Theoretical Computer Science 560 (2014) 46–61

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Quantum key distribution using a two-way quantum channel

Marco Lucamarini [1], Stefano Mancini *

School of Science and Technology, University of Camerino, via Madonna delle Carceri, 9, 62032 Camerino, Italy

ARTICLE INFO

Article history:
Received 2 March 2009
Accepted 5 January 2011
Available online 21 September 2014

Keywords:
Quantum cryptography
Communication security

ABSTRACT

We review a quantum key distribution protocol, recently proposed by us, that makes use of a two-way quantum channel. We provide a characterization of such a protocol from a practical perspective, and consider the most relevant individual-particle eavesdropping strategies against it. This allows us to compare its potentialities with those of the standard BB84 protocol which uses a one-way quantum channel.

1. Introduction

Since the seminal works by Bennett and Brassard [1] and by Ekert [2] Quantum Key Distribution (QKD) has made impressive progresses [3], which can be roughly grouped into two main categories: on the one side there are theoretical progresses, among which the unconditional security of QKD is the most relevant one [4–8]; on the other side there are experimental progresses, almost exclusively in the field of quantum optics, which recently led to long-haul and high-rate QKD experiments [9–12]. The relevance of these advances promoted QKD as the most applicative research of quantum information, and also triggered the start-up of companies based on this technology [13].

Recent research on QKD is mainly focused on closing the existing gap between the perfect theory of the unconditional security proofs and the imperfect application of such a theory in the real world. This originated the definition of *practical QKD* [14,15] which deals with the proper modeling of devices like photon sources, light modulators and single-photon detectors [16,17]. By consequence, any new proposal relevant to the field of QKD can not set aside the practicality issue. This is even truer if one looks at the quantum hacking strategies based on practical imperfections recently accomplished by the group of Trondheim [18].

In this paper we want to characterize from a practical point of view a novel form of QKD based on a two-way quantum channel. Two-way channels are already used in QKD either in those setups based on a Plug-and-Play configuration [19] or in those using the Cascade error correction procedure [20]. However these two examples do not represent a two-way *quantum* channel: in the first case only the backward channel ought to be considered quantum; in the second case neither the forward nor the backward channel are quantum.

The first input to *two-way QKD* came from Boström and Felbinger's Ping–Pong protocol [21], where the question of the security of Quantum Dense Coding [22] was posed in terms of “deterministic and secure direct communication in presence of entanglement”. The Ping–Pong protocol was demonstrated insecure [23,24] but revised, more secure, versions were proposed later on [25–28], until the recent achievement of absolute security [29].

* Corresponding author.

[1] Present address: Cambridge Research Laboratory, Toshiba Research Europe Ltd., 208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, United Kingdom.

http://dx.doi.org/10.1016/j.tcs.2014.09.017
0304-3975/© 2014 Elsevier B.V. All rights reserved.

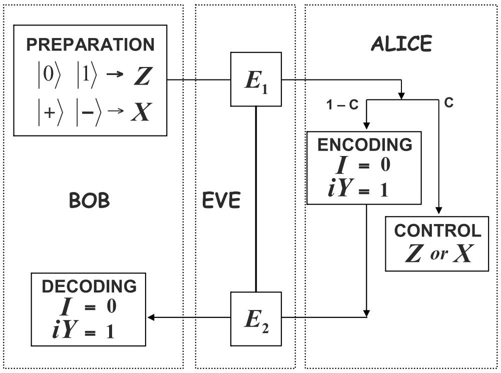

Fig. 1. Schematics of the practical LM05 protocol. Bob randomly prepares qubits of $\hat{X}$ and $\hat{Z}$ bases. With probability (1-c) Alice encodes data on the qubits (Encoding Mode, EM) and with probability (c) she measures the qubits (Control Mode, CM). Bob measures the returning qubits in the same bases they were prepared and finally decodes Alice's information. The noise check on the backward path, present in the original protocol [32], is removed in the present version.

Moving from these initial steps novel two-way schemes *without entanglement* were presented in [30], in [31] and then by us in [32]. This last scheme, named "LM05", had the merit of being more feasible and secure than the protocol in [21] and it came with the first security proof against non-trivial individual-particle attacks. As a matter of fact its experimental realization was proposed [33], proved in principle [34] and recently realized in the third telecom window [35]. Also, the protocol was generalized to a higher number of states [36,37] and to higher-dimensional Hilbert spaces [38–40].

Despite these improvements, a complete realization of the LM05 still remains an experimental challenge. The main problem is that in the original protocol both the forward and the backward channels are tested by the users to guarantee the security of the protocol. In particular the test of the backward channel requires that with a certain probability one of the users (Alice) prepares a qubit in exactly the same physical state as the one prepared by the other user (Bob) [32]. This is difficult in practice because all the relevant degrees of freedom of the qubit (wavelength, timing, bandwidth, etc.) must be accurately controlled by Alice.

In this work we modify the original LM05 protocol by removing the test of the backward channel and show that the resulting protocol is still secure against several single-particle attacks by the eavesdropper (Eve).

We also provide the state-of-the-art of the so called "deterministic QKD" [41] with a two-way quantum channel, together with a set of tools which can be used and further improved towards a final security proof of the scheme.

Throughout the work we compare our *deterministic* protocol with the standard *non-deterministic* BB84 [43].

2. The protocol

The practical rendering of the LM05 protocol (see Fig. 1) can be obtained from the original protocol [32] by removing the test performed by the users on the backward channel. Bob prepares a qubit in one of the four states $|0\rangle$, $|1\rangle$ (the Pauli $\hat{Z}$ eigenstates), $|+\rangle$, $|-\rangle$ (the Pauli $\hat{X}$ eigenstates), and sends it to his counterpart Alice. With probability c Alice switches to Control Mode (CM) and uses the qubit to test the channel noise or, with probability $1-c$, she switches to Encoding Mode (EM) and uses the qubit to encode a bit of information. The CM consists in a projective measurement of the qubit along a basis randomly chosen between $\hat{Z}$ and $\hat{X}$, in a way equal to the protocol BB84 [1]. In the original protocol [32] this step was followed by the preparation of a new qubit in the same state as the outcome of the measurement; however this step is removed from the present protocol as it is not practical to implement. In fact, to conceal the chosen modality to Eve, Alice should prepare a qubit in exactly the same physical state as the one prepared by Bob, i.e. same wavelength, bandwidth, time-width and intensity. This is not possible without a sophisticated control of the experimental devices. The lack of a direct test of the backward channel thus represents the fundamental difference respect to the protocol described in [32]. The EM is a modification of the qubit state according to one of the following transformations: the identity operation $\hat{I}$, which leaves the qubit unchanged and encodes the logical '0', or $i\hat{Y} \equiv \hat{Z}\hat{X}$ operation, which flips any of the qubits prepared by Bob and encodes the logical '1'. After the encoding step Alice sends the qubit back to Bob who measures it in the same basis he prepared it; in case of an EM run this feature allows Bob to *deterministically* infer Alice's operation, without any need of a basis reconciliation procedure, typical of a *non-deterministic* setup like BB84 [47]. Notice that Bob's measurement does not depend on the modality chosen by Alice (EM or CM): Bob will perform in any case his measurement, with a nonzero probability to detect a vacuum pulse due either to the natural losses of the channel or to a CM run by Alice or to a specific attack by Eve. After the quantum communication, Alice will tell on the classical channel which runs were CM and which were EM. We also point out that the direct test of at least one of the two channels is a necessary procedure for any two-way quantum protocol. In fact there exist attacks, like Trojan-horse [48], Quantum Man-in-the-Middle [49] and Double-CNOT [49,36], described in next Section 3.3, which can not be detected by Alice and Bob using only the EM runs.

Even if the bases are not revealed for the EM runs, they are revealed for comparing the data acquired during the CM runs. This, in complete analogy with the BB84, will provide the users with an estimate of the noise present on the forward channel in terms of the QBER (Quantum Bit Error Rate) q_1, defined as the ratio of the number of wrong bits over the number of total bits coming from CM runs. Beside q_1, the users can also estimate a second QBER Q_{AB} which comes from a fraction of the EM runs, in which Alice reveals on the public channel her encoding.

While q_1 is used to give an upper bound on Eve's information, Q_{AB} is used to provide an estimate of Alice and Bob mutual information, I_{AB}, with $I_{AB} = H(A) - H(A|B)$ and H the usual Shannon entropy [50]. In case A is a random binary variable we have:

$$I_{AB}(Q_{AB}) = 1 - H(Q_{AB}). \tag{1}$$

Note that there is no definite relation between the two QBERs q_1 and Q_{AB}. A precise relation can only be found by assuming a particular strategy by Eve, as done in [32] or by adopting a particular noise model, as we shall do in the following.

Eve's information is given in terms of mutual information between Eve and Alice, I_{AE}, or Eve and Bob, I_{BE}. Then the Csiszár–Körner (CK) theorem [51] is used to decide whether the QKD session is secure or not: Alice and Bob can establish a secret key (using Forward Error Correction and Privacy Amplification) if and only if $I_{AB} \geq I_{AE}$ or $I_{AB} \geq I_{BE}$. Depending on the use of the I_{AE} or I_{BE} in the CK theorem, it is possible to define respectively the *secrecy capacity* of the Direct Reconciliation (DR), C_s^{DR}, and of the Reverse Reconciliation (RR), C_s^{RR}, as follows:

$$C_s^{DR}(Q_{AB}, q_1) = I_{AB}(Q_{AB}) - \bar{I}_{AE}(q_1), \tag{2}$$

$$C_s^{RR}(Q_{AB}, q_1) = I_{AB}(Q_{AB}) - \bar{I}_{BE}(q_1), \tag{3}$$

where $\bar{I}_{AE}$, $\bar{I}_{BE}$ are the upper bounds to Eve's mutual information with Alice and Bob respectively, which as said are functions of q_1 only. Notice that according to the CK theorem is sufficient that only one of the secrecy capacities is greater than zero to have a secure communication. In order to accomplish a DR, the users must execute the Forward Error Correction in the direction that goes from Alice to Bob; in other terms it will be Alice to transmit to Bob the parity bits to correct the errors, and it will be Bob to correct the errors in his string to match Alice's string. For the RR the roles of the users are the opposite. We remark that to have a tentatively deterministic Direct Communication [21], it must be Alice to lead the reconciliation procedure, because only her knows the random choice between CM and EM. This means that the security of a deterministic communication closely depends on the mutual information I_{AE} and on the DR procedure.

The LM05 protocol has already been tested in free-space at the wavelength of 800 nm using the photon polarization as a quantum carrier of the information [34,52]. However this choice is not ideal in optical fibers because birefringence makes the polarization change randomly. The optimal implementation is to use an encoding based on the relative phase between two pulses separated in time. In this way the channel noise seen by the two pulses is the same, and their relative phase remains stable. The only left noise is the one coming from a misalignment between Alice's and Bob's apparatuses. To eliminate this source of noise one can adopt the mechanism of passive compensation, invented in [53] and employed for QKD in the Plug-and-Play system [54–57]. This technique fits very natural with the EM of LM05, thus letting the implementation reported in [35].

In the next sections we consider the most relevant individual attacks against LM05. Following the approach given in [58] we group the attacks into two main categories: *zero-loss* and *zero-QBER* attacks. The former, analyzed in Section 3, do not introduce any loss in the channel but introduce noise; the latter, treated in Section 4, introduce losses, but no noise. This description allows to a certain extent a fair comparison between one-way and two-way deterministic QKD.

3. Zero-loss eavesdropping

3.1. Intercept and resend attack – IR

The simplest attack in which Eve acquires information from the communication channel, thus unavoidably introducing noise in the same channel, is the *Intercept and Resend* (IR), which follows for the LM05 protocol the same steps as for the BB84 protocol [1,58].

In the IR against LM05 Eve measures the photon coming out from Bob along one basis chosen at random between the two bases used by Bob, i.e. $\hat{Z}$ and $\hat{X}$ [59]. Then she takes note of the outcome and forwards to Alice the qubit projected by her measurement in a certain state $|\psi\rangle$. Alice, in EM, will flip or not-flip this state, and sends it back to Bob. Eve measures on the backward path the state emerging from Alice box, using the same basis previously used in the forward path, thus learning the information; finally she forwards the qubit to Bob.

This attack can be detected through the QBER q_1 while running the CM. It is easy to see that when Eve perchance measures in the same basis of Alice and Bob, she creates no error in the forward channel; on the contrary, for different basis, she creates an error with probability 1/2. In both cases she acquires full information about Alice's encoding, causing an average value of q_1 equal to 1/4.

While IR provides Eve with full knowledge about Alice's encoding it does not provide her with full knowledge about the result of Bob's measurement. In fact the first measurement by Eve destroys the initial state prepared by Bob; furthermore the basis used by Bob is never revealed in LM05. This entails that Eve can foresees Bob's result only three times over four, that is when she perchance measures along the same basis as Bob and when she measures along the wrong basis but

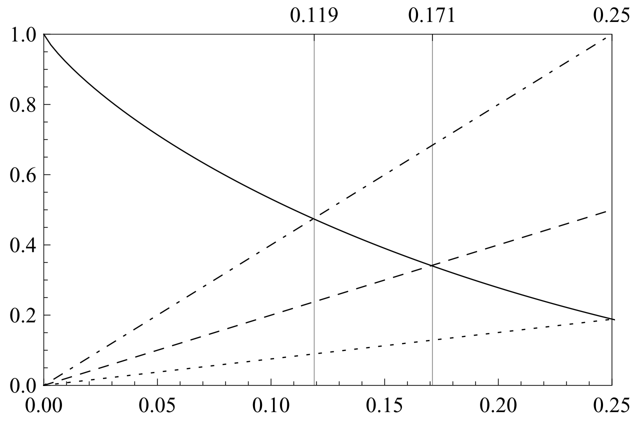

Fig. 2. Mutual information versus q_1 in LM05 and BB84 in case of IR attack by Eve. I_{AB}: solid line; I_{AE}^{LM05}: dot–dashed line; I_{BE}^{LM05}: dotted line; $I_{AE}^{BB84} = I_{BE}^{BB84}$: dashed line. The security thresholds are reported at the top of the frame.

accidentally guesses the correct final result. This argument, together with the previous one, implies the following relations for the IR:

$$\begin{aligned} &q_1 = 0.25, \\ &Q_{AE} = 0 \Rightarrow I_{AE} = 1, \\ &Q_{BE} = 0.25 \Rightarrow I_{BE} = 1 - H(Q_{BE}) \simeq 0.19. \end{aligned} \tag{4}$$

In the above equations Q_{AE} and Q_{BE} are defined in a way similar to Q_{AB}. For example Q_{AE} can be thought as the QBER that Alice and Eve would find if they compare their classical strings which are composed, respectively, by all the encodings transmitted to Bob and by all the data acquired by Eve by means of the IR. Recall that the above equations are connected with the direct (DR) and reverse (RR) reconciliation of the LM05 and provide the direct and reverse secrecy capacity of the protocol. The situation described by Eq. (4) can be compared with that of BB84, where for $q_1 = 0.25$ the information acquired by Eve is $I_{AE} = I_{BE} = 1/2$ [3].

Of course Eve can decide to effect or not to effect IR in a certain run. In other terms she can effect IR only on a fraction $\xi \in [0, 1]$ of the runs. This modifies Eqs. (4) into the new ones:

$$\begin{aligned} &q_1 = 0.25\xi, \\ &I_{AE} = \xi, \\ &I_{BE} \simeq 0.19\xi. \end{aligned} \tag{5}$$

As said above, the mutual information between Alice and Bob is a simple function of the QBER Q_{AB}, which is measured by the users by sacrificing a part of the data collected during the EM. It is straightforward to realize that for IR the two QBERs of the LM05 are equal:

$$Q_{AB} = q_1. \tag{6}$$

Eq. (6) defines a first relation between the two QBERs measured in the LM05 protocol. Although this relation is not general, it deserves attention for it describes quite accurately the noise model pertaining to an experimental fiber-based setup like the one in Ref. [35], where the phase-drift noise arising in the optical fiber can be compensated both at the end of the forward channel and at the end of the backward channel through the passive Plug-and-Play auto-compensation technique [54–57].

Hence, we will use again the noise model of Eq. (6) to settle a homogeneous comparison between the various attacks put forward by Eve against the LM05 protocol. Of course, other models of noise are possible (see e.g. Ref. [34]).

In Fig. 2 we summarize what obtained thus far with the curves pertaining to the mutual information between Alice, Bob and Eve in LM05. In the same figure we also plot the curve pertaining to the analogous IR attack against BB84 (Section VI.D of [3]), for which $I_{AE} = I_{BE}$.

It can be seen that the curve I_{AE} in LM05 is always above the curve of BB84, while the curve I_{BE} is always below it. This, according to the CK theorem, Eq. (2), implies that the reverse (direct) secrecy capacity of LM05 is always higher (lower) than that of BB84 for the IR attack. The security thresholds obtained from the CK theorem against the IR attack for LM05 in DR and RR and for BB84, in the noise model of Eq. (6), are given by the intersection points of the plotted curves, and are explicitly written below:

$$LM05^{DR} : \text{secure against IR if } q_1 < 11.9\%$$

$$LM05^{RR} : \text{secure against IR if } q_1 < 25.0\%$$

$$BB84 : \text{secure against IR if } q_1 < 17.1\%$$

Note that the BB84 security threshold of 17.1% is higher than the one pertaining to the optimal individual eavesdropping [60] which amounts to 14.6%. In fact the simple-minded IR attack just described is not optimal either for BB84 or for LM05. However they have been used in [58] and later in [35] to provide direct measurable quantities easily applicable in the experimental situation.

3.2. Non-orthogonal attack – NORT

The IR analyzed above can give Eve an information linearly varying with the QBER q_1, as synthesized by Eqs. (5) and Fig. 2. It is possible for Eve to increase her information as a function of q_1 by performing non-orthogonal measurements [3] on both the forward and the backward paths. This strategy has been initially described in [32] by considering the mutual information as function of the "detection probability". Now we use the same approach but in terms of QBER.

Given the four states prepared by Bob, and Eve's ancillary states $|\varepsilon\rangle$, we can write the most general operation Eve can do on traveling qubit at point E_1 of Fig. 1 as:

$$\begin{aligned}
&|0\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle = \sqrt{F}|0\rangle|\widetilde{\varepsilon}_{00}\rangle + \sqrt{D}|1\rangle|\widetilde{\varepsilon}_{01}\rangle,\\
&|1\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle = \sqrt{D}|0\rangle|\widetilde{\varepsilon}_{10}\rangle + \sqrt{F}|1\rangle|\widetilde{\varepsilon}_{11}\rangle,\\
&|+\rangle|\varepsilon\rangle \to \frac{1}{\sqrt{2}}\big[|0\rangle\big(|\varepsilon_{00}\rangle + |\varepsilon_{10}\rangle\big) + |1\rangle\big(|\varepsilon_{01}\rangle + |\varepsilon_{11}\rangle\big)\big] \equiv |+\rangle|\varepsilon_{++}\rangle + |-\rangle|\varepsilon_{+-}\rangle,\\
&|-\rangle|\varepsilon\rangle \to \frac{1}{\sqrt{2}}\big[|0\rangle\big(|\varepsilon_{00}\rangle - |\varepsilon_{10}\rangle\big) + |1\rangle\big(|\varepsilon_{01}\rangle - |\varepsilon_{11}\rangle\big)\big] \equiv |+\rangle|\varepsilon_{-+}\rangle + |-\rangle|\varepsilon_{--}\rangle,
\end{aligned} \tag{7}$$

where the states $|\varepsilon_{ij}\rangle$ belong to the four-dimensional Hilbert space of Eve's probe. Ancillary states with tilde are intended to be normalized. The following conditions make transformations (7) unitary:

$$\langle\varepsilon_{00}|\varepsilon_{00}\rangle + \langle\varepsilon_{01}|\varepsilon_{01}\rangle \equiv F + D = 1, \tag{8}$$

$$\langle\varepsilon_{10}|\varepsilon_{10}\rangle + \langle\varepsilon_{11}|\varepsilon_{11}\rangle \equiv D + F = 1, \tag{9}$$

$$\langle\varepsilon_{00}|\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0. \tag{10}$$

Within condition (10) we can set $\langle\varepsilon_{00}|\varepsilon_{10}\rangle = \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0$ if we assume that the attack brought about by Eve is symmetric [3]. A symmetric attack is obtained when the disturbance introduced by Eve results to be the same in the two bases measured by the users. Alice and Bob can test the occurrence of a symmetric attack by measuring the noise levels in the two bases separately and verifying that they are equal. Intuitively, a symmetric attack corresponds to the symmetric structure of the states prepared by the transmitter, both in the LM05 and in the BB84 protocol. In fact, for the BB84, it has been shown to be optimal (see Section VI.E of [3]). Our results are then limited to this class of individual symmetric attacks. We specify the angles between non-orthogonal vectors as:

$$\langle\widetilde{\varepsilon}_{00}|\widetilde{\varepsilon}_{11}\rangle = \cos x, \qquad \langle\widetilde{\varepsilon}_{01}|\widetilde{\varepsilon}_{10}\rangle = \cos y, \tag{11}$$

with $0 \le x, y \le \pi/2$. In this sense the present strategy represents a non-orthogonal attack. Here, we do not fix values of the parameters we introduced.

At point E_2 of Fig. 1 Eve performs an attack similar to that at point E_1, but with fresh ancillae $|\eta\rangle$ (hence new parameters F' and D' are in order), to gain information about Alice's encoding:

$$\begin{aligned}
&|0\rangle|\eta\rangle \to \sqrt{F'}|0\rangle|\widetilde{\eta}_{00}\rangle + \sqrt{D'}|1\rangle|\widetilde{\eta}_{01}\rangle,\\
&|1\rangle|\eta\rangle \to \sqrt{D'}|0\rangle|\widetilde{\eta}_{10}\rangle + \sqrt{F'}|1\rangle|\widetilde{\eta}_{11}\rangle,\\
&|+\rangle|\eta\rangle \to |+\rangle|\eta_{++}\rangle + |-\rangle|\eta_{+-}\rangle,\\
&|-\rangle|\eta\rangle \to |+\rangle|\eta_{-+}\rangle + |-\rangle|\eta_{--}\rangle.
\end{aligned} \tag{12}$$

At the end of the transmission Eve will measure ε and η ancillae and she will gain information. Our next task is to recover the optimal eavesdropping strategy by Eve, i.e. determine parameters' values that maximize Alice–Eve and Bob–Eve mutual information (I_{AE}, I_{BE}) minimizing the QBERs q_1 and Q_{AB}.

From transformations (7) and conditions (8)–(10) we can easily evaluate q_1 for each basis prepared by Bob:

$$q_1(\hat{Z}) = \langle \varepsilon_{01}|\varepsilon_{01}\rangle = \langle \varepsilon_{10}|\varepsilon_{10}\rangle = D, \tag{13}$$

$$\begin{aligned} q_1(\hat{X}) &= \langle \varepsilon_{+-}|\varepsilon_{+-}\rangle = \langle \varepsilon_{-+}|\varepsilon_{-+}\rangle \\ &= [1 - F\cos x - D\cos y]/2. \end{aligned} \tag{14}$$

A good choice for Eve to minimize the QBER q_1 is to align her measuring apparatus with $\hat{Z}$ and $\hat{X}$ at random. If she aligns along $\hat{Z}$ then $q_1(\hat{Z}) = D = 0$, otherwise it will be $q_1(\hat{X})$ to be zero. On average, after setting $D = 0$ (and so $F = 1$), we will have:

$$q_1^{av} = \frac{1 - \cos x}{4}, \tag{15}$$

and Eqs. (7) become:

$$\begin{aligned} &|0\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{00}\rangle, \\ &|1\rangle|\varepsilon\rangle \to |1\rangle|\varepsilon_{11}\rangle, \\ &|+\rangle|\varepsilon\rangle \to \frac{1}{\sqrt{2}}\big(|0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{11}\rangle\big), \\ &|-\rangle|\varepsilon\rangle \to \frac{1}{\sqrt{2}}\big(|0\rangle|\varepsilon_{00}\rangle - |1\rangle|\varepsilon_{11}\rangle\big). \end{aligned} \tag{16}$$

From the above equations it is clear that the only relevant parameter is x: if it is zero then Eve's ancillae are parallel and do not provide any information to her, nor do they cause any error on the channel since any evolved state remains equal to the initial one. On the contrary, if $x = \pi/2$ Eve's ancillae are maximally informative to Eve, but maximum is also the noise created on the channel, according to Eq. (15). Similar arguments hold for the backward path, after E_2-attack, with primed parameters replacing not-primed ones.

In order to evaluate the mutual information I_{AE} let us write Bob's initial states as:

$$|\Psi\rangle = \sum_{\alpha=0,1} c_\alpha |\alpha\rangle, \tag{17}$$

where we made the following ansatze correspondingly to the initial states:

$$\begin{aligned} &|0\rangle \to c_\alpha = \delta_{\alpha,0}, \\ &|1\rangle \to c_\alpha = \delta_{\alpha,1}, \\ &|+\rangle \to c_\alpha = \frac{1}{\sqrt{2}}, \\ &|-\rangle \to c_\alpha = (-1)^\alpha \frac{1}{\sqrt{2}}. \end{aligned} \tag{18}$$

Then we can rewrite transformations (7) as

$$|\Psi\rangle|\varepsilon\rangle = \sum_{\alpha=0,1} c_\alpha |\alpha\rangle|\varepsilon\rangle \to \sum_\alpha c_\alpha \sum_\beta |\varepsilon_{\alpha\beta}\rangle|\beta\rangle, \tag{19}$$

and transformations (12) as

$$|\Psi\rangle|\eta\rangle = \sum_{\alpha=0,1} c_\alpha |\alpha\rangle|\eta\rangle \to \sum_\alpha c_\alpha \sum_\beta |\eta_{\alpha\beta}\rangle|\beta\rangle. \tag{20}$$

Now suppose that Alice performs the identity $\hat{I}$ between the two Eve's attacks. The following sequence describes the state transformations:

$$\begin{aligned} |\Psi\rangle|\varepsilon\rangle|\eta\rangle &\xrightarrow{E_1} \sum_\alpha c_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \\ &\xrightarrow{I} \sum_\alpha c_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \\ &\xrightarrow{E_2} \sum_\alpha c_\alpha \sum_{\beta,\gamma} |\gamma\rangle|\varepsilon_{\alpha\beta}\rangle|\eta_{\beta\gamma}\rangle. \end{aligned} \tag{21}$$

The ancillary states involved in this operation are:

$$\begin{aligned}
&|\varepsilon_{00},\eta_{00}\rangle, \quad |\varepsilon_{00},\eta_{01}\rangle, \quad |\varepsilon_{01},\eta_{10}\rangle, \quad |\varepsilon_{01},\eta_{11}\rangle,\\
&|\varepsilon_{10},\eta_{00}\rangle, \quad |\varepsilon_{10},\eta_{01}\rangle, \quad |\varepsilon_{11},\eta_{10}\rangle, \quad |\varepsilon_{11},\eta_{11}\rangle.
\end{aligned} \tag{22}$$

If, instead of the identity $\hat{I}$, Alice performs the $i\hat{Y}$ operation we have:

$$\begin{aligned}
|\Psi\rangle|\varepsilon\rangle|\eta\rangle &\xrightarrow{E_1} \sum_\alpha c_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle\\
&\xrightarrow{iY} \sum_\alpha c_\alpha \sum_\beta (-1)^{\beta+1}|\beta\oplus 1\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle\\
&\xrightarrow{E_2} \sum_\alpha c_\alpha \sum_{\beta,\gamma} (-1)^{\beta+1}|\gamma\rangle|\varepsilon_{\alpha\beta}\rangle|\eta_{(\beta\oplus 1)\gamma}\rangle,
\end{aligned} \tag{23}$$

and the involved ancillary states are:

$$\begin{aligned}
&|\varepsilon_{00},\eta_{10}\rangle, \quad |\varepsilon_{00},\eta_{11}\rangle, \quad |\varepsilon_{01},\eta_{00}\rangle, \quad |\varepsilon_{01},\eta_{01}\rangle,\\
&|\varepsilon_{10},\eta_{10}\rangle, \quad |\varepsilon_{10},\eta_{11}\rangle, \quad |\varepsilon_{11},\eta_{00}\rangle, \quad |\varepsilon_{11},\eta_{01}\rangle.
\end{aligned} \tag{24}$$

In order to acquire information from states (21) and (23) Eve must measure both her ancillae. Keeping in mind orthogonality relations (10) and following, we see that the best way to do that is to distinguish orthogonal subspaces before, and then non-orthogonal states. The probability to make an error in distinguishing between two states with scalar product $\cos x$ is $(1-\sin x)/2$ [61]. Observing states (21) and (23) we can notice that if Eve mistakes to identify her first ancilla (ε states) then she guesses the wrong Alice's operation, since she flips from states (21) and (23) or viceversa. The same is true if she guesses right ε state but mistakes η state. Nevertheless, if she mistakes twice, then with the first error she misinterprets (21) and (23) and with the second error she compensates the first one, eventually guessing right Alice's operation. This leads to estimate the probability Eve wrongly guesses Alice's operation, i.e. the QBER Q_{AE} between Alice and Eve, and from it, considering $F=F'=1$, we find the following expression for I_{AE}:

$$I_{AE} = \left\{1 - H\left[\left(\frac{1+\sin x}{2}\right)\left(\frac{1+\sin x'}{2}\right) + \left(\frac{1-\sin x}{2}\right)\left(\frac{1-\sin x'}{2}\right)\right]\right\}. \tag{25}$$

Then, to upper bound Eve's information without affecting q_1, we can simply use orthogonal ancillae on the backward path, that means to set $x'=\pi/2$. In this case we obtain:

$$I_{AE} = 1 - H\left(\frac{1-\sin x}{2}\right). \tag{26}$$

The last question concerns the mutual information between Bob and Eve. This is limited by the fact that Bob does not reveal any basis in LM05. So if Eve guesses the right basis in transformations (7) (probability equal to 1/2) then she has a probability of error equal to her capability to discriminate her ancillae, given then by $(1-\sin x)/2$. Otherwise, with probability 1/2, she guesses the wrong basis and she has a probability of 1/2 to be wrong with the qubit also. In the whole:

$$Q_{BE} = \frac{2-\sin x}{4}. \tag{27}$$

The security of the protocol now depends on the relation between Q_{AB} and q_1. For the purpose of comparison we assume here the same model as per Eq. (6), obtained for IR attacks: $Q_{AB}=q_1$. This is reasonable as the present strategy is a generalization of IR to nonorthogonal Eve's ancillae. With such an assumption it is possible to draw the curves in Fig. 3.

The increased information acquired by Eve using NORT rather than IR is apparent. The security threshold for BB84 is now 14.6%, equal to the one obtained in [60] for the optimal single-particle eavesdropping. On the contrary, the thresholds for LM05 are 10.0% and 25.0% for DR and RR respectively. Hence LM05 used in RR is more tolerant to noise than BB84, provided that Eve's action is limited to a NORT attack.

3.3. Double CNOT attack – DCNOT

So far we have analyzed attacks in which Eve measures the qubit coming out from Bob's station. As we have seen this kind of attack can provide Eve with a high mutual information with Alice. However the mutual information between Eve and Bob is poor, as illustrated by Figs. 2 and 3. The reason is that Eve's initial measurement modifies the state prepared by Bob, and prevents her from knowing the outcome of Bob's final measurement. It is then natural to ask whether is possible for Eve to perform her attack without altering Bob's state, thus maximizing her mutual information with Bob. This attack exists and has been introduced for the first time in [49]. It is composed by a sequence of two CNOT gates from Eve, one for

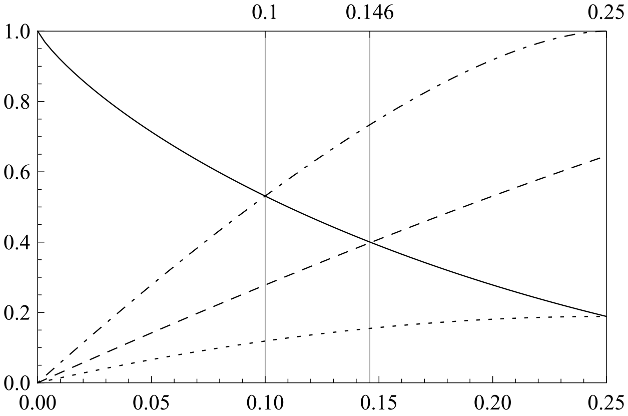

Fig. 3. Mutual information vs q_1 in NORT attack. The curves are: I_{AE}^{LM05} (dot–dashed line), I_{BE}^{LM05} (dotted line), $I_{AE}^{BB84} = I_{BE}^{BB84}$ (dashed line). The security thresholds are reported at the top of the frame.

each path of the LM05; hence we call it *Double CNOT* attack, in short "DCNOT". We will show that DCNOT can make I_{BE}, distilled in the RR modality, equal to its maximum and to I_{AE}, thus reducing the LM05 security to the security obtained in the DR modality.

Let us study the evolution of the states prepared by Bob under the action of the first CNOT gate by Eve. Eve appends an ancilla in the state $|0\rangle_e$ to the initial states prepared by Bob; then she performs a first CNOT gate before Alice's station using the traveling qubit as control and her ancilla as target. The states become:

$$\begin{aligned}
&|0\rangle|0\rangle_e \to |0\rangle|0\rangle_e, \\
&|1\rangle|0\rangle_e \to |1\rangle|1\rangle_e, \\
&|+\rangle|0\rangle_e \to \frac{|0\rangle|0\rangle_e + |1\rangle|1\rangle_e}{\sqrt{2}}, \\
&|-\rangle|0\rangle_e \to \frac{|0\rangle|0\rangle_e - |1\rangle|1\rangle_e}{\sqrt{2}}.
\end{aligned} \tag{28}$$

We can notice that when Bob prepares states in the basis $\hat{X}$ the CNOT gate creates an entangled state with the traveling qubit and Eve's ancilla. After that Eve forwards the control qubit to Alice, who performs her encoding $\hat{A}_i$ ($\hat{A}_0 = \hat{I}$ and $\hat{A}_1 = i\hat{Y}$) on it and then sends it back to Bob. Eve, on the backward path, executes a second CNOT gate on the whole system. We report Alice's and Eve's actions as:

$$\begin{aligned}
&\big(\hat{A}_i|0\rangle\big)|0\rangle_e \to \big(\hat{A}_i|0\rangle\big)|i\rangle_e, \\
&\big(\hat{A}_i|1\rangle\big)|1\rangle_e \to \big(\hat{A}_i|1\rangle\big)|i\rangle_e, \\
&\frac{(\hat{A}_i|0\rangle)|0\rangle_e + (\hat{A}_i|1\rangle)|1\rangle_e}{\sqrt{2}} \to \big(\hat{A}_i|+\rangle\big)|i\rangle_e, \\
&\frac{(\hat{A}_i|0\rangle)|0\rangle_e - (\hat{A}_i|1\rangle)|1\rangle_e}{\sqrt{2}} \to -\big(\hat{A}_i|-\rangle\big)|i\rangle_e.
\end{aligned} \tag{29}$$

From these equations we can recognize that the entanglement created by Eve in the first CNOT gate disappears with the second CNOT. Furthermore, Eve's ancillae take exactly the information encoded by Alice; hence it is sufficient for Eve to measure them in the basis $\hat{Z}$ to find out Alice's encoding: $|0\rangle_e$ indicates that Alice performed the identity, while $|1\rangle_e$ indicates the spin-flip operation. Finally, after the second CNOT the state arriving to Bob is just the right state he expected to receive! This entails two consequences:

i) in the DCNOT $Q_{AB} = 0$. If Alice and Bob use only Q_{AB} as a security parameter, they will never detect this kind of attack by Eve. However, for the same reason, the mutual information between Alice and Bob, which is a function of Q_{AB}, is always equal to 1.

ii) Eve acquires full information about both Alice (I_{AE}) and Bob (I_{BE}). In fact she knows perfectly the encoded transformation and the result that is going to be obtained by Bob.

The DCNOT attack can be detected in CM. If the qubit is prepared in the basis $\hat{Z}$ Eve does not perturb the state at all while if it was prepared in the basis $\hat{X}$ the QBER q_1 is equal to 1/2. Hence the overall QBERs and information situation for this attack is:

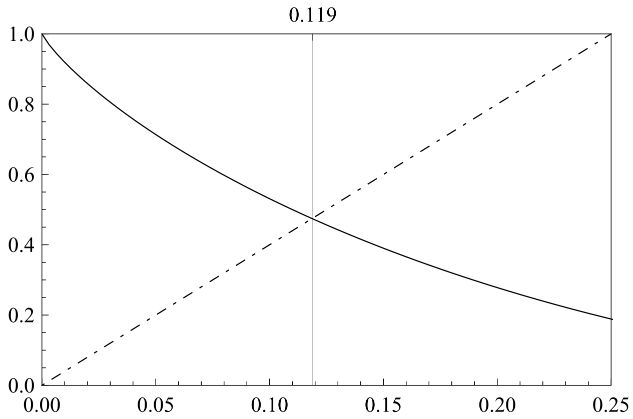

Fig. 4. Mutual information I_{AB} (solid line) and $I_{AE}^{LM05} = I_{BE}^{LM05}$ (dot–dashed line) versus q_1 in the DCNOT attack against LM05. The security threshold is reported at the top of the frame.

$$q_1 = 0.25, \tag{30}$$

$$Q_{AB} = 0 \Rightarrow I_{AB} = 1, \tag{31}$$

$$I_{AE} = I_{BE} = 1. \tag{32}$$

These equations are quite similar to Eqs. (5) obtained for the IR attack, with the important difference that Q_{AB} is now zero and, by consequence, I_{AB} is always equal to 1, as per Eq. (32). Hence, by making use of the CK theorem, Eq. (2), we can conclude that the LM05 provides a secure rate against DCNOT over the whole interval of q_1.

Likewise IR, if Eve performs the DCNOT in a partial way, her information will be a linear function of the QBER q_1; then the corresponding curve would be exactly the same as the one depicting I_{AE}^{LM05} in Fig. 2. We report such a curve in Fig. 4.

An important modification to the DCNOT is the following. Eve executes a random flip/no-flip unitary operation, analogous to the one effected by Alice, after the second CNOT, on the backward path. In this way Eve increases Q_{AB}, from its minimum value 0 to any desired value χ and decreases the mutual information between Alice and Bob from its maximum value 1 to any other value imposed by her. Furthermore, with this kind of modified DCNOT attack, which we term DCNOT*, Eve still maintains the control about Bob's final measurement outcome, as in the non-modified DCNOT. The situation for the DCNOT* attack is then summarized by the following equations:

$$\begin{aligned} &q_1 = 0.25\xi, \\ &Q_{AB} = \chi \Rightarrow I_{AB} = 1 - H(\chi), \\ &I_{AE} = I_{BE} = \xi, \end{aligned} \tag{33}$$

with $\chi \in [0, 0.5]$ a parameter controlled by Eve and ξ the fraction of attacked qubits, as already defined for IR attacks. We can again assume the noise model of Eq. (6) to compare this new attack with the previous ones, i.e. $Q_{AB} = q_1$. The corresponding curves are plotted in Fig. 4.

The LM05 protocol results secure, both in DR and in RR, if $q_1 < 11.9\%$. Hence, by comparing with Figs. 2 and 3, it is seen that this attack is less dangerous than NORT as far as I_{AE} is concerned, but is far more dangerous for what concerns the security threshold pertaining to I_{BE}, which decreases from 25.0% to 11.9%.

3.4. Generic individual attack

In this section we provide an upper bound to Eve's information in case of single-particle attack. We adapt to LM05 an argument recently introduced in [25], which in turn is based on the main argument of [5] limited to the case of an individual attack. We remark that such a proof holds when LM05 is used for QKD, not for a deterministic Direct Communication [21]. We also stress that the proof given in [25] and repeated here for LM05 does not represent a security proof against the most general attack by Eve, i.e. a coherent attack of a two-way deterministic protocol. In fact, the argument does not include any multi-particle distillation of quantum states performed by the users, nor multi-particle attacks by Eve [62].

As a first step of the generic individual attack by Eve suppose that the users are provided by Eve with a state which is claimed to be a perfect singlet:

$$|\psi_{AB}\rangle = \big(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\big)/\sqrt{2}, \tag{34}$$

where the states $|0\rangle$ and $|1\rangle$ are the eigenstates of the basis Z, the computational basis. If the state (34) was a truly singlet, the users would perform LM05 as follows. Bob measures his particle in one of the two bases Z or X chosen at random, thus preparing Alice's particle's state in a state orthogonal to his state. In EM, Alice performs on her particle the desired operation $\hat{I}$ or iY, exactly as she would do in the standard prepare-and-measure LM05. All the same, in CM, Alice measures her particle in a basis randomly chosen between Z or X. This reduces the entanglement-based LM05 to a prepare-and-measure protocol. Once the security is shown for the former it is automatically true for the latter.

The next task is for the users to verify that they actually have been given by Eve the claimed state. In practice they must verify that the fidelity $F(|\psi_{AB}\rangle, \rho_{AB})$ between the claimed state and the state ρ_{AB} in their hands is very close to 1. Hence consider a tripartite state $|\Phi\rangle_{ABE}$ which is a purification of ρ_{AB} and which is in Eve's hands:

$$\rho_{AB} = tr_E\big(|\Phi\rangle_{ABE}\langle\Phi|\big) \tag{35}$$

$$\rho_E = tr_{AB}\big(|\Phi\rangle_{ABE}\langle\Phi|\big). \tag{36}$$

Then $S(\rho_{AB}) = S(\rho_E)$, where S is the Von Neumann entropy [50], because $|\Phi\rangle_{ABE}$ is pure and then ρ_{AB} and ρ_E have the same spectrum. Hence Alice and Bob can calculate Eve's maximum information from the relation $S(\rho_{AB}) = S(\rho_E)$ provided they can estimate $S(\rho_{AB})$. To this aim the users perform the CM. In particular they measure the QBER q_1 which is equal to the *infidelity* δ of Ref. [5], which is defined by the relation

$$F\big(|\psi_{AB}\rangle, \rho_{AB}\big)^2 \geq 1 - \delta. \tag{37}$$

As a result, if q_1 is not too large, the state ρ_{AB} is acknowledged to be very similar to $|\psi_{AB}\rangle$ by the users. In particular, since they verify that $F(|\psi_{AB}\rangle, \rho_{AB})^2 \geq 1 - q_1$ then from the Lemma "High fidelity implies low entropy" of Ref. [5] one has:

$$S(\rho_{AB}) = S(\rho_E) \leq -(1 - q_1)\log_2(1 - q_1) - q_1 \log_2\left(\frac{q_1}{3}\right). \tag{38}$$

This represents an upper bound to Eve's absolute information at the end of the forward path, in full analogy with what happens in the BB84 protocol. What we need now is a connection with the backward path. Between the two paths, Alice encodes information on her particle. So let us make a step back and focus on the mutual information between Alice and Eve, I_{AE}.

It is known that the *Holevo information* is an upper bound to the mutual information [50]:

$$I_{AE} \leq \chi(\rho_{AE}), \tag{39}$$

with $\rho_{AE} = tr_B(|\Phi\rangle_{ABE}\langle\Phi|)$ and $\chi(\rho) = S(\rho) - \sum_k S(\rho_k)$. Furthermore the following relations trivially hold:

$$\chi(\rho_{AE}) \leq S(\rho_{AE}) \leq S(\rho_E), \tag{40}$$

with $\rho_E = tr_A(\rho_{AE})$. The last equation is an intuitive corollary to the Holevo theorem cited as "Lemma 2" in Ref. [5]. So, it turns out that the upper bound $S(\rho_E)$ available to Alice and Bob is an upper bound both to the mutual information I_{AE} and to the Holevo quantity $\chi(\rho_{AE})$. As stated in Ref. [25] the Holevo quantity does not increase under quantum operations. In particular Alice's encoding operations cannot increase $\chi(\rho_{AE})$. By consequence one has:

$$\chi(\rho_{AE})^{\text{after}} \leq \chi(\rho_{AE})^{\text{before}} \leq S(\rho_E) \tag{41}$$

where the labels "before" and "after" refer to Alice's encoding. So $S(\rho_E)$ represents a bound to Eve's information even after Alice's encoding.

To conclude the proof it suffices to note that even if Eve can increase $S(\rho_E)$ on the backward path, e.g. by attaching new ancillae to the traveling states, the increase in information does not concern Alice's encoding. So it would be the same for Eve if she increases her information since the beginning on the forward path; but in that case the users already have the bound of Eq. (41).

Now it is possible to use the CK theorem, Eq. (2), and the noise model of Eq. (6) to make a guess about how tight the given bound is. In this model the mutual information I_{AB} is given by $1 - H(q_1)$ while from Eq. (38) we get an upper bound to Eve's average information. The curves pertaining to the mutual information are plotted in Fig. 5. They are compatible with the previous results since the found threshold, $q_1 \leq 8.8\%$, is lower than all previous single-particle attacks, both in DR and in RR. Note however that the given bound is meaningful only for LM05 in DR since it is based on the Holevo information bound Eq. (41) which makes explicit reference to Alice's encoding and none to Bob's measurement. However although the security threshold pertaining to RR could be higher than that for DR, it cannot be too much different because we provided an explicit attack, the DCNOT*, which gives a security threshold of 11.9% for LM05 in RR, only 35% higher than the above threshold. Moreover, limiting the analysis to DR, it turns out that the security bound just given is quite tight. In fact, with the NORT attack we found a security threshold of 10.0%, which is only 13.6% higher than the given bound.

Finally let us note that the above bound holds trivially for BB84 as well, where Alice does not encode information on the received state. In this case however the bound is not tight as 8.8% is far smaller than the 14.6% pertaining to the optimal individual attack against BB84 [60].

Before moving to the next section and study the zero-QBER attacks, we summarize the results found for the zero-loss individual eavesdropping in Table 1.

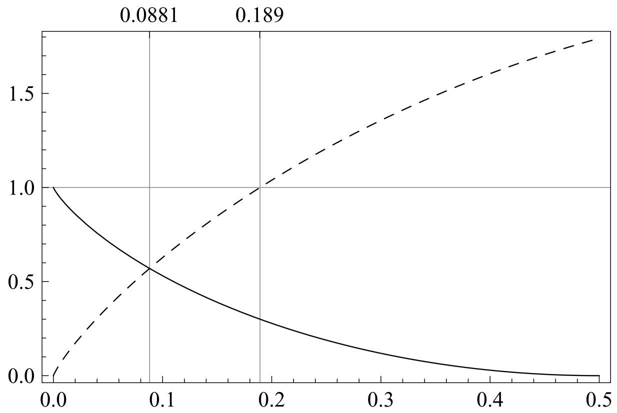

Fig. 5. General attack security for LM05 in DR. The security threshold amounts to $q_1 = 8.8\%$. For $q_1 > 18.9\%$ Eve gets full information about Alice's encoding.

Table 1
security thresholds for single-particle attacks against LM05 in DR, LM05 in RR and BB84.

Eve's strategy	LM05-DR (%)	LM05-RR (%)	BB84 (%)
IR	11.9	25.0	17.1
NORT	10.0	25.0	14.6
DCNOT*	11.9	11.9	–
Generic	8.8	–	8.8

4. Zero-QBER eavesdropping

We now consider attacks that introduce losses, but no noise. If Alice uses a perfect single-photon source the single photon can only be detected *either* by Eve *or* by Bob. However in practice Alice uses an approximated single-photon source i.e. an attenuated laser beam. For this source the number of photon per pulse follows a Poisson statistics. It is then possible that a single pulse contains more than one photon in the same quantum state, and that *both* Eve *and* Bob detect the same qubit. In this case Eve steals one bit of information without introducing any noise in Bob's measurement; however she introduces losses. Alice and Bob, from the knowledge of the loss rate, should be able to infer how much information has been stolen and remove it by means of Privacy Amplification [63,64]. It is worth noting that in the hypothesis of zero-QBER attacks the mutual information between Alice and Bob is always maximum and no Error Correction is needed to reconcile users' keys. Another obvious consequence of this assumption is that Eve does not acquire any further information from the Error Correction procedure. So her knowledge will derive entirely from her attack to the quantum channel.

4.1. Beam splitting attack – BS

In the Beam Splitting attack (BS) Eve uses a beam-splitter of transmissivity $T = 1 - R$ to deviate a fraction R of the main beam towards her detectors, which are supposed to be ideal (100% quantum efficiency, no dark counts). The approach for BS is very similar to the one adopted for the IR attack: we first evaluate the probability of success for Eve eavesdropping one bit of information; then we relate the photon emitted by the source to the eavesdropped bits via the Binomial distribution.

Let us first analyze the BB84 [58].

Define μ as the average number of photons contained in each pulse prepared by Alice. With her beam-splitter Eve splits a fraction $R\mu$ from the main beam towards her (ideal) detectors, so that the probability to successfully detect a photon is given by:

$$P = 1 - e^{-R\mu} \approx R\mu. \tag{42}$$

The above approximation holds when $\mu \ll 1$. Usually in the experiments on BB84 $\mu = 0.1$. It is reasonable to assume that $R \simeq 1$ because usually the attenuation rate measured by Alice and Bob is very close to the unity at wavelength of 1550 nm. Hence Eve's probability to successfully detect a photon is about μ. We also conservatively assume that Eve possesses a perfect quantum memory to store the bits until the moment in which the basis is revealed by Alice and Bob, so that every stored photon is detected by Eve in the right basis. This means that μ represents the average information collected by Eve against BB84 through the BS attack in the asymptotic limit of a large number N of pulses traveling on the channel:

$$I_E^{BB84} = \mu. \tag{43}$$

This expression can be used to provide a secure gain similar to that obtained for IR attack. Specifically the secure gain G^{BB84} is:

$$G^{BB84} = G^{BB84}_{raw} \times \left(1 - I^{BB84}_{E}\right), \tag{44}$$

where:

$$G^{BB84}_{raw} = 1 - \exp\left[-\mu \times \eta_d \times \Gamma^{BB84}(L)\right], \tag{45}$$

$$\Gamma^{BB84}(L) = \Gamma_{QC}(L) \times \Gamma_B \quad \text{(total transmission)}, \tag{46}$$

$$\Gamma_{QC}(L) = 10^{-0.02 \times L} \quad \text{(transmission of the quantum channel)}, \tag{47}$$

with parameters $\eta_d = 0.12$ (efficiency of Bob's detectors), $\Gamma_B = 0.4$ (transmission of Bob's box), and μ is optimized for every distance L in order to give the maximum secure gain.

In analogy with BB84 one can calculate the amount of Privacy Amplification [63,64] necessary to cope with BS in LM05. Being LM05 a two-way protocol the BS must be accomplished using two beam-splitters rather than one, positioned in the two paths of the communication channel. In this way it may happen that Eve measures two photons, one from the forward path and one from the backward one; then, by comparing her outcomes, Eve can ascertain the encoded information. Let R_1 and R_2 be the reflectivity of the two beam-splitters. After the first beam-splitter Eve has a probability of successful detection

$$P_1 = 1 - e^{-R_1\mu}. \tag{48}$$

The fraction of the beam transmitted through the first beam-splitter is $T_1\mu = (1 - R_1)\mu$. Then the fraction of the beam deviated by the second beam-splitter is $R_2(1 - R_1)\mu$, and Eve's probability to detect a photon in the second path is:

$$P_2 = 1 - e^{-R_2(1-R_1)\mu}. \tag{49}$$

A successful eavesdropping is given by two successful detection events in the same run:

$$P_{BS_{12}} = P_1 \cdot P_2 = \left(1 - e^{-R_1\mu}\right)\left(1 - e^{-R_2(1-R_1)\mu}\right). \tag{50}$$

From this expression it is straightforward to check that the value of $R_1 = 1/2$ maximizes $P_{BS_{12}}$ for any μ. An intuitive way to understand this is to take $R_2 \simeq 1$, to let Eve read as much information as possible from the backward path, and to realize that in this case Eve's best choice is to analyze half of the beam from the forward path and half from the backward one, i.e. to set $R_1 = 1/2$. Inserting these values into Eq. (50) we have:

$$P_{BS_{12}} \leq \left(1 - e^{-\mu/2}\right)^2 \equiv P^* = 1 - 2e^{-\mu/2} + e^{-\mu}, \tag{51}$$

which represents the average information acquired by Eve through the BS attack against the LM05 protocol, both in DR and RR, in the asymptotic limit of an infinite number of pulses traveling on the two-way quantum channel [35]:

$$I^{LM05}_{E} = P^*. \tag{52}$$

This expression can be used to provide a secure gain similar to that previously obtained for BB84. Specifically the secure gain G^{LM05} is:

$$G^{LM05} = G^{LM05}_{raw} \times \left(1 - I^{LM05}_{E}\right), \tag{53}$$

where:

$$G^{LM05}_{raw} = 1 - \exp\left[-\mu \times \eta_d \times \Gamma^{LM05}(L)\right], \tag{54}$$

$$\Gamma^{LM05}(L) = \Gamma^2_{QC}(L) \times \Gamma_B \times \Gamma^2_A \quad \text{(total transmission)}, \tag{55}$$

$$\Gamma_{QC}(L) = 10^{-0.02 \times L} \quad \text{(transmission of the quantum channel)}, \tag{56}$$

with parameters $\eta_d = 0.12$ (efficiency of Bob's detectors), $\Gamma_B = 0.4$ (transmission of Bob's box), $\Gamma_A = 0.45$ (transmission of Alice's box) and μ is optimized for every distance L. Note that the crucial equation is that defining $\Gamma^{LM05}(L)$ which, with respect to BB84, contains the square of $\Gamma_{QC}(L)$, because the channel is two-way, and the term Γ^2_A, which represents the double-transmission of Alice's setup because the photon passes twice in it before going back to Bob. The values of the parameters reported after Eq. (56) are similar to those experimentally measured in Ref. [35].

In Fig. 6 we plot $\log_{10} G^{BB84}$ and $\log_{10} G^{LM05}$. It can be noted that the secure rate pertaining to LM05 is far smaller than that pertaining to BB84. This crucially depends on the higher loss-rate of the two-way channel of LM05.

However in the next section we show that the difference between the two protocols in the frame of zero-QBER attacks can be dramatically reduced when the Photon-Number Splitting (PNS) attack by Eve is considered. This is due to the higher resistance offered by LM05 against this kind of attacks.

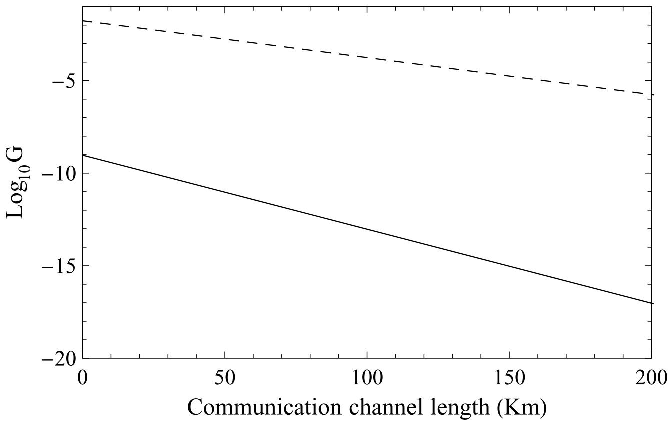

Fig. 6. Plot of the secure gain of BB84 (G^{BB84}, Eq. (44), dashed line) and LM05 (G^{LM05}, Eq. (53), solid line) versus the length of the communication channel, in case of BS attack by Eve. The BB84 is superior to LM05 for all the distances. This is due to the double loss-rate of the two-way LM05 protocol.

4.2. Photon-number splitting attack – PNS

In the following we describe the Photon-Number Splitting (PNS) attack [65,66,15,67,68] against the present version of the LM05 protocol. This attack has been previously described in [52] for the original LM05 protocol. The removal of the test on the backward channel does not present any major subtleties: it is simply replaced by the test of the QBER Q_{AB}, which obliges Eve to perform an attack on at least three photons (see the following explanation) to not introduce any disturbance on the channel.

As mentioned in the previous Section 4.1, when the photon source is a laser attenuated with an average photon number per pulse μ, the probability to have n photons in a single pulse is given by a Poisson distribution:

$$P_n(\mu) = \frac{\mu^n}{n!}e^{-\mu}. \tag{57}$$

This means that with a probability $P_n(\mu)$ Bob prepares the state $|\psi\rangle^{\otimes n}$ rather than the desired state $|\psi\rangle$ (ψ indicates one of the four states prepared by Bob in BB84 and LM05). This accidental redundancy can be exploited by Eve to perform a perfect zero-QBER attack.

It is known [69] that when $n = 3$ it exists a measurement $\mathcal{M}$ that provides a conclusive result about the absolute polarization ψ with (optimal) probability 1/2. Eve can exploit this fact to eavesdrop on LM05 protocol in the following way. She performs a quantum nondemolition measurement (QND) on the pulses as soon as they exit Bob's station; this can be done without perturbing the state ψ: when she finds $n < 3$ she blocks the pulses; on the pulses with at least three photons she executes $\mathcal{M}$ and if the outcome is not conclusive she blocks these pulses as well; when $n \geq 3$ and the outcome of $\mathcal{M}$ is conclusive she prepares a new photon in the right state ψ and forwards it to Alice. Until here this attack is completely analogous to the 'IRUD-attack' described in [69]. The only variant is that Eve measures again the photon on the backward path after Alice's encoding, to capture the information. Since Eve did know the state entering Alice's box she can extract the information without perturbing the state. After that she forwards the photon in the correct state to Bob. We call this first PNS attack $\mathrm{PNS}_{\mathcal{M}}$.

A second attack is more peculiar to LM05. Suppose that $n = 2$ and call the two photons in the pulse p_1 and p_2. As before Eve can know the number of photons per pulse through a QND measure. When $n < 2$ Eve blocks the pulses. When $n = 2$ she stores p_1 and forwards p_2 to Alice; this let her remain undetected during a possible CM on the forward path. On the way back Eve captures again p_2. To gain Alice's information she must decide whether the polarizations of p_1 and p_2 are parallel or antiparallel: in the first case she would deduce the logical value '0'; in the second case she would deduce '1'. However, the discrimination between parallel and antiparallel spins is not as simple as it appears at a first glimpse: while the parallel-spin-state $|P\rangle = |\psi\rangle_{p_1}|\psi\rangle_{p_2}$ is symmetric, the antiparallel-spin-state $|AP\rangle = |\psi\rangle_{p_1}|\psi^{\perp}\rangle_{p_2}$ is neither symmetric nor antisymmetric. Upon symmetrizing $|AP\rangle$ we can realize that it is not orthogonal to $|P\rangle$, and by consequence it is not perfectly distinguishable from it (we remand to [70,71] for a complete treatment of this problem). Actually an optimal measurement $\mathcal{M}'$ is a nonlocal one and gives Eve a conclusive result (between $|P\rangle$ and $|AP\rangle$) with a probability 1/4 [70]. Hence Eve can block all the "inconclusive" pulses to gain full information and still remain undetected. However it remains open the question of which photon must Eve forward to Bob: upon obtaining this result, Eve does not know whether to give Bob the state $|\psi\rangle$ or the state $|\psi^{\perp}\rangle$, because she ignores the absolute value of ψ prepared by Bob. This shows that two photons are not sufficient for a perfect eavesdropping with $\mathcal{M}'$. Yet the complete attack can be accomplished with an additional photon p_3: Eve should store p_3, execute $\mathcal{M}'$, and eventually encode p_3 according to the conclusive outcome of $\mathcal{M}'$; the photon prepared in this way can be forwarded to Bob without risk of detection.

The above analysis establishes that a perfect eavesdropping can be realized with at least three photons in a pulse. It also establishes that the measurement $\mathcal{M}$ represents a more powerful resource for Eve than $\mathcal{M}'$, for a number of reasons:

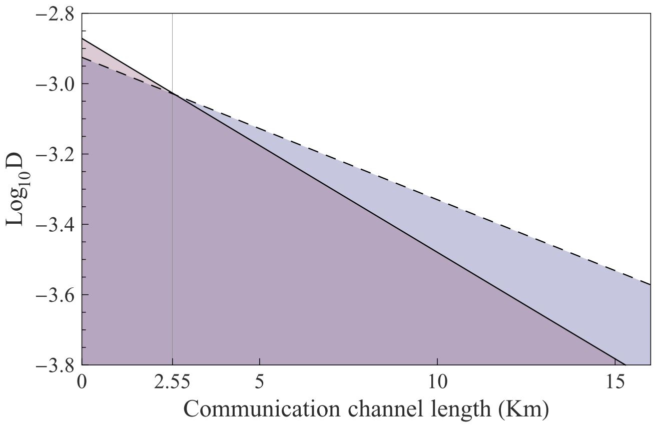

Fig. 7. Plot of the security regions of BB84 (D^{BB84}, Eq. (58), from the dashed line to the axis of abscissae) and LM05 (D^{LM05}, Eq. (59), from the solid line to the axis of abscissae) versus the length of the communication channel, in case of PNS attack by Eve. The BB84 is superior to LM05 for longer distances, but LM05 is superior on shorter distances. This is due to the higher resistance of LM05 to PNS-like attacks.

it gives information on the complete state ψ of the photons, not only on Alice's operation; the probability of conclusive results is 1/2 rather than 1/4; Eve knows about the conclusiveness of her measurement immediately, rather than after Alice's encoding, and can use this information to improve her strategy. For these reasons we only consider the robustness of LM05 against the PNS$_{\mathcal{M}}$ attack following [52].

In case of PNS attacks it was shown in [67] that a communication is secure until the signal sent by Alice arrives at Bob's with a probability higher than the probability to generate a multi-photon. In our present case the signal is the raw gain G_{raw}, previously introduced for BB84, Eq. (45), and LM05, Eq. (54), where we have neglected the contribution of the dark counts. Hence, for BB84, the transmission is secure when the following condition is fulfilled:

$$D^{BB84} = G_{raw}^{BB84} - P_{PNS}^{BB84} > 0, \tag{58}$$

with G_{raw}^{BB84} defined by Eq. (45) and

$$P_{PNS}^{BB84} = \sum_{i=2}^{\infty} e^{-\mu} \frac{\mu^i}{i!} = 1 - e^{-\mu}(1+\mu)$$

the probability that Alice accidentally emits 2 or more photons in a single pulse.

All the same, for the LM05 we have:

$$D^{LM05} = G_{raw}^{LM05} - P_{PNS}^{LM05} > 0, \tag{59}$$

with G_{raw}^{LM05} defined by Eq. (54) and

$$P_{PNS}^{LM05} = \left(\sum_{i=3}^{\infty} e^{-\mu} \frac{\mu^i}{i!}\right) - \frac{1}{2}\frac{\mu^3}{6} e^{-\mu} = 1 - e^{-\mu}\left(1 + \mu + \frac{\mu^2}{2} + \frac{1}{2}\frac{\mu^3}{6}\right)$$

the probability that Alice emits a number of photons dangerous for LM05, as discussed above.

Then we plot in Fig. 7 $\log_{10} D^{BB84}$ and $\log_{10} D^{LM05}$ and obtain a comparison of the security regions pertaining to BB84 and LM05. Differently from the BS attack, for the PNS attacks the BB84 is more performant than LM05 on longer distances, higher than 2.55 km with our parameters, but LM05 is more performant on shorter distances. Hence, while losses remain an important limiting factor for any two-way quantum communication, the higher protection from PNS attacks of the LM05 with respect to BB84 could enable an advantage in terms of the secure rate for small-range setups like the one in [72].

5. Conclusion

In the present work we have described and characterized a practical version of the two-way QKD protocol LM05 by considering the most relevant single-particle eavesdropping strategies against it.

The security of the scheme is guaranteed by two QBERs, q_1 and Q_{AB}, which are not trivially related one to each other. By assuming a noise model where $q_1 = Q_{AB}$ it turns out that the most powerful attack against LM05 in *direct reconciliation* is the NORT, which provides an upper bound to secure QKD equal to $q_1 = Q_{AB} = 10.0\%$, while the most powerful attack in *reverse reconciliation* is the DCNOT*, which provides a threshold of $q_1 = Q_{AB} = 11.9\%$. The adopted noise model is based on the experimental evidence that one-way and two-way channels can be controlled with the same level of precision. However other noise models can be considered as well, for instance one in which $q_1 = 15\%$ and $Q_{AB} = 0$. In this case, if Eve performs individual attacks only, it is not possible to distill a secure key with the BB84 protocol, while it is possible with the LM05. This in our opinion underlines the intrinsic difference between the two ways of performing QKD and encourages further research in this area. Moreover it is worth recalling that in the present version of LM05 we did not include a QBER test on the backward path of the communication channel; such an option, though not very practical, can improve the obtained secrecy capacities.

In the limited scenario of single-particle attacks, we have compared the two-way LM05 protocol with the standard BB84, which uses a one-way quantum channel. We have found that the main limitation of two-way QKD is the high loss-rate, even if it is partially counter-balanced by the higher resistance to PNS-like attacks. This entails that the field of application of two-way QKD shall be limited to short communication channels, like those typical of a QKD network, where the optimal average distance is about 17 km [73]. Even so a conclusive answer about the two modes of performing QKD can come only from a quantitative unconditional security proof for two-way QKD, which is still lacking at present. In this respect, it is our opinion that specific tools should be developed for this task, e.g. an entanglement-based description specific to two-way QKD. In fact, any argument too closely related to one-way QKD fails to capture all the peculiarities of two-way QKD, like the encoding on operators rather than on states and the reverse reconciliation of the key.

While we are aware that further studies are needed to make the LM05 protocol and two-way QKD in general viable for applications, we are also confident that the multi-way use of a quantum channel could play an important role in future developments of quantum cryptography.

Acknowledgements

Fruitful discussions with N. Lütkenhaus, G. Di Giuseppe and R. Kumar are acknowledged. This work has been partly supported by the European Commission under the Integrated Project “Qubit APplications” (QAP), Contract No. 015848, funded by the IST directorate and partly by those Italian citizens who assigned the 5% of their income tax to the University of Camerino.

References

[1] C.H. Bennett, G. Brassard, in: Proceedings of IEEE Int. Conf. on Comp., Sys. and Sign. Proc, Bangalore, India, 1984, p. 175.
[2] A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
[3] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Modern Phys. 74 (2002) 145.
[4] D. Mayers, Lecture Notes in Comput. Sci. 1109 (1996) 343.
[5] H.-K. Lo, H. Chau, Science 283 (1999) 2050.
[6] P.W. Shor, J. Preskill, Phys. Rev. Lett. 85 (2000) 441.
[7] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, J. Oppenheim, Lecture Notes in Comput. Sci. 3378 (2005) 386.
[8] R. Renner, Nat. Phys. 3 (2007) 645.
[9] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden, New J. Phys. 4 (2002) 41.
[10] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J.G. Rarity, A. Zeilinger, H. Weinfurter, Phys. Rev. Lett. 98 (2007) 010504.
[11] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger, Nat. Phys. 3 (2007) 481.
[12] H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki, Y. Yamamoto, Nat. Phot. 1 (2007) 343.
[13] www.idquantique.com, www.magiqtech.com.
[14] N. Lütkenhaus, Phys. Rev. A 59 (1999) 3301.
[15] N. Lütkenhaus, Phys. Rev. A 61 (2000) 052304.
[16] M. Dusek, N. Lütkenhaus, M. Hendrych, Progr. Opt. 49 (2006) 381.
[17] H.-K. Lo, N. Lütkenhaus, arXiv:quant-ph/0702202, 2007.
[18] V. Makarov, A. Anisimov, J. Skaar, Phys. Rev. A 74 (2006) 022313.
[19] A. Muller, H. Zbinde, N. Gisin, Europhys. Lett. 33 (1996) 335.
[20] G. Brassard, L. Salvail, Lecture Notes in Comput. Sci. 765 (1994) 410.
[21] K. Boström, T. Felbinger, Phys. Rev. Lett. 89 (2002) 187902.
[22] C. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881.
[23] Q.-Y. Cai, Phys. Rev. Lett. 91 (2003) 109801.
[24] A. Wójcik, Phys. Rev. Lett. 90 (2003) 157901.
[25] Q.-Y. Cai, B.-W. Li, Phys. Rev. A 69 (2004) 054301.
[26] I.P. Degiovanni, I. Ruo Berchera, S. Castelletto, M.L. Rastello, F.A. Bovino, A.M. Colla, G. Castagnoli, Phys. Rev. A 69 (2004) 032310.
[27] A. Wójcik, Phys. Rev. A 71 (2005) 016301.
[28] I.P. Degiovanni, I. Ruo Berchera, S. Castelletto, M.L. Rastello, F.A. Bovino, A.M. Colla, G. Castagnoli, Phys. Rev. A 71 (2005) 16302.
[29] N.J. Beaudry, M. Lucamarini, S. Mancini, R. Renner, Phys. Rev. A 88 (2013) 062302.
[30] Q.-Y. Cai, B.-W. Li, Chin. Phys. Lett. 21 (2004) 601.
[31] F.-G. Deng, G.L. Long, Phys. Rev. A 69 (2004) 52319;
F.-G. Deng, G.L. Long, Phys. Rev. A 70 (2004) 012311.
[32] M. Lucamarini, S. Mancini, Phys. Rev. Lett. 94 (2005) 140501.
[33] M. Lucamarini, G. Di Giuseppe, Int. J. Quant. Inf. 3 (2005) 189.
[34] A. Cerè, M. Lucamarini, G. Di Giuseppe, P. Tombesi, Phys. Rev. Lett. 96 (2006) 200501.
[35] R. Kumar, M. Lucamarini, G. Di Giuseppe, R. Natali, G. Mancini, P. Tombesi, Phys. Rev. A 77 (2008) 22304.
[36] J.S. Shaari, M. Lucamarini, M.R.B. Wahiddin, Phys. Lett. A 358 (2006) 85.
[37] A.P. Shurupov, S.S. Straupe, S.P. Kulik, M. Gharib, M.R.B. Wahiddin, Europhys. Lett. 87 (2009) 10008.

[38] J.S. Shaari, M.R. Wahiddin, S. Mancini, Phys. Lett. A 372 (2008) 1963.
[39] A. Eusebi, S. Mancini, Quantum Inf. Comput. 9 (2009) 950.
[40] S. Pirandola, S. Mancini, S. Lloyd, S.L. Braunstein, Nat. Phys. 4 (2008) 726.
[41] The expression "deterministic cryptography" has been introduced in January 2001 by A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, arXiv:quant-ph/0101066v2; later on published with minor changes as A. Beige et al., J. Phys. A 35 (2002) L407. Nonetheless a number of protocols with deterministic features did already appear before that date. See for instance Ref. [42].
[42] L. Goldenberg, L. Vaidman, Phys. Rev. Lett. 75 (1995) 1239;
M.D. Reid, Phys. Rev. A 62 (2000) 62308;
A. Cabello, Phys. Rev. A 61 (2000) 052312;
G.L. Long, X.S. Liu, Phys. Rev. A 65 (2002) 32302. Also to be mentioned the deterministic version of BB84, suggested in 1992 by A. Ekert to C.H. Bennett, G. Brassard, and N.D. Mermin and recently modified into a practical version in M. Lucamarini, J.S. Shaari, M.R.B. Wahiddin, arXiv:0707.3913 (2007).
[43] We do not compare the present protocol with the *efficient* version of BB84 described in [44], or with other efficient variants like the one reported in [45], for a few reasons. First of all, contrary to LM05, the above-mentioned schemes are deterministic only in the asymptotic limit, i.e. when the number of qubits exchanged by the users is infinite, or in the zero-noise limit of the transmission. The efficiency of the protocol in [44] is $\mathcal{E} = p^2 + (1-p)^2$, with $p \in [0, 1/2]$ the probability to choose the non-preferred basis, and it goes to 1 only for $p \to 0$. This has concrete consequences when one considers the practical situation of a finite-size sample. The less opted out basis must be chosen frequently enough to guarantee a sufficient statistics for the sampling arguments in the security proofs to be true. This problem has been recently addressed in [46] where it is seen (i) that no secure key can be distilled if the sample is too small, e.g. smaller than about 10^5 when the QBER is 5%; (ii) that the probability p depends on the size of the sample, e.g. when the QBER is 5% the probability p is 14%, 7.9%, 4.4% and 2.5% for data samples respectively of 10^6, 10^7, 10^8, and 10^9. Second, the principal aim of our paper is to provide a number of elements to directly compare deterministic QKD with non-deterministic one. So it is clear that if some advantage is found for the deterministic QKD, the same advantage is shared by all those protocols which tends to a deterministic one in some limit.
[44] H.-K. Lo, H.F. Chau, M. Ardehali, J. Cryptology 18 (2005) 133. Also available at arXiv:quant-ph/0011056.
[45] W.Y. Hwang, I.G. Koh, Y.D. Han, Phys. Lett. A 244 (1998) 489;
W.-Y. Hwang, X.-B. Wang, K. Matsumoto, J. Kim, H.-W. Lee, Phys. Rev. A 67 (2003) 012302.
[46] V. Scarani, R. Renner, Phys. Rev. Lett. 100 (2008) 200501.
[47] The deterministic decoding by Bob can only occur in the ideal lossless case. In realistic situations, although the protocol remains deterministic, the overall communication does not.
[48] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, Phys. Rev. A 73 (2006) 022320.
[49] M. Lucamarini, PhD thesis, University of Rome 'La Sapienza', 2005, available at http://padis.uniroma1.it/search.py?recid=178.
[50] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
[51] I. Csiszár, J. Körner, IEEE Trans. Inform. Theory 24 (1978) 339.
[52] M. Lucamarini, A. Cerè, G. Di Giuseppe, S. Mancini, D. Vitali, P. Tombesi, Open Syst. Inf. Dyn. 14 (2007) 169.
[53] M. Martinelli, Opt. Commun. 72 (1989) 341.
[54] H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, W. Tittel, Electron. Lett. 33 (1997) 586.
[55] G. Ribordy, J.D. Gautier, H. Zbinden, N. Gisin, Appl. Optim. 37 (1998) 2272.
[56] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, J. Modern Opt. 47 (2000) 517.
[57] D. Bethune, W. Risk, IEEE J. Quantum Electron. 36 (2000) 340.
[58] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology 5 (1992) 3.
[59] To, Eve it does not really matter the choice of the basis until it is chosen on the equator of the Poincaré sphere. In fact all the "equatorial states" are flipped by Alice's operation $i\hat{Y}$, so they provide her with full information. Moreover the noise introduced on the forward path does not depend on the basis choice, as shown in [3].
[60] C. Fuchs, R.B. Griffiths, C.S. Niu, A. Peres, N. Gisin, Phys. Rev. A 56 (1997) 1163.
[61] A. Peres, Quantum Theory: Concepts and Methods, Kluwer Academic, Dordrecht, The Netherlands, 1997.
[62] To the best of our knowledge an unconditional security proof for two-way QKD is not yet available, although some authors used the arguments of Ref. [25] to claim that.
[63] C.H. Bennett, G. Brassard, J.-M. Robert, SIAM J. Comput., Soc. Ind. Appl. Math. 17 (1988) 210–229.
[64] C.H. Bennett, G. Brassard, C. Crépeau, U.M. Maurer, IEEE Trans. Inform. Theory 41 (1995) 1915.
[65] B. Huttner, N. Imoto, N. Gisin, T. Mor, Phys. Rev. A 51 (1995) 1863.
[66] H.P. Yuen, Quant. Semiclassical Opt. 8 (1996) 939.
[67] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. 85 (2000) 1330.
[68] N. Lütkenhaus, M. Jahma, New J. Phys. 4 (2002) 44.
[69] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92 (2004) 057901.
[70] S.D. Bartlett, T. Rudolph, R.W. Spekkens, Phys. Rev. A 70 (2004) 032321.
[71] G.J. Pryde, J.L. O'Brien, A.G. White, Stephen D. Bartlett, Phys. Rev. Lett. 94 (2005) 220406.
[72] J.L. Duligall, M.S. Godfrey, K.A. Harrison, W.J. Munro, J.G. Rarity, New J. Phys. 8 (2006) 249.
[73] R. Alléaume, F. Roueff, E. Diamanti, N. Lütkenhaus, New J. Phys. 11 (2009) 075002.