Secure Deterministic Communication without Entanglement

Marco Lucamarini[1] and Stefano Mancini[2]

[1]*Dipartimento di Fisica, Università di Roma "La Sapienza," I-00185 Roma, Italy*
[2]*Dipartimento di Fisica, Università di Camerino, I-62032 Camerino, Italy*

(Received 15 May 2004; revised manuscript received 21 December 2004; published 14 April 2005)

We propose a protocol for deterministic communication that does not make use of entanglement. It exploits nonorthogonal states in a two-way quantum channel to attain unconditional security and high efficiency of the transmission. We explicitly show the scheme is secure against a class of individual attacks regardless of the noise on the channel. Its experimental realization is feasible with current technology.

DOI: 10.1103/PhysRevLett.94.140501 PACS numbers: 03.67.Dd, 03.65.Nk

The transmission of secret information along a physical channel is doubtless one of the most attractive perspectives related to the late developments of quantum physics. The pioneering works of Bennett-Brassard (BB84) [1] and Ekert (E91) [2] showed how to exploit quantum resources for cryptographic purposes. Specifically, the usage of either nonorthogonal quantum states (BB84) or entanglement (E91) allows for a secret generation of a random key through which legitimate users can accomplish a thoroughly private communication. This task is usually referred to as quantum key distribution (QKD). Later on, the two schemes were demonstrated to be equivalent [3], and this stimulated the research toward a general security proof (for a review see [4]).

In a recent Letter [5] Boström and Felbinger proposed a protocol for private communication, called ping-pong (PP) for its peculiar use of a two-way quantum channel. In PP entanglement is exploited to attain a deterministic transmission of information. This avoids the waste of qubits arising from basis reconciliation, and allows for a number of new tasks besides QKD such as direct communication (DC) [6] and quantum dialogue [7]. Unfortunately, PP was proved to be not secure [8,9]. Since then, several protocols have been introduced to solve this problem [10], but none of them quantifies the amount of tolerable noise under which the communication remains secure.

In this Letter we introduce a novel communication protocol that achieves secure deterministic communication without resorting to entanglement. The transmission's safety is ensured by the nonorthogonality of the states traveling forward and backward on the quantum channel. A "double control" against eavesdropping provides a high security threshold in the presence of noise.

Our protocol is depicted in Fig. 1. The user "Bob" prepares a qubit in one of the four states $|0\rangle$, $|1\rangle$ (eigenstates of Pauli operator Z), $|+\rangle$, $|-\rangle$ (eigenstates of Pauli operator X), and sends it to his counterpart "Alice." With probability c Alice measures the prepared state (control mode) or, with probability $1 - c$, she uses it to encode a bit (message mode). After that she sends the qubit back to Bob. Encoding is realized by the following transformations on the qubit state [11]: identity operation I encodes "0," while operation $iY \equiv ZX$ encodes "1." Notice that iY acts as a spin flip on all the beginning states:

$$iY(|0\rangle, |1\rangle) = (-|1\rangle, |0\rangle), \qquad iY(|+\rangle, |-\rangle) = (|-\rangle, -|+\rangle).$$

In this way Alice does not need to know the incoming state to perform the encoding. In turn, Bob can deterministically decode Alice's message by measuring the qubit in the same basis he prepared it, without a demand for a classical channel. Avoiding the use of a classical channel during message mode increases both the security and the efficiency of the protocol, as we show hereafter. Furthermore, notice the multitask aspect gained from determinism: in principle Alice can transmit either a meaningless random string of symbols, performing a QKD, or a meaningful one, like the message itself, performing a DC.

To guarantee the security of the scheme, Alice has to switch to control mode with probability $c \neq 0$. In this modality she performs a projective measurement on the incoming qubit along a basis randomly chosen between Z and X. Then, she sends the projected qubit back to Bob. In turn, after declaring on the classical channel receipt of the qubit, Bob carries out his own measurement exactly as he would do if Alice had decided on a message mode (actually, he still does not know Alice's choice). At this point, Alice reveals on the classical channel whether or not she measured (and in which basis), and a public debate on results is settled with Bob in the former case. If Eve is not

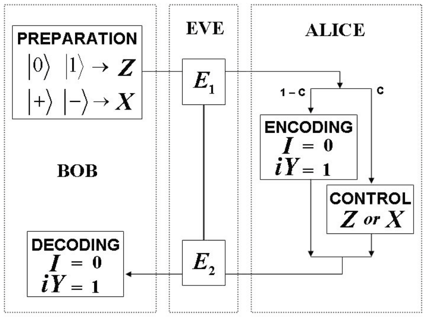

FIG. 1. Scheme of the communication protocol.

© 2005 The American Physical Society

on the line a perfect "double correlation" (on the forward and backward path) of measurement outcomes must be found by legitimate users. The failure of even only one of the two correlations is a signature for Eve's presence.

The "double" control mode described above includes two single tests on the quantum channel, each of which is equivalent to that performed in the one-way BB84 [1,4]. This entails at once the unconditional security of our scheme. However, let us now envisage a simple eavesdropping strategy to show how our double control increases the security of the protocol. Suppose Eve, to learn Alice's operation, decides to perform projective measurements on both paths of the traveling qubit, randomly choosing the measuring basis between Z or X. She can guess the correct basis with 50% probability, and in this case she is not detected at all. If otherwise Eve chooses the wrong basis, she still has a 50% probability to evade detection at point E_1 (Fig. 1) and 50% at point E_2, leading to an overall 25% probability to remain undetected. This means that the double test of Alice and Bob reveals Eve with an average probability $(0 + 3/4)/2 = 3/8 \equiv 37.5\%$, while if they had limited to single tests, either on the forward or on the backward path, this would have been 25%.

In the following we introduce a class of attacks in order to cope with the problem of QKD on a noisy channel, with the aim of finding out some security threshold for this issue. To do that we follow the line sketched in [4] but with some relevant differences. Given the initial four states, and Eve's ancillary states $|\varepsilon\rangle$, we can write the most general operation Eve can do on the traveling qubit as

$$|0\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle = \sqrt{F}|0\rangle|\tilde{\varepsilon}_{00}\rangle + \sqrt{D}|1\rangle|\tilde{\varepsilon}_{01}\rangle, \qquad |1\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle = \sqrt{D}|0\rangle|\tilde{\varepsilon}_{10}\rangle + \sqrt{F}|1\rangle|\tilde{\varepsilon}_{11}\rangle,$$
$$|+\rangle|\varepsilon\rangle \to \frac{1}{\sqrt{2}}[|0\rangle(|\varepsilon_{00}\rangle + |\varepsilon_{10}\rangle) + |1\rangle(|\varepsilon_{01}\rangle + |\varepsilon_{11}\rangle)] \equiv |+\rangle|\varepsilon_{++}\rangle + |-\rangle|\varepsilon_{+-}\rangle,$$
$$|-\rangle|\varepsilon\rangle \to \frac{1}{\sqrt{2}}[|0\rangle(|\varepsilon_{00}\rangle - |\varepsilon_{10}\rangle) + |1\rangle(|\varepsilon_{01}\rangle - |\varepsilon_{11}\rangle)] \equiv |+\rangle|\varepsilon_{-+}\rangle + |-\rangle|\varepsilon_{--}\rangle. \tag{1}$$

Ancillary states are neither orthogonal nor normalized; states with tildes are instead normalized. The following conditions make the transformations (1) unitary:

$$\begin{aligned} \langle\varepsilon_{00}|\varepsilon_{00}\rangle + \langle\varepsilon_{01}|\varepsilon_{01}\rangle &\equiv F + D = 1, \\ \langle\varepsilon_{10}|\varepsilon_{10}\rangle + \langle\varepsilon_{11}|\varepsilon_{11}\rangle &\equiv D + F = 1, \\ \langle\varepsilon_{00}|\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle &= 0. \end{aligned} \tag{2}$$

We can set, without loss of generality $\langle\varepsilon_{00}|\varepsilon_{01}\rangle = \langle\varepsilon_{10}|\varepsilon_{11}\rangle = \langle\varepsilon_{00}|\varepsilon_{10}\rangle = \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0$. Furthermore, we specify the angles between nonorthogonal vectors as $\langle\tilde{\varepsilon}_{00}|\tilde{\varepsilon}_{11}\rangle = \cos x$ and $\langle\tilde{\varepsilon}_{01}|\tilde{\varepsilon}_{10}\rangle = \cos y$ with $0 \le x,\ y \le \pi/2$. All these steps are perfectly equivalent to those considered in [4] for individual nonorthogonal attacks in BB84. However, in [4] symmetry arguments lead one to assume $F = \langle\varepsilon_{00}|\varepsilon_{00}\rangle = \langle\varepsilon_{++}|\varepsilon_{++}\rangle$ for the states of Eqs. (1). This reasoning is not applicable here: the absence of a public basis revelation forces Eve to break the symmetry, deciding by herself the bases of ancillary states. In this way, the fact that a classical channel is unnecessary to the encoding-decoding stage affects the security of the protocol. The next step is to consider that at point E_2 Eve performs a nonorthogonal attack similar to that at point E_1, but with fresh ancillae $|\eta\rangle$ (hence, new parameters F' and D'):

$$\begin{aligned} |0\rangle|\eta\rangle &\to \sqrt{F'}|0\rangle|\tilde{\eta}_{00}\rangle + \sqrt{D'}|1\rangle|\tilde{\eta}_{01}\rangle, \\ |1\rangle|\eta\rangle &\to \sqrt{D'}|0\rangle|\tilde{\eta}_{10}\rangle + \sqrt{F'}|1\rangle|\tilde{\eta}_{11}\rangle, \\ |+\rangle|\eta\rangle &\to |+\rangle|\eta_{++}\rangle + |-\rangle|\eta_{+-}\rangle, \\ |-\rangle|\eta\rangle &\to |+\rangle|\eta_{-+}\rangle + |-\rangle|\eta_{--}\rangle. \end{aligned} \tag{3}$$

At the end of transmission Eve will measure ε and η ancillae and, by comparing results, she will gain information. Although this is not the most general operation Eve can do on the whole, it is worth being studied because its consequences are quite general. We want to recover Eve's optimal eavesdropping strategy, i.e., determine parameters' values that maximize Alice-Eve and Bob-Eve mutual information (I_{AE}, I_{BE}) minimizing the probability of detecting Eve (P_d). From transformations (1) and conditions (2) we can evaluate the probability that Eve is not detected in the forward path, after her E_1 attack, simply by squaring the coefficients of the states that remain unaltered after Eve's action:

$$\begin{aligned} P_{nd}(|0\rangle) &= \langle\varepsilon_{00}|\varepsilon_{00}\rangle = \langle\varepsilon_{11}|\varepsilon_{11}\rangle = P_{nd}(|1\rangle) = F, \\ P_{nd}(|+\rangle) &= P_{nd}(|-\rangle) = (1/2)[1 + F\cos x + D\cos y]. \end{aligned} \tag{4}$$

Similar arguments hold for the backward path, after the E_2 attack, with primed parameters replacing not-primed ones. The probability that Eve is not detected after a whole run is then the product of the two partial probabilities; by taking its complement we obtain the probability of detecting Eve. Averaging it over all input states we get

$$\begin{aligned} P_d = (1/8)\{&7 - 4FF' - F\cos x - D\cos y - F'\cos x' \\ &- D'\cos y' - FF'\cos x\cos x' - FD'\cos x\cos y' \\ &- DF'\cos y\cos x' - DD'\cos y\cos y'\}. \end{aligned} \tag{5}$$

It is possible to show [12] that P_d takes the minimum

$$d \equiv \min P_d = [1 - (1 + \cos x)(1 + \cos x')/4]/2 \tag{6}$$

for $F = F' = 1$; this condition represents the best Eve can do to conceal her presence. The maximum value for d ($d = 3/8$) is obtained when $x = x' = \pi/2$, corresponding, as we will see, to Eve's maximum information.

To evaluate I_{AE} let us write the state prepared by Bob as $|\Psi\rangle = \sum_{\alpha=0,1} C_\alpha |\alpha\rangle$, with $C_\alpha = \alpha$, $(1-\alpha)$ for basis Z, and $1/\sqrt{2}$, $(-1)^\alpha/\sqrt{2}$ for basis X. Now, suppose we are in message mode and Alice wants to encode a "0"; hence, she performs the identity between Eve's two attacks:

$$|\Psi\rangle|\varepsilon\rangle|\eta\rangle \xrightarrow{E_1} \sum_\alpha C_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \xrightarrow{I} \sum_\alpha C_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle \times |\eta\rangle \xrightarrow{E_2} \sum_\alpha C_\alpha \sum_{\beta,\gamma} |\gamma\rangle|\varepsilon_{\alpha\beta}\rangle|\eta_{\beta\gamma}\rangle.$$

The ancillary states involved in this operation are

$$\begin{array}{llll} |\varepsilon_{00}, \eta_{00}\rangle, & |\varepsilon_{00}, \eta_{01}\rangle, & |\varepsilon_{01}, \eta_{10}\rangle, & |\varepsilon_{01}, \eta_{11}\rangle, \\ |\varepsilon_{10}, \eta_{00}\rangle, & |\varepsilon_{10}, \eta_{01}\rangle, & |\varepsilon_{11}, \eta_{10}\rangle, & |\varepsilon_{11}, \eta_{11}\rangle. \end{array} \tag{7}$$

If, instead, Alice performs a flip operation we have

$$|\Psi\rangle|\varepsilon\rangle|\eta\rangle \xrightarrow{E_1} \sum_\alpha C_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \xrightarrow{iY} \sum_\alpha C_\alpha \sum_\beta (-1)^{\beta+1} |\beta \oplus 1\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \xrightarrow{E_2} \sum_\alpha C_\alpha \sum_{\beta,\gamma} (-1)^{\beta+1} |\gamma\rangle|\varepsilon_{\alpha\beta}\rangle|\eta_{(\beta\oplus 1)\gamma}\rangle,$$

and ancillary states involved are

$$\begin{array}{llll} |\varepsilon_{00}, \eta_{10}\rangle, & |\varepsilon_{00}, \eta_{11}\rangle, & |\varepsilon_{01}, \eta_{00}\rangle, & |\varepsilon_{01}, \eta_{01}\rangle, \\ |\varepsilon_{10}, \eta_{10}\rangle, & |\varepsilon_{10}, \eta_{11}\rangle, & |\varepsilon_{11}, \eta_{00}\rangle, & |\varepsilon_{11}, \eta_{01}\rangle. \end{array} \tag{8}$$

To acquire information from states (7) and (8), Eve must measure both her ancillae. Keeping in mind orthogonality relations (2) and following, we see that the best way to do that is to distinguish orthogonal subspaces before, and then nonorthogonal states within, them. The probability to correctly distinguish between two states with scalar product $\cos x$ is $(1 + \sin x)/2$ [4]. Observing states (7) and (8) we notice that if Eve mistakes to identify her first ancilla (ε states) then she guesses wrong Alice's operation, since she flips from states (7) to (8) or vice versa. The same is true if she guesses the right ε state but mistakes the η state. Nevertheless, if she mistakes twice, then with the first error she misinterprets (7) with (8) and with the second error she compensates for the first, eventually guessing right Alice's operation. This leads to a lengthy expression for I_{AE} as a function of the six parameters describing ancillae states, but it can be simplified recalling that Eve wants to keep P_d as low as possible, and so the condition $F = F' = 1$ seen before applies. In this case Eve's strategy is optimal and I_{AE} becomes

$$I_{AE} = 1 - h[(1 + \sin x \sin x')/2], \tag{9}$$

where h indicates the Shannon binary entropy [4]. Now we would like to express the information I_{AE} as a function of the detection probability d only, but the presence of two parameters (x and x') in Eqs. (6) and (9) prevents us from doing that. However, the following lemma holds:

Lemma. *The optimal Eve incoherent attack consists in a balanced one for which* $x = x'$.

This lemma can be justified with a qualitative argument [12]. The degree of orthogonality Eve imposes on her ancillae is somewhat related to the information she can extract from the qubit: the more orthogonal they are, the higher is the information gained. If she sets $x > x'$, the ancillae ε will be more orthogonal than ancillae η, and this entails a loss of information when going from the forward to the backward path. If she sets $x < x'$, we can argue the reverse. Then $x = x'$ follows.

The above lemma with Eqs. (6) and (9) leads to

$$d = [1 - (1/4)(1 + \cos x)^2]/2, \tag{10}$$

$$I_{AE} = 1 - h[(1 + \sin^2 x)/2]. \tag{11}$$

Now it suffices for a simple inversion to write I_{AE} as a function of d. Similar arguments hold for I_{BE}, whose expression as a function of x is

$$I_{BE} = \frac{1}{2}\left[2 - h\left(\frac{1}{2} + \frac{\sin^2 2x}{8}\right) - h\left(\frac{1}{2} + \frac{\sin^2 x}{2}\right)\right]. \tag{12}$$

For a QKD to be secure, Alice-Bob mutual information must be greater than Alice-Eve or Bob-Eve information [4]; the next step is then to evaluate Alice-Bob mutual information. Also in this case we must set $F = F' = 1$, because Bob receives a perturbed state according to Eve's choice of minimizing P_d. By using this condition and the lemma stated above, and by averaging information on the input states, we get

$$I_{AB} = 1 - (1/2)h[(1 + \cos^2 x)/2]. \tag{13}$$

All the mutual information of I_{AB}, I_{AE}, and I_{BE} is plotted as functions of the detection probability d in Fig. 2. It can be noted that the mutual information of I_{AE} and of I_{BE} is different. This represents a resource for Alice and Bob since the condition $I_{AB} \geq I_{BE}$ is fullfilled for every value

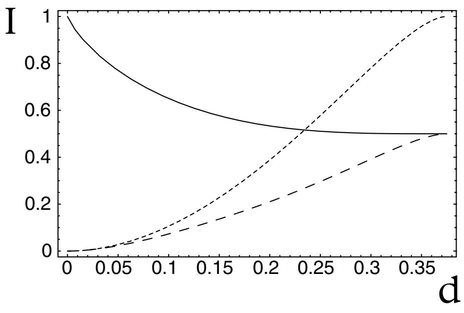

FIG. 2. Mutual information vs detection probability in individual attacks. The descent curve represents Alice and Bob mutual information I_{AB}. The crescent curves are Alice-Eve mutual information I_{AE} (dotted line) and Bob-Eve mutual information I_{BE} (dashed line).

of d; i.e., a secret key can always be established, regardless of the noise on the channel. This situation resembles what happens with "reverse reconciliation" in continuous variables' quantum cryptography when lossy channels are taken into account [13]. On the other hand, $\mathcal{I}_{AB} \geq \mathcal{I}_{AE}$ when $d \lesssim 23\%$. Yet, the analysis of $\mathcal{I}_{AE}$ can still be useful for Eve's upper-bound information when a more general individual attack is considered, i.e., the one in which Eve creates coherence between points E_1 and E_2 (Fig. 1) to improve her attack. In this case, it turns out that the communication is secure until $d \lesssim 18\%$ (under similar circumstances BB84 leads to $d \lesssim 15\%$ [4]). We also note that the maximum of $\mathcal{I}_{AE}$ corresponds to a detection probability $d = 3/8 \equiv 37.5\%$, which is the least disturbance Eve can introduce on the channel when she steals a full amount of information from Alice. This value can be used to calculate the asymptotical security [5] of the protocol when it is used to perform a run-by-run DC. Given the probability c that a control mode occurs, and an average probability d to detect Eve during a control run, the probability that Eve steals n bits of full information without being detected is $\mathcal{P}_n(c, d) = (1 - c)^n/[1 - c(1 - d)]^n$. To picture a reasonable scenario, besides $d = 3/8$ we set $c = 1/2$. In this case, Eve has a probability of about 7.8% to successfully eavesdrop 1 byte (i.e., 8 bits) of information and of about 0.6% to eavesdrop 2 bytes. Increasing the value of c increases the security of the protocol, but at the expense of the transmission rate.

For the sake of completeness we briefly describe the behavior of the presented scheme on a lossy channel. In this case two aspects are important: security against losses-based attacks and efficiency of transmission. As far as the former is concerned, the risk is that an almighty Eve could substitute an imperfect channel with a perfect one and conceal her presence behind losses interpreted as natural by Alice and Bob. This possibility exploits the lack of symmetry in either the control or the encoding stage [9] and is not effective in our case. We have also considered subtle attacks based on a sort of "quantum nondemolition eavesdropping," but Alice and Bob can always detect Eve either by comparing losses measured during control runs with those of message runs or by using a message authentication procedure as well. Also, asking Alice to add a random phase to the encoded qubit could be useful, though not essential, in this case.

Regarding the efficiency, we consider the definition given in [14], $\mathcal{E} = b_s/(q_t + b_t)$, where b_s is the expected number of secret bits received by Bob, q_t is the number of transmitted qubits on the quantum channel, and b_t is the number of transmitted bits on the classical channel. Since in our scheme no classical information is needed in the message mode, we have $b_t = 0$ that together with $b_s = 1$, $q_t = 1$ provides $\mathcal{E} = 1$. However, the practical efficiency takes into account the channel's transmittance also [15]. In our protocol a qubit travels for a distance $2L$, L being the separation between Alice and Bob. If $\mathcal{T}$ is the transmittance of the qubit over a distance L, the transmittance pertaining to a distance $2L$ is $\mathcal{T}^2$. Then, the practical efficiency can be evaluated as $\mathcal{E}' = \mathcal{E}\mathcal{T}^2 = \mathcal{T}^2$. For comparison, in BB84 it is $\mathcal{E}' = (1/6)\mathcal{T}$ because $b_s = 0.5$, $q_t = 1$, $b_t = 2$, and a qubit travels for a distance L. This entails that the presented scheme is more efficient than BB84 provided the transmittance of the channel is $\mathcal{T} > 1/6$. It is also possible to see [15] that the practical efficiency pertaining to entanglement-based schemes contains a factor $\mathcal{T}^4$, making it lower than ours.

A final remark concerns the feasibility of our scheme. The absence of entanglement makes it almost as practical as BB84. More so, if we require a control on the backward path, i.e., only one passive (for an "in-principle" demonstration) or active (for a complete implementation) linear optical element, like a $\frac{\lambda}{2}$-wave plate or an electro-optic modulator, both introducing a small amount of losses. Suitable schemes working with faint laser pulses can be found in [16].

In conclusion, we have presented a two-way protocol for deterministic communication without entanglement. Besides its unconditional security, it has explicitly been proved secure against individual attacks regardless of the noise on the channel. The proposed scheme also is efficient on lossy channels and is suitable for experimental realization.

We acknowledge useful discussions with G. Di Giuseppe and S. Pirandola. One of us (M. L.) thanks his parents for funding.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Signal Processing* (Indian Institute of Science, Bangalore, India, 1984).

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett *et al.*, Phys. Rev. Lett. **68**, 557 (1992).

[4] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002), and references therein.

[5] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[6] A. Beige *et al.*, Acta Phys. Pol. A **101**, 357 (2002).

[7] N. Ba An, Phys. Lett. A **328**, 6 (2004).

[8] Qing-Yu Cai, Phys. Rev. Lett. **91**, 109801 (2003).

[9] A. Wojcik, Phys. Rev. Lett. **90**, 157901 (2003).

[10] F.-G. Deng *et al.*, Phys. Rev. A **68**, 042317 (2003); F.-G. Deng and G. L. Long, *ibid.* **69**, 052319 (2004); Q.-Y. Cai and B.-W. Li, *ibid.* **69**, 054301 (2004).

[11] Q.-Y. Cai and B.-W. Li, Chin. Phys. Lett. **21**, 601 (2004).

[12] Detailed calculations will be presented elsewhere for space reasons.

[13] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).

[14] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).

[15] I. P. Degiovanni *et al.*, Phys. Rev. A **69**, 032310 (2004).

[16] F.-G. Deng and G. L. Long, Phys. Rev. A **70**, 012311 (2004); M. Lucamarini and G. Di Giuseppe, Int. J. Quantum. Inform. **3**, 189 (2005).