In quantum direct communication an undetectable eavesdropper can always tell Ψ from Φ Bell states in the message mode

Mladen Pavičić*

Department of Physics–Nano-optics, Faculty of Mathematics & Natural Science I, Humboldt University of Berlin, Germany and Chair of Physics, GF, University of Zagreb, Croatia

(Received 8 November 2012; published 22 April 2013)

We show that in any quantum direct communication protocol that is based on Ψ and Φ Bell states, an eavesdropper can always tell Ψ from Φ states without altering the transmission in any way in the message mode. This renders all protocols that make use of only one Ψ state and one Φ state completely insecure in the message mode. All four-Bell-state protocols require a revision and this might be of importance for new implementations of entanglement-based cryptographic protocols. The detection rate of an eavesdropper is 25% per control transmission, i.e., a half of the rate in the two-state (ping-pong) protocol. An eavesdropper can detect control probes with certainty in the standard control transmission without a photon in the Alice-to-Bob's travel mode and with near certainty in a transmission with a fake photon in the travel mode. Resending of measured control photons via the travel mode would make an eavesdropper completely invisible.

DOI: 10.1103/PhysRevA.87.042326 PACS number(s): 03.67.Hk, 03.67.Ac, 03.67.Dd, 42.50.Ex

I. INTRODUCTION

Today, cryptography mostly relies on the conjectured but unproven assumption that there is no polynomial algorithm for factorization of large numbers. Therefore, secure and unbreakable communication schemes based on the quantum physical properties of the information carriers are clearly preferable. Single-photon quantum key distribution (QKD) protocols have already been implemented in the U.S., Europe, and Japan. However, the present single-photon implementations have to be redesigned because it was "demonstrated experimentally that...it [is] possible to tracelessly acquire the full secret key [with] an eavesdropping apparatus built from off-the-shelf components...The attack is surprisingly general [since] all commercial QKD systems and the vast majority of research systems use avalanche photodiodes-based detectors...[Our] findings clearly show the necessity of investigating the practical security of QKD [1]."

On the other hand, although it has been widely accepted that "[the] security of the key can in principle be guaranteed without putting any restriction on an eavesdropper's power [2]," the following reference shows that polarization-coded quantum key distribution protocols with single photons are insecure against attacks from technology in the far future. Brun *et al.* have shown that had Eve an access to *closed timelike curves*, she would be able to "learn the basis and bit values of each state [within a BB84 protocol] (and then prepare an identical state) without introducing any loss or disturbance in the quantum transmission [3]." We say "far future" because today no observer actually has access to closed timelike curves and, therefore, they are not a realistic threat for technology today or in the near future.

Also, the following references show that the technology from the near future will at least impose very demanding conditions to achieve the required level of privacy amplification for a secure transmission. Brandt [4,5] and Shapiro and co-workers [6,7] have considered single CNOT gate attacks feasible in the near future. Eve makes use of a CNOT whose target photons have polarizations in directions rotated for 22.5° with respect to H,V and +45° (D, diagonal) and −45° (A, antidiagonal) orientations of photons in two BB84 bases. In this way, she obtains maximal Rényi information equal to 1 for the error probability her eavesdropping creates that is equal to 1/3.

The above examples show that a disadvantage of protocols with single photons is that they have definite polarizations in some bases and that it would be viable to reexamine protocols based on entangled photons which are genuinely unpolarized to see how reliable they can be.

The first proposal of an entangled-photon-based QKD implementation was put forward in 1991 by Ekert [8] and a number of experiments have been carried out since [9].

A different kind of proposal with entangled photons was put forward in 2002 by Boström and Felbinger [10] and an experiment was carried out in 2008 [11]. It was designed to enable the *quantum (secure) direct communication* (QDC) for sending long and not-so-sensitive messages directly, thus avoiding a communication overhead. But it can also be used for an alternative implementation of QKD.

Many kinds of QDC protocols have been proposed since 2002, but we will mention only those that make use of the Bell states. Boström and Felbinger proposed two-Bell-state deterministic QDC using entanglement (also called a *ping-pong protocol* [10,12]); Long and Liu proposed a four-Bell-state QDC protocol [13]; Deng *et al.* proposed a four-Bell-state two-step QDC [14]; Cai and Li proposed a four-Bell-state extension of the ping-pong QDC [15]; Wang *et al.* proposed a four-Bell-state QDC with high-dimension quantum superdense coding [16]; Zhu *et al.* proposed a four-Bell-state QDC based on secret transmitting order of particles [17]; Lee *et al.* proposed a QDC with authentication (control) carried out by a third party by means of Greenberger-Horne-Zeilinger (GHZ) states [18–20]; Yen *et al.* proposed a QDC with mutual authentication with four Bell states [21]; Liu *et al.* proposed a two-Bell-state (Ψ and Φ) protocol [22]; Zhang *et al.* proposed another two-Bell-state (Ψ and Φ) protocol [23]; and QDC proposals with a higher number of qubits (up to six) using Bell states [24–26] have also been proposed.

*pavicic@grad.hr

Therefore, we think it is important to know the limitations of QDC protocols regarding possible future implementations and, in this paper, we show the following: (a) In any QDC protocol which makes use of one of $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)$ and one of $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)$ Bell states (e.g., [22,23] mentioned above), Eve can read off all messages without being detected in the message mode, even when there are no losses in the channels. (b) In any QDC protocol which makes use of all four Bell states (e.g., all the others mentioned above), Eve can tell Ψ from Φ states without being detected in the message mode, even when there are no losses in the channels. This issue [point (b)] is the most important result of the paper; point (a) only indicates that the two-state Ψ–Φ protocol should not be attempted at all.

In obtaining our main result, we shall make use of a modification of Wójcik's attack [27] on the Boström-Felbinger ping-pong protocol [10].

II. MESSAGE MODE

A *message mode* in a QDC protocol is a mode in which Alice sends messages to Bob, in contrast to the *control mode* in which Alice and Bob attempt to catch Eve and which we are going to elaborate on in the next section [10].

A schematic of the protocol and Eve's attack is given in Fig. 1. Bob prepares entangled-photon pairs in the $|\Psi^{-}\rangle_{ht}$ state. From each pair, he keeps one (*home*) photon and sends the other (*travel*) photon to Alice. Eve prepares two auxiliary modes (x and y) with one ancilla photon in the state $|\mathrm{vac}\rangle_x|H\rangle_y$, where $|\mathrm{vac}\rangle$ denotes the empty mode and applies the travel photon to them. The part of the figure denoted as the CD (control device), which includes optical switches, is only relevant for the control mode elaborated in the next section. Here we assume that all photons go through optical switches (os) to the last $Q^{\dagger}$ box as if the CD were not there.

The state of the whole system is

$$|in\rangle_{htxy} = |\Psi^{-}\rangle_{ht}|\mathrm{vac}\rangle_x|H\rangle_y. \tag{1}$$

We represent any ket by a 3×1 matrix: first row, H; second row V; third row, vac. The tensor products $|\cdot\rangle_t|\cdot\rangle_x|\cdot\rangle_y$ are represented by $3^3 \times 1 = 27 \times 1$ Kronecker products. Making use of such matrices with the help of appropriate software such as MATHEMATICA is very handy, in particular for operations with 27×27 Q and $Q^{\dagger}$ matrices below.

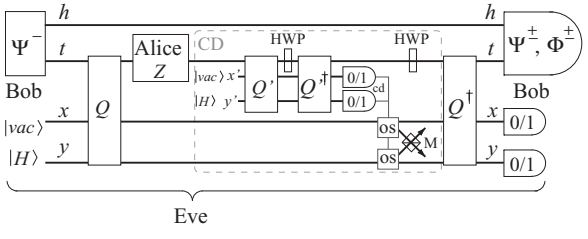

FIG. 1. Schematic of eavesdropping on the four-state direct communication; h and t denote the home and travel photons, respectively; x and y denote the auxiliary modes. The Z operators describe Alice's actions on photons in t mode; os are optical switches. The control device (CD) redirects paths x, y only in the control mode. In the message mode, photons flow from the first Q box to the last $Q^{\dagger}$ box as if the CD were not there. The half-wave plate (HWP) ($\pi/4$) flips the polarization of the t photon; cd are control detectors.

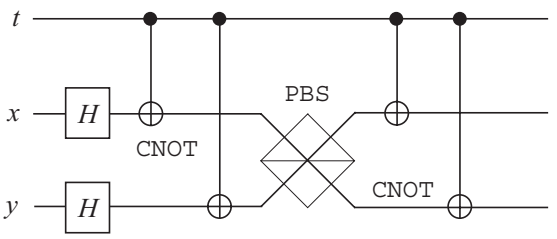

FIG. 2. Circuit representation Q_{txy} given by Eq. (2).

Our Eve attacks Alice's channel with a modification of Wójcik's attack [27]. As shown in Fig. 2, she will apply a series of gates to the input state given by Eq. (1). However, she will not use Wójcik's swap. Also, she is adding an additional Hadamard gate to the x mode.

Eve first applies Hadamard gates to the x and y mode, then two CNOT gates, a polarizing beam splitter (PBS) gate, and two more CNOT gates (Q is represented by a $3^3 \times 3^3$ matrix):

$$\begin{aligned} Q_{txy} = {} & \mathrm{CNOT}_{ty}(\mathrm{CNOT}_{tx} \otimes I_y)(I_t \otimes \mathrm{PBS}_{xy}) \\ & \times \mathrm{CNOT}_{ty}(\mathrm{CNOT}_{tx} \otimes I_y)(I_t \otimes H_x \otimes H_y), \end{aligned} \tag{2}$$

where I stands for a unit operator and CNOT_{ty} stands for a controlled NOT operator with a control qubit in mode t and a target qubit in mode y in the 27 dim space txy. Explicitly, CNOT_{ty} is represented by a 27×27 matrix with diagonal elements $d(16,16) = d(17,17) = 0$ and the other diagonals $= 1$, and off-diagonal elements $o(16,17) = o(17,16) = 1$ and the other off-diagonals $=0$. It acts on ty kets as follows: $\mathrm{CNOT}_{ty}|H\rangle_t|H\rangle_y = |H\rangle_t|H\rangle_y$, $\mathrm{CNOT}_{ty}|H\rangle_t|V\rangle_y = |H\rangle_t|V\rangle_y$, $\mathrm{CNOT}_{ty}|V\rangle_t|H\rangle_y = |V\rangle_t|V\rangle_y$, and $\mathrm{CNOT}_{ty}|V\rangle_t|V\rangle_y = |V\rangle_t|H\rangle_y$.

The PBS gate lets horizontally polarized photons through and reflects the vertically polarized ones. The gate is taken from [27]. It acts on xy kets as follows: $\mathrm{PBS}|\mathrm{vac}\rangle_x|H\rangle_y = |H\rangle_x|\mathrm{vac}\rangle_y$, $\mathrm{PBS}|\mathrm{vac}\rangle_x|V\rangle_y = |\mathrm{vac}\rangle_x|V\rangle_y$, $\mathrm{PBS}|H\rangle_x|\mathrm{vac}\rangle_y = |\mathrm{vac}\rangle_x|H\rangle_y$, and $\mathrm{PBS}|V\rangle_x|\mathrm{vac}\rangle_y = |V\rangle_x|\mathrm{vac}\rangle_y$. Since there is only one photon in the x,y modes, there are no other combinations.

Applied to the initial Eve's state given by Eq. (1), the operator Q_{txy} yields the following state:

$$\begin{aligned} |B-A\rangle &= Q_{txy}|in\rangle_{htxy} \\ &= \tfrac{1}{2}|H\rangle_h(|V\rangle_t|V\rangle_x|\mathrm{vac}\rangle_y + |V\rangle_t|\mathrm{vac}\rangle_x|H\rangle_y) \\ &\quad - \tfrac{1}{2}|V\rangle_h(|H\rangle_t|H\rangle_x|\mathrm{vac}\rangle_y + |H\rangle_t|\mathrm{vac}\rangle_x|V\rangle_y). \end{aligned} \tag{3}$$

We see that all travel photons sent by Bob reach Alice. Alice prepares $|\Psi^{\pm}\rangle_{ht}$ and $|\Phi^{\pm}\rangle_{ht}$ by means of the following operators:

$$\begin{aligned} Z^{(\Psi^{\pm})} &= |V\rangle_{t\,t}\langle V| \mp |H\rangle_{t\,t}\langle H|, \\ Z^{(\Phi^{\pm})} &= \pm(|H\rangle_{t\,t}\langle V| \mp |V\rangle_{t\,t}\langle H|), \end{aligned} \tag{4}$$

and send it further along mode t. $Z^{(\Psi^{-})}$ plays a role of an identity operator for polarizations in mode t and corresponds to Alice's "doing nothing" to prepare $|\Psi^{-}\rangle$.

Now Eve acts on $Z|B-A\rangle$ by means of her devices in a reverse order and therefore described by $Q^{\dagger}_{txy}$,

$$|A-B^{(\Psi^{\pm})}\rangle = Q^{\dagger}_{txy}Z^{(\Psi^{\pm})}|B-A\rangle = |\Psi^{\pm}\rangle_{ht}|\mathrm{vac}\rangle_x|H\rangle_y,$$
$$|A-B^{(\Phi^{\pm})}\rangle = Q^{\dagger}_{txy}Z^{(\Phi^{\pm})}|B-A\rangle = \mp|\Phi^{\pm}\rangle_{ht}|H\rangle_x|\mathrm{vac}\rangle_y. \tag{5}$$

In this way, Eve knows that a click of her y detector means either $|\Psi^{+}\rangle$ or $|\Psi^{-}\rangle$ and a click of her x detector means either $|\Phi^{+}\rangle$ or $|\Phi^{-}\rangle$. Also, Eve is completely hidden here.

Undetectability of Eve is proven by Eq. (5), which shows decoupling of Eve's ancillas from the home and the travel qubit. This can be intuitively understood by looking at Eq. (2) and Fig. 2. We see that Alice's photons only interact with Eve's ancillas by means of Eve's CNOT gates. Since they enter CNOTs only as control qubits, and since Alice's and Bob's photons disentangle after interaction, Alice and Bob cannot detect Eve.

Only by setting CNOTs so as to have Alice's photons as their targets would Eve leave some traces of her hacking. This is what Wójcik [27] used for his attack when he applied his SWAP. But we do not make use of a SWAP gate and therefore Eve is undetectable independently of which particular protocol from the literature we consider.

Here, we stress that since Eve does not change any state of any of Alice's message photons and can detect Alice's control probes, she will not attempt to implement a denial-of-service attack [28] because such an attack does not provide her with any information and can only reveal her (cf. [12]).

III. CONTROL MODE

As we mentioned above, the *control mode* is for catching Eve. In it, Alice simply measures some randomly chosen photons. Bob does the same and, by comparing their outcomes, they can see whether Eve corrupted any of their pairs. Since the input is $|\Psi^{-}\rangle$, their photons should be perpendicularly polarized. Parallel polarization would indicate Eve's presence.

Alice and Bob can adopt two main scenarios of the control mode: a *standard* one, which is almost exclusively used in the literature, and a *cloning* one, in which Alice forwards clones of some or all of her measured photons. In the former scenario, there is no photon in the travel mode, and in the latter one, there is.

A. No photon in the travel mode

To lower the probability of being caught, Eve devised a device [control device (CD), in Fig. 1] which enables her to detect the control mode and manipulate her ancilla in a different way than in the message mode.

Alice's detection of Bob's photon for Eve means that there will be no photon in her $Q^{\dagger}$ box. She can detect the absence of the photon as follows. Eve knows that the action of Q and then of $Q^{\dagger}$ would leave the same state, $|\Psi^{\mp}\rangle$ or $|\Phi^{\mp}\rangle$, unchanged. So, she puts Q' and $Q'^{\dagger}$ boxes in the path of the travel photon. The Q boxes and Q' boxes are identically built.

When there is no photon coming into the Q' box, the input reads [cf. Eq. (1)]

$$|in\rangle_{\mathrm{vac},x'y'} = |\mathrm{vac}\rangle_t|\mathrm{vac}\rangle_{x'}|H\rangle_{y'}. \tag{6}$$

Instead of Eq. (3), we obtain

$$|B-A\rangle_{\mathrm{control}} = Q'_{tx'y'}|in\rangle_{\mathrm{vac}\,x'y'}$$
$$= \frac{1}{\sqrt{2}}|\mathrm{vac}\rangle_t(|H\rangle_{x'}|\mathrm{vac}\rangle_{y'} + |\mathrm{vac}\rangle_{x'}|V\rangle_{y'}). \tag{7}$$

Now, letting x',y' photons through $Q'^{\dagger}$ gives the same output for unchanged travel photon and for no travel photon ($|\mathrm{vac}\rangle_t$). So Eve puts a half-wave plate, HWP $(\pi/4)=\sigma_x$ (Pauli matrix), in the path of the travel photon. It flips the polarization of the travel photon $H \leftrightarrow V$ (when there is one present—in the message mode or in the control mode with cloned photons) so that we have $|\Psi^{\pm}\rangle \leftrightarrow |\Phi^{\pm}\rangle$. After that, the travel photon (together with Eve's ancilla) passes through the $Q'^{\dagger}$ box and Eve will detect $|H\rangle_{x'}|\mathrm{vac}\rangle_{y'}$, as in the second line of Eq. (5). The optical switches stay inactive. Eve flips the polarization of travel photons once again (in the message mode or in the control mode with cloned photons) by means of the second HWP and the travel photons reach the $Q^{\dagger}$ box in the state Alice prepared them in.

When there is no photon in the travel mode, in the control mode Eve will detect $|\mathrm{vac}\rangle_{x'}|H\rangle_{y'}$ instead of $|H\rangle_{x'}|\mathrm{vac}\rangle_{y'}$ that she would have detected if a photon had been in the travel mode:

$$|A-B^{\mathrm{vac}}\rangle_{\mathrm{control}} = Q^{\dagger}_{txy}|B-A\rangle_{\mathrm{control}} = |\mathrm{vac}\rangle_t|\mathrm{vac}\rangle_{x'}|H\rangle_{y'}. \tag{8}$$

That activates optical switches (os in Fig. 1), which redirect paths of her ancilla to a polarizing beam splitter M in Fig. 1.

The tripartite state describing Bob's photon, Alice's photon—before she measures it, and Eve's ancilla will read

$$|B-A\rangle_{\mathrm{os}} = \tfrac{1}{2}|H\rangle_h|V\rangle_t(|V\rangle_x + |H\rangle_y)$$
$$-\tfrac{1}{2}|V\rangle_h|H\rangle_t(|H\rangle_x + |V\rangle_y), \tag{9}$$

which is actually Eq. (3) where we omitted $|\mathrm{vac}\rangle$ states to simplify the notation.

Three photons in h, t, x, and y modes are therefore entangled before Alice carries her measurement. Alice can carry out her measurement in the $|H\rangle_t,|V\rangle_t$ basis or in the $|H\rangle_t \pm |V\rangle_t$ basis. In the former basis, Alice disentangles Bob's photons from Eve's ancillas and he obtains perfect anticorrelation. Let, e.g., Alice measure a vertical polarization $|V\rangle_t$ (non-normalized):

$${}_t\langle V|B-A\rangle_{\mathrm{os}} = |H\rangle_h(|V\rangle_x + |H\rangle_y). \tag{10}$$

Alice's measurement of $|H\rangle_t$ yields

$${}_t\langle H|B-A\rangle_{\mathrm{os}} = |V\rangle_h(|H\rangle_x + |V\rangle_y). \tag{11}$$

This disentangles Bob's photons from Eve's ancillas. Eve's measurement would provide her with full information on Bob's subsequent outcome determined by Alice's measurement if Alice performed her measurements only in the H_t,V_t basis. Knowing that, Alice will also perform her measurements in the $|H\rangle_t \pm |V\rangle_t$ basis.

In the latter basis, Alice measures, say, a diagonal polarization $|D\rangle_t = \frac{1}{\sqrt{2}}(|H\rangle_t + |V\rangle_t)$. (She cannot predetermine it, but let us assume she obtained the "+" sign.) We obtain

(non-normalized)

$$({}_t\langle H| + {}_t\langle V|)|\mathrm{B}-\mathrm{A}\rangle_{\mathrm{os}} = |H\rangle_h(|V\rangle_x + |H\rangle_y) - |V\rangle_h(|H\rangle_x| + |V\rangle_y). \quad (12)$$

When the photons pass through the polarizing beam splitter M, Eqs. (10)–(12) yield

$$\begin{aligned} &|H\rangle_h(|V\rangle_x + |H\rangle_x),\ \ |V\rangle_h(|H\rangle_y + |V\rangle_y),\\ &|H\rangle_h(|V\rangle_x + |H\rangle_x) - |V\rangle_h(|H\rangle_y| + |V\rangle_y), \end{aligned} \quad (13)$$

respectively.

We then let x and y modes through Hadamard gates (not shown in the figure; a gate in each mode) to obtain (for all four states in both bases)

$$|H\rangle_h|H\rangle_x,\ \ |V\rangle_h|H\rangle_y,\ \ |H\rangle_h|H\rangle_x \mp |V\rangle_h|H\rangle_y, \quad (14)$$

respectively.

In the diagonal basis, for Alice's aforementioned choice, Bob can measure both $|A\rangle_h = |H\rangle_h - |V\rangle_h$ and $|D\rangle_h = |H\rangle_h + |V\rangle_h$ states. The former measurement will project Eve's ancilla state into $|H\rangle_x + |H\rangle_y$ and the latter into $|H\rangle_x - |H\rangle_y$. Bob will know with a probability of 50% (for the diagonal choice; together with the $|H\rangle_t, |V\rangle_t$ basis, 25%) that Eve is in the line.

So, the biggest gain Eve will have in the standard control mode without a photon in the Alice-to-Bob's travel mode is that she will know that Alice switched to the control mode with certainty before Bob receives Alice's information over a classical public channel. As soon as she detects a probe, Eve can decide to decouple from the line before Alice and Bob had any realistic chance to detect her with any certainty, even in the case when Bob delays measuring his qubits to allow several subsequent Alice's measurements before he starts measuring any of them. In every realistic communication, there are wrong readings because of misalignments of analyzers, dark counts, multiple (more than one) photons in the line due to their statistical generation at the source, etc. So, Alice and Bob cannot allow themselves to abort the protocol each time they obtain a click that might indicate that Eve is in the line. One in four control probes per control transmission might reveal Eve and, if she decouples after the first one, Alice and Bob will not switch the protocol off even if they obtain an indication of Eve's presence, and Eve can resume her eavesdropping soon enough.

Alice and Bob cannot increase their 25% probability of discovering Eve by staying only in the diagonal basis because Eve would then rotate her ancilla to it and would become completely invisible.

The details of this are as follows. In the message mode, it is irrelevant in which direction Eve's target ancilla $|H\rangle$ is oriented, since the home and travel qubits are entangled and the travel qubit itself is in superposition of $|H\rangle$ and $|V\rangle$. However, Eve has to take the control mode into account and therefore she chooses the orientation of her $|H\rangle$ so as to coincide with the $|H\rangle$ that Alice and Bob use in their control mode. They have to agree on the orientation of their $|H\rangle$ either beforehand or over a public classical channel and Eve will know that. As shown above, if Alice and Bob used only the $H - V$ basis, they cannot detect Eve because then Eve's ancillas disentangle from Bob's photons. Even if Alice and Bob managed to keep secret which of their orientations is actually their preferred basis, Eve can easily discover it either by letting her ancillas through multiple M devices or through a device introduced in Sec. III B.

Alice and Bob can detect Eve in the $D - A$ basis provided Eve stays in the $H - V$ basis. But if they chose to stay in the $D - A$ basis forever, Eve will know that because Alice and Bob must agree on the policy of the protocol. Then she will simply rotate her target ancilla for 45°. We can easily calculate that by making use of a $|V\rangle$ target ancilla; Eve obtains $|\mathrm{vac}\rangle_x|V\rangle_y$ and $|V\rangle_x|\mathrm{vac}\rangle_y$ instead of $|\mathrm{vac}\rangle_x|H\rangle_y$ and $|H\rangle_x|\mathrm{vac}\rangle_y$ in Eq. (5). Therefore, if Eve used target ancillas in the diagonal basis, they would disentangle from Bob's qubits whenever Alice carries her measurement in the very same basis, in the same way in which ancillas disentangle from Bob's home qubit in Eqs. (10) and (11) in the $H - V$ basis. In conclusion, if they all stayed in the same basis, Eve would be invisible and, therefore, Alice and Bob would be forced to change the bases randomly. (Eve might decide to change the bases for ancilla randomly as well.)

This is to Bob and Alice's disadvantage since they not only have a 25% probability to detect Eve, but also must introduce either long delays in announcing their results or make use of a postselection of randomly made measurements, which means discarding at least 50% of the data and which further reduces their probability to 12.5%.

B. Photon in the travel mode

Can Alice avoid providing Eve with information about her sending successful control probes by cloning her measured photons and sending them to Bob via travel mode? Alice can try to do this so as to clone every photon as she measured it or to always send a photon in a chosen state, say in state $|H\rangle$, no matter what she obtains by measurement (she will send the outcome of her measurement to Bob via a public channel, though). The answer to our question is in the negative for both kinds of cloning.

In the former kind of cloning every photon as measured, the travel photon goes through Eve's CD device and through her $Q^\dagger$ box, which detaches her ancilla from Bob's home photon, as the following calculations show. For Alice's measurements and cloning in the $|H\rangle_t, |V\rangle_t$ basis, we obtain

$$\begin{aligned} &Q^\dagger_{txy}|H\rangle_{tt}\langle H|B - A\rangle = |V\rangle_h|H\rangle_t|\mathrm{vac}\rangle_x|H\rangle_y,\\ &Q^\dagger_{txy}|V\rangle_{tt}\langle V|B - A\rangle = |H\rangle_h|V\rangle_t|\mathrm{vac}\rangle_x|H\rangle_y. \end{aligned} \quad (15)$$

Therefore, for Alice's measurement and cloning in the $|H\rangle_t \pm |V\rangle_t$ basis, we also obtain $|\mathrm{vac}\rangle_x|H\rangle_y$. Eve will not be able to distinguish between such control data and the data she eavesdropped over the message mode, but she will be able to discard the control data after listening to Alice's announcements over a classical public channel, later on.

Hence, by adopting a strategy of cloning of all Alice's photons, Alice and Bob would actually make Eve completely invisible in both the message and control modes. So, the answer to our question is here in the negative simply because there are no successful control probes.

The latter approach taken by Alice is to always send a photon in state $|H\rangle$ via the travel mode. Therefore, instead of Eq. (15) we get Eq. (16),

$$Q^\dagger_{txy}|H\rangle_{tt}\langle H|B - A\rangle = |V\rangle_h|H\rangle_t|\mathrm{vac}\rangle_x|H\rangle_y,$$

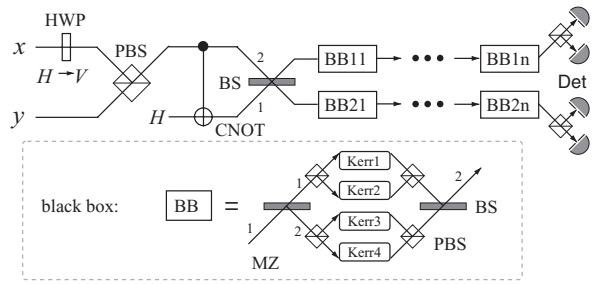

FIG. 3. Schematic of Eve's discriminating message photons from control photons. HWP ($\frac{\pi}{4}$), represented by the Pauli matrix σ_x, flips the polarization; BS is a beam splitter; PBS is a polarizing beam splitter. MZ is a Mach-Zehnder interferometer, Kerr is a nonlinear switch, and Det means a detector.

$$Q^{\dagger}_{txy}|H\rangle_{tt}\langle V|B-A\rangle = |H\rangle_h|H\rangle_t|H\rangle_x|\mathrm{vac}\rangle_y, \tag{16}$$

and in the $|H\rangle_t \pm |V\rangle_t$ basis, we obtain

$$\begin{aligned} Q^{\dagger}_{txy}|H\rangle_{tt}\langle H \pm V|B-A\rangle &= |V\rangle_h|H\rangle_t|\mathrm{vac}\rangle_x|H\rangle_y \\ &\mp |H\rangle_h|H\rangle_t|H\rangle_x|\mathrm{vac}\rangle_y, \end{aligned} \tag{17}$$

i.e., Eve's ancilla remains entangled with Bob's photon and Bob has 50% probability of detecting Eve in the latter basis, which is 25% per control transmission.

However, Eve can again detect Alice's probes in the diagonal basis with near certainty. She will make use of the device shown in Fig. 3 placed after the $Q^{\dagger}$. The device will not discriminate between the states of photons in the message mode and in the states of photons in the control mode in the $|H\rangle,|V\rangle$ basis [shown in Eq. (16)]. But again Eve will be able to discard the received control data after listening to Alice's announcements over a classical public channel, later on. Also, Eve is invisible to the probes in the $|H\rangle,|V\rangle$ mode since, as we can see from Eq. (16), they do not entangle with Eve's ancilla. Therefore, we shall only analyze how the probes in the diagonal basis behave in the device and compare it with the behavior of the photons in the message mode in it.

The half-wave plate (HWP) flips $|H\rangle$ in the x mode into $|V\rangle$. Thus, the message ancilla $|H\rangle_x$ exit the polarizing beam splitter (PBS) in the state $|V\rangle$ and the message ancilla $|H\rangle_y$ in the state $|H\rangle$. The control ancillas from Eq. (17) exit the PBS in the state $|H\rangle \pm |V\rangle$. They pass the CNOT gate as follows: $|V\rangle_x \to |V\rangle_1|V\rangle_2$, $|H\rangle_y \to |H\rangle_1|H\rangle_2$, and $|H\rangle_y \pm |V\rangle_x \to |V\rangle_1|V\rangle_2 \pm |H\rangle_1|H\rangle_2$, respectively.

They exit the beam splitter (BS) in the NOON states [29,30] (non-normalized),

$$\begin{aligned} &|H\rangle_1|H\rangle_1 - |H\rangle_2|H\rangle_2, \quad |V\rangle_1|V\rangle_1 - |V\rangle_2|V\rangle_2, \\ &|H\rangle_1|H\rangle_1 - |H\rangle_2|H\rangle_2 \mp |V\rangle_1|V\rangle_1 \pm |V\rangle_2|V\rangle_2, \end{aligned} \tag{18}$$

respectively.

We cannot deterministically discriminate the third state in Eq. (18) from the first two in a single step with linear optics elements, but we can do so near-deterministically with nonlinear all-optical switches based on Kerr interaction (Kerr switches). The switches perform nondemolition measurements. They detect a single photon but do not react to two photons. The measurement preserves the coherence and the state is available for further manipulations afterwards. [31] A Kerr switch is a kind of a Fock filter. It can be designed as a ring cavity containing a nonlinear crystal with a third-order susceptibility which is coupled to the photon mode we want to test. A cross-phase modulation imposes a phase shift proportional to the number of coupled photons onto the cavity mode. The phase shift can be measured so as to discriminate between a single photon and two photons in the coupled mode. Further details and references can be found in Ref. [31]. We stress here that Kerr switches are not more technologically demanding than the discrimination of all four Bell states, which is required by the four-state QDC protocol that is considered in the literature, and neither one of these two sophisticated technologies is implementable today.

At the first BS of the Mach-Zehnder interferometer (MZ) in the first two black boxes (BB1, BB2), the message- and control-generated photon pairs transform as follows (non-normalized) [29,30,32–34]:

$$\begin{aligned} &|H\rangle_1|H\rangle_1 \to |H\rangle_1|H\rangle_1 - 2|H\rangle_1|H\rangle_2 + |H\rangle_2|H\rangle_2, \\ &|V\rangle_1|V\rangle_1 \to |V\rangle_1|V\rangle_1 - 2|V\rangle_1|V\rangle_2 + |V\rangle_2|V\rangle_2, \\ &|H\rangle_1|H\rangle_1 \mp |V\rangle_1|V\rangle_1 \\ &\quad \to |H\rangle_1|H\rangle_1 \mp |V\rangle_1|V\rangle_1 - 2(|H\rangle_1|H\rangle_2 \mp |V\rangle_1|V\rangle_2) \\ &\quad -|H\rangle_2|H\rangle_2 \pm |V\rangle_2|V\rangle_2. \end{aligned} \tag{19}$$

Bunched photons (e.g., $|H\rangle_1|H\rangle_1$) will not trigger the Kerr switches, but antibunched ones (e.g., $|H\rangle_1|H\rangle_2$) will. The latter triggering happens with the probability of 50% for all three states. So we must have a sequence of black boxes (BBs), in each of which we attempt to detect antibunched photons by means of Kerr switches. All of the photons exit each of the BBs (MZs) in the same state in which they entered them [29,30].

Since the Kerr switches do not discriminate polarization, we split the photons into two spatial modes H and V inside each MZ by means of PBSs. After passing through Kerr switches, they are recombined with the help of another PBS. (These splittings and recombinations do not affect the fourth-order interference in any way, provided the paths are equal.) In Table I, we show all possible outcomes of Kerr switches. Note that the detectors Det at the far right of Fig. 3 will show either $2 \times H$ or $2 \times V$ for $|H\rangle_x \pm |H\rangle_y$, so without Kerr detections, these states cannot be discriminated from $|H\rangle_x$ or $|H\rangle_y$ in a single step.

What enables Eve to near-deterministically discriminate the states in one step is the following. The Kerr switches, Kerr1 and Kerr4, detect passages of H and H, respectively, whenever an antibunched photon state $|H\rangle_1|H\rangle_2$, which is contained in the state originated from $|H\rangle_y$ and shown in Eq. (19), triggers them. Photons in the state originated from $|H\rangle_y$ cannot trigger

TABLE I. Possible measurement outcomes of Kerr switches from Fig 3.

	Outcomes of Kerr switches			
	1	2	3	4
$\|H\rangle_x$		V	V	
$\|H\rangle_y$	H			H
$\|H\rangle_x \pm \|H\rangle_y$	H			H
$\|H\rangle_x \pm \|H\rangle_y$		V	V	

Kerr2 and Kerr3. They are triggered by photons originated from $|H\rangle_x$ (i.e., by $|V\rangle_1|V\rangle_2$).

Photons coming as $|H\rangle_x \pm |H\rangle_y$ can trigger all four Kerr switches and, after sufficiently many BBs, they will do so near-certainly. In a sequence of four BBs, they will trigger a different pair of Kerr switches (either Kerr1 and Kerr4 or Kerr2 and Kerr3) with a probability of 25%. As soon as this happens, Eve knows with certainty that Bob and Alice are checking on her with control photons. How many Kerr switches Eve will implement depends on how certain she wants to be, on average. The probability that Eve would detect every control probe grows rapidly with the number m of such four-Kerr-switch sequences,

$$p = 1 - 0.75^m, \tag{20}$$

e.g., for $m = 17$, $p < 1\%$. At first glance, this looks like many elements, but they are matched by more than 1000 linear optics elements required for equally nearly deterministic discrimination of all four Bell states in the KLM (Knill-Laflamme-Milburn) approach [35].

IV. SECURITY

In the standard control mode without a photon in the Alice-to-Bob's travel mode (used by almost all QDC protocols), Eve will know with certainty when Alice decided to switch to the control mode. Then Eve might decide to decouple from the line before Alice and Bob are sure she was there. Alice and Bob cannot attempt to increase their 25% probability of discovering Eve by staying with the diagonal basis because Eve would then switch her ancilla to the same basis, would be able to detect their probes with certainty, and would become completely invisible.

In a possible realistic application, a 50:50 message-to-control ratio (to discover Eve fast enough) would be unacceptably high and, on the other hand, Eve could decouple after only one probe, thus minimizing her chances of being discovered. That makes all QDC protocols with four Bell states vulnerable. In the standard realistic applications with a lossy channel, we can assume that Alice and Bob would not be able to discover Eve after one or two control transmissions.

We can estimate how much information Eve could snatch before Alice and Bob decide to shut down the communication channel as follows. Let us assume that they abort the protocol when the probability of Eve's presence reaches 75%. The probability of Alice and Bob having correlated instead of anticorrelated results is one in four attempts: 0.25. Let us next assume that there is one set of control-mode verifications (four different probes) per ten bytes. Bob's probability should be reached after n complete verifications:

$$0.75 = 1 - \left(\tfrac{3}{4}\right)^n \quad \Rightarrow \quad n \approx 5. \tag{21}$$

This amounts to 50 leaked bytes—a short telegram. So, Eve can decouple with, say, 45 caught bytes without making Alice and Bob abort the communication.

Another possible way of implementing a *control mode* in other protocols is by means of Alice's sending an announced message (with a delay), say $|\Psi^-\rangle$. Bob carries out a measurement on both qubits and compares it with Alice's announcement. In our case, this will not reveal Eve either because her Q boxes just let all of Alice's photons through unchanged.

A way of detecting Eve that is often used in standard cryptographic protocols is checking the quantum bit error rate (QBER—the average probability of a bit flip in received messages, i.e., a probability that Bob's measurement yields an incorrect result). Since our Eve does not leave any trace in the message mode, the QBER with or without her will be the same.

Now, an important question here is whether Eve can tell $|\Psi^+\rangle$ from $|\Psi^-\rangle$ or $|\Phi^+\rangle$ from $|\Phi^-\rangle$ in an analogous way. We tried a number of combinations of CNOT and other gates and did numerical calculations for them, but have not found any indication that Eve can obtain any information about messages within the Ψ or Φ bundles. Only when making use of the gates that have photons in the travel mode as their target qubits can Eve extract such information. But that amounts to a SWAP gate and that would reveal her. Such a SWAP gate was used by Wójcik. [27].

The security breaching can be elaborated on and patched as follows. Alice and Bob share two bits (four messages: $|\Psi^-\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$, and $|\Phi^+\rangle$), therefore, their maximal mutual information is also two bits. (In the original two-state ping-pong protocol, it is one bit.) Mutual information between Alice and Eve is one bit—0.5 bits for detecting Ψ messages and 0.5 for Φ ones. This means that the security verifications and estimations carried out in the aforementioned references should be reworked to include this additional one bit of Alice-Eve's mutual information. That, e.g., changes the Holevo efficiency calculated in the references (e.g., [28]). Alice-Eve's one bit should be taken as one additional classical bit in the Holevo efficiency.

The main remedy against discriminating between the Ψ and Φ Bell state is encoding mutually uncorrelated information in each of them because otherwise Eve can then crack them by a lexicographic algorithm. That does not mean that any four-Bell-state QDC protocol is only as secure as two separated two-state ping-pong protocols. It can be shown that a transfer will be more secure when two streams are bundled simultaneously together, but that is outside of the scope of this paper.

V. CONCLUSION

Taken together, we have shown that in any QDC protocol, Eve can tell Ψ from Φ Bell states without ever being detected in the message mode, even when there are no losses in the channels at all. We have also shown that the highest probability of detecting Eve in the control mode by means of four different measurements in a sequence is 25% and that this probability stems from an entanglement between Bob's home photons, Alice's travel photons, and Eve's ancilla photons.

This probability is not only half of the probability we have in the two-state QDC protocols (e.g., Boström-Felbinger's ping-pong one [10]), but it is also lower than the error probability with a Brandt-Shapiro CNOT attack on the BB84 single-photon QKD mentioned in Sec. I.

In summary:

(1) In all QDC protocols that make use of all four Bell states, Eve can tell Ψ from Φ Bell states without ever being detected in the message mode, even when there are no losses

in the mode. In the control mode, Alice and Bob have only a 25% probability of catching Eve per control transmission. Eve can detect each control mode before Bob receives his control photon with certainty in the standard approach with no photon in the travel mode and with near certainty with a fake photon in the travel mode. Therefore, such protocols (in the literature) should be revised with respect to their security.

(2) QDC protocols using one of $|\Psi^{\pm}\rangle$ Bell and one of $|\Phi^{\pm}\rangle$ Bell states are completely insecure in the message mode.

(3) QDC protocols with three Bell states (e.g., by making use of *dense coding* [36]) or with the so-called mixed basis states (two Bell states and two states from the numerical basis [37,38]) are in between—two Bell states are secure, while the third one or the two from the computational basis, respectively, are not.

In the end, we stress that the presented design for distinguishing the Ψ Bell states from the Φ ones might have an application in the field of quantum computation.

We also stress that we did not consider lossy channels and transmissions because our result does not amount to a new QDC protocol, but rather a general possible attacking scheme against QDC protocols that have been or will be proposed in the literature. An analysis of lossy transmissions would, therefore, be the task of the proponents of such protocols and is outside of the scope of the present paper.

ACKNOWLEDGMENTS

The author acknowledges support by the Alexander von Humboldt Foundation, Germany and by the Ministry of Science, Education, and Sports of Croatia through Project No. 082-0982562-3160. He thanks Janik Wolters and Andreas Schell for many interesting discussions, which inspired him to write the present paper.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photon. **4**, 686 (2011).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] T. A. Brun, J. Harrington, and M. M. Wilde, Phys. Rev. Lett. **102**, 210402 (2009).
[4] H. E. Brandt, Phys. Rev. A **71**, 042312 (2005).
[5] H. E. Brandt, J. Mod. Opt **53**, 2251 (2006).
[6] J. H. Shapiro, Quantum Inf. Proc. **5**, 11 (2006).
[7] J. H. Shapiro and F. N. C. Wong, Phys. Rev. A **73**, 012315 (2006).
[8] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[10] K. Boströem and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[11] M. Ostermeyer and N. Walenta, Opt. Commun. **281**, 4540 (2008).
[12] K. Boström and T. Felbinger, Phys. Lett. A **372**, 3953 (2008).
[13] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
[14] F.-G. Deng, G. L. Long, and X.-S. Liu, Phys. Rev. A **68**, 042317 (2003).
[15] Q. Y. Cai and B. W. Li, Phys. Rev. A **69**, 054301 (2004).
[16] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, Phys. Rev. A **71**, 044305 (2005).
[17] A.-D. Zhu, Y. Xia, Q.-B. Fan, and S. Zhang, Phys. Rev. A **73**, 022338 (2006).
[18] H. Lee, J. Lim, and H. Yang, Phys. Rev. A **73**, 042305 (2006).
[19] Y. Xia, J. Song, and H. Shan Song, Int. J. Quantum Inf. **6**, 463 (2008).
[20] A. Chamoli and C. M. Bhandari, Quantum Inf. Proc. **8**, 347 (2009).
[21] C.-A. Yen, S.-J. Horng, H.-S. Goan, T.-W. Kao, and Y.-H. Chou, Quantum Inf. Comput. **9**, 376 (2009).
[22] Y. Liu, S. Hua, X.-X. Wang, S.-S. Huang, Y. Li, J. YE, and J. Li, Chin. Phys. Lett. **23**, 3152 (2006).
[23] B.-B. Zhang, D.-Q. Wang, S.-S. Huang, and Y. Liu, Chin. Phys. Lett. **26**, 100305 (2009).
[24] S. Lin, Q.-Y. Wen, F. Gao, and F.-C. Zhu, Phys. Rev. A **78**, 064304 (2008).
[25] L. Dong, H.-K. Dong, X.-M. Xiu, Y.-J. Gao, and F. Chi, Int. J. Quantum Inf. **7**, 645 (2009).
[26] J. Li, D. Song, X. Guo, and B. Jing, Chinese J. Electron. **20**, 457 (2011).
[27] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
[28] Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[29] Z.-Y. J. Ou, *Multi-Photon Quantum Interference* (Springer, New York, 2007).
[30] M. Pavičić, *Companion to Quantum Computation and Communication* (Wiley-VCH, Berlin, 2013).
[31] M. G. A. Paris, M. B. Plenio, S. Bose, D. Jonathan, and G. M. D'Ariano, Phys. Lett. A **273**, 153 (2000).
[32] M. Pavičić and J. Summhammer, Phys. Rev. Lett. **73**, 3191 (1994).
[33] M. Pavičić, Phys. Rev. A **50**, 3486 (1994).
[34] M. Pavičić, J. Opt. Soc. Am. B **12**, 821 (1995).
[35] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[36] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
[37] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
[38] M. Pavičić, Int. J. Quantum Inf. **9**, 1737 (2011).