Device-independent entanglement-based Bennett 1992 protocol

Marco Lucamarini,[1] Giuseppe Vallone,[2,3] Ilaria Gianani,[2] Paolo Mataloni,[2,4] and Giovanni Di Giuseppe[1,5]

[1]*Scuola di Scienze e Tecnologie, Divisione di Fisica, I-62032 Camerino (MC), Italy*
[2]*Dipartimento di Fisica, Università Sapienza di Roma, I-00185 Roma, Italy*
[3]*Department of Information Engineering, University of Padova, I-35131 Padova, Italy*
[4]*Istituto Nazionale di Ottica, Consiglio Nazionale delle Ricerche (INO-CNR), Largo Enrico Fermi 6, I-50125 Firenze, Italy*
[5]*CriptoCam srl, Via Madonna delle Carceri 9, I-62032 Camerino (MC), Italy*

(Received 15 May 2012; published 18 September 2012)

In this paper we set forth a connection between the Bennett 1992 protocol and a Bell inequality. This allows us to extend the usual prepare-and-measure protocol to its entanglement-based formulation. We exploit a recent result in the framework of device-independent quantum key distribution to provide a simple, model-independent, security proof for the protocol. The minimum efficiency required for a practical implementation of the scheme can be as low as 75% in the completely untrusted case and 50% in case the sender is assumed to be trusted.

DOI: 10.1103/PhysRevA.86.032325 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

In 1992 Charles Bennett introduced his famous minimal-state protocol for quantum key distribution (QKD), named after him "B92" [1]. It makes use of two nonorthogonal quantum states to convey one bit of information from a transmitting user (Alice) to a receiving user (Bob).

The single-photon B92 protocol was proven unconditionally secure in [2,3]. Its main problem is the unambiguous state discrimination (USD) [4] attack, initially discussed in [1] and later on analyzed in [3], which dramatically reduces its tolerance to the losses of the communication channel and, by consequence, its applicability to a practical scenario. In this respect, a version of the single-photon B92 protocol, robust against the USD attack, was recently introduced in [5]. It exploits two additional states in Alice's preparation, called "uninformative states," to let the users detect a USD attack. For this reason it was called "us-B92" [5].

At variance with the more popular BB84 protocol [6], the B92 does not allow for an entanglement-based realization and can only be implemented in a prepare-and-measure (PM) configuration. This means that in order to guarantee its unconditional security it is necessary to enclose the source of photons in Alice's territory, well shielded against a malicious presence (Eve) eavesdropping on the quantum channel. So, for instance, it is not possible to place the light source in the middle of Alice and Bob in order to increase the maximum working distance [7,8] of a B92-based QKD session. The us-B92 protocol follows the same fate as the B92, and is only PM as well. However, we realized that it admits a straightforward extension to a description and implementation which are based on the entanglement, called "ent-B92" henceforth.

Several security proofs of B92 rely on entanglement distillation. However, the entanglement is used only as a mathematical tool to demonstrate security, but the physical realization was always based on a PM scheme. Here we propose to use the entanglement as the physical resource to realize the cryptographic protocol. In this case it is possible to implement the protocol with the entanglement source placed in an untrusted location, between Alice and Bob. The security proofs of the standard B92 [2,5] and of the us-B92 [5] are valid only assuming that the entangled source is shielded on Alice's side. In our protocol even if the entanglement source is under Eve's control, we demonstrate that it is possible to prove its security by connecting it with a particular form of Bell inequality [9], put forward for the first time by Clauser and Horne in 1974 [10] and later adapted to nonmaximally entangled states by Eberhard [11]. This connection, besides giving physical insight into a long-standing protocol like the B92, allows us to provide a simple security proof for the new protocol, which exploits a recent work by Masanes *et al.* [12] in the frame of device-independent (DI) QKD.

Hence, the ent-B92 is proven secure regardless of the particular implementation of the protocol. The security proof employed is totally different from the standard one [2,3], which is based on the approach described in [13,14]. Notwithstanding, the obtained security threshold is remarkably close to the one given in the literature, thus confirming the B92 state of the art. In addition to this, we managed to exploit the protocol and its security proof to decrease considerably the minimum detection efficiency for a possible realization of a DI-QKD, from 92.4% reported in [15] to 75% in our approach.

II. ENT-B92 PROTOCOL

Here we introduce the entanglement-based ent-B92 protocol that can be reduced to the B92 [1] or us-B92 [5] protocols. Let us suppose that Alice and Bob share the following nonmaximally entangled state:

$$\begin{aligned}|\Phi\rangle_{AB} &= (|0_z\rangle_A|\varphi_0\rangle_B + |1_z\rangle_A|\varphi_1\rangle_B)/\sqrt{2}\\ &= \beta|0_x\rangle_A|0_x\rangle_B + \alpha|1_x\rangle_A|1_x\rangle_B,\end{aligned} \tag{1}$$

where

$$|\varphi_j\rangle = \beta|0_x\rangle + (-1)^j\alpha|1_x\rangle, \tag{2}$$

$\{|0_z\rangle,|1_z\rangle\}$ ($\{|0_x\rangle,|1_x\rangle\}$) are the eigenstates of the $\mathbf{Z}$ ($\mathbf{X}$) basis with $|j_x\rangle = [|0_z\rangle + (-1)^j|1_z\rangle]/\sqrt{2}$, $\beta = \cos(\theta/2)$, $\alpha = \sin(\theta/2)$, and $\theta \in (0,\pi/2)$. The state $|\Phi\rangle_{AB}$ has been used in [16] and [11] to propose novel tests of local realism and is routinely implemented in laboratory [17–20].

If Alice measures along the $\mathbf{Z}$ basis, she will project Bob's state in either $|\varphi_0\rangle$ or $|\varphi_1\rangle$, with equal probabilities. This was at the basis of the B92 unconditional security proof given in Ref. [2]. However, it was accompanied by the further assumption that the source of the entangled photons must be placed in Alice's secure location, hence unreachable to Eve. This assumption is very reasonable if one is interested to use a PM protocol. When the actual protocol is entanglement-based, such an assumption should be avoided. Here we show that the protocol is still secure even when the light source is placed midway between the users. This ent-B92 scheme can be seen as the entanglement version of the PM B92 scheme [1] in which Alice prepares and sends to Bob with equal probability the states $|\varphi_0\rangle$ or $|\varphi_1\rangle$. The bit encoded by Alice is $j=0$ or $j=1$ depending on the $|\varphi_j\rangle$ state received by Bob. The density matrix ρ_B held by Bob (or prepared by Alice in the PM scheme) can be written as

$$\rho_B = \frac{|\varphi_0\rangle\langle\varphi_0| + |\varphi_1\rangle\langle\varphi_1|}{2} = \beta^2|0_x\rangle\langle 0_x| + \alpha^2|1_x\rangle\langle 1_x|. \qquad (3)$$

To decode the information, Bob measures the incoming states in the basis $\mathbf{B}_k = \{|\varphi_k\rangle,|\overline{\varphi}_k\rangle\}$, $k=\{0,1\}$, where $|\overline{\varphi}_k\rangle = \alpha|0_x\rangle - (-1)^k\beta|1_x\rangle$. Upon obtaining the state $|\overline{\varphi}_k\rangle$, Bob decodes Alice's bit as $j = k \oplus 1$ (the symbol "$\oplus$" means "addition modulo 2") and labels the result as *conclusive*; on the contrary, upon obtaining the state $|\varphi_k\rangle$, Bob is not able to decode Alice's bit deterministically and simply labels the result as *inconclusive*.

The same entangled state can be also used to perform the so-called us-B92 [5], where, with probability $1-p$, everything goes as in the standard B92; on the other hand, with probability $p \ll 1$, Alice prepares two additional, uninformative, states, which are chosen as follows:

$$|us_1\rangle = |0_x\rangle; \quad |us_2\rangle = |1_x\rangle. \qquad (4)$$

In particular, the states $|0_x\rangle$ and $|1_x\rangle$ are prepared with probabilities $p\times\beta^2$ and $p\times\alpha^2$, respectively. This is necessary to assure that Eve cannot discriminate between the density matrix pertaining to the signal states or to the uninformative states [Eq. (3)]. If Alice measures along the $\mathbf{X}$ basis the entangled state (1), she will project Bob's state in either $|0_x\rangle$, with probability β^2, or $|1_x\rangle$, with probability α^2, thus preparing the uninformative states of the us-B92 protocol [Eq. (4)] with the correct probabilities. So, the ent-B92 reduces to the us-B92 if one considers that the results from Alice's $\mathbf{Z}$ basis measurements are used as bits of the final secret key, while those from the $\mathbf{X}$ basis measurements are used to perform a test against the USD attack, as in the us-B92. Bob's measurement remains the same as in the standard B92. However, the presence of the uninformative states allow the users to detect a possible USD attack [5].

To prove the security of the ent-B92 we follow the approach of a DI security proof [12] by establishing a connection between the ent-B92 protocol and a particular Bell inequality.

Let us write the following Bell inequality, which was first introduced by Clauser and Horne [10] ("CH inequality" for short):

$$\begin{aligned} S_{\rm CH} = {} & P(a_1,b_1) + P(a_0,b_1) + P(a_1,b_0) \\ & - P(a_0,b_0) - P(a_1) - P(b_1) \leqslant 0. \end{aligned} \qquad (5)$$

Here $P(a_i,b_j)$ is the joint probability that Alice detects the state $|a_i\rangle$ and Bob detects the state $|b_i\rangle$, while $P(a_1)$ and $P(b_1)$ are the probabilities that Alice and Bob respectively measure $|a_1\rangle$ and $|b_1\rangle$, regardless of what is measured by the other user. This takes into account also those instances in which one of the users receives a vacuum count. For instance, the term $P(a_1)$ includes the probability $P(a_1,b_v)$ that Alice measures the state $|a_1\rangle$ and Bob measures a vacuum. If both Alice and Bob detect a vacuum count, the event does not contribute to the CH inequality. Local realism is verified until the above inequality is true. On the contrary, quantum mechanics is expected to violate such an inequality in some range of values.

The goal is usually to maximize the CH violation, but, in this paper, our first aim is to connect the violation of a Bell inequality to the ent-B92 protocol. It is then natural to choose the states $|a_i\rangle$ and $|b_j\rangle$ among the ent-B92 states. We select for Alice the states

$$|a_0\rangle = |0_z\rangle, \quad |a_1\rangle = |1_x\rangle, \qquad (6)$$

while we choose for Bob

$$|b_0\rangle = |\overline{\varphi}_0\rangle, \quad |b_1\rangle = |\overline{\varphi}_1\rangle. \qquad (7)$$

Using these states we are able to calculate the different probabilities appearing in Eq. (5) and see for which specific values of θ the CH inequality is violated. After some algebra, the value of $S_{\rm CH}$ as a function of θ is found to be

$$S_{\rm CH}(\theta) = \tfrac{1}{2}\cos\theta(1-\cos\theta). \qquad (8)$$

This quantity is plotted in Fig. 1 with a solid line. It is positive for all values of θ in the open interval $(0,\pi/2)$; that is, it violates the Bell inequality for the same interval of θ in which the ent-B92 protocol is defined. Only the extremal points $\theta=0$ and $\theta=\pi/2$ are excluded. The maximum violation occurs at $\theta_{\max}=\pi/3$, corresponding to $S_{\rm CH}=1/8$. We also plot the maximum violation $S_{\rm CH}^{\max}(\theta)$ that can be obtained with generic measurements on $|\Phi\rangle_{AB}$ [21].

We notice that the choice $|a_1\rangle = |1_x\rangle$, which is not present in the traditional B92 protocol and is present in the us-B92 protocol only for detecting the USD attack, here derives directly from the Bell inequality. In fact, after choosing $|a_0\rangle$, $|b_0\rangle$, and $|b_1\rangle$ as in the B92 protocol [Eqs. (6) and (7)], the choice of $|a_1\rangle = |1_x\rangle$ is the one which maximizes the violation of the CH inequality.

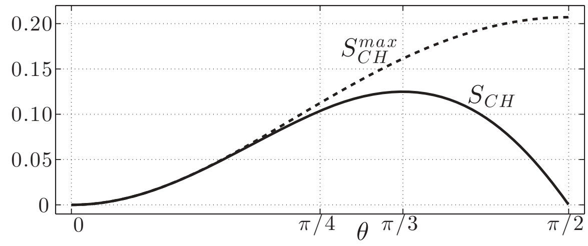

FIG. 1. Plot of $S_{\rm CH}$ (solid line) as function of θ. We also plot with dashed line the maximum violation achievable with the nonmaximally entangled state (1), namely $S_{\rm CH}^{\max}(\theta) = \frac{1}{2}(\sqrt{\sin^2\theta+1}-1)$. The maximum violation can be obtained if Alice measure along the states (6), and Bob along the new states $|b_0'\rangle = |\overline{\varphi}_0'\rangle$, $|b_1'\rangle = |\overline{\varphi}_1'\rangle$, where $|\overline{\varphi}_0'\rangle$ and $|\overline{\varphi}_1'\rangle$ are chosen like in Eq. (2) but with an angle θ' satisfying $\tan\theta' = \sin\theta$.

III. SECURITY PROOF OF THE ENT-B92

In this section we exploit a recent work by Masanes *et al.* [12] to demonstrate the unconditional security of the newly introduced ent-B92 protocol. Since the security proof is based on the measured correlations, the security is assured even if the entanglement source is under the Eve's control. Moreover, since in Ref. [12] a bound for the min-entropy is found, the security obtained for the ent-B92 protocol is composable [22,23].

In [12] it is explicitly given the final *secure gain* [25] R of a QKD protocol which uses a Bell inequality in the form of a CHSH inequality [26] to guarantee the overall security of the transmission. The length $r = n_{\rm conc} \times R$ of the secret key obtained by processing the raw key with an error-correcting protocol and a two-universal random function is, up to terms of order $\sqrt{n_{\rm conc}}$, lower bounded by $H_{\min}(A|E) - N_{\rm pub}$, where $H_{\min}(A|E)$ is the min-entropy of Alice's outcomes conditioned on Eve's information on the joined Alice-Eve state, and $N_{\rm pub}$ is the number of bits published by Alice in the error-correcting phase. The length of the public message necessary for correcting Bob's errors is $N_{\rm pub} = n_{\rm conc} \times H(a|b)$, up to terms of order $\sqrt{n_{\rm conc}}$. From the violation of the CHSH inequality, Masanes *et al.* in [12] showed that the min-entropy is bounded and obtained the following bound on the secure gain:

$$R \geqslant -\log_2\left(\frac{1}{2}+\frac{1}{2}\sqrt{2-\frac{S_{\rm CHSH}^2}{4}}\right) - H(a|b), \tag{9}$$

where

$$S_{\rm CHSH} = \langle A_1 B_1\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_0 B_0\rangle. \tag{10}$$

The correlation term are $\langle A_i B_j\rangle = P(a_i,b_j) + P(\overline{a}_i,\overline{b}_j) - P(\overline{a}_i,b_j) - P(a_i,\overline{b}_j)$ and $\overline{a}_i$ ($\overline{b}_j$) is the state orthogonal to $|a_i\rangle$ ($|b_j\rangle$). The term containing the quantity $S_{\rm CHSH}$ is the one corresponding to the *phase-error* rate of the protocol [14]. It takes into account how much privacy amplification [27] should be performed by the users to remove any residual information from Eve's hands. The term $H(a|b)$ is related to the error correction procedure [28], amounting to h(Q), with h the binary entropy [29] and Q the QBER (quantum bit error rate) measured on the quantum channel.

The bit error rate for the ent-B92 is a measurable quantity of the protocol and does not represent any problem. It comes from the number of errors $n_{\rm err}$, found by the users during the error correction procedure, divided by the number of conclusive events, $n_{\rm con}$. The phase error rate is given by a lower bound on Eve's information as a function of the CHSH value. This is the main result of Ref. [12] that we want to apply here. However, the results of [12] apply to the CHSH inequality and we have to relate it to the CH. By using $P(a_i,b_j) + P(\overline{a}_i,b_j) = P(b_j)$ and $P(a_i,b_j) + P(a_i,\overline{b}_j) = P(a_i)$ it is possible to show that the generic correlation term $\langle A_i B_j\rangle$ of $S_{\rm CHSH}$ can be written as $4P(a_i,b_j) - 2P(a_i) - 2P(b_j) + 1$. Note that this relation holds even if the vacuum counts are taken into account. In fact, in this case it suffices to modify the correlation terms in order to consider the losses. We use the rule of considering the vacuum counts as a detection on the orthogonal states $|\overline{a}_i\rangle$ and $|\overline{b}_j\rangle$ (when the observable A_i and B_j are measured, respectively). In this way the correlation term can be written as $\langle A_i B_j\rangle = P(a_i,b_j) + [P(\overline{a}_i,\overline{b}_j) + P(a_v,\overline{b}_j) + P(\overline{a}_i,b_v) + P(a_v,b_v)] - [P(\overline{a}_i,b_j) + P(a_v,b_j)] - [P(a_i,\overline{b}_j) + P(a_i,b_v)]$. Since $P(a_i) = P(a_i,b_i) + P(a_i,\overline{b}_i) + P(a_i,b_v)$, even in this case we obtain $\langle A_i B_j\rangle = 4P(a_i,b_j) - 2P(a_i) - 2P(b_j) + 1$.

Starting from this relation it is straightforward to show that the two inequalities are related by $S_{\rm CHSH} = 4S_{\rm CH} + 2$ and the secure gain becomes

$$R = 1 - \log_2(1 + \sqrt{1 - 4S_{\rm CH} - 4S_{\rm CH}{}^2}) - h\left(\frac{n_{\rm err}}{n_{\rm con}}\right). \tag{11}$$

We can notice that there is a one-to-one correspondence between nonlocality and security: In fact, the above secure gain is always negative when $S_{\rm CH} < 0$, that is, when the CH inequality is no more violated, and is positive when $S_{\rm CH} > 0$, if $n_{\rm err} = 0$. In analogy with the standard approach, in order to obtain the secure rate of the ent-B92 protocol, we have to multiply the obtained gain by the number of conclusive events collected by Alice and Bob:

$$r_{{\rm ent}-B92} = n_{\rm con} R. \tag{12}$$

Let us remark that this last step just concerns the *efficiency* of the protocol, not its *security*, which only depends on the gain R and on the estimation of the CHSH value from the measured CH inequality.

A. Resistance to losses

The DI security proof adopted for the ent-B92 offers the immense advantage of making the protocol independent of the practical details of the implementation: Alice and Bob could even purchase their devices directly from Eve, because the violation of a Bell inequality would certify the secrecy of the transmission in any case. On the other side, this certification is based on a Bell test, which is hardly feasible with current technology (see, however, the proposals in [30,31] and the high-efficiency detectors reported in [32,33]). The most difficult step is to close the detection loophole, which requires a very low global loss rate, from the light source to the detectors. The maximum tolerable loss rate or, equivalently, the minimum global efficiency η_g required to close the detection loophole, is a figure of merit of a given protocol: The lower the η_g, the more feasible is the protocol. It is known that to close the detection loophole η_g cannot be lower than 2/3 (67%), a result for the first time found by Eberhard [11] by an inequality very similar to our Eq. (5). Here we want to quantify η_g for the ent-B92, so to study its resistance against the losses of the communication when the channel noise is zero. Using the ent-B92 states given in Eqs. (6) and (7), it is not difficult to see that the resulting CH inequality can be written in terms of θ, η_A (Alice total efficiency) and η_B (Bob total efficiency) as

$$S'_{\rm CH}(\theta) = \left(\eta_A - \frac{1}{2}\right)\eta_B \sin^2\theta - \eta_A \sin^2\frac{\theta}{2}. \tag{13}$$

Note that if $\eta_A = \eta_B = 1$ this quantity coincides with that of Eq. (8). It is interesting to detail a few particular cases related to this result: (I) if $\eta_A = 1$, then $S''_{\rm CH} = \eta_B(\sin^2\theta)/2 - \sin^2(\theta/2)$ and local realism can be violated for $\eta_B > 1/2$; (II) if $\eta_B = 1$, then $S''_{\rm CH} = (\eta_A - 1/2)\sin^2\theta - \eta_A \sin^2(\theta/2)$, and local realism can be violated for $\eta_A > 2/3$; (III) if $\eta_A = \eta_B = \eta$, then

$S''_{\mathrm{CH}} = (\eta - 1/2)\eta \sin^2\theta - \eta \sin^2(\theta/2)$, and local realism can be violated for $\eta > 3/4$.

Case (III) above corresponds to a symmetric configuration, that is, when Alice and Bob efficiencies are equal. In this case $\eta_g = 3/4$, which is higher than the expected value $2/3$, corresponding to Eberhard's result [11]. This is due to the fact that the ent-B92 states are fixed and cannot be further optimized. However, even though not optimal, this result is quite interesting. In fact, due to the one-to-one correspondence between secure gain and nonlocality, we can conclude that the ent-B92 provides a positive, model-independent, secure gain if the users' efficiencies are higher than 75%. This value can be compared, for example, with that of Ref. [15], where the minimum efficiency required is 92.4%.

We can further improve on our result by exploiting case (I), which refers to a nonsymmetric configuration (see also [34,35]), and introducing an additional assumption. In concrete, we place the source of the entangled state [Eq. (1)] in Alice's territory, *shielded against Eve's intrusion*. This is a standard assumption in QKD, which holds for all PM protocols. So we are going back to a PM configuration and consider the PM version of the device-independent ent-B92 just introduced. This new situation does not cover anymore the possibility that Alice's setup is provided by Eve, but still covers the possible, involuntary, calibration errors in Alice's devices; moreover, it covers, of course, the possibility that Bob's setup is provided directly by Eve. This can be also understood by considering that Alice devices are *trusted*, even though this alternative view is slightly stronger than our assumption, since we let a certain degree of untrustworthiness in Alice devices, represented by the calibration errors.

Since Eve cannot modify the result of a Bell test by acting on Alice's setup, we can safely assume that Alice's efficiency is 100%, thus falling into case (I) above, which entails that Bob's efficiency can be as low as 50% in order to provide a positive secure gain independent of the implementation details. This result coincides with that obtained in [36] by a different approach and resembles an entanglement-steering scenario [37], where detectors are asymmetrically treated by the users in the search of an EPR-steering inequality violation [38] (see also [39,40]).

B. Resistance to noise

In order to perform a fair comparison with the standard PM protocols, we place the entangled light source very close to Alice station. Then we consider a depolarizing channel acting on the state going from Alice to Bob, as follows:

$$\rho \rightarrow \rho' = (1-p)\rho + \frac{p}{3}(\sigma_x \rho \sigma_x + \sigma_y \rho \sigma_y + \sigma_z \rho \sigma_z), \qquad (14)$$

with σ_i the usual Pauli matrices. It is straightforward to show that the quantity S_{CH} is modified by the depolarizing channel as follows: $S'_{\mathrm{CH}} = 1 - \frac{4p}{3} S_{\mathrm{CH}} - \frac{2p}{3}$, where S_{CH} is given by Eq. (5). By substituting S'_{CH} in Eq. (12) we obtain the secure rate of the ent-B92 as a function of the depolarizing parameter p. The result, normalized by the total number of events detected by the users, is plotted in Fig. 2. In the same figure we also plot the secure normalized rate $\tilde{R}$ pertaining to the PM B92 protocols, that is, the standard B92 and the us-B92. In fact, they both share the same resistance against a depolarizing channel [41]. The ent-B92 rate remains positive up to $p_{\max}^{\text{ent}-\text{B92}} \simeq 0.0336$, which is about the same value known in the literature for PM-B92 ($p_{\max}^{\text{PM}-\text{B92}} = 0.034$ [2]). In obtaining these results, the optimal angle θ for the ent-B92 is nearly constant regardless of the value of p; it is 61.56° for $p = 0.01$, 62.65° for $p = 0.02$, and 63.57° for $p = 0.03$. These values of the optimal θ are quite close to those corresponding to the optimal θ for the us-B92 (about 55°) [5] and for the asymmetric feedback (about 60°) [42]. It can be noted that none of the secure rates reported in Fig. 2 starts from the value 1. This is due to the presence of inconclusive counts in all the B92-like protocols. Other DI protocols provide a better efficiency and a higher resistance to noise [12,43].

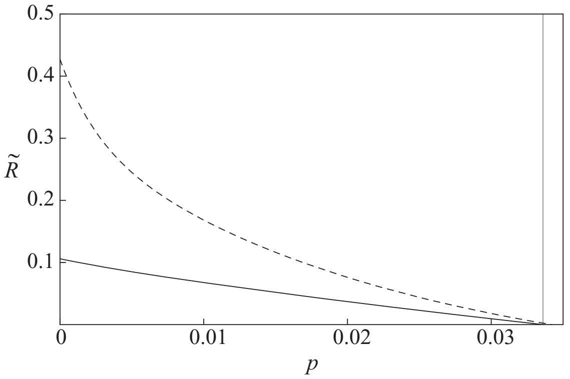

FIG. 2. Secure normalized rate pertaining to the DI entanglement-based ent-B92 (solid line) and to PM B92 and us-B92 (dashed line) as function of the depolarizing rate p (see text). The maximum depolarizing rate tolerated by the ent-B92 is $p_{\max}^{\text{ent}-\text{B92}} \simeq 0.0336$, nearly the same as PM-B92, $p_{\max}^{\text{PM}-\text{B92}} = 0.034$ [2].

It is interesting to observe that if the users perform generalized measurements thus obtaining an estimate for the quantity $S_{\mathrm{CH}}^{\max}$, this does not improve the final secure rate of the ent-B92. The problem is that in order to estimate $S_{\mathrm{CH}}^{\max}$ the user Bob has to measure along an angle θ', which is different from the angle θ characterizing the initial entangled state [Eq. (1)]. This increases the error correction term $h(\frac{n_{\mathrm{err}}}{n_{\mathrm{con}}})$ in Eq. (12), thus reducing the overall rate. In fact, we have verified that the maximum tolerated noise in this case amounts to $p \simeq 0.0234$, obtained with an angle $\theta \simeq 75°$.

C. Resistance to USD attack

The security proof of the ent-B92 is DI and covers all possible attacks performed by Eve, including the USD attack, which typically represents the most dangerous menace against B92-like protocols. In the simplest USD attack [1] Eve performs the same measurement as Bob. When she measures $|\overline{\varphi}_0\rangle$ or $|\overline{\varphi}_1\rangle$ she sends $|\varphi_1\rangle$ or $|\varphi_0\rangle$, respectively. When she measures $|\varphi_0\rangle$ or $|\varphi_1\rangle$, she does not send anything to Bob, making him detect a loss. She thus performs the following POVM: $\Pi_1 = \frac{1}{2}|\overline{\varphi}_0\rangle\langle\overline{\varphi}_0|$, $\Pi_2 = \frac{1}{2}|\overline{\varphi}_1\rangle\langle\overline{\varphi}_1|$, $\Pi_3 = \frac{1}{2}|\varphi_0\rangle\langle\varphi_0|$, $\Pi_4 = \frac{1}{2}|\varphi_0\rangle\langle\varphi_0|$. Depending on the measured Π_i, she sends to Bob the corresponding following states $|\chi_1\rangle \equiv |\varphi_1\rangle, |\chi_2\rangle \equiv |\varphi_0\rangle, |\chi_3\rangle = |\chi_4\rangle \equiv |\mathrm{vac}\rangle$, where $|\mathrm{vac}\rangle$ is the vacuum state. If such an attack is brought against the quantum communication, it alters the quantum state shared by Alice and Bob, which is no more given by Eq. (1) but becomes $\rho' = \sum_{i=1}^{4} \mathrm{Tr}_b[|\Phi\rangle_{ab}\langle\Phi|\Pi_i] \otimes |\chi_i\rangle_b\langle\chi_i|$. Since the state ρ' is separable it cannot violate any Bell inequality, including the CH inequality [Eq. (5)], thus letting the users detect the attack. It is worth noticing that this simple argument applies to any generic intercept-and-resend attack.

IV. CONCLUSION

In the present paper we have connected the long-standing B92 protocol to a particular form of Bell inequality. This allowed us to provide a simple security proof for an entanglement-based B92-like protocol which is independent of how the QKD apparatus is modeled. In the proposed protocol, called ent-B92, the same quantum states can be used either to distill the final key or to test the violation of a Bell inequality. Together with the fact that only two measurement bases are required in Alice and Bob sites, this represents a practical advantage with respect to other device-independent protocols, which have to switch between different measurement bases in order to distill secret bits or to perform a Bell test [15,44]. The gain and tolerance to noise of the ent-B92 are lower than in other device-independent protocols [12,43], but both the figures can be improved by extending to the new protocol the same techniques available for the prepare-and-measure B92 [5]. Furthermore the minimum required efficiency to run the ent-B92 is 75% if the users' efficiencies are assumed to be equal, and 50% if the source of entangled states is enclosed in Alice's territory. For other protocols [15] a value of at least 92.4% was necessary.

The ent-B92 protocol turns out to be a particular case of an entanglement-distribution problem. It originates from a nonmaximally entangled state which is distributed to two distant users. As a matter of fact, this kind of entanglement gives rise to a local nonsymmetric density matrix which can be exploited by the users to efficiently stabilize the transmission channel without any external communication [42]. This could represent an important resource when entanglement has to be distributed from a satellite or on very long distances.

A test confirming the feasibility of the ent-B92 protocol can be experimentally performed with current technology. The nonmaximally entangled state of Eq. (1) can be produced in the laboratory [17–20] and a proof-of-principle experiment is on the way.

ACKNOWLEDGMENTS

We thank K. Tamaki for fundamental discussions and Ll. Masanes, S. Pironio, and A. Acín for a feedback on their work. Our work was supported by EU-Project CHISTERAQUASAR and by PRIN 2009 of MIUR (Ministero dell'Istruzione, dell'Università e della Ricerca). M.L. was supported by the 5% Grant No. C.F. 81001910439. G.V. was partially supported by the Strategic-Research-Project QUINTET of the Department of Information Engineering, University of Padova, and the Strategic-Research-Project QUANTUMFUTURE of the University of Padova.

[1] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[2] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[3] K. Tamaki and N. Lütkenhaus, Phys. Rev. A **69**, 032316 (2004).
[4] A. Chefles, Phys. Lett. A **239**, 339 (1998).
[5] M. Lucamarini, G. Di Giuseppe, and K. Tamaki, Phys. Rev. A **80**, 032327 (2009).
[6] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
[7] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[8] X. Ma, Chi-Hang Fred Fung, and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).
[9] J. S. Bell, Physics **1**, 195 (1964).
[10] J. F. Clauser and M. A. Horne, Phys. Rev. D **10**, 526 (1974).
[11] P. H. Eberhard, Phys. Rev. A **47**, R747 (1993).
[12] Ll. Masanes, S. Pironio, and A. Acin, Nat. Commun. **2**, 238 (2011).
[13] H.-K. Lo and H. Chau, Science **283**, 2050 (1999).
[14] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[15] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New. J. Phys. **11**, 045021 (2009).
[16] L. Hardy, Phys. Rev. Lett. **71**, 1665 (1993).
[17] A. G. White, D. F. V. James, P. H. Eberhard, and P. G. Kwiat, Phys. Rev. Lett. **83**, 3103 (1999).
[18] C. Cinelli, G. Di Nepi, F. De Martini, M. Barbieri, and P. Mataloni, Phys. Rev. A **70**, 022321 (2004).
[19] G. Vallone, E. Pomarico, F. De Martini, P. Mataloni, and M. Barbieri, Phys. Rev. A **76**, 012319 (2007).
[20] G. Vallone, I. Gianani, E. B. Inostroza, C. Saavedra, G. Lima, A. Cabello, and P. Mataloni, Phys. Rev. A **83**, 042105 (2011).
[21] S. Popescu and D. Rohrlich, Phys. Lett. A **166**, 293 (1992).
[22] R. König, R. Renner, A. Bariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502 (2007).
[23] The min-entropy can be related to the trace distance by the quantum leftover hash lemma (see, e.g., [24]).
[24] M. Tomamichel, C. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[25] The *secure gain* is the probability that one initial qubit effectively becomes one bit of the final secure key distilled by the users. If multiplied by the transmission rate of the communication, the secure gain provides the *secure rate* of the secret key.
[26] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[27] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[28] G. Brassard and L. T. Salvail, Lect. Notes Comput. Sci. **765**, 410 (1994).
[29] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[30] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[31] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304 (2011).

[32] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).

[33] D. Fukuda, G. Fujii, T. Numata, K. Amemiya, A. Yoshizawa, H. Tsuchida, H. Fujino, H. Ishii, T. Itatani, S. Inoue, and T. Zama, Opt. Express **19**, 870 (2011).

[34] A. Cabello and J.-A. Larsson, Phys. Rev. Lett. **98**, 220402 (2007).

[35] N. Brunner, N. Gisin, V. Scarani, and C. Simon, Phys. Rev. Lett. **98**, 220403 (2007).

[36] X. Ma, T. Moroder, and N. Lütkenhaus, arXiv:0812.4301v1.

[37] E. Schrödinger, Math. Proc. Cambridge Philos. Soc. **31**, 555 (1935).

[38] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).

[39] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 0203 (2012).

[40] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).

[41] The only effect of the uninformative states is to make the single-photon B92 independent of losses. As far as the resistance of the B92 against noise over a lossless channel is concerned, the performances of the two protocols B92 and us-B92 are exactly the same.

[42] M. Lucamarini, R. Kumar, G. Di Giuseppe, D. Vitali, and P. Tombesi, Phys. Rev. Lett. **105**, 140504 (2010).

[43] E. Hänggi and R. Renner, arXiv:1009.1833v2.

[44] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).