Eur. Phys. J. D **40**, 453–464 (2006)
DOI: 10.1140/epjd/e2006-00167-2

THE EUROPEAN PHYSICAL JOURNAL D

Postponement of dark-count effects in practical quantum key-distribution by two-way post-processing

A. Khalique, G.M. Nikolopoulos[a], and G. Alber

Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Germany

Received 4 April 2006 / Received in final form 20 June 2006
Published online 14 July 2006 –

Abstract. The influence of imperfections on achievable secret-key generation rates of quantum key distribution protocols is investigated. As examples of relevant imperfections, we consider tagging of Alice's qubits and dark counts at Bob's detectors, while we focus on a powerful eavesdropping strategy which takes full advantage of tagged signals. It is demonstrated that error correction and privacy amplification based on a combination of a two-way classical communication protocol and asymmetric Calderbank-Shor-Steane codes may significantly postpone the disastrous influence of dark counts. As a result, the distances are increased considerably over which a secret key can be distributed in optical fibres reliably. Results are presented for the four-state, the six-state, and the decoy-state protocols.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication

QICS. 20. Quantum communication – 22.10.+k High key rates – 23.10.+l Limits for shared entanglement

1 Introduction

The unconditional security of the four-state [1] and the six-state [2] quantum-key-distribution (QKD) protocols has been addressed by many authors (see e.g., [3–6]). Although such security proofs allow for the most general eavesdropping attacks consistent with quantum theory (so-called coherent or joint attacks), they impose certain constraints on possible imperfections in the source and the detectors used in the protocol by the two legitimate users (Alice and Bob). One way to deal with such imperfections is to absorb their effect into the attack employed by a potential eavesdropper (Eve). In this spirit, most of the security proofs assume that any flaws due to imperfections in the source and/or the detectors do not depend on the bases used in the protocol i.e., they do not reveal any information about the basis-choice to Eve. Unfortunately, such security proofs are not directly applicable to practical implementations of the protocols as typical imperfections can be basis-dependent [7].

In particular, due to the lack of efficient single-photon sources, most of the current realizations of QKD protocols use as information carriers weak coherent pulses (WCPs), with a sufficiently low probability of containing more than one photon [9]. Multiphoton pulses, however, threaten the security of the QKD protocols as they can be exploited cleverly by Eve to gain perfect information about part of the exchanged random key without being detected [10,11]. To this end, she may launch the so-called photon-number-splitting (PNS) attack which, after the announcement of the bases used during preparation, enables her to obtain full information about the bit encoded in each of the multiphoton pulses [10,11]. In that respect, each multiphoton signal can be viewed as a tagged signal (qubit) which will yield its complete information to Eve without introducing detectable errors in the sifted key. Finally, even today's available single-photon detectors are not ideal [9]. At telecommunication wavelengths, for example, detection efficiencies are typically much smaller than unity while high dark-count rates severely limit the maximum distances over which a secret random key can be distributed by means of optical fibers [9–12].

In an effort to bring unconditional security proofs closer to practical QKD implementations, recent proofs relax the assumption about basis-independent eavesdropping [8,13]. In this context, Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) derived a general expression for the asymptotically achievable secret-key generation rate for the four-state protocol, under the assumption of weakly basis-dependent eavesdropping attacks [8]. Among many types of imperfections, the GLLP unconditional security proof takes into account possible tagging at Alice's source. From the technical point of view, the GLLP investigation concentrates on CSS-based post-processing i.e., error correction and privacy amplification protocols involving one-way classical communication only and whose achievable secret-key rates result from random encoding and decoding by asymmetric Calderbank-Shor-Steane (CSS) quantum codes [14]. In fact the security is first established in the framework of an associated protocol based on a CSS-like one-way entanglement purification protocol

[a] e-mail: nikolg@physik.tu-darmstadt.de

(see definition 4 of Ref. [15]), which is mathematically equivalent to CSS quantum codes [16]. Subsequently, the entanglement-based protocol is reduced to the standard four-state prepare-and-measure scheme without compromising security.

Motivated by these results, in this paper we investigate to which extent maximum achievable distances of secret-key distribution in the presence of imperfections, can be increased by additional use of an error-rejection procedure involving two-way classical communication. For this purpose we concentrate on the aforementioned types of experimentally relevant imperfections namely, tagging of qubits at Alice's source, dark counts, low efficiency of Bob's detectors and losses in the quantum channel connecting them. As a particular example of an error-rejection procedure we adopt the so-called B-steps of the recently proposed two-way post-processing protocol of Gottesman and Lo [15]. In our subsequent investigation we discuss the four-state, the six-state, and the decoy-state [17,18] QKD protocols. As a main result it will be demonstrated that with the help of a succession of B-steps followed by a CSS-based post-processing, the achievable distances of secret-key generation in optical fibers can be enhanced significantly.

This paper is organized as follows: in Section 2, we briefly recapitulate basic facts about practical QKD implementations and highlight the main (disastrous) effect of dark counts on the rates for secret-key generation. In Section 3 we discuss the quantum state of Alice and Bob after a powerful eavesdropping attack which takes into account tagged signals, losses and dark counts at Bob's detection unit. In Section 4 the influence of B-steps onto this quantum state and its resulting secret-key generation rate is investigated. For this latter purpose we focus on a post-processing protocol combining B-steps and asymmetric CSS codes. The degree to which such a post-processing can suppress the disastrous effect of dark counts on the rates for secret-key generation is investigated numerically.

2 Practical QKD implementations

In this section, for the sake of completeness, we briefly summarize basic facts about practical QKD, which are essential for the subsequent discussion. In particular, we establish a model for possible imperfections in practical implementations of the four- and the six-state QKD protocols, and discuss asymptotic secret-key generation rates.

2.1 Ideal QKD protocols

Let us start with a summary of the ideal prepare-and-measure four-state and six-state QKD protocols, which typically involve three stages. In the *distribution stage*, Alice encodes her random bit-string in a random sequence of non-orthogonal signal states (e.g., polarized single photons). Such a preparation involves two mutually unbiased bases (MUBs) in the four-state protocol and three in the fully symmetric six-state protocol. A first *raw key* is established when Bob measures each received signal at random in one of the possible bases and registers his outcomes. In the *sifting stage*, Alice and Bob reject all (ideally half for BB84 and 2/3 for the six-state protocol) bits originated from measurements in bases different from the preparation ones. Finally, Alice and Bob post-process this *sifted key* to distill a secret key. The *post-processing stage* typically involves error-correction and privacy amplification.

Following [8,15], throughout this work we adopt the *equivalent* entanglement-based versions of the prepare-and-measure schemes [19,20], based on a two-way CSS-like entanglement purification protocol (EPP). Let us start by recapitulating briefly the main steps involved in them. Alice prepares N qubit-pairs in the Bell state $|\Phi^+\rangle^{\otimes N}$ [21], where $|\Phi^+\rangle = (|0\rangle_{\rm A} \otimes |0\rangle_{\rm B} + |1\rangle_{\rm A} \otimes |1\rangle_{\rm B})/\sqrt{2}$ is a simultaneous eigenstate of the two Pauli operators $\mathcal{X}_{\rm A} \otimes \mathcal{X}_{\rm B}$ and $\mathcal{Z}_{\rm A} \otimes \mathcal{Z}_{\rm B}$, where $\mathcal{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$ and $\mathcal{X} = |0\rangle\langle 1| + |1\rangle\langle 0|$. She keeps half of each pair (denoted by A) and sends the other half (denoted by B) to Bob in one of the, say β, possible MUBs. In other words she applies a random rotation $\mathcal{R}_{\rm B}^b$, where the random variable $b \in \{0, \ldots, \beta\}$ [15]. From now on, we refer to the eigenstates of $\mathcal{Z}$, i.e. $\{|0\rangle, |1\rangle\}$, as the Z-basis (computational basis). As is well known, the two MUBs ($\beta = 2$) involved in the four-state protocol [1] are related via the Hadamard transformation $\mathcal{H} = \sum_{i,j}(-1)^{ij}\,|i\rangle\langle j|\,/\sqrt{2}$ where $i, j \in \{0, 1\}$ [15, 22], while the three MUBs ($\beta = 3$) of the six-state protocol [2] are related via successive actions of the unitary operator $\mathcal{T} = \sum_j \left[\,|j\rangle\langle 0| - {\rm i}(-1)^j\,|j\rangle\langle 1|\,\right]/\sqrt{2}$ [15,22]. Hence, in the former case $\mathcal{R}_{\rm B} = \mathcal{H}_{\rm B}$ whereas in the latter $\mathcal{R}_{\rm B} = \mathcal{T}_{\rm B}$.

After Bob has received all the transmitted qubits, Alice announces the sequence of rotations she performed and Bob undoes all of them. Subsequently Alice and Bob randomly permute their qubit-pairs so that their resulting N-pair quantum state becomes *permutation invariant*. They select a random subset of their pairs and they measure each one of them along the Z-basis, to estimate the qubit error probability δ of the residual qubit-pairs [22]. If δ exceeds a certain threshold, secret-key distillation cannot be guaranteed and the protocol is aborted. Otherwise, Alice and Bob perform a two-way CSS-like EPP to extract pure (high-fidelity) entangled pairs, which they measure along the Z-basis to obtain the final secret key. Most importantly, if the applied two-way CSS-like EPP (such as the one considered in the subsequent discussion) fulfills the requirements of theorem 6 in reference [15], the entanglement-based protocol can be reduced to a prepare-and-measure scheme without compromising the security. The results we are going to present therefore also apply to the corresponding prepare-and-measure schemes.

2.2 A model for imperfections and losses

Typical QKD implementations deviate from the ideal protocols mainly in two respects: the signal sources are not ideal and the link (channel and detectors) between the

two legitimate users is lossy and noisy. The model we adopt throughout this work for the description of such imperfections has been discussed thoroughly in the literature [9–12]. Here, for the sake of completeness, we briefly summarize its main ingredients.

We consider an imperfect source which with probability $p_{\rm tag}$ produces tagged qubits (signals), in the sense that Eve is capable of extracting from these qubits the information which random rotation (basis) has been used by Alice on them before their submission to Bob. Thus, Eve is able to measure each one of these qubits in such a way that she can unambiguously determine its quantum state without disturbing it i.e., without introducing any detectable errors. On the contrary, the remaining untagged (ideal) qubits which are produced by our source with probability $1-p_{\rm tag}$, do not reveal any information to Eve and any intervention of her (consistent with quantum mechanics) affecting them will eventually introduce errors. Hence, the overall bit-error rate estimated by Alice and Bob during the verification test [23] is basically due to untagged qubits only i.e., $\delta=(1-p_{\rm tag})\delta_{\rm b,u}$, where $\delta_{\rm b,u}$ is the probability with which an untagged qubit contributes to the overall bit-error rate. Given the symmetry between all the bases used in the QKD protocols under consideration, we expect for the corresponding phase-error probability $\delta_{\rm p,u}=\delta_{\rm b,u}$ i.e., $\delta_{\rm p,u}=\delta/(1-p_{\rm tag})$.

A practically relevant special case of tagging is the signal sources currently used in various realistic set-ups, which produce polarized phase-randomized WCPs [9–12]. In this case, the photon number distribution p_i $(i=0,1,...)$ of each pulse is Poissonian, i.e. $p_i=\exp(-\mu)\,\mu^i/i!$ with μ denoting the mean photon-number in the pulse. Alice, therefore, encodes each of her random bits in a polarized WCP which is sent to Bob. However, in addition to single-photon pulses such a source may produce multiphoton pulses and in that respect it deviates from the ideal single-photon source. More precisely, single-photons are produced with probability p_1 while multiphoton pulses with probability $p_{\rm tag}=1-p_0-p_1$. As will be explained in detail later on, Eve can obtain full information on all the bits encoded in multiphoton pulses by means of the so-called PNS attack. For a source producing WCPs therefore, multiphoton and single-photon pulses can be viewed as tagged and untagged qubits, respectively. Typically in WCP-based QKD implementations μ is chosen sufficiently small, so that the WCP source imitates an ideal single-photon source as close as possible [9]. The limitations of our model for the source will be discussed later on in Section 5.

In addition to imperfect signal sources, realistic set-ups involve imperfect quantum channels and detectors. As a result, the raw-key rate $P_{\rm exp}$ (i.e., the probability for a single detection event to occur at Bob's site), is in general distance-dependent and less than unity. More precisely, $P_{\rm exp}$ has contributions from both real signals arriving at Bob's detector and dark counts. In the adopted model, and for the aforementioned WCP source, we expect that actual signals trigger Bob's detector with probability $P_{\rm exp}^{\rm signal}=1-\exp(-\mu\eta_{\rm c}\eta_{\rm det})$, where $\eta_{\rm c}$ and $\eta_{\rm det}$ denote the transmission efficiency of the relevant quantum channel and the detection efficiency of Bob's detector, respectively. For QKD implementations at telecommunication wavelengths [9], $\eta_{\rm det}\sim 0.1$–0.2 and $\mu\ll 1$ while the quantum channels are optical fibers for which

$$\eta_{\rm c}=10^{-(\alpha l+L_{\rm c})/10}. \tag{1}$$

Thereby, α denotes a polarization independent loss coefficient of the fiber, l is the length of the fiber, and $L_{\rm c}$ characterizes a distance-independent loss of the channel. Moreover, the total dark-count probability for Bob's detection unit involving two identical detectors is $P_{\rm exp}^{\rm dark}\sim 10^{-4}$–$10^{-5}$. Hence, we typically have [9–12]

$$P_{\rm exp}\approx P_{\rm exp}^{\rm signal}+P_{\rm exp}^{\rm dark}=1-{\rm e}^{-\mu\eta_{\rm c}\eta_{\rm det}}+P_{\rm exp}^{\rm dark}. \tag{2}$$

Clearly, for an ideal link involving a lossless quantum channel and ideal detectors we have $P_{\rm exp}=1-{\rm e}^{-\mu}$.

The overall bit-error rate in the sifted key has also two contributions and is modeled by [9–12]

$$\delta=\delta_{\rm opt}+\delta_{\rm det}=\frac{\delta_0\;P_{\rm exp}^{\rm signal}+\frac{1}{2}P_{\rm exp}^{\rm dark}}{P_{\rm exp}}. \tag{3}$$

The first contribution is independent of the transmission distance and is a measure of the optical quality of the whole set-up. In particular, the constant δ_0 accounts for possible alignment errors, polarization diffusion or fringe visibility. The second contribution $\delta_{\rm det}$, originates from dark counts at Bob's detectors, with the factor $1/2$ indicating that a dark count represents one of the two possible random measurement results of Bob. Hence, an error will be generated in half of the cases only. In the most pessimistic scenario usually adopted in security proofs, all the error rate δ is attributed to Eve.

Finally, any imperfections, losses, and noise significantly affect the fraction of tagged qubits arriving at Bob's site. In general, the new (effective) tagging probability Δ, can be expressed in terms of the parameters characterizing the channel, the source and the detectors. An upper bound on Δ, for example, may be obtained by the following consideration, in the case of a photon source emitting phase-averaged WCPs [10,11]. An eavesdropper, Eve, with unlimited power may not only obtain perfect information about all the classical bits originating from multiphoton pulses but she may also increase the fraction of these multiphoton pulses as much as possible without affecting Bob's expected click-rate probability. For this purpose she can replace the lossy quantum channel by a perfect one (i.e., $\eta_{\rm c}=1$) so that all multiphoton pulses are transmitted perfectly. In order to keep $P_{\rm exp}$ constant she has to block an appropriate number of single-photon pulses. Thus, the maximum probability of tagged pulses arriving at Bob's detector, which Eve can have perfect knowledge about, is given by [10,11]

$$\Delta\approx\frac{1-(1+\mu)\exp(-\mu)}{P_{\rm exp}}, \tag{4}$$

while the corresponding probability for single-photon pulses is given by $(1-\Delta)$, so that they sum up to unity.

2.3 Asymptotic secret-key generation rates

As shown by GLLP in reference [8], losses and weak basis-dependent imperfections such as tagging do not render any of the QKD protocols under consideration insecure, but they affect the rates for secret-key generation. More precisely, for one-way CSS-based post-processing it has been shown that a secret key can be generated by Alice and Bob with the asymptotic rate

$$R_{\mathrm{CSS}} = \frac{P_{\mathrm{exp}}}{\beta}\left[1 - \Delta - H(\delta) - (1-\Delta)\, H\left(\delta_{\mathrm{p,u}}\right)\right], \quad (5)$$

where $H(x) := -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy.

Let us briefly analyze the quantities entering this expression. First of all, in the most pessimistic scenario, all the errors detected by Alice and Bob during the verification test are due to Eve's intervention. Furthermore, assuming that Eve has maximized the contribution of the tagged qubits in the sifted key by replacing the lossy channel with a perfect one, the estimated bit-error rate appearing in (5) is now given by $\delta = (1-\Delta)\delta_{\mathrm{b,u}}$, while the phase-error probability for an untagged qubit reads

$$\delta_{\mathrm{p,u}} = \delta/(1-\Delta), \quad (6)$$

accordingly. The raw-key rate is given by (2), while the factor $1/\beta$ accounts for the fraction of the raw bits passing the sifting procedure in a typical prepare-and-measure scheme. Clearly, for the four-state (two-basis) QKD protocol we have $\beta = 2$, whereas for the six-state (three-basis) protocol $\beta = 3$. Moreover, it has to be noted that for post-processing procedures taking into account possible correlations between bit-flip and phase error, the rate (5) can be improved [5]. However, throughout this work we adopt for both protocols the worst-case scenario which corresponds to having no such correlations thus implying zero mutual information between bit-flip and phase errors.

Typical behavior of the secret-key generation rate as a function of the distance (i.e., the length of the optical fiber l) is depicted in Figure 1. Using equations (1–4) and (6), we plot the rate R_{CSS} (as determined by Eq. (5)) for the four- and the six-state QKD protocols. A sudden drop of the key generation rate at about 25 km is clearly apparent in both protocols. A comparison with the corresponding secret-key generation rate of the four-state QKD protocol in the absence of dark counts (dotted curve) exhibits that this drop originates from dark counts. Indeed, in the case of a lossy quantum channel, the contribution to δ due to signals decreases with increasing l, so that eventually almost all the contributions to the error rate δ originate from dark counts. At the critical distance of 25 km the contribution of dark counts becomes dominant and almost all the key is lost by error correction and privacy amplification [9,10,12]. The critical distance turns out to be the same for the two protocols as a result of equation (5) which was used for both of them. However, as discussed in [5], the secret-key rate for the six-state protocol can be improved by means of a post-processing procedure which takes into account correlations between bit-flip and phase errors.

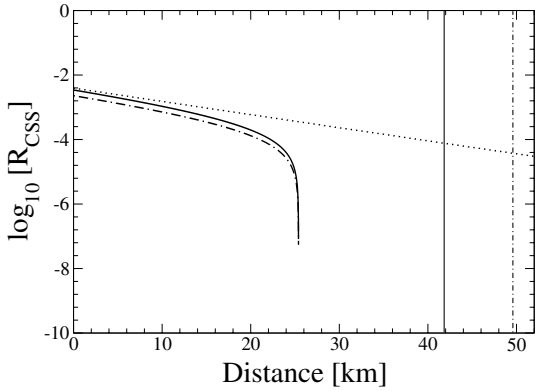

Fig. 1. Achievable secret-key rates as given by equation (5), for non-ideal implementations of the four-state (full curve) and the six-state (dot-dashed curve) QKD protocols: error correction and privacy amplification are performed by means of asymmetric CSS codes which involve one-way classical communication only. The vertical lines indicate the maximum allowed distances for secret-key generation as determined by equation (7) for the four-state (solid line at ∼42 km) and the six-state protocol (dot-dashed line at ∼50 km). Also shown is the secret-key rate of the four-state protocol in the absence of dark counts (dotted curve). All relevant parameters are chosen as in the experiment of reference [25] i.e., $\alpha = 0.2$ dB/km, $L_{\mathrm{c}} = 1$ dB, $\delta_0 = 1\%$, $P_{\mathrm{exp}}^{\mathrm{dark}} = 2\times 10^{-4}$, $\eta_{\mathrm{det}} = 0.18$. At each distance the mean number of photons μ is optimized such that the corresponding rate is maximal.

An upper bound on achievable distances can be obtained from the maximally tolerable error rates for single-photon pulses [9,10]. More precisely, given that Eve has full information on the error-free part of the key stemming from multiphoton pulses, Alice and Bob can extract a secret key only if they can prove the presence of quantum correlations (provable entanglement) in the remaining part of the sifted key originating entirely from single-photon pulses [26,27]. However, this is possible only if the corresponding (rescaled) error rate $\delta/(1-\Delta)$ does not exceed 1/4 for the four-state and 1/3 for the six-state QKD protocol i.e.,

$$\frac{\delta}{(1-\Delta)} < \frac{\beta-1}{2\beta}, \quad \text{for} \quad \beta \in \{2,3\}. \quad (7)$$

This is a generalization of the necessary conditions for secret-key generation in the context of the four- and the six-state protocols respectively, in the absence of tagging [22,26,27]. Indeed, an intercept-resend eavesdropping attack can always break entanglement between Alice and Bob giving rise to an error rate $\delta \geq (1-\Delta)(\beta-1)/2\beta$.

The necessary condition (7) limits the distances up to which a secret key can be distilled since both Δ and δ depend on the length of the optical fiber connecting Alice and Bob. This bound is indicated in Figure 1 by the solid vertical line for the four-state and by the dot-dashed vertical line for the six-state protocol. In Section 4 we will demonstrate how the gap between these borders and

the drop of the secret-key generation rates due to dark counts can be decreased considerably by applying a two-way error-rejection procedure before switching to one-way CSS-based post-processing. Before that, we have to derive the quantum state shared between Alice and Bob at the end of the distribution stage.

3 Formulation of QKD with tagged qubits

In order to derive the quantum state of Alice and Bob immediately before the post-processing stage under a realistic scenario, we have to take into account the influence of a tagging source and possible imperfections in the link (quantum channel and detectors). Most importantly, we also have to consider in detail Eve's strategy which can, in principle, take full advantage of all imperfections and losses. Following [8,15], we adopt the entanglement-based version of the four- and the six-state QKD protocols described in Section 2.1.

3.1 An optimal eavesdropping strategy

Consider the tagging scenario described at the end of Section 2.2, in which tagged qubits arrive at Bob's site with probability Δ. Let also N be the total number of qubit-pairs shared between Alice and Bob at the end of the distribution stage. For sufficiently large values of N, we expect that $N_{\rm u} \approx (1-\Delta)N$ pairs involve untagged qubits and $N_{\rm t} \approx \Delta N$ pairs involve tagged qubits (to be referred to hereafter as the tagged qubit-pairs). In general, the form of the reduced state of all N pairs, $\rho_{\rm tot}^{(N)}$, depends on the eavesdropping attack employeed by Eve.

As we discussed earlier, a tagged qubit reveals to Eve its basis of preparation i.e., which random rotation has Alice applied on it before its submission to Bob. Thus, Eve is able to measure each tagged qubit in such a way that she can unambiguously determine its quantum state without disturbing it i.e., without introducing any errors. On the contrary, the remaining untagged qubits are ideal for Alice and Bob, in the sense that they do not reveal any information to Eve. In particular, given that each untagged qubit is randomly prepared in non-orthogonal states, information gain for Eve is only possible at the expense of disturbing its state, thus introducing errors in the sifted key [20]. It has to be noted here that in the model under consideration, the source simply tags any ΔN of the signals in an uncorrelated and independent way. In other words, we do not allow for coherent superpositions of tagging procedures or other highly correlated basis-dependent imperfections [8]. Moreover, we assume that apart from the tagging scenario we have just described, the source behaves in a perfect way while the tagged signals do not convey any information about the untagged ones. In this framework, we restrict ourselves to a particular class of powerful eavesdropping strategies where Eve treats tagged and untagged qubits separately. Indeed, tagging allows Eve to attack a fraction of the qubits without introducing errors. Any other eavesdropping strategy which is consistent with quantum mechanics and does not take into account the tagging may only result in higher error rates in the sifted key. Finally, given that Eve can have full information on all the bits encoded in tagged qubits, she may launch the most powerful attack i.e., a coherent attack, on the remaining untagged qubits to extract as much information as possible about the final key.

Therefore, as long as Eve attacks the sets of tagged and untagged qubits separately, these sets are not entangled between each other. From now on, the reduced state of all tagged qubit-pairs is denoted by $\rho_{\rm t}^{(N_{\rm t})}$ whereas the corresponding state of all untagged qubit-pairs is denoted by $\rho_{\rm u}^{(N_{\rm u})}$. Our task is to estimate the precise form of these states and to this end we have to consider a particular tagging scenario.

3.1.1 Attack on tagged qubits

We will focus on the practically relevant special case of tagging discussed in Section 2.2 that is, a source which produces phase-randomized WCPs. For each multiphoton pulse sent by Alice to Bob, first of all Eve can measure the photon number. She can do this by means of a quantum non-demolition measurement without introducing any disturbance. In a second step, Eve can extract from each of these multiphoton pulses one photon, as described in the appendix of reference [10], which is stored in a quantum memory while the remaining signal is sent to Bob. After the announcement of the bases used during preparation, Eve measures each of her photons in the correct basis and obtains full information about the corresponding encoded bit.

Clearly, by such a PNS attack Eve can eventually determine all the key bits which originate from multiphoton pulses without introducing any bit-flip errors. Moreover, she may adjust her attack so that her intervention remains undetected, even if Alice and Bob proceed to monitor the complete photon-number distribution [28]. Hence, the PNS attack turns out to be Eve's optimal attack on the multiphoton pulses [10].

Now we turn to estimate the reduced state of Alice and Bob for all tagged qubit-pairs, $\rho_{\rm t}^{(N_{\rm t})}$. Since Eve attacks each tagged pair individually, we have $\rho_{\rm t}^{(N_{\rm t})} = \sigma^{\otimes N_{\rm t}}$. Therefore, it is sufficient to consider one of these qubit pairs. After Bob has undone the rotation applied by Alice on his qubit, the purified quantum state of a tagged qubit-pair for which Bob's half has suffered a PNS attack is of the form

$$|\chi\rangle_{\rm ABE} = \frac{1}{\sqrt{2}}\left(|0\rangle_{\rm A}\otimes|0\rangle_{\rm B}\otimes|\tilde{0}\rangle_{\rm E} + |1\rangle_{\rm A}\otimes|1\rangle_{\rm B}\otimes|\tilde{1}\rangle_{\rm E}\right)$$
$$\equiv \frac{1}{\sqrt{2}}\left(|\Phi^{+}\rangle\otimes|0\rangle_{\rm E} + |\Phi^{-}\rangle\otimes|1\rangle_{\rm E}\right). \quad (8)$$

This state can be obtained, for example, in the context of the Jaynes-Cummings Hamiltonian discussed in the appendix of reference [10]. Thereby, Eve's pure ancilla states

$|0\rangle_{\rm E} = \left(|\tilde{0}\rangle_{\rm E} + |\tilde{1}\rangle_{\rm E}\right)/\sqrt{2}$ and $|1\rangle_{\rm E} = \left(|\tilde{0}\rangle_{\rm E} - |\tilde{1}\rangle_{\rm E}\right)/\sqrt{2}$ are orthogonal. The Bell state $|\Phi^-\rangle = (|0\rangle_{\rm A} \otimes |0\rangle_{\rm B} - |1\rangle_{\rm A} \otimes |1\rangle_{\rm B})/\sqrt{2}$ characterizes the phase errors introduced by Eve's ideal attack. The equal amplitudes of magnitude $1/\sqrt{2}$ reflect the fact that Eve does not perturb Alice's and Bob's measurement statistics by her attack. Correspondingly, the reduced quantum state of Alice and Bob resulting from such an ideal attack is a random mixture of the ideal Bell state $|\Phi^+\rangle$ and the corresponding phase-flipped Bell state $|\Phi^-\rangle$, i.e.,

$$\sigma = \frac{1}{2}(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|). \tag{9}$$

The separability of the state (9) reflects the fact that Eve has a perfect copy of Bob's qubit and thus secret-key distillation is impossible [22,26,27].

3.1.2 Attack on untagged qubits

Being able to obtain full information on the fraction of the key originating from tagged qubits, Eve may attack the remaining $N_{\rm u}$ untagged qubits coherently in order to obtain additional information on the final key. In general, at the end of such a coherent attack the reduced state of the untagged pairs $\rho_{\rm u}^{(N_{\rm u})}$ has a rather complicated form. In particular each pair can be entangled with Eve's ancilla as well as with other untagged qubit-pairs.

However, the key point is that Alice and Bob randomly permute all their (tagged and untagged) pairs immediately after Bob has announced the reception of all his qubits. As a result, the state $\rho_{\rm u}^{(N_{\rm u})}$ becomes permutation invariant. Hence, according to lemmas 2 and 3 (including the related proofs) of reference [15], it suffices for our purposes to consider uncorrelated Pauli attacks only, where Eve applies a random Pauli operator independently on each submitted qubit. In particular, she applies $\mathcal{X}$ with probability $q_{\rm x}$, $\mathcal{Z}$ with probability $q_{\rm z}$, $\mathcal{Y} \equiv {\rm i}\mathcal{X}\mathcal{Z}$ with probability $q_{\rm y}$, and the identity $\mathcal{I}$ with probability $q_{\rm I} = 1 - q_{\rm x} - q_{\rm y} - q_{\rm z}$. The resulting state of an uncorrelated Pauli attack is therefore of the form $\rho_{\rm u}^{(N_{\rm u})} = \tau^{\otimes N_{\rm u}}$, where the single-pair state τ is diagonal in the Bell-basis [21] i.e.,

$$\begin{aligned}\tau = {} & q_{\rm I}|\Phi^+\rangle\langle\Phi^+| + q_{\rm z}|\Phi^-\rangle\langle\Phi^-| \\ & + q_{\rm x}|\Psi^+\rangle\langle\Psi^+| + q_{\rm y}|\Psi^-\rangle\langle\Psi^-|.\end{aligned} \tag{10}$$

Note now that due to Alice's random rotation the quantum state τ is also rotation invariant i.e., it is symmetrized with respect to the corresponding group of unitary transformations $\mathcal{G} = \{\mathcal{R}_{\rm A}^b \otimes \mathcal{R}_{\rm B}^b \mid b = 0, \ldots, \beta\}$. This symmetry, implies additional constraints on the (error) probabilities $(q_{\rm x}, q_{\rm y}, q_{\rm z})$ of the state (10). In particular, for the four-state protocol we have $q_{\rm x} = q_{\rm z}$ whereas for the more symmetric six-state protocol $q_{\rm x} = q_{\rm y} = q_{\rm z}$. Thereby, these symmetry constraints are characteristic for the two (three) MUBs used in the four (six)-state QKD protocol. It is worth noting, however, that this rotation-invariance does not apply to the case of PNS attacks, as the tagged qubits inform Eve about their bases of preparation. Eve can always therefore follow the rotations applied by Alice and remain undetected.

3.2 Alice's and Bob's point of view

Let us now assume that Alice and Bob do not have Eve's technology and thus are not able to distinguish between tagged and untagged qubit-pairs. In other words, from their point of view all the pairs are equivalent. They only know that their imperfect source produces ideal qubits with some probability, and tags the qubits otherwise. Formally speaking, Alice and Bob share N qubit-pairs in the quantum state

$$\rho_{\rm tot}^{(N)} = \frac{1}{\Pi} \sum_{\Pi} \Pi \left(\sigma^{\otimes N_{\rm t}} \otimes \tau^{\otimes N_{\rm u}}\right) \Pi^\dagger, \tag{11}$$

where the summation runs over all possible permutations and expresses Alice's and Bob's ignorance about the precise location of the tagged pairs within the block of N pairs. In the limit of large N we have $N_{\rm u} \approx (1-\Delta)N$ and $N_{\rm t} \approx \Delta N$, thus obtaining from equation (11)

$$\rho_{\rm tot}^{(N)} \approx \rho^{\otimes N}, \tag{12}$$

where

$$\rho = \Delta\sigma + (1-\Delta)\tau. \tag{13}$$

An easy way to see this, is by using the binomial theorem since the density operators σ and τ commute.

Hence, in view of the state (12, 13), the overall bit-error rate estimated by Alice and Bob during the verification test by random pair-sampling and measurements along the Z-basis [23] is given by

$$\delta = (1-\Delta)\delta_{\rm b,u} = (1-\Delta)(q_{\rm x} + q_{\rm y}), \tag{14}$$

where $\delta_{\rm b,u}$ is the error probability for a single untagged pair as determined by its state (10). In view of the symmetry between all the bases used in the protocols we also have for the phase-error probability of the untagged pairs $\delta_{\rm p,u} = \delta_{\rm b,u}$.

Having derived the state shared between Alice and Bob at the beginning of the post-processing stage, we now turn to discuss asymptotic secret-key generation rates in the context of a two-way CSS-like EPP.

4 Increasing secure distances using two-way post-processing

In this section, we demonstrate how one can suppress the disastrous effect of dark counts (exhibited as a sudden drop of $R_{\rm CSS}$ in Fig. 1), thus increasing the distance over which a secret key can be distributed. Our approach relies on a two-way error-rejection procedure followed by a one-way CSS-like EPP.

4.1 Error-rejection with two-way classical communication

The error-rejection procedure under consideration is the so-called B-step entering a two-way post-processing of the Gottesman-Lo-type [15,29]. It is basically a purification process with two-way classical communication and its properties have been thoroughly discussed in the literature [15,29–32]. In all these investigations, the authors mainly focus on the influence of the B-steps on the error rates as all the involved qubit-pairs are identical. In our case, however, the situation is substantially different as the qubit-pairs involved in a B-step may be tagged or untagged. Given that Eve has full information on Bob's qubit in the former case, in addition to error rates we have to keep track of any changes in the rate of tagged qubit-pairs during B-steps.

Let us start by briefly recapitulating the stages of a B-step. Alice and Bob randomly form tetrads of qubits by pairing up their qubit-pairs. Then, within each tetrad they apply a bilateral exclusive-OR operation (BXOR) i.e., they apply the local unitary operation $\mathrm{XOR}_{\mathrm{a}\to\mathrm{b}}$: $|x\rangle_{\mathrm{a}} \otimes |y\rangle_{\mathrm{b}} \mapsto |x\rangle_{\mathrm{a}} \otimes |x \oplus y\rangle_{\mathrm{b}}$, on their halves. Thereby, $\oplus$ denotes addition modulo 2 while a and b denote the control and target qubit, respectively. Accordingly, for the two qubit-pairs constituting the random tetrad we have the following map in the Bell basis

$$\mathrm{BXOR}_{\mathrm{a}\to\mathrm{b}}\colon\ |\Psi^{(\mathrm{a})}_{i,j}\rangle \otimes |\Psi^{(\mathrm{b})}_{x,y}\rangle \mapsto |\Psi^{(\mathrm{a})}_{i,j\oplus y}\rangle \otimes |\Psi^{(\mathrm{b})}_{i\oplus x,y}\rangle, \quad (15)$$

where $i, j, x, y \in \{0, 1\}$ and the Bell states are denoted by $|\Psi_{0,0}\rangle \equiv |\Phi^+\rangle$, $|\Psi_{0,1}\rangle \equiv |\Phi^-\rangle$, $|\Psi_{1,0}\rangle \equiv |\Psi^+\rangle$, and $|\Psi_{1,1}\rangle \equiv |\Psi^-\rangle$. Subsequently, Alice and Bob measure their target qubits (b) in the Z-basis and compare their outcomes. The target pair is always discarded while the control qubit-pair is kept if and only if their outcomes agree i.e., if and only if $i = x$. In general, this procedure is repeated many times (many rounds of B-step).

Consider now that Alice and Bob apply the B-step procedure we have just described on their pairs before switching to a CSS-like EPP. Recall also that the quantum state of all N qubit-pairs shared between Alice and Bob at this stage of the QKD protocol has the general tensor-product form given in equations (12, 13). Depending on whether the qubit-pairs forming a random tetrad are untagged or tagged or only one of them is tagged we may distinguish four different cases.

1. *Untagged target and control pairs.* According to equations (12, 13), such a pairing occurs with probability $(1-\Delta)^2$, while each of the qubit-pairs is in the Bell-diagonal quantum state (10). Hence, provided that Alice's and Bob's measurements agree, the control pair is kept and is mapped again onto a Bell-diagonal quantum state of the same form, but with renormalized parameters [15]

$$\begin{aligned} q'_{\mathrm{I}} &= \frac{(q_{\mathrm{I}}+q_{\mathrm{z}})^2 + (q_{\mathrm{I}}-q_{\mathrm{z}})^2}{2Q_{\mathrm{u,s}}}, \\ q'_{\mathrm{z}} &= \frac{(q_{\mathrm{I}}+q_{\mathrm{z}})^2 - (q_{\mathrm{I}}-q_{\mathrm{z}})^2}{2Q_{\mathrm{u,s}}}, \\ q'_{\mathrm{x}} &= \frac{(q_{\mathrm{x}}+q_{\mathrm{y}})^2 + (q_{\mathrm{x}}-q_{\mathrm{y}})^2}{2Q_{\mathrm{u,s}}}, \\ q'_{\mathrm{y}} &= \frac{(q_{\mathrm{x}}+q_{\mathrm{y}})^2 - (q_{\mathrm{x}}-q_{\mathrm{y}})^2}{2Q_{\mathrm{u,s}}}, \end{aligned} \quad (16)$$

   where $Q_{\mathrm{u,s}} = (q_{\mathrm{I}}+q_{\mathrm{z}})^2 + (q_{\mathrm{x}}+q_{\mathrm{y}})^2$ is the probability with which the control qubit-pair is kept. Moreover, conservation of probability requires the relation $q_{\mathrm{I}} + q_{\mathrm{z}} + q_{\mathrm{x}} + q_{\mathrm{y}} = q'_{\mathrm{I}} + q'_{\mathrm{z}} + q'_{\mathrm{x}} + q'_{\mathrm{y}} = 1$.
2. *Tagged target and control pairs.* In view of equations (12, 13) such a pairing takes place with probability Δ^2. The two pairs are in the same Bell-diagonal state given by equation (9), and thus the map (16) applies also in this case. Setting $q_{\mathrm{x}} = q_{\mathrm{y}} = 0$ and $q_{\mathrm{I}} = q_{\mathrm{z}} = 1/2$, we have that the control pair always survives and is again tagged i.e., its state is given by (9).
3. *Tagged target pair and untagged control pair.* Such a pairing occurs with probability $\Delta(1-\Delta)$. Using the map (15) and the form of the states τ and σ given by equations (10) and (9) respectively, one immediately obtains that for the case under consideration the control pair survives with probability $Q_{\mathrm{t,s}} = (q_{\mathrm{I}} + q_{\mathrm{z}})$ and is left in a quantum state of the form (9). Knowing that one of the purifications of such a state is equation (8), and giving all the purification to Eve [20], we may conclude that the state of the surviving control pair refers to the tagged state of equation (8). In other words, the initially untagged control pair becomes tagged when paired with a tagged target pair. This is equivalent to the XOR operation of an unknown classical bit S with a totally known classical bit M. Since the target bit $T = S \oplus M$ is announced publically, S becomes perfectly known to Eve.
4. *Untagged target pair and tagged control pair.* This is equivalent to the previous case.

In summary, only cases in which both pairs involved in a random tetrad are untagged can lead to an untagged surviving qubit-pair which may later on result to a secret bit for Alice and Bob. In all other cases, Eve has a perfect copy of Bob's surviving tagged qubit.

A qubit-pair initially prepared in the mixed quantum state (13) with σ and τ given by equations (9) and (10) respectively, survives the first B-step with probability

$$P'_{\mathrm{s}} = (1-\Delta)^2 Q_{\mathrm{u,s}} + 2\Delta(1-\Delta)Q_{\mathrm{t,s}} + \Delta^2. \quad (17)$$

Moreover, its new quantum state is given by

$$\rho' = \Delta'\sigma + (1-\Delta')\tau', \quad (18)$$

with the renormalized tagging probability

$$\Delta' = \frac{[\Delta^2 + 2\Delta(1-\Delta)(q_{\mathrm{I}}+q_{\mathrm{z}})]}{P'_{\mathrm{s}}}, \quad (19)$$

and with the untagged renormalized quantum state

$$\tau' = q'_{\rm I}|\Phi^+\rangle\langle\Phi^+| + q'_{\rm z}|\Phi^-\rangle\langle\Phi^-| + q'_{\rm x}|\Psi^+\rangle\langle\Psi^+| + q'_{\rm y}|\Psi^-\rangle\langle\Psi^-| \quad (20)$$

where the new probabilities $(q'_{\rm I}, q'_{\rm z}, q'_{\rm y}, q'_{\rm z})$ are determined by equations (16). Correspondingly, the bit-error probability of this new quantum state is given by

$$\delta' = (1-\Delta')\delta'_{\rm b,u} = (1-\Delta')(q'_{\rm x} + q'_{\rm y}). \quad (21)$$

As a result of the B-step, however, the probabilities of bit and phase errors for an untagged qubit are not equal anymore. In particular, we have

$$\delta'_{\rm p,u} = (q'_{\rm z} + q'_{\rm y}). \quad (22)$$

Consider now that immediately after one such B-step Alice and Bob switch to a one-way CSS-like EPP to distill a secret key. The overall asymptotically achievable secret-key generation rate is given by the corresponding modification of equation (5) i.e.,

$$R_{\rm BCSS} = \frac{P_{\rm exp}P'_{\rm s}}{2\beta}\left(1-\Delta'-H(\delta')-(1-\Delta')H(\delta'_{\rm p,u})\right), \quad (23)$$

where Δ', δ' and $\delta'_{\rm p,u}$ are given by equations (17–22). The additional factor of 1/2 accounts for the target qubit-pairs which are always thrown away during the B-step. With the help of the recursion relations (16) and (19) asymptotically achievable secret-key generation rates can also be determined for cases in which B-steps are applied iteratively before the final use of the one-way CSS-like EPP. In that case, however, the factor of 1/2 should be replaced by $1/2^n$, for n B-steps. The rate $R_{\rm BCSS}$ is therefore a generalization of the GLLP rate $R_{\rm CSS}$ to a post-processing where the one-way CSS-like EPP is initialized by a number of B-steps. Indeed, the rate (23) directly reduces to the rate (5) in the absence of B-steps i.e., by setting $(q'_{\rm I}, q'_{\rm x}, q'_{\rm y}, q'_{\rm z}) = (q_{\rm I}, q_{\rm x}, q_{\rm y}, q_{\rm z})$, $P'_{\rm s} = 1$, $\Delta' = \Delta$, and dropping the factor 1/2.

4.2 Numerical simulations and discussion

In our simulations, we adopt the most pessimistic approach i.e, we consider an eavesdropper with unlimited technological power [10]. In particular, we attribute all the estimated bit-error rate δ to Eve, assuming that she possesses the corresponding information on the key. We thus give Eve all the power to replace the lossy channel by a perfect one (as described in Sect. 2.2), and to adjust the two contributions in δ (that is, $\delta_{\rm opt}$ and $\delta_{\rm det}$) at her own benefit (see also related discussion in Ref. [12]). Formally speaking, combining equations (3) and (14), at the beginning of the first B-step we have

$$\delta = (1-\Delta)(q_{\rm x}+q_{\rm y}) = \frac{\delta_0\ P^{\rm signal}_{\rm exp} + \frac{1}{2}P^{\rm dark}_{\rm exp}}{P_{\rm exp}}, \quad (24)$$

where $P_{\rm exp}$, $P^{\rm signal}_{\rm exp}$ and Δ are defined in Section 2.2. However, as we discussed in Section 3.1, the probabilities $(q_{\rm I}, q_{\rm x}, q_{\rm y}, q_{\rm z})$ entering the map (16) are not independent. The normalization condition for the state (10) implies that

$$q_{\rm I} = 1 - q_{\rm x} - q_{\rm y} - q_{\rm z}, \quad (25)$$

while due to symmetry between all the bases used in the QKD protocols under consideration we have one additional constraint. That is,

$$q_{\rm x} = q_{\rm z} = q_{\rm y} \quad (26)$$

for the six-state protocol, and

$$q_{\rm x} = q_{\rm z} \quad (27)$$

for the four-state protocol, respectively.

In the case of the six-state protocol the constraints (24–26) fully determine the initial values of the probabilities $(q_{\rm I}, q_{\rm x}, q_{\rm y}, q_{\rm z})$. More precisely, we have

$$q_{\rm x} = q_{\rm y} = q_{\rm z} = \frac{\delta_0\ P^{\rm signal}_{\rm exp} + \frac{1}{2}P^{\rm dark}_{\rm exp}}{2(1-\Delta)P_{\rm exp}},$$
$$q_{\rm I} = 1 - \frac{3\left(\delta_0\ P^{\rm signal}_{\rm exp} + \frac{1}{2}P^{\rm dark}_{\rm exp}\right)}{2(1-\Delta)P_{\rm exp}}. \quad (28)$$

On the contrary, such a unique choice is not possible for the four-state protocol and we have one open parameter left that is, $0 \le q_{\rm y} \le 1$. It is known, however, that for the map (16), the choice $q_{\rm y} = 0$ gives rise to the largest resulting value of the phase-error probability and to the smallest resulting secret-key rate [15]. Therefore, in the case of the four-state QKD protocol we can restrict our subsequent discussion to the initial condition

$$q_{\rm y} = 0,$$
$$q_{\rm x} = q_{\rm z} = \frac{\delta_0\ P^{\rm signal}_{\rm exp} + \frac{1}{2}P^{\rm dark}_{\rm exp}}{(1-\Delta)P_{\rm exp}},$$
$$q_{\rm I} = 1 - \frac{2\left(\delta_0\ P^{\rm signal}_{\rm exp} + \frac{1}{2}P^{\rm dark}_{\rm exp}\right)}{(1-\Delta)P_{\rm exp}}. \quad (29)$$

Clearly, in both cases all the probabilities are distance-dependent. Indeed, the larger the distance between Alice and Bob becomes, the more power Eve has as she may take full advantage of all losses, noise, and imperfections.

We turn now to present and discuss numerical results regarding the effect of applied B-steps on the secret-key rates, for various QKD qubit-based protocols. For short distances (i.e., length of the fiber l) where no B-steps are necessary, the secret-key rate is basically determined by equations (5), (6) and (3), as in Section 2.3. However, for secret-key distribution over larger distances application of B-steps prior to post-processing by one-way CSS-like EPP is a necessity and the corresponding secret-key rate is given by (23) combined with equations (17–22) and the initial condition for B-steps (28) or (29). In any case, for a given distance we optimize the mean number of photons to obtain the maximum possible secret-key rate.

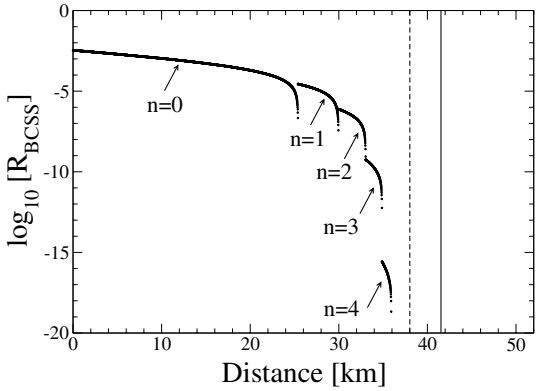

Fig. 2. Four-state protocol. Secret-key generation rates resulting from multiple applications of B-steps followed by one-way CSS-based post-processing: the solid vertical line indicates the maximum allowed distances according to inequality (7). The dotted line is the asymptotically achievable distance according to inequality (31). The parameters are the same as in Figure 1.

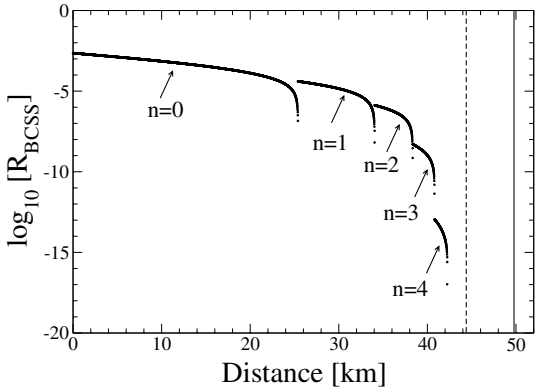

Fig. 3. Six-state protocol. The parameters are the same as in Figure 2.

The influence of different numbers of B-steps on R_{BCSS} is depicted in Figures 2 and 3 for the four- and the six-state protocol, respectively. Whereas for the parameters chosen in the absence of any B-steps the maximum possible distance over which a secret key can be distilled with a significant rate is of the order of 25 km for both protocols, this distance increases significantly if Alice and Bob perform a few B-steps before switching to the one-way CSS-like EPP. More precisely, one application of a B-step already increases this maximum possible distance to approximately 30 km in the four-state and to 34 km in the six-state protocol. One may observe a sudden increase in the secret-key generation rate on applying a B-step. This is because a B-step decreases the bit-error rate significantly and thus the effect of dark counts becomes less significant. However, for larger distances, dark counts again become dominant, resulting in a new dip in the key generation rate unless a second B-step is applied. For increasing numbers of B-steps this effect becomes less dominating as the phase-error probability of the untagged pairs increases after each B-step [15,29] and therefore dark counts become effective in the phase-error part. It can also be noticed that in the six-state protocol each B-step results in a larger increase of the maximal achievable distance with less reduction of the secret-key generation rate compared to the four-state protocol. Basically, this is due to the fact that the six-state protocol can sustain higher error rates. Finally, as depicted in Figure 4, multiple applications of B-steps quickly increase the maximum possible distances almost up to approximately 37 km for the four-state and to 44 km for the six-state protocol.

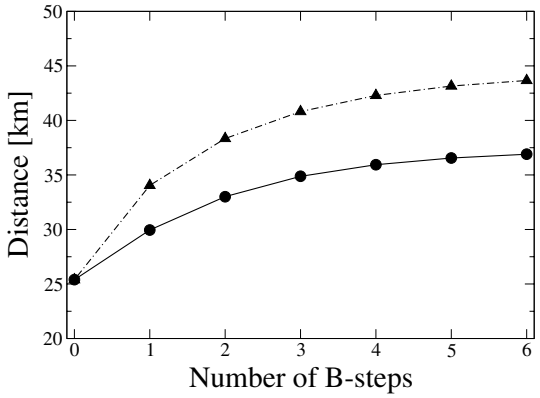

Fig. 4. Maximum achievable distance for different numbers of B-steps for the four-state (lower curve) and the six-state protocol (upper curve).

Let us now explore to which extent multiple applications of B-steps are capable of approaching the limiting distances resulting from equation (7) for the two QKD protocols under consideration. These latter distances are indicated by full vertical lines in Figures 2 and 3. Following the arguments of reference [8] which form the basis for the secret-key generation rates of equations (5) and (23), for our purpose it is sufficient to explore the possibility of purifying only the untagged qubit-pairs by B-steps. As demonstrated in reference [32], the inequality

$$\left(q_{\mathrm{I}} - \frac{1}{4}\right)^2 + \left(q_{\mathrm{z}} - \frac{1}{4}\right)^2 > \frac{1}{8}, \tag{30}$$

is a necessary condition for the purification of a Bell-diagonal state of the form (10) by a sequence of B-steps followed by a CSS-like EPP. Therefore, using equations (24–27) inequality (30) yields for the two protocols

$$\Delta < \begin{cases} 1 - 5\delta & \text{four-state protocol} \\ \frac{1}{2}\left(2 - 5\delta - \sqrt{5}\delta\right) & \text{six-state protocol.} \end{cases} \tag{31}$$

The other solutions of the inequality (30) do not satisfy the necessary condition for secret-key generation given by (7).

In Figure 5, we plot the possible values of the effective tagging probability Δ and the estimated bit-error rate δ consistent with the necessary conditions (7) and (31), for the four- and the six-state protocols. These are basically parameters which can be estimated by Alice and Bob. According to the necessary condition (7), secret-key distillation is, in principle, possible everywhere except in the black regime. One may notice, however, the small grey region which (although allowed by inequality (7)) is not

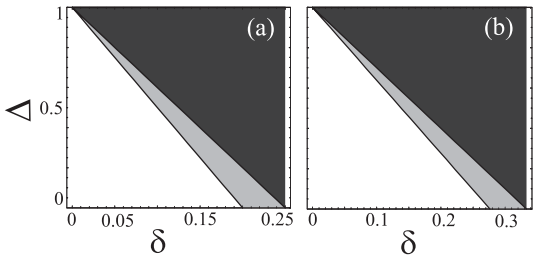

Fig. 5. Regions bounded by equations (7) (white+grey) and (31) (white) for the four-state (a) and the six-state (b) QKD protocols. Secret key distillation is not possible by any means in the black region. The grey region is not accessible to B-steps and CSS-like EPP.

accessible to a post-processing involving B-steps and a CSS-like EPP. The upper bounds on distances resulting from the inequalities (31) are indicated by the vertical dotted lines in Figures 2 and 3.

From Figures 2, 3 and 4, it is apparent that these latter threshold values for the maximum possible distances are approached already after a few iterations of B-steps followed by a CSS-like EPP. Thus, such a combination yields a useful method for counteracting the influence of dark counts on the secret-key rate in practical QKD implementations. However, from Figures 2 and 3 it is also apparent that at the same time the secret-key rate decreases considerably with the application of more than two B-steps.

As decoy-state protocols were developed in order to suppress imperfections arising from multiphoton pulses it is of interest to explore the influence of B-steps on the corresponding achievable secret-key generation rates. For this purpose let us consider a decoy-state protocol involving two decoy WCPs with mean photon numbers $\kappa < \nu$ fulfilling the additional requirement $\kappa \exp(-\kappa) < \nu \exp(-\nu)$, and a signal pulse with mean photon number $\mu > \kappa + \nu$. Therefore, the decoy pulses are detected with probabilities $P_{\rm exp}^{(\kappa)}$ and $P_{\rm exp}^{(\nu)}$ obeying the relations [17,18]

$$P_{\rm exp}^{(\kappa)} = P_{\rm exp}^{\rm dark} e^{-\kappa} + s_1 \kappa e^{-\kappa} + s_{\rm m}(1 - e^{-\kappa} - \kappa e^{-\kappa}),$$
$$P_{\rm exp}^{(\nu)} \geq P_{\rm exp}^{\rm dark} e^{-\nu} + s_1 \nu e^{-\nu} + s_{\rm m}(1 - e^{-\kappa} - \kappa e^{-\kappa}) \frac{\nu^2 e^{-\nu}}{\kappa^2 e^{-\kappa}}. \quad (32)$$

Thereby, $s_{\rm m}$ is the conditional probability that the detector clicks provided a multiphoton pulse with mean photon number κ hits the detector, whereas s_1 is the corresponding probability for single-photon pulses. Using (32) we obtain

$$s_1 \geq \frac{\nu^2 e^{\kappa} P_{\rm exp}^{(\kappa)} - \kappa^2 e^{\nu} P_{\rm exp}^{(\nu)} - (\nu^2 - \kappa^2) P_{\rm exp}^{\rm dark}}{\kappa\nu(\nu - \kappa)} := \overline{s}_1. \quad (33)$$

The inequality in the second line of (32) is valid provided the inequalities $\kappa < \nu$ and $\kappa \exp(-\kappa) < \nu \exp(-\nu)$ are fulfilled. Correspondingly, the probability Δ_μ of multiphoton signal pulses can be upper-bounded as follows

$$\Delta_\mu \leq 1 - \frac{\overline{s}_1 \mu e^{-\mu}}{P_{\rm exp}^{(\mu)}} := \tilde{\Delta}_\mu. \quad (34)$$

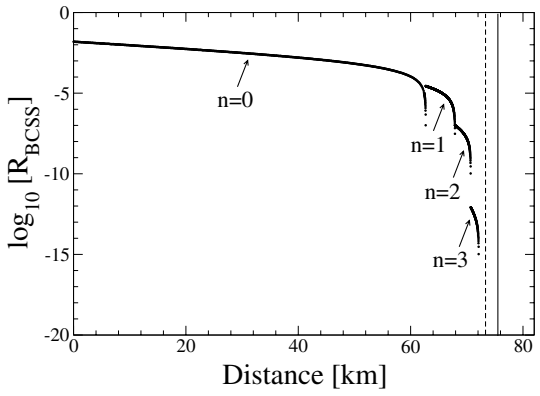

Fig. 6. Four-state protocol with decoy pulses: the parameters are the same as in Figure 2, while $\mu = 0.55$, $\kappa = 0.10$, and $\nu = 0.27$.

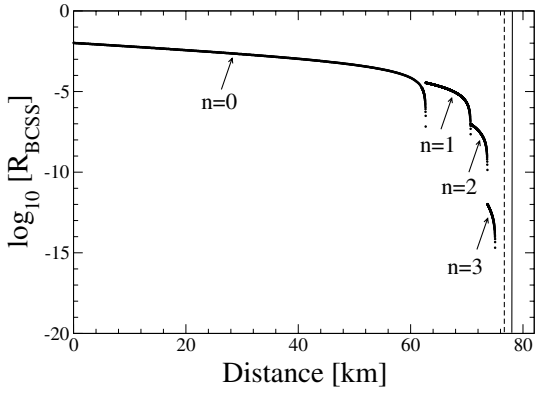

Fig. 7. Six-state protocol with decoy pulses: the parameters are the same as in Figure 6.

To investigate the influence of B-steps on the achievable secret-key rates in the context of QKD protocols with decoy pulses, we can adapt our previous arguments easily. In particular, a lower bound on the resulting secret-key generation rate is obtained from equations (16), (17), (19), (21), and (23). Thereby, the recursive relations have to be solved by setting $\Delta = \tilde{\Delta}_\mu$ in the initial conditions (28) and (29) for the six- and the four-state protocol, respectively. These initial conditions take into account that the phase-error probability can be bounded from above by $\delta/(1 - \tilde{\Delta}_\mu)$. The resulting lower bound on the secret-key generation rate and its dependence on the length of the optical fibre used for the transmission of photons are depicted in Figures 6 and 7 for the four- and the six-state protocol, respectively. Following reference [17], we have chosen μ, κ and ν equal to 0.55, 0.10 and 0.27, respectively. Typically, multiple application of B-steps increase the distance over which a secret key can be exchanged significantly. The maximum distances and their dependence on the number of applied B-steps is shown in Figure 8 for both protocols with decoy pulses. The asymptotically achievable maximum distances of the order of 80 km are reached already after a few B-steps. Moreover, it is worth noting that the net increase in distance of about 15 km (after 2 or 3 B-steps) is the same as that for the conventional four- and six-state protocols.

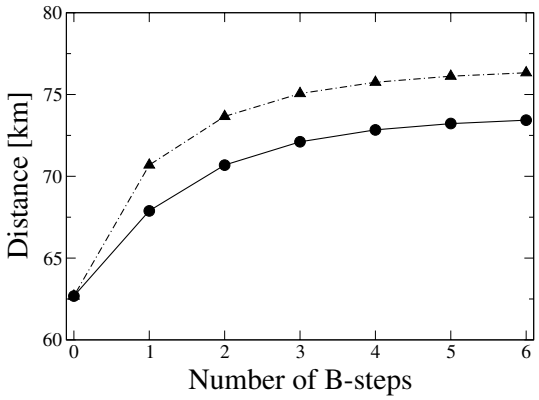

Fig. 8. Maximum achievable distances for different numbers of B-steps for the four-state (lower curve) and the six-state (upper curve) protocols with decoy pulses.

In closing, we would like to stress once more that, although our results have been formulated in the framework of the two-way EPP-based versions of the four- and the six-state QKD protocols, they also apply to the corresponding prepare-and-measure schemes. According to theorems 5 and 6 in reference [15] such a reduction is possible without compromising security, due to basic properties of the B-step and the one-way CSS-like EPP. Let us briefly highlight the main steps in this reduction. In the terminology of [15], a B-step involves only measurements of the form $\mathcal{Z}_{\mathrm{A}} \otimes \mathcal{Z}_{\mathrm{B}}$ for the purpose of bit-flip error detection and subsequent rejection. Hence, no post-selection based on phase-error syndromes takes place during the two-way part of the post-processing. In the one-way CSS-like part each operator being measured is either of $\mathcal{X}$- or $\mathcal{Z}$-type (definitions 1 and 4 of reference [15]) while, at any rate, earlier measurements do not affect the sequence of subsequent measurements. Moreover, all the operators commute with each other and thus all the measurements of $\mathcal{Z}$-type can be performed before all the measurements of $\mathcal{X}$-type. To complete the reduction, one has to note that $\mathcal{X}$-type measurements at the end of post-processing yield phase-error syndromes which do not affect the value of the final key and thus Alice and Bob do not have to perform them [3]. In the resulting prepare-and-measure schemes the classical post-processing involves a number of two-way error-rejection steps (parity checks) and additional one-way post-processing (error-correction and privacy amplification) based on asymmetric CSS codes. The phase-error syndrome measurements become effectively privacy amplification [3].

5 Concluding remarks

We have analyzed secret-key generation rates in the presence of imperfections arising from tagging of Alice's source and from dark counts at Bob's detectors. In particular, we considered a post-processing procedure (error correction and privacy amplification) based on a combination of B-steps and asymmetric CSS codes. As a main result, for the four-state, the six-state, and the decoy-state protocols, it was demonstrated that such a post-processing may considerably increase the maximum distances over which a secure key can be distributed in optical-fiber links.

Hence, incorporation of B-steps in the post-processing stage of practical implementations of the protocols is proven to be particularly useful. The usefulness of B-steps is also one of the main results of a recent thorough investigation of decoy-state protocols presented in reference [33]. On the contrary, P-steps of the Gottesman-Lo type do not seem to be as useful as B-steps. Indeed, all our numerical simulations demonstrate that a few applications of B-steps are sufficient to bring the maximal secure distances very close to the upper bound. Recently, this inessentiality of P-steps has been pointed out by other authors as well [32–34].

We would like to conclude this work with a discussion about certain assumptions underlying our approach and related possible open questions. Our model for sources and detectors is not as general as possible and it suffers from the same limitations as the model adopted in references [8,10–12]. For instance, we have focused on imperfect sources which tag a fraction of the signals in an uncorrelated and independent manner. In other words, we have not considered the case of coherent or other highly correlated basis-dependent tagging [8]. In this context, our analysis has been based on a particular class of eavesdropping attacks where the sets of tagged and untagged qubits are attacked separately. Each tagged qubit is treated individually (by means of a PNS attack) whereas untagged qubits undergo a coherent (joint) attack. In this way, on the one hand we essentially give Eve a perfect copy of the part of the key originating from tagged signals, while on the other hand we give her all the power to retrieve as much information as possible about the remaining bits of the key. It is plausible that, for a fixed bit-error rate, this is the most powerful attack one may consider in the framework of the particular model for sources and detectors. However, we would like to emphasize that this work shows how incorporation of B-steps prior to one-way CSS-based post-processing can postpone certain dark-count effects thus increasing the distances over which a secret-key can be distributed. This result is quite general and is not expected to change in the case of other, perhaps more efficient and more powerful, eavesdropping strategies. Indeed, as pointed out in references [10,12], the maximum secure distances for WCP-based QKD are not limited by the eavesdropping strategy under consideration but rather by the actual detector performance and especially by the dark-count rate. Finally, throughout this work we have also not addressed the case of imperfect sources which emit weak coherent pulses with nonrandom phases or highly dimensional signals [8]. At any rate, all of these issues depend on how well the two legitimate users know their devices (e.g., source and detectors) and how reliably they can characterize them by means of other, perhaps untrusted, apparatus [35].

This work is supported by the EU within the IP SECOQC. Informative discussions with N. Lütkenhaus, K.S. Ranade, and J.M. Renes are acknowledged. GMN also acknowledges support by "Pythagoras II" of the EPEAEK research program.

References

1. C.H. Bennett, G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), p. 175
2. D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998)
3. P.W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000)
4. M. Koashi, J. Preskill, Phys. Rev. Lett. **90**, 057902 (2002)
5. H.-K. Lo, Quant. Inf. Comput. **1**, 81 (2001)
6. D. Mayers, J. ACM **48**, 351 (2001)
7. For details see, for instance, related discussion in reference [8]
8. D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, Quant. Inf. Comput. **4**, 325 (2004)
9. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
10. N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000)
11. G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000)
12. S. Felix, N. Gisin, A. Stefanov, H. Zbinden, J. Mod. Opt. **48**, 2009 (2001)
13. H. Inamori, N. Lütkenhaus, D. Mayers, e-print `arXiv:quant-ph/0107017`
14. A.R. Calderbank, P.W. Shor, Phys. Rev. A **54**, 1098 (1996); A.M. Stean, Proc. Roy. Soc. Lond. A **452**, 2551 (1996)
15. D. Gottesman, H.-K. Lo, IEEE Trans. Inf. Theory **49,** 457 (2003)
16. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wooters, Phys. Rev. A **54**, 3824 (1996)
17. X.B. Wang, Phys. Rev. A **72**, 012322 (2005)
18. X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Phys. Rev. A **72**, 012326 (2005)
19. C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
20. M.A. Nielsen, I.L. Chuang, *Quantum computation and Quantum Information* (Cambridge University Press, cambridge, 2000)
21. The Bell states, $|\Phi^{\pm}\rangle \equiv (|0\rangle_{\rm A} \otimes |0\rangle_{\rm B} \pm |1\rangle_{\rm A} \otimes |1\rangle_{\rm B})/\sqrt{2}$ and $|\Psi^{\pm}\rangle \equiv (|0\rangle_{\rm A} \otimes |1\rangle_{\rm B} \pm |1\rangle_{\rm A} \otimes |0\rangle_{\rm B})/\sqrt{2}$, form an orthonormal basis in the two-qubit Hilbert space
22. G.M. Nikolopoulos, A. Khalique, G. Alber, Eur. Phys. J. D **37**, 441 (2006)
23. Classical random sampling theory can be applied safely for the estimation of error rates and the establishment of related confidence levels during the verification test (see, for instance, reference [24] for details). For the sake of simplicity, throughout this work we assume that the bit-error rate estimated during the tests is the actual bit-error rate in the pairs shared between Alice and Bob
24. H.-K. Lo, H.F. Chau, M. Ardehali, J. Cryptology **18**, 133 (2005)
25. M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonson, D. Ljunggren, E. Sundberg, Opt. Expr. **4,** 383 (1999)
26. M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2003)
27. A. Acín, N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005)
28. N. Lütkenhaus, M. Jahma, New J. Phys. **4**, 44 (2002)
29. H.F. Chau, Phys. Rev. A **66**, 060302 (2002)
30. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996)
31. C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wooters, Phys. Rev. Lett. **76**, 722 (1996)
32. K. Ranade, G. Alber, J. Phys. A **39**, 1701 (2006)
33. X. Ma, C.-H. Fred Fung, F. Dupuis, K. Chen, K. Tamaki, H.-K. Lo, e-print `arXiv:quant-ph/0604094`
34. A. Acín, J. Bae, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz-Tapia, Phys. Rev. A **73**, 012327 (2006)
35. D. Mayers, A. Yao, Quant. Inf. Comput. **4**, 273 (2004)