Hargeet Kaur and Atul Kumar*

An Improved Ping-Pong Protocol Using Three-Qubit Nonmaximally Nonorthogonal Entangled States

https://doi.org/10.1515/zna-2018-0448
Received October 4, 2018; accepted April 23, 2019; previously published online May 29, 2019

Abstract: We analyse the ping-pong (PP) protocol [K. Bostrom and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002)] using different sets of partially entangled three-qubit states. Interestingly, our results show that the partially entangled nonorthogonal three-qubit states are more useful as resources in comparison to three-qubit maximally entangled Greenberger–Horne–Zeilinger (GHZ) states. The properties of orthogonal set of partially entangled states as resources for PP protocol, however, are similar to that of maximally entangled GHZ states – both the states are not preferable due to the vulnerability towards eavesdropping. On the other hand, partially entangled nonorthogonal basis set holds importance for transferring two-bit information, one each from a sender, to a single receiver. The protocol is further analysed for various eavesdropping attacks, and the results are compared with the use of two shared Bell pairs for two-bit information transfer. Surprisingly, the use of partially entangled nonorthogonal set of states is found to offer better qubit efficiency and increased security, as against the use of two separate maximally entangled Bell states with orthogonal basis. In addition, we also propose a mixed-state sharing protocol to further enhance the security of the PP protocol.

Keywords: GHZ State; Ping-Pong Protocol; Three-Qubit State.

1 Introduction

Ever since Bennett and Brassard [1] proposed the BB84 protocol for Quantum Key Distribution (QKD), a lot of progress has been made to discuss and analyze new protocols for secure transmission of a key [2–6]. Quantum Secure Direct Communication (QSDC) added another dimension to cryptographic protocols where the users in the protocol can communicate directly without generating a secure key in advance [7–11]. The first QSDC protocol was a block transmission–based Einstein, Podolsky and Rosen (EPR) state–encoded scheme with high capacity since the four possible states of EPR pair were used to encode two bits of information [7]. In this scheme, however, the key or information sent was known to the sender even before sending the block of EPR pair partner particles to the receiver [8]. Using the similar concept of sharing sequence of particles in EPR pairs, a two-way operation encoded QSDC was suggested [9]. These two schemes have recently been experimentally demonstrated for long-distance quantum communication [12, 13]. Inspired by the BB84 QKD scheme [1], QSDC scheme using single photons in bathes was proposed, where two-bit secret message was encoded on single photons using two different unitary operations [10]. As a proof-of-principle demonstration, a new protocol based on the above concept has been practically implemented with single-photon frequency coding [14]. Moreover, recently, the single-photon QSDC scheme [10] has been practically realised with communications at a distance of 1.5 kilometres [15]. Interestingly, Lucamarini and Mancini [11] proposed a two-way deterministic communication protocol without entanglement, which was a special case of the single-photon QSDC scheme suggested by Deng and Long [10]. Furthermore, Deng and Long showed that this protocol can be used as a practical two-way QKD protocol with the use of faint laser pulses containing not more than two single photons [16]. Quite recently, measurement device–independent QSDC protocol has been reported using EPR pairs and single photons [17, 18].

In this article, we have considered the ping-pong (PP) protocol based on an entangled resource, proposed by Bostrom and Felbinger [19] for the purpose of analysis. It allows asymptotically secure key distribution and quasi-secure direct communication. Following this, Ostermeyer and Walenta [20] have demonstrated a prototype implementation of a deterministic secure coding based on PP protocol using polarisation entangled photons. In addition, Chen et al. [21] experimentally demonstrated a loss-tolerant deterministic QKD session by following a modified PP protocol. The security of PP protocol, however, was questioned by Wojcik [22] and

***Corresponding author: Atul Kumar,** Indian Institute of Technology Jodhpur, Jodhpur, Rajasthan, India, E-mail: atulk@iitj.ac.in
Hargeet Kaur: Indian Institute of Technology Jodhpur, Jodhpur, Rajasthan, India, E-mail: kaur.1@iitj.ac.in

Zhang et al. [23]. Furthermore, Cai [24] implemented a denial-of-service (DoS) attack on the protocol and also suggested improvements to protect the protocol against this attack. On similar lines, an invisible photon eavesdropping attack was proposed on the protocol, and modifications to avoid this attack were also suggested [25]. A seminal contribution in this regard was the proposal of addition of quantum dialogue version to PP protocol so as to prevent Intercept-and-Resend (IR) attack on the travel photons [26]. Although many different eavesdropping operations were studied to attack PP protocol, it proved secure for the ideal case of a perfect quantum channel [27–30]. For imperfect and noisy channels, however, there was no general security proof existing initially, and hence many modified versions of the control mode were suggested to improve the security of the protocol [26, 31–33]. Later, experimentally feasible modification to the protocol were proposed which proved its security in noisy and lossy channels as well [34].

As the protocol was proved a quasi-secure means of direct communication in a two-party system, many multiparty extensions of the protocol were proposed [35–37]. Chamoli and Bhandari [35] showed that Greenberger–Horne–Zeilinger (GHZ) states can be used to send three-bit information where one-bit information can be sent by sender 1 and two-bit information can be sent by sender 2 to a common receiver. Naseri [38] commented on this protocol by pointing out that if one of the sender is dishonest, he or she can very easily know the information being sent by the other sender, without being caught. For two-qubit entanglement based on ψ and ϕ Bell states, Pavicic [39] has shown that in most quantum direct communication protocols an eavesdropper is able to distinguish between ψ and ϕ states without disturbing the desired message in the message mode and without being detected in the control mode [39]. The modified version of control mode, however, is able to detect an eavesdropper performing Pavicic's attack on quantum direct communication protocols using Bell states [32, 33].

In this article, we demonstrate that Pavicic attack leads to a much bigger threat to the PP protocol proposed by Chamoli and Bhandari [35] for communicating three bits of information. Further, in general, quantum quasi-secure direct communication protocols utilise maximally entangled states such as two-qubit Bell states or three-qubit GHZ states for quasi-secure transmission of messages and secure transmission of quantum key from a sender to a receiver. We therefore, raise a question of analysing the usefulness of three-qubit partially entangled states for the PP protocol. For this, we use two different sets of partially entangled three-qubit orthogonal and non orthogonal states. Our analysis shows that the use of set of orthogonal partially entangled three-qubit states for PP protocol leads to similar results as can be obtained by using maximally entangled three-qubit GHZ states. Moreover, we found that the use of nonorthogonal set of partially entangled states for PP protocol is preferable over the use of orthogonal set of partially entangled states. Interestingly, for communicating two bits of information, the nonorthogonal set of states further offer enhanced security and better qubit efficiency [40] over two two-qubit Bell states. Clearly, the enhanced security and efficiency comes at the cost of performing positive operator-valued measurements for distinguishing the nonorthogonal states. During the analysis of various Eavesdropping attacks, we further demonstrate that an eavesdropper gets caught in control mode, message mode and/or Quantum Bit Error Rate (QBER) evaluation with better prospects, whenever partially entangled nonorthogonal set of states are shared between the users instead of two Bell states. However, for Nguyen's attack [26, 41], we find that our states are vulnerable to IR attack in a similar manner as two-qubit Bell states. In addition, we demonstrate that a more secure protocol can be formulated by randomly sharing maximally entangled GHZ state along with a partially entangled three-qubit state.

2 Failure of Ping Pong Protocol to Transfer Three-Bit Information

Chamoli and Bhandari [35] proposed a PP protocol with three-qubit GHZ state as the initial resource where the receiver can simultaneously receive three-bit information from two parties. For this, Alice prepares the initial state in any of the following GHZ states:

$$
\begin{aligned}
|\psi_{1,2}\rangle &= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle)_{ABC} \\
|\psi_{3,4}\rangle &= \frac{1}{\sqrt{2}}(|100\rangle \pm |011\rangle)_{ABC} \\
|\psi_{5,6}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)_{ABC} \\
|\psi_{7,8}\rangle &= \frac{1}{\sqrt{2}}(|110\rangle \pm |001\rangle)_{ABC}
\end{aligned} \tag{1}
$$

After preparing the three-qubit state, Alice sends particles B and C (travel photons) to Bob and Charlie, respectively, retaining particle A (home photon) with her. In control mode, Bob and Charlie simply measure the polarisation of their photons in the computational basis and inform Alice about their measurement outcomes via a public channel. Alice also measures the polarisation of her home photon

and verifies if the measurement results are consistent with the initial shared state. In case of inconsistency of results, eavesdropping is suspected, and communication is terminated. In message mode, Charlie performs one of the four unitary operations on his particle C, i.e. $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, or $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ to encode two-bit information 00, 01, 10, or 11, respectively. Similarly, Bob performs either I or $i\sigma_y$ on his particle B to encode one-bit information. These eight operations have been constructed while studying general superdense coding protocol between multiparties [42]. After performing their individual unitary operations on both the travel photons B and C, Bob and Charlie send them back to Alice, who then performs a three-qubit GHZ state measurement to distinguish the eight different set of encodings. For eavesdropping, Chamoli and Bhandari [35] considered an attack, where Eve prepares four auxiliary photons (B_x, B_y, C_x, and C_y) with two ancilla photons in the state $|\nu\nu\rangle_{B_xC_x}$ and the other two ancilla photons in the state $|00\rangle_{B_yC_y}$ (where "ν" denotes vacuum). As per her strategy, Eve combines two of the auxiliary modes ($|\nu 0\rangle_{B_xB_y}$) with the particle B and the remaining two ($|\nu 0\rangle_{C_xC_y}$) with the particle C. Eve's operations on the combined state lead to 50 % channel loss in the control mode, 25 % of which occurs due to travel photon B sent to Bob and the remaining 25 % occurs due to travel photon C sent to Charlie. Moreover, by performing such an attack, Eve also gets detected in the message mode, due to induced channel loss, in 50 % of the cases, and by Alice receiving two photons through Bob's and Charlie's channels, in 25 % of the cases. Therefore, they suggested that the protocol with a three-particle GHZ state as the initial shared state stands secure against such an attack [35].

In this section, we show that using the extensions of Pavicic's [39] attack, an eavesdropper can gain vital information without being detected in the control mode. Interestingly, Eve can perform the eavesdropping attack to know two out of the three bits of information communicated securely. If Pavicic's attack is applied by Eve on travel paths of photons B and C, respectively; in the PP protocol proposed by Chamoli and Bhandari [35], the encoding operations I and $i\sigma_y$ of Bob can be easily distinguished by Eve. Also, two out of the four operations of Charlie could be easily recognised by an eavesdropper without being caught in the control mode. This can be accomplished by Eve if she prepares the same four auxiliary modes (B_x, C_x, B_y and C_y) and attaches them to the travel photons B and C. The proposed attack operation for two travel photons can be given as

$$P = P_{BB_xB_y} \otimes P_{CC_xC_y}$$

where

$$\begin{aligned} P_{BB_xB_y} &= CNOT_{BB_y}(CNOT_{BB_x} \otimes I_{B_y})(I_B \otimes PBS_{B_xB_y}) \\ &\quad \times CNOT_{BB_y}(CNOT_{BB_x} \otimes I_{B_y})(I_B \otimes H_{B_x} \otimes H_{B_y}) \\ P_{CC_xC_y} &= CNOT_{CC_y}(CNOT_{CC_x} \otimes I_{C_y})(I_C \otimes PBS_{B_xB_y}) \\ &\quad \times CNOT_{CC_y}(CNOT_{CC_x} \otimes I_{C_y})(I_C \otimes H_{C_x} \otimes H_{C_y}) \end{aligned} \tag{2}$$

Eve performs attack P on the travel photons when they are sent from Alice to Bob and Charlie. After Bob and Charlie encode their information and send travel photons back to Alice, Eve performs $P^\dagger$ on photons B and C where $P^\dagger$ is conjugate transpose of P. The presence of Eve goes undetected in control mode, as the correlation of the initial shared state is undisturbed by the attack P. Assuming that three parties share the GHZ state $|\psi_1\rangle_{ABC}$ [from (1)] as a starting resource, the final state of Alice's and Eve's photons after each encoding operation and attack is as follows:

$$\begin{aligned} &[P^\dagger(I^B \otimes I^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = |\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y}, \\ &[P^\dagger(I^B \otimes \sigma_z^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = |\psi_2\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y}, \\ &[P^\dagger(I^B \otimes \sigma_x^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = |\psi_3\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|0\nu\rangle_{C_xC_y}, \\ &[P^\dagger(I^B \otimes i\sigma_y^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = |\psi_4\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|0\nu\rangle_{C_xC_y}, \\ &[P^\dagger(i\sigma_y^B \otimes I^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = |\psi_6\rangle_{ABC}|0\nu\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y}, \\ &[P^\dagger(i\sigma_y^B \otimes \sigma_z^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = |\psi_5\rangle_{ABC}|0\nu\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y}, \\ &[P^\dagger(i\sigma_y^B \otimes \sigma_x^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = -|\psi_8\rangle_{ABC}|0\nu\rangle_{B_xB_y}|0\nu\rangle_{C_xC_y}, \\ &[P^\dagger(i\sigma_y^B \otimes i\sigma_y^C)P]|\psi_1\rangle_{ABC}|\nu 0\rangle_{B_xB_y}|\nu 0\rangle_{C_xC_y} \\ &\quad = -|\psi_7\rangle_{ABC}|0\nu\rangle_{B_xB_y}|0\nu\rangle_{C_xC_y} \end{aligned} \tag{3}$$

Therefore, Eve can conclude that

- a click of B_y and C_y detectors means either $I^B \otimes I^C$ or $I^B \otimes \sigma_z^C$ has been applied by Bob and Charlie,
- a click of B_y and C_x detectors means either $I^B \otimes \sigma_x^C$ or $I^B \otimes i\sigma_y^C$ has been applied by Bob and Charlie,
- a click of B_x and C_y detectors means either $i\sigma_y^B \otimes I^C$ or $i\sigma_y^B \otimes \sigma_z^C$ has been applied by Bob and Charlie, and
- a click of B_x and C_x detectors means either $i\sigma_y^B \otimes \sigma_x^C$ or $i\sigma_y^B \otimes i\sigma_y^C$ has been applied by Bob and Charlie.

Hence, four of eight encoding operations of Bob and Charlie can be distinguished by Eve without being detected as Eve's ancillary states are decoupled from the shared state between Alice, Bob, and Charlie. So, Eve can accurately know two out of three classical bits of information being transferred from Bob, and Charlie to Alice. It can also be easily computed that for Eve's operation set in (2) the mutual information between Alice and Eve, or Bob and Eve, is two bits. Therefore, the protocol becomes highly insecure in terms of information leaked to a third party.

3 Use of Partially Entangled States in PP Protocol

In this section, we analyse the efficiency of partially entangled three-qubit states for PP protocol. For this, we propose to use partially entangled states belonging to the GHZ class, i.e. $|\chi\rangle = \frac{1}{\sqrt{2}}[\sin\theta|000\rangle + \sin\theta|011\rangle - \cos\theta|101\rangle + \cos\theta|110\rangle]$. The reason for selecting partially entangled $|\chi\rangle$ states over partially entangled generalised GHZ states, i.e. $|\psi\rangle_{GHZ} = \sin\theta|000\rangle + \cos\theta|111\rangle$, lies in the fact that the nonlocal correlations between qubits in $|\chi\rangle$ states are always more in comparison to the nonlocal correlations between qubits in $|\psi\rangle_{GHZ}$ states. For example, considering quantum discord as a measure of nonclassical correlations for a quantum system, Figure 1 shows the comparison between the value of discord for $|\chi\rangle$ and $|\psi\rangle_{GHZ}$ states. Clearly, the value of quantum discord for $|\chi\rangle$ states exceeds that of GHZ class states for any given value of the state parameter θ.

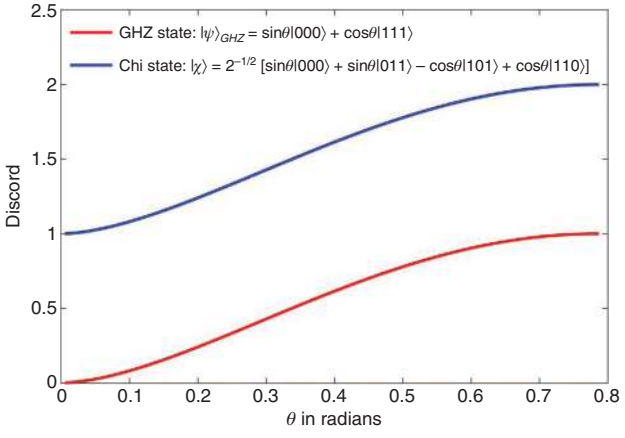

Figure 1: Comparison of quantum discord for generalised GHZ and $|\chi\rangle$ states.

3.1 Nonmaximally Entangled States with Orthogonal Basis

The above protocol can also be accomplished if Alice, Bob, and Charlie share one of the following nonmaximally entangled orthonormal set of states:

$$
\begin{aligned}
|\chi_1\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle + \sin\theta|101\rangle + \cos\theta|110\rangle \\
&\quad - \cos\theta|011\rangle]_{ABC} \\
|\chi_2\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle - \sin\theta|101\rangle + \cos\theta|110\rangle \\
&\quad + \cos\theta|011\rangle]_{ABC} \\
|\chi_3\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|001\rangle + \sin\theta|100\rangle + \cos\theta|111\rangle \\
&\quad - \cos\theta|010\rangle]_{ABC} \\
|\chi_4\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|001\rangle - \sin\theta|100\rangle + \cos\theta|111\rangle \\
&\quad + \cos\theta|010\rangle]_{ABC} \\
|\chi_5\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|010\rangle + \sin\theta|111\rangle + \cos\theta|100\rangle \\
&\quad - \cos\theta|001\rangle]_{ABC} \\
|\chi_6\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|010\rangle - \sin\theta|111\rangle + \cos\theta|100\rangle \\
&\quad + \cos\theta|001\rangle]_{ABC} \\
|\chi_7\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|011\rangle + \sin\theta|110\rangle + \cos\theta|101\rangle \\
&\quad - \cos\theta|000\rangle]_{ABC} \\
|\chi_8\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|011\rangle - \sin\theta|110\rangle + \cos\theta|101\rangle \\
&\quad + \cos\theta|000\rangle]_{ABC}
\end{aligned} \tag{4}
$$

After preparing the three particles A, B, and C in one of the above states, Alice sends particle B to Bob and particle C to Charlie, retaining particle A (home photon) with her. The control mode is the same as presented by Chamoli and Bhandari [35]. In message mode, Charlie performs either of the four unitary operations (I, σ_x, $i\sigma_y$, or σ_z) on his particle C to encode two-bit information 00, 01, 10, and 11, respectively. Similarly, Bob performs I or σ_x on his particle B to encode one-bit information. After performing these operations, Bob and Charlie send back their respective photons to Alice, who then performs a joint three-qubit measurement or consecutive single-qubit and Bell basis measurement to find out the operations performed by Bob and Charlie.

Assuming that the three parties share the state $|\chi_1\rangle_{ABC}$ in the beginning of the protocol and Eve performs the same

attack operation P and $P^\dagger$ on travel photons as in (2), the final state evolves as follows:

$$\begin{aligned}
&[P^\dagger(I^B \otimes I^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
&[P^\dagger(I^B \otimes \sigma_z^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\chi_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
&[P^\dagger(I^B \otimes \sigma_x^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\chi_3\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
&[P^\dagger(I^B \otimes i\sigma_y^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = -|\chi_4\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
&[P^\dagger(\sigma_x^B \otimes I^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\chi_5\rangle_{ABC}|0v\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
&[P^\dagger(\sigma_x^B \otimes \sigma_z^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\chi_6\rangle_{ABC}|0v\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
&[P^\dagger(\sigma_x^B \otimes \sigma_x^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\chi_7\rangle_{ABC}|0v\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \text{ and} \\
&[P^\dagger(\sigma_x^B \otimes i\sigma_y^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = -|\chi_8\rangle_{ABC}|0v\rangle_{B_xB_y}|0v\rangle_{C_xC_y} \qquad (5)
\end{aligned}$$

Thus, Eve infers that

- a click of B_y and C_y detectors means either $I^B \otimes I^C$ or $I^B \otimes \sigma_z^C$ has been applied by Bob and Charlie,
- a click of B_y and C_x detectors means either $I^B \otimes \sigma_x^C$ or $I^B \otimes i\sigma_y^C$ has been applied by Bob and Charlie,
- a click of B_x and C_y detectors means either $\sigma_x^B \otimes I^C$ or $\sigma_x^B \otimes \sigma_z^C$ has been applied by Bob and Charlie, and
- a click of B_x and C_x detectors means either $\sigma_x^B \otimes \sigma_x^C$ or $\sigma_x^B \otimes i\sigma_y^C$ has been applied by Bob and Charlie.

Similar to the previous case, Eve can accurately get two out of three classical bits of information being transferred from Bob and Charlie to Alice without being detected in the control mode. Therefore, by sharing a nonmaximally entangled state, the PP protocol remains vulnerable to the attack in (2). We found that if we start with a set of nonmaximally entangled nonorthogonal states, then the amount of information leaked to the eavesdropper can be significantly reduced. Therefore, we propose a PP protocol for transfer of three-bit information using nonmaximally entangled nonorthogonal basis.

3.2 Nonmaximally Entangled States with Nonorthogonal Basis

For this, let Alice prepare one of the following states (any four of which form an orthonormal set):

$$\begin{aligned}
|\omega_1\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle + \sin\theta|011\rangle + \cos\theta|101\rangle \\
&\quad - \cos\theta|110\rangle]_{ABC} \\
|\omega_2\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle + \sin\theta|011\rangle - \cos\theta|101\rangle \\
&\quad + \cos\theta|110\rangle]_{ABC} \\
|\omega_3\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle - \sin\theta|011\rangle + \cos\theta|101\rangle \\
&\quad + \cos\theta|110\rangle]_{ABC} \\
|\omega_4\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle - \sin\theta|011\rangle - \cos\theta|101\rangle \\
&\quad - \cos\theta|110\rangle]_{ABC} \\
|\omega_5\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|001\rangle + \sin\theta|010\rangle + \cos\theta|100\rangle \\
&\quad - \cos\theta|111\rangle]_{ABC} \\
|\omega_6\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|001\rangle + \sin\theta|010\rangle - \cos\theta|100\rangle \\
&\quad + \cos\theta|111\rangle]_{ABC} \\
|\omega_7\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|001\rangle - \sin\theta|010\rangle + \cos\theta|100\rangle \\
&\quad + \cos\theta|111\rangle]_{ABC} \\
|\omega_8\rangle &= \frac{1}{\sqrt{2}}[\sin\theta|001\rangle - \sin\theta|010\rangle - \cos\theta|100\rangle \\
&\quad - \cos\theta|111\rangle]_{ABC} \qquad (6)
\end{aligned}$$

After preparing the three particles A, B, and C in one of the above states, Alice sends particle B to Bob and particle C to Charlie, retaining particle A (home photon) with her. The control mode is the same as presented by Chamoli and Bhandari [35]. In message mode, Charlie performs either of the four unitary operations (I, σ_x, $i\sigma_y$, or σ_z) on his particle C to encode two-bit information 00, 01, 10, and 11, respectively. Similarly, Bob performs I or σ_z on his particle B to encode one-bit information. After performing these operations, Bob and Charlie send back their photons to Alice, who in order to distinguish between the nonorthogonal states first performs $R = CNOT_{AC}CNOT_{CB}H_BCNOT_{BC}CNOT_{CA}CNOT_{BA}$ on three photons. Alice further performs a single-qubit measurement in computational basis on photons A and B followed by a positive operator-valued measurement on photon C with the following operators:

$$\begin{aligned}
E_1 &= \cos^2\theta|0\rangle\langle 0| - \sin\theta\cos\theta|0\rangle\langle 1| - \sin\theta\cos\theta|1\rangle\langle 0| \\
&\quad + \sin^2\theta|1\rangle\langle 1| \\
E_2 &= \cos^2\theta|0\rangle\langle 0| + \sin\theta\cos\theta|0\rangle\langle 1| + \sin\theta\cos\theta|1\rangle\langle 0| \\
&\quad + \sin^2\theta|1\rangle\langle 1| \qquad (7) \\
E_3 &= I - E_1 - E_2
\end{aligned}$$

The effect of these operations can be summarised as follows:

$$
\begin{aligned}
R|\omega_1\rangle_{ABC} &= |0\rangle_A|0\rangle_B(\sin\theta|0\rangle + \cos\theta|1\rangle)_C \\
R|\omega_2\rangle_{ABC} &= |0\rangle_A|0\rangle_B(\sin\theta|0\rangle - \cos\theta|1\rangle)_C \\
R|\omega_3\rangle_{ABC} &= |0\rangle_A|1\rangle_B(\sin\theta|0\rangle + \cos\theta|1\rangle)_C \\
R|\omega_4\rangle_{ABC} &= |0\rangle_A|1\rangle_B(\sin\theta|0\rangle - \cos\theta|1\rangle)_C \\
R|\omega_5\rangle_{ABC} &= |1\rangle_A|1\rangle_B(\sin\theta|0\rangle + \cos\theta|1\rangle)_C \\
R|\omega_6\rangle_{ABC} &= |1\rangle_A|1\rangle_B(\sin\theta|0\rangle - \cos\theta|1\rangle)_C \\
R|\omega_7\rangle_{ABC} &= |1\rangle_A|0\rangle_B(\sin\theta|0\rangle + \cos\theta|1\rangle)_C \\
R|\omega_8\rangle_{ABC} &= |1\rangle_A|0\rangle_B(\sin\theta|0\rangle - \cos\theta|1\rangle)_C \qquad (8)
\end{aligned}
$$

As Bob encodes using I and σ_z operations, Bob's information is secure against Eve's attack [39]. But, half of the encoding operations of Charlie can be easily understood by Eve without being caught in the control mode. Assuming that the three parties share the state $|\omega_2\rangle_{ABC}$ in the beginning of the protocol and assuming that Eve performs the same attack operation P on the travel photons as in (2), the final state evolves as follows:

$$
\begin{aligned}
&[P^\dagger(I^B \otimes I^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
&[P^\dagger(I^B \otimes \sigma_z^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\omega_3\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
&[P^\dagger(\sigma_z^B \otimes I^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\omega_4\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
&[P^\dagger(\sigma_z^B \otimes \sigma_z^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\omega_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \qquad (9)
\end{aligned}
$$

$$
\begin{aligned}
&[P^\dagger(I^B \otimes \sigma_x^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\omega_6\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
&[P^\dagger(I^B \otimes i\sigma_y^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = -|\omega_7\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
&[P^\dagger(\sigma_z^B \otimes \sigma_x^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = |\omega_8\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
&[P^\dagger(\sigma_z^B \otimes i\sigma_y^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} \\
&\quad = -|\omega_5\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y} \qquad (10)
\end{aligned}
$$

In this way, Eve knows that

- a click of B_y and C_y detectors means either $I^B \otimes I^C$, $I^B \otimes \sigma_z^C$, $\sigma_z^B \otimes I^C$, or $\sigma_z^B \otimes \sigma_z^C$ has been applied by Bob and Charlie (9), and
- a click of B_y and C_x detectors means either $I^B \otimes \sigma_x^C$, $I^B \otimes i\sigma_y^C$, $\sigma_z^B \otimes \sigma_x^C$, or $\sigma_z^B \otimes i\sigma_y^C$ has been applied by Bob and Charlie (10).

Therefore, in this case, only two sets of encoding operations of Bob and Charlie can be distinguished by Eve. Hence, Eve can correctly guess one classical bit of transferred information without being detected in the control mode.

The above analysis clearly demonstrates that for transfer of three classical bits of information using a quantum direct communication protocol, if the initial shared state between the parties is a partially entangled state chosen from a set of nonorthogonal basis, then the protocol is less susceptible to eavesdropping than sharing a GHZ state. The only cost one has to pay is the application of some gates and positive operator-valued measurement to distinguish these nonorthogonal states. In any case, the protocol is not completely secure for three bits of information transfer.

4 Two-Bit Information Transfer Using Partially Entangled Nonorthogonal States

Only one-bit secure information can be sent using three-qubit maximally entangled GHZ states as explained above. In order to propose a secure protocol, one needs to use partially entangled nonorthogonal states in a PP protocol for transferring two bits of information instead of three. Then, the four operations in (9) can be used for encoding two classical bits of information as follows:

- $S_{0,0}^{BC} = I^B \otimes I^C$ to send 00
- $S_{0,1}^{BC} = I^B \otimes \sigma_z^C$ to send 01
- $S_{1,0}^{BC} = \sigma_z^B \otimes I^C$ to send 10
- $S_{1,1}^{BC} = \sigma_z^B \otimes \sigma_z^C$ to send 11

Alice prepares any of the states in (6) and sends photons B and C to Bob and keeps photon A with herself. Now, Bob can perform the above operations on B and C to send two bits of information to Alice. Alice and Bob may also share two Bell states to share two bits of information [19]. But, it is shown in the following section of our article how Bell states being completely entangled are more susceptible to eavesdropping than a partially entangled state. The control mode remains the same as in the original PP protocol [19].

5 Vulnerability to Various Attacks

In this section, we compare the vulnerability of the above protocol to transfer two-bit information using Wojcik's

attack [22], Pavicic's attack [39], and two efficient attacks proposed by us, one of which uses controlled functionality of a polarisation beam splitter. In each attack, Eve attaches two ancillary photons (a vacuum and a horizontally polarised photon) for each travel photon. The analysis is compared with a protocol where two Bell states are used as initial resource as against the set of states in (6). Without eavesdropping, when Alice prepares $|\omega_2\rangle_{ABC}$ as the starting source, the four encoding operations yield the following states:

$$\begin{aligned} I^B \otimes I^C|\omega_2\rangle_{ABC} &= |\omega_2\rangle_{ABC} \\ I^B \otimes \sigma_z^C|\omega_2\rangle_{ABC} &= |\omega_3\rangle_{ABC} \\ \sigma_z^B \otimes I^C|\omega_2\rangle_{ABC} &= |\omega_4\rangle_{ABC} \\ \sigma_z^B \otimes \sigma_z^C|\omega_2\rangle_{ABC} &= |\omega_1\rangle_{ABC} \end{aligned} \tag{11}$$

On the other hand, when Alice prepares two Bell states $|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}$ as the starting source, the four encoding operations yield the following states:

$$\begin{aligned} I^B \otimes I^C[|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= |\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C} \\ I^B \otimes \sigma_z^C[|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= -|\psi^+\rangle_{A_1B}|\psi^-\rangle_{A_2C} \\ \sigma_z^B \otimes I^C[|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= -|\psi^-\rangle_{A_1B}|\psi^+\rangle_{A_2C} \\ \sigma_z^B \otimes \sigma_z^C[|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= |\psi^-\rangle_{A_1B}|\psi^-\rangle_{A_2C} \end{aligned} \tag{12}$$

1. According to Wojcik's [22] attack operation, Eve attaches $|v0\rangle_{x_1y_1}|v0\rangle_{x_2y_2}$ to the initial shared state and performs an attack $W = S_{Bx_1}S_{Cx_2}CPBS_{Bx_1y_1}$ $CPBS_{Cx_2y_2}H_{y_1}H_{y_2}$ when Alice sends the two travel photons to Bob, where $CPBS_{Bx_1y_1} = CNOT_{By_1}(CNOT_{Bx_1} \otimes I_{y_1})(I_B \otimes PBS_{x_1y_1}) \times CNOT_{By_1}(CNOT_{Bx_1} \otimes I_{y_1})$ and $CPBS_{Cx_2y_2} = CNOT_{Cy_2}(CNOT_{Cx_2} \otimes I_{y_2})(I_C \otimes PBS_{x_2y_2}) \times CNOT_{By_2}(CNOT_{Bx_2} \otimes I_{y_2})$. Here S stands for a swap operation, *CNOT* for a *Controlled-NOT* operation, where *NOT* is a spin flip operation, and H for a Hadamard transformation. Assuming that Alice prepares a partially entangled state $|\omega_2\rangle_{ABC}$ and sends photons B and C to Bob, if Eve performs Wojcik's attack on the travel photons from Alice to Bob, the state reduces to

$$\begin{aligned} W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} = \frac{\sin\theta}{2\sqrt{2}}[&00000vv + 00v00v1 \\ &+ 0v0001v + 0vv0011 + 0vv1100 + 0v1110v \\ &+ 01v11v0 + 01111vv] + \frac{\cos\theta}{2\sqrt{2}}[1v0100v \\ &+ 1vv1001 + 11010vv + 11v10v1 - 10v01v0 \\ &- 10101vv - 1vv0110 - 1v1011v]_{ABCx_1x_2y_1y_2} \end{aligned} \tag{13}$$

Now, if Bob chooses to operate in control mode, Eve will be caught in 75 % of cases due to the introduction of vacuum states in the travel photons B and C. But, if Bob opts for message mode, he will encode using one of the above four unitary operations in (11). Photons B and C that are replaced by vacuum states will remain unaffected by those encoding operations, and hence the final state that Alice will measure after the travel photons reach back to her will be different from (11). After eavesdropping, the measurement results will be as follows:

$$\begin{aligned} &W^\dagger[I^B \otimes I^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\ &\quad = |\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\ &W^\dagger[I^B \otimes \sigma_z^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\ &\quad = \frac{1}{2}\big[(|\omega_2\rangle + |\omega_3\rangle]_{ABC})|vv00\rangle_{x_1x_2y_1y_2} \\ &\quad +(|\omega_2\rangle - |\omega_3\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2}\big] \\ &W^\dagger[\sigma_z^B \otimes I^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\ &\quad = \frac{1}{2}\big[(|\omega_2\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\ &\quad +(|\omega_2\rangle - |\omega_4\rangle)_{ABC}|vv10\rangle_{x_1x_2y_1y_2}\big] \\ &W^\dagger[\sigma_z^B \otimes \sigma_z^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\ &\quad = \frac{1}{4}[(|\omega_1\rangle + |\omega_2\rangle + |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\ &\quad + (|\omega_1\rangle + |\omega_2\rangle - |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv11\rangle_{x_1x_2y_1y_2} \\ &\quad - (|\omega_1\rangle - |\omega_2\rangle - |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv10\rangle_{x_1x_2y_1y_2} \\ &\quad -(|\omega_1\rangle - |\omega_2\rangle + |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2}\big] \end{aligned} \tag{14}$$

As Alice does not get the measurement result as desired by Bob, the mutual information between Alice (receiver) and Bob (sender) reduces from 2 bits to 0.6225 bit. Also, the mutual information between Bob (sender) and Eve is 0.6225 bit, and that between Alice (receiver) and Eve is 0.1474 bit. The mutual information obtained between different users is the same as the mutual information when Eve performs Wojcik's operation on the two travel photons, which are a part of two Bell pairs [22]. The only difference between the two protocols is in terms of Eve's chances of getting detected in control mode. While using two Bell pairs, Eve introduces vacuum in the travel photons in half the cases, and hence her probability of being detected in control mode is 50 % [22]. On the other hand, when the protocol employs an ω state as the initial shared state, then Eve's detection probability rises to 75 %. Thus, to avoid information leak under such attacks, a $|\omega\rangle$ state will be preferred over two Bell states.

2. Now if we consider Pavicic's [39] attack operation, which has no swap operation but additional Hadamard on the "x" photons of Eve, i.e. $P = CPBS_{Bx_1y_1} CPBS_{Cx_2y_2} H_{x_1} H_{x_2} H_{y_1} H_{y_2}$, then Eve does not get detected in the control mode as no vacuum photons are introduced. Also, Eve does not get any information by performing such an operation whether the protocol uses a $|\omega\rangle$ state or two Bell states.
3. To further analyse the security of this protocol, we propose an efficient attack operation, similar to the attack proposed by Zhang et al. [23]. In this eavesdropping attack, Eve gets same information as in Wojcik's attack, but gets detected with a lesser probability. Eve attaches $|v0\rangle_{x_1y_1}|v0\rangle_{x_2y_2}$ to the initial shared state and performs $Q = CPBS_{y_1Bx_1} CPBS_{y_2Cx_2} CNOT_{By_1} CNOT_{Cy_2} CPBS_{Bx_1y_1}$ $CPBS_{Cx_2y_2} H_{y_1} H_{y_2}$ when Alice sends two travel photons to Bob. This proposed eavesdropping operation contains 36 controlled *NOT* operations, eight polarisation beam splitters, and four Hadamard operations, as opposed to Wojcik's attack, which contains 16 controlled *NOT* operations, four polarisation beam splitters, four swap operations, and four Hadamard operations. Although the above proposed attack involves more operations than Wojcik's attack, it is worthwhile to study this attack because of the assumption that Eve has unlimited power constrained only by the laws of physics, and it further leads to reduction in Eve's chances of detection.

Assuming that Alice prepares a partially entangled state $|\omega_2\rangle_{ABC}$ and sends photons B and C to Bob, if Eve performs our proposed attack on the travel photons from Alice to Bob, the state reduces to

$$\begin{aligned} Q|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} = \frac{\sin\theta}{2\sqrt{2}}[&00000vv + 0000vv1 \\ &+ 000v01v + 000vv11 + 0vv1111 + 0v1111v \\ &+ 01v11v1 + 01111vv] + \frac{\cos\theta}{2\sqrt{2}}[1v0101v \\ &+ 1v01v11 + 11010vv + 1101vv1 - 10v01v1 \\ &- 10101vv - 10vv111 - 101v11v]_{ABCx_1x_2y_1y_2} \end{aligned} \tag{15}$$

Now, if Bob chooses to operate in control mode, Eve will be caught in $\left(\frac{3+\cos^2\theta}{8} \times 100\right)\%$ cases due to the introduction of vacuum states in the travel photons B and C. But, if Bob opts for message mode, he will encode using one of the above four unitary operations in (11), and hence the final state that Alice will measure after the travel photons reach back to her will be the same [as (14)] as the measurement results after Wojcik's attack. Therefore, mutual information between the parties remains the same, as after Wojcik's attack. However, when two Bell states are shared between Alice and Bob, Eve introduces vacuum with a probability of 0.4375 and hence gets caught in 43.75 % of cases. For $\theta \in (0^\circ, 45^\circ)$, the control mode detection is better when an ω state is shared, because the probability of Eve getting caught is more than the scenario in which two Bell states are shared.

4. Furthermore, we found another attack operation in which Eve attaches $|v0\rangle_{x_1y_1}|v0\rangle_{x_2y_2}$ to the initial shared state and performs two attacks when Alice sends two travel photons to Bob. Eve first performs the same operation Q as proposed above, and then she applies an additional beam splitter ("*bs*" gate), which lets the photons B and x_1 pass through a beam splitter. The beam splitter is constructed such that it transmits (reflects) 1 (0). Although the eavesdropping operation proposed here contains an additional polarisation beam splitters as compared to our first eavesdropping operation, it is an efficient attack operation because Eve gets relatively hidden by balancing the errors introduced in both control and message mode. This operation when performed on a partially entangled state $|\omega_2\rangle_{ABC}$ yields

$$\begin{aligned} bs[Q|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2}] = \frac{\sin\theta}{2\sqrt{2}}[&00000vv \\ &+ 0000vv1 + 000v01v + 000vv11 + 01vv111 \\ &+ 011v11v + 01v11v1 + 01111vv] \\ &+ \frac{\cos\theta}{2\sqrt{2}}[110v01v + 110vv11 + 11010vv \\ &+ 1101vv1 - 10v01v1 - 10101vv - 10vv111 \\ &- 101v11v]_{ABCx_1x_2y_1y_2} \end{aligned} \tag{16}$$

and when the same operation is performed on two Bell states, gives

$$\begin{aligned} bs[Q|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2}] \\ = \frac{1}{4}\left[|01\rangle_{A_1B}|v1 + 1v\rangle_{x_1y_1} + |10\rangle_{A_1B}|0v + v1\rangle_{x_1y_1}\right] \\ \otimes [|0v11 + 011v + 100v + 10v1\rangle_{A_2Cx_2y_2}] \end{aligned} \tag{17}$$

Now, Bob (sender) can perform the encoding operations on the partially entangled state in (16) and assume that Alice (receiver) will get the states as in (11) on each measurement as per her operations. In case of Bell pairs, Bob (sender) assumes Alice (receiver) will get the states as in (12).

But in presence of Eve, the above ideal case does not occur. Eve performs $Q^\dagger$ operation, and the final state evolves as follows:

$$
\begin{aligned}
&Q^\dagger[I^B \otimes I^C]bs(Q(|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2})) \\
&\quad = \frac{1}{2}(|\omega_2\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&\quad + \frac{1}{4}(|\omega_2\rangle - |\omega_4\rangle)_{ABC}|vv00 - vv10\rangle_{x_1x_2y_1y_2} \\
&\quad + \frac{1}{2\sqrt{2}}(\sin\theta|0v1\rangle + \cos\theta|1v0\rangle)_{ABC}|1v00 \\
&\quad - 1v10\rangle_{x_1x_2y_1y_2} \\
&Q^\dagger[I^B \otimes \sigma_z^C]bs(Q(|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2})) \\
&\quad = \frac{1}{4}(|\omega_1\rangle + |\omega_2\rangle + |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&\quad + \frac{1}{8}(|\omega_1\rangle + |\omega_2\rangle - |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01 \\
&\quad - vv11\rangle_{x_1x_2y_1y_2} - \frac{1}{4}(|\omega_1\rangle - |\omega_2\rangle + |\omega_3\rangle \\
&\quad - |\omega_4\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2} - \frac{1}{8}(|\omega_1\rangle - |\omega_2\rangle - |\omega_3\rangle \\
&\quad + |\omega_4\rangle)_{ABC}|vv00 - vv10\rangle_{x_1x_2y_1y_2} \\
&\quad + \frac{\sin\theta}{2\sqrt{2}}|0v1\rangle_{ABC}|1v01 - 1v11\rangle_{x_1x_2y_1y_2} \\
&\quad + \frac{\cos\theta}{2\sqrt{2}}|1v0\rangle_{ABC}|1v00 - 1v10\rangle_{x_1x_2y_1y_2} \\
&Q^\dagger[\sigma_z^B \otimes I^C]bs(Q(|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2})) \\
&\quad = \frac{1}{2}(|\omega_2\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&\quad - \frac{1}{4}(|\omega_2\rangle - |\omega_4\rangle)_{ABC}|vv00 - vv10\rangle_{x_1x_2y_1y_2} \\
&\quad - \frac{1}{2\sqrt{2}}(\sin\theta|0v1\rangle + \cos\theta|1v0\rangle)_{ABC}|1v00 \\
&\quad - 1v10\rangle_{x_1x_2y_1y_2} \\
&Q^\dagger[\sigma_z^B \otimes \sigma_z^C]bs(Q(|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2})) \\
&\quad = \frac{1}{4}(|\omega_1\rangle + |\omega_2\rangle + |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&\quad - \frac{1}{8}(|\omega_1\rangle + |\omega_2\rangle - |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01 \\
&\quad - vv11\rangle_{x_1x_2y_1y_2} - \frac{1}{4}(|\omega_1\rangle - |\omega_2\rangle + |\omega_3\rangle \\
&\quad - |\omega_4\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2} + \frac{1}{8}(|\omega_1\rangle - |\omega_2\rangle - |\omega_3\rangle \\
&\quad + |\omega_4\rangle)_{ABC}|vv00 - vv10\rangle_{x_1x_2y_1y_2} \\
&\quad - \frac{\sin\theta}{2\sqrt{2}}|0v1\rangle_{ABC}|1v01 - 1v11\rangle_{x_1x_2y_1y_2} \\
&\quad - \frac{\cos\theta}{2\sqrt{2}}|1v0\rangle_{ABC}|1v00 - 1v10\rangle_{x_1x_2y_1y_2} \qquad (18)
\end{aligned}
$$

or

$$
\begin{aligned}
&Q^\dagger[I^B \otimes I^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) \\
&\quad = \frac{1}{4}[|\psi^+\rangle_{A_1B}(3|v0\rangle - |v1\rangle)_{x_1y_1} - |\psi^-\rangle_{A_1B}(|v0\rangle \\
&\quad + |v1\rangle)_{x_1y_1} + \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \\
&\quad \otimes [|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2}] \\
&Q^\dagger[I^B \otimes \sigma_z^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) \\
&\quad = \frac{1}{8}[|\psi^+\rangle_{A_1B}(3|v0\rangle - |v1\rangle)_{x_1y_1} - |\psi^-\rangle_{A_1B}(|v0\rangle \\
&\quad + |v1\rangle)_{x_1y_1} + \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \\
&\quad \otimes [|\psi^+\rangle_{A_2C}(|v0\rangle + |v1\rangle)_{x_2y_2} - |\psi^-\rangle_{A_2C}(|v0\rangle \\
&\quad - |v1\rangle)_{x_2y_2}] \\
&Q^\dagger[\sigma_z^B \otimes I^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) \\
&\quad = \frac{1}{4}[|\psi^+\rangle_{A_1B}(|v0\rangle + |v1\rangle)_{x_1y_1} - |\psi^-\rangle_{A_1B}(3|v0\rangle \\
&\quad - |v1\rangle)_{x_1y_1} - \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \\
&\quad \otimes [|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2}] \\
&Q^\dagger[\sigma_z^B \otimes \sigma_z^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) \\
&\quad = \frac{1}{8}[|\psi^+\rangle_{A_1B}(|v0\rangle + |v1\rangle)_{x_1y_1} - |\psi^-\rangle_{A_1B}(3|v0\rangle \\
&\quad - |v1\rangle)_{x_1y_1} - \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \\
&\quad \otimes [|\psi^+\rangle_{A_2C}(|v0\rangle + |v1\rangle)_{x_2y_2} - |\psi^-\rangle_{A_2C}(|v0\rangle \\
&\quad - |v1\rangle)_{x_2y_2}] \qquad (19)
\end{aligned}
$$

Equation (18) shows the measurement outcomes in case of $|\omega_2\rangle$ state, and (19) shows the measurement outcomes in case of two Bell states. The above equations clearly indicate that in control mode Eve gets detected in 25 % of cases. Moreover, in message mode, because Alice has received a vacuum photon instead of a polarised photon in 25 % of cases, she does not get any measurement result with a probability of 25 %. This consistency of getting vacuum or no result in both control mode and message mode in almost equal, i.e. 25 % of cases, may confuse Alice and Bob about a possible induced channel loss, and eavesdropping may get concealed easily.

5. Finally, we analyze an efficient attack proposed by Nguyen [26]. Similar to the case of PP protocol using a Bell pair, the DoS attack by an eavesdropper goes undetected in the discussed protocol setup as well. However, one can always implement a similar modification in the control mode as suggested by Nguyen for the three-qubit PP protocol at the cost of performing a three-qubit measurement at the receiver's end at every control mode. This modification prevents the occurrence of

disturbance attack but is still susceptible to IR attack [26]. For example, when the travel qubits "B" and "C" are sent from Alice to Bob, Eve captures them on the "ping" route and instead sends qubits "b" and "c" of the prepared dummy state to Bob. The dummy qubits can be part of two entangled dummy Bell pairs. Bob now performs the message encoding on these dummy photons and sends them back to Alice. On the "pong" route, Eve again captures the dummy qubits and performs the required measurements (Bell state measurements) on the home and travel qubits of the dummy state. Thus, Eve will know the message sent by Bob through the encoding operations with certainty. Eve then performs the same encoding operations on the travel photons (B and C) sent by Alice and sends them back to Alice through the "pong" route. This way, in the original PPP setting, Eve knows the entire two-bit message sent by Bob, without being caught. In order to make our protocol resistant to the IR attack pointed out by Nguyen [26], we incorporate the quantum dialogue version into the PPP using partially entangled states with nonorthogonal basis, which is discussed in the following paragraph.

Similar to the modification suggested by Nguyen, we assume that Alice encodes her message bits (k, l) by applying $S^{BC}_{k,l}$ on the prepared state and sends the travel photons to Bob through the "ping" route. Alice also announces that she has sent the travel qubits, which is later acknowledged by Bob on receipt of the qubits. Then, Bob encodes his message bits (i, j) by performing the encoding $S^{BC}_{i,j}$ on the travel photons and sends back the travel qubits to Alice. On receiving the qubits, Alice performs the required measurements on the qubits as discussed previously to distinguish the four states and thus decodes the encoded message. On performing these measurements, Alice publicly announces the resultant message bits (let (x, y)) to Bob. As

$$S^{BC}_{i,j} S^{BC}_{k,l} = S^{BC}_{i\oplus k, j\oplus l} \tag{20}$$

Alice comes to know Bob's encoding by XORing the resultant bits (x, y) with her own message bits (k, l), i.e. $i = x \oplus k = |x - k|$ and $j = y \oplus l = |y - l|$. Similarly, Bob comes to know Alice's encoding by XORing the publicly announced bits (x, y) with his own message bits (i, j), i.e. $k = x \oplus i = |x - i|$ and $l = y \oplus j = |y - j|$. An eavesdropper's attempt of intervention will only involve guessing the correct message bits: (i, j) or (k, l) as (x, y) bits are already broadcasted. Eve may make a correct guess in one of four cases. Therefore, the detection probability of Eve for transmitting $2N$ bits message to (and from) Alice from (and to) Bob is $D = 1 - \left(1 - \frac{3c}{4}\right)^{\frac{N}{1-c}}$ where c is the probability of control mode runs in the total runs of the protocol [26].

Table 1 shows the values of mutual information and eavesdropper detection for various attacks with the use of an ω state, two Bell states, and a GHZ state, respectively,

Table 1: Various attacks on PPP using an ω state, two Bell states, or a GHZ state for two-bit information transfer using a combination of identity or σ_z operations on the travel photons.

	Attacks by Eve	Wojcik's attack	Pavicic's attack	Proposed attack 1	Proposed attack 2
One ω state	$I(sender : receiver)$	0.6225	2	0.6225	0.5447
	$I(sender : eavesdropper)$	0.6225	0	0.6225	0.5447
	$I(receiver : eavesdropper)$	0.1474	0	0.1474	0.3666
	Eve's chances of detection in control mode	75 %	0 %	$12.5(3 + \cos^2\theta)$ %	25 %
	Eve's chances of detection in message mode	0 %	0 %	0 %	25 %
	Quantum Bit Error Rate (QBER)	0.4375	0	0.4375	0.46875
Two Bell states	$I(sender : receiver)$	0.6225	2	0.6225	0.8071
	$I(sender : eavesdropper)$	0.6225	0	0.6225	0.5447
	$I(receiver : eavesdropper)$	0.1474	0	0.1474	0.3666
	Eve's chances of detection in control mode	50 %	0 %	43.75 %	25 %
	Eve's chances of detection in message mode	0 %	0 %	0 %	25 %
	QBER	0.4375	0	0.4375	0.28125
One GHZ state	$I(sender : receiver)$	0.0488	1	0.0488	0.3112
	$I(sender : eavesdropper)$	0	0	0	0
	$I(receiver : eavesdropper)$	0.0488	0	0.0488	0.3112
	Eve's chances of detection in control mode	75 %	0 %	50 %	25 %
	Eve's chances of detection in message mode	0 %	0 %	0 %	25 %
	QBER	0.375	0	0.375	0.625

with the encoding operations I and σ_z on each travel qubit. Although the probability of Eve's detection remains the same for both the $|\omega_2\rangle$ state and two Bell states, the mutual information between the sender and the receiver introduced by our second proposed attack is different in each case. Although the mutual information between the sender and the receiver is lesser in the case of ω states, this attack introduces higher error when an ω state is used as compared to two Bell states. Therefore, when an ω state is shared, there are higher chances of Eve being caught when QBER is calculated at the end of the protocol by compromising few message bits, making the protocol more secure towards information leak. On the other hand, when two Bell states are shared, Eve gains the same amount of information, but may evade detection during verification by QBER (as lesser QBER is attained).

Therefore, use of an ω state is preferable over two Bell states. Another reason for preferring ω states is the three-particle entanglement shared by them. Moreover, we can compare the qubit efficiency of the protocol while using an ω state with the use of two Bell states. For our comparison, we have made a slight modification to the efficiency proposed by Cabello [40, 43, 44]. Here we take efficiency of our protocol as

$$\eta = \frac{s}{q} \tag{21}$$

where s is the number of secret bits transferred, and q is the number of qubits used as a resource in the protocol. As the success probability of the proposed positive operator-valued measurement in (7) is $1 - \cos 2\theta$, the efficiency of PP protocol when using a three-qubit partially entangled ω state from a nonorthogonal basis set, for transfer of two-bit information, will be $\eta_{omega} = \frac{2\times(1-\cos 2\theta)}{3}$. But, the efficiency of PP protocol when using two maximally entangled Bell states, for transfer of two-bit information is $\eta_{bell} = \frac{2}{4} = 0.5$. We can easily see that for all values of $37.7612^\circ < \theta \leqslant 45^\circ$, use of an ω state makes the protocol more efficient over the use of two Bell states.

Moreover, we can see that the information shared between the sender, receiver, and the eavesdropper falls down when a GHZ state is used as a resource. However, Eve's detection probability in control and message mode remains the same. Moreover, the QBER increases in presence of proposed attack 2, which can otherwise go undetected in control mode when the channel is more than 25 % noisy. This makes GHZ states a useful sharing resource for eavesdropper's detection. Thus, mixing ω states and GHZ states increases chances of an eavesdropper detection on intervention at the cost of slight downfall in the qubit efficiency, as discussed in the following section.

6 Mixed Sharing of GHZ and ω States for Secure QKD

In this section, we propose a more efficient PP protocol where Alice and Bob share either a $|\omega\rangle$ state (for transfer of two-bit information) or a GHZ state (for better eavesdropper's detection). Bob randomly chooses to prepare a $|\omega\rangle$ state or a GHZ state (optimal ratio of number of GHZ states and number of ω states shared in the protocol is described in the end of this section) and sends the travel photons of the prepared qubits to Alice. Alice (sender) clearly does not know Bob's selection and hence the shared state between them. Similarly, a potential eavesdropper is also ignorant about the shared state between Alice and Bob. Alice (sender) performs the encoding operations: $I^B \otimes I^C$, $I^B \otimes \sigma_z^C$, $\sigma_z^B \otimes I^C$, or $\sigma_z^B \otimes \sigma_z^C$ in the message mode in order to send 00, 01, 10, or 11, respectively. Therefore, when a $|\omega\rangle$ state is shared, Bob (receiver) uses required gates and a positive operator-valued measurement to distinguish nonorthogonal $|\omega\rangle$ states. On the other hand, when a GHZ state is shared, Bob performs a measurement in GHZ basis to distinguish two out of four operations as $I^B \otimes I^C$ generates the same outcome as $\sigma_z^B \otimes \sigma_z^C$, and $I^B \otimes \sigma_z^C$ generates the same outcome as $\sigma_z^B \otimes I^C$. Alice may randomly also switch to control mode as discussed by Bostrom and Felbinger [19] and announce the state of her travel photons to verify it with the state of home photon with Bob.

After all protocol runs either in message mode or control mode, Bob announces the turns when he had shared a GHZ state and asks Alice to announce her encoding operations performed in those turns. Then, Bob evaluates total QBER at each GHZ shared turn and aborts the protocol when QBER and detection due to control mode exceed the threshold of noise in the channel. This process also captures an eavesdropper who only attacks the travel photons in the "pong" route of the message mode. Thus, the motivation to use QBER for checking the presence of Eve comes from the modified control mode suggested by Nguyen to avoid DoS or disturbance attacks [26]. As QBER calculation is done when a GHZ state is shared, Bob can deterministically distinguish the measurement outcomes of a three-qubit measurement in an orthogonal GHZ basis shown in (1). On the other hand, three-qubit measurement in a nonorthogonal basis shown in (6) would lead to probabilistic distinguishability between the states, thus leading to an incorrect QBER.

The protocol no longer remains a means of secure direct communication. Rather, it can be used as a QKD protocol with enhanced security. If Alice and Bob share "w" $|\omega\rangle$ states and "g" GHZ states, then $2w(1-\cos 2\theta)$ information gets transferred from Alice to Bob. Moreover, the qubit efficiency in this case of mixed sharing would be

$$\eta_{mix} = \frac{2w(1-\cos 2\theta)}{3(w+g)} = \left(\frac{w}{w+g}\right)\eta_{omega} \qquad (22)$$

The above equation clearly shows that $\eta_{mix} \leqslant \eta_{omega}$. Now, for η_{mix} to be greater than η_{bell}, $\frac{w}{w+g} \geqslant \frac{3}{4(1-\cos 2\theta)}$, and therefore the minimum optimum ratio of "w" is to "g" for better qubit efficiency is

$$(w:g)_{min} = \frac{3}{1-4\cos 2\theta} \qquad (23)$$

where $37.7612^\circ < \theta \leqslant 45^\circ$. Thus, we can adjust the number of GHZ states and ω states according to the value of θ, so as to achieve enhanced efficiency for our protocol.

Furthermore, we can utilise the above mixing strategy in a quantum dialogue fashion. When Alice wishes to send message bits (k, l) and Bob wishes to send message bits (i, j), then the following steps occur: Alice randomly prepares a GHZ state or an ω state, performs $S^{BC}_{k,l}$ on the travel qubits, and sends these qubits to Bob; Bob, in turn, performs $S^{BC}_{i,j}$ on the qubits and sends them back to Alice. The same operations $S^{BC}_{i,j}$ and $S^{BC}_{k,l}$ are performed on travel photons of a GHZ state as that on the travel photons of an ω state as discussed in the article before. As only Alice knows the quantum state that is prepared, she performs the required measurement operations to find out the resultant bits (x, y), which she announces publicly. This not only allows her to find out the message bits (i, j) sent by Bob, but also enables Bob to calculate the message bits (k, l) that Alice sent him [26].

7 Conclusion

Our analysis shows the importance of partially entangled states such as $|\omega\rangle$ states over three-qubit maximally entangled GHZ states and two qubit maximally entangled Bell states for transfer of two-bit information using PP protocol. Although the use of partially entangled $|\omega\rangle$ states in the protocol involves distinguishing nonorthogonal states by positive operator-valued measurement, these states help us achieve higher qubit efficiency and increased security for the PP protocol. For example, Table 1 clearly shows that the protocol stands more secure against various eavesdropping operations, whenever an ω state is shared, as opposed to two Bell states. Further, Table 1 shows that the information shared between the sender and the receiver using a GHZ state is always very less as compared to the other two resources. Moreover, QBER increases for the proposed attack 2 (Tab. 1), where the control mode detection was lesser and an eavesdropper could easily evade detection in a more than 25 % noisy channel. Motivated by these results, we have shown that a mixed strategy involving mixed sharing of $|\omega\rangle$ state and GHZ state makes the protocol even more secure against various eavesdropping attacks with a slight downfall in the protocol's qubit efficiency. In order to further enhance the efficiency, we have suggested incorporation of Nguyen's efficient proposal for a quantum dialogue protocol in PPP using partially entangled ω states.

It will be interesting to extend our protocol with the proposed modifications in control modes [32, 33] to witness the improvements in PPP using three-qubit nonmaximally nonorthogonal entangled states. Further, in the future, it will be of interest to find out and compare the usefulness of nonmaximally entangled $|\omega\rangle$ states over maximally entangled states in other quantum cryptography protocols.

Acknowledgements: The authors thank MHRD and IIT Jodhpur for providing the research facility.

References

[1] C. H. Bennett and G. Brassard, in: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, New York 1985, vol. 175, p. 8.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] C. H. Bennett, G. Brassard, and D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[6] A. Beige, B. G. Engler, C. Kutrsiefer, and H. Weinfurter, Acta. Phys. Pol. A **101**, 357 (2002).
[7] G.-L. Long and X.-S. Liu, Phys. Rev. A **65**, 032302 (2002).
[8] G.-L. Long and X.-S. Liu, arXiv:quant-ph/0012056v2 (2000).
[9] F.-G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[10] F.-G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[11] M. Lucamarini, and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
[12] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, et al., Phys. Rev. Lett **118**, 220501 (2017).
[13] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, Sci. Bull. **62**, 1519 (2017).
[14] J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, et al., Sci. Appl. **5**, e16144 (2016).
[15] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, et al., Light Sci. Appl. **8**, 22 (2019).

[16] F.-G. Deng and G. L. Long, Phys. Rev. A **70**, 012311 (2004).
[17] P.-H. Niu, Z.-R. Zhou, Z.-S. Lin, Y.-B. Sheng, L.-G. Yin, et al., Sci. Bull. **63**, 1345 (2018).
[18] Z.-R. Zhou, Y.-B. Sheng, P.-H. Niu, L.-G. Yin, and G.-L. Long, arXiv:1805.07228 (2018).
[19] K. Bostrom and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[20] M. Ostermeyer and N. Walenta, Opt. Commun. **281**, 4540 (2008).
[21] H. Chen, Z.-Y. Zhou, A. J. J. Zangana, Z.-Q. Yin, J. Wu, et al., Sci. Reports **6**, 20962 (2016).
[22] A. Wojcik, Phys. Rev. Lett. **90**, 157901 (2003).
[23] Z. Zhang, Z. Man, and Y. Li, Phys. Lett. A **333**, 46 (2004).
[24] Q.-Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[25] Q.-Y. Cai, Phys. Lett. A **351**, 23 (2006).
[26] B. A. Nguyen, Phys. Lett. A **328**, 6 (2004).
[27] K. Bostrom and T. Felbinger, Phys. Lett. A **372**, 3953 (2008).
[28] P. Zawadzki, Quantum Inf. Process. **11**, 1419 (2012).
[29] M. Yoshida, T. Miyadera, and H. Imai, Journal of Quant. Inf. Sci. **3**, 16 (2013).
[30] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, Phys. Rev. A **88**, 062302 (2013).
[31] P. Zawadzki, Z. Puchala, and J. A. Miszczak, Quantum Inf. Process. **12**, 569 (2013).
[32] P. Zawadzki, Quantum Inf. Process. **14**, 2589 (2015).
[33] B. Zhang, W.-X. Shi, J. Wang, and C.-J. Tang, Int. J. Quantum Inf. **13**, 1550052 (2015).
[34] Y.-G. Han, Z.-Q. Yin, H.-W. Li, W. Chen, S. Wang, et al., Sci. Rep. **4**, 4936 (2014).
[35] A. Chamoli and C. M. Bhandari, Quantum Inf. Process. **8**, 347 (2009).
[36] G. Fei, G. FenZhuo, W. QiaoYan, and Z. FuChen, Sci. China Ser. G-Phys. Mech. Astron. **39**, 161 (2009).
[37] L. Jian, J. HaiFei, and J. Bo, Sci. China Phys. Mech. Astron. **54**, 1612 (2011).
[38] M. Naseri, Quantum Inf. Process. **9**, 693 (2010).
[39] M. Pavicic, Phys. Rev. A **87**, 042326 (2013).
[40] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
[41] M. Pavicic, Nanoscale Res. Lett. **12**, 552 (2017).
[42] X. S. Liu, G. L. Long, D. M. Tong, and F. Li, Phys. Rev. A **65**, 022304 (2002).
[43] A. Fahmi and M. Golshani, Phys. Rev. Lett. **100**, 018901 (2008).
[44] A. Cabello, Phys. Rev. Lett. **100**, 018902 (2008).