Entropy **2014**, *16*, 3121-3135; doi:10.3390/e16043121

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Quantum Flows for Secret Key Distribution in the Presence of the Photon Number Splitting Attack

Luis A. Lizama-Pérez [1,*], J. Mauricio López [1], Eduardo De Carlos-López [1] and Salvador E. Venegas-Andraca [2]

[1] Time and Frequency Division, Centro Nacional de Metrología, Carr. a los Cués Km. 4.5, Municipio El Marqués, Querétaro C.P. 76246, Mexico;
E-Mails: jlopez@cenam.mx (J.M.L.); edlopez@cenam.mx (E.D.C.-L.)

[2] Tecnológico de Monterrey, Campus Estado de México, Carr. a Lago de Guadalupe Km. 3.5, Atizapán de Zaragoza, Estado de México C.P. 52926, Mexico;
E-Mail:salvador.venegas-andraca@keble.oxon.org

* Author to whom correspondence should be addressed; E-Mail: llizama@cenam.mx; Tel.: +1-52-442-211-0543.

Received: 8 April 2014; in revised form: 23 May 2014 / Accepted: 29 May 2014 / Published: 5 June 2014

Abstract: Physical implementations of quantum key distribution (QKD) protocols, like the Bennett-Brassard (BB84), are forced to use attenuated coherent quantum states, because the sources of single photon states are not functional yet for QKD applications. However, when using attenuated coherent states, the relatively high rate of multi-photonic pulses introduces vulnerabilities that can be exploited by the photon number splitting (PNS) attack to brake the quantum key. Some QKD protocols have been developed to be resistant to the PNS attack, like the decoy method, but those define a single photonic gain in the quantum channel. To overcome this limitation, we have developed a new QKD protocol, called ack-QKD, which is resistant to the PNS attack. Even more, it uses attenuated quantum states, but defines two interleaved photonic quantum flows to detect the eavesdropper activity by means of the quantum photonic error gain (QPEG) or the quantum bit error rate (QBER). The physical implementation of the ack-QKD is similar to the well-known BB84 protocol.

Keywords: QKD; PNS; ack-QKD; bi-qubit; quantum photonic error gain; ΔQ

---

1. Introduction

In the Bennett-Brassard (BB84) protocol [1], ideally, the quantum states that Alice sends to Bob correspond to single photons. However, due to perfect single photon sources not being technologically available yet [2], many quantum key distribution (QKD) implementations use laser pulses, which are attenuated to a very low level. On average, these laser pulses contain a very small number of photons, typically around 0.2 photons per pulse, distributed according to a Poissonian distribution. In other words, most pulses actually contain no photons; few pulses only contain just one photon, and only a very small amount of pulses contain two or more photons. The photon Number Splitting (PNS) attack can be resumed as follow. If a laser pulse contains more than one photon Eve can split off the extra photons from it. Then, she allows just one photon to reach Bob's detector. In doing that, Eve can store the photons she got from the pulse and wait until Bob reveals the measurement basis he applied. Eve measures the stored photons with the same measurement basis as Bob, obtaining information about the key. Eve's activity on the quantum channel is unnoticed by Alice and Bob. References related with security proofs on the PNS attack can be found in [3–7].

Few protocols are known to be PNS resistant: Decoy QKD [8], Scarani-Acin-Ribordy-Gisin (SARG04) [9], the Differential Phase Shift Keying (DPSK) [10] and Coherent One Way (COW) [11]. One of the most promissory alternatives is the decoy method. In this protocol additional states are interleaved to the standard BB84 states with the purpose to detect an eavesdropper. These are called decoy states. The decoy states are generated by applying, to the photonic source, different mean photonic numbers (μ). The only difference between the standard BB84 protocol states and the decoy states is μ. Eve cannot make difference between decoy states and BB84 states. When Eve intercepts the decoy states to steal photons, she modifies the mean photonic number on the decoy pulses arriving to Bob's detector. In this way the decoy method reveals the presence of an eavesdropper. Decoy QKD enhances the security of the BB84 protocol against PNS attacks while allowing high key rates.

The same as the BB84 protocol, the decoy QKD method establishes a single photonic gain in the quantum channel. Unfortunately, decoy QKD can be successfully attacked if Eve is able to adjust the gain of the quantum channel in order to set the QBER to zero. In this paper, we introduce a novel QKD protocol, named ack-QKD, which is simultaneously immune to a PNS attack and changes on the gain of the quantum channel. These two main features of the ack-QKD protocol are possible if two photonic quantum flows, from parallel and non-orthogonal states, are interleaved to produce two or more quantum gains that cannot be simultaneously adjusted, by changing the gain of the quantum channel, in order to set the two QBER to zero. Our method to detect the PNS attack using the ack-QKD protocol can be summarized in the following:

(1) In the PNS attack, the eavesdropper blocks the one-photon states, but she stores the multi-photon states, allowing at least one photon to reach Bob's detection system.
(2) Eve cannot substitute the quantum channel, because she cannot adjust simultaneously the multiple channel gain, QPEG, from single and double detection events. As a consequence, Eve is forced to measure the one-photon states, from single and double states, in order to guess the quantum states sent by Alice. In measuring the single states, parallel and non-orthogonal, the eavesdropper produces QBER=0.25 (as in the BB84). On the other

side, in measuring the double (non-empty) states, parallel and non-orthogonal, Eve produces QBER=0.5.

(3) The QBER from the multi-photonic non-orthogonal states decrease by half for each copy of the quantum states in Eve's memory. By contrast, the multi-photonic parallel states do not contribute to increasing the QBER, because Bob reveals the basis measurements he used.

The security of the ack-QKD protocol relies on Eve's impossibility to mount a channel substitution attack without being detected and because the eavesdropper produces a QBER=0.5 in the one-photon double (non-empty) states, parallel and non-orthogonal. By substituting the channel, Eve can adjust one of the two gains, single or double (non-empty) states, but she produces a QBER in the other gain. This contrasts with other PNS-resistant methods in which Eve blocks the one-photon states, but she is capable of mounting a channel substitution to adjust the photonic gain. Thus, in the ack-QKD, the presence of Eve in the channel cannot remain undetectable.

The paper is organized as follow. In Section 2, we describe the BB84, SARG04 and the ack-QKD protocols. Section 3 elaborates by describing the ack-QKD protocol with parallel and non-orthogonal states. Section 4 describes the photon number splitting (PNS) attack and indicates how it can be detected when applied to the ack-QKD protocol. Finally, in Section 6, we introduce the unstructured ack-QKD protocol, which constitutes a variation of the ack-QKD, protocol to avoid consecutiveness in detection events.

2. BB84, SARG04 and ack-QKD

Consider a BB84-based protocol that encodes a classical bit using one of the four non-orthogonal quantum states, $|+_X\rangle, |-_X\rangle, |+_Z\rangle$ and $|-_Z\rangle$ (See Figure 1). In the SARG04 protocol [9], Alice prepares one of the four BB84 quantum states to be sent to Bob, that is, she prepares a state that belongs to two conjugate bases (X and Z). In SARG04, the classical bits are encoded as follows: zero is coded with $|+_Z\rangle$ and $|-_Z\rangle$ and one is coded with $|+_X\rangle$ and $|-_X\rangle$ (see Figure 2), where the qubits are represented as black dots in the bi-dimensional Bloch sphere (the non-orthogonal states are right-angled; the orthogonal states are drawn diametrically opposed, and the parallel states occupy the same place in the sphere). The basis measurements, X and Z, are depicted as horizontal and vertical lines, respectively. By contrast, in the $BB84$ protocol, the bit, 0, is encoded with $|+_Z\rangle$ and $|-_X\rangle$ while the bit, 1, is encoded with $|-_Z\rangle$ and $|+_X\rangle$.

In the sifting phase of the SARG04 protocol, Alice does not reveal the basis she used (this would reveal the bit). Instead, she announces the sifting set to which the state belongs according to the following four sifting sets: $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$, $S_{(+,-)} = \{|+_X\rangle, |-_Z\rangle\}$, $S_{(-,+)} = \{|-_X\rangle, |+_Z\rangle\}$ and $S_{(-,-)} = \{|-_X\rangle, |-_Z\rangle\}$. For example, if Alice sends $|+_X\rangle$, she announces the set, $S_{(+,+)}$. Bob measured in the X basis measurement, and he gets the result $|+_X\rangle$; but, since this result is possible for both states in the set, $S_{(+,+)}$, he has to discard the bit, 1, from $|+_X\rangle$. If Bob has measured with the Z basis measurement and gotten $|+_Z\rangle$, again, he cannot discriminate the state sent by Alice. However, if he has measured in the Z basis and got $|-_Z\rangle$, then he knows that Alice has sent $|+_X\rangle$ and adds a zero to his key. In order for the eavesdropper to get the same secret bit as Bob, Eve would need to perform

a measurement using the conjugate bases, X and Z, thus requiring multi-photonic pulses with at least three photons.

Figure 1. Simplified representation of the two-dimensional Bloch sphere where the quantum states and measurement bases are shown. The $BB84$qubits are the non-orthogonal states: $\{|0_Z\rangle, |1_Z\rangle, |0_X\rangle, |1_X\rangle\}$. The measurement bases, Z and X, are shown as vertical and horizontal lines, respectively. If Bob uses basis X (Z) to measure Alice's state, $|i_X\rangle$ ($|i_Z\rangle$), he effectively gets bit i ($i = 0, 1$); otherwise, if he applies basis X (Z) to measure $|i_Z\rangle$ ($|i_X\rangle$), the probability to get i is $\frac{1}{2}$. For example, if Bob measures the $|0_X\rangle$ state with the Z basis, he could obtain $|0_Z\rangle$ or $|1_Z\rangle$ with equal probability.

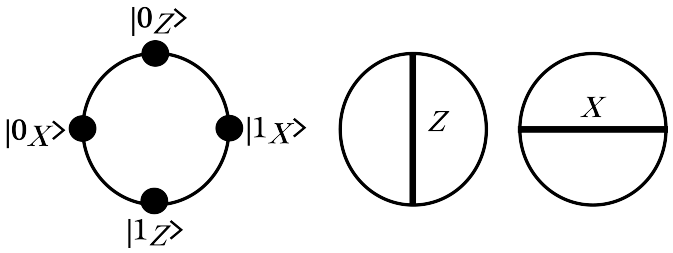
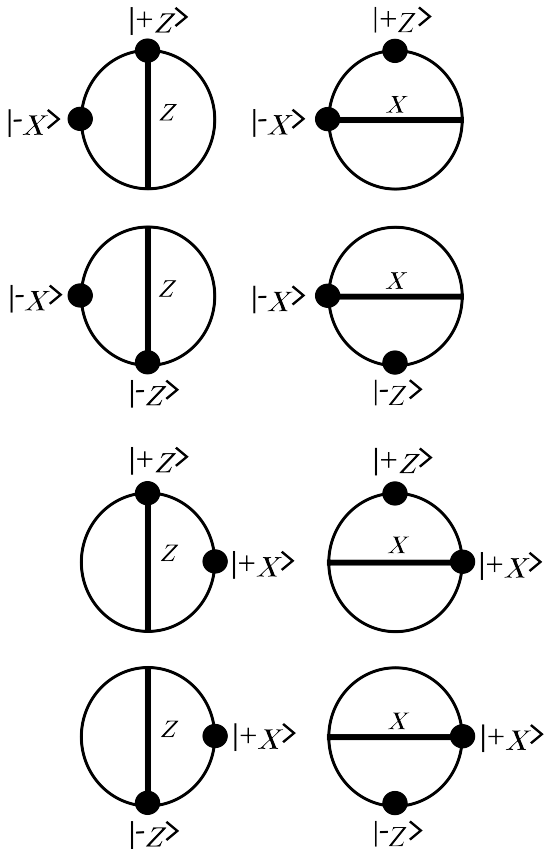


Figure 2. The non-orthogonal states used in the $SARG04$protocol encodes the bit, 0, with the states, $|+_Z\rangle$ and $|-_Z\rangle$, and the bit, 1, is encoded with $|+_X\rangle$ and $|-_X\rangle$.



In the ack-QKD protocol, Alice encodes a classical bit as in the BB84: zero is encoded with $|+_Z\rangle$ and $|-_X\rangle$ and one is encoded with $|-_Z\rangle$ and $|+_X\rangle$. Furthermore, as in the SARG04 protocol, the

ack-QKD uses the four sets of non-orthogonal states $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$, $S_{(+,-)} = \{|+_X\rangle, |-_Z\rangle\}$, $S_{(-,+)} = \{|-_X\rangle, |+_Z\rangle\}$ and $S_{(-,-)} = \{|-_X\rangle, |-_Z\rangle\}$. However, in the ack-QKD protocol, Alice never reveals the set she used, $S_{(+,+)}, S_{(+,-)}, S_{(-,+)}$ or $S_{(-,-)}$. For example, suppose Alice chooses the set $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$. Instead of sending one of the two states, say $|+_X\rangle$ and announcing publicly the sifting instance, $S_{(+,+)}$, she actually sends the two states, $|+_X\rangle$ and $|+_Z\rangle$. Then, Bob measures them using the same basis, X or Z, one by one, as the two states arrive consecutively. If Bob has measured with the X basis, he certainly has obtained $|+_X\rangle$ (after he measured the first state), but he can obtain $|+_X\rangle$ or $|-_X\rangle$ in the second measurement, with a 0.5 probability each outcome. If Bob got $\{|+_X\rangle, |-_X\rangle\}$ after the two measurements, the result is ambiguous for him, and it must discarded. In contrast, if he obtained $\{|+_X\rangle, |+_X\rangle\}$, the result is unambiguous, and he adds a bit, 1, to his key. In order to allow Alice to recover the same bit, Bob announces the basis measurement, X, and the matching condition according to the following rule: $(2M)$ if the two detection events gives a click on the same detector, it includes the cases $\{|+_X\rangle, |+_X\rangle\}, \{|-_X\rangle, |-_X\rangle\}, \{|+_Z\rangle, |+_Z\rangle\}, \{|-_Z\rangle, |-_Z\rangle\}$, or $(2nM)$ if the detection events gives a click on the opposite detectors, e.g., $\{|+_X\rangle, |-_X\rangle\}, \{|-_X\rangle, |+_X\rangle\}$, $\{|+_Z\rangle, |-_Z\rangle\}, \{|-_Z\rangle, |+_Z\rangle\}$. Alice gets the secret bit, because the $\{|+_X\rangle, |+_Z\rangle\}$ states she sent, the X basis and the $(2M)$ measurement result, allow her to infer that Bob certainly got $\{+_X, +_X\}$ (consider the cases depicted in Table 1).

Table 1. An event in which Bob measures with the X basis the two states sent by Alice and obtains a $(2M)$ result.

Alice Sends	Bob Obtains a $(2M)$	Secret Bit
$\{|+_X\rangle, |+_Z\rangle\}$	$\{|+_X\rangle, |+_X\rangle\}$	1
$\{|+_X\rangle, |-_Z\rangle\}$	$\{|+_X\rangle, |+_X\rangle\}$	1
$\{|-_X\rangle, |+_Z\rangle\}$	$\{|-_X\rangle, |-_X\}\rangle$	0
$\{|-_X\rangle, |-_Z\rangle\}$	$\{|-_X\rangle, |-_X\rangle\}$	0

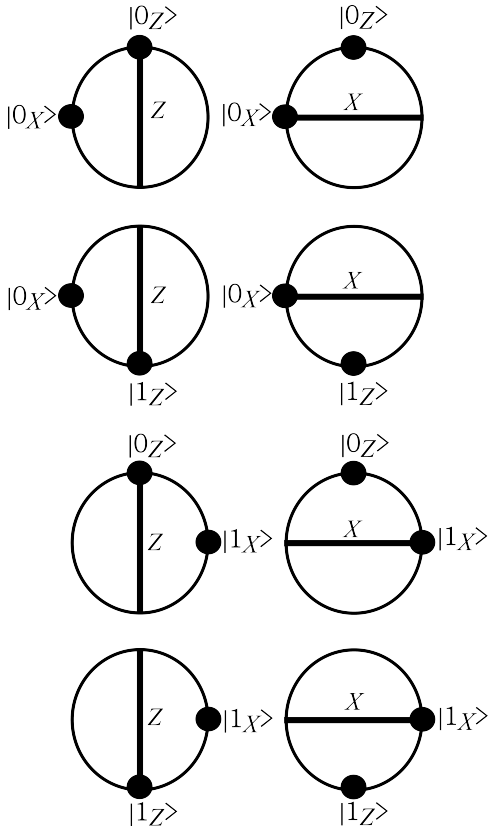
On the other hand, if Bob has measured the two states, $|+_X\rangle$ and $|+_Z\rangle$, with the Z basis, then he would obtain one of the two possible outcomes: $(2M) = \{|+_Z\rangle, |+_Z\rangle\}$ or $(2nM) = \{|-_Z\rangle, |+_Z\rangle\}$. In the first case, he announces publicly the Z basis and the $(2M)$ result; then, Alice and Bob add a zero to the key. In the second case, Bob announces the Z basis and the $(2nM)$ result, but he discards the outcome. In the ack-QKD protocol, the $(2M)$ outcomes are useful to distill secret bits; but, the $(2nM)$ are ambiguous, and those measurement results must be discarded.

3. The ack-QKD Protocol with Non-Orthogonal and Parallel States

In the ack-QKD protocol, one classical bit is encoded using two quantum states. Such encoding is done by means of non-orthogonal or parallel states (see Figures 3 and 4). In quantum physics, if X=$\{|0_X\rangle, |1_X\rangle\}$ and Z=$\{|0_Z\rangle, |1_Z\rangle\}$ are orthonormal bases, then the magnitude of each basis vector is the unity, and any vector in such a space can be written as a linear combination of such a basis. For example, we can rewrite $|0_X\rangle$ as $\frac{1}{\sqrt{2}}|0_Z\rangle + \frac{1}{\sqrt{2}}|1_Z\rangle$. Two qubits, $|0_X\rangle$ and $|0_Z\rangle$, are non-orthogonal if the inner product between them is different from zero, symbolically $\langle 0_X|0_Z\rangle \neq 0$. In this regard,

$\langle 0_X|0_Z\rangle = \frac{1}{\sqrt{2}}(1) + \frac{1}{\sqrt{2}}(0)$ and $\langle 0_X|0_Z\rangle = \frac{1}{\sqrt{2}}$. The inner product of *orthogonal* qubits is zero, e.g., $\langle 0_X|1_X\rangle = 0$, and identical (or parallel) qubits produce the unity under the inner product, thus $\langle 0_X|0_X\rangle = 1$.

Figure 3. In the ack-QKD protocol, Bob uses the basis, X (Z), to measure Alice's two non-orthogonal states, $\{|i_X\rangle, |j_Z\rangle\}$. He effectively gets the bit, i (j), provided he measures $\{|i_X\rangle, |i_X\rangle\}$ or $\{|j_Z\rangle, |j_Z\rangle\}$, which occurs with a $\frac{1}{2}$ probability. For example, if Bob measures the incoming states, $\{|0_X\rangle, |1_Z\rangle\}$, with the Z basis, he could obtain $\{|0_Z\rangle, |1_Z\rangle\}$ or $\{|1_Z\rangle, |1_Z\rangle\}$, which occurs with equal probability. Alice chooses to send randomly two consecutive non-orthogonal states from the set: $\{(|0_X\rangle, |0_Z\rangle), (|0_X\rangle, |1_Z\rangle), (|0_Z\rangle, |1_X\rangle), (|1_Z\rangle, |1_X\rangle)\}$. Such states will be measured by Bob using the same randomly chosen measurement bases, X or Z.



In the ack-QKD protocol, Alice chooses randomly between sending a pair of parallel or non-orthogonal states. At the other side, Bob measures the two consecutive pulses with the same basis measurement, X or Z (see Figures 3 and 4). In this context, the pair of quantum states sent by Alice is called bi-qubit. Parallel bi-qubits define the parallel quantum flow, and non-orthogonal bi-qubits define the non-orthogonal quantum flow.

Now, we summarize the ack-QKD protocol with non-orthogonal and parallel states. The ack-QKD protocol was introduced in [12]. In this reference, the non-orthogonal states are called protocol states, while parallel states are named decoy states:

(1) Alice chooses randomly between a non-orthogonal bi-qubit and a parallel bi-qubit. If she chooses a non-orthogonal bi-qubit, she must pick up randomly one of the following states:

$\{(|0_X\rangle, |0_Z\rangle), (|0_X\rangle, |1_Z\rangle), (|1_X\rangle, |0_Z\rangle), (|1_X\rangle, |1_Z\rangle)\}$; where the order between states X or Z is also chosen randomly. If she chooses a parallel bi-qubit, she must select at random a bi-qubit from the set: $\{(|0_X\rangle, |0_X\rangle), (|1_X\rangle, |1_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_Z\rangle, |1_Z\rangle)\}$. Then, she prepares the bi-qubit and sends it to Bob.

(2) Bob selects randomly the basis, X or Z, to measure the incoming bi-qubit.

(3) Bob announces over the public channel his basis measurement, and he also reveals weather the outcome he obtained is a double-detected event ($2M$ or $2nM$), a single-detected event (S-1 or S-2) or a lost bi-qubit ($2L$) (See discussion below).

(4) In analyzing such results, Alice tells Bob which cases must be discarded.

Figure 4. The parallel bi-qubits include the following states: $\{(|0_X\rangle, |0_X\rangle), (|1_X\rangle, |1_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_Z\rangle, |1_Z\rangle)\}$. Alice randomly interleaves non-orthogonal and parallel states to construct an interleaved quantum flow. Alice can verify the matching cases of the non-orthogonal and the parallel states. However, Eve cannot distinguish between them.

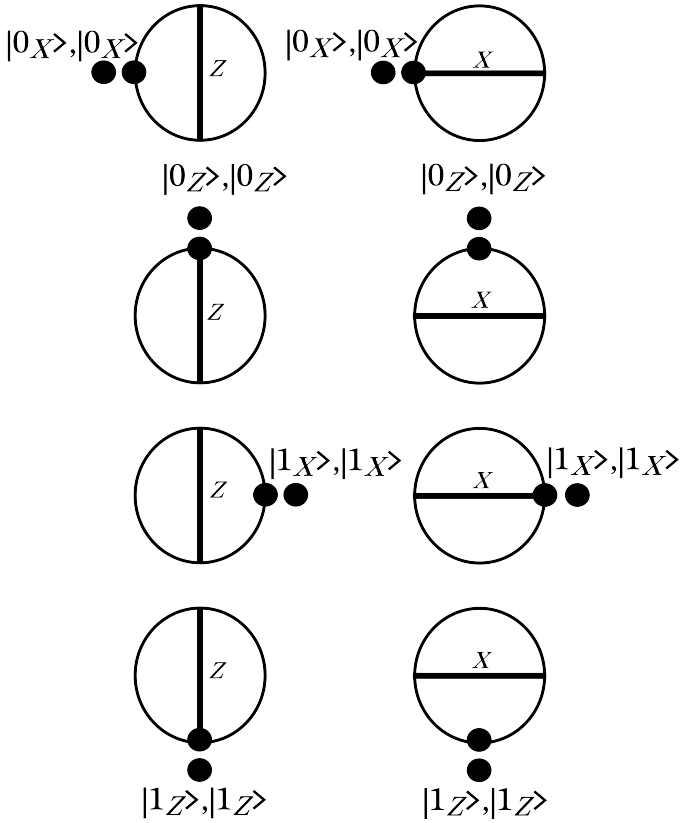


Table 2 shows a running example of the ack-QKD protocol. Each time Bob measures two consecutive states, one of the following detection events can be obtained:

(i) The states produce a double detection event. We use the symbol, $(+,+)$, to denote the photonic gain of the double detection event. If the detection events are registered in the same detector, then we have a double-matching ($2M$) detection event. Otherwise, if the measurement of the states yields opposite result, then we have a double non-matching ($2nM$) detection event. While ($2M$) non-orthogonal results are useful for distilling secret bits, the ($2nM$) results are useless and must be discarded. In the ($2M$) detection event, we say that

the second measurement is the acknowledgment (the ack) of the first measurement. In the example of Figure 3 (upper-right), Alice sends first the qubit, $|0_X\rangle$, and then the qubit, $|0_Z\rangle$. Since Bob uses the X basis to measure both qubits, he measures the qubit, $|0_X\rangle$, as $|0_X\rangle$, but he measures the qubit, $|0_Z\rangle$, as $|0_X\rangle$ or $|1_X\rangle$ with the same 50% probability. In the case that Bob's measurement produces $|0_X\rangle$, we say that this measurement is the ack of the first $|0_X\rangle$ state. Conversely, if Bob obtains $|1_X\rangle$, we say that $|1_X\rangle$ is the negative acknowledgment (the nack) of $|0_X\rangle$.

In a channel with losses, there are two more possible outcomes:

(ii) The single detection event, which occurs when Bob obtains only one detection event, because the other state is lost. We use the symbol, $(\pm, \mp)$, to denote the single detection event. To be more specific, Bob will use the symbol, (S-i), to represent the single detection event, where i can be one or two, depending of the state-number that gives a click after he applies the basis measurement, X or Z, to the two consecutive incoming states. Thus, the number, i, will be announced publicly by Bob.

(iii) The two pulses are lost. This case is represented with the symbol, $(-, -)$, or alternatively as $2L$.

Table 2. Alice sends to Bob the non-orthogonal states $(|0_X\rangle, |0_Z\rangle)$. Table 2 shows all of the possible measurement results at Bob's side.

Alice's bi-qubit	**Bob's Side**			
	Basis Used	**Detection Event**	**Public Disclosure**	**Result**
$|0_X\rangle, |0_Z\rangle$	X	$|0_X\rangle, |0_X\rangle$	X, ($2M$)	useful
	X	$|0_X\rangle, |1_X\rangle$	X, ($2nM$)	discard
	X	$|0_X\rangle, -$	X, (S-1)	useful
	X	$-, |0_X\rangle$	X, (S-2)	discard
	X	$-, |1_X\rangle$	X, (S-2)	discard
	X	$-, -$	X, ($2L$)	discard
	Z	$|0_Z\rangle, |0_Z\rangle$	Z, ($2M$)	useful
	Z	$|1_Z\rangle, |0_Z\rangle$	Z, ($2nM$)	discard
	Z	$-, |0_Z\rangle$	Z, (S-2)	useful
	Z	$|0_Z\rangle, -$	Z, (S-1)	discard
	Z	$|1_Z\rangle, -$	Z, (S-1)	discard
	Z	$-, -$	Z, ($2L$)	discard

In the ack-QKD protocol, Alice and Bob use two consecutive non-orthogonal states to distill one secret bit. Bob announces publicly the basis measurement, X or Z, and the sifting instances he obtained: ($2M$), ($2nM$), (S-1), (S-2) and ($2L$). In addition, Alice use the bits obtained from the single detection events, (S-1) and (S-2), to verify the single photonic gain of the quantum channel.

The reason for using parallel and non-orthogonal bi-qubits in the ack-QKD protocol is that parallel or non-orthogonal states cannot be discriminated by the eavesdropper under the usual basis measurement. If the eavesdropper blocks one-photon states, she changes the photonic gain of single- and double-detection events. However, only Alice can verify the photonic gain of the single and double detection events, parallel and non-orthogonal.

4. The Photon Number Splitting Attack

In the PNS attack, the eavesdropper captures at least one photon from each of the multi-photon states with the aim of storing them in quantum memory, while she blocks the single photon states in the quantum channel. Once Bob has revealed over the public channel the basis measurements he has used, the eavesdropper performs the same measurements on the quantum states she has stored [9].

When the PNS attack is applied to the ack-QKD protocol, the eavesdropper captures at least one photon of the multi-photon states (parallel and non-orthogonal), and she waits for Bob's announcements about the measurement bases he has used in order to apply the same measurements on her stored states. At Bob's side, a distribution over the following sifting instances is obtained: $(2M)$, $(2nM)$, $(S\text{-}1)$, $(S\text{-}2)$ and $(2L)$; where each one may come from parallel or non-orthogonal states, but only Alice knows those results.

After Bob announces both the measurement bases (X or Z) and the sifting instances, Eve performs the measurements using the same measurement bases, and she gets the same bits from the multi-photonic single sifting instances: $(S\text{-}1)$ and $(S\text{-}2)$, parallel and non-orthogonal. Furthermore, the eavesdropper obtains the same results from the $(2M)$ measurements of the parallel and (a half of the) non-orthogonal multi-photonic states. However, she cannot obtain the secret bits from the one-state $(S\text{-}i)$ and $(2M)$ sifting instances, because the eavesdropper cannot distinguish between parallel and non-orthogonal states.

To get the secret bits, Eve blocks the one-photon states, which include single- and double-detection events from parallel and non-orthogonal states. In doing that, Eve introduces an error gain in the photonic gain of the single- and double-detection events. Then, Eve performs a channel substitution increasing the transmittance of the channel. 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 represented as $t_B\eta_D$, 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 $\eta_{BT} = t_B\eta_D T_{AB}$ [8].

However, in replacing T_{AB}, Eve can adjust the photonic gain of the single detection events or the double detection events, but not both simultaneously. In contrast, Alice uses the double matching detection events $(2M)$ and the $(S\text{-}i)$ sifting instances, which are compatible with the states she prepared, to verify corresponding photonic gains, parallel and non-orthogonal.

We define the quantum photonic error gain (QPEG or, simply, ΔQ) as the deviation gain from the reference photonic gain that is caused by Eve's apparatus at Bob's receiver station (see Table 3). We will denote the QPEG of double $(+,+)$ detection events as $\Delta Q_{(+,+)}$ and the QPEG of single $(\pm,\mp)$ detection events as $\Delta Q_{(\pm,\mp)}$. We calculate $\Delta Q_{(+,+)}$ as the difference $Q_{(+,+)_{AB}} - Q_{(+,+)_{EB}}$, where the

symbol, $(+,+)_{AB}$, defines the reference photonic gain at calibration time 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 at running time). Similarly, we calculate $\Delta Q_{(\pm,\mp)}$ as $Q_{(\pm,\mp)_{AB}} - Q_{(\pm,\mp)_{EB}}$, where we use the subindex of $(\pm,\mp)_{AB}$ and $(\pm,\mp)_{EB}$ with the same purpose.

As mentioned before, the eavesdropper blocks the one-photon states and she performs a channel substitution to adjust the transmittance of the channel, T_{AB}. However, this activity produces error gains in the single- and double-detection events that are verifiable by Alice.

The QPEG after Eve blocks the one-photon states can be written as $\Delta Q = Q_1$, where Q_1 is the gain of the one-photon states, and it must be computed for the single- and the double-detection events. The error gain is $\Delta Q_{(+,+)} = Q^2_{1_{(+)}} = Q_1^2$ and $\Delta Q_{(\pm,\mp)} = Q_1 \cdot Q_{(-)}$ for double-detection events and single-detection events, respectively, where $Q_{1_{(+)}} = (Y_0 + \eta - Y_0\eta)\mu e^{-\mu}$, $Q_{(-)} = e^{-\mu\eta} - Y_0$, η is the transmittance of the channel and the detectors at Bob's side of the one-photon states and Y_0 is the background noise according to [8].

To remain hidden in the channel, the eavesdropper must adjust the transmittance, T_{AB}, to achieve the two reference photonic gains, $Q_{(+,+)}$ and $Q_{(\pm,\mp)}$, for the double detection events and single detection events, respectively. Since $Q_{(+,+)} \neq Q_{(\pm,\mp)}$, Eve can adjust T_{AB} to Q_1^2 or $Q_1 \cdot Q_{(-)}$, but not both simultaneously. In other words, she cannot fulfill the conditions $\Delta Q_{(+,+)} = 0$ and $\Delta Q_{(\pm,\mp)} = 0$; thus, the attack becomes detectable. If the eavesdropper adjusts T_{AB}, so that it produces a photonic deviation in one or in both gains, she will introduce a detectable QBER to the system.

As a consequence, Eve knows that she must not change T_{AB}, otherwise she will be detected. Now, the QBER that Eve produces is $\frac{0.5Q_0+0.5^2Q_1+0.5^3Q_2+...}{Q_0+Q_1+Q_2+...}$, because the QBER of single-detection events is 0.5^2, as in the BB84. In contrast, in absence of the attack, the QBER of the system is given by $\frac{0.5Q_0+e_d(Q_1+Q_2+Q_3+...)}{Q_0+Q_1+Q_2+...}$, where e_d is the detection error according to [8].

Table 3. The reference photonic gain of the double $(+,+)$ detection events is written as $Q_{(+,+)}$, and the gain of the single detection events $(\pm,\mp)$ is represented as $Q_{(\pm,\mp)}$, where Y_0 is the background noise, μ is the mean value of the photonic source and η_{BT} is the overall efficiency at Bob's side.

Quantum Flow	**Alice**	**Bob**
$Q_{(-,-)}$	$e^{-2\mu}$	$(e^{-\mu\eta_{BT}} - Y_0)^2$
$Q_{(+,+)}$	$(1 - e^{-\mu})^2$	$(Y_0 + 1 - e^{-\mu\eta_{BT}})^2$
$Q_{(\pm,\mp)}$	$2e^{-\mu}(1 - e^{-\mu})$	$2(e^{-\mu\eta_{BT}} - Y_0)(Y_0 + 1 - e^{-\mu\eta_{BT}})$

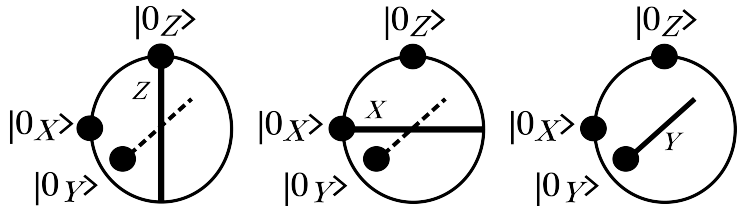
Since the probability of getting a (compatible) matching measurement from the non-orthogonal double detection events is 0.5^2, we derived the error rate of the non-orthogonal double detection events as $\frac{0.5(Q_0+Q_1)+0.5^2Q_2+0.5^3Q_3+...}{Q_0+Q_1+Q_2+...}$. The QBER from the multi-photonic non-orthogonal states decrease by half for each copy of quantum states in Eve's memory. By contrast, the multi-photonic parallel states do not contribute to increasing the QBER, because Bob reveals the basis measurements he used.

5. The 3Q Protocol

The ack-QKD protocol is a two-quantum-flow based protocol (2Q for simplicity), but it can be extended to a three-quantum-flow protocol (3Q)). In the 3Q protocol, Alice chooses randomly three non-orthogonal states from the set: $\{(|0_X\rangle, |0_Y\rangle, |0_Z\rangle), (|0_X\rangle, |0_Y\rangle, |1_Z\rangle), (|0_X\rangle, |1_Y\rangle, |0_Z\rangle), (|0_X\rangle, |1_Y\rangle, |1_Z\rangle), (|1_X\rangle, |0_Y\rangle, |0_Z\rangle), (|1_X\rangle, |0_Y\rangle, |1_Z\rangle), (|1_X\rangle, |1_Y\rangle, |0_Z\rangle), (|1_X\rangle, |1_Y\rangle, |1_Z\rangle)\}$.

The corresponding parallel states are: $\{(|0_X\rangle, |0_X\rangle, |0_X\rangle), (|0_Y\rangle, |0_Y\rangle, |0_Y\rangle), (|0_Z\rangle, |0_Z\rangle, |0_Z\rangle), (|1_X\rangle, |1_X\rangle, |1_X\rangle), (|1_Y\rangle, |1_Y\rangle, |1_Y\rangle), (|1_Z\rangle, |1_Z\rangle, |1_Z\rangle)\}$. Figure 5 shows an example of the non-orthogonal states, e.g., $(|0_X\rangle, |0_Y,\rangle |0_Z\rangle)$.

Figure 5. A representation of the non-orthogonal states of the three-quantum-flow protocol (3Q) protocol in the three-dimensional Bloch sphere. The polarization states, $|0_X\rangle$, $|0_Y\rangle$ and $|0_Z\rangle$, are mutually non-orthogonal. The conjugated basis measurements are X, Y and Z.



In the 3Q protocol, the eavesdropper cannot adjust simultaneously the three reference photonic gains, $Q_{(+3)}$, $Q_{(+2)}$ and $Q_{(+1)}$, for the triple-, double- and single-detection events, respectively. We found for the 3Q protocol that the corresponding error rate is $\frac{0.5(Q_0+Q_1+Q_2)+0.5^2Q_3+0.5^3Q_4+...}{Q_0+Q_1+Q_2+...}$.

The security of the ack-QKD protocol is supported by Alice's capability to verify the photonic gain of single matching (S-i) and double matching $(2M)$ detection events, parallel and non-orthogonal, which cannot be controlled by the eavesdropper without introducing errors.

The ack-QKD protocol preserves the general behavior of the BB84 protocol, which includes the usual optical equipment. However, as the rate of the double detection events is small ($\sim 10^{-8}$), the protocol requires that the amount of photonic pulses sent by the transmitter station to be large and fast, which can be achieved in practice with the current technology (it may reach the order of 10^8 pulses per second). Furthermore, the mean value of the photonic source (μ) can be increased in order to augment the final gain of double-detection events, e.g., when $\mu \sim 0.5$, the gain goes to 10^{-7} and $\mu \sim 1$ increases the gain to 10^{-6} in the 2Q version of the protocol.

6. The Unstructured ack-QKD Protocol

In the ack-QKD protocol, most of the bi-qubits pulses sent by Alice arrive to Bob's station as single pulses that behave as BB84 pulses. Usually, in QKD implementations, it is necessary to reduce after-pulsing errors in the protocol. To achieve this, Alice sends pulses at well-defined times, and Bob accepts a detection click only during a narrow time window, discarding events outside these time windows. For any QKD system, one major limitation is the dead time of the avalanche photo diodes (APD), which is the hold-off time following each detection event during which no photon can be

detected. If a photon click occurs in a certain pulse, the probability to have one or more photon clicks within the next few gate pulses immediately following the avalanche is very low (see [13]). In such a case, it seems suitable to hold-off on an appropriate number of gate pulses after each registered detection click. However, in the ack-QKD protocol, we must not hold off gate pulses in order to allow Bob's detectors to be capable of detecting consecutive photonic pulses.

We will introduce the unstructured ack-QKD protocol, where Alice chooses, as usually in the ack-QKD, the pairs of quantum states, parallel and non-orthogonal, but she sends the quantum states as single qubits, choosing to send each of them randomly (See Table 4). After Bob measures the quantum states choosing randomly the basis measurement, X or Z, for each pulse, Alice reveals the bi-qubit pairs, but she does not specify if each pair corresponds to parallel or non-orthogonal states. Once Alice reveals the bi-qubit pairs, Bob is able to look for the matching and non-matching detection events, allowing himself, after this step, to follow the sifting procedure of the ack-QKD protocol.

Table 4. Simulation of the unstructured ack-QKD protocol over an ideal channel. Alice sends, out of order, some bi-qubits of the ack-QKD protocol. Once Bob has revealed his basis measurements, Alice announces the bi-qubits she used in order to allow Bob to get the secret bits from the matching events.

1.Alice	$\|0_Z\rangle$	$\|1_Z\rangle$	$\|0_X\rangle$	$\|0_Z\rangle$	$\|0_Z\rangle$	$\|0_X\rangle$	$\|0_X\rangle$	$\|1_Z\rangle$	$\|1_Z\rangle$	$\|1_X\rangle$	$\|1_X\rangle$	$\|1_Z\rangle$	$\|1_X\rangle$	$\|0_Z\rangle$
2.Bob	X	X	X	Z	Z	X	Z	X	X	Z	X	Z	Z	Z
3.Alice	2	5	6	1	7	3	1	4	3	6	4	5	2	7

Suppose Alice wants to send the following quantum pairs of the ack-QKD protocol: $(|0_X\rangle, |0_Z\rangle)_1, (|1_X\rangle, |0_Z\rangle)_2, (|0_X\rangle, |1_Z\rangle)_3, (|1_X\rangle, |1_Z\rangle)_4, (|1_Z\rangle, |1_Z\rangle)_5, (|0_X\rangle, |1_X\rangle)_6, (|0_Z\rangle, |0_Z\rangle)_7$.

However, as can be seen in the Step 1, Alice sends such states individually and randomly. In Step 2, Bob chooses the measurement basis for each incoming quantum state at random. Then, in Step 3, Alice announces publicly the corresponding quantum states, so Bob determines on which cases he applied correctly his basis measurement. Once Alice reveals her bi-qubit pairs, Bob is able to look for the matching and non-matching detection events, allowing himself, after this step, to follow the sifting procedure of the ack-QKD protocol. In this example, Bob applied the same basis measurement over the quantum pairs, 1, 3, 4 and 7.

Since the probability of getting the correct (same) basis measurement for the corresponding pair of pulses is 50%, the photonic gains decrease by a half. The unstructured ack-QKD protocol is feasible, because the photonic gains depend on the final computation of two independent detection probabilities, which can be consecutive events or not.

It should be noticed that the unstructured ack-QKD protocol can be applied to the 3Q version of the protocol. To the best of our knowledge, the ack-QKD is the first protocol that uses qubits of two "colors", namely the non-orthogonal bi-qubit and the parallel bi-qubit, which are useful for composing two quantum flows randomly interleaved. We believe that this may open up new possibilities to increase the ultimate security of the QKD protocols towards the achievement of a device independent protocol.

7. Conclusions

We have discussed the security of the ack-QKD protocol with parallel and non-orthogonal states in the presence of the photon number splitting (PNS) attack, which is detected firstly by means of the quantum photonic error gain (ΔQ) of the protocol, but also by the QBER caused by the eavesdropper. The PNS attack is detectable, because the eavesdropper cannot perform a channel substitution without being detected, so $\Delta \mathrm{Q} \neq 0$ or QBER$\neq 0$.

We introduced the unstructured ack-QKD protocol to avoid the consecutiveness of the states so that methods to reduce the dead time of detectors can be applied.

We emphasize that the ack-QKD protocol does not require additional hardware other than the BB84 protocol hardware and that it can be implemented mostly at a high level as a software application.

Acknowledgments

The authors would like to thank Centro Nacional de Metrología (CENAM) of México, and Tecnológico de Monterrey Campus Estado de México, for the support in developing this research. Salvador E. Venegas-Andraca would like to thank his family for their unconditional support. He would also like to acknowledge the financial support of CONACyT-SNI (SNI member number 41594).

Author Contributions

LALP was responsible for the ack-QKD protocol definition and the security analysis. JMLR contributed to the discussion of the ack-QKD protocol improving the design, security analysis and the article revision. EDL contributed to the article revision and discussion of the ack-QKD protocol. SEVA contributed to the article revision. All authors have read and approved the final manuscript.

A. The Photonic Gain of the 2Q Protocol

We represent the gain of single detected events, such as $Q_{(\pm,\mp)}$, and the gain of double-detected events, such as $Q_{(+,+)}$. From [8], we know that for a photonic source with mean μ, the photonic gain of non-empty pulses, $Q_{(+)}$, is $Y_0 + 1 - e^{-\mu\eta_{BT}}$, where η_{BT} is the overall efficiency at Bob's side and Y_0 is the background noise. Now, let us assume that the gain of two consecutive non-empty pulses is independent of each other. Then, we can compute $Q_{(+,+)}$ by multiplying the individual photonic gains $(Q_0Q_0 + Q_0Q_1 + ... + Q_0Q_i + ...) + (Q_1Q_0 + Q_1Q_1 + ...Q_1Q_i + ...) + ...$, with $i = 0, 1, 2, ...$, which can be rewritten as $Q_0(Q_0 + Q_1 + ... + Q_i + ...) + Q_1(Q_0 + Q_1 + ... + Q_i + ...) + ... + Q_j(Q_0 + Q_1 + ... + Q_i + ...) + ...$, with $j = 0, 1, 2, ...$ Thus, factorizing, we get $\sum_{i=0}^{\infty} Q_i \sum_{j=0}^{\infty} Q_j$, but replacing $\sum_{k=0}^{\infty} Q_k$ by $Y_0 + 1 - e^{-\mu\eta_{BT}}$, the photonic gain of two consecutive non-empty pulses can be written as $Q_{(+,+)}$ is $(Y_0 + 1 - e^{-\mu\eta_{BT}})^2$.

Similarly, we can compute the corresponding photonic gain for single detection events, $Q_{(\pm,\mp)}$. Such detection events consist in detecting one pulse, while the other measurement gives no click or *vice versa*. Thus, the symbol, $(+,-)$, means that the first state produces a click, while the second state is lost (no-click). The other symbol, $(-,+)$, is used to represent the event where the order of the detection is inverted. Since the gain of empty and non-empty pulses are $e^{-\mu\eta_{BT}} - Y_0$ and $Y_0 + 1 - e^{-\mu\eta_{BT}}$, respectively,

we have that the gain of single-detected events $Q_{(\pm,\mp)}$ can be written as the product $2\cdot(e^{-\mu\eta_{BT}}-Y_0)(Y_0+1-e^{-\mu\eta_{BT}})$. In such a manner, the photonic gains of the 3Q protocol can be derived.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10-19 December, 1984; pp. 175–179.
2. Lunghi, C.; Barreiro, C.; Guinnard, O.; Houlmann, R.; Jiang, X.D.; Itzler, M.A.; Zbinden, H. Free-running single-photon detection based on a negative feedback InGaAs APD. *J. Mod. Opt.* **2012**, *59*, 1481–1488.
3. Brassard, G.; Lutkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333.
4. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28.
5. Gottesman, D.; Lo, H.-K. Proof of security of quantum key distribution with two-way classical communication. *IEEE Trans. Inf. Theory* **2003**, *49*, 457–475.
6. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444.
7. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dusek, M.; Lutkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301.
8. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326.
9. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901.
10. Takesue, H.; Diamanti, E.; Honjo, T.; Langrock, C.; Fejer, M.M.; Inoue, K.; Yamamoto, Y. Differential phase shift quantum key distribution experiment over 105 km fiber. *New J. Phys.* **2005**, *7*, 232.
11. Stucki, D.; Fasel, S.; Gisin, N.; Thoma, Y.; Zbinden, H. Coherent one-way quantum key distribution. In Proceedings of the SPIE, Photon Counting Applications, Quantum Optics, and Quantum Cryptography, Prague, Czech Republic, 11 May 2007; Volume 6583.
12. Lizama, L.; Lopez, J.M.; de Carlos Lopez, E.; Venegas-Andraca, S.E. Enhancing quantum key distribution (QKD) to address quantum hacking. In *Procedia Technology by Elsevier*, Proceedings of the the 2012 Iberoamerican Conference on Electronics Engineering and Computer Science CIIECC, Guadalajara, Jal., México, 16-18 May, 2012; Vol. 3; pp. 80–88

13. Bouzid, A.; Park, J.-B.; Moon, S. Effects of the active hold-off technique in 1.55-μm single-photon detection. *J. Korean Phys. Soc.* **2010**, *56*, 1418–1422.