Quantum Information and Computation, Vol. 9, No. 1&2 (2009) 0062–0080

UPPER BOUNDS ON THE PERFORMANCE OF DIFFERENTIAL-PHASE-SHIFT QUANTUM KEY DISTRIBUTION

HIPÓLITO GÓMEZ-SOUSA, MARCOS CURTY
ETSI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Campus Universitario, E-36310 Vigo, Spain

Received June 5, 2008
Revised August 11, 2008

In this paper, we investigate limitations imposed by sequential attacks on the performance of a differential-phase-shift (DPS) quantum key distribution (QKD) protocol with weak coherent pulses. Specifically, we analyze a sequential attack based on optimal unambiguous discrimination of the relative phases between consecutive signal states emitted by the source. We show that this attack can provide tighter upper bounds for the security of a DPS QKD scheme than those derived from sequential attacks where the eavesdropper aims to identify the state of each signal emitted by the source unambiguously.

Keywords: quantum cryptography, quantum key distribution, differential-phase-shift quantum key distribution, unambiguous state discrimination, sequential attack, intercept-resend attack, security
Communicated by: H-K Lo & R Laflamme

1 Introduction

The main security threat of quantum key distribution (QKD) protocols based on weak coherent pulses (WCP) arises from the fact that some signals contain more than one photon prepared in the same polarization state. In this situation, the eavesdropper (Eve) can perform, for instance, the so-called *Photon Number Splitting* (PNS) attack on the multi-photon pulses [1]. As a result, it turns out that the BB84 protocol [2] with WCP can give a key generation rate of order $O(\eta^2)$, where η denotes the transmission efficiency of the quantum channel [3, 4].

To obtain higher secure key rates over longer distances, different practical QKD schemes, that are robust against the PNS attack, have been proposed in recent years. One of these schemes is the so-called decoy-states [5], where the sender (Alice) randomly varies the mean photon number of the signal states that are forwarded to the receiver (Bob). This method can deliver a secure key rate of order $O(\eta)$. Another possibility is based on the transmission of two non-orthogonal coherent states together with a strong reference pulse [6]. This technique also provides a key generation rate of order $O(\eta)$ [7]. Finally, another potential approach is to use a differential-phase-shift (DPS) QKD protocol [8, 9]. In this scheme, 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 consecutive pulses. In this last case,

however, a secure key rate of order $O(\eta)$ has only been proven so far against a special type of individual attacks where Eve acts and measures *photons* individually, rather than *signals* [9], and also against a particular class of collective attacks where Eve attaches ancillary systems to each pulse or to each pair of successive pulses sent by Alice [10]. While a complete security proof of a DPS QKD protocol against the most general attack is still missing, recently it has been shown that sequential attacks [9] already impose strong restrictions on the performance of this QKD scheme with WCP. For instance, in [11, 12, 13] it was proven that the long-distance implementations of DPS QKD reported in [14, 15, 16, 17] would be insecure against a sequential attack based on unambiguous state discrimination (USD) of Alice's signal states [18, 19, 20].

In this paper, we analyze a novel sequential attack based on an improved version of the unambiguous relative phase discrimination measurement presented in [9]. Moreover, we show that the measurement strategy investigated is optimal, *i.e.*, it minimizes the probability of obtaining an inconclusive result when distinguishing all the relative phases of Alice's signal states. When combined with a sequential attack, this optimal unambiguous relative phase discrimination measurement can deliver ultimate upper bounds on the maximal distance achievable by a DPS QKD scheme as a function of the error rate in the sifted key, 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. We show that a sequential attack based on such a measurement always delivers tighter upper bounds for the security of a DPS QKD scheme than those derived from a sequential attack where Eve performs USD of each signal state emitted by Alice [11, 12, 13].

We consider the so-called *uncalibrated device scenario*, where Eve can always control some imperfections in Alice and Bob's devices (*e.g.*, the detection efficiency, the dark count probability, and the dead-time of Bob's detectors), together with the losses in the quantum channel, and she exploits them to obtain maximal information about the shared key [21].

The paper is organized as follows. In section 2 we describe in more detail a DPS QKD protocol. Then, in section 3, we present a sequential attack against this QKD scheme based on optimal unambiguous discrimination of the relative phases between Alice's signal states. Here we obtain upper bounds on the performance of a DPS QKD scheme as a function of the error rate in the sifted key and the mean photon number of Alice's signal states. Finally, section 4 concludes the paper with a summary. The manuscript contains as well one appendix with additional calculations.

2 Differential-phase-shift QKD

The basic setup is illustrated in figure 1. 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 $|-\alpha\rangle$ that are 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 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 consecutive pulses. Whenever the relative phase between two consecutive signals 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

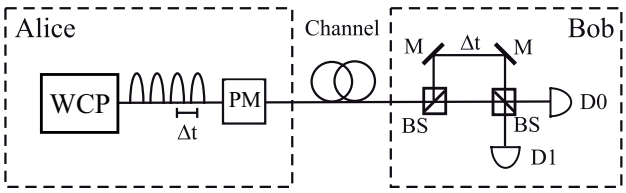

Fig. 1. Basic setup of a DPS QKD scheme. PM denotes a phase modulator, BS, a 50 : 50 beam splitter, M, a mirror, D0 and D1 are two photon detectors and Δt represents the time difference between two consecutive pulses.

time slot where he obtained a click and the actual detector that fired.

Once the quantum communication phase of the protocol is completed, Bob uses a classical authenticated channel to announce the time slots where he obtained a click, but he does not reveal which detector fired each time. From this information provided by Bob, together with the knowledge of the phase value used to modulate each pulse, Alice can infer which photon detector had clicked at Bob's side each given time. Then, Alice and Bob agree, for instance, to select a bit value "0" whenever the photon detector $D0$ fired, and a bit value "1" if the detector $D1$ clicked. 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 and Bob's devices, 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, [22].)

3 Sequential attacks against differential-phase-shift QKD

A sequential attack can be seen as a special type of intercept-resend attack [9, 11, 12, 13]. First, Eve measures out every signal 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 new train of non-vacuum signal states that is forwarded to Bob. Otherwise, Eve typically sends vacuum signals to Bob to avoid errors.[a] Whether a measurement result is considered to be successful or not, and which type of signal 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 [23] and, therefore, they do not allow the distribution of quantum correlations needed to establish a secret key [24].

The first sequential attack against a DPS QKD protocol was introduced very briefly in [9]. In this proposal, Eve employs a detection apparatus equivalent to Bob's setup. A successful result is associated with Eve obtaining a click in her measurement device. This click identifies unambiguously the relative phase (0 or $\pm\pi$) between two consecutive pulses emitted by Alice and, therefore, it reveals Eve the bit value encoded by the sender. A failure corresponds to

[a] In order to simplify our notation, from now on we will employ the term "signal 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 will be always denoted as a "vacuum state".

the absence of a click. However, since Alice emits WCP with typical average photon number quite low, so is the probability that Eve obtains a successful result in this scenario. In order to increase Eve's successful probability other sequential attacks have been proposed more recently [11, 12, 13]. These attacks are typically based on Eve realizing USD of each signal state emitted by Alice, since Eve can always access a local oscillator that is phase-locked to the coherent light source employed by the sender [13]. In particular, when Eve identifies unambiguously a signal state emitted by Alice, *i.e.*, she determines without error whether it is $|\alpha\rangle$ or $|-\alpha\rangle$, then she considers this result as successful. Otherwise, she considers it a failure. In [11] it was shown that this class of sequential attacks can provide tighter upper bounds on the performance of a DPS QKD protocol than those derived from a sequential attack where Eve uses the same measurement apparatus like Bob, or from the class of individual attacks considered in [9].

In this section, we introduce an improved version of the unambiguous relative phase discrimination measurement presented in [9], and we investigate again the situation where Eve tries to identify the relative phases between Alice's signal states unambiguously. As a result, we show that the sequential attack considered can provide stronger limitations for the security of a DPS QKD scheme than those reported in [9, 11, 12, 13].

3.1 Optimal unambiguous discrimination between relative phases

In a DPS QKD protocol Alice sends to Bob a train of WCP each of them prepared in the state $|\alpha\rangle$ or $|-\alpha\rangle$. These two coherent states span a two-dimensional Hilbert space $\mathcal{H}_2$ and, therefore, they can always be expressed in some orthogonal basis $\{|0\rangle, |1\rangle\}$ as follows

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

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

$$\begin{aligned} a &= \sqrt{\frac{1}{2}[1+\exp(-2\mu_\alpha)]}, \\ b &= \sqrt{\frac{1}{2}[1-\exp(-2\mu_\alpha)]}, \end{aligned} \tag{2}$$

with $\mu_\alpha = |\alpha|^2$ denoting the mean photon number of Alice's signal states. That is, a and b satisfy: $a \in \mathbb{R}$, $b \in \mathbb{R}$, $a^2 + b^2 = 1$, and $a > b$.

The state of a block of M consecutive WCP emitted by Alice, that we shall denote as $|\psi(\vec{x}_M)\rangle$, can be written as

$$|\psi(\vec{x}_M)\rangle = \bigotimes_{i=1}^{M} |(-1)^{x_i}\alpha\rangle = \sum_{n_1,\ldots,n_M=0}^{1} (-1)^{\sum_{i=1}^{M} x_i n_i} a^{M-\sum_{i=1}^{M} n_i} b^{\sum_{i=1}^{M} n_i} |n_1, ..., n_M\rangle, \tag{3}$$

with the coefficients a and b given by (2), and where the vector $\vec{x}_M = (x_1, ..., x_M)$, with $x_i \in \{0, 1\}$, contains the information about the value of the phase (0 or π) imprinted by Alice in each pulse within the block.

In order to access to the relative phase information encoded in a block of signals sent by Alice, however, it is not necessary to completely identify the vector $\vec{x}_M$. For instance, the relative phase between pulse N and pulse $N-1$ in $|\psi(\vec{x}_M)\rangle$, with $2 \leq N \leq M$, is simply given

by 0 ($\pm\pi$) when $x_N \oplus x_{N-1} = 0$ (1). In general, for any given state $|\psi(\vec{x}_M)\rangle$, there exists always another state $|\psi(\vec{x}_M \oplus \vec{1}_M)\rangle$, with $\vec{x}_M \oplus \vec{1}_M = (x_1 \oplus 1, ..., x_M \oplus 1)$, that has precisely the same $M-1$ relative phases as $|\psi(\vec{x}_M)\rangle$. This means, in particular, that the problem of determining the relative phases of Alice's signal states can be formulated as a discrimination problem between 2^{M-1} mixed states given by

$$\rho(\vec{x}_M) = \frac{1}{2}\Big(|\psi(\vec{x}_M)\rangle\langle\psi(\vec{x}_M)| + |\psi(\vec{x}_M \oplus \vec{1}_M)\rangle\langle\psi(\vec{x}_M \oplus \vec{1}_M)|\Big), \tag{4}$$

with the coefficient $x_M = 0$. That is, the vector $\vec{x}_M$ has now the form

$$\vec{x}_M = (x_1, ..., x_{M-1}, 0), \tag{5}$$

with $x_i \in \{0, 1\}$. This last condition arises because $\rho(\vec{x}_M)$ satisfies $\rho(x_1, ..., x_{M-1}, 0) = \rho(x_1 \oplus 1, ..., x_{M-1} \oplus 1, 1)$. The normalization term $\frac{1}{2}$ that appears in (4) is due to the fact that all the states $|\psi(\vec{x}_M)\rangle$ have equal a priori probabilities.

To distinguish between the signals states given by (4), we shall consider that Eve follows a USD strategy. That is, the constraint is that the measurement employed by Eve should never wrongly identify a state $\rho(\vec{x}_M)$, but it can provide sometimes an inconclusive result [18, 19, 20]. The goal is to keep the fraction of inconclusive outcomes as low as possible.

Let the set of binary vectors $V_{y,M}$, with $y \in \{A, B\}$, be defined as

$$V_{y,M} = \Big\{(n_1, ..., n_M) \mid n_i \in \{0, 1\}, \text{ and } \sum_{i=1}^{M} n_i \text{ even if } y = A, \text{ odd if } y = B\Big\}, \tag{6}$$

and let $\mathcal{Y}_{\mathcal{M}}$ denote the subspace spanned by the orthogonal states $\{|n_1, ..., n_M\rangle\}$, with the vectors $(n_1, ..., n_M) \in V_{y,M}$. The signal states $\rho(\vec{x}_M)$ given by (4) can be written in a block-diagonal form as

$$\rho(\vec{x}_M) = \sum_{y \in \{A,B\}} p_{y,M} |\psi_y(\vec{x}_M)\rangle\langle\psi_y(\vec{x}_M)|, \tag{7}$$

where the probabilities $p_{y,M}$ are given by

$$p_{y,M} = \sum_{\substack{n_1,...,n_M=0 \\ \vec{n}_M \in V_{y,M}}}^{1} \left(a^{M-\sum_{i=1}^{M} n_i} b^{\sum_{i=1}^{M} n_i}\right)^2, \tag{8}$$

with the vector $\vec{n}_M \equiv (n_1, ..., n_M)$, and where the states $|\psi_y(\vec{x}_M)\rangle$ have the form

$$|\psi_y(\vec{x}_M)\rangle = \frac{1}{\sqrt{p_{y,M}}} \sum_{\substack{n_1,...,n_M=0 \\ \vec{n}_M \in V_{y,M}}}^{1} (-1)^{\sum_{i=1}^{M-1} x_i n_i} a^{M-\sum_{i=1}^{M} n_i} b^{\sum_{i=1}^{M} n_i} |n_1, ..., n_M\rangle. \tag{9}$$

That is, the signals $|\psi_y(\vec{x}_M)\rangle \in \mathcal{Y}_{\mathcal{M}}$.

This means, in particular, that we can always assume, without loss of generality, that Eve's measurement strategy includes an initial step which projects the mixed states $\rho(\vec{x}_M)$ onto the orthogonal subspaces $\mathcal{A}_{\mathcal{M}}$ and $\mathcal{B}_{\mathcal{M}}$. This projective measurement is characterized by the following two operators: $\Pi_{y,M} = \sum_{n_1,...,n_M=0, \vec{n}_M \in V_{y,M}}^{1} |n_1, ..., n_M\rangle\langle n_1, ..., n_M|$ with

$y \in \{A, B\}$. It satisfies $[\mathrm{Tr}(\Pi_{y,M}\rho(\vec{x}_M))]^{-1}\Pi_{y,M}\rho(\vec{x}_M)\Pi_{y,M}^{\dagger} = |\psi_y(\vec{x}_M)\rangle\langle\psi_y(\vec{x}_M)|$. That is, it outputs the state $|\psi_y(\vec{x}_M)\rangle$ with probability $p_{y,M}$.

The question of discriminating the 2^{M-1} mixed states given by (4) can then be reduced to the problem of distinguishing 2^{M-1} pure states $|\psi_y(\vec{x}_M)\rangle$. To discriminate between the signals $|\psi_y(\vec{x}_M)\rangle$, we shall consider a measurement strategy which can involve at most $M-1$ steps. Before providing the exact details of the measurement, let us sketch very briefly its principal parts. Eve starts by performing a filter operation on $|\psi_y(\vec{x}_M)\rangle$. If the filter operation succeeds, Eve obtains $x_{M-1} \oplus x_M$. That is, Eve learns with certainty the relative phase between the first two pulses in the block. Moreover, this filter operation also outputs a quantum state which still contains complete information about the remaining $M-2$ relative phases within the block. On the contrary, if the filter operation fails, the value of x_{M-1} is not accessible anymore, and Eve cannot obtain the first two relative phases (*i.e.*, $x_{M-1} \oplus x_M$, and $x_{M-2} \oplus x_{M-1}$) within the block. In this last case, however, the filter operation outputs a state which contains information about the remaining $M-3$ relative phases within the block. Eve repeats the same procedure several times, but now applied to the quantum state provided by the filter operation in the previous step. To gain full information about *all* the relative phases contained in $|\psi_y(\vec{x}_M)\rangle$, Eve needs to obtain $M-1$ consecutive successful filtering results.

The main motivation to select such a particular implementation of a USD measurement is closely related to Eve's eavesdropping strategy, which will be introduced in section 3.2. The principal idea behind this method is that, with some finite probability, Eve can always determine the value of some relative phases in $|\psi_y(\vec{x}_M)\rangle$, even if she is not able to identify all of them. Moreover, as we show in Appendix A, it turns out that this measurement strategy is optimal, *i.e.*, it minimizes the probability of obtaining an inconclusive result when distinguishing all the $M-1$ relative phases of Alice's signal states. Next, we provide the technical details of Eve's measurement.

The set of $M-1$ possible filter operations employed by Eve is defined by the following two Kraus operators:

$$\begin{aligned} F_{succ,y,N} &= G_{y,N-1} \otimes |0\rangle\langle 0| + I_{N-1} \otimes |1\rangle\langle 1|, \\ F_{fail,y,N} &= (I_{N-1} - G_{y,N-1}^{\dagger} G_{y,N-1})^{1/2} \otimes |0\rangle\langle 0|, \end{aligned} \tag{10}$$

with $2 \leq N \leq M$, and where I_{N-1} denotes the identity operator in $\mathcal{H}_{2^{N-1}}$, and the operator $G_{y,N-1}$ is given by

$$G_{y,N-1} = \sum_{\substack{n_1,\ldots,n_{N-1}=0 \\ \vec{n}_{N-1} \in V_{y,N-1}}}^{1} \left(\frac{b}{a}\right)^{2(n_{N-1}\oplus 1)} |n_1, n_2, ..., n_{N-1} \oplus 1\rangle\langle n_1, n_2, ..., n_{N-1}|. \tag{11}$$

Let $|\phi_y(\vec{x}_N)\rangle$ denote a quantum state of the form

$$|\phi_y(\vec{x}_N)\rangle = \frac{1}{\sqrt{p_{y,N}}} \sum_{\substack{n_1,\ldots,n_N=0 \\ \vec{n}_N \in V_{y,N}}}^{1} (-1)^{\sum_{i=1}^{N-1}(x_i \oplus x_N)n_i} a^{N-\sum_{i=1}^{N} n_i} b^{\sum_{i=1}^{N} n_i} |n_1, ..., n_N\rangle, \tag{12}$$

with $1 \leq N \leq M$. That is, when $N = M$ these states satisfy $|\phi_y(\vec{x}_M)\rangle = |\psi_y(\vec{x}_M)\rangle$ for all $\vec{x}_M$ given by (5). Let $\vec{x}_{N-1}$ denote the vector that is formed by the first $N-1$ elements of $\vec{x}_M$.

For any N satisfying $2 \leq N \leq M$, the signal states given by (12) can be written as a function of $|\phi_y(\vec{x}_{N-1})\rangle$ and $|\phi_{\bar{y}}(\vec{x}_{N-1})\rangle$, with $\bar{y} = B$ when $y = A$ and $\bar{y} = A$ when $y = B$, as

$$|\phi_y(\vec{x}_N)\rangle = \frac{1}{\sqrt{p_{y,N}}}\Big(a\sqrt{p_{y,N-1}}|\phi_y(\vec{x}_{N-1})\rangle|0\rangle + (-1)^{x_{N-1}\oplus x_N} b\sqrt{p_{\bar{y},N-1}}|\phi_{\bar{y}}(\vec{x}_{N-1})\rangle|1\rangle\Big), \quad (13)$$

up to a global phase.

Suppose now that the filter operation defined by (10) receives as input the state $|\psi_y(\vec{x}_M)\rangle \equiv |\phi_y(\vec{x}_M)\rangle$. The probability of getting a successful result, that we shall represent as $p_{succ,y,M}$, can be calculated as $p_{succ,y,M} = \langle\phi_y(\vec{x}_M)|F^{\dagger}_{succ,y,M}F_{succ,y,M}|\phi_y(\vec{x}_M)\rangle$. This quantity is given by $p_{succ,y,M} = (p_{y,M})^{-1}2b^2 p_{\bar{y},M-1}$. If the filter operation succeeded, the resulting normalized filtered state, that we shall denote as $|\phi_{succ,y}(\vec{x}_M)\rangle$, can be calculated as $|\phi_{succ,y}(\vec{x}_M)\rangle = (\sqrt{p_{succ,y,M}})^{-1}F_{succ,y,M}|\phi_y(\vec{x}_M)\rangle$. We obtain $|\phi_{succ,y}(\vec{x}_M)\rangle = |\phi_{\bar{y}}(\vec{x}_{M-1})\rangle \otimes |\psi_M\rangle$, with the state $|\psi_M\rangle$ given by $|\psi_M\rangle = (\sqrt{2})^{-1}[|0\rangle + (-1)^{x_{M-1}\oplus x_M}|1\rangle]$, up to a global phase. That is, the relative phase between pulse M and pulse $M-1$ is now completely accessible to Eve. She only has to measure the state $|\psi_M\rangle$ in the orthogonal basis $|\pm\rangle = (\sqrt{2})^{-1}(|0\rangle \pm |1\rangle)$ to learn its value.

On the contrary, the probability of obtaining a failure, that we shall denote as $p_{fail,y,M}$, can be calculated as $p_{fail,y,M} = \langle\phi_y(\vec{x}_M)|F^{\dagger}_{fail,y,M}F_{fail,y,M}|\phi_y(\vec{x}_M)\rangle$. This quantity is given by $p_{fail,y,M} = (p_{y,M})^{-1}(1-2b^2)p_{y,M-2} = 1 - p_{succ,y,M}$. Whenever the filter operation failed, the resulting normalized filtered state, that we shall denote as $|\phi_{fail,y}(\vec{x}_M)\rangle$, can be calculated as $|\phi_{fail,y}(\vec{x}_M)\rangle = (\sqrt{p_{fail,y,M}})^{-1}F_{fail,y,M}|\phi_y(\vec{x}_M)\rangle$. We obtain $|\phi_{fail,y}(\vec{x}_M)\rangle = |\phi_y(\vec{x}_{M-2})\rangle \otimes |00\rangle$, up to a global phase. That is, if Eve fails when filtering the state $|\phi_y(\vec{x}_M)\rangle$, then the value of x_{M-1} is not accessible to her anymore, and Eve cannot obtain the relative phase information between pulse M and pulse $M-1$, and also between pulse $M-1$ and pulse $M-2$, within the block.

Once the first filter operation finished, Eve is left with a quantum state which contains the signal $|\phi_{\bar{y}}(\vec{x}_{M-1})\rangle$ if the filter succeeded, or the signal $|\phi_y(\vec{x}_{M-2})\rangle$ if it failed. Then, she can repeat the same procedure again, and filter these signal states to try to obtain $x_{M-2}\oplus x_{M-1}$ if the original state was $|\phi_{\bar{y}}(\vec{x}_{M-1})\rangle$, or $x_{M-3}\oplus x_{M-2}$ if it was $|\phi_y(\vec{x}_{M-2})\rangle$. In general, whenever a filter operation given by (10) receives as input the state $|\phi_y(\vec{x}_N)\rangle$, with $2 \leq N \leq M$, then the probability of getting a successful result is given by

$$p_{succ,y,N} = 2b^2\frac{p_{\bar{y},N-1}}{p_{y,N}}. \quad (14)$$

If the filter operation succeeded, the resulting normalized filtered state has the form

$$|\phi_{succ,y}(\vec{x}_N)\rangle = |\phi_{\bar{y}}(\vec{x}_{N-1})\rangle \otimes |\psi_N\rangle, \quad (15)$$

with the signal $|\psi_N\rangle$ given by

$$|\psi_N\rangle = \frac{1}{\sqrt{2}}\Big[|0\rangle + (-1)^{x_{N-1}\oplus x_N}|1\rangle\Big], \quad (16)$$

up to a global phase. On the contrary, the probability of obtaining a failure can be expressed as

$$p_{fail,y,N} = (1-2b^2)\frac{p_{y,N-2}}{p_{y,N}}, \quad (17)$$

with the probabilities $p_{A,0} \equiv 1$ and $p_{B,0} \equiv 0$. In this last case, the resulting normalized filtered state is given by

$$|\phi_{fail,y}(\vec{x}_N)\rangle = |\phi_y(\vec{x}_{N-2})\rangle \otimes |00\rangle, \tag{18}$$

up to a global phase.

Let us now calculate the probability that Eve learns the first $k \in [1, M-1]$ relative phases of $\rho(\vec{x}_M)$. As we have seen above, to obtain the relative phase between pulse N and pulse $N-1$ within a block of M signals sent by Alice, Eve has to successfully filter a state of the form $|\phi_y(\vec{x}_N)\rangle$. Let $p_{succ,N}$ denote the probability that Eve obtains the value of $x_{N-1} \oplus x_N$ conditioned on the fact that Eve has access to a signal $|\phi_y(\vec{x}_N)\rangle$, with $y \in \{A, B\}$. This probability can be written as

$$p_{succ,N} = \sum_{y \in \{A,B\}} p_N^y p_{succ,y,N}, \tag{19}$$

where p_N^y represents the probability that the state filtered by Eve when trying to obtain $x_{N-1} \oplus x_N$ belongs to the subspace $\mathcal{Y}_{\mathcal{N}}$. When $N = M$, we have that p_M^y is simply given by $p_M^y = p_{y,M}$, with $p_{y,M}$ of the form (8). This means, in particular, that $p_{succ,M} = 2b^2(p_{y,M-1} + p_{\bar{y},M-1}) = 2b^2$, since $p_{y,M-1} + p_{\bar{y},M-1} = 1$. If $N = M-1$, the probabilities p_{M-1}^y can be expressed as $p_{M-1}^y = (p_{succ,M})^{-1} p_M^{\bar{y}} p_{succ,\bar{y},M}$. Using (14), together with the fact that $p_{succ,M} = 2b^2$ and $p_M^{\bar{y}} = p_{\bar{y},M}$, we obtain $p_{M-1}^y = p_{y,M-1}$. That is, $p_{succ,M-1}$ is given by $p_{succ,M-1} = 2b^2(p_{y,M-2} + p_{\bar{y},M-2}) = 2b^2$. Similarly, when $2 \leq N \leq M-2$, the state $|\phi_y(\vec{x}_N)\rangle$ can only arise from a filter operation on a signal $|\phi_{\bar{y}}(\vec{x}_{N+1})\rangle$ that succeeded, or from a filter operation on a signal $|\phi_y(\vec{x}_{N+2})\rangle$ that failed. If it comes from a successful filter operation on $|\phi_{\bar{y}}(\vec{x}_{N+1})\rangle$, then p_N^y can be written as $p_N^y = (p_{succ,N+1})^{-1} p_{N+1}^{\bar{y}} p_{succ,\bar{y},N+1}$. Starting with the case $N = M-2$, we already showed that $p_{succ,M-1} = 2b^2$ and $p_{M-1}^{\bar{y}} = p_{\bar{y},M-1}$. This means, therefore, that $p_{M-2}^y = p_{y,M-2}$. If the state $|\phi_y(\vec{x}_N)\rangle$ arises from a filter operation on $|\phi_y(\vec{x}_{N+2})\rangle$ which failed, then p_N^y is given by $p_N^y = (p_{fail,N+2})^{-1} p_{N+2}^y p_{fail,y,N+2}$. Starting again with the case $N = M-2$, and using (17) together with the fact that $p_{fail,M} = 1 - p_{succ,M} = 1 - 2b^2$ and $p_M^y = p_{y,M}$, we have that $p_{M-2}^y = p_{y,M-2}$ also in this scenario. Finally, from (19) we obtain that $p_{succ,M-2}$ satisfies $p_{succ,M-2} = 2b^2$. Following a recursive argumentation, it is straightforward to show that

$$p_{succ,N} = 2b^2 = 1 - \exp(-2\mu_\alpha), \tag{20}$$

for all N satisfying $2 \leq N \leq M$, and where in the last equality we have used (2). This means, in particular, that the probability that Eve learns the first $k \in [1, M-1]$ relative phases of $\rho(\vec{x}_M)$ can now be expressed as

$$\prod_{i=0}^{k-1} p_{succ,M-i} = [1 - \exp(-2\mu_\alpha)]^k. \tag{21}$$

As already mentioned before, it can be proven that this measurement is optimal, *i.e.*, it minimizes the probability of having an inconclusive result when distinguishing all the relative phases of Alice's signal states. (See Appendix A.)

3.2 Eavesdropping strategy

For simplicity, we shall consider that Eve treats all the signal states sent by Alice as a single block of signals, and she tries to discriminate each relative phase within the block. Whenever she identifies unambiguously a predetermined number of consecutive relative phases sent by Alice, *i.e.*, she determines without error whether each relative phase is 0 or $\pm\pi$, she considers this sequence of measurement outcomes successful. Otherwise she considers it a failure. We define the integer parameter $M_{\min}$ as the minimum number of consecutive relative phases that Eve needs to correctly identify in order to consider the sequence of measurement outcomes successful. More precisely, if $k \geq 0$ denotes the total number of consecutive relative phases unambiguously identified by Eve before her filter operation fails, then, whenever $k > M_{\min}$, Eve prepares a new train of signal states that is forwarded to Bob. On the other hand, if $k < M_{\min}$ Eve sends to Bob $k+2$ vacuum states, where the last vacuum state corresponds to Eve's failure when using her filter operation. Finally, whenever $k = M_{\min}$ we shall consider that Eve employs a probabilistic strategy that combines the two previous ones. In particular, we assume that Eve sends to Bob a new train of signal states with probability q and, with probability $1-q$, she sends to Bob $M_{\min}+2$ vacuum states. That is, the parameter q allows Eve to smoothly fit her eavesdropping strategy to the observed data [11].

Moreover, for simplicity, we define the integer parameter $M_{\max} > M_{\min}$ as the maximum number of consecutive unambiguous discrimination successful results that Eve can obtain in order to send to Bob a train of signal states. That is, whenever Eve determines unambiguously $M_{\max}$ consecutive relative phases within a block of them then she discards the next two phases, sends to Bob a train of signal states, and begins again the measurement process of the remaining phases. The reason to discard two consecutive relative phases in this scenario is just to guarantee that between any two blocks of signal states sent by Eve there always exists, at least, one vacuum state. Specifically, suppose, for instance, that after $M_{\max}$ successful results, Eve's filter operation outputs, with probability p_N^y, a state $|\phi_y(\vec{x}_N)\rangle$ given by (12). For $N > 2$, the state $|\phi_y(\vec{x}_N)\rangle$ can be written as

$$|\phi_y(\vec{x}_N)\rangle = \frac{1}{\sqrt{p_{y,N}}}\Big\{\sqrt{p_{y,N-2}}|\phi_y(\vec{x}_{N-2})\rangle[a^2|00\rangle_C + (-1)^{x_{N-1}\oplus x_N} b^2|11\rangle_C] \\ + ab\sqrt{p_{\bar{y},N-2}}|\phi_{\bar{y}}(\vec{x}_{N-2})\rangle[(-1)^{x_{N-2}\oplus x_N}|01\rangle_C + (-1)^{x_{N-2}\oplus x_{N-1}}|10\rangle_C]\Big\}, \tag{22}$$

up to a global phase. If now Eve discards subsystem C, the resulting signal state can be expressed as $\sum_{y\in\{A,B\}} p_N^y \mathrm{Tr}_C(|\phi_y(\vec{x}_N)\rangle\langle\phi_y(\vec{x}_N)|)$. After some calculations, and using the fact that $p_N^y = p_{y,N}$ (see Section 3.1), we obtain that this state is of the form given by (7), with $M = N-2$. That is, the value of x_{N-1} is not accessible anymore, but Eve can start again her measurement strategy on $\rho(\vec{x}_{N-2})$.

Let us now introduce the type of signal states that Eve forwards to Bob when she obtains $M_{\min} \leq k \leq M_{\max}$ consecutive successful measurement outcomes. To guarantee that Eve's presence remains unnoticeable to the legitimate users, she needs to select these signal states such that they can reproduce the statistics expected by the legitimate users after their measurements. For this, we shall consider the standard version of a DPS QKD protocol, where Alice and Bob only monitor the raw bit rate (before the key distillation phase) together with the time instances in which Bob obtains a click. It was shown in [13] that the main limitation on the class of signal states that Eve can send to Bob in this scenario arises from the

dead-time of Bobs detectors. In particular, to be able to mimic the expected dead-time of the detectors, Eve has to select trains of signal states that can produce only one click on Bob's side within a dead-time period.[b] To achieve this goal, we shall assume that whenever Eve identifies k consecutive relative phases encoded by Alice then she chooses her signal states, that we denote as $|\psi_{\rm e}^k\rangle$, containing only one photon distributed among $k+1$ temporal modes. These modes correspond to $k+1$ consecutive pulses sent by Alice, *i.e.*, the time difference between any two consecutive temporal modes is set equal to the time difference Δt between two consecutive pulses. Specifically, we shall consider that the states $|\psi_{\rm e}^k\rangle$ are given by [12, 13]

$$|\psi_{\rm e}^k\rangle = \sum_{n=1}^{k+1} A_n^{(k)} \exp{(i\theta_n)} \hat{a}_n^\dagger |vac\rangle, \tag{23}$$

with the coefficients $A_n^{(k)} \in \mathbb{C}$ and where the normalization condition $\sum_{n=1}^{k+1} |A_n^{(k)}|^2 = 1$ is always satisfied. The angles θ_n are selected such that they reproduce the relative phases identified by Eve's measurement, *i.e.*, $\theta_n - \theta_{n-1}$, with $1 < n \leq k+1$, is equal to the relative phase between pulse n and pulse $n-1$ sent by Alice. The operator $\hat{a}_n^\dagger$ represents a creation operator for one photon in temporal mode n, and the state $|vac\rangle$ refers to the vacuum state. The superscript k labeling the coefficients $A_n^{(k)}$ emphasizes the fact that the value of these coefficients may depend on the number of temporal modes contained in $|\psi_{\rm e}^k\rangle$.

Eve also appends some vacuum states to each signal $|\psi_{\rm e}^k\rangle$. The main idea behind this procedure is to guarantee that whenever Bob obtains a click on his detection apparatus, then he cannot obtain any other click afterwards during a period of time at least equal to the dead-time of his detectors. The minimum number of vacuum states that Eve needs to send to Bob after each signal $|\psi_{\rm e}^k\rangle$ is given by $1+d$, with $d = \lceil t_{\rm d} f_{\rm c} \rceil$, and where $t_{\rm d}$ and $f_{\rm c}$ denote, respectively, the dead-time of Bob's detectors and the clock frequency of the system [13]. The minimum value of d arises from the case where Bob obtains a click in the last possible temporal mode. Whenever Eve forwards to Bob a state $|\psi_{\rm e}^k\rangle$ together with $1+d$ vacuum states then she also has to discard some extra relative phases of $|\phi_y(\vec{x}_N)\rangle$ according to the procedure explained above before she begins again with her measurement of the remaining relative phases within the block.

In section 3.1 we showed that, given $\rho(\vec{x}_M)$, the probability that Eve learns the first $k \in [1, M-1]$ relative phases of $\rho(\vec{x}_M)$ is given by p^k with

$$p = 1 - \exp{(-2\mu_\alpha)}. \tag{24}$$

This means, in particular, that the probability that Eve sends to Bob a train of signal states $|\psi_{\rm e}^k\rangle$, together with $1+d$ vacuum states, is given by

$$p_{\rm s}(k) = \begin{cases} qp^{M_{\rm min}}(1-p) & \text{if } k = M_{\rm min} \\ p^k(1-p) & \text{if } M_{\rm min} < k < M_{\rm max} \\ p^{M_{\rm max}} & \text{if } k = M_{\rm max} \\ 0 & \text{otherwise,} \end{cases} \tag{25}$$

[b] In order to simplify our analysis, we shall assume that both detectors $D0$ and $D1$ in figure 1 are indistinguishable. Moreover, we shall consider a conservative scenario where every time that one of these detectors clicks, then both detectors do not respond to any other incident photon during a period of time equal to the dead-time, *i.e.*, we shall assume that after a click both detectors suffer *simultaneously* from a dead time [13].

with p given by (24). Similarly, we shall denote with $p_{\rm v}(k)$ the probability that Eve sends to Bob $k+2$ vacuum states. This probability is given by

$$p_{\rm v}(k) = \begin{cases} p^k(1-p) & \text{if } 0 \leq k < M_{\rm min} \\ (1-q)p^{M_{\rm min}}(1-p) & \text{if } k = M_{\rm min} \\ 0 & \text{otherwise.} \end{cases} \tag{26}$$

We illustrate all these possible cases in figure 2, where we also include the different a priori probabilities to be in each of these scenarios.

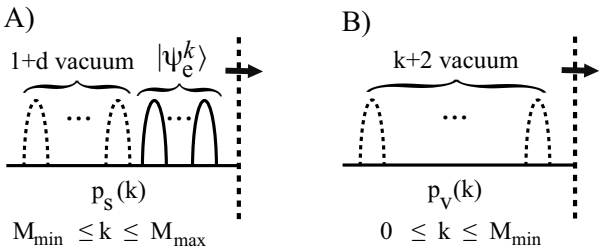

Fig. 2. Possible signal states that Eve sends to Bob together with their a priori probabilities. The arrow indicates the transmission direction.

Next, we obtain an expression for the gain, *i.e.*, the probability that Bob obtains a click per signal state sent by Alice, together with the quantum bit error rate (QBER) introduced by Eve with this sequential attack. The analysis is analogous to that included in [13], but now taking into account the a priori probabilities $p_{\rm s}(k)$ and $p_{\rm v}(k)$ given by (25) and (26), respectively.

3.3 Gain

The gain, that we shall denote as G, can be expressed as $G = N_{\rm clicks}/N_{\rm s}$, where $N_{\rm clicks}$ represents the average total number of clicks obtained by Bob, and $N_{\rm s}$ is the total number of signal states sent by Alice. The parameter $N_{\rm clicks}$ can be expressed as $N_{\rm clicks} = (N_{\rm s}/N^{\rm e})N^{\rm e}_{\rm clicks}$, with $N^{\rm e}$ denoting the average total number of pulses of the signal states sent by Eve (see figure 2), and where $N^{\rm e}_{\rm clicks}$ represents the average total number of clicks obtained by Bob when Eve sends to him precisely these signal states. With this notation, the gain of a sequential attack can be written as

$$G = \frac{N^{\rm e}_{\rm clicks}}{N^{\rm e}}. \tag{27}$$

Let us start by calculating $N^{\rm e}_{\rm clicks}$. Whenever Eve sends to Bob a signal state $|\psi_{\rm e}^k\rangle$ followed by $1+d$ vacuum states (Case A in figure 2) Bob always obtains one click in his detection apparatus. On the other hand, if Eve sends to Bob only vacuum states (Case B in figure 2) Bob never obtains a click. This means, in particular, that $N^{\rm e}_{\rm clicks}$ can be expressed as

$$N^{\rm e}_{\rm clicks} = \sum_{k=M_{\rm min}}^{M_{\rm max}} p_{\rm s}(k) = p^{M_{\rm min}}(p+q-pq). \tag{28}$$

The analysis to obtain $N^{\rm e}$ is similar. A signal state $|\psi_{\rm e}^k\rangle$ followed by $1+d$ vacuum states can be seen as containing $k+2+d$ pulses. On the other hand, the number of vacuum pulses

alone that Eve sends to Bob can vary from 2 to $M_{\min}+2$ (see figure 2). Adding all these terms together, and taking into account their a priori probabilities, we obtain that N^{e} can be written as

$$N^{\mathrm{e}} = \sum_{k=0}^{M_{\max}} p_{\mathrm{v}}(k)(k+2) + p_{\mathrm{s}}(k)(k+2+d) = \frac{2-p-p^{M_{\max}+1}}{1-p} + dN^{\mathrm{e}}_{\mathrm{clicks}}, \tag{29}$$

with $N^{\mathrm{e}}_{\mathrm{clicks}}$ given by (28).

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

$$G = 1 - \exp\left(-\mu_\alpha \eta_{\mathrm{det}} \eta_{\mathrm{t}}\right), \tag{30}$$

where η_{det} represents the detection efficiency of Bob's detectors, and η_{t} denotes the transmittivity 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

$$\eta_{\mathrm{t}} = 10^{-\frac{\gamma l + L}{10}}. \tag{31}$$

From (30) and (31), we find that the transmission distance l that provides a gain G is given by

$$l = -\frac{1}{\gamma}\left[L + 10\log_{10}\left(\frac{-\ln\left(1-G\right)}{\mu_\alpha \eta_{\mathrm{det}}}\right)\right]. \tag{32}$$

3.4 Quantum bit error rate

The QBER, that we shall denote as Q, is defined as $Q = N_{\mathrm{errors}}/N_{\mathrm{clicks}}$, 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 $N_{\mathrm{errors}} = (N_{\mathrm{s}}/N^{\mathrm{e}})N^{\mathrm{e}}_{\mathrm{errors}}$, with $N^{\mathrm{e}}_{\mathrm{errors}}$ denoting the average total number of errors obtained by Bob when Eve sends him the different signal states considered in her strategy (see figure 2). With this notation, and using again the fact that $N_{\mathrm{clicks}} = (N_{\mathrm{s}}/N^{\mathrm{e}})N^{\mathrm{e}}_{\mathrm{clicks}}$, we obtain that the QBER of a sequential attack can be expressed as

$$Q = \frac{N^{\mathrm{e}}_{\mathrm{errors}}}{N^{\mathrm{e}}_{\mathrm{clicks}}}. \tag{33}$$

The parameter $N^{\mathrm{e}}_{\mathrm{clicks}}$ was calculated in the previous section and it is given by (28). In order to obtain an expression for $N^{\mathrm{e}}_{\mathrm{errors}}$, one can distinguish the same cases like in the previous section, depending on the type of signal states that Eve sends to Bob. Whenever Eve sends to Bob a signal state $|\psi^k_{\mathrm{e}}\rangle$ followed by $1+d$ vacuum states (Case A in figure 2), the average total number of errors in this scenario, that we shall denote as $e(k)$, is given by

$$e(k) = \frac{1}{2}\left(1 - \sum_{n=1}^{k} |A^{(k)}_{n+1} A^{(k)}_{n}|\right). \tag{34}$$

On the other hand, if Eve sends to Bob only vacuum states (Case B in figure 2) Bob never obtains an error. This means, in particular, that $N^{\mathrm{e}}_{\mathrm{errors}}$ can be expressed as

$$N^{\mathrm{e}}_{\mathrm{errors}} = \sum_{k=M_{\min}}^{M_{\max}} p_{\mathrm{s}}(k) e(k). \tag{35}$$

3.5 Evaluation

The sequential attack introduced in section 3.2 can be parametrized by the minimum number $M_{\min}$ of consecutive unambiguous discrimination successful results that Eve needs to obtain in order to consider the sequence of measurement outcomes successful, the maximum number $M_{\max}$ of consecutive successful results that Eve can obtain in order to send to Bob a train of signal states, the value of the probability q, *i.e.*, the probability that Eve actually decides to send to Bob the signal state $|\psi_{\mathrm{e}}^{M_{\min}}\rangle$ followed by $1+d$ vacuum states instead of $M_{\min}+2$ vacuum states, and the state coefficients $A_n^{(k)} \in \mathbb{C}$ that characterize the signal states $|\psi_{\mathrm{e}}^{k}\rangle$, with $M_{\min} \leq k \leq M_{\max}$.

Figures 3, 4, 5 and 6 show a graphical representation of the gain versus the QBER in this sequential attack for different values of the mean photon number μ_α of Alice's signal states, and the parameter d. 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 these examples we consider the optimal distribution for the state coefficients $A_n^{(k)}$, *i.e.*, the one which provides the lowest QBER for a given value of the gain. This distribution was obtained in [13], where it was shown that the vector of optimal state coefficients $(A_1^{(k)}, ..., A_{k+1}^{(k)})$ coincides with the normalized eigenvector associated with the maximal eigenvalue of a $(k+1)\times(k+1)$ matrix with ones only on the first off-diagonals and zeros elsewhere. These figures assume that $M_{\max}$ is fixed and given by $M_{\max}=25$, and we vary the parameters $M_{\min} < M_{\max}$ and $q \in [0,1]$. These examples also include the case of a sequential attack where Eve realizes USD of each signal state sent by Alice [13], together with experimental data from [14, 15, 16, 17]. For instance, in the experiment reported in [17] the dead-time of Bob's detectors is $t_{\mathrm{d}} = 50$ ns and the clock frequency of the system is $f_{\mathrm{c}} = 10$ GHz. We obtain, therefore, that $d = \lceil t_{\mathrm{d}} f_{\mathrm{c}} \rceil = 500$. (See figure 3.) Similarly, in the experiments realized in [14, 15, 16] we have that $t_{\mathrm{d}} = 50$ ns and $f_{\mathrm{c}} = 1$ GHz. This means, in particular, that in all these cases $d = 50$. (See figures 4, 5 and 6.)

According to these results, we find that the sequential attack proposed in section 3.2 can provide tighter upper bounds for the security of a DPS QKD scheme than those derived from a sequential attack where Eve performs USD of each signal state emitted by the source. Basically, this result arises due to the different a priori probabilities of Eve sending to Bob a train of signal states $|\psi_{\mathrm{e}}^{k}\rangle$, together with $1+d$ vacuum states, in each of these two possible attacks. In particular, while in the attack introduced in section 3.2 these probabilities are given by $p_{\mathrm{s}}(k)$, in a sequential USD attack these probabilities have the form $p_{\mathrm{s}}(k)p$, with p given by (24). Note that in this last case Eve has to discriminate the state of $k+1$ consecutive signals sent by Alice unambiguously.

4 Conclusion

In this paper we have analyzed limitations imposed by sequential attacks on the performance of a differential-phase-shift (DPS) quantum key distribution (QKD) protocol based on weak

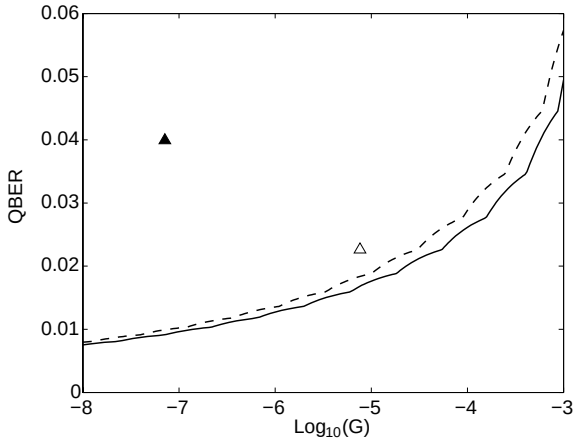

Fig. 3. Gain (G) versus QBER in the sequential attack introduced in section 3.2 for the optimal distribution of the state coefficients $A_n^{(k)}$ (solid line). The dashed line represents a sequential USD attack [13]. The mean photon number of Alice's signal states is $\mu_\alpha = 0.2$, and the parameter $d = 500$. The triangles represent experimental data from [17].

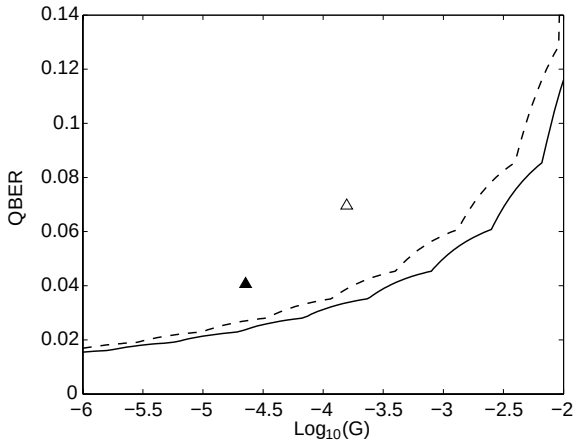

Fig. 4. Gain (G) versus QBER in the sequential attack introduced in section 3.2 for the optimal distribution of the state coefficients $A_n^{(k)}$ (solid line). The dashed line represents a sequential USD attack [13]. The mean photon number of Alice's signal states is $\mu_\alpha = 0.17$, and the parameter $d = 50$. The triangles represent experimental data from [14]. (See also [16].)

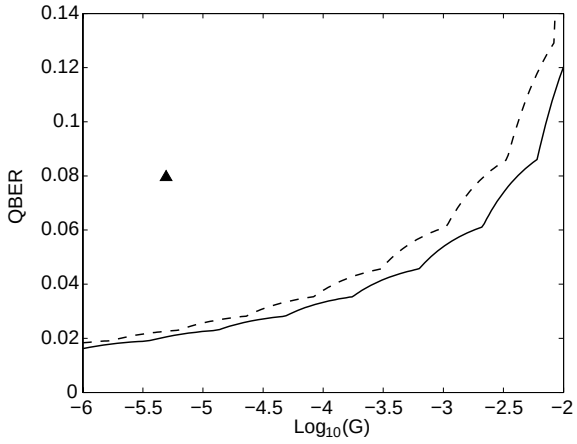

Fig. 5. Gain (G) versus QBER in the sequential attack introduced in section 3.2 for the optimal distribution of the state coefficients $A_n^{(k)}$ (solid line). The dashed line represents a sequential USD attack [13]. The mean photon number of Alice's signal states is $\mu_\alpha = 0.16$, and the parameter $d = 50$. The triangle represents experimental data from [14]. (See also [16].)

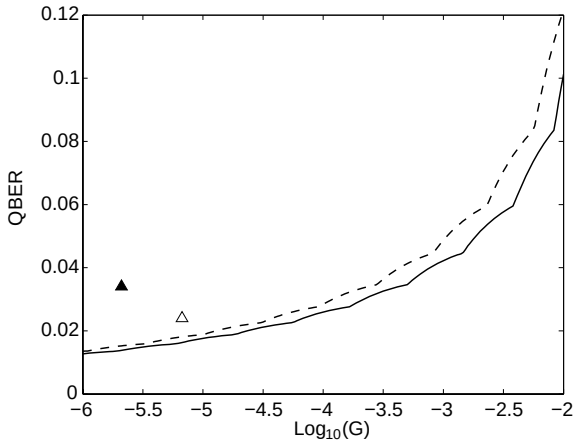

Fig. 6. Gain (G) versus QBER in the sequential attack introduced in section 3.2 for the optimal distribution of the state coefficients $A_n^{(k)}$ (solid line). The dashed line represents a sequential USD attack [13]. The mean photon number of Alice's signal states is $\mu_\alpha = 0.2$, and the parameter $d = 50$. The triangles represent experimental data from [15]. (See also [16].)

coherent pulses. A sequential attack consists of Eve measuring out every coherent state emitted by Alice and, afterwards, she 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 new train of non-vacuum signal states that is forwarded to Bob. Otherwise, Eve can send 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 investigated a sequential attack where Eve realizes optimal unambiguous discrimination of the relative phases between Alice's signal states. When Eve identifies unambiguously the relative phase between two consecutive signal states sent by Alice, then she considers this result as successful. Otherwise, she considers it a failure. As a result, we obtained ultimate upper bounds on the maximal distance achievable by a DPS QKD scheme as a function of the error rate in the sifted key, and the mean photon number of Alice's signals. It states that there exists no improved classical communication protocol or improved security analysis which can turn the correlations established by the users into a secret key. Moreover, our analysis indicates that this attack can provide tighter upper bounds for the security of a DPS QKD scheme than those derived from sequential attacks where Eve performs unambiguous state discrimination of each signal state emitted by the source.

Acknowledgements

The authors wish to thank Norbert Lütkenhaus and Tobias Moroder for very fruitful discussions on the topic of this paper and very useful comments on the manuscript. M.C. especially thanks Norbert Lütkenhaus for hospitality and support during his stay at the Institute for Quantum Computing (University of Waterloo) where this manuscript was finished. Financial support from Xunta de Galicia (Spain, Grant No. INCITE08PXIB322257PR) is gratefully acknowledged.

References

1. B. Huttner, N. Imoto, N. Gisin and T. Mor (1995), *Quantum cryptography with coherent states*, Phys. Rev. A **51**, pp. 1863.
2. 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.
3. H. Inamori, N. Lütkenhaus and D. Mayers (2007), *Unconditional security of practical quantum key distribution*, Eur. Phys. J. D **41**, pp. 599.
4. 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.
5. W.-Y. Hwang (2003), *Quantum key distribution with high loss: toward global secure communication*, Phys. Rev. Lett. **91**, pp. 057901; H.-K. Lo, X. Ma and K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett. **94**, pp. 230504; X.-B. Wang (2005), *Beating the Photon-Number-Splitting attack in practical quantum cryptography*, Phys. Rev. Lett. **94**, pp. 230503.
6. C. H. Bennett (1992), *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. **68**, pp. 3121.
7. M. Koashi (2004), *Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse*, Phys. Rev. Lett. **93**, pp. 120501; 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.

8. K. Inoue, E. Waks and Y. Yamamoto (2002), *Differential phase shift quantum key distribution*, Phys. Rev. Lett. **89**, pp. 037902; K. Inoue, E. Waks and Y. Yamamoto (2003), *Differential-phase-shift quantum key distribution using coherent light*, Phys. Rev. A **68**, pp. 022317.
9. 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.
10. C. Branciard, N. Gisin and V. Scarani (2008), *Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography*, New J. Phys. **10**, pp. 013031.
11. M. Curty, L. L. Zhang, H-K Lo and N. Lütkenhaus (2007), *Sequential attacks against differential-phase-shift quantum key distribution with coherent states*, Quant. Inf. Comp. **7**, pp. 665.
12. T. Tsurumaru (2007), *Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol*, Phys. Rev. A **75**, pp. 062319.
13. M. Curty, K. Tamaki and T. Moroder (2008), *Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks*, Phys. Rev. A **77**, pp. 052321.
14. 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.
15. 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.
16. E. Diamanti (2006), Ph.D Thesis, Stanford University.
17. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki and Y. Yamamoto (2007), *Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors*, Nature Photonics **1**, pp. 343.
18. I. D. Ivanovic (1987), *How to differentiate between non-orthogonal states*, Phys. Lett. A **123**, pp. 257; D. Dieks (1988), *Overlap and distinguishability of quantum states*, Phys. Lett. A **126**, pp. 303; A. Peres (1988), *How to differentiate between non-orthogonal states*, Phys. Lett. A **128**, pp. 19; G. Jaeger and A. Shimony (1995), *Optimal distinction between two non-orthogonal quantum states*, Phys. Lett. A **197**, pp. 83.
19. A. Chefles and S. M. Barnett (1998), *Optimum unambiguous discrimination between linearly independent symmetric states*, Phys. Lett. A **250**, pp. 223.
20. M. Dušek, M. Jahma and N. Lütkenhaus (2000), *Unambiguous state discrimination in quantum cryptography with weak coherent states*, Phys. Rev. A **62**, pp. 022306.
21. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev (2008), *A framework for practical quantum cryptography*, quant-ph/0802.4155.
22. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden (2002), *Quantum cryptography*, Rev. Mod. Phys. **74**, pp. 145; M. Dušek, N. Lütkenhaus and M. Hendrych (2006), *Quantum cryptography*, Prog. Opt. **49**, Edt. E. Wolf (Elsevier), pp. 381
23. M. Horodecki, P. W. Shor and M. B. Ruskai (2003), *Entanglement breaking channels*, Rev. Math. Phys. **15**, pp. 629; M. B. Ruskai (2003), *Qubit entanglement breaking channels*, Rev. Math. Phys. **15**, pp. 643.
24. M. Curty, M. Lewenstein and N. Lütkenhaus (2004), *Entanglement as a precondition for secure quantum key distribution*, Phys. Rev. Lett. **92**, pp. 217903; 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.
25. G. D. Forney (1991), *Geometrically uniform codes*, IEEE Trans. Inform. Theory **37**, pp. 1241; Y. C. Eldar and G. D. Forney (2001), *On quantum detection and the square-root measurement*, IEEE Trans. Inform. Theory **47**, pp. 858; Y. C. Eldar, A. Megretski and G. C. Verghese (2003), *Designing optimal quantum detectors via semidefinite programming*, IEEE Trans. Inform. Theory **49**, pp. 1007.

26. Y. C. Eldar (2003), *A semidefinite programming approach to optimal unambiguous discrimination of quantum states*, IEEE Trans. Inform. Theory **49**, pp. 446.

Appendix A: Optimality of Eve's measurement

In this appendix we show that the unambiguous discrimination measurement presented in section 3.1 is optimal, *i.e.*, it minimizes the probability of having an inconclusive result when distinguishing all the relative phases between Alice's signal states. For that, we calculate the maximal probability of unambiguously determining all the relative phases contained in the signal states $\rho(\vec{x}_M)$ given by (7), and we show that this probability coincides with that provided by the measurement introduced in section 3.1.

As already mentioned before, due to the special block structure of the signal states $\rho(\vec{x}_M)$, we can always assume, without loss of generality, that Eve first projects $\rho(\vec{x}_M)$ onto the orthogonal subspaces $\mathcal{A}_{\mathcal{M}}$ and $\mathcal{B}_{\mathcal{M}}$ and, afterwards, she measures the relative phase information contained in $|\psi_y(\vec{x}_M)\rangle$, with $y \in \{A, B\}$.

The set of states $|\psi_y(\vec{x}_M)\rangle \in \mathcal{Y}_{\mathcal{M}}$ constitutes a so-called geometrically uniform (GU) set [25, 26]. That is, these states are defined over a group of unitary matrices and they can be generated by a single generating vector. In particular, let $\mathcal{G}$ be the finite group of 2^{M-1} unitary matrices $U(\vec{x}_M)$ defined as

$$U(\vec{x}_M) = \sum_{n_1,...,n_M=0}^{1} (-1)^{\sum_{i=1}^{M-1} x_i n_i} |n_1, ..., n_M\rangle\langle n_1, ..., n_M|, \tag{A.1}$$

with $\vec{x}_M$ given by (5). If we denote as $\vec{0}_M = (0_1, ..., 0_M)$ the vector that has all its M elements equal to zero, then the states $|\psi_y(\vec{x}_M)\rangle$ can always be written as $|\psi_y(\vec{x}_M)\rangle = U(\vec{x}_M)|\psi_y(\vec{0}_M)\rangle$, with $|\psi_y(\vec{0}_M)\rangle$ being the generating vector of the set.

Let $\Phi_{y,M}$ denote the matrix whose columns are the state vectors $|\psi_y(\vec{x}_M)\rangle$, and let $\Phi^*_{y,M}$ represent its conjugate transpose. It was proven in [26] that the maximal probability of correctly distinguishing between GU pure states with equal a priori probabilities is given by the smallest eigenvalue of $\Phi_{y,M}\Phi^*_{y,M}$. The matrices $\Phi_{y,M}$, with $y \in \{A, B\}$ and $M \geq 3$, can be written, respectively, as

$$\Phi_{A,M} = \frac{1}{\sqrt{p_{A,M}}} \begin{pmatrix} a\sqrt{p_{A,M-1}}\Phi_{A,M-1} & a\sqrt{p_{A,M-1}}\Phi_{A,M-1} \\ b\sqrt{p_{B,M-1}}\Phi_{B,M-1} & -b\sqrt{p_{B,M-1}}\Phi_{B,M-1} \end{pmatrix}, \tag{A.2}$$

and

$$\Phi_{B,M} = \frac{1}{\sqrt{p_{B,M}}} \begin{pmatrix} a\sqrt{p_{B,M-1}}\Phi_{B,M-1} & -a\sqrt{p_{B,M-1}}\Phi_{B,M-1} \\ b\sqrt{p_{A,M-1}}\Phi_{A,M-1} & b\sqrt{p_{A,M-1}}\Phi_{A,M-1} \end{pmatrix}, \tag{A.3}$$

where $\Phi_{y,M-1}$ denotes the matrix whose columns are the state vectors $|\phi_y(\vec{x}_{M-1})\rangle$ given by (12). This means, in particular, that $\Phi_{y,M}\Phi^*_{y,M}$ can be expressed as a block-diagonal matrix as

$$\Phi_{y,M}\Phi^*_{y,M} = \frac{2}{p_{y,M}} \begin{pmatrix} a^2 p_{y,M-1}\Phi_{y,M-1}\Phi^*_{y,M-1} & \bar{0} \\ \bar{0} & b^2 p_{\bar{y},M-1}\Phi_{\bar{y},M-1}\Phi^*_{\bar{y},M-1} \end{pmatrix}, \tag{A.4}$$

with $\bar{0}$ denoting a zero matrix, *i.e.*, a matrix which contains only zeros. The smallest eigenvalue of $\Phi_{y,M}\Phi_{y,M}^{*}$, that we shall denote as $\lambda_{y,M}^{min}$, is given by

$$\lambda_{y,M}^{min} = \frac{2}{p_{y,M}} \min \left\{ a^2 p_{y,M-1} \lambda_{y,M-1}^{min}, b^2 p_{\bar{y},M-1} \lambda_{\bar{y},M-1}^{min} \right\}, \tag{A.5}$$

with $\lambda_{y,M-1}^{min}$ denoting the smallest eigenvalue of $\Phi_{y,M-1}\Phi_{y,M-1}^{*}$. We solve (A.5) by induction. In particular, we start by analyzing the case $M = 2$, and then we show that

$$a^2 p_{y,M-1} \lambda_{y,M-1}^{min} \geq b^2 p_{\bar{y},M-1} \lambda_{\bar{y},M-1}^{min}, \tag{A.6}$$

for all $M \geq 3$.

When $M = 2$, we have that $\Phi_{A,2}\Phi_{A,2}^{*} = 2(p_{A,2})^{-1}[a^4, 0; 0, b^4]$, and also $\Phi_{B,2}\Phi_{B,2}^{*} = 2a^2b^2(p_{B,2})^{-1}[1, 0; 0, 1]$. Then, since $a > b$, it is guaranteed that $a^4 = a^2 p_{A,1} > b^4 = b^2 p_{B,1}$, and $a^2 b^2 = a^2 p_{B,1} = b^2 p_{A,1}$, respectively. That is, if we define $\lambda_{y,1}^{min} = 1$ for all $y \in \{A, B\}$, then (A.6) is satisfied. When $M = 3$, it turns out that $a^2 p_{A,2} \lambda_{A,2}^{min} = b^2 p_{B,2} \lambda_{B,2}^{min} = 2a^2 b^4$, and $a^2 p_{B,2} \lambda_{B,2}^{min} = 2a^4 b^2 > b^2 p_{A,2} \lambda_{A,2}^{min} = 2b^6$. That is, (A.6) is also satisfied. Let us now assume that $a^2 p_{y,M-2} \lambda_{y,M-2}^{min} \geq b^2 p_{\bar{y},M-2} \lambda_{\bar{y},M-2}^{min}$ is true. Then, from (A.5) we have that $a^2 p_{y,M-1} \lambda_{y,M-1}^{min} = 2a^2 \min \{a^2 p_{y,M-2} \lambda_{y,M-2}^{min}, b^2 p_{\bar{y},M-2} \lambda_{\bar{y},M-2}^{min}\} = 2a^2 b^2 p_{\bar{y},M-2} \lambda_{\bar{y},M-2}^{min} \geq 2b^4 p_{y,M-2} \lambda_{y,M-2}^{min} = b^2 p_{\bar{y},M-1} \lambda_{\bar{y},M-1}^{min}$.

This means, therefore, that $\lambda_{y,M}^{min}$ is given by

$$\lambda_{y,M}^{min} = \frac{2}{p_{y,M}} \left(b^2 p_{\bar{y},M-1} \lambda_{\bar{y},M-1}^{min} \right) = p_{succ,y,M} \lambda_{\bar{y},M-1}^{min}, \tag{A.7}$$

where in the last equality we have used (14). When M is even, this expression can be written as

$$\lambda_{y,M}^{min} = \prod_{i=1}^{M/2} p_{succ,y,2i} \prod_{j=1}^{M/2-1} p_{succ,\bar{y},2j+1}, \tag{A.8}$$

while, whenever M is odd then (A.7) has the form

$$\lambda_{y,M}^{min} = \prod_{i=1}^{(M-1)/2} p_{succ,y,2i+1} p_{succ,\bar{y},2i}. \tag{A.9}$$

The maximal probability of unambiguously determining all the relative phases contained in the signal states $\rho(\vec{x}_M)$ is given by

$$\sum_{y \in \{A,B\}} p_{y,M} \lambda_{y,M}^{min}. \tag{A.10}$$

After some straightforward calculations, we obtain that this quantity can be written as $[1 - \exp(-2\mu_\alpha)]^{M-1}$, which coincides with that obtained in section 3.1.