3

An improved Ping-Pong Protocol using three-qubit non-maximally non-orthogonal entangled states

3.1 INTRODUCTION

Ever since the proposal of Ping-Pong Protocol (PPP), its security has been questioned through efficient eavesdropping operations that can hamper secure communication using the protocol [Wójcik, 2003; Zhang *et al.*, 2004]. Cai discussed the vulnerability of protocol to DoS attack and an invisible photon eavesdropping attack, and further suggested improvements to protect the PP protocol against such attacks [Cai, 2003, 2006]. One of the major drawbacks of PPP was considered as its susceptibility to IR attack, however, the security of protocol was shown to be improved using the notions of a quantum dialogue [Nguyen, 2004]. Therefore, even after several security threats to the protocol, it remained a topic of intense discussion and used as a secure means of communication for an ideal quantum channel [Boström and Felbinger, 2008; Zawadzki, 2012; Yoshida *et al.*, 2013; Beaudry *et al.*, 2013]. In case of noisy or imperfect channels, a general security proof did not exist, and thus many modifications to the CM were put forth to enhance the security of the protocol [Zawadzki *et al.*, 2013; Zawadzki, 2015; Zhang *et al.*, 2015]. Later the security of the protocol was also proved in lossy channels, with the proposal of experimentally feasible enhancements to the protocol [Han *et al.*, 2014].

Multi-party extensions of PPP were also proposed [Chamoli and Bhandari, 2009; Gao *et al.*, 2008; Li *et al.*, 2011]. Chamoli and Bhandari have proposed that GHZ states can be used to send one bit and two bit information each from two different senders respectively, to a common receiver [Chamoli and Bhandari, 2009]. However, it was later analysed that if one of the senders is dishonest, he or she can gain all three bit information without being detected [Naseri, 2010]. In addition, it was further shown that in most QSDC protocols involving four encoded Bell pairs, an eavesdropper is able to distinguish between ψ and ϕ Bell states without being caught or detected [Pavičić, 2013]. On the other hand, the modified versions of CM [Zawadzki, 2015; Zhang *et al.*, 2015] enhance the security to detect an eavesdropper performing Pavičić's attack on quantum direct communication protocols using entangled Bell states.

In general, maximally entangled states such as two-qubit Bell states or three-qubit GHZ states are used for quasi-secure QSDC and secure QKD. However, the three-party extension of the protocol using the maximally entangled GHZ state [Chamoli and Bhandari, 2009] is highly susceptible to eavesdropping attacks [Naseri, 2010; Pavičić, 2013], as explained above. In this chapter, we study the usefulness of three-qubit non-maximally entangled states for the PPP. For our purpose, we analyse the protocol using two different sets of states separately as resources, i.e., three-qubit non-maximally entangled orthogonal set of states and three-qubit non-maximally entangled non-orthogonal set of states.

Our analysis suggests that three-qubit non-maximally entangled orthogonal states give same results as the maximally entangled three-qubit GHZ state. We find that the use of non-orthogonal non-maximally entangled states as resources is preferable as against the use of orthogonal set of non-maximally entangled states. Interestingly, the use of non-orthogonal three-qubit non-maximally entangled states lead to better qubit efficiency [Cabello, 2000] and

enhanced security in comparison to the use of two maximally entangled Bell states for transfer of two bit information. Nevertheless, the enhanced security and qubit efficiency is achieved at the cost of performing Positive Operator-valued Measurements (POVM) in order to differentiate non-orthogonal states. Although, we find the use of non-maximally entangled non-orthogonal states beneficial, the protocol is still susceptible to IR attack [Nguyen, 2004; Pavičić, 2017], which leads our discussions towards analysing the quantum dialogue version of the protocol. Further in the chapter, we demonstrate that a more secure protocol would comprise of a hybrid model with random sharing of maximally entangled GHZ states along with a three-qubit non-maximally entangled non-orthogonal states. Finally, we also extend our analysis in the realms of quantum game theory to analyse the three-party PP protocol.

3.2 EXTENSION OF THE PING-PONG PROTOCOL TO TRANSFER THREE BIT INFORMATION

The Ping-Pong protocol can be extended to communicate three bits of information to a receiver; two from one of the senders and one from the other sender using a three-qubit maximally entangled state shared between them [Chamoli and Bhandari, 2009]. For this, Alice prepares the initial state in any of the following GHZ states,

$$\begin{aligned} |\psi_{1,2}\rangle &= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle)_{ABC} \quad |\psi_{3,4}\rangle &= \frac{1}{\sqrt{2}}(|100\rangle \pm |011\rangle)_{ABC} \\ |\psi_{5,6}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)_{ABC} \quad |\psi_{7,8}\rangle &= \frac{1}{\sqrt{2}}(|110\rangle \pm |001\rangle)_{ABC} \end{aligned} \tag{3.1}$$

After preparing the three-qubit state, Alice sends travel photons B and C to Bob and Charlie, respectively, keeping the home photon A with her. In CM, Bob and Charlie measure the polarization of their photons in the computational basis and inform Alice about their measurement outcomes via a public channel. Alice also measures the polarization of her home photon and verifies if the measurement results are consistent with the initial shared state. In case of inconsistency of measurement results, eavesdropping is suspected and communication is terminated. In the MM, Charlie performs one of the four unitary operations on his qubit 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 qubit B to encode one bit information. These eight operations are same as the ones designed for a superdense coding protocol between multiparties to send a three bit information [Liu *et al.*, 2002]. After performing their individual unitary operations on both travel photons B and C, Bob and Charlie send them back to Alice, who then performs a joint three-qubit GHZ state measurement to distinguish the eight different set of encodings.

For eavesdropping on the proposed protocol, it was assumed that Eve prepares four auxiliary modes (B_x, B_y, C_x and C_y)- with two auxiliary modes in the state $|vv\rangle_{B_xC_x}$, and the other two auxiliary modes in the state $|00\rangle_{B_yC_y}$ (where "v" denotes vacuum). Eve then combines two of the auxiliary modes ($|v0\rangle_{B_xB_y}$) with the qubit B and the remaining two auxiliary modes ($|v0\rangle_{C_xC_y}$) with the qubit C. Eve's operations on the combined state lead to 50% channel loss in the CM; 25% of which occurs due to travel photon B sent to Bob and remaining 25% occurs due to travel photon C sent to Charlie. Moreover, Eve also gets detected in the MM, due to the induced channel loss in 50% of the cases, and by Alice receiving two photons through Bob's and Charlie's channels in 25% of cases. Therefore, they suggested that this protocol stands secure against such an attack [Chamoli and Bhandari, 2009].

3.2.1 Failure of the protocol on using maximally entangled states

In this section, it is shown that by performing extensions of Pavičić's attack [Pavičić, 2013], an eavesdropper can gain a lot of secret information without being caught in the CM. Interestingly,

Eve comes to know two out of three bits of information, which was assumed to be securely communicated. In fact, by performing the Pavičić's attack on travel photons B and C, respectively, the encoding operations I and $i\sigma_y$ of Bob can be easily distinguished by Eve. Moreover, two out of four operations of Charlie can also be easily recognized by an eavesdropper without being detected in the CM. For this, Eve can prepare the same four auxiliary modes (B_x, C_x, B_y and C_y) as suggested in the original protocol. Therefore, the proposed eavesdropping operation for two travel photons can be given as $P = P_{BB_xB_y} \otimes P_{CC_xC_y}$ where

$$\begin{aligned} P_{BB_xB_y} &= CNOT_{BB_y}(CNOT_{BB_x} \otimes I_{B_y})(I_B \otimes PBS_{B_xB_y}) \times CNOT_{BB_y}(CNOT_{BB_x} \otimes I_{B_y})(I_B \otimes H_{B_x} \otimes H_{B_y}) \\ P_{CC_xC_y} &= CNOT_{CC_y}(CNOT_{CC_x} \otimes I_{C_y})(I_C \otimes PBS_{B_xB_y}) \times CNOT_{CC_y}(CNOT_{CC_x} \otimes I_{C_y})(I_C \otimes H_{C_x} \otimes H_{C_y}) \end{aligned} \tag{3.2}$$

Eve performs attack P on 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. Interestingly, the presence of Eve in the travel path of photons remains hidden in the CM, as the correlation of the shared initial state does not change due to the eavesdropping attack P. Assuming that three parties share the GHZ state $|\psi_1\rangle_{ABC}$ (from Eq. (3.1)) as a starting resource, the final state of Alice's and Eve's photons after each encoding operation and attack is

$$\begin{aligned} |\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\ [P^\dagger(I^B \otimes \sigma_z^C)P]|\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\psi_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\ [P^\dagger(I^B \otimes \sigma_x^C)P]|\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\psi_3\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\ [P^\dagger(I^B \otimes i\sigma_y^C)P]|\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\psi_4\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\ [P^\dagger(i\sigma_y^B \otimes I^C)P]|\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\psi_6\rangle_{ABC}|0v\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\ [P^\dagger(i\sigma_y^B \otimes \sigma_z^C)P]|\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\psi_5\rangle_{ABC}|0v\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\ [P^\dagger(i\sigma_y^B \otimes \sigma_x^C)P]|\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= -|\psi_8\rangle_{ABC}|0v\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\ [P^\dagger(i\sigma_y^B \otimes i\sigma_y^C)P]|\psi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= -|\psi_7\rangle_{ABC}|0v\rangle_{B_xB_y}|0v\rangle_{C_xC_y} \end{aligned} \tag{3.3}$$

Therefore, Eve can conclude that,

(a) A click at B_y and C_y detectors implies either $I^B \otimes I^C$ or $I^B \otimes \sigma_z^C$ have been performed by Bob and Charlie,

(b) A click at B_y and C_x detectors implies either $I^B \otimes \sigma_x^C$ or $I^B \otimes i\sigma_y^C$ have been performed by Bob and Charlie,

(c) A click at B_x and C_y detectors implies either $i\sigma_y^B \otimes I^C$ or $i\sigma_y^B \otimes \sigma_z^C$ have been performed by Bob and Charlie, and

(d) A click at B_x and C_x detectors implies either $i\sigma_y^B \otimes \sigma_x^C$ or $i\sigma_y^B \otimes i\sigma_y^C$ have been performed by Bob and Charlie

Hence, four out of eight encoding operations of Bob and Charlie can be distinguished by Eve without being detected as Eve's ancillary states decouple completely from the initial shared state. Thus, the eavesdropper accurately knows two out of three classical bits of information being transferred from Bob and Charlie to Alice, thus compromising the security of the protocol. Moreover, one can also easily compute that 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, also indicating the inefficiency of maximally entangled GHZ states as a shared quantum resource in the protocol.

3.2.2 Use of non-maximally entangled states with orthogonal basis

In this section, the efficiency of a set of three-qubit non-maximally entangled states is analysed for PPP. For this, non-maximally entangled states belonging to the GHZ class, i.e., $|\chi\rangle = \frac{1}{\sqrt{2}}[sin\theta|000\rangle + sin\theta|011\rangle - cos\theta|101\rangle + cos\theta|110\rangle]$ are considered. Here, a set of three-qubit non-maximally entangled $|\chi\rangle$ states are used as resources over non-maximally entangled generalized GHZ states, i.e., $|\psi\rangle_{GHZ} = sin\theta|000\rangle + cos\theta|111\rangle$ due to higher nonlocal correlations between qubits in $|\chi\rangle$ states as compared to the nonlocal correlations between qubits in $|\psi\rangle_{GHZ}$ states. Figure 3.1 shows plots of quantum discord [Rulli and Sarandy, 2011] (as a measure of nonlocal correlations) for $|\chi\rangle$ and $|\psi\rangle_{GHZ}$ states. Clearly, the value of nonlocal correlations for $|\chi\rangle$ states exceeds that of GHZ class states for any given value of the state parameter θ.

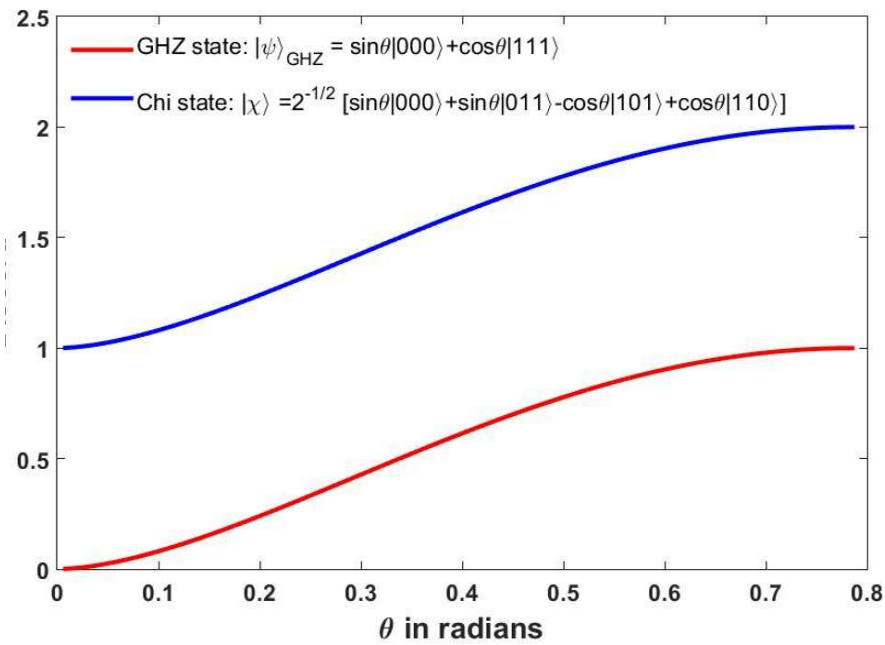

Figure 3.1 : A comparison of quantum discord for generalized GHZ and $|\chi\rangle$ states

After preparing the three qubits A, B, and C in one of the following non-maximally entangled orthonormal set of states, Alice sends qubit B to Bob and qubit C to Charlie, retaining

qubit A (home photon) with her.

$$
\begin{aligned}
|\chi_1\rangle &= \frac{1}{\sqrt{2}}[sin\theta|000\rangle + sin\theta|101\rangle + cos\theta|110\rangle - cos\theta|011\rangle]_{ABC} \\
|\chi_2\rangle &= \frac{1}{\sqrt{2}}[sin\theta|000\rangle - sin\theta|101\rangle + cos\theta|110\rangle + cos\theta|011\rangle]_{ABC} \\
|\chi_3\rangle &= \frac{1}{\sqrt{2}}[sin\theta|001\rangle + sin\theta|100\rangle + cos\theta|111\rangle - cos\theta|010\rangle]_{ABC} \\
|\chi_4\rangle &= \frac{1}{\sqrt{2}}[sin\theta|001\rangle - sin\theta|100\rangle + cos\theta|111\rangle + cos\theta|010\rangle]_{ABC} \\
|\chi_5\rangle &= \frac{1}{\sqrt{2}}[sin\theta|010\rangle + sin\theta|111\rangle + cos\theta|100\rangle - cos\theta|001\rangle]_{ABC} \\
|\chi_6\rangle &= \frac{1}{\sqrt{2}}[sin\theta|010\rangle - sin\theta|111\rangle + cos\theta|100\rangle + cos\theta|001\rangle]_{ABC} \\
|\chi_7\rangle &= \frac{1}{\sqrt{2}}[sin\theta|011\rangle + sin\theta|110\rangle + cos\theta|101\rangle - cos\theta|000\rangle]_{ABC} \\
|\chi_8\rangle &= \frac{1}{\sqrt{2}}[sin\theta|011\rangle - sin\theta|110\rangle + cos\theta|101\rangle + cos\theta|000\rangle]_{ABC}
\end{aligned}
\tag{3.4}
$$

The proposed CM here is same as discussed by Chamoli and Bhandari [Chamoli and Bhandari, 2009]. In MM, Charlie performs any of the four unitary operations (I, σ_x, $i\sigma_y$, or σ_z) on his qubit C to encode two-bit information 00, 01, 10 and 11, respectively. Similarly, Bob performs I or σ_x on his qubit 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 a single qubit measurement followed by a two-qubit Bell basis measurement to figure out the operations performed by Bob and Charlie.

Assuming that three parties share the state $|\chi_1\rangle_{ABC}$ in the beginning of the protocol and an eavesdropper performs an attack operation as described in Eq. (3.2), the final state evolves as,

$$
\begin{aligned}
|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
[P^\dagger(I^B \otimes \sigma_z^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\chi_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
[P^\dagger(I^B \otimes \sigma_x^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\chi_3\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
[P^\dagger(I^B \otimes i\sigma_y^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= -|\chi_4\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
[P^\dagger(\sigma_x^B \otimes I^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\chi_5\rangle_{ABC}|0v\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
[P^\dagger(\sigma_x^B \otimes \sigma_z^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\chi_6\rangle_{ABC}|0v\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
[P^\dagger(\sigma_x^B \otimes \sigma_x^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\chi_7\rangle_{ABC}|0v\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, and \\
[P^\dagger(\sigma_x^B \otimes i\sigma_y^C)P]|\chi_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= -|\chi_8\rangle_{ABC}|0v\rangle_{B_xB_y}|0v\rangle_{C_xC_y}
\end{aligned}
\tag{3.5}
$$

Thus, Eve infers that,

(a) A click at B_y and C_y detectors implies either $I^B \otimes I^C$ or $I^B \otimes \sigma_z^C$ have been performed by Bob and Charlie,

(b) A click at B_y and C_x detectors implies either $I^B \otimes \sigma_x^C$ or $I^B \otimes i\sigma_y^C$ have been performed by Bob and Charlie,

(c) A click at B_x and C_y detectors implies either $\sigma_x^B \otimes I^C$ or $\sigma_x^B \otimes \sigma_z^C$ have been performed by Bob and Charlie, and

(d) A click at B_x and C_x detectors implies either $\sigma_x^B \otimes \sigma_x^C$ or $\sigma_x^B \otimes i\sigma_y^C$ have been performed by Bob and Charlie

Similar to the previous case, Eve can accurately gain two bits of information being transferred from Bob and Charlie to Alice, and will still remain hidden in the CM. Therefore, by sharing a non-maximally entangled state, PPP still remains vulnerable to the eavesdropping operation in Eq. (3.2). It is thus proposed that if the parties involved share a set of non-maximally entangled non-orthogonal states, then the information revealed to an eavesdropper can be significantly reduced. Consequently, a PPP for transfer of three bit information using non-maximally entangled non-orthogonal states is proposed and analysed in detail.

3.2.3 Use of non-maximally entangled states with non-orthogonal basis

In order to study the usefulness of non-maximally entangled states with non-orthogonal basis, let Alice prepare one of the states (any four of which form an orthonormal set) as shown in Eq. (3.6). After preparing the initial resource, Alice sends qubit B to Bob and qubit C to Charlie, retaining qubit A (home photon) with her. The design of CM is the same as described by Chamoli and Bhandari [2009]. In MM, Charlie performs one of the four unitary operations (I, σ_x, $i\sigma_y$, or σ_z) on his qubit C to encode two-bit information 00, 01, 10 or 11, respectively. Similarly, Bob performs I or σ_z on his qubit B to encode one bit information.

$$
\begin{aligned}
|\omega_1\rangle &= \frac{1}{\sqrt{2}}[sin\theta|000\rangle + sin\theta|011\rangle + cos\theta|101\rangle - cos\theta|110\rangle]_{ABC} \\
|\omega_2\rangle &= \frac{1}{\sqrt{2}}[sin\theta|000\rangle + sin\theta|011\rangle - cos\theta|101\rangle + cos\theta|110\rangle]_{ABC} \\
|\omega_3\rangle &= \frac{1}{\sqrt{2}}[sin\theta|000\rangle - sin\theta|011\rangle + cos\theta|101\rangle + cos\theta|110\rangle]_{ABC} \\
|\omega_4\rangle &= \frac{1}{\sqrt{2}}[sin\theta|000\rangle - sin\theta|011\rangle - cos\theta|101\rangle - cos\theta|110\rangle]_{ABC} \\
|\omega_5\rangle &= \frac{1}{\sqrt{2}}[sin\theta|001\rangle + sin\theta|010\rangle + cos\theta|100\rangle - cos\theta|111\rangle]_{ABC} \\
|\omega_6\rangle &= \frac{1}{\sqrt{2}}[sin\theta|001\rangle + sin\theta|010\rangle - cos\theta|100\rangle + cos\theta|111\rangle]_{ABC} \\
|\omega_7\rangle &= \frac{1}{\sqrt{2}}[sin\theta|001\rangle - sin\theta|010\rangle + cos\theta|100\rangle + cos\theta|111\rangle]_{ABC} \\
|\omega_8\rangle &= \frac{1}{\sqrt{2}}[sin\theta|001\rangle - sin\theta|010\rangle - cos\theta|100\rangle - cos\theta|111\rangle]_{ABC}
\end{aligned}
\tag{3.6}
$$

After performing these operations, Bob and Charlie send back their photons to Alice, who then performs $R = CNOT_{AC}CNOT_{CB}H_BCNOT_{BC}CNOT_{CA}CNOT_{BA}$ on the photons in order to distinguish between the non-orthogonal states. Alice further performs a single qubit measurement in computational basis on photons A and B followed by a POVM on photon C with the following operators:

$$
\begin{aligned}
T_1 &= cos^2\theta|0\rangle\langle 0| - sin\theta cos\theta|0\rangle\langle 1| - sin\theta cos\theta|1\rangle\langle 0| + sin^2\theta|1\rangle\langle 1| \\
T_2 &= cos^2\theta|0\rangle\langle 0| + sin\theta cos\theta|0\rangle\langle 1| + sin\theta cos\theta|1\rangle\langle 0| + sin^2\theta|1\rangle\langle 1| \\
T_3 &= I - T_1 - T_2
\end{aligned}
\tag{3.7}
$$

The effect of R operation on different input states are shown in the following equation.

$$\begin{aligned}
R|\omega_1\rangle_{ABC} &= |0\rangle_A|0\rangle_B(sin\theta|0\rangle + cos\theta|1\rangle)_C \\
R|\omega_2\rangle_{ABC} &= |0\rangle_A|0\rangle_B(sin\theta|0\rangle - cos\theta|1\rangle)_C \\
R|\omega_3\rangle_{ABC} &= |0\rangle_A|1\rangle_B(sin\theta|0\rangle + cos\theta|1\rangle)_C \\
R|\omega_4\rangle_{ABC} &= |0\rangle_A|1\rangle_B(sin\theta|0\rangle - cos\theta|1\rangle)_C \\
R|\omega_5\rangle_{ABC} &= |1\rangle_A|1\rangle_B(sin\theta|0\rangle + cos\theta|1\rangle)_C \\
R|\omega_6\rangle_{ABC} &= |1\rangle_A|1\rangle_B(sin\theta|0\rangle - cos\theta|1\rangle)_C \\
R|\omega_7\rangle_{ABC} &= |1\rangle_A|0\rangle_B(sin\theta|0\rangle + cos\theta|1\rangle)_C \\
R|\omega_8\rangle_{ABC} &= |1\rangle_A|0\rangle_B(sin\theta|0\rangle - cos\theta|1\rangle)_C
\end{aligned} \tag{3.8}$$

Since Bob encodes using I and σ_z operations, Bob's information is secure against Eve's attack [Pavičić, 2013]. But, half of the encoding operations of Charlie can be distinguished by Eve without being caught in the CM. If three parties share the state $|\omega_2\rangle_{ABC}$ in the beginning of the protocol and an eavesdropper performs the attack operation as described in Eq. (3.2), the final state evolves as,

$$\begin{aligned}
|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
[P^\dagger(I^B \otimes \sigma_z^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\omega_3\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
[P^\dagger(\sigma_z^B \otimes I^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\omega_4\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}, \\
[P^\dagger(\sigma_z^B \otimes \sigma_z^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\omega_1\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y}
\end{aligned} \tag{3.9}$$

$$\begin{aligned}
|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\omega_6\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
[P^\dagger(I^B \otimes i\sigma_y^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= -|\omega_7\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
[P^\dagger(\sigma_z^B \otimes \sigma_x^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= |\omega_8\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}, \\
[P^\dagger(\sigma_z^B \otimes i\sigma_y^C)P]|\omega_2\rangle_{ABC}|v0\rangle_{B_xB_y}|v0\rangle_{C_xC_y} &= -|\omega_5\rangle_{ABC}|v0\rangle_{B_xB_y}|0v\rangle_{C_xC_y}
\end{aligned} \tag{3.10}$$

Thus, by performing appropriate measurements, Eve gains information analysing different clicks of the detectors. For example,

(a) A click at B_y and C_y detectors implies 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 performed by Bob and Charlie (Eq. (3.9)), and

(b) A click at B_y and C_x detectors implies 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 performed by Bob and Charlie (Eq. (3.10))

Therefore, two sets of encoding operations of Bob and Charlie can be distinguished by the eavesdropper. Hence, Eve can accurately guess one bit of secret information without being detected in the CM.

Thus from the above analysis, it can be concluded that in order to transfer three bits of information using a QSDC protocol, if the initial shared state between users is a non-maximally entangled state chosen from a set of non-orthogonal basis, then the protocol is less vulnerable to eavesdropping than sharing a maximally entangled GHZ state. The enhanced security comes at the cost of performing few unitary operations and a POVM to distinguish these non-orthogonal states. However, the protocol is not completely secure for three bits of information transfer. The security aspect of the protocol for different eavesdropping attacks is assessed in the next section.

3.3 ANALYSING SECURITY OF THE PP PROTOCOL FOR SENDING TWO BIT INFORMATION USING NON-MAXIMALLY ENTANGLED NON-ORTHOGONAL STATES

Only one bit secure information can be sent using three qubit maximally entangled GHZ states as explained in Section 3.2.1. In order to propose a secure protocol, one needs to use non-maximally entangled non-orthogonal states in PPP for transferring two bits of information instead of three. In such a scenario, the above discussed four operations in Eq. (3.9) can be used for encoding two 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 one of the states discussed in Eq. (3.6) and sends photons B and C to Bob and keeps photon A with herself. Now, Bob can perform the above operations $S_{i,j}^{BC}$ on qubits B and C to send two bits of information to Alice. Alternately, Alice and Bob may share two Bell pairs to transfer two bits of information using the original PPP [Boström and Felbinger, 2002]. Therefore, the vulnerability of above protocols to transfer two bit information is studied using Wojcik's attack [Wójcik, 2003], Pavičić's attack [Pavičić, 2013], and two efficient attacks proposed by us, one of which uses controlled functionality of a polarization beam splitter. In all eavesdropping operations, Eve introduces two ancillary photons (a vacuum and a horizontally polarized photon) to each travel photon. A detailed comparison is made between a protocol where two Bell states are used as an initial resource against the set of states in Eq. (3.6). In absence of an eavesdropper, if Alice uses $|\omega_2\rangle_{ABC}$ as the initial shared resource, the four encoding operations yield the following states:

$$\begin{aligned} I^B \otimes I^C |\omega_2\rangle_{ABC} &= |\omega_2\rangle_{ABC} \\ I^B \otimes \sigma_z^C |\omega_2\rangle_{ABC} &= |\omega_3\rangle_{ABC} \\ \sigma_z^B \otimes I^C |\omega_2\rangle_{ABC} &= |\omega_4\rangle_{ABC} \\ \sigma_z^B \otimes \sigma_z^C |\omega_2\rangle_{ABC} &= |\omega_1\rangle_{ABC} \end{aligned} \tag{3.11}$$

On the other hand, if Alice prefers to use two Bell states $|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}$ as the initial shared resource, following are the states after the encoding operations:

$$\begin{aligned} I^B \otimes I^C [|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= |\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C} \\ I^B \otimes \sigma_z^C [|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= -|\psi^+\rangle_{A_1B}|\psi^-\rangle_{A_2C} \\ \sigma_z^B \otimes I^C [|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= -|\psi^-\rangle_{A_1B}|\psi^+\rangle_{A_2C} \\ \sigma_z^B \otimes \sigma_z^C [|\psi^+\rangle_{A_1B}|\psi^+\rangle_{A_2C}] &= |\psi^-\rangle_{A_1B}|\psi^-\rangle_{A_2C} \end{aligned} \tag{3.12}$$

Following the first eavesdropping attack [Wójcik, 2003], Eve introduces $|v0\rangle_{x_1y_1}|v0\rangle_{x_2y_2}$ to the initial shared state and performs an operation $W = \mathsf{SWAP}_{Bx_1}\mathsf{SWAP}_{Cx_2}\mathsf{CPBS}_{Bx_1y_1}\mathsf{CPBS}_{Cx_2y_2}\mathsf{H}_{y_1}\mathsf{H}_{y_2}$ when Alice sends the two travel photons to Bob, where $\mathsf{CPBS}_{Bx_1y_1} = \mathsf{CNOT}_{By_1}(\mathsf{CNOT}_{Bx_1} \otimes I_{y_1})(I_B \otimes \mathsf{PBS}_{x_1y_1}) \times \mathsf{CNOT}_{By_1}(\mathsf{CNOT}_{Bx_1} \otimes I_{y_1})$ and $\mathsf{CPBS}_{Cx_2y_2} = \mathsf{CNOT}_{Cy_2}(\mathsf{CNOT}_{Cx_2} \otimes I_{y_2})(I_C \otimes \mathsf{PBS}_{x_2y_2}) \times \mathsf{CNOT}_{By_2}(\mathsf{CNOT}_{Bx_2} \otimes I_{y_2})$. Assuming that Alice prepares a non-maximally 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

$$
\begin{aligned}
W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} = \frac{sin\theta}{2\sqrt{2}}[&00000vv + 00v00v1 + 0v0001v + 0vv0011 + 0vv1100 + 0v1110v \\
&+ 01v11v0 + 01111vv] + \frac{cos\theta}{2\sqrt{2}}[1v0100v + 1vv1001 + 11010 + 11v10v1 \\
&- 10v01v0 - 10101vv - 1vv0110 - 1v1011v]_{ABCx_1x_2y_1y_2}
\end{aligned}
\tag{3.13}
$$

Now, if Bob chooses to operate in CM, Eve will be caught in 75% cases due to the introduction of vacuum states in the travel photons B and C. Alternately, if Bob opts for MM, he will encode the message using one of the four unitary operations $S_{i,j}^{BC}$ in Eq. (3.11). After performing the desired operation, Bob sends the travel qubits to Alice, where Eve performs the inverse eavesdropping operation $W^\dagger$ on en-route travel qubits. Considering the overall effects of eavesdropping on photons B and C, one expects the measurement results of Alice after receiving travel photons to be significantly different from Eq. (3.11). Therefore, the initial state after eavesdropping attack, depending on the encoding operations of Bob, will evolve as

$$
\begin{aligned}
W^\dagger[I^B \otimes I^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} &= |\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
W^\dagger[I^B \otimes \sigma_z^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} &= \frac{1}{2}[(|\omega_2\rangle + |\omega_3\rangle]_{ABC})|vv00\rangle_{x_1x_2y_1y_2} \\
&\quad + (|\omega_2\rangle - |\omega_3\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2}] \\
W^\dagger[\sigma_z^B \otimes I^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} &= \frac{1}{2}[(|\omega_2\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&\quad + (|\omega_2\rangle - |\omega_4\rangle)_{ABC}|vv10\rangle_{x_1x_2y_1y_2}] \\
W^\dagger[\sigma_z^B \otimes \sigma_z^C]W|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} &= \frac{1}{4}[(|\omega_1\rangle + |\omega_2\rangle + |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&\quad + (|\omega_1\rangle + |\omega_2\rangle - |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv11\rangle_{x_1x_2y_1y_2} \\
&\quad - (|\omega_1\rangle - |\omega_2\rangle - |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv10\rangle_{x_1x_2y_1y_2} \\
&\quad - (|\omega_1\rangle - |\omega_2\rangle + |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2}]
\end{aligned}
\tag{3.14}
$$

Since 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 bits. Also, the mutual information between Bob (sender) and Eve is 0.6225 bits and that between Alice (receiver) and Eve is 0.1474 bits. The mutual information evaluated between different users is exactly the same as the mutual information if Eve performs Wojcik's operation on two travel photons which are individual parts of two Bell pairs [Wójcik, 2003]. The only difference between two protocols is in terms of Eve's chances of getting detected in CM. While using two Bell pairs, Eve introduces losses due to vacuum in half of the cases, and hence her probability of being detected in CM is 50% [Wójcik, 2003]. On the other hand, if the protocol employs an ω state as the initial shared state, then Eve's detection probability increases to 75%. Thus to avoid information leak under such attacks, a $|\omega\rangle$ state will be preferred over two Bell states.

Now if another eavesdropping attack is considered, which has no swap operation, but has additional Hadamard operations on the "x" photons of Eve, i.e., $P = \mathsf{CPBS}_{Bx_1y_1}\mathsf{CPBS}_{Cx_2y_2}\mathsf{H}_{x_1}\mathsf{H}_{x_2}\mathsf{H}_{y_1}\mathsf{H}_{y_2}$ [Pavičić, 2013], then Eve does not get detected in the CM since no vacuum photons are introduced. Also, Eve does not get any information by performing such an operation irrespective of whether the protocol uses a $|\omega\rangle$ state or two Bell states.

To further analyse the security of this protocol, an eavesdropping operation, similar to the one proposed by Zhang *et al.* [Zhang *et al.*, 2004] is proposed. By performing this eavesdropping attack, Eve gains same information in the case of Wojcik's attack, but reduces its probability of

being detected. For this, Eve introduces $|v0\rangle_{x_1y_1}|v0\rangle_{x_2y_2}$ to the initial shared state and performs $Q = \mathsf{CPBS}_{y_1Bx_1}\mathsf{CPBS}_{y_2Cx_2}\mathsf{CNOT}_{By_1}\mathsf{CNOT}_{Cy_2}\mathsf{CPBS}_{Bx_1y_1}\mathsf{CPBS}_{Cx_2y_2}\mathsf{H}_{y_1}\mathsf{H}_{y_2}$ when Alice sends two travel photons to Bob. This proposed eavesdropping operation contains 36 controlled spin flip operations, 8 polarization beam splitters, and 4 Hadamard operations, as opposed to Wojcik's attack which contains 16 controlled spin flip operations, 4 polarization beam splitters, 4 swap operations, and 4 Hadamard operations. Although the above proposed attack involves more operations than Wojcik's attack, it is assumed that Eve has unlimited power constrained only by the laws of physics. The attack further leads to reduction in Eve's chances of detection while gaining partial information, making it significantly important to study.

The study now proceeds to discuss the proposed attack in detail. Assuming that Alice prepares a non-maximally entangled state $|\omega_2\rangle_{ABC}$, sends photons B and C to Bob, and Eve performs our proposed attack on the travel path from Alice to Bob, the state reduces to

$$\begin{aligned} Q|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2} = \frac{sin\theta}{2\sqrt{2}}[&00000vv + 0000vv1 + 000v01v + 000vv11 + 0vv1111 \\ &+ 0v1111v + 01v11v1 + 01111vv] + \frac{cos\theta}{2\sqrt{2}}[1v0101v + 1v01v11 + 11010vv \\ &+ 1101vv1 - 10v01v1 - 10101vv - 10vv111 - 101v11v]_{ABCx_1x_2y_1y_2} \end{aligned} \tag{3.15}$$

Now, if Bob chooses to operate in CM, Eve will be detected in $\left(\frac{3+cos^2\theta}{8} \times 100\right)\%$ cases due to the introduction of losses in form of vacuum as shown in Eq. (3.15). Alternately, if Bob opts for MM, he will encode the message through one of the above four unitary operations in Eq. (3.11). After operation in either mode, Bob sends back the travel qubits to Alice, where Eve captures these qubits mid-way and performs the inverse eavesdropping attack $Q^\dagger$ before the qubits reach Alice. Upon receiving the qubits, Alice performs required measurements, thus obtaining the same measurement result (as shown in Eq. (3.14)) that was attained when an eavesdropper performed Wojcik's attack in similar fashion. Therefore mutual information between respective parties also remains the same, as after Wojcik's attack. On the other hand, if two Bell states are shared between Alice and Bob, Eve introduces losses in form of vacuum with a probability of 0.4375, and hence gets detected in 43.75% cases. Clearly, for all values of $\theta \in (0°, 45°)$, Eve's detection probability is always more when an ω state is shared as against two Bell states.

Furthermore, another attack operation is proposed in which Eve introduces $|v0\rangle_{x_1y_1}|v0\rangle_{x_2y_2}$ to the initial shared state and performs two attacks when Alice sends the 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 polarization beam splitter 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. The operation when performed on a non-maximally entangled state $|\omega_2\rangle_{ABC}$, yields

$$\begin{aligned} bs[Q|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2}] = \frac{sin\theta}{2\sqrt{2}}[&00000vv + 0000vv1 + 000v01v + 000vv11 + 01vv111 + 011v11 \\ &+ 01v11v1 + 01111vv] + \frac{cos\theta}{2\sqrt{2}}[110v01v + 110vv11 + 11010vv + 1101vv1 \\ &- 10v01v1 - 10101vv - 10vv111 - 101v11v]_{ABCx_1x_2y_1y_2} \end{aligned} \tag{3.16}$$

If the same operation is performed on two Bell states, it leads to

$$
\begin{aligned}
&bs[Q|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2}] \\
&= \frac{1}{4}[|01\rangle_{A_1B}|v1+1v\rangle_{x_1y_1} + |10\rangle_{A_1B}|0v+v1\rangle_{x_1y_1}] \otimes [|0v11+011v+100v+10v1\rangle_{A_2Cx_2y_2}]
\end{aligned}
\tag{3.17}
$$

Now, Bob (sender) performs his encoding operations on the non-maximally entangled state represented in Eq. (3.16), and assumes that on performing her required measurements will get measurements outcomes as represented in Eq. (3.11). Similarly, in case of Bell pairs, Bob (sender) assumes Alice (receiver) to get her measurement outcomes as represented in Eq. (3.12). However, in presence of Eve, the ideal case does not occur. When the travel photons are sent back to Alice, Eve performs $Q^\dagger$ operation and the final state evolves differently. Eq. (3.18) shows the measurement outcomes when $|\omega_2\rangle$ state is used as a resource and Eq. (3.19) shows the measurement outcomes when a pair of Bell states are used as a resource. In addition, Eqs. (3.16) and (3.17) clearly indicate that in CM, Eve gets detected in 25% cases when $|\omega_2\rangle$ state and Bell pairs are used as resources, respectively. Moreover, in MM, since Alice has received a vacuum photon instead of a polarized photon in 25% cases, she does not get any measurement result with a probability of 25%. This consistency of getting vacuum or no result in both CM and MM in almost equal i.e., 25% cases may confuse Alice and Bob about a possible induced channel loss and eavesdropping may get concealed easily.

Table 3.1 compares values of mutual information and probabilities of eavesdropper's detection for various attacks with the use of an ω state, two Bell states, and a GHZ state, respectively with the encoding operations I and σ_z on each travel qubit. Clearly, the probability of Eve's detection remains same if one starts with either $|\omega_2\rangle$ state or a pair of Bell states, the mutual information between the sender and the receiver introduced by our second attack is different in each case. Although, the mutual information between the sender and the receiver is lesser if an ω state is used, nevertheless, 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 detecting an eavesdropper through evaluation of QBER at the end of the protocol by compromising few message bits; making the protocol more secure. On the other hand, when two Bell states are shared, an eavesdropper learns same amount of information, but may evade detection during QBER analysis

(as lesser QBER is attained).

$$
\begin{aligned}
Q^{\dagger}[I^B \otimes I^C]bs(Q(|\omega_2\rangle_{ABC}|vv00\rangle_{x_1x_2y_1y_2})) &= \frac{1}{2\sqrt{2}}(sin\theta|0v1\rangle + cos\theta|1v0\rangle)_{ABC}|1v00 - 1v10\rangle_{x_1x_2y_1y_2} \\
&+ \frac{1}{2}(|\omega_2\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} + \frac{1}{4}(|\omega_2\rangle - |\omega_4\rangle)_{ABC}|vv00 - vv10\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})) &= \frac{1}{4}(|\omega_1\rangle + |\omega_2\rangle + |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&+ \frac{1}{8}(|\omega_1\rangle + |\omega_2\rangle - |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01 - vv11\rangle_{x_1x_2y_1y_2} \\
&- \frac{1}{4}(|\omega_1\rangle - |\omega_2\rangle + |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2} \\
&- \frac{1}{8}(|\omega_1\rangle - |\omega_2\rangle - |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00 - vv10\rangle_{x_1x_2y_1y_2} \\
&+ \frac{sin\theta}{2\sqrt{2}}|0v1\rangle_{ABC}|1v01 - 1v11\rangle_{x_1x_2y_1y_2} + \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})) &= -\frac{1}{2\sqrt{2}}(sin\theta|0v1\rangle + cos\theta|1v0\rangle)_{ABC}|1v00 - 1v10\rangle_{x_1x_2y_1y_2} \\
&+ \frac{1}{2}(|\omega_2\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} - \frac{1}{4}(|\omega_2\rangle - |\omega_4\rangle)_{ABC}|vv00 - vv10\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})) &= \frac{1}{4}(|\omega_1\rangle + |\omega_2\rangle + |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00\rangle_{x_1x_2y_1y_2} \\
&- \frac{1}{8}(|\omega_1\rangle + |\omega_2\rangle - |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01 - vv11\rangle_{x_1x_2y_1y_2} \\
&- \frac{1}{4}(|\omega_1\rangle - |\omega_2\rangle + |\omega_3\rangle - |\omega_4\rangle)_{ABC}|vv01\rangle_{x_1x_2y_1y_2} \\
&+ \frac{1}{8}(|\omega_1\rangle - |\omega_2\rangle - |\omega_3\rangle + |\omega_4\rangle)_{ABC}|vv00 - vv10\rangle_{x_1x_2y_1y_2} \\
&- \frac{sin\theta}{2\sqrt{2}}|0v1\rangle_{ABC}|1v01 - 1v11\rangle_{x_1x_2y_1y_2} - \frac{cos\theta}{2\sqrt{2}}|1v0\rangle_{ABC}|1v00 - 1v10\rangle_{x_1x_2y_1y_2}
\end{aligned}
\tag{3.18}
$$

$$
\begin{aligned}
Q^{\dagger}[I^B \otimes I^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) &= \frac{1}{4}[|\psi^+\rangle_{A_1B}(3|v0\rangle - |v1\rangle)_{x_1y_1} \\
&- |\psi^-\rangle_{A_1B}(|v0\rangle + |v1\rangle)_{x_1y_1} + \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \otimes [|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2}] \\
Q^{\dagger}[I^B \otimes \sigma_z^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) &= \frac{1}{8}[|\psi^+\rangle_{A_1B}(3|v0\rangle - |v1\rangle)_{x_1y_1} - |\psi^-\rangle_{A_1B}(|v0\rangle \\
&+ |v1\rangle)_{x_1y_1} + \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \otimes [|\psi^+\rangle_{A_2C}(|v0\rangle + |v1\rangle)_{x_2y_2} - |\psi^-\rangle_{A_2C}(|v0\rangle - |v1\rangle)_{x_2y_2}] \\
Q^{\dagger}[\sigma_z^B \otimes I^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) &= \frac{1}{4}[|\psi^+\rangle_{A_1B}(|v0\rangle + |v1\rangle)_{x_1y_1} \\
&- |\psi^-\rangle_{A_1B}(3|v0\rangle - |v1\rangle)_{x_1y_1} - \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \otimes [|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2}] \\
Q^{\dagger}[\sigma_z^B \otimes \sigma_z^C]bs(Q(|\psi^+\rangle_{A_1B}|v0\rangle_{x_1y_1}|\psi^+\rangle_{A_2C}|v0\rangle_{x_2y_2})) &= \frac{1}{8}[|\psi^+\rangle_{A_1B}(|v0\rangle + |v1\rangle)_{x_1y_1} - |\psi^-\rangle_{A_1B}(3|v0\rangle \\
&- |v1\rangle)_{x_1y_1} - \sqrt{2}|0v\rangle_{A_1B}(|10\rangle - |11\rangle)_{x_1y_1}] \otimes [|\psi^+\rangle_{A_2C}(|v0\rangle + |v1\rangle)_{x_2y_2} - |\psi^-\rangle_{A_2C}(|v0\rangle - |v1\rangle)_{x_2y_2}]
\end{aligned}
\tag{3.19}
$$

Therefore, use of an ω state is preferable over two Bell states. Moreover, since ω states bear tripartite entanglement, they further become useful for multi-party communication, as opposed to

Table 3.1 : 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	Pavičić's attack	Proposed attack 1	Proposed attack 2
One ω state	$I_1 = \mathsf{I}(sender : receiver)$	0.6225	2	0.6225	0.5447
	$I_2 = \mathsf{I}(sender : eavesdropper)$	0.6225	0	0.6225	0.5447
	$I_3 = \mathsf{I}(receiver : eavesdropper)$	0.1474	0	0.1474	0.3666
	Eve's chances of detection in CM:	75%	0%	$12.5(3+cos^2\theta)\%$	25%
	Eve's chances of detection in MM:	0%	0%	0%	25%
	QBER:	0.4375	0	0.4375	0.46875
Two Bell states	$I_1 = \mathsf{I}(sender : receiver)$	0.6225	2	0.6225	0.8071
	$I_2 = \mathsf{I}(sender : eavesdropper)$	0.6225	0	0.6225	0.5447
	$I_3 = \mathsf{I}(receiver : eavesdropper)$	0.1474	0	0.1474	0.3666
	Eve's chances of detection in CM:	50%	0%	43.75%	25%
	Eve's chances of detection in MM:	0%	0%	0%	25%
	QBER:	0.4375	0	0.4375	0.28125
One GHZ state	$I_1 = \mathsf{I}(sender : receiver)$	0.0488	1	0.0488	0.3112
	$I_2 = \mathsf{I}(sender : eavesdropper)$	0	0	0	0
	$I_3 = \mathsf{I}(receiver : eavesdropper)$	0.0488	0	0.0488	0.3112
	Eve's chances of detection in CM:	75%	0%	50%	25%
	Eve's chances of detection in MM:	0%	0%	0%	25%
	QBER:	0.375	0	0.375	0.625

Bell states. Moreover, one can compare the qubit efficiency of the protocol while using an ω state with the use of two Bell states. For our comparison, a slight modification to the efficiency proposed by Cabello [Cabello, 2000; Fahmi and Golshani, 2008; Cabello, 2008] is made. Here, the efficiency of our protocol is defined as

$$\eta^{eff} = \frac{s}{q} \tag{3.20}$$

where "s" is the number of secret bits transferred and "q" is the number of qubits of a quantum resource in the protocol. Since the success probability of the proposed POVM in Eq. (3.7) is $1-cos2\theta$, the efficiency of PP protocol using a three-qubit non-maximally entangled ω state for transfer of two bits of information, will be $\eta_{omega}^{eff} = \frac{2\times(1-cos2\theta)}{3}$. Further, the efficiency of PP protocol using two maximally entangled Bell states, for transfer of two bits of information is $\eta_{bell}^{eff} = \frac{2}{4} = 0.5$. It can be easily seen that for all values of $37.7612^\circ < \theta \leq 45^\circ$, use of an ω state makes the protocol more efficient over the use of two Bell states. Furthermore, the numerals in Table 3.1 show 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 CM and MM remains same. Moreover, the QBER increases in presence of proposed attack 2, which can otherwise remain concealed in CM when the channel is more than 25% noisy. This makes GHZ states a useful resource for eavesdropper's detection. This indicates a possibility that mixing ω states and GHZ states increases chances of Eve being caught on intervention at the cost of slight downfall in the qubit efficiency. This is discussed in detail in the upcoming Section 3.3.3 of this chapter.

3.3.1 A game-theoretic model for PPP to send two bits of information

In order to enable easy analysis of values shown in Table 3.1, the game-theoretic model of the game is studied, where the payoffs of the team of a sender and the intended receiver (Player 1), and the eavesdropper (Player 2) defined as

$$\$_{sender-receiver} = w_a I_1 - w_b[I_2+I_3] + w_c\left[\frac{p_d+\text{QBER}}{2}\right] \tag{3.21}$$

and

$$\$_{eavesdropper} = w_d[I_2+I_3] - w_e I_1 + w_f\left[1-\frac{p_d+\text{QBER}}{2}\right] \tag{3.22}$$

respectively, where I_1, I_2, I_3 are pairwise mutual information between the sender, receiver, and the eavesdropper; $w_a, w_b, w_c, w_d, w_e, w_f$ are positive real numbers and considered as weights attached to each quantity in the payoff; p_d is the probability of detection of Eve; and QBER is evaluated by verifying few encoded bits in MM. On considering different strategies of the sender and receiver as sharing qubits of different quantum states among themselves, i.e., A_1 corresponds to sharing one ω state (three-qubit non-orthogonal basis), A_2 corresponds to sharing two Bell states, and A_3 corresponds to sharing one GHZ state (three-qubit orthogonal basis). On the other hand, the strategies of an eavesdropper are: E_1 (Wojcik's attack), E_2 (Pavičić's attack), E_3 (Proposed attack 1), and E_4 (Proposed attack 2). Thus, payoffs of both players for the above defined different strategies are shown in Table 3.2 and 3.3, respectively.

Inspired by the analysis performed in Section 2.4 of Chapter 2, the conditions for NE in the game can be evaluated as demonstrated in Table 3.4. If $w_a = w_b = w_d = w_e = w_I$ and $w_c = w_f = w_P$, then the game comprises of the NE as shown in Table 3.5. Depending on the different values of weights w_I and w_P, (A_1, E_2), (A_2, E_2), (A_2, E_3), (A_3, E_3), and/or (A_3, E_4) become the NE points in this PPP game.

3.3.2 Quantum dialogue analogue for PPP

Additionally, the feasibility of our proposed protocol against the attack proposed by Nguyen [Nguyen, 2004] is further checked. Similar to the case of PPP using a Bell pair, the DoS attack by an eavesdropper goes undetected in the discussed protocol set-up (using non-maximally entangled non-orthogonal states) as well. However, one can always implement a similar modification in the CM as suggested by Nguyen for the three qubit PPP at the cost

Table 3.2 : Payoffs of the team of a sender and a receiver in the game-theoretic model of PPP for transmission of two bits of message

Player1 \ Player2	E_1	E_2	E_3	E_4
A_1	$0.6225w_a - 0.7699w_b$ $+0.59375w_c$	$2w_a$	$0.6225w_a - 0.7699w_b$ $+(0.40625$ $+0.0625cos^2\theta)w_c$	$0.5447w_a - 0.9113w_b$ $+0.359375w_c$
A_2	$0.6225w_a - 0.7699w_b$ $+0.46875w_c$	$2w_a$	$0.6225w_a - 0.7699w_b$ $+0.4375w_c$	$0.8071w_a - 0.9113w_b$ $+0.265625w_c$
A_3	$0.0488w_a - 0.0488w_b$ $+0.5625w_c$	w_a	$0.0488w_a - 0.0488w_b$ $+0.4375w_c$	$0.3112w_a - 0.3112w_b$ $+0.4375w_c$

Table 3.3 : Payoffs of an eavesdropper in the game-theoretic model of PPP for transmission of two bits of message

Player1 \ Player2	E_1	E_2	E_3	E_4
A_1	$0.7699w_d - 0.6225w_e$ $+0.40625w_f$	$-2w_e$ $+w_f$	$0.7699w_d - 0.6225w_e$ $+(0.59375$ $-0.0625cos^2\theta)w_f$	$0.9113w_d - 0.5447w_e$ $+0.640625w_f$
A_2	$0.7699w_d - 0.6225w_e$ $+0.53125w_f$	$-2w_e$ $+w_f$	$0.7699w_d - 0.6225w_e$ $+0.5625w_f$	$0.9113w_d - 0.8071w_e$ $+0.734375w_f$
A_3	$0.0488w_d - 0.0488w_e$ $+0.4375w_f$	$-w_e$ $+w_f$	$0.0488w_d - 0.0488w_e$ $+0.5625w_f$	$0.3112w_d - 0.3112w_e$ $+0.5625w_f$

of performing a three-qubit measurement at the receiver's end at every CM. This modification prevents the occurrence of disturbance attack but is still susceptible to IR attack [Nguyen, 2004]. 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 are respective parts of two entangled dummy Bell pairs. Bob now performs 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 by knowing 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 and still remains undetected. In order to make our protocol resistant to the IR attack, the quantum dialogue version [Nguyen, 2004] is incorporated into the PPP using non-maximally entangled states with non-orthogonal basis.

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 "ping" route. Alice also announces that she has sent the travel

Table 3.4 : Conditions for (A_i, E_j) to be a Nash equilibrium in a three-qubit PP game

Nash Equilibrium	Conditions
(A_1, E_2)	$0.359375w_f \geq 0.9113w_d + 1.4553w_e$
(A_1, E_4)	$0.359375w_f \leq 0.9113w_d + 1.4553w_e$, $w_c \geq 2.799w_a$, and $0.2335w_a \geq 0.6001w_b + 0.078125w_c$
(A_2, E_2)	$0.265625w_f \geq 0.9113w_d + 1.929w_e$
(A_2, E_3)	$0.1846w_e \geq 0.1414w_d + 0.171875w_f$, and $cos^2\theta \leq 0.5$, and $0.4375w_f \leq 0.7699w_d + 1.3775w_e$, and $w_a \geq 1.257w_b$
(A_2, E_4)	$0.1846w_e \leq 0.1414w_d + 0.171875w_f$, and $0.265625w_f \leq 0.9113w_d + 1.1929w_e$, and $w_c \leq 2.7989w_a$, and $0.4959w_a \geq 0.6001w_b + 0.171875w_c$
(A_3, E_3)	$w_d \geq w_e$, and $0.4375w_f \leq 0.0488w_d + 0.9512w_e$, and $w_a \leq 1.257w_b$
(A_3, E_4)	$w_d \leq w_e$, and $0.4375w_f \leq 0.3112w_d + 0.6888w_e$, and $0.2335w_a \leq 0.6001w_b + 0.078125w_c$, and $0.4959w_a \leq 0.6001w_b + 0.171875w_c$

qubits, which is later acknowledged by Bob on the receipt of qubits. Then, Bob encodes his message bits (i, j) by performing the encoding $S^{BC}_{i,j}$ on travel photons, and sends back travel qubits to Alice. On receiving the qubits, Alice performs required measurements on qubits to distinguish the four states, and thus decodes the encoded secret message. On performing these measurements, Alice publicly announces the resultant message bits (let (x, y)) to Bob. Since,

$$S^{BC}_{i,j} S^{BC}_{k,l} = S^{BC}_{i\oplus k, j\oplus l} \tag{3.23}$$

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 $\frac{1}{4}$ 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 CM runs in the total runs of the protocol [Nguyen, 2004].

Table 3.5 : Conditions for different Nash equilibria in a three-qubit PP game

Nash Equilibrium	Conditions
(A_1, E_2)	$w_P \geq 6.585 w_I$
(A_2, E_2)	$w_P \geq 10.693 w_I$
(A_2, E_3)	$cos^2\theta \leq 0.5$, and $w_I \leq 0$, and $w_I \geq 0.2037 w_P$
(A_3, E_3)	$w_I \geq 0$
(A_3, E_4)	$w_I \geq 0.4375 w_P$, and $w_P \geq 0$

3.3.3 A hybrid model for secure QKD

In this section, a more efficient PPP is proposed where Alice and Bob either share 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, and sends the travel photons to Alice. The optimal ratio of number of GHZ states and number of ω states shared in the protocol is discussed in the end of this section. Alice (sender) does not know Bob's selection, and hence the shared state (GHZ or ω state) between them. Similarly, possible 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 MM in order to send 00, 01, 10 or 11, respectively. Therefore, when a $|\omega\rangle$ state is shared, Bob (receiver) performs appropriate unitary transformations and a POVM to distinguish non-orthogonal $|\omega\rangle$ 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 since $I^B \otimes I^C$ 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 CM as discussed in the original PPP [Boström and Felbinger, 2002], and announce the state of her travel photons to verify it with the state of home photon with Bob.

After all MM and CM runs of the protocol, 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 detection during CM exceeds 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 MM. Thus, the motivation to use QBER for checking the presence of Eve comes from the modified CM suggested by Nguyen to avoid DoS or disturbance attacks [Nguyen, 2004]. Since QBER calculation is performed when a GHZ state is shared, Bob can deterministically distinguish the measurement outcomes of a three-qubit measurements in an orthogonal GHZ basis shown in Eq. (3.1). On the other hand, three-qubit measurement in a non-orthogonal basis shown in Eq. (3.6) would lead to probabilistic distinguishability between the states, thus leading to an incorrect QBER.

The protocol no longer remains a means of QSDC. 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 the amount of information transferred from Alice to Bob is $2w(1 - cos2\theta)$. Moreover, the qubit efficiency in this

case of mixed sharing would be

$$\eta_{mix}^{eff} = \frac{2w(1-cos2\theta)}{3(w+g)} = \left(\frac{w}{w+g}\right)\eta_{omega}^{eff} \tag{3.24}$$

The above equation clearly shows that $\eta_{mix}^{eff} \leq \eta_{omega}^{eff}$. Now, for η_{mix}^{eff} to be more than η_{bell}^{eff}, $\frac{w}{w+g} \geq \frac{3}{4(1-cos2\theta)}$, and hence the minimum optimum ratio of "w" is to "g" for enhanced qubit efficiency is

$$(w:g)_{min} = \frac{3}{1-4cos2\theta} \tag{3.25}$$

where $37.7612^\circ < \theta \leq 45^\circ$. Thus, the number of GHZ states and ω states can be adjusted according to the value of θ, so as to achieve improved qubit efficiency for our protocol.

Furthermore, the above hybrid model can be utilized 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 $S_{k,l}^{BC}$ on the travel qubits, and sends these qubits to Bob; Bob, in turn, performs $S_{i,j}^{BC}$ on the qubits, and sends them back to Alice. The same operations $S_{i,j}^{BC}$ and $S_{k,l}^{BC}$ are performed on travel photons of a GHZ state as that on the travel photons of an ω state as discussed in the chapter before. Since 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 [Nguyen, 2004].

3.4 CONCLUSIONS

The analysis presented here showed the importance of non-maximally 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 PPP. Though the use of non-maximally entangled $|\omega\rangle$ states in the protocol involves distinguishing non-orthogonal states by POVM, these states helped us achieve higher qubit efficiency and increased security for the PPP. For example, Table 3.1 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 3.1 shows that the information shared between the sender and the receiver using a GHZ state is always very less as compared to other two resources. Moreover, we also found that QBER increases for the Proposed attack 2 where the CM detection was lesser and an eavesdropper could easily evade detection in a more than 25% noisy channel. Motivated by these results, we further demonstrated that a mixed strategy involving mixed sharing of $|\omega\rangle$ and GHZ states 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 suggested to incorporate an efficient proposal for a quantum dialogue protocol in PPP using non-maximally entangled ω states. In order to facilitate the analysis, a PPP game similar to the one discussed in Chapter 2 is also designed. Our analysis further described different equilibrium strategies of the sender along with the receiver, and an eavesdropper.

...