Quantum Information and Computation, Vol. 7, No. 7 (2007) 665–688
© Rinton Press

SEQUENTIAL ATTACKS AGAINST DIFFERENTIAL-PHASE-SHIFT QUANTUM KEY DISTRIBUTION WITH WEAK COHERENT STATES

MARCOS CURTY[1,2], LUCY LIUXUAN ZHANG[1], HOI-KWONG LO[1], NORBERT LÜTKENHAUS[2,3]

1 Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto Toronto, Ontario, M5S 3G4, Canada

2 Institute for Quantum Computing, University of Waterloo Waterloo, Ontario, N2L 3G1, Canada

3 Quantum Information Theory Group, Institut für Theoretische Physik I, and Max-Planck Research Group, Institute of Optics, Information and Photonics, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany

Received September 22, 2006
Revised March 22, 2007

We investigate limitations imposed by sequential attacks on the performance of differential-phase-shift quantum key distribution protocols that use pulsed coherent light. In particular, we analyze two sequential attacks based on unambiguous state discrimination and minimum error discrimination, respectively, of the signal states emitted by the source. Sequential attacks represent a special type of intercept-resend attacks and, therefore, they provide ultimate upper bounds on the maximal distance achievable by quantum key distribution schemes.

Keywords: quantum cryptography, quantum key distribution, differential-phase-shift quantum key distribution, sequential attack, intercept-resend attack, security

Communicated by: S Braunstein & H Zbinden

1. Introduction

Quantum key distribution (QKD) [1, 2] is a technique that exploits quantum effects to establish a secure secret key between two parties (usually called Alice and Bob). This secret key is the essential ingredient of the one-time-pad or Vernam cipher [3], the only known encryption method that can provide information-theoretic secure communications.

The first complete scheme for QKD is that introduced by Bennett and Brassard in 1984 (BB84 for short) [4]. A full proof of the security for the whole protocol has been given in Ref. [5, 6, 7, 8]. After the first demonstration of the feasibility of this scheme [9], several long-distance implementations have been realized in the last years (see, for instance, Ref. [10, 11, 12, 13, 14, 15] and references therein). However, these practical approaches differ in many important aspects from the original theoretical proposal which demands technologies that are beyond our present experimental capability. In particular, the signals emitted by the source, instead of being single-photons, are usually weak coherent pulses (WCP) with typical average photon numbers of 0.1 or higher. Moreover, the detectors employed by the receiver have a

low detection efficiency and are noisy due to dark counts. These facts, together with the loss and the noise introduced by the quantum channel, jeopardize the security of the protocol, and lead to limitations of rate and distance that can be achieved by these techniques [16, 17].

The main security threat of QKD based on WCP arises from the fact that some pulses contain more than one photon prepared in the same polarization state. Now, an eavesdropper (Eve) can perform, for instance, the so-called *Photon Number Splitting* (PNS) attack on the multi-photon pulses [16]. This attack provides Eve with full information about the part of the key generated from the multi-photon signals, without causing any disturbance in the signal polarization. As a result, it turns out that the BB84 protocol with WCP can give a key generation rate of order $O(\eta^2)$, where η denotes the transmission efficiency of only the quantum channel [18, 19].

To obtain higher secure key rates over longer distances, different QKD schemes which are robust against the PNS attack have been proposed in recent years. One of these schemes is the so-called decoy-states [20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33], where Alice randomly varies the mean photon number of the signal states sent to Bob by using different intensity settings. This technique delivers a key generation rate of order $O(\eta)$ [20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33]. Other possibility is based on the transmission of two non-orthogonal coherent states together with a strong reference pulse [34]. This scheme has been analyzed in Ref. [35, 36], where it was confirmed that also in this scenario the secure key rate is of order $O(\eta)$. Finally, another possible approach is the use of differential-phase-shift (DPS) QKD protocols [37, 38, 39, 40, 41]. In this kind of schemes, Alice sends to Bob a train of WCP whose phases are randomly modulated by 0 or π. On the receiving side, Bob measures out each incoming signal by means of an interferometer whose path-length difference is set equal to the time difference between two pulses. In this case, however, a secure key rate of order $O(\eta)$ has only been proven so far against a particular type of individual attacks where Eve acts on *photons* individually, rather than *signals* [39]. Whether DPS QKD is secure against the most general attack remains an important open question.

In this paper, we investigate limitations imposed by sequential attacks on the performance of DPS QKD protocols. In this kind of attacks, Eve measures out every coherent state emitted by Alice and prepares new signal states, depending on the results obtained, that are given to Bob. Whenever Eve obtains a predetermined number of consecutive successful measurement outcomes, then she prepares a train of WCP that is forwarded to Bob. Otherwise, Eve sends vacuum signals to Bob to avoid errors. Sequential attacks constitute a special type of intercept-resend attacks [42, 43, 44] and, therefore, they provide ultimate upper bounds on the performance of quantum key distribution schemes [45, 46]. Here we shall consider a conservative definition of security, *i.e.*, we assume that Eve can control some flaws in Alice's and Bob's devices (*e.g.*, the detection efficiency and the dark count probability of the detectors), together with the losses in the channel, and she exploits them to obtain maximal information about the shared key.

We analyze two possible sequential attacks. In the first one, Eve realizes unambiguous state discrimination (USD) of Alice's signal states [42, 47, 48, 49, 50, 51]. When Eve identifies unambiguously a signal state sent by Alice, she considers this result as successful. Otherwise, she considers it a failure. In the second attack, Eve performs first a filtering operation on each signal emitted by Alice and, afterwards, she measures out each successful filtered state

following the approach of minimum error discrimination (MED) [52, 53], *i.e.*, she guesses the identity of the filtered state with the minimum probability of making an error. (See also Ref. [44].) As a result, we obtain upper bounds on the maximal distance achievable by DPS QKD schemes as a function of the error rate in the sifted key, the double click rate at Bob's side, and the mean photon-number of the signals sent by Alice.

Instead of using an USD measurement on each signal state sent by Alice, like in the first sequential attack that we consider, Eve could as well employ the same detection device like Bob. This sequential attack was very briefly introduced in Ref. [39]. A successful result is now associated with obtaining a click in Eve's apparatus, while a failure corresponds to the absence of a click. However, since Alice's signal states are typically coherent pulses with small average photon number, the probability of obtaining a successful result in this scenario is always smaller than the one of a sequential USD attack. Therefore, a sequential USD attack can provide tighter upper bounds on the performance of DPS QKD protocols than those derived from an eavesdropping strategy where Eve uses the same measurement apparatus like Bob.

A different QKD scheme, but also related to DPS QKD protocols, has been proposed recently in Ref. [56]. (See also Ref. [57].) However, since the abstract signal structure of this protocol is different from the one of DPS QKD schemes, the analysis contained in this paper does not apply to that scenario. Sequential attacks against the QKD protocol introduced in Ref. [56] have been investigated in Ref. [58] following a similar approach as in this paper.

The paper is organized as follows. In Sec. 2 we describe in more detail DPS QKD protocols. Then, in Sec. 3, we present sequential attacks against DPS QKD schemes. Sec. 4 includes the analysis for a sequential USD attack. Here we obtain an upper bound on the maximal distance achievable by DPS QKD schemes as a function of the error rate, the double click rate at Bob's side, and the mean photon-number of Alice's signal states. Similar results are derived in Sec. 5, now for the case of sequential attacks based on MED of the signals sent by Alice. Finally, Sec. 6 concludes the paper with a summary.

2. Differential-phase-shift QKD

The setup is illustrated in Fig. 1 [37, 38, 39, 40, 41].

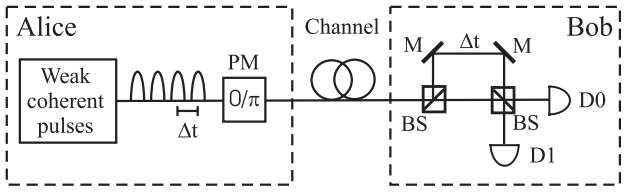

Fig. 1. Basic setup of a DPS QKD scheme. PM denotes a phase modulator, BS, a 50 : 50 beam-splitter, M, a mirror, D0 and D1 are two photon detectors, and Δt represents the time difference between two consecutive pulses.

Alice prepares first a train of coherent states $|\alpha\rangle$ and, afterwards, she modulates, at random and independently every time, the phase of each pulse to be 0 or π. As a result, she produces a random train of signal states $|\alpha\rangle$ or $|-\alpha\rangle$ which are then sent to Bob through the quantum channel. On the receiving side, Bob uses a 50 : 50 beam-splitter to divide the incoming pulses

into two possible paths of different length and then he recombines them again using another $50:50$ beam-splitter. The time delay introduced by Bob's interferometer is set equal to the time difference Δt between two pulses. Whenever the relative phase between two consecutive pulses is 0 ($\pm\pi$) only the photon detector $D0$ ($D1$) may produce a "click" (at least one photon is detected). For each detected event, Bob records the exact time where he obtained a click and the actual detector that fired.

Once the quantum communication phase is completed, Bob uses a classical authenticated channel to announce the time instances where he detected at least one photon. From this information, together with the knowledge of the phase value used to modulate each pulse, Alice can infer which photon detector fired at Bob's side at each given time. Then, Alice and Bob can agree, for instance, to select a bit value "0" whenever the photon detector $D0$ clicked, and a bit value "1" if the detector $D1$ fired. In an ideal scenario, Alice and Bob end up with an identical string of bits representing the *sifted key*. Due to the noise introduced by the quantum channel together with possible imperfections of Alice's and Bob's devises, however, the sifted key typically contains some errors. Then, Alice and Bob perform error-correction to reconcile the data, and privacy amplification to decouple the data from Eve. (See, for instance, Ref. [1, 2].)

In the next section we analyze simple sequential attacks against the DPS QKD protocol introduced above that are particularly suited for the signal states and detection methods employed by Alice and Bob, together with the attenuation introduced by the channel. Let us emphasize here that these attacks might not be optimal, but, as we will show below, they already impose strong restrictions on the performance of DPS QKD schemes with weak coherent pulses.

3. Sequential attacks against differential-phase-shift QKD

A sequential attack can be seen as a special type of intercept-resend attack. First, Eve measures every coherent state emitted by Alice with a detection apparatus located very close to the sender. Afterwards, she transmits each measurement result through a lossless classical channel to a source close to Bob. Whenever Eve obtains a predetermined number of consecutive *successful* measurement outcomes, this source prepares a train of new signal states that is forwarded to Bob. Otherwise, Eve sends vacuum signals to Bob to avoid errors. Whether a measurement result is considered to be successful or not and which type of non-vacuum states Eve sends to Bob depends on Eve's particular eavesdropping strategy and on her measurement device. Sequential attacks transform the original quantum channel between Alice and Bob into an entanglement breaking channel [54, 55] and, therefore, they do not allow the distribution of quantum correlations needed to establish a secret key [45, 46].

We begin by introducing Eve's measurement apparatus. As mentioned previously, we shall study two possible alternatives. Each alternative provides a different sequential attack. Moreover, in both cases, we shall consider the conservative security assumption that Eve always has access to a local oscillator that is phase-locked to the coherent light source employed by Alice. In experiments, the number of pulses over which the phase remains stable will be limited, but this effect is outside of the protocol model we consider here.

In the first attack, Eve realizes USD [47, 48, 49, 50, 51] of Alice's signal states. Whenever Eve identifies unambiguously a signal state sent by Alice, *i.e.*, she determines without error

whether it is $|\alpha\rangle$ or $|-\alpha\rangle$, she considers this result as successful. If the measurement outcome corresponds to an inconclusive result then she considers it a failure. The second eavesdropping strategy can be decomposed into two steps: first, Eve performs a filtering operation on each signal state sent by Alice with the intention to make them, with some finite probability, more "distinguishable". A failure refers now to those signal states for which the filtering operation does not succeed. Afterwards, Eve measures out each successful filtered state following the approach of MED [52, 53]. Her goal is to guess the identity of the filtered states with the minimum probability of making an error. Notice that the first eavesdropping strategy can be considered as a special case of the second eavesdropping strategy where the probability that Eve makes an error in distinguishing a state $|\alpha\rangle$ and $|-\alpha\rangle$ is exactly zero. We shall denote as p_{succ} the probability that Eve obtains a successful result whatever the measurement device she employs.

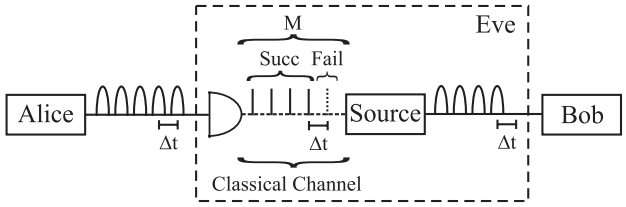

Fig. 2. Illustration of a sequential attack. In this example the length of each block is $M = 5$, the minimum number of consecutive successful results within a block is given by $M_{min} = 3$, and we assume that Eve obtains $m = 4$ consecutive successful results within a block. A successful outcome is represented with a vertical solid line in the classical channel, while a failure result is denoted with a vertical dashed line.

In order to evaluate her measurement outcomes, we shall consider that Eve divides her data into different blocks of length M, where each block contains M consecutive measurement results. Moreover, we assume that Eve analyzes each block of data independently, *i.e.*, without considering the data included in other blocks. As we will show later on, this eavesdropping strategy will necessarily create some error rate that decreases when incrementing the block length M. In this scenario, we define the integer parameter M_{min} as the minimum number of consecutive successful results within a block that Eve needs to obtain in order to send Bob a new train of coherent states $|\beta e^{i\theta_j}\rangle$. This definition of M_{min} arises from the particular eavesdropping strategies that we consider here, and the role of this parameter M_{min} will become clear later on. More precisely, if m denotes the total number of consecutive successful outcomes obtained by Eve within a block, then, whenever m is bigger than M_{min}, Eve prepares m consecutive coherent states $|\beta e^{i\theta_1}\rangle, |\beta e^{i\theta_2}\rangle, \ldots, |\beta e^{i\theta_m}\rangle$, together with $M - m$ vacuum states for those unsuccessful results within the block and sends these signals to Bob. On the other hand, if $m < M_{min}$ Eve sends to Bob M vacuum states. The case $m = M_{min}$ deserves a special attention. We shall consider that in this case Eve employs a probabilistic strategy that combines the two previous ones. In particular, we assume that Eve sends to Bob M_{min} consecutive coherent states $|\beta e^{i\theta_1}\rangle, |\beta e^{i\theta_2}\rangle, \ldots, |\beta e^{i\theta_{M_{min}}}\rangle$ with probability q and, with probability $1 - q$, she sends to Bob M vacuum states. That is, the parameter q allows Eve to smoothly fit her eavesdropping strategy to the observed data. Moreover, for simplicity,

we shall consider that M_{min} satisfies $\lfloor M/2+1 \rfloor \leq M_{min} < M$. This condition guarantees that, within each block of length M, there is, at most, only *one* subblock containing M_{min}, or more, consecutive successful results.

The angle θ_j of a coherent state $|\beta e^{i\theta_j}\rangle$ prepared by Eve depends on her particular measurement strategy. When she utilizes an USD measurement, then $\theta_j = 0$ if the state identified by her measurement is $|\alpha\rangle$, and $\theta_j = \pi$ if the state identified is $|-\alpha\rangle$. A similar criterion can also be applied to the case where Eve performs a filtering operation followed by a MED measurement on the successful filtered states: If the result obtained is associated with the signal state $|\alpha\rangle$ then $\theta_j = 0$, otherwise $\theta_j = \pi$. Fig. 2 shows a graphical representation of such a sequential attack for the case $M = 5$ and $M_{min} = 3$. In this example, moreover, we assume that Eve obtains $m = 4$ consecutive successful results within a block.

Next, we obtain an expression for the gain of a sequential attack, *i.e.*, the probability that Bob obtains a click per signal state sent by Alice, as a function of the parameters M, M_{min}, q, the probability p_{succ} of obtaining a successful result, and the mean photon-number $\mu_\beta = |\beta|^2$ of the coherent states sent by Eve. As we will show, the gain of a sequential attack is directly related with the maximal distance achievable by a QKD scheme. Afterwards, we study the two sequential attacks introduced above in more detail. The objective is to find an expression for the quantum bit error rate (QBER) introduced by Eve, and for the resulting double click rate at Bob's side in each of these two attacks.

3.1. *Gain of a sequential attack*

The gain of a sequential attack is defined as N_{clicks}/N, where N_{clicks} represents the average total number of clicks obtained by Bob, and N is the total number of signal states sent by Alice. In this definition, we consider that double clicks contribute to N_{clicks} like single clicks. The parameter N_{clicks} can be expressed as $N_{clicks} = (N/M)N^M_{clicks}$, with N^M_{clicks} denoting the average total number of clicks per block of length M at Bob's side. With this notation, the gain of a sequential attack, that we shall denote as G, can then be written as

$$G = \frac{1}{M} N^M_{clicks}. \tag{1}$$

Next, we obtain an expression for N^M_{clicks}. We shall distinguish several cases, depending on the number m of coherent states $|\beta e^{i\theta_1}\rangle, |\beta e^{i\theta_2}\rangle, \ldots, |\beta e^{i\theta_m}\rangle$ that Eve sends to Bob inside a given block and the position of these coherent states in the block [a]. These cases are illustrated in Fig. 3, where we also include the *a priori* probabilities to be in each of these scenarios. Note, however, that the average total number of clicks in each of these cases will also depend on whether the last signal state of a previous block is actually a coherent state or not. To include this boundary effect between blocks in our analysis, we shall always distinguish two possible alternatives for each case included in Fig. 3, depending on the identity of the last signal state contained in the previous block. The probability of this last signal being a coherent state, that we shall denote as p, is calculated in Appendix 1 and it is given by

$$p = \big[p_{succ} + (1 - p_{succ})q\big] p^{M_{min}}_{succ}. \tag{2}$$

[a] In order to simplify our notation, from now on we will employ the term "coherent state" only to denote those light pulses with a mean photon number bigger than zero. A light pulse with an average photon number equal to zero, although it is also a coherent state, will be always denoted as a "vacuum state".

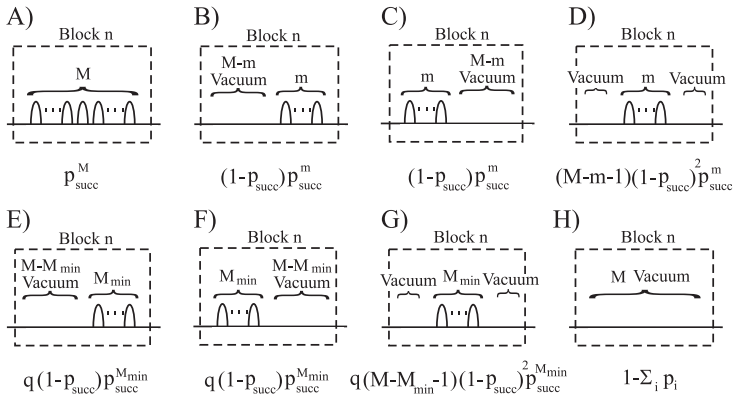

Fig. 3. Possible blocks of M signals that Eve sends to Bob together with their a priori probabilities. Case A: The block contains M coherent states. Case B: The first $m \in (M_{min}, M)$ signals of the block are coherent states, while the last $M-m$ signals are vacuum states. Case C: The block contains first $M-m$ vacuum states followed by $m \in (M_{min}, M)$ coherent states. Case D: The block has $m \in (M_{min}, M)$ coherent states and, at least, the first and the last signal of the block are vacuum states. Case E: The first M_{min} signals of the block are coherent states, while the last $M-M_{min}$ signals are vacuum states. Case F: The block contains first $M-M_{min}$ vacuum states together with M_{min} coherent states. Case G: The block has M_{min} coherent states and, at least, the first and the last signal of the block are vacuum states. Case H: The block contains only vacuum states. The a priori probability of this last scenario is given by $1-\sum_i p_i$, with p_i representing the a priori probabilities of each of the previous cases.

Similarly, $1-p$ represents the probability that the last signal in a block is a vacuum state. Fig. 4 illustrates these two alternatives for the case where Eve sends to Bob a block of signals containing M coherent states.

Let us now analyze the different scenarios included in Fig. 3 in more detail. When Eve sends to Bob a block of signals containing M coherent states (Case A in Fig. 3) then: If the last signal state of the previous block is a coherent state, then it turns out that the average total number of clicks obtained by Bob is given by Ms, where the parameter s has the form

$$s = 1 - \exp(-\mu_\beta), \tag{3}$$

with μ_β being again the mean photon-number of the coherent states $|\beta e^{i\theta_j}\rangle$ sent by Eve. Otherwise, the average total number of clicks at Bob's side can be written as $t + (M-1)s$, where the parameter t is given by

$$t = 1 - \exp\Big(-\frac{\mu_\beta}{2}\Big). \tag{4}$$

The analysis of the remaining cases is similar. If the first $m \in (M_{min}, M)$ signal states of the block are coherent states, while the last $M-m$ signals are vacuum states (Case B in Fig. 3) then: If the last state of the previous block is a coherent state, the average total number of clicks obtained by Bob is given by $t + ms$. Otherwise, the average total number of clicks at Bob's side can be written as $2t + (m-1)s$. Eve can as well send to Bob a block containing first $M-m$ vacuum states followed by $m \in (M_{min}, M)$ coherent states (Case C in Fig. 3).

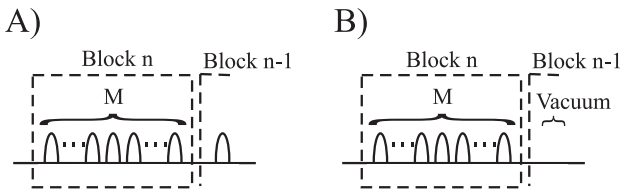

Fig. 4. Eve sends to Bob a block of signals containing M coherent states (Block n in the Figure). Case A: with probability p, where p is given by Eq. (2), the last signal state of the previous block is a coherent state. Case B: with probability $1-p$ the last signal state of the previous block is a vacuum state.

In this situation, if the last state of the previous block is a coherent state, the average total number of clicks obtained by Bob is given by $2t+(m-1)s$. Otherwise, the average total number of clicks has the form $t+(m-1)s$. When Eve sends to Bob a block of signals where, at least, the first and the last signals of the block are vacuum states (Case D in Fig. 3) then: If the last state of the previous block is a coherent state, the average total number of clicks obtained by Bob is given by $3t+(m-1)s$. Otherwise, the average total number of clicks has the form $2t+(m-1)s$. The cases E, F, and G, in Fig. 3 are completely analogous to the the cases B, C, and D, respectively. The only difference arises in the a priori probabilities to be in each of these scenarios. Now, these a priori probabilities need to be multiplied by the factor q introduced in Sec. 3, *i.e.*, by the probability that Eve actually decides to send M_{min} coherent states in the block. Finally, when the block contains only vacuum states (Case H in Fig. 3) then: If the last state of the previous block is a coherent state the average total number of clicks obtained by Bob is given by t. Otherwise, the average total number of clicks is zero.

After adding all these terms, together with their a priori probabilities, we obtain that the average total number of clicks per block of length M at Bob's side in a sequential attack can be expressed as

$$N^{M}_{clicks} = pt + p^{M}_{succ}u_M + \sum_{M_{min}\leq m<M} q^{\delta_{mM_{min}}}(1-p_{succ})p^{m}_{succ}\Big[v_m + (M-m-1)(1-p_{succ})w_m\Big], \tag{5}$$

where $\delta_{mM_{min}}$ is equal to one if $m = M_{min}$ and it is zero otherwise, and the parameters u_M, v_m, and w_m, are given by

$$\begin{aligned} u_M &= (1-2p)t + (M-1+p)s, \\ v_m &= (3-2p)t + (2m+p-2)s, \\ w_m &= 2t + (m-1)s. \end{aligned} \tag{6}$$

The gain G can be related with a transmission distance l for a given QKD scheme, *i.e.*, a distance that provides an expected click rate at Bob's side given by G. This last condition can be written as

$$G = 1 - \exp\left(-\mu_\alpha \eta_{det}\eta_t\right), \tag{7}$$

where μ_α is the mean photon-number of the signal states sent by Alice, *i.e.*, $\mu_\alpha = |\alpha|^2$, η_{det} represents the detection efficiency of the detectors employed by Bob, and η_t denotes the

transmission efficiency of the quantum channel. In the case of a DPS QKD scheme, the value of η_t can be derived from the loss coefficient γ of the optical fiber measured in dB/km, the transmission distance l measured in km, and the loss in Bob's interferometer L measured in dB as

$$\eta_t = 10^{-\frac{\gamma l + L}{10}}. \tag{8}$$

From Eq. (7) and Eq. (8), we find that the transmission distance l that provides a gain G is given by

$$l = -\frac{1}{\gamma}\left[L + 10\log_{10}\left(\frac{-\ln(1-G)}{\mu_\alpha \eta_{det}}\right)\right] \tag{9}$$

4. Sequential unambiguous state discrimination attack

As already mentioned in the previous section, in this attack Eve performs unambiguous state discrimination (USD) [47, 48, 49, 50, 51] of Alice's signal states. Whenever Eve identifies without error a signal state sent by Alice then she considers this result as successful. If the identification process does not succeed, then she considers it a failure. The probability of obtaining a successful result per signal state sent by Alice has the form [47, 48, 49, 50]

$$p_{succ} = 1 - |\langle \alpha | -\alpha \rangle| = 1 - \exp(-2\mu_\alpha). \tag{10}$$

Next, we obtain an expression for the quantum bit error rate (QBER) introduced by Eve with this attack, and also for the resulting double click rate at Bob's side.

4.1. *Quantum bit error rate*

The QBER is defined as N_{errors}/N_{clicks}, where N_{errors} represents the average total number of errors obtained by Bob, and N_{clicks} is again the average total number of clicks at Bob's side. The parameter N_{errors} can be expressed as $N_{errors} = (N/M)N^M_{errors}$, with N^M_{errors} denoting the average total number of errors per block of length M. With this notation, the QBER of a sequential attack, that we shall denote as Q, can then be expressed as

$$Q = \frac{1}{M}\frac{N^M_{errors}}{G}. \tag{11}$$

Next, we obtain an expression for N^M_{errors}. We shall distinguish the same cases as in the previous section, depending on the number m of coherent states $|\beta e^{i\theta_1}\rangle, |\beta e^{i\theta_2}\rangle, \ldots, |\beta e^{i\theta_m}\rangle$ inside a block and their position in the block.

Whenever the previous signal of a coherent state inside the block is a coherent state, then no errors occur since both signals have the proper relative phase between them. On the contrary, if the previous signal of a coherent state is a vacuum state or if the previous signal of a vacuum state is a coherent state then it turns out that an error can happen with probability $\exp(-\mu_\beta/4)[1-\exp(-\mu_\beta/4)] + [1-\exp(-\mu_\beta/4)]^2/2 = t/2$, where the parameter t is given by Eq. (4). The error term $[1-\exp(-\mu_\beta/4)]^2/2$ that appears in the previous expression arises from double clicks at Bob's side. Here, we consider that double click events are not discarded by Bob, but they contribute to the sifted key. Every time Bob obtains a double click, he just decides randomly the bit value [59].

Let us begin with Case A in Fig. 3. According to the previous paragraph, if the last signal state of the previous block is a coherent state, then the average total number of errors obtained by Bob is zero. Otherwise, it is given by $t/2$. When the first $m \in (M_{min}, M)$ signal states of the block are coherent states (Case B in Fig. 3) and the last state of the previous block is also a coherent state, then the average total number of errors obtained by Bob is given by $t/2$. Otherwise, the average total number of errors is t. Similarly, if Eve sends to Bob a block containing first $M-m$ vacuum states followed by $m \in (M_{min}, M)$ coherent states (Case C in Fig. 3) and the last signal of the previous block is a coherent state, then the average total number of errors is given by t. Otherwise, the average total number of errors has the form $t/2$. Eve can also send a block of signals where, at least, the first and the last signals of the block are vacuum states (Case D in Fig. 3). Then, if the last state of the previous block is a coherent state, the average total number of errors obtained by Bob is given by $3t/2$. Otherwise, the average total number of errors is t. Like in the previous section, the results for the cases E, F, and G, in Fig. 3 can be obtained directly from the cases B, C, and D, respectively. One only needs to multiply the a priori probabilities to be in each of these last three scenarios by the factor q. Finally, if the block contains only vacuum states (Case H in Fig. 3) and the last state of the previous block is a coherent state, then the average total number of errors is given by $t/2$. Otherwise, the average total number of errors is zero.

After adding all the terms together, and taking into account the a priori probabilities of each case, we obtain that the average total number of errors per block of length M in a sequential USD attack has the following form

$$N_{errors}^{M} = tS, \tag{12}$$

where the parameter S is given by

$$S = \frac{p}{2} + p_{succ}^{M}\left(\frac{1}{2} - p\right) + \sum_{M_{min} \leq m < M} q^{\delta_{mM_{min}}}(1-p_{succ})p_{succ}^{m}\left[\left(\frac{3}{2} - p\right) + (M-m-1)(1-p_{succ})\right]. \tag{13}$$

4.2. *Double click rate*

The double click rate at Bob's side, that we shall denote as D_c, is typically defined as $D_c = N_{D_c}/N$, where N_{D_c} refers to the average total number of double clicks obtained by Bob, and N is again the total number of signal states sent by Alice. N_{D_c} is given by $N_{D_c} = (N/M)N_{D_c}^{M}$, with $N_{D_c}^{M}$ denoting the average total number of double clicks per block sent by Eve at Bob's side. The D_c can be written as

$$D_c = \frac{1}{M} N_{D_c}^{M}. \tag{14}$$

In order to obtain an expression for $N_{D_c}^{M}$, we can again distinguish the same different cases included in Fig. 3. Double clicks can only occur when the previous signal of a coherent state is a vacuum state or when the previous signal of a vacuum state is a coherent state. The probability to obtain a double click in each of these two scenarios, that we shall denote as d, is given by

$$d = [1 - \exp(-\frac{\mu_\beta}{4})]^2. \tag{15}$$

Otherwise, the probability to have a double click is always zero. The analysis is then completely equivalent to the one included in Sec. 4.1, one only needs to substitute the parameter $t/2$ by d. We obtain, therefore, that the average total number of double clicks per block sent by Eve in a sequential USD attack can be written as

$$N_{D_c}^{M} = 2dS, \tag{16}$$

with S given by Eq. (13).

4.3. *Evaluation*

We have seen above that a sequential USD attack can be parameterized by the block size M, the minimum number M_{min} of consecutive successful results within a block that Eve needs to obtain in order to send Bob a new train of coherent states, the mean photon-number μ_β of these coherent states sent by Eve, and the value of the probability q, *i.e.*, the probability that Eve actually decides to send M_{min} coherent states in a block instead of only vacuum states.

Fig. 5 shows a graphical representation of the gain versus the QBER in this attack for different values of the maximum tolerable double click rate at Bob's side. It states that no key distillation protocol can provide a secret key from the correlations established by the users above the curves, *i.e.*, the secret key rate in that region is zero. In this example we consider

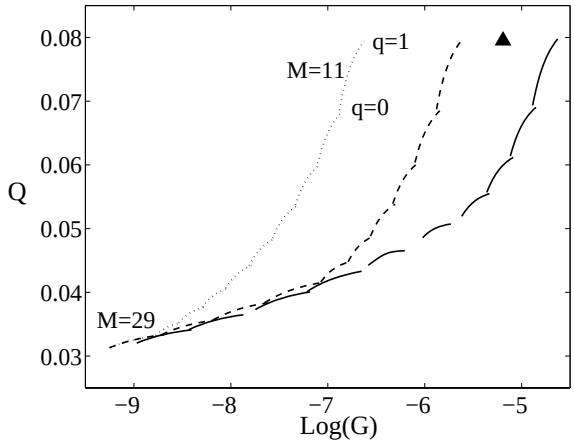

Fig. 5. Gain (G) versus QBER (Q) in a sequential USD attack for different values of the maximum tolerable double click rate at Bob's side: $D_c < 10^{-8}$ (solid), $D_c < 10^{-10}$ (dashed), and $D_c < 10^{-12}$ (dotted). The mean photon number of Alice's signal states is $\mu_\alpha = 0.16$. The triangle represents experimental data from Ref. [40].

that the mean photon number of Alice's signal states is given by $\mu_\alpha = 0.16$. Moreover, we fix the value of M_{min} as $M_{min} = \lfloor M/2 + 1 \rfloor$ and, for each given values of the parameters M, $q \in [0, 1]$, and the maximum tolerable double click rate obtained by Bob, we perform a numerical optimization to find the optimal mean photon number μ_β for each case, *i.e.*, the one that provides a lower QBER for a given value of the gain. Fig. 5 also includes experimental data from Ref. [40]. According to these results we find that, if Alice and Bob do not reject

a double click rate as low as 10^{-8}, the DPS QKD experiment reported in Ref. [40] would be insecure against a sequential USD attack. More precisely, our analysis suggest that in this kind of QKD protocols is not enough for Alice and Bob to include the effect of the double clicks obtained by Bob in the QBER [59], but it might be very useful for the legitimate users to monitor also the double click rate to guarantee security against a sequential attack. The authors of Ref. [40] already noticed in Ref. [41] that their experiment is not covered by the existing initial security analysis provided in Ref. [39]. Our result is strong as it also shows that when the double click rate at Bob's side is above 10^{-8} no improved classical communication protocol or improved security analysis might allow the data of Ref. [40] to be turned into secret key.

Fig. 6 shows a graphical representation for the case where Alice and Bob do not monitor separately the double click rate and Eve can optimize the mean photon number μ_β for each given values of M, $M_{min} = \lfloor M/2 + 1 \rfloor$, and the parameter q, without any restriction on the maximum tolerable double click rate at Bob's side.

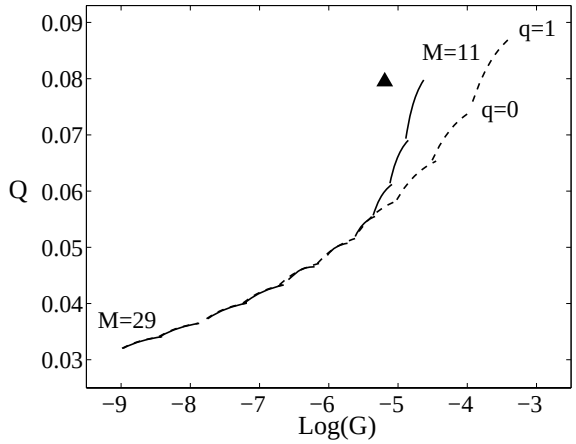

Fig. 6. Gain (G) versus QBER (Q) in a sequential USD attack. The solid line corresponds to a maximum tolerable double click rate at Bob's side of $D_c < 10^{-8}$. The dashed line represents the case where Alice and Bob do not monitor separately the double click rate obtained by Bob. The mean photon number of Alice's signal states is $\mu_\alpha = 0.16$. The triangle represents experimental data from Ref. [40].

A similar representation is plotted in Fig. 7, but now for the case $\mu_\alpha = 0.2$ and for different values of the maximum double click rate at Bob's side. In this figure we also include data from a recent experiment reported in Ref. [41], where the QBER was reduced to a value of only 3.4%. The scenario where Alice and Bob do not monitor separately the double click rate obtained by Bob is illustrated in Fig. 8. In both cases, our results are consistent with the possibility to create secret keys.

According to the figures presented in this section, whenever Eve tries to increase the gain of this attack by reducing, for instance, the size M of her blocks, she also increases the resulting QBER obtained by Bob. The maximum value of the gain that Eve can achieve, however, is actually limited by the probability $p_{succ} = 1 - \exp(-2\mu_\alpha)$ of obtaining a successful result when

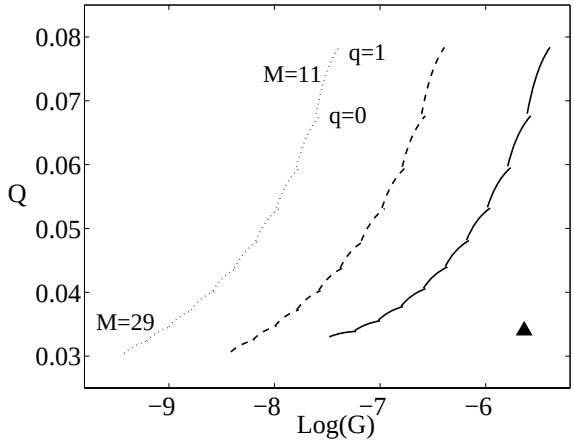

Fig. 7. Gain (G) versus QBER (Q) in a sequential USD attack for different values of the maximum tolerable double click rate at Bob's side: $D_c < 10^{-10}$ (solid), $D_c < 10^{-12}$ (dashed), and $D_c < 10^{-14}$ (dotted). The mean photon number of Alice's signal states is $\mu_\alpha = 0.2$. The triangle represents experimental data from Ref. [41].

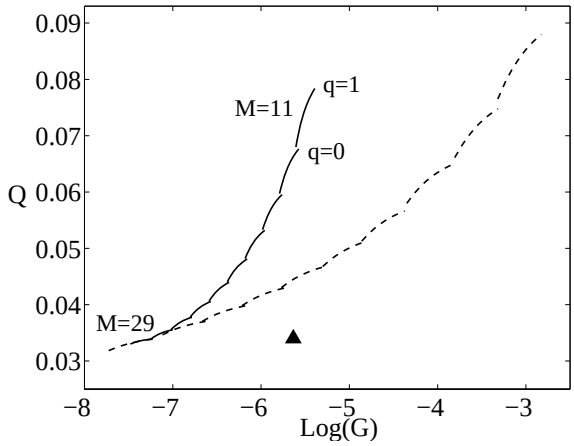

Fig. 8. Gain (G) versus QBER (Q) in a sequential USD attack. The solid line corresponds to a maximum tolerable double click rate at Bob's side of $D_c < 10^{-10}$. The dashed line represents the case where Alice and Bob do not monitor separately the double click rate obtained by Bob. The mean photon number of Alice's signal states is $\mu_\alpha = 0.2$. The triangle represents experimental data from Ref. [41].

distinguishing unambiguously the states $|\pm\alpha\rangle$. Since, by definition, $\lfloor M/2+1 \rfloor \leq M_{min} < M$, the minimum value of a valid block size M is given by $M = 3$. This means, in particular, that in order to maximize the gain of a sequential USD attack the best choice for Eve is to select $M = 3$ and $M_{min} = 2$. Moreover, we can assume that Eve always sends to Bob M_{min} coherent states $|\beta e^{i\theta_1}\rangle, |\beta e^{i\theta_2}\rangle, \ldots, |\beta e^{i\theta_{M_{min}}}\rangle$ when she obtains M_{min} successful results (*i.e.*, $q = 1$), and that these coherent states have a really high mean photon number such as she increases Bob's probability of obtaining a click (*i.e.*, $\mu_\beta \gg 1$ and, therefore, $s \approx 1$, $t \approx 1$, and $d \approx 1$). Using these values in Eq. (1) and Eq. (5) we obtain that the maximum value of the gain in this attack is given by

$$G_{max} \approx \frac{1}{3}(6 - 2p_{succ} - p_{succ}^2)p_{succ}^2. \tag{17}$$

In this case the QBER, and the double click rate at Bob's side are, respectively, given by $Q \approx (2 - p_{succ} - p_{succ}^2)/(6 - 2p_{succ} - p_{succ}^2)$ and $D_c \approx 2(2 - p_{succ} - p_{succ}^2)p_{succ}^2/3$.

On the contrary, the minimum value of the gain occurs when Eve treats the total number of signals N sent by Alice as a single block, *i.e.*, $M = N$, and she further imposes $M_{min} = M-1$, $q = 0$, and $s \approx 1$. In this case, the minimum gain is given by p_{succ}^N, and the QBER and double click rate at Bob's side are both zero. This scenario corresponds to the situation where Eve only sends N coherent states $|\beta e^{i\theta_1}\rangle, |\beta e^{i\theta_2}\rangle, \ldots, |\beta e^{i\theta_N}\rangle$ to Bob when she succeeds discriminating without error *all* the signal states sent by Alice.

As mentioned previously in e.g. Eq.(9), the gain G of a sequential attack is directly related with a transmission distance for a given QKD scheme. Therefore, the figures presented in this section could as well be straightforwardly rescaled according to Eq.(9) to represent the maximal distance achievable by the QKD protocol as a function of the QBER for given values of the parameters η_{det}, γ, and L. For instance, if we use the experimental data provided in Ref. [40] ($\eta_{det} = 0.009$, $\gamma = 0.2$ dB/km, and $L = 2.5$ dB) we find that the values $\log_{10}(G) = -5$ and $\log_{10}(G) = -9$ in Fig. 5 correspond to a transmission distance of $l \approx 95$ km and $l \approx 295$ km, respectively.

Finally, let us mention that, instead of using an USD measurement on each signal state sent by Alice, Eve could as well employ the same detection device like Bob. This sequential attack was very briefly introduced in Ref. [39]. In this case, a successful result is associated with obtaining a click in Eve's apparatus, while a failure corresponds to the absence of a click. The train of coherent states $|\beta e^{i\theta_1}\rangle, |\beta e^{i\theta_2}\rangle, \ldots, |\beta e^{i\theta_m}\rangle$ that Eve sends to Bob is now selected such as the relative phase between consecutive signals agree with Eve's measurement results. If we assume that Eve does not analyze each block of data independently, but she also includes a proper relative phase between blocks when the last signal of a previous block and the first signal of the following one are coherent states, then the results included in this section also apply to that case. Otherwise, the QBER in such kind of attack will be always higher than in a sequential USD attack. However, since Alice's signal states are typically coherent pulses with small average photon number (*i.e.*, $\mu_\alpha \ll 1$), Eve observes click events only occasionally. In particular, when she uses the same detection apparatus like Bob then the probability of obtaining a successful result will be always smaller than the one of a sequential USD attack. More precisely, this success probability has now the form $p_{succ} = 1 - \exp(-\mu_\alpha)$, and is smaller than the success probability given by Eq. (10). Fig. 9 shows a graphical representation of the gain versus the QBER for a sequential USD attack together with a sequential attack where

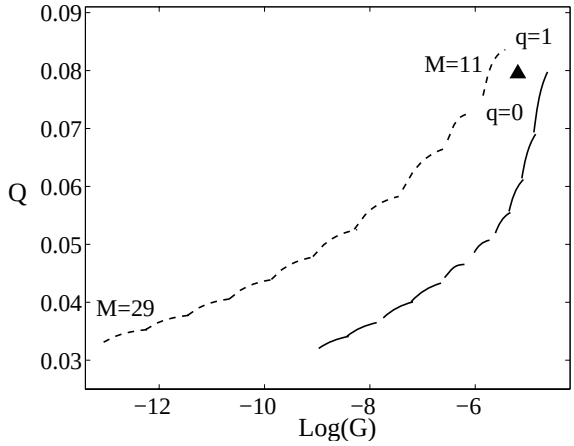

Fig. 9. Gain (G) versus QBER (Q) for a sequential USD attack (solid) and for a sequential attack where Eve employs the same detection device like Bob (dashed). The maximum tolerable double click rate at Bob's side is $D_c < 10^{-8}$ and the mean photon number of Alice's signal states is $\mu_\alpha = 0.16$. The triangle represents experimental data from Ref. [40].

Eve employs the same detection apparatus like Bob. In this example the maximum tolerable double click rate at Bob's side is given by $D_c < 10^{-8}$ and the mean photon number of Alice's signal states is $\mu_\alpha = 0.16$. Moreover, we fix again the value of M_{min} as $M_{min} = \lfloor M/2+1 \rfloor$ and, for each given values of the parameters M and $q \in [0,1]$, we perform a numerical optimization to find the optimal μ_β for each case like before. From the results included in Fig. 9 we see that a sequential USD attack can provide tighter upper bounds on the performance of DPS QKD schemes than a sequential attack with Eve employing the same detection device like Bob.

5. Sequential minimum error discrimination attack

In this eavesdropping strategy Eve performs first a filtering operation on each signal state sent by Alice with the intention to make them, with some finite probability, more "distinguishable". Afterwards, Eve measures out each successful filtered state with a measurement device that gives her the minimum value of the error probability when identifying the states [52, 53]. Her goal is to try to determine whether the filtered states originate from $|\alpha\rangle$ or from $|-\alpha\rangle$.

The coherent states sent by Alice can be expressed in some orthogonal basis $\{|0\rangle, |1\rangle\}$ as follows

$$|\pm\alpha\rangle = a|0\rangle \pm b|1\rangle, \tag{18}$$

where we assume, without of generality, that the coefficients a and b are given by

$$a = \sqrt{\frac{1}{2}\left[1+\exp\left(-2\mu_\alpha\right)\right]} \tag{19}$$

$$b = \sqrt{\frac{1}{2}\left[1-\exp\left(-2\mu_\alpha\right)\right]}, \tag{20}$$

(21)

that is, they satisfy, $a \in \Re$, $b \in \Re$, $a^2 + b^2 = 1$, and $a > b$ when $\mu_\alpha \neq 0$.

We shall consider that Eve uses a filtering operation defined by the following two Kraus operators [60]:

$$A_{succ}(\lambda) = \lambda|0\rangle\langle 0| + |1\rangle\langle 1|, \tag{22}$$

$$A_{fail}(\lambda) = \sqrt{1-\lambda^2}|0\rangle\langle 0|, \tag{23}$$

where the coefficient λ satisfies $\lambda \in [b/a, 1]$. This parameter allows Eve to increase the probability of obtaining a successful result and, therefore, she can increase the gain of her attack. On the other hand, Eve can introduce also more errors at Bob's side.

Suppose that the filtering operation receives as input the state $|\pm\alpha\rangle$. The probability of getting a successful result can be calculated as $p_{succ} \equiv p^{\lambda}_{succ} = \mathrm{Tr}[|\pm\alpha\rangle\langle\pm\alpha| A^{\dagger}_{succ}(\lambda) A_{succ}(\lambda)]$. This quantity is given by

$$p^{\lambda}_{succ} = a^2\lambda^2 + b^2. \tag{24}$$

If the filtering operation succeeded, the resulting normalized filtered state, that we shall denote as $|\pm\alpha_{succ}\rangle$, can be calculated as $|\pm\alpha_{succ}\rangle = (1/\sqrt{p^{\lambda}_{succ}})\ A_{succ}(\lambda)|\pm\alpha\rangle$. We obtain

$$|\pm\alpha_{succ}\rangle = \frac{1}{\sqrt{p^{\lambda}_{succ}}}(\lambda a|0\rangle \pm b|1\rangle). \tag{25}$$

As already mentioned previously, in order to decide which signal state was used by Alice, we consider that Eve follows the approach of MED. That is, she employs a measurement strategy that guesses the identity of the signals $|\pm\alpha_{succ}\rangle$ with the minimum probability of making an error. For the case of two pure states with equal a priori probabilities, like it is the case that we have here, the optimal value of the error probability, that we shall denote as p_{err}, is given by $p_{err} = [1 - \sqrt{1 - |\langle -\alpha_{succ}|\alpha_{succ}\rangle|^2}]/2$ [52]. From Eq. (25) we obtain, therefore,

$$p_{err} = \frac{1}{2}\frac{(a\lambda - b)^2}{a^2\lambda^2 + b^2}. \tag{26}$$

The von Neumann measurement which can be used to attain this error probability is given by the optimum detector states $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$.

Note that the sequential USD attack introduced in Sec. 4 can then be seen as a special case of this sequential MED attack. When $\lambda = b/a$, the success probability in a sequential MED attack is given by $p^{\lambda}_{succ} = 2b^2 = 1 - \exp(-2\mu_\alpha)$, which coincides with the success probability given by Eq. (10). Moreover, in this case the error probability p_{err} is zero.

Next, we obtain an expression for the QBER introduced by Eve with this attack, and also for the resulting double click rate at Bob's side.

5.1. *Quantum bit error rate*

From Eq. (11) we learn that in order to obtain an expression for the QBER in a sequential attack we only need to find the average total number of errors N^{M}_{errors} per block of length M.

Now, however, the analysis is slightly different from that considered in Sec. 4.1 since two consecutive coherent states in a block can also produce errors. This arises from the fact that sometimes Eve does not identify correctly the signal states $|\pm\alpha\rangle$ sent by Alice. In particular, whenever the previous signal of a coherent state inside a block is also a coherent state, then an error can occur with probability $[p_{err}(1-p_{err})+p_{err}(1-p_{err})]s$, where p_{err} is given by Eq. (26) and s is given by Eq. (3). This is the probability that only one of the two coherent states is wrongly identify by Eve and Bob detects the error by means of a click in his apparatus. We shall denote this error probability as $\tilde{p}_{err}$. Using Eq. (26), we can write $\tilde{p}_{err}$ as

$$\tilde{p}_{err} = \frac{1}{2}\left(\frac{a^2\lambda^2 - b^2}{a^2\lambda^2 + b^2}\right)^2 s. \tag{27}$$

If the previous signal of a coherent state is a vacuum state or if the previous signal of a vacuum state is a coherent state then the error probability is the same as in Sec. 4.1, *i.e.*, it has the form $t/2$ with t given by Eq. (4).

We can now address the different cases contained in Fig. 3 like in the previous sections and obtain an expression for N^M_{errors} as a function of these two error probabilities. The analysis is included in Appendix B. We find that N^M_{errors} can be written as

$$N^M_{errors} = \frac{pt}{2} + p^M_{succ}\tilde{u}_M + \sum_{M_{min}\leq m<M} q^{\delta_{m M_{min}}}(1-p_{succ})p^m_{succ}\Big[\tilde{v}_m + (M-m-1)(1-p_{succ})\tilde{w}_m\Big], \tag{28}$$

where the parameters $\tilde{u}_M$, $\tilde{v}_m$, and $\tilde{w}_m$, are given by

$$\begin{aligned} \tilde{u}_M &= \frac{(1-2p)t}{2} + (M-1+p)\tilde{p}_{err}, \\ \tilde{v}_m &= \frac{(3-2p)t}{2} + (2m+p-2)\tilde{p}_{err}, \\ \tilde{w}_m &= t + (m-1)\tilde{p}_{err}, \end{aligned} \tag{29}$$

and with p given by Eq. (2).

5.2. *Double click rate*

Like in the case of a sequential USD attack, also in this attack double clicks can happen only when the previous signal of a coherent state is a vacuum state or when the previous signal of a vacuum state is a coherent state. The probability to obtain a double click in each of these two scenarios does not depend on the value of the phase θ_j of the coherent state $|\beta e^{i\theta_j}\rangle$ involved, but it depends only on the mean photon-number μ_β. This means that the analysis included in Sec. 4.2 also applies here, and the average total number of double clicks per block sent by Eve in a sequential MED attack is also given by Eq. (16).

5.3. *Evaluation*

In Fig. 10 we plot the gain versus the QBER in a sequential MED attack for a fix value of the maximum tolerable double click rate at Bob's side ($D_c < 10^{-8}$) and for different values of the parameter λ. As before, it states that the secret key rate above the curves is zero. Like in Sec. 4.3, we fix the value of M_{min} as $M_{min} = \lfloor M/2 + 1 \rfloor$, and we perform a

numerical optimization to find the optimal mean photon number μ_β for each given values of the parameters M, q, and λ. Moreover, in this example, we consider that the mean photon number of Alice's signal states is given by $\mu_\alpha = 0.16$ and we also include the experimental data obtained in Ref. [40].

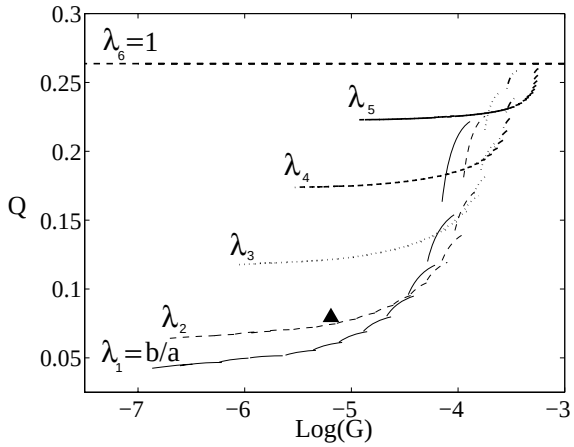

Fig. 10. Gain (G) versus QBER (Q) in a sequential MED attack for a fix value of the maximum tolerable double click rate at Bob's side ($D_c < 10^{-8}$), and for different values of the parameter λ: $\lambda_1 = b/a$ (solid), $\lambda_2 = b/a + (1 - b/a)/5$ (dashed), $\lambda_3 = b/a + 2(1 - b/a)/5$ (dotted), $\lambda_4 = b/a + 3(1 - b/a)/5$ (dashed-dotted), $\lambda_5 = b/a + 4(1 - b/a)/5$ (thick solid), and $\lambda_6 = 1$ (thick dashed). The mean photon number of Alice's signal states is $\mu_\alpha = 0.16$. The triangle represents experimental data from Ref. [40].

A similar graphical representation is included in Fig. 11, but now for the case where Alice and Bob do not monitor separately the double click rate and Eve can optimize the mean photon number μ_β for each given values of M, $M_{min} = \lfloor M/2 + 1 \rfloor$, q, and the parameter λ, without any restriction on the maximum tolerable double click rate at Bob's side.

While in a sequential USD attack the maximum value of the gain is given by Eq. (17), in a sequential MED attack Eve can always increase the value of the gain at the expense of also increasing the resulting QBER at Bob's side, just by incrementing the parameter λ. In particular, in the limit case of $\lambda = 1$, *i.e.*, the filtering operation is just the identity operation, we have that $p = 1$ and $p_{succ}^{\lambda=1} = 1$. In this situation, the gain, the QBER, and the double clock rate at Bob's side are, respectively, given by $G = 1 - \exp(-\mu_\beta)$, $Q = \exp(-4\mu_\alpha)/2$, and $D_c = 0$. That is, by selecting a proper mean photon number μ_β Eve can always access any high value of the gain.

6. Conclusion

In this paper we have quantitatively analyzed limitations on the performance of differential-phase-shift (DPS) quantum key distribution (QKD) protocols based on weak coherent pulses. For that, we have investigated simple eavesdropping strategies based on sequential attacks: Eve measures out every coherent state emitted by Alice and prepares new signal states, depending on the results obtained, that are given to Bob. Whenever Eve obtains a predeter-

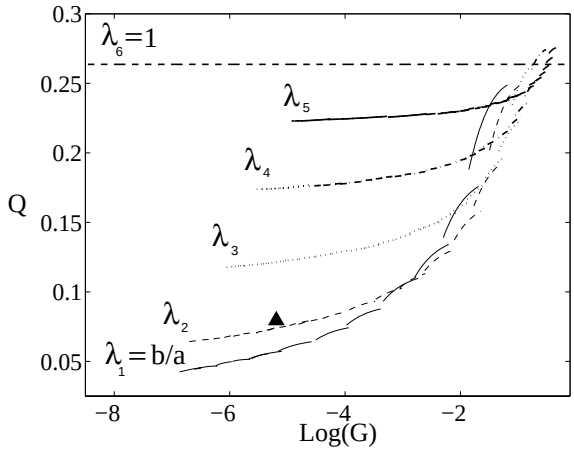

Fig. 11. Gain (G) versus QBER (Q) in a sequential MED attack for the case where Alice and Bob do not monitor separately the double click rate obtained by Bob, and for different values of the parameter λ: $\lambda_1 = b/a$ (solid), $\lambda_2 = b/a + (1 - b/a)/5$ (dashed), $\lambda_3 = b/a + 2(1 - b/a)/5$ (dotted), $\lambda_4 = b/a + 3(1 - b/a)/5$ (dashed-dotted), $\lambda_5 = b/a + 4(1 - b/a)/5$ (thick solid), and $\lambda_6 = 1$ (thick dashed). The mean photon number of Alice's signal states is $\mu_\alpha = 0.16$. The triangle represents experimental data from Ref. [40].

mined number of consecutive successful measurement outcomes, then she prepares a train of new coherent pulses that is forwarded to Bob. Otherwise, Eve sends vacuum signals to Bob to avoid errors. Sequential attacks transform the original quantum channel between Alice and Bob into an entanglement breaking channel and, therefore, they do not allow the distribution of quantum correlations needed to establish a secret key.

Specifically, we have considered two possible sequential attacks. In the first one, Eve realizes unambiguous state discrimination (USD) of Alice's signal states. When Eve identifies unambiguously a signal state sent by Alice, then she considers this result as successful. Otherwise, she considers it a failure. In the second attack, Eve performs first a filtering operation on each signal emitted by Alice and, afterwards, she measures out each successful filtered state following the approach of minimum error discrimination, *i.e.*, she guesses the identity of the filtered state with the minimum probability of making an error. As a result, we obtained upper bounds on the maximal distance achievable by differential-phase-shift quantum key distribution schemes as a function of the error rate in the sifted key, the double click rate at Bob's side, and the mean photon-number of the signals sent by Alice. It states that no key distillation protocol can provide a secret key from the correlations established by the users.

Instead of using an USD measurement on each signal state sent by Alice, like in the first eavesdropping strategy that we considered, Eve could as well employ the same detection device like Bob [39]. A successful result is now associated with obtaining a click in Eve's apparatus, while a failure corresponds to the absence of a click. However, since Alice's signal states are typically coherent pulses with small average photon number, the probability of obtaining a successful result in this scenario is always smaller than the one of a sequential USD attack. Therefore, a sequential USD attack can provide tighter upper bounds on the performance of

DPS QKD protocols than those derived from a sequential attack where Eve uses the same measurement apparatus like Bob.

While in the standard Bennett-Brassard 1984 (BB84) QKD protocol with phase randomized weak coherent state sources it generally suffices that the legitimate users monitor the error rate and gain of the scheme to guarantee unconditional security, our analysis suggest that, in DPS QKD, it might be very useful for the legitimate users to monitor also the double click rate or the correlations of detection probabilities between adjacent time-slots [b]. This fact might increase Alice and Bob's ability in defeating sequential attacks. Therefore, it might be advantageous for a security proof of DPS QKD to include also Alice and Bob's knowledge of double click rates and correlations of detection events. Such a security proof would be rather different from existing security proofs of the standard BB84 protocol which often involves random permutation and random sampling arguments and it is beyond the scope of this paper.

Acknowledgements

The authors thank Bing Qi for very fruitful discussions on the topic of this paper, and two anonymous referees for their helpful suggestions. Financial support from NSERC, CIPI, CRC program, CFI, OIT, CIAR, PREA, MITACS, DFG under the Emmy Noether programme, and the European Commission (Integrated Project SECOQC) are gratefully acknowledged. This research was supported by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported in part by the Government of Canada through NSERC and by the province of Ontario through MEDT. M.C. also acknowledges the financial support from a Post-doctoral grant from the Spanish Ministry of Science (MEC).

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden (2002), *Quantum cryptography*, Rev. Mod. Phys. **74**, pp. 145.
2. M. Dušek, N. Lütkenhaus, M. Hendrych, *Quantum cryptography*, to appear in Progress in Optics **49**, Edt. E. Wolf (Elsevier).
3. G. S. Vernam (1926), *Cipher printing telegraph systems*, Trans. of the AIEE **45**, pp. 295.
4. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: public key distribution and coin tossing*, Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE Press, New York), pp. 175.
5. D. Mayers (2001), *Unconditional security in quantum cryptography*, J. of ACM **48**, pp. 351.
6. H.-K. Lo and H. F. Chau (1999), *Unconditional security of quantum key distribution over arbitrarily long distances*, Science **283**, pp. 2050.
7. E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury (2000), *A proof of the security of quantum key distribution*, in Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computing, New York, USA (ACM Press, New York, 2000), pp. 715.
8. P. W. Shor and J. Preskill (2000), *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett. **85**, pp. 441.
9. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin (1992), *Experimental Quantum Cryptography*, J. Cryptology **5**, pp. 3.

[b] Technical difficulties might arise in the attempt to determine this additional information; for example, dead time of detectors might prevent Bob from observing sequential clicks on his detectors while affecting also the gain and QBER of the system.

10. C. Marand and P. D. Townsend (1995), *Quantum key distribution over distances as long as 30 km*, Opt. Lett. **20**, pp. 1695.
11. D. S. Bethune, M. Navarro and W. P. Risk (2002), *Enhanced autocompensating quantum cryptography system*, Applied Opt. LP **41**, pp. 1640.
12. R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson (2002), *Practical free-space quantum key distribution over 10 km in daylight and at night*, New J. Phys. **4**, pp. 43.
13. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden (2002), *Quantum key distribution over 67 km with a plug&play system*, New J. Phys., **4** pp. 41.
14. C. Gobby, Z. L. Yuan, and A. J. Shields (2004), *Quantum key distribution over 122 km of standard telecom fiber*, Appl. Phys. Lett. **84**, pp. 3762.
15. C. Gobby, Z. L. Yuan, and A. J. Shields (2004), *Unconditionally secure quantum key distribution over 50 km of standard telecom fibre*, Electron. Lett. **40**, pp. 1603.
16. B. Huttner, N. Imoto, N. Gisin and T. Mor (1995), *Quantum cryptography with coherent states*, Phys. Rev. A **51**, pp. 1863.
17. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders (2000), *Limitations on practical quantum cryptography*, Phys. Rev. Lett. **85**, pp. 1330.
18. H. Inamori, N. Lütkenhaus, and D. Mayers (2001),*Unconditional security of practical quantum key distribution*, quant-ph/0107017.
19. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill (2004), *Security of quantum key distribution with imperfect devices*, Quant. Inf. Comp. **4**, pp. 325.
20. W.-Y. Hwang (2003), *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, Phys. Rev. Lett. **91**, pp. 057901.
21. H.-K. Lo, X. Ma, K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett. **94**, pp. 230504.
22. X.-B. Wang (2005), *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography*, Phys. Rev. Lett. **94**, pp. 230503.
23. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo (2005), *Practical decoy state for quantum key distribution*, Phys. Rev. A. **72**, pp. 012326.
24. X.-B. Wang (2005), *Decoy-state protocol for quantum cryptography with four different intensities of coherent light*, Phys. Rev. A **72**, pp. 012322.
25. X.-B. Wang (2005), *Erratum: Decoy-state protocol for quantum cryptography with four different intensities of coherent light [Phys. Rev. A 72, 012322 (2005)]*, Phys. Rev. A **72**, pp. 049908.
26. J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt (2005), *Enhancing practical security of quantum key distribution with a few decoy states*, quant-ph/0503002.
27. X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo (2006), *Decoy-state quantum key distribution with two-way classical postprocessing*, Phys. Rev. A **74**, pp. 032330.
28. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian (2006), *Experimental Quantum Key Distribution with Decoy States*, Phys. Rev. Lett. **96**, pp. 070502.
29. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian (2006), *Simulation and Implementation of Decoy State Quantum Key Distribution over 60 km Telecom Fiber*, Proc. of IEEE International Symposium on Information Theory (ISIT'06), pp. 2094.
30. C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan (2007), *Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding*, Phys. Rev. Lett. **98**, pp. 010505.
31. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt (2007), *Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber*, Phys. Rev. Lett. **98**, pp. 010503.
32. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter (2007), *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km*, Phys. Rev. Lett. **98**, pp. 010504.

33. Z. L. Yuan, A. W. Sharpe, A. J. Shields (2007), *Unconditionally secure one-way quantum key distribution using decoy pulses*, Appl. Phys. Lett. **90**, pp. 011118.
34. C. H. Bennett (1992), *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. **68**, pp. 3121.
35. M. Koashi (2004), *Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse*, Phys. Rev. Lett. **93**, pp. 120501.
36. K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe (2006), *Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse*, quant-ph/0607082.
37. K. Inoue, E. Waks, and Y. Yamamoto (2002), *Differential Phase Shift Quantum Key Distribution*, Phys. Rev. Lett. **89**, pp. 037902.
38. K. Inoue, E. Waks, and Y. Yamamoto (2003), *Differential-phase-shift quantum key distribution using coherent light*, Phys. Rev. A **68**, pp. 022317.
39. E. Waks, H. Takesue, and Y. Yamamoto (2006), *Security of differential-phase-shift quantum key distribution against individual attacks*, Phys. Rev. A **73**, pp. 012344.
40. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto (2005), *Differential phase shift quantum key distribution experiment over 105 km fibre*, New J. Phys. **7**, pp. 232.
41. E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto (2006), *100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors*, Opt. Express **14**, pp. 13073.
42. M. Dušek, M. Jahma, and N. Lütkenhaus (2000), *Unambiguous state discrimination in quantum cryptography with weak coherent states*, Phys. Rev. A **62**, pp. 022306.
43. S. Félix, N. Gisin, A. Stefanov and H. Zbinden (2001), *Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses*, J. Mod. Opt. **48**, pp. 2009.
44. M. Curty, and N. Lütkenhaus (2005), *Intercept-resend attacks in the Bennett-Brassard 1984 quantum key distribution protocol with weak coherent pulses*, Phys. Rev. A **71**, pp. 062301.
45. M. Curty, M. Lewenstein, and N. Lütkenhaus (2004), *Entanglement as a precondition for secure quantum key distribution*, Phys. Rev. Lett. **92**, pp. 217903.
46. M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus (2005), *Detecting two-party correlations in quantum key distribution protocols*, Phys. Rev. A **71**, pp. 022306.
47. I. D. Ivanovic (1987), *How to differentiate between non-orthogonal states*, Phys. Lett. A **123**, pp. 257.
48. D. Dieks (1988), *Overlap and distinguishability of quantum states*, Phys. Lett. A **126**, pp. 303.
49. A. Peres (1988), *How to differentiate between non-orthogonal states*, Phys. Lett. A **128**, pp. 19.
50. G. Jaeger, and A. Shimony (1995), *Optimal distinction between two non-orthogonal quantum states*, Phys. Lett. A **197**, pp. 83.
51. A. Chefles, and S. M. Barnett (1998), *Optimum unambiguous discrimination between linearly independent symmetric states*, Phys. Lett. A **250**, pp. 223.
52. C. W. Helstrom (1976), *Quantum Detection and Estimation Theory*, (Academic Press, New York).
53. A. Chefles (2000), *Quantum state discrimination*, Contemporary Phys. **41**, pp. 401.
54. M. Horodecki, P. W. Shor, and M. B. Ruskai (2003), *Entanglement breaking channels*, Rev. Math. Phys. **15**, pp. 629.
55. M. B. Ruskai (2003), *Qubit entanglement breaking channels*, Rev. Math. Phys. **15**, pp. 643.
56. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden (2005), *Fast and simple one-way quantum key distribution*, Appl. Phys. Lett. **87**, pp. 194108.
57. N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani (2004), *Towards practical and fast Quantum Cryptography*, quant-ph/0411022.
58. C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani (2007), *Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography*, Quant. Inf. Comp.

7, pp. 639.
59. N. Lütkenhaus (1999), *Quantum key distribution: theory for application*, Applied Phys. B **69**, pp. 395.
60. K. Kraus (1983), in *States, Effects, and Operations*, No. 190 in Lecture Notes in Physics, A. Böhm, J. D. Dollard and W. Wootters eds., Springer, Berlin.

Appendix A: Probability p

In this Appendix we obtain an expression for the probability p that the last signal in a given block is a coherent state $|\beta e^{i\theta_j}\rangle$.

Let p_m be the probability of Eve sending to Bob m consecutive coherent states within a block of length M such that the last signal of the block is a coherent state. This probability is given by

$$p_m = \begin{cases} 0 & \text{if } m < M_{min} \\ q(1-p_{succ})p_{succ}^{M_{min}} & \text{if } m = M_{min} \\ (1-p_{succ})p_{succ}^{m} & \text{if } M_{min} < m < M \\ p_{succ}^{M} & \text{if } m = M. \end{cases} \tag{A.1}$$

For each given block of signals that Eve sends to Bob we have, therefore, that p can be written as

$$p = \sum_{m=M_{min}}^{M} p_m = \big[p_{succ} + (1-p_{succ})q\big] p_{succ}^{M_{min}}. \tag{A.2}$$

Similarly, $1-p$ represents the probability that the last signal in a block is a vacuum state.

Appendix B: N_{errors}^{M} in a sequential minimum error discrimination attack

In this Appendix we obtain an expression for the average total number of errors N_{errors}^{M} per block of length M sent by Eve in a sequential MED attack.

We shall distinguish the different cases included in Fig. 3, *i.e.*, as a function of the number m of coherent states inside a block and their position in the block.

Let us begin with Case A in Fig. 3. According to Sec. 5.1, whenever the last signal state of the previous block is a coherent state then the average total number of errors obtained by Bob is given by $M\tilde{p}_{err}$. Otherwise, it is given by $(M-1)\tilde{p}_{err} + t/2$. If the first $m \in (M_{min}, M)$ signal states of the block are coherent states (Case B in Fig. 3) and the last state of the previous block is also a coherent state, then the average total number of errors obtained by Bob is given $m\tilde{p}_{err} + t/2$. Otherwise, the average total number of errors is $(m-1)\tilde{p}_{err} + t$. Similarly, if Eve sends to Bob a block containing first $M-m$ vacuum states followed by $m \in (M_{min}, M)$ coherent states (Case C in Fig. 3) and the last signal of the previous block is a coherent state, then the average total number of errors is given by $(m-1)\tilde{p}_{err}+t$. Otherwise, the average total number of errors has the form $(m-1)\tilde{p}_{err} + t/2$. Eve can also send to Bob a block of signals where, at least, the first and the last signals of the block are vacuum states (Case D in Fig. 3). Then, if the last state of the previous block is a coherent state, the average total number of errors obtained by Bob is given by $(m-1)\tilde{p}_{err} + 3t/2$. Otherwise, the average total number of errors is $(m-1)\tilde{p}_{err} + t$.

The results for the cases E, F, and G, in Fig. 3 can be obtained directly from the cases B, C, and D, respectively. One only needs to multiply the a priori probabilities to be in each of these last three scenarios by the factor q.

Finally, whenever the block that Eve sends to Bob contains only vacuum states (Case H in Fig. 3) and the last signal of the previous block is a coherent state, then the average total number of errors is given by $t/2$. Otherwise, the average total number of clicks is zero.

After including all the a priori probabilities to be in each of the different cases discussed above, we obtain that the average total number of errors per block of length M in a sequential MED attack is given by Eq. (28).