching cases, the final probabilities are $pc_{parallel} = \frac{p_c^2}{p_c^2+p_e^2}$ and $pe_{parallel} = \frac{p_e^2}{p_c^2+p_e^2}$. The same reasoning can be applied to the orthogonal biqubits case depicted in Figure C1b.

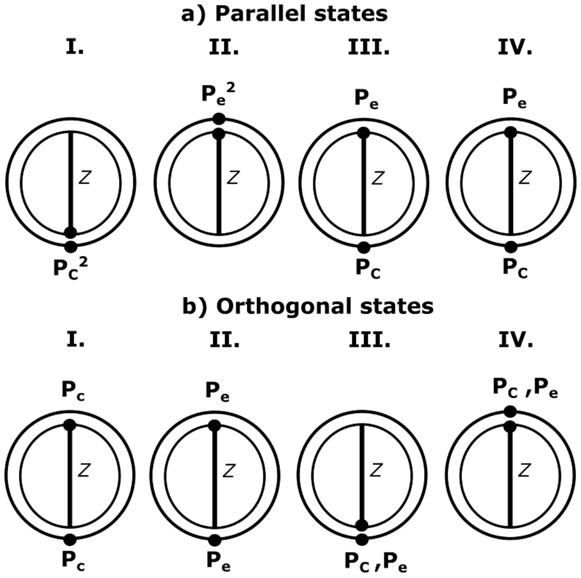

Figure C1. The $QBER$ of parallel and orthogonal states: Cases III and IV of (**a**,**b**) can be discarded by Alice, so they do not produce errors.

Those relations lead us to the $QBER$ of the parallel and orthogonal states $QBER = \frac{(1-V)^2}{(1-V)^2+(1+V)^2}$. Figure C2 illustrates the $QBER$ of one-photon states of such protocols. Since the $QBER$ of the *nack sate* is lower than the $BB84$, it is interesting to consider that future technologies could increase the double detection gain. Although there is not yet a formal derivation of the secret key rate for double detection events, it would be expected that the small $QBER$ would lead to reaching longer QKD distances.

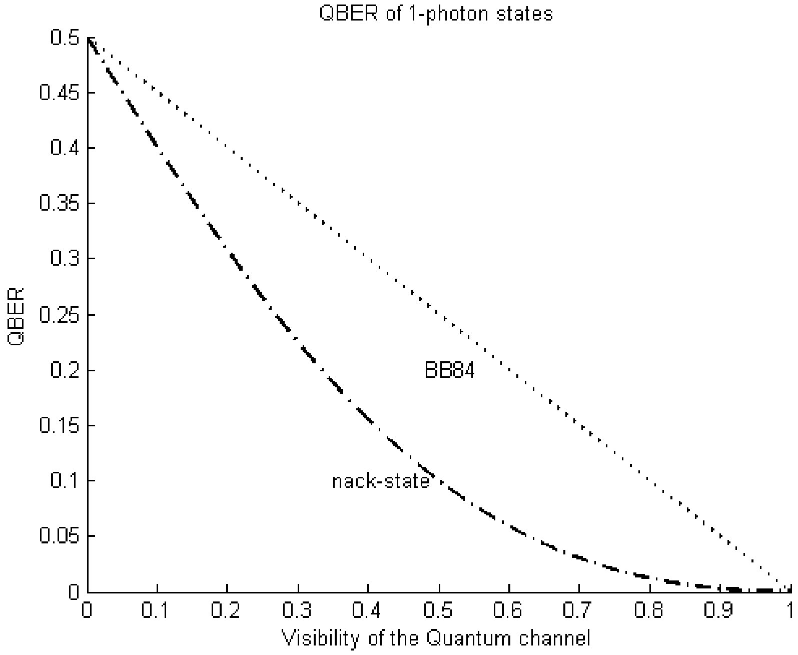

Figure C2. The *nack state* protocol uses pairs of parallel and orthogonal states. The *QBER* of parallel and orthogonal states is derived using the probabilities of two consecutive *BB*84 measurements.

References

1. Bennett, C.H. Quantum cryptography: Public key distribution and coin tossing. In Proceddings of the 1984 International Conference on Computer System and Signal Processing, Bangalore, India, 10–19 December 1984.
2. Van Assche, G. *Quantum Cryptography and Secret-Key Distillation*; Cambridge University Press: Cambridge, UK, 2006
3. Hughes, R.; Nordholt, J.; Rarity, J. Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography—A Quantum Information Science and Technology Roadmap. Available online: http://qist.lanl.gov/pdfs/6.5-continuous.pdf (accessed on 19 December 2016).
4. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28.
5. Fung, C.F.; Qi, B.; Tamaki, K.; Lo, H. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **2007**, *75*, 032314.
6. Xu, F.; Qi, B.; Lo, H. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **2010**, *12*, 113026.
7. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 691–705.
8. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313.
9. Makarov, V.; Skaar, J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Inf. Comput.* **2008**, *8*, 622–635.
10. Qi, B.; Fung, C.F.; Lo, H.; Ma, X. Time-shift attack in practical quantum cryptosystems. *arXiv* **2005**, arXiv:quant-ph/0512080.
11. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689.
12. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2011**, *2*, 349.
13. Wiechers, C.; Lydersen, L.; Wittmann, C.; Elser, D.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. After-gate attack on a quantum cryptosystem. *New J. Phys.* **2011**, *13*, 013043.

14. Weier, H.; Krauss, H.; Rau, M.; Fuerst, M.; Nauerth, S.; Weinfurter, H. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. *New J. Phys.* **2011**, *13*, 073024.
15. Ma, X.; Qi, B.; Zhao, Y.; Lo, H. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326.
16. Hughes, R.; Nordholt, J. Refining quantum cryptography. *Science* **2011**, *333*, 1584–1586.
17. Lo, H.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503.
18. Lizama, L.; López, J.M.; De Carlos, E.; Venegas-Andraca, S.E. Enhancing quantum key distribution (QKD) to address quantum hacking. *Procedia Technol.* **2012**, *3*, 80–88.
19. Lizama-Pérez, L.A.; López, J.M.; De Carlos-López, E.; Venegas-Andraca, S.E. Quantum Flows for Secret Key Distribution in the Presence of the Photon Number Splitting Attack. *Entropy* **2014**, *16*, 3121–3135.
20. Sun, S.; Jiang, M.; Ma, X.; Li, C.; Liang, L. Hacking on decoy-state quantum key distribution system with partial phase randomization. *Sci. Rep.* **2014**, *4*, 013043.
21. Song, T.; Qin, S.; Wen, Q.; Wang, Y.; Jia, H. Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources. *Sci. Rep.* **2015**, *5*, 735–753.
22. Collins, D.; Gisin, N.; De Riedmatten, H. Quantum relays for long distance quantum cryptography. *J. Mod. Opt.* **2005**, *52*, 735–753.
23. Lo, H.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504.
24. Rubenok, A.; Slater, J.A.; Chan, P.; Lucio-Martinez, I.; Tittel, W. A quantum key distribution system immune to detector attacks. *arXiv* **2012**, arXiv:1204.0738.
25. Xu, F.; Curty, M.; Qi, B.; Lo, H.-K. Measurement-device-independent quantum cryptography. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 148–158.
26. Lim, C.C.W.; Walenta, N.; Legré, M.; Gisin, N.; Zbinden, H. Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 192–196.
27. Honjo, T.; Fujiwara, M.; Shimizu, K.; Tamaki, K.; Miki, S.; Yamashita, T.; Terai, H.; Wang, Z.; Sasaki, M. Countermeasure against tailored bright illumination attack for DPS-QKD. *Opt. Express* **2013**, *21*, 2667–2673.
28. Jain, N.; Stiller, B.; Khan, I.; Elser, D.; Marquardt, C.; Leuchs, G. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemp. Phys.* **2016**, *57*, 366–387.
29. Jeong, Y.; Kim, Y.-S.; Kim, Y.-H. Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols. *Laser Phys.* **2011**, *21*, 1438–1442.