Game-theoretic perspective of Ping-Pong protocol

Hargeet Kaur, Atul Kumar *
Indian Institute of Technology Jodhpur, Jodhpur, Rajasthan, India

Abstract

We analyse Ping-Pong protocol from the point of view of a game. The analysis helps us in understanding the different strategies of a sender and an eavesdropper to gain the maximum payoff in the game. The study presented here characterizes strategies that lead to different Nash equilibriums. We further demonstrate the condition for Pareto optimality depending on the parameters used in the game. Moreover, we also analysed LM05 protocol and compared it with PP protocol from the point of view of a generic two-way QKD game with or without entanglement. Our results provide a deeper understanding of general two-way QKD protocols in terms of the security and payoffs of different stakeholders in the protocol.

1. Introduction

A game is a competitive activity among more than one rational players, where there are a set of rules and conditions of win and loss. Each player makes a strategic move depending on certain background details such as knowledge about other players, knowledge about allowed moves, and how different moves will lead to varying outcomes of the game. Every move that a player takes correspond to a Payoff - payoffs are numbers which represent the benefit that each player gets by their respective moves. It quantifies the utility or the desirability of each player to perform a particular strategy. For a finite game, John F. Nash [1,2] described a stable point – Nash Equilibrium – that is formulated by those strategy sets where no player gets an incentive by unilaterally changing her/his strategy. A strategy set of a game is Pareto efficient (or Pareto optimal) if 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 [3]. Since its inception, the theory has found applications in diverse academic spaces such as economics, political science, biology, computer science, physics etc. [4–13]. With the advent of quantum information and computation, the quest to analyse classical game theory in quantum realm became central to the foundations of quantum mechanics [14]. Meyer [15] and Eisert [16] independently put classical game theory in the context of quantum strategies. The central idea to introduce quantum strategies in comparison to classical strategies is to achieve a better payoff in the game. For example, Meyer
demonstrated that a quantum player always outperforms a classical player in a Penny flip game and Eisert described how quantum strategies help players to avoid the original dilemma present in the classical Prisoners’ dilemma (PD). On the experimental front, the quantum version of the PD game is also realized using a NMR quantum computer [17]. Moreover, Vaidman [18] illustrated a simple game in which players always win the game when they share a GHZ state in advance. In comparison to three classical players where the probability of winning the game is always probabilistic. Quantum strategies are also utilized to introduce the elements of fairness in remote gambling [19], and in designing algorithms for implementing quantum auctions which offer many security advantages [20]. Fitney and Abbott [21] have analysed quantum versions of Parrondo’s games. Such analysis not only helps to design secure networks that lead to identification of new quantum algorithms, but also provide a completely different dimension to characterize a game or a protocol. Furthermore, eavesdropping [22,23] and optimal cloning [24] can also be visualized as games between players.

Applications of Quantum game theory are gaining importance, since lesser bits are used to play quantum games [20]. Quantum game theory also becomes important as one can represent quantum communication protocols, and algorithms, in terms of games between quantum and classical players [25]. 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 qubits. In this article, we revisit the Ping-Pong (PP) protocol [26] from the perspective of a game between the sender and the eavesdropper. Here, we have not considered superposition of strategies for the players, and hence, our analysis is based on a classical game-theoretic picture of PP protocol.

Our results demonstrate how pure strategy Nash equilibrium changes depending on the payoffs of the two players. From the point of view of Alice, the Nash equilibrium would illustrate a strategy that Alice must use for encoding information and from Eve’s point of view, the Nash equilibrium will be the most information gaining attack. We further analyse the strategy that a sender must employ to ensure minimum payoff to an eavesdropper. On the other hand, we also describe the best strategy for the sender and eavesdropper to settle for a Pareto optimal Nash equilibrium, only from the perspective of a general game and not from the perspective of a secure protocol, depending on certain parameters which play essential role in the protocol. In addition, we also study another two-way QKD protocol, i.e., LM05 protocol from the perspective of a game and compare it with PP game to analyse general payoffs of the players in a game with or without entanglement. We found 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 Nash equilibriums. The perspective used here, therefore, provides a deeper understanding of the protocol in terms of security, eavesdropping and importance of different parameters which are part of the protocol.

2. Ping-Pong protocol as a game

Any activity which involves dealing with competitive situations can be a game. For example, any communication protocol where a sender (Alice) wants to securely transfer information to a receiver (Bob) can be a game between Alice and an eavesdropper (Eve) who does not want Alice to successfully complete her job. In order to win the game, Eve may try to gain the secret information and/or modify the information that Alice wants to send to Bob. On the contrary, Alice will try to employ a strategy such that Eve is unable to intervene in any way. This will result in a game for different strategies of Alice and Eve in a protocol. Therefore, game theory can be used for easy and detailed understanding of many communication protocols, e.g., key distribution protocols.

Quantum key distribution (QKD) protocols are proposed with single and entangled quantum systems. For example BB84 [27] is an example of one-way single-photon QKD protocol and PP Protocol is an example of two-way QKD protocol based on entangled photons. BB84 protocol has been earlier studied well within the set-up of a game [28]. In this article, we will study PP protocol to analyse the strategies of a sender and an eavesdropper. PP protocol uses entanglement to allow asymptotically secure key distribution and quasi-secure direct communication. Here, Eve has access to one of the photons at two different stages: once during entanglement distribution and once after the encoding of secret information. Therefore, there are chances that the Eavesdropper may try to gain some information communicated from a sender to the intended receiver. For practical purposes, Ostermeyer and Walenta [29] have also proposed the experimental realization of PP protocol. In order to facilitate our analysis, we first describe the PP protocol to understand the different aspects of the protocol.

In the original protocol, Bob prepares a Bell state $|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)_{AB}$ and sends the particle A (travel photon) to Alice and keeps particle B (home photon) with himself. Alice randomly operates between control and message modes. In control mode, she measures the travel photon in computational basis and announces the result to Bob, who then measures his photon in the same basis. If the measurement outcomes of Alice and Bob are correlated as in $|\psi^+\rangle_{AB}$, then they proceed with the communication; else an eavesdropper is detected and the protocol is aborted. In message mode, Alice performs unitary operation $I$ or $\sigma_x$ on the travel photon to encode 0 or 1, respectively. After encoding, she sends the travel photon back to Bob, who 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 $\sigma_x$ operation. Therefore depending on the measurement outcomes, Bob decodes the one-bit information communicated by Alice.

In the entire protocol, there are two instances where the travel photon could be attacked by Eve. First, when it was sent from Bob to Alice for entanglement distribution and second, when it was sent from Alice to Bob after encoding. Since
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات