Security of counterfactual quantum cryptography

Zhen-Qiang Yin, Hong-Wei Li, Wei Chen, Zheng-Fu Han,* and Guang-Can Guo
Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
(Received 10 May 2010; published 27 October 2010)

Recently, a "counterfactual" quantum-key-distribution scheme was proposed by T.-G. Noh [Phys. Rev. Lett. **103**, 230501 (2009)]. In this scheme, two legitimate distant peers may share secret keys even when the information carriers are not traveled in the quantum channel. We find that this protocol is equivalent to an entanglement distillation protocol. According to this equivalence, a strict security proof and the asymptotic key bit rate are both obtained when a perfect single-photon source is applied and a Trojan horse attack can be detected. We also find that the security of this scheme is strongly related to not only the bit error rate but also the yields of photons. And our security proof may shed light on the security of other two-way protocols.

DOI: 10.1103/PhysRevA.82.042335 PACS number(s): 03.67.Dd

The quantum key distribution (QKD) [1–3] can enable two distant peers (Alice and Bob) to share secret random string of bits, called key. With the QKD and one time pad, unconditional secure communication is possible. The most commonly used QKD protocol is Bennett-Brassard 1984 (BB84), in which Alice encodes the state of a single photon, transmits it to Bob through a quantum channel that is accessed by an eavesdropper Eve, and, finally, Bob projects this photon into some states. Not just the BB84 protocol, but nearly all QKD protocols, must transmit information carriers (usually a single photon) in a public quantum channel. Many successful QKD experiments [4–10] have been realized during the past decade.

Quite interestingly, T.-G. Noh proposed a QKD protocol (N09) [11] in which the distribution of a secret key bit can be accomplished even though a photon carrying secret information is not in fact transmitted through the quantum channel. Let us introduce the process of the N09 protocol briefly.

In the N09 protocol, Alice randomly encodes a single-photon in a horizontally polarized state $|H\rangle$ as bit 0 or a vertically polarized state $|V\rangle$ as bit 1 and then inputs this photon to port 2 of a beam splitter (BS), whose reflection and transmission modes are written a and b, respectively. For example, if Alice emits $|H\rangle$, the quantum state of this photon will be $|\psi_{H(V)}\rangle = [i|H(V)\rangle_a|0\rangle_b + |0\rangle_a|H(V)\rangle_b]/\sqrt{2}$, where we consider that a $\pi/2$ phase is always added to the reflection case and there is no phase change to the transmission mode. The key point is that mode a is kept by Alice, while mode b represents the quantum channel between Alice and Bob. Thus, Eve can only access mode b, while mode a is unaffected by Eve. Bob will choose either to detect $|H\rangle_b$ with his single-photon detector (SPD) D_3 and just reflect other components of mode b as bit 0 or to detect $|V\rangle_b$ through D_3 and just reflect other components of mode b as bit 1. This operation can be viewed as a random projection to $|X\rangle_b\langle X|$, which will be detected by detector D_3 and $1 - |X\rangle_b\langle X|$, in which $X = H$ or $X = V$. Bob's operation can be implemented with optical switches and a polarization beam splitter (PBS). To detect the intrusion of Eve, Alice and Bob may compare the initial polarization state and the detected polarization state, if D_3 clicks.

Mode b reflected by Bob will return to Alice's BS, and at the same time mode a will also arrive at this BS due to the reflection by a mirror owned by Alice. If the bit choices of Alice and Bob are different, the photon will output from port 2 of Alice's BS and then hit Alice's SPD D_2 due to quantum interference. Conversely, if their bit choices are the same, Bob will get a click in D_3 with probability $1/2$, which means that the photon was in mode b. But, also with a probability of $1/2$, the photon is in mode a and thus will Bob get no click in D_3, and Alice will get one click in D_2 or D_1 with equal chances. Therefore, a click from D_1 means the generation of one secret key bit. D_1 clicks can only step from the photon in mode a, not the quantum channel mode b. Thus we say that in N09 the task of distributing a secret key bit is finished when the information carriers are not traveling in the quantum channel.

The security of N09 has not been proved, though there has been some discussion of particular attacks. The security of this protocol cannot be followed by the claim that Eve cannot access the whole information carrier. However, some simple attacks, such as Eve detecting the polarization of mode b, will spoil the quantum interference and introduce a bit error rate of key bits. Eve may entangle her ancilla with the information carrier and apply different operations to the "go and return" mode . Eve is able to get some key bits without introducing a bit error. This is totally different from the BB84 protocol, in which Eve cannot launch an effective attack without introducing a bit error in the ideal case. Thus a strict security proof is urgently needed for the N09 protocol.

In this paper, we put forward a security proof of the N09 protocol when a Trojan-horse-like attack [12] is prohibited. We find that the security of N09 is highly related not only to the bit error rate of the key, but also to the counting rates of D_1 and D_2. Inspired by Ref. [13], we propose an entanglement distillation protocol (EDP) that is completely equivalent to the N09 protocol. Here, the meaning of this equivalence between the two protocols is as follows: To Alice and Bob, the generated secret key is the same; to Eve, the available information is also the same. The EDP is illustrated in Fig. 1 and the detailed steps are as follows.

1. Alice prepares N pairs of entanglement states $|\Psi\rangle_A = (|H\rangle_A|\psi_H\rangle + |V\rangle_A|\psi_V\rangle)/\sqrt{2}$, in which $|\psi_{H(V)}\rangle = [i|H(V)\rangle_a|0\rangle_b + |0\rangle_a|H(V)\rangle_b]/\sqrt{2}$; H and V represent single-photon horizontally polarized and vertically polarized

*zfhan@ustc.edu.cn

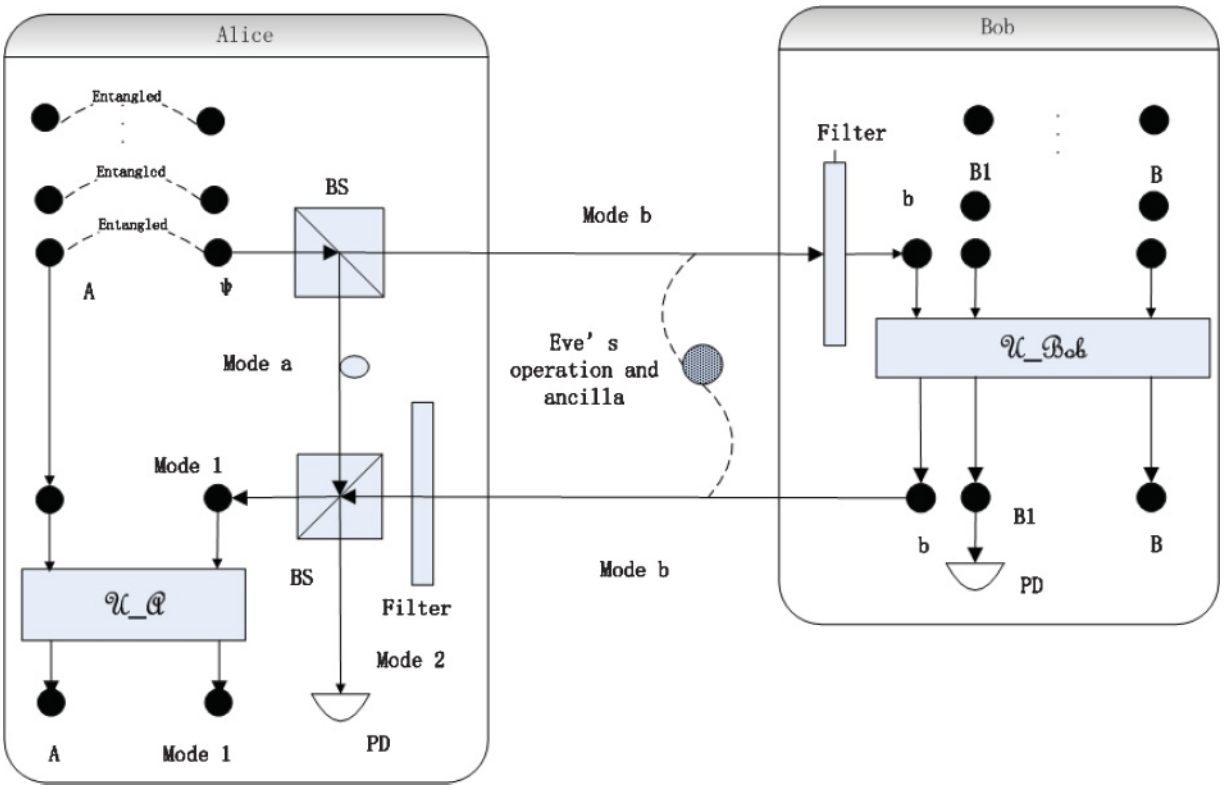

FIG. 1. (Color online) A and ψ represent Alice's initial entangled particles. Filter: a quantum operation controlled by Alice or Bob, which can project mode b into the Hilbert space spanned by $|0\rangle$, $|H\rangle$, and $|V\rangle$. Failure of this filtering operation results in the abortion of the whole protocol. $B1$ and B represent Bob's initial particles. PD: polarization detector which detects particles with projectors $|0\rangle\langle 0|$, $|H\rangle\langle H|$, and $|V\rangle\langle V|$. BS: beam splitter.

states, respectively; and $|0\rangle$ is a vacuum state. Particle A and mode a are protected in Alice's security zone, while mode b will be transmitted to Bob by the channel between Alice and Bob. Bob also prepares N pairs of states $|\Psi\rangle_B = (|H\rangle_B + |V\rangle_B)|0\rangle_{B1}/\sqrt{2}$, where particles B and $B1$ are all ancillae owned by Bob, and Eve has no chance to access them. Alice sends all of the modes b of the N pairs of entanglement states and announces this fact publicly.

2. After passing through the quantum channel controlled by Eve, mode b of the nth $|\Psi\rangle_A$ will enter Bob's security zone. Bob will first project mode b with projectors $|0\rangle_b\langle 0| + |H\rangle_b\langle H| + |V\rangle_b\langle V|$ and $I - |0\rangle_b\langle 0| - |H\rangle_b\langle H| - |V\rangle_b\langle V|$. If Bob detects mode b through the projective measurement $I - |0\rangle_b\langle 0| - |H\rangle_b\langle H| - |V\rangle_b\langle V|$, he will abort the protocol. This operation is carried out by the filter in Bob's security zone as in Fig. 1. If not, Bob will apply a unitary transformation $\mathcal{U}_{\text{Bob}}$ to this mode b and particles B and $B1$ of the nth $|\Psi\rangle_B$. $\mathcal{U}_{\text{Bob}}$ is defined as $\mathcal{U}_{\text{Bob}}|H\rangle_B|0\rangle_{B1}|0\rangle_b = |H\rangle_B|0\rangle_{B1}|0\rangle_b$, $\mathcal{U}_{\text{Bob}}|H\rangle_B|0\rangle_{B1}|H\rangle_b = |H\rangle_B|H\rangle_{B1}|0\rangle_b$, $\mathcal{U}_{\text{Bob}}|H\rangle_B|0\rangle_{B1}|V\rangle_b = |H\rangle_B|0\rangle_{B1}|V\rangle_b$, $\mathcal{U}_{\text{Bob}}|V\rangle_{B1}|0\rangle_{B1}|0\rangle_b = |V\rangle_B|0\rangle_{B1}|0\rangle_b$, $\mathcal{U}_{\text{Bob}}|V\rangle_{B1}|0\rangle_{B1}|H\rangle_b = |V\rangle_B|0\rangle_{B1}|H\rangle_b$, and $\mathcal{U}_{\text{Bob}}|V\rangle_{B1}|0\rangle_{B1}|V\rangle_b = |V\rangle_B|V\rangle_{B1}|0\rangle_b$. After this transformation, Bob will detect particle $B1$ with projectors $|0\rangle_{B1}\langle 0|$, $|H\rangle_{B1}\langle H|$, and $|V\rangle_{B1}\langle V|$ and record the result. After that, mode b will reenter the quantum channel.

3. After traveling along the quantum channel controlled by Eve, the nth mode b will reenter Alice's security zone. Before Alice combines this mode a and mode b of the nth $|\Psi\rangle_A$ in a BS at the same time, she must apply the same projection as for Bob's projection in step 2 to detect any possible Trojan horse attack. This is done by the filter in Alice's security zone as in Fig. 1. Consider that the normal attenuation of mode a is η, the effective state of mode a after this BS is $|H(V)\rangle_a \longrightarrow \sqrt{\eta}[|H(V)\rangle_1 + i|H(V)\rangle_2]$. For mode b, $|H(V)\rangle_b \longrightarrow [|iH(V)\rangle_1 + |H(V)\rangle_2]/\sqrt{2}$.

4. For each trial, Alice measures mode 2 with the following projectors: $|0\rangle_2\langle 0|$, $|H\rangle_2\langle H|$, and $|V\rangle_2\langle V|$. This operation corresponds to the PD in Fig. 1. If a polarization state H or V of mode 2 is observed by Alice, she will measure the polarization of the corresponding particle A and record the result. If Alice gets $|0\rangle_2$ in her measurement, she will detect whether the polarization of mode 1 and the corresponding particle A is the same. This operation can be done by a unitary transformation defined by $\mathcal{U}_A|H(V)\rangle_A|0\rangle_1|s_0\rangle_s = |H(V)\rangle_A|0\rangle_1|s_0\rangle_s$, $\mathcal{U}_A|H(V)\rangle_A|H\rangle_1|s_0\rangle_s = |H(V)\rangle_A|H\rangle_1|s_1(s_2)\rangle_s$, and $\mathcal{U}_A|H(V)\rangle_A|V\rangle_1|s_0\rangle_s = |H(V)\rangle_A|V\rangle_1|s_2(s_1)\rangle_s$, where $|s_0\rangle_s$, $|s_1\rangle_s$, and $|s_2\rangle_s$ are all quantum states of Alice's ancilla s and orthogonal to each other. Now Alice detects this ancilla s with projectors $|s_0\rangle_s\langle s_0|$, $|s_1\rangle_s\langle s_1|$ and $|s_2\rangle_s\langle s_2|$. If the output of Alice's measurement of a is $|s_1\rangle_s$, Alice will preserve the corresponding particles A and 1 in the following process. These A and 1 are called polarization-consistent particles. If Alice obtains $|s_2\rangle_s$, she measures the polarization state of the corresponding particles 1 and A, which are called non-polarization-consistent particles, and records the results.

5. After the transmission of N particles is completed, Bob tells Alice the results of detection of each $B1$. Alice and Bob disregard all the particles corresponding to nonvacuum $B1$. Now, the following steps are carried out only for cases where $B1$ is in vacuum. Alice asks Bob to measure the polarization of particles B corresponding to non-polarization-consistent particles A. Then Alice and Bob randomly select half of the polarization-consistent particles A and 1, and the corresponding B, and measure them with the projectors $|H\rangle\langle H|$ and $|V\rangle\langle V|$. Hence, the probabilities $\mathrm{Prob}(X_A Y_B 0_{B1} Z_D)$, where $X,Y,Z = H,V$ and $D = 1,2$ are obtained by Alice and Bob.

6. According to all of the probabilities observed in step 5, Alice and Bob may carry out EDP for the other half of the polarization-consistent particles A and 1 and the corresponding B.

Since Eve cannot access Alice and Bob's ancillae, this virtual entanglement protocol is equivalent to N09 from Eve's view. To Alice and Bob, the key generated by the two protocols is completely the same. Therefore, the security analysis of the N09 protocol can be carried out by this EDP. In contrast, the EDP can be reduced to N09 using Shor and Preskill's method [13,14].

The initial state of Alice is given by

$$|\Psi_{\mathrm{ini}}\rangle_A^{\otimes N} = \left(\frac{1}{\sqrt{2}}|\phi^+\rangle_{Aa}|0\rangle_b + \frac{1}{2}|H\rangle_{Aa}|H\rangle_b + \frac{1}{2}|V\rangle_{Aa}|V\rangle_b\right)^{\otimes N}, \tag{1}$$

where $|\phi^+\rangle_{Aa} = (i|H\rangle_A|H\rangle_a + i|V\rangle_A|V\rangle_a)/\sqrt{2}$, $|H\rangle_{Aa} = |H\rangle_A|0\rangle_a$, and $|V\rangle_{Aa} = |V\rangle_A|0\rangle_a$. We also define $|0\rangle = (1,0,0)^T$, $|H\rangle = (0,1,0)^T$, and $|V\rangle = (0,0,1)^T$.

We must point out that only mode b can be input into Alice and Bob, and the state of any modes b after Eve's operation must be in a Hilbert space spanned by $|0\rangle_b$, $|H\rangle_b$, and $|V\rangle_b$, since any state out of the Hilbert space may be detected by Bob and Alice's projection $I - |0\rangle_b\langle 0| - |H\rangle_b\langle H| - |V\rangle_b\langle V|$, which results in the abortion of the whole protocol. The foregoing assumptions justify the negligence of a Trojan attack, which makes the security of nearly all "go and return" QKD protocols inexplicit. The most general attack is as follows: First, Eve may apply a unitary transformation $\mathcal{U}_{\mathrm{Eve}}$ to all the N b modes and her ancilla e. In particular, we consider the evolution of the lth communication. This step can be described mathematically as

$$\begin{aligned}\mathcal{U}_{\mathrm{Eve}}|\Psi_{\mathrm{ini}}\rangle_A^{\otimes N}|e\rangle &= \sum_{T(n\neq l)} [C_{T,T(l)=0}|T,T(l)=0\rangle_{Aa}\mathcal{U}_{\mathrm{Eve}}|T,T(l)=0\rangle_b|e_0\rangle \\ &+ C_{T,T(l)=H}|T,T(l)=H\rangle_{Aa}\mathcal{U}_{\mathrm{Eve}}|T,T(l)=H\rangle_b|e_0\rangle \\ &+ C_{T,T(l)=V}|T,T(l)=V\rangle_{Aa}\mathcal{U}_{\mathrm{Eve}}|T,T(l)=V\rangle_b|e_0\rangle],\end{aligned} \tag{2}$$

where T is a list like $t_1 \ldots t_n \ldots t_N$, $t_n = 0,H,V$, $|T(l) = 0\rangle_{Aa} = |\phi^+\rangle_{Aa}$, and C is constant. Consider any state $|T = t_1 \ldots t_l \ldots t_N\rangle_b|e_0\rangle$, which must be transformed to a superposition that consists of three classes: $t_l = 0$, $t_l = H$, and $t_l = V$. Note that for brevity we omit the bracket notations and use the symbols ϕ^+, H, V, 0, and Γ instead of $|\phi^+\rangle$, $|H\rangle$, $|V\rangle$, $|0\rangle$, and $|\Gamma\rangle$, respectively, in the following. We can rewrite Eq. (2) as

$$\begin{aligned}\mathcal{U}_{\mathrm{Eve}}|\Psi_{\mathrm{ini}}\rangle_A^{\otimes N}|e\rangle &= \frac{1}{\sqrt{2}}\phi^{+(l)_{Aa}}\left[\Gamma_{00}0_b^{(l)} + \Gamma_{0H}H_b^{(l)} + \Gamma_{0V}V_b^{(l)}\right] \\ &+ \frac{1}{2}H_{Aa}^{(l)}\left[\Gamma_{H0}0_b^{(l)} + \Gamma_{HH}H_b^{(l)} + \Gamma_{HV}V_b^{(l)}\right] \\ &+ \frac{1}{2}V_{Aa}^{(l)}\left[\Gamma_{V0}0_b^{(l)} + \Gamma_{VH}H_b^{(l)} + \Gamma_{VV}V_b^{(l)}\right],\end{aligned} \tag{3}$$

where the symbol (l) represents the lth mode we have considered, and Γ represents the arbitrary state of all particles of $n \neq l$ and Eve's ancilla. The exact meaning of Γ_{XY}, $X,Y = 0,H,V$ is the quantum state of the whole system except the lth mode b, A, and a, corresponding to the case where the state of mode b is initially X and then changes to Y when it enters Bob's security zone.

We must point out that although Eve's unitary operation $\mathcal{U}_{\mathrm{Eve}}$ on the N modes b and ancilla is arbitrary and impossible to give in a definite mathematic form, Eq. (3) is still valid for any possible attack since we consider that the quantum state Γ_{XY}, $X,Y = 0,H,V$ can be arbitrary.

In the next step Bob applies $\mathcal{U}_{\mathrm{Bob}}$ to the N b modes, B and $B1$. The result of Bob's operation can be rewritten like this:

$$\begin{aligned}&\mathcal{U}_{\mathrm{Bob}}\left[\frac{1}{\sqrt{2}}(H_B + V_B)0_{B1}\right]^{\otimes N}\mathcal{U}_{\mathrm{Eve}}|\Psi_{\mathrm{ini}}\rangle_A^{\otimes N}|e_0\rangle \\ &= \frac{1}{2}\phi_{Aa}^{+(l)}\{\Gamma_{00}\left[H_B^{(l)} + V_B^{(l)}\right]0_{B1}^{(l)}0_b^{(l)} \\ &+ \Gamma_{0H}\left[H_B^{(l)}H_{B1}^{(l)}0_b^{(l)} + V_B^{(l)}0_{B1}^{(l)}H_b^{(l)}\right] \\ &+ \Gamma_{0V}\left[H_B^{(l)}0_{B1}^{(l)}V_b^{(l)} + V_B^{(l)}V_{B1}^{(l)}0_b^{(l)}\right]\} \\ &+ \frac{1}{2\sqrt{2}}H_{Aa}^{(l)}\{\Gamma_{H0}\left[H_B^{(l)} + V_B^{(l)}\right]0_{B1}^{(l)}0_b^{(l)} \\ &+ \Gamma_{HH}\left[H_B^{(l)}H_{B1}^{(l)}0_b^{(l)} + V_B^{(l)}0_{B1}^{(l)}H_b^{(l)}\right] \\ &+ \Gamma_{HV}\left[H_B^{(l)}0_{B1}^{(l)}V_b^{(l)} + V_B^{(l)}V_{B1}^{(l)}0_b^{(l)}\right]\} \\ &+ \frac{1}{2\sqrt{2}}V_{Aa}^{(l)}\{\Gamma_{V0}\left[H_B^{(l)} + V_B^{(l)}\right]0_{B1}^{(l)}0_b^{(l)} \\ &+ \Gamma_{VH}\left[H_B^{(l)}H_{B1}^{(l)}0_b^{(l)} + V_B^{(l)}0_{B1}^{(l)}H_b^{(l)}\right] \\ &+ \Gamma_{VV}\left[H_B^{(l)}0_{B1}^{(l)}V_b^{(l)} + V_B^{(l)}V_{B1}^{(l)}0_b^{(l)}\right]\}.\end{aligned} \tag{4}$$

Third, another unitary transformation, $\mathcal{U}'_{\mathrm{Eve}}$, will be applied to all modes b and Γ by Eve. We note that although $\mathcal{U}'_{\mathrm{Eve}}$ is arbitrary, without loss of generality we can assume that $\mathcal{U}'_{\mathrm{Eve}}\Gamma_{XY}Z_b^{(l)} = \Gamma_{XYZ0}0_b^{(l)} + \Gamma_{XYZH}H_b^{(l)} + \Gamma_{XYZV}V_b^{(l)}$, where $X,Y,Z = 0,H,V$, since the state Γ_{ABCD} can be viewed as an arbitrary state. For simplicity, we consider that Alice's and Bob's detectors never click twice in one communication. This condition can be justified in practical cases, due to the lower dark counts of the SPD. Hence, we obtain that Γ_{0H} and Γ_{0V} must be a 0 vector, and $\mathcal{U}'_{\mathrm{Eve}}\Gamma_{00}0_b^{(l)} = \Gamma_{0000}0_b^{(l)}$, $\mathcal{U}'_{\mathrm{Eve}}\Gamma_{HH}0_b^{(l)} = \Gamma_{HH00}0_b^{(l)}$, $\mathcal{U}'_{\mathrm{Eve}}\Gamma_{HV}0_b^{(l)} = \Gamma_{HV00}0_b^{(l)}$, $\mathcal{U}'_{\mathrm{Eve}}\Gamma_{VH}0_b^{(l)} = \Gamma_{VH00}0_b^{(l)}$, and

$\mathscr{U}'_{\mathrm{Eve}}\Gamma_{VV}0_b^{(l)} = \Gamma_{VV00}0_b^{(l)}$. With these assumptions, we can give the state when the lth mode B returns to Alice's security zone:

$$
\begin{aligned}
|\Psi\rangle_{ABE} &= \mathscr{U}'_{\mathrm{Eve}}\mathscr{U}_{\mathrm{Bob}}\left[\frac{1}{\sqrt{2}}(H_B+V_B)0_{B1}\right]^{\otimes N}\mathscr{U}_{\mathrm{Eve}}|\Psi_{\mathrm{ini}}\rangle_A^{\otimes N}|e_0\rangle \\
&= \frac{1}{2}\phi_{Aa}^{+(l)}\Gamma_{00}\left[H_B^{(l)}+V_B^{(l)}\right]0_{B1}^{(l)}0_b^{(l)} \\
&\quad + \sum_x \frac{1}{2\sqrt{2}}H_{Aa}^{(l)}\left\{\left[H_B^{(l)}+V_B^{(l)}\right]0_{B1}^{(l)}\Gamma_{H00x}x_b^{(l)}\right. \\
&\quad + H_B^{(l)}H_{B1}^{(l)}\Gamma_{HH00}0_b^{(l)} + V_B^{(l)}0_{B1}^{(l)}\Gamma_{HHHx}x_b^{(l)} \\
&\quad \left. + H_B^{(l)}0_{B1}^{(l)}\Gamma_{HVVx}x_b^{(l)} + V_B^{(l)}V_{B1}^{(l)}\Gamma_{HV00}0_b^{(l)}\right\} \\
&\quad + \sum_x \frac{1}{2\sqrt{2}}V_{Aa}^{(l)}\left\{\left[H_B^{(l)}+V_B^{(l)}\right]0_{B1}^{(l)}\Gamma_{V00x}x_b^{(l)}\right. \\
&\quad + H_B^{(l)}H_{B1}^{(l)}\Gamma_{VH00}0_b^{(l)} + V_B^{(l)}0_{B1}^{(l)}\Gamma_{VHHx}x_b^{(l)} \\
&\quad \left. + H_B^{(l)}0_{B1}^{(l)}\Gamma_{VV0x}x_b^{(l)} + V_B^{(l)}V_{B1}^{(l)}\Gamma_{VV00}0_b^{(l)}\right\}. \qquad (5)
\end{aligned}
$$

Here, $P\{X\} = |X\rangle\langle X|$ and x in the summation notation must be $0,H,V$.

We define $|K\rangle_\Gamma$, $K = 0,1,2,\ldots$, is a set of well-defined basis for all Γ states, and $C_K(ABCD) = {}_\Gamma\langle K|\Gamma_{ABCD}\rangle$, $A,B,C,D = 0,H,V$. According to the foregoing assumptions and Eq. (4), we may give the reduced density matrix for the lth particles A, B, and $B1$ and modes a and b in the following equation:

$$
\begin{aligned}
\rho_{AB}^{(l)} &= \mathrm{tr}_\Gamma(|\Phi\rangle_{ABE}\langle\Phi|) = \sum_K {}_\Gamma\langle K|\Phi\rangle_{ABE}\langle\Phi|K\rangle_\Gamma \\
&= \frac{1}{4}\sum_K P\left\{\phi_{Aa}^{+(l)}[(H_B+V_B)0_{B1}C_K(0000)0_b]\right. \\
&\quad + \frac{1}{\sqrt{2}}H_{Aa}\sum_x[(H_B+V_B)0_{B1}C_K(H00x)x_b \\
&\quad + H_BH_{B1}C_K(HH00)0_b + V_B0_{B1}C_K(HHHx)x_b \\
&\quad + H_B0_{B1}C_K(HVVx)x_b + V_BV_{B1}C_K(HV00)0_b] \\
&\quad + \frac{1}{\sqrt{2}}V_{Aa}\sum_x[(H_B+V_B)0_{B1}C_K(V00x)x_b \\
&\quad + H_BH_{B1}C_K(VH00)0_b + V_B0_{B1}C_K(VHHx)x_b \\
&\quad \left. + H_B0_{B1}C_K(VVVx)x_b + V_BV_{B1}C_K(VV00)0_b]\right\}. \qquad (6)
\end{aligned}
$$

Note that the unitarity of Eve's operation and the assumption $\mathscr{U}'_{\mathrm{Eve}}\Gamma_{00}0_b^{(l)} = \Gamma_{0000}0_b^{(l)}$ must result in $\sum_K |C_K(0000)|^2 = 1$. Now the effective operation done by Alice can be described as $H(V)_a \to \sqrt{\eta}(H(V)_1 + iH(V)_2)/\sqrt{2}$ and $H(V)_b \to [iH(V)_1 + H(V)_2]/\sqrt{2}$.

For simplicity, we define $\alpha_K^{(l)} = C_K(0000)$, $\beta_K^{(l)} = iC_K(H00H) + iC_K(HVVH)$, $\beta_K^{\prime(l)} = iC_K(V00V) + iC_K(VHHV)$, $\xi_K^{(l)} = iC_K(H00H) + iC_K(HHHH)$, and $\xi_K^{\prime(l)} = iC_K(V00V) + iC_K(VVVV)$. If Bob gets $|0\rangle_{B1}$ and Alice gets $|s_1\rangle_s$ in step 4 of the EDP, the subsystem of A, B, and mode 1 will be projected into

$$
\begin{aligned}
\rho_{AB1}^{\prime(l)} &= \frac{1}{\Lambda^{(l)}}\sum_K P\left\{H_AH_BH_1\left(\sqrt{\eta}\alpha_K^{(l)} + \beta_K^{(l)}\right)\right. \\
&\quad + V_AV_BV_1\left(\sqrt{\eta}\alpha_K^{(l)} + \beta_K^{\prime(l)}\right) \\
&\quad + H_AV_BH_1\left(\sqrt{\eta}\alpha_K^{(l)} + \xi_K^{(l)}\right) \\
&\quad \left. + V_AH_BV_1\left(\sqrt{\eta}\alpha_K^{(l)} + \xi_K^{\prime(l)}\right)\right\}, \qquad (7)
\end{aligned}
$$

where $\Lambda^{(l)}$ is the normalization constant. Now we can analyze the bit error rate and phase error rate of $\rho_{AB1}^{\prime(l)}$. Define $|\phi^+\rangle_{AB1} = (H_AH_BH_1 + V_AV_BV_1)/\sqrt{2}$, $|\phi^-\rangle_{AB1} = (H_AH_BH_1 - V_AV_BV_1)/\sqrt{2}$, $|\psi^+\rangle_{AB1} = (H_AV_BH_1 + V_AH_BV_1)/\sqrt{2}$, and $|\psi^-\rangle_{AB1} = (H_AV_BH_1 - V_AH_BV_1)/\sqrt{2}$; we can deduce the bit error rate, $e_{\mathrm{bit}}^{(l)} = {}_{AB1}\langle\psi^+|\rho_{AB1}^{\prime(l)}|\psi^+\rangle_{AB1} + {}_{AB1}\langle\psi^-|\rho_{AB1}^{\prime(l)}|\psi^-\rangle_{AB1}$, and the phase error rate, $e_{\mathrm{ph}}^{(l)} = {}_{AB1}\langle\phi^-|\rho_{AB1}^{\prime(l)}|\phi^-\rangle_{AB1} + {}_{AB1}\langle\psi^-|\rho_{AB1}^{\prime(l)}|\psi^-\rangle_{AB1}$.

With the expression of $\rho_{AB}^{(l)}$ we can deduce the following probabilities for the lth communication:

$$
\begin{aligned}
2\mathrm{Prob}^{(l)}(H_AV_B0_{B1}H_1) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} + \xi_K^{(l)}\right|^2, \\
\mathrm{Prob}^{(l)}(H_AV_B0_{B1}H_2) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} - \xi_K^{(l)}\right|^2, \\
2\mathrm{Prob}^{(l)}(V_AH_B0_{B1}V_1) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} + \xi_K^{\prime(l)}\right|^2, \\
\mathrm{Prob}^{(l)}(V_AH_B0_{B1}V_2) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} - \xi_K^{\prime(l)}\right|^2, \\
2\mathrm{Prob}^{(l)}(H_AH_B0_{B1}H_1) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} + \beta_K^{(l)}\right|^2, \\
\mathrm{Prob}^{(l)}(H_AH_B0_{B1}H_2) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} - \beta_K^{(l)}\right|^2, \\
2\mathrm{Prob}^{(l)}(V_AV_B0_{B1}V_1) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} + \beta_K^{\prime(l)}\right|^2, \\
\mathrm{Prob}^{(l)}(V_AV_B0_{B1}V_2) &= \frac{1}{16}\sum_K\left|\sqrt{\eta}\alpha_K^{(l)} - \beta_K^{\prime(l)}\right|^2. \qquad (8)
\end{aligned}
$$

Recall that $\sum_K |\alpha_K|^2 = 1$, $\sum_K |\sqrt{\eta}\alpha_K^{(l)} + \beta_K^{(l)}|^2/16 = 2\mathrm{Prob}^{(l)}(H_AH_B0_{B1}H_1)$, and $\sum_K |\sqrt{\eta}\alpha_K^{(l)} - \beta_K^{(l)}|^2/16 = \mathrm{Prob}^{(l)}(H_AH_B0_{B1}H_2)$, we obtain $\beta^{(l)} = \sum_K |\beta_K^{(l)}|^2 = 8[2\mathrm{Prob}^{(l)}(H_AH_B0_{B1}H_1) + \mathrm{Prob}^{(l)}(H_AH_B0_{B1}H_2)] - \eta$. In the same way, we obtain $\beta^{\prime(l)} = \sum_K |\beta_K^{\prime(l)}|^2 = 8[2\mathrm{Prob}^{(l)}(V_AV_B0_{B1}V_1) + \mathrm{Prob}^{(l)}(V_AV_B0_{B1}V_2)] - \eta$. Thanks to Cauchy's inequality, $(\sqrt{\sum_K |a_K|^2} - \sqrt{\sum_K |b_K|^2})^2 \leqslant \sum_K |a_K + b_K|^2 \leqslant (\sqrt{\sum_K |a_K|^2} + \sqrt{\sum_K |b_K|^2})^2$ always holds for arbitrary complex numbers a_K and b_K. Because $\sum_K |\xi_K^{(l)} - \xi_K^{\prime(l)}|^2 = \sum_K |\sqrt{\eta}\alpha_K^{(l)} + \xi_K^{(l)} - \sqrt{\eta}\alpha_K^{(l)} - \xi_K^{\prime(l)}|^2/4$, we obtain that the upper bound of $\sum_K |\xi_K^{(l)} - \xi_K^{\prime(l)}|^2$ is

$\xi^{(l)} = 8[\sqrt{\text{Prob}^{(l)}(H_A V_B 0_{B1} H_1)} + \sqrt{\text{Prob}^{(l)}(V_A H_B 0_{B1} V_1)}]^2$. With these parameters, $e_{\text{ph}}^{(l)}$ can be given by

$$e_{\text{ph}}^{(l)} = \frac{1}{2\Lambda^{(l)}} \sum_K \left[\left| \beta_K^{(l)} - \beta_K^{\prime(l)} \right|^2 + \left| \xi_K^{(l)} - \xi_k^{\prime(l)} \right|^2 \right] \leqslant \frac{1}{2\Lambda^{(l)}} [(\sqrt{\beta^{(l)}} + \sqrt{\beta^{\prime(l)}})^2 + \xi^{(l)}]. \quad (9)$$

Though $e_{\text{ph}}^{(l)}$ has been given, we cannot give the overall e_{ph} since $e_{\text{ph}}^{(l)}$ may be arbitrarily correlated with previous $l-1$ events. Thanks to Azuma's inequality [15,16], for sufficiently large N pairs of A, B and 1, differences between e_{ph} and $\sum_{l=1}^N e_{\text{ph}}^{(l)}/N$ are arbitrary small. Therefore, we obtain the overall phase error rate $e_{\text{ph}} = \sum_{l=1}^N e_{\text{ph}}^{(l)}/N$.

Also according to Azuma's inequality, we have that $\beta \triangleq \sum_{l=1}^N \beta^{(l)}/N = 8[2\text{Prob}(H_A H_B 0_{B1} H_1) + \text{Prob}(H_A H_B 0_{B1} H_2)] - \eta$, $\beta' \triangleq \sum_{l=1}^N \beta^{\prime(l)}/N = 8[2\text{Prob}(V_A H_B 0_{B1} V_1) + \text{Prob}[V_A H_B 0_{B1} V_2)] - \eta$, and $\sum_{l=1}^N \xi^{(l)}/N \leqslant 8[\sqrt{\text{Prob}(H_A V_B 0_{B1} H_1)} + \sqrt{\text{Prob}(V_A H_B 0_{B1} V_1)}]^2 \triangleq \xi$ always hold when N is sufficiently large. Recalling that $\sum_K |\alpha_K^{(l)}|^2 = 1$, we obtain

$$\Lambda^{(l)} = \sum_K \left(\left| \sqrt{\eta}\alpha_K^{(l)} + \beta_K^{(l)} \right|^2 + \left| \sqrt{\eta}\alpha_K^{(l)} + \beta_K^{\prime(l)} \right|^2 + \left| \sqrt{\eta}\alpha_K^{(l)} + \xi_K^{(l)} \right|^2 + \left| \sqrt{\eta}\alpha_K^{(l)} + \xi_K^{\prime(l)} \right|^2 \right) \geqslant (\sqrt{\eta} - \sqrt{\beta^{(l)}})^2 + (\sqrt{\eta} - \sqrt{\beta^{\prime(l)}})^2. \quad (10)$$

Therefore, the overall phase error rate can be bounded through the inequality

$$\begin{aligned} e_{\text{ph}} &= \sum_{l=1}^N e_{\text{ph}}^{(l)}/N \\ &\leqslant \frac{1}{N} \sum_{l=1}^N \min \left\{ \frac{(\sqrt{\beta^{(l)}} + \sqrt{\beta^{\prime(l)}})^2 + \xi^{(l)}}{2[(\sqrt{\eta} - \sqrt{\beta^{(l)}})^2 + (\sqrt{\eta} - \sqrt{\beta^{\prime(l)}})^2]}, 1 \right\} \\ &\leqslant \frac{1}{N} \sum_{l=1}^N \left[\min \left\{ \frac{\beta^{(l)}}{(\sqrt{\eta} - \sqrt{\beta^{(l)}})^2}, 1 \right\} + \min \left\{ \frac{\beta^{\prime(l)}}{(\sqrt{\eta} - \sqrt{\beta^{\prime(l)}})^2}, 1 \right\} + \min \left\{ \frac{\xi^{(l)}}{4(\sqrt{\eta} - \sqrt{\beta^{(l)}})^2}, 1 \right\} + \min \left\{ \frac{\xi^{(l)}}{4(\sqrt{\eta} - \sqrt{\beta^{\prime(l)}})^2}, 1 \right\} \right], \end{aligned} \quad (11)$$

where $\min\{x,y\}$ equals the smaller one of x and y. Now the final problem is how to calculate the upper bound of e_{ph} with constraints $\beta = \sum_{l=1}^N \beta^{(l)}/N$, $\beta' = \sum_{l=1}^N \beta^{\prime(l)}/N$, and $\xi = \sum_{l=1}^N \xi^{(l)}/N$. Note that $\min\{x/(\sqrt{\eta} - \sqrt{x})^2, 1\}$ is a nonconvex function about x ($x = \beta^{(l)}, \beta^{\prime(l)}$). And it is easy to verify that $\sum_{l=1}^N \min\{\xi^{(l)}/4(\sqrt{\eta} - \sqrt{\beta^{(l)}})^2, 1\}$ will be maximized when all the denominators are equal. Hence, we can obtain the following upper bound of e_{ph}:

$$e_{\text{ph}} \leqslant \frac{4\beta + 4\beta'}{\eta} + \frac{\xi}{4(\sqrt{\eta} - \sqrt{\beta})^2} + \frac{\xi}{4(\sqrt{\eta} - \sqrt{\beta'})^2}. \quad (12)$$

In fact, if there is no Eve's attack, and no channel noises, Alice and Bob must find $2\text{Prob}(H_A H_B 0_{B1} H_1) = \eta/16$ and $\text{Prob}(H_A H_B 0_{B1} H_2) = \eta/16$, and thus $\beta = 0$. In the same way we obtain $\beta' = 0$, $\xi = 0$. Thus pure maximal entanglement states $(H_A H_B H_1 + V_A V_B V_1)/\sqrt{2}$ can be shared between Alice and Bob. Due to the equivalence of the N09 and the EDP, we conclude that N09 is unconditionally secure in the noiseless case. We must point out that the unconditional security is under the assumption that Eve cannot control the transmission efficiency of Alice's mode a and the quantum efficiency of Alice and Bob's SPDs. This is different from BB84, which is secure even if the efficiency of the detectors is controlled by Eve.

We also consider a typical noise channel case, in which the visibility is V and the polarization flip probability when the photon is flying in the quantum channel is p. Then we may obtain $\text{Prob}(H_A H_B 0_{B1} H_1) = \eta/32$, $\text{Prob}(H_A H_B 0_{B1} H_2) = \eta/16$, $\text{Prob}(H_A V_B 0_{B1} H_1) = (1-V)(1-p)\eta/16$, and $\text{Prob}(V_A H_B 0_{B1} V_1) = (1-V)(1-p)\eta/16$, from which we can deduce that $e_{\text{bit}} = 2(1-V)(1-p)/[1+2(1-V)(1-p)]$ and $e_{\text{ph}} = (1-V)(1-p)/2$. For example, let $V = 0.98$, $p = 0$; then we find $e_{\text{bit}} = 3.85\%$, while $e_{\text{ph}} = 1\%$. It is interesting that e_{ph} may be smaller than e_{bit}.

In this paper, we have proved the unconditional security of the N09 protocol by considering its equivalence to an EDP process. According to Ref. [17], our security proof is also composable. By estimating the upper bound of the e_{ph}, we obtain the key bit rate. We find that the security of the N09 protocol relies not only on the bit error rate but also on some of the counting rates of the SPDs. We must point out that our security analysis is in an ideal situation, in which we assume that a perfect single-photon source is applied, Alice and Bob can detect any type of Trojan horse attacks, mode a's evolution is perfect, and the efficiencies of SPDs are all constant. We believe that our security analysis has given a solid foundation for the real-life N09. That the phase error rate is possibly lower than the bit error rate may be an advantage of the N09 protocol.

This work was supported by the National Fundamental Research Program of China (Grant No. 2006CB921900), the National Natural Science Foundation of China (Grant No. 60537020,60621064), and Innovation Funds of the Chinese Academy of Sciences.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

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

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[5] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[6] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[7] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[8] Y. Zhao, B. Qi, X.-F. Ma, H.-K. Lo, and L. Qian, in *Proceedings of IEEE International Symposium on Information Theory* (IEEE, New York, 2006), pp. 2094–2098.
[9] L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
[10] Z.-Q. Yin *et al.*, Chin. Phys. Lett. **25**, 3547 (2008).
[11] T.-G. Noh, Phys. Rev. Lett. **103**, 230501 (2009).
[12] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[13] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[14] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[15] K. Azuma, Tôhuku Math. J. **19**, 357 (1967).
[16] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).
[17] R. Renner, e-print arXiv:quant-ph/0512258.