2
A game-theoretic perspective of Ping-Pong Protocol

The art of doing mathematics consists in finding that special case which contains all the germs of generality.

—*David Hilbert*

2.1 INTRODUCTION

A game is a competitive task accomplished by two or more rational players, following a set of rules governing their actions in the task, and conditions of win and loss in the competition. Each player opts for a particular strategic move depending on the certain background details in a game such as knowledge about other players, knowledge about allowed strategies, and how different strategies will lead to varying outcomes of the game. Clearly, every move that a player takes corresponds to a certain *Payoff* or reward. Payoff or reward or utility are numbers which quantify the advantage each player gets for their respective moves. Therefore, it signifies the desirability of each player to perform a particular strategy. Obviously, the aim of each player is to opt for a strategy that optimizes his/her payoff. For a finite game, John F. Nash [Nash, 1950, 1951] described a stable point -Nash Equilibrium (NE)- which optimizes the payoffs of all players in the game and which corresponds to those strategy sets where no player gets an incentive by unilaterally changing her/his strategy. In addition to the NE, there also exists a strategy set known as Pareto-efficient (or Pareto-optimal) such that there is no other strategy set that makes at least one player better off without making any other player worse off. The detailed analysis of such a strategic decision-making in any competitive situation is inherent in game theory [Neumann and Morgenstern, 1944].

Applications of quantum game theory are gaining importance as it allows representation of quantum communication protocols and algorithms in terms of games between quantum and classical players [Iqbal, 2005]. A quantum game naturally differs from a classical game largely due to three principal requirements, namely, (a) the states employed in a quantum game can be visualized as a quantum superposition of two or more basis states; (b) the players must initially share entangled states; and (c) the players can choose to perform superposition of strategies on their respective qubits. In this chapter, we revisit the Ping-Pong Protocol (PPP) [Boström and Felbinger, 2002] from the perspective of a game between the sender and the eavesdropper. Here, superposition of strategies for the players is not considered, and hence, the analysis is based on a classical game-theoretic picture of PPP.

The results obtained in this chapter demonstrate how pure strategy NE varies on changing the payoffs of two players. From Alice's point of view, the NE illustrates a strategy that Alice must opt for encoding information and from Eve's point of view, the NE corresponds to the most information gaining and mischievous strategy set. Further, we investigate the strategy that a sender must employ to ensure minimum payoff to an eavesdropper. On the other hand, our analysis also describe the best strategy set for the sender and eavesdropper that will lead towards

settling for a Pareto-optimal NE. Here, we present the entire analysis only from the perspective of a general game, representing a communication protocol, and not from the perspective of analysing the security of the protocol. This has been accomplished by taking into account certain parameters (which play an essential role in the protocol) and then allotting different weights to these parameters while designing the payoffs of players. In addition, we further study another two-way QKD protocol, i.e., LM05 protocol [Lucamarini and Mancini, 2005] in the game-theoretic framework and compare it with PPP game to analyse general payoffs of players in a game with or without entanglement. We find that depending on the protocol or game (with or without entanglement) and weights involved in the payoff term, different strategies of players may lead to different NE. The perspective used here, therefore, provides an efficient understanding of the protocol in terms of security, eavesdropping and importance of different parameters which are part of the protocol.

2.2 VISUALIZATION OF QUANTUM KEY DISTRIBUTION PROTOCOLS AS A GAME

If a task comprises of competing actions between the participants such that each participant desires to win that task, or perform better than the other participant, then that task can be called as a "game". Therefore a communication protocol where a sender (let Alice) wants to secretly send information to a receiver (let Bob), and an eavesdropper (let Eve) wants to interfere and eavesdrop the secret message, can be a game between Alice and Eve. In such a game scenario, since both Alice and Eve have competing intentions, i.e., Alice wishes to secretly transfer a message to Bob, whereas Eve does not want the message to be secret, and therefore, does not wish to let Alice complete her job with 100% privacy. Hence, if sending messages through this protocol is a game, then to win the game, Eve tries to learn the secret message and/or alter the message that Alice is communicating to Bob. On the other hand, Alice prefers different strategies for sending the message such that Eve is unable to intervene efficiently and gain either no or as less information as possible. This scenario can be collectively analysed with the aid of different strategies of Alice and Eve in a protocol. Thus, game theory can be an efficient mechanism for detailed representation, better understanding, and deeper insights into various communication protocols, e.g., Quantum Key Distribution (QKD) protocols. Various QKD protocols have been proposed [Gisin *et al.*, 2002]; some of them use single qubit un-entangled quantum systems, whereas some use entangled states. BB84 [Bennett and Brassard, 1984] is an example of one-way single-photon QKD protocol and PPP [Boström and Felbinger, 2002] is an example of two-way QKD protocol based on entangled photons. BB84 protocol has been represented and analysed as a game between a sender, a receiver, and an eavesdropper [Houshmand *et al.*, 2010]. The discussions in this chapter are an attempt to visualize two-way QKD protocols in the set-up of a game. For this, in sections 2.3 and 2.4 emphasis is laid on the study of PPP to analyse various possible strategies of a sender and an eavesdropper. Later in Section 2.5, comparison is made between PPP and LM05 protocols [Lucamarini and Mancini, 2005] by representing a general two-way QKD scheme as a game.

2.3 PING-PONG PROTOCOL AS A GAME

2.3.1 QKD the using Ping-Pong Protocol

In order to facilitate secure key transmission using the PPP, Bob first prepares a Bell state $|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}$ and sends the qubit A (travel photon) to Alice and keeps the qubit B (home photon) with himself. Now Alice randomly chooses to operate between Control mode (CM)s and Message mode (MM)s. During the CM, Alice performs measurement on the travel photon in Z basis and in-turn reveals the measurement outcome to Bob. Bob then performs measurement on his photon in Z basis. If the correlations between measurement outcomes of Alice and Bob are not in the same order as expected in $|\psi^+\rangle_{AB}$, then an eavesdropping attack is detected and the

protocol is aborted. Otherwise, the communication continues and the protocol proceeds further. During the MM, Alice performs unitary encodings, i.e., Identity operation (I) or Pauli-Z operation (σ_z) on the travel photon to encode 0 or 1, respectively. After encoding the message, Alice sends the travel photon back to Bob. Bob then, performs a Bell state measurement on the joint state of two photons. The measurement outcome $|\psi^+\rangle$ indicates that Alice performed I operation and the measurement outcome $|\psi^-\rangle$ indicates that Alice performed σ_z operation. Therefore, depending on the different indications of encoding revealed from measurement outcomes, Bob deciphers the one-bit information communicated by Alice.

2.3.2 Eavesdropping attacks on the Ping-Pong Protocol

In the entire protocol, the travel photon can be attacked by Eve on two occasions. Once, when the photon was sent from Bob to Alice for entanglement distribution and second, when it was sent from Alice to Bob after encoding the message. Since the eavesdropper is unaware of the mode (control/message) in which Alice operates on each turn, she will attack the travel photon each time it is sent through a public channel, irrespective of the CM or MM. Thus, Eve introduces auxiliary photons $|v\rangle_x|0\rangle_y$ to the shared state during entanglement distribution, where $|v\rangle$ denotes a vacuum state. Eve then alters the joint state of travel and auxiliary photons by performing a unitary operation Q. The first eavesdropping attack operation on the protocol was described by Wójcik [Wójcik, 2003], wherein Eve performs the following unitary operation

$$Q = \mathsf{SWAP}_{Ax}\mathsf{CPBS}_{Axy}\mathsf{H}_y \tag{2.1}$$

, and in the process gets detected with 50% probability in the CM. Here SWAP represents the swap operation between two qubits, CPBS represents the three-qubit Controlled Polarizing Beam Splitter (CPBS) [Wójcik, 2003], and H represents a single qubit Hadamard gate. The eavesdropper performs unitary operation Q when the travel and auxiliary photons are sent from Bob to Alice, and the reverse operation i.e., Q^{-1} is performed when the travel photon is sent back to Bob. By performing this attack, Eve gains substantial information, thereby reducing the mutual information between the sender and the receiver. In fact, a symmetrization procedure to this attack further reduces the amount of mutual information between Alice and Bob. Zhang later improved Wójcik's eavesdropping attack to reduce the induced channel loss in CM from 50% to 25% [Zhang *et al.*, 2004]. Moreover, a Denial-of-Service (DoS) attack and a mechanism to enhance the capacity of PPP was also discussed [Cai, 2003; Cai and Li, 2004]. It was further shown by Cai that how an imperfect implementation of the protocol could be exploited by an invisible photon eavesdropping with zero risk of detection [Cai, 2006]. The security of the PPP was however, reviewed in light of several attacks [Boström and Felbinger, 2008] and references therein.

Later, Pavičić [Pavičić, 2013] introduced a different, rather interesting attack operation on PPP where Eve could not be detected in the CM, but in the process Eve also does not get any information about the secret key/message. Pavičić's proposed attack operations on travel and auxiliary photons are represented as

$$Q = \mathsf{CPBS}_{Axy}\mathsf{H}_y \tag{2.2}$$

In this chapter, analysis is performed for Wójcik's attack, symmetrized Wójcik's attack, Pavičić's attack, and an additional situation wherein an eavesdropper refrains from performing any attack and simply performs an identity operation. By performing such an operation on PPP, Eve remains undetected in the CM but does not gain any information either. The advantage with this no attack situation is in terms of resources, i.e., Eve uses no quantum gate in comparison to Pavičić's attack.

2.3.3 The design of payoffs in the Ping-Pong game

To proceed with the above discussed analysis of PPP from the perspective of a game, it is worthwhile to emphasize on the discussion of design of payoffs in the game. The payoffs of players

can be established according to the various requirements of well-being of players that one wishes to examine in detail. In our present study, the rules of the game are designed in such a way such that Alice's payoff increases with the amount of information Alice sends to Bob; and decreases with the amount of secret information leaked out to Eve. Thus, the mutual information shared between Alice and Bob appears as a positive quantity in the payoff of Alice; and the mutual information shared between Alice and Eve, and Bob and Eve appears as a negative quantity in the payoff of Alice. Also, if Alice detects the presence of Eve during the execution of the protocol, it will lead to Alice achieving a better payoff in this competitive situation. In other words, the probability of Eve being caught will contribute as a positive quantity in the payoff of Alice.

On the other hand, Eve's payoff increases by an increase in the amount of secret information that Eve learns from Alice and Bob; and falls by an increase in mutual information between Alice and Bob. In addition, Eve's payoff will be negatively affected if she gets detected during the protocol's execution, and therefore the probability of Eve not being detected increases the payoff of Eve. Furthermore, in order to gain information from Alice and Bob, Eve applies respective quantum gates depending on different eavesdropping attacks. More the number of gates, more will be the overhead of Eve, and this will appear as a negative term in the payoff of Eve. Hence, summing up all the factors described above, the payoff of Alice is formulated as

$$P_A = w_a I(A:B) - w_b[I(A:E) + I(B:E)] + w_c p_d \tag{2.3}$$

and the payoff of Eve as

$$P_E = w_d[I(A:E) + I(B:E)] - w_e I(A:B) + w_f[1 - p_d] - w_1 n_1 - w_2 n_2 - w_3 n_3 \tag{2.4}$$

where $w_a, w_b, w_c, w_d, w_e, w_f, w_1, w_2, w_3$ are positive real numbers and considered as weights attached to each quantity in the payoff, $I(A:B)$ is the mutual information between Alice and Bob, $I(A:E)$ is the mutual information between Alice and Eve, $I(B:E)$ is the mutual information between Bob and Eve, p_d is the probability of detection of Eve, n_1 is the number of two qubit gates, n_2 is the number of single qubit gates and n_3 is the number of beam splitters in the attack operation of Eve. The payoffs of Alice and Eve in this game, depend on different values of weights assigned in payoffs, and thus the condition of complete win or complete loss for any player does not arise for the game. In other words, it can be clearly stated that this kind of game is not a zero-sum game. The players are always benefited to some degree quantified by P_A and P_E in Eq. (2.3) and Eq. (2.4), respectively. A positive payoff signifies benefit and a negative payoff signifies drawback.

The payoff of Alice and Eve have been designed to study a generic scheme, and therefore all possible terms that will play a role in their payoffs are taken into account. In order to study a specific setting of the game, different values of weights are chosen in the payoff. For example, by assuming weights w_b and w_e to be zero, one can study eavesdropping attacks without considering *denial-of-service* type attacks. Similarly, if one wishes to analyse a PPP game where the eavesdropper has unlimited power constrained only by the laws of physics, i.e., Eve is not bound by the cost of resources then the weights w_1, w_2, and w_3 can be assumed to be zero. Later in this chapter, these specific settings as explained above have been analysed. Similarly, for studying other special cases of the game, different values can be assigned to the weights in the payoff.

Moreover, for our present study, the need is to decide a restrictive set of different strategies of Alice and Eve which can be used for the formulation of a game between them. From the point of view of strategies adopted by Alice and Eve, four different attack operations as the strategy of Eve, namely Wójcik's original attack [Wójcik, 2003], Wójcik's symmetrized attack [Wójcik, 2003], Pavičić's attack [Pavičić, 2013] and no attack or an identity operation as in Eq. (1) are considered. Further, two different strategies of Alice are considered for encoding one bit information as it is indispensable to review more than one allowed strategy (move) for Alice, for a comparative

examination. Therefore, phase flip and bit flip encoding are taken as the two distinct strategy sets of Alice. Phase flip encoding can be implemented by performing identity operation on the travel photon to send 0 and Pauli-Z operation on the travel photon to send 1. On the other hand, bit flip encoding can be implemented by performing identity operation on the travel photon to send 0 and Pauli-X operation on the travel photon to send 1.

The setting of our game is such that each player remains unaware of the other player's move. This is ensured by slightly modifying the PPP for the two strategies of Alice. In the protocol, Bob is able to perform two-qubit measurement and decode information about the encoding scheme after the travel photon finally reaches him. The modification is that Alice should announce her strategy A_1 or A_2 only after Bob announces the receipt of the travel photon. Thus, Eve may come to know about the encoding scheme of Alice, after she is done with her move and cannot apply additional operations or moves. This way, Eve can perform her move (eavesdropping operation) without knowing Alice's move (encoding operation).

2.3.4 Similarity of Ping-Pong Protocol to the messenger game

The representation of PPP as a game is similar to a modified form of the childhood game known as *Messenger Game* or *Whisper Down the Lane Game*. In this game, there are multiple players (let, $n+2$) sitting in a queue. The first player whispers a message into the ear of the next person through a line of (n) players until the last player receives the final message. Here, the first player corresponds to the sender (Alice) and the last player corresponds to the receiver (Bob) in any communication protocol. Let us assume that the primary motive of playing this game is same as that of any communication protocol that a secret message should be sent from the sender to the receiver without being altered. Further a small modification can be made in the game with the assumption that there is a mischievous player (corresponds to Eve in any communication protocol) among (n) players who listens (eavesdrops) the original message the sender wants to send to the receiver. However, after listening, she alters the content of the original message and passes an altered message to her next neighbor in the queue. She does so because her aim in the game is not to let the receiver or last player learn the correct message. Thus, the competitive interests of the sender and the mischievous player constitutes a game setting for a modified messenger game.

Similar to the PP protocol, Alice randomly chooses between operating either in CM or in MM. The MM is similar to the usual messenger game, where Alice whispers the desired message through a sequence of players until Bob receives the message and acknowledges the receipt of the message. In CM, Alice instead of sending the desired message, sends a dummy message. When Bob announces the receipt of message in CM, Alice randomly asks a question to one of the players in the sequence. Depending on the answer received, Alice decides on a segment of doubt, i.e. presence or absence of Eve; if present then the segment where she might be present. For the next CM, Alice is bound to choose a random player to be questioned falling in the identified segment of doubt. For example, if Alice asks the i^{th} person in the sequence about the message he/she was asked to transfer to his/her neighbor in the line. If the i^{th} person acknowledges the correct dummy message as the answer, then the segment of doubt reduces to players between i^{th} to n^{th} position. On the other hand, if the i^{th} person acknowledges a message which is different from the correct dummy message as the answer, then the segment of doubt reduces to players between 1^{st} to i^{th} position. Therefore, after a finite number of control runs in the game, if "d" is the number of players in the segment of doubt, then the probability of detection of the mischievous player, i.e. Eve, will be $1/d$. Moreover, Eve knows that there can be random control runs between MMs, and therefore she sometimes does not alter the message before transferring to her neighbor, so as to avoid being caught during the CM. This random choice (or guessing strategy) of Eve of not manipulating the message could correspond to the overhead of Eve in the form of single and double qubit gates, and polarization beam splitters in the PPP. Thus, the payoffs of players in the PPP game as designed

in Eq. (2.3) and Eq. (2.4) hold similarity to the payoffs of Alice and Eve for the above described modified messenger game. Therefore, it becomes easy to relate and understand PPP as a game with the visualization of a familiar messenger game.

2.4 ANALYSIS OF DIFFERENT STRATEGIES FOR THE PING-PONG GAME

In order to analyse the game for different strategies of Alice and Eve, two different strategies for Alice are considered, namely

(i) $A_1 = encodingScheme(0 : Identity, 1 : Pauli-Z)$

(ii) $A_2 = encodingScheme(0 : Identity, 1 : Pauli-X)$

and four different strategies for Eve, namely

(i) E_1 - Wójciks's attack

(ii) E_2 - symmetrized Wójcik's attack

(iii) E_3 - Pavičić's attack

(iv) E_4 - no attack

For every strategy A_i and E_j of Alice and Eve, respectively, where $i \in \{1,2\}$,$j \in \{1,2,3,4\}$, the payoffs of Alice and Eve can be calculated from Eq. (2.3) and Eq. (2.4), respectively.

Table 2.1 : Payoffs of Alice in the general PPP game

Alice \ Eve	E_1	E_2	E_3	E_4
A_1	$0.311w_a - 0.385w_b + 0.5w_c$	$0.188w_a - 0.377w_b + 0.5w_c$	w_a	w_a
A_2	$0.311w_a - 0.86w_b + 0.5w_c$	$0.423w_a - 0.768w_b + 0.5w_c$	$w_a - 2w_b$	w_a

Table 2.2 : Payoffs of Eve in the general PPP game

Alice \ Eve	E_1	E_2	E_3	E_4
A_1	$0.385w_d - 0.311w_e$ $+0.5w_f - 10w_1$ $-4w_2 - 2w_3$	$0.377w_d - 0.188w_e$ $+0.5w_f - 10.5w_1$ $-5.5w_2 - 2w_3$	$-w_e + w_f - 8w_1$ $-4w_2 - 2w_3$	$-w_e + w_f$
A_2	$0.86w_d - 0.311w_e$ $+0.5w_f - 10w_1$ $-4w_2 - 2w_3$	$0.768w_d - 0.423w_e$ $+0.5w_f - 10.5w_1$ $-5.5w_2 - 2w_3$	$2w_d - w_e + w_f$ $-8w_1 - 4w_2 - 2w_3$	$-w_e + w_f$

Based on the strategies opted by Alice and Eve in the game, Table 2.1 and Table 2.2 summarize their respective payoffs. One can observe from Table 2.2 that whenever Alice performs strategy A_1, the eavesdropper always gets a reduced or equal (only in case of E_4) payoff irrespective of the strategy she chooses. Thus, from the perspective of the security of protocol which lies in reducing eavesdropping or benefits to an eavesdropper, Alice may prefer to opt for the strategy A_1. However, from the perspective of a game between Alice and Eve, different preferences of

one player as against varying strategies opted by the other player are explored further. Here, an elaborate analysis of the game is summarized, such that

(a) If Eve performs E_1 or E_3 then Alice gets a better payoff by performing A_1 because

$$\begin{aligned} 0.311w_a - 0.385w_b + 0.5w_c \geq 0.311w_a - 0.86w_b + 0.5w_c, \textit{ and} \\ w_a \geq w_a - 2w_b \end{aligned} \tag{2.5}$$

(b) If Eve performs E_4, then Alice gets an equal payoff by performing either A_1 or A_2

(c) If Eve performs E_2, then Alice can be better off by performing A_1 or A_2 depending on the values of w_a and w_b, i.e.,

$$\begin{aligned} &For A_1\ 0.188w_a - 0.377w_b + 0.5w_c \geq 0.423w_a - 0.768w_b + 0.5w_c \Rightarrow w_b \geq 0.601w_a, \textit{ and} \\ &For A_2\ 0.188w_a - 0.377w_b + 0.5w_c \leq 0.423w_a - 0.768w_b + 0.5w_c \Rightarrow w_b \leq 0.601w_a \end{aligned} \tag{2.6}$$

(d) Assuming that $0.123w_e - 0.008w_d \leq 0.5w_1 + 1.5w_2$, if Alice performs A_1 then Eve gets lesser payoff by performing E_2 and E_3 in comparison to performing E_1 or E_4. Furthermore, Eve can opt for the strategy E_1 or E_4 depending on the value of weights w_d, w_e, w_f, w_1, w_2 and w_3, i.e., if

$$\begin{aligned} 0.385w_d - 0.311w_e + 0.5w_f - 10w_1 - 4w_2 - 2w_3 \geq -w_e + w_f \\ \Rightarrow 0.385w_d + 0.689w_e \geq 0.5w_f + 10w_1 + 4w_2 + 2w_3 \end{aligned} \tag{2.7}$$

then Eve prefers E_1, else she prefers E_4.

(e) Similarly, if $0.123w_e - 0.008w_d \geq 0.5w_1 + 1.5w_2$ and Alice performs A_1, then Eve gets higher payoff by performing the strategy E_2 or E_4. Therefore, from Table 2.2, if

$$\begin{aligned} 0.3775w_d - 0.188w_e + 0.5w_f - 10.5w_1 - 5.5w_2 - 2w_3 \geq -w_e + w_f \\ \Rightarrow 0.377w_d + 0.812w_e \geq 0.5w_f + 10.5w_1 + 5.5w_2 + 2w_3 \end{aligned} \tag{2.8}$$

then Eve prefers E_2, else she prefers E_4.

(f) Moreover, if $w_d \leq 4w_1 + 2w_2 + w_3$ and Alice performs A_2, then Eve gets a better payoff by performing E_1 or E_4. The highest payoff strategy between E_1 and E_4 clearly depends on the value of the weights w_d, w_e, w_f, w_1, w_2 and w_3, such that if

$$\begin{aligned} 0.86w_d - 0.311w_e + 0.5w_f - 10w_1 - 4w_2 - 2w_3 \geq -w_e + w_f \\ \Rightarrow 0.86w_d + 0.689w_e \geq 0.5w_f + 10w_1 + 4w_2 + 2w_3 \end{aligned} \tag{2.9}$$

then Eve is better off by performing E_1, else she performs E_4.

(g) Similarly for $w_d \geq 4w_1 + 2w_2 + w_3$ and Alice's strategy A_2, Eve gets higher payoff by performing E_1 or E_3, such that if

$$\begin{aligned} 0.86w_d - 0.311w_e + 0.5w_f - 10w_1 - 4w_2 - 2w_3 \geq 2w_d - w_e + w_f - 8w_1 - 4w_2 - 2w_3 \\ \Rightarrow 0.689w_e - 1.14w_d \geq 0.5w_f + 2w_1 \end{aligned} \tag{2.10}$$

then Eve prefers E_1, else she prefers E_3.

Table 2.3 : Conditions for (A_i, E_j) to be a Nash equilibrium

Nash Equilibrium	Conditions
(A_1, E_1)	$0.123w_e - 0.008w_d \leq 0.5w_1 + 1.5w_2$, and $0.385w_d + 0.689w_e \geq 0.5w_f + 10w_1 + 4w_2 + 2w_3$
(A_1, E_2)	$w_b \geq 0.601w_a$, $0.123w_e - 0.008w_d \geq 0.5w_1 + 1.5w_2$, and $0.377w_d + 0.812w_e \geq 0.5w_f + 10.5w_1 + 5.5w_2 + 2w_3$
(A_1, E_4)	$0.123w_e - 0.008w_d \leq 0.5w_1 + 1.5w_2$, and $0.385w_d + 0.689w_e \leq 0.5w_f + 10w_1 + 4w_2 + 2w_3$
(A_2, E_4)	$w_d \leq 4w_1 + 2w_2 + w_3$, and $0.86w_d + 0.689w_e \leq 0.5w_f + 10w_1 + 4w_2 + 2w_3$

To summarize the above analysis, it can be concluded that the NE of the generic game is either (A_1,E_1), (A_1,E_2), (A_1,E_4) or (A_2,E_4) depending on the values of the weights as indicated in Table 2.3. The NE for specific cases such as eavesdropping with Eve equipped with unlimited resources will differ from the ones represented in Table 2.3. These specific cases will be discussed later in this section. For simplicity, all weights attached to the mutual information terms and all weights attached to the probability terms are considered to be independently equal to each other, i.e.,

$$w_a = w_b = w_d = w_e = w_I, \qquad \textit{and} \qquad w_c = w_f = w_P \tag{2.11}$$

Table 2.3 together with Eq. (2.11) illustrates that for (A_1, E_1) or (A_1, E_2) to be the NE of the game, w_I must have a very high value in comparison to the values of w_P, w_1, and w_2 which may not be a feasible choice under fair conditions. Therefore, (A_1,E_4) and/or (A_2,E_4) become the NE of the represented one bit ping-pong game. Interestingly, E_4 is Eve's strategy where she does not get

Table 2.4 : Payoffs of Alice in the PPP game with only two weight terms

Alice \ Eve	E_1	E_2	E_3	E_4
A_1	$-0.074w_I + 0.5w_P$	$-0.189w_I + 0.5w_P$	w_I	w_I
A_2	$-0.549w_I + 0.5w_P$	$-0.345w_I + 0.5w_P$	$-w_I$	w_I

detected, gains no information, and uses no gates. Therefore, for a particular situation where Eve may need to optimize her resources, even the attack operation E_4 (equivalent to Eve doing nothing) becomes useful in a game situation. The attack operation E_4, however, may not be relevant for situations where Eve is equipped with unlimited resources. From Eq. (2.11), one can show that Table 2.1 and Table 2.2 can be re-expressed as Table 2.4 and Table 2.5, respectively.

Although from the perspective of a PPP, players will never strive for a Pareto-optimal NE, however, when a communication protocol is visualized as a game, the prominence of a Pareto-optimal NE becomes much more significant. In a game's perspective, there is either a win

Table 2.5 : Payoffs of Eve in the PPP game with only two weight terms

Alice \ Eve	E_1	E_2	E_3	E_4
A_1	$0.074w_I + 0.5w_P$ $-10w_1 - 4w_2 - 2w_3$	$0.189w_I + 0.5w_P$ $-10.5w_1 - 5.5w_2 - 2w_3$	$-w_I + w_P - 8w_1$ $-4w_2 - 2w_3$	$-w_I + w_P$
A_2	$0.549w_I + 0.5w_P$ $-10w_1 - 4w_2 - 2w_3$	$0.345w_I + 0.5w_P$ $-10.5w_1 - 5.5w_2 - 2w_3$	$w_I + w_P - 8w_1$ $-4w_2 - 2w_3$	$-w_I + w_P$

or a lose situation; whereas in a communication protocol, there can be many aspects, like secure transmission of information, control runs for any third party detection, etc. Therefore, whenever there is switching from a protocol to its game counterpart, it becomes essential to analyse the NE of the game. Clearly, the NE strategies may not be the ones that players would opt for in a secure protocol. But, in the game-theoretic view, the greed of players for achieving maximum possible payoff drives them to go for strategies and payoffs at NE. Therefore, the Pareto-optimal NE strategy for both the players. For the PPP game described above, (A_1, E_4) and (A_2, E_4) will be the Pareto-optimal NE of the game if w_I is the highest payoff of Alice in Table 2.4, and $-w_I + w_P$ is the highest payoff of Eve in Table 2.5. Since a Pareto-optimal strategy is the one in which players do not get a higher incentive by changing their strategies; (A_1, E_4) and (A_2, E_4) will be Pareto-optimal NE of the game if the following condition holds true

$$0.4655w_P \leq w_I \leq 4w_1 + 2w_2 + w_3 \tag{2.12}$$

Further, the analysis of the PPP game is done for different choices of weights which may lead the game to different NE, which may or may not be Pareto-optimal. In the following subsections, two different cases of eavesdropping, i.e. (i) excluding DoS attacks and (ii) when Eavesdropper has unlimited resources are discussed.

2.4.1 Analysis of the PP game in case of eavesdropping excluding DoS attacks

In order to study eavesdropping excluding DoS attacks, it is considered that $w_e = w_b = 0$, which leads us to the set of NE in the PPP game, shown in Table 2.6

Table 2.6 : Conditions for (A_i, E_j) to be a NE for eavesdropping excluding DoS attacks

Nash Equilibrium	Conditions
(A_1, E_1)	$w_d \geq 1.2987w_f + 25.974w_1 + 10.3896w_2 + 5.1948w_3$
(A_1, E_4)	$w_d \leq 1.2987w_f + 25.974w_1 + 10.3896w_2 + 5.1948w_3$
(A_2, E_3)	$w_d \geq 4w_1 + 2w_2 + w_3$
(A_2, E_4)	$w_d \leq 4w_1 + 2w_2 + w_3$

2.4.2 Analysis of the PP game in case of eavesdropper having unlimited resources

For an Eve equipped with unlimited resources, $w_1 = w_2 = w_3 = 0$ is considered, which leads us to the set of NE in the PPP game, as shown in Table 2.7

Table 2.7 : Conditions for (A_i, E_j) to be a Nash equilibrium for an eavesdropper with unlimited power

Nash Equilibrium	Conditions
(A_1, E_1)	$w_d \geq 15.375 w_e$, and $0.385 w_d + 0.689 w_e \geq 0.5 w_f$
(A_1, E_2)	$w_d \leq 15.375 w_e$, $0.377 w_d + 0.812 w_e \geq 0.5 w_f$, and $w_b \geq 0.601 w_a$
(A_1, E_3)	$0.385 w_d + 0.689 w_e \leq 0.5 w_f$, and $0.377 w_d + 0.812 w_e \leq 0.5 w_f$
(A_1, E_4)	$0.385 w_d + 0.689 w_e \leq 0.5 w_f$, and $0.377 w_d + 0.812 w_e \leq 0.5 w_f$

From 2.7, it is clear that for an eavesdropper with unlimited resources the condition for (A_1, E_3) or (A_1, E_4) to be the NE is same which is justified as there are no costs involved for resources to be used in eavesdropping. Therefore, the attack (A_1, E_4) becomes irrelevant if Eve has unlimited power in terms of resources to be used.

2.4.3 Prospective enhancements in the analysis of the PP game

Considering the above analysis, an iterated version of the PPP can be studied in detail where the knowledge of previous moves of opponents will help players in deciding their next strategy. The analysis of an iterated version of PPP game leads to the conclusion that Alice will always prefer performing A_1, irrespective of what strategy Eve adopts in the previous step; and thus Eve may come to know that Alice always adopts A_1 and hence takes her move accordingly. Therefore, the NE of the game for an iterated protocol may only correspond to A_1 strategy of Alice. Apart from Eve slowly knowing the tendency of Alice adopting A_1, all other operations of Alice and Eve and the payoffs for the respective strategies may remain same.

In this section, the PPP game is discussed where payoffs of Alice and Eve are given by Eq. 2.3 and 2.4 respectively. It would be interesting to study the PPP game by modifying the payoffs to include various other factors playing an important role during the execution of the protocol. An example of one such factor that can be included in the payoffs could be Quantum Bit Error Rate (QBER) in Alice's and Eve's payoff. By adding additional terms in the payoffs, one can include improvements introduced for making the protocol more secure [Wójcik, 2003].

2.5 COMPARISON OF PING-PONG PROTOCOL WITH LM05 PROTOCOL WITH THE HELP OF A GENERAL TWO-WAY QKD GAME

Standard QKD protocols, such as the BB84 protocol, do not allow the receiver to decode the information in a deterministic way. This problem, however, can be rectified using a two-way QKD protocol such as a PPP or LM05 protocol [Qing-Yu and Bai-Wen, 2004; Lucamarini and Mancini, 2005]. The LM05 protocol is based on non-orthogonal states instead of entangled resources as in a PPP. In general, two-way QKD protocols have been proved better and secure against general

eavesdropping attacks [Beaudry *et al.*, 2013]. In this section, similar to the study of PPP game, a generic two-way QKD game is designed to analyse and compare PPP and LMO5 protocols for few zero-loss eavesdropping attacks [Lucamarini and Mancini, 2014]. The payoffs of Alice and Eve in the general two-way QKD game can be described as

$$P_A = w_g I(A:B) - w_h[I(A:E)+I(B:E)] + w_i\left[\frac{p_d + \text{QBER}}{2}\right] \tag{2.13}$$

$$P_E = w_k[I(A:E)+I(B:E)] - w_l I(A:B) + w_m\left[1 - \frac{p_d + \text{QBER}}{2}\right] \tag{2.14}$$

where QBER is calculated by comparing some encoded bits (in MM) shared between Alice and Bob; n is the number of entangled states used; $w_g, w_h, w_i, w_j, w_k, w_l, w_m$ are positive real numbers and considered as weights attached to each quantity in the payoff. For various strategies of Eve, Intercept and Resend (IR) [Lucamarini and Mancini, 2014] attack, Double Control NOT (DCNOT) [Lucamarini and Mancini, 2014] attack (which is also similar to Pavičić's attack [Pavičić, 2013; Zawadzki and Miszczak, 2016]), and Wójcik's attack [Wójcik, 2003]is studied. In our present analysis, the PPP with encoding scheme A_1 as described above, and LM05 [Lucamarini and Mancini, 2005] protocol are considered. The payoffs of Alice and Eve for Ping-Pong (PP) and LM05 protocols during various eavesdropping attacks are summarized in Table 2.8 and Table 2.9, respectively.

Table 2.8 : Payoffs of Alice in the two-way QKD game

Alice \ Eve	IR	DCNOT	$Wojcik'sAttack\ (E_1)$
PPP	$0.1887w_g - 1.1887w_h + 0.125w_i - w_j$	$w_g - w_j$	$0.311w_g - 0.385w_h + 0.375w_i - w_j$
LM05	$0.1887w_g - 1.1887w_h + 0.125w_i$	$w_g - 2w_h + 0.125w_i$	$0.5488w_g - 1.096w_h + 0.375w_i$

Table 2.9 : Payoffs of Eve in the two-way QKD game

Alice \ Eve	IR	DCNOT	$Wojcik'sAttack\ (E_1)$
PPP	$1.1887w_k - 0.1887w_l + 0.875w_m$	$-w_l + w_m$	$0.385w_k - 0.311w_l + 0.625w_m$
LM05	$1.1887w_k - 0.1887w_l + 0.875w_m$	$2w_k - w_l + 0.875w_m$	$1.096w_k - 0.5488w_l + 0.625w_m$

Table 2.8 clearly shows that LM05 game results in a better payoff for Alice in comparison to the PPP game, for the IR attack. However, if Eve performs DCNOT or Wójcik's attack, Alice may get a better payoff by playing either a PP game or LM05 game depending on the values of the weights w_g, w_h, w_i, and w_j. Similarly, Table 2.9 suggests that Eve will prefer IR attack over Wójcik's attack for both games. Moreover, Eve may prefer either IR or DCNOT attack depending on the values of weights w_k, w_l, and w_m. Hence, NE of the two-way QKD game varies for different conditions of weights as shown in Table 2.10.

Table 2.10 : Conditions for (A_i, E_j) to be a Nash equilibrium in the two-way QKD game

Nash Equilibrium	Conditions
(LM05, IR)	$w_k \leq w_l$
(PPP, DCNOT)	$2w_h - w_j \geq 0.125w_i$ $w_m \geq 9.5096w_k + 6.4904w_l$
(LM05, DCNOT)	$2w_h - w_j \leq 0.125w_i$ $w_k \geq w_l$ $w_m \geq 1.8048w_l - 3.616w_k$

2.6 CONCLUSIONS

PPP has been witnessed from the point of view of a game and its detailed analysis is presented. The results established a relation between pure strategy NE, and payoffs of the sender and the eavesdropper depending on the value of weights assigned to mutual information between different players, probability of detection of the eavesdropper, and number of gates applied by an eavesdropper to gain information. We further demonstrated the strategy that a sender must opt to minimize the payoff of an eavesdropper within the conditions of the game. The analysis further described the condition for a Pareto-optimal NE. With the aim of studying a general two-way QKD protocol with and without entanglement, the PPP is compared with the LM05 protocol. We found that the payoffs of the sender and the eavesdropper depend on the type of eavesdropping attacks, and the weights of different terms that play an important part in design of payoffs. We believe that the analysis presented here will help in enhancing the understanding of interesting features of PPP from the perspective of strategies employed by a sender or an eavesdropper to achieve a better payoff.

…