Game Theory based View to the Quantum Key Distribution BB84 Protocol

Mahboobeh Houshmand
Dept. of computer engineering
Ferdowsi University
Mashhad, Iran
Ma.Hooshmand@stu-mail.um.ac.ir

Monireh Houshmand
Dept. of electrical engineering
Imam Reza University
Mashhad, Iran
Monirehhoushmand@gmail.com

Habib Rajabi Mashhadi
Dept. of electrical engineering
Ferdowsi University
Mashhad, Iran
h_mashhadi@um.ac.ir

***Abstract*- Quantum key distribution uses quantum mechanics to guarantee secure communication. BB84 is a widely used quantum key distribution that provides a way for two parties, a sender, Alice, and a receiver, Bob, to share an unconditionally secure key in the presence of an eavesdropper, Eve. In a new approach, we view this protocol as a three player static game in which Alice and Bob are two cooperative players and Eve is a competitive one. In our game model Alice's and Bob's objective is to maximize the probability of detecting Eve, while Eve's objective is to minimize this probability. Using this model we show how game theory can be used to find the strategies for Alice, Bob and Eve.**

Keywords- BB84 protocol, static game theory, mixed strategy Nash equilibrium.

I. INTRODUCTION

Cryptography is the art of providing secure communication over insecure communication channels. To achieve this goal, an algorithm is used to combine a message with some additional information—known as the key—to produce a cryptogram. For this reason, secure key distribution is a crucial problem in cryptography [1-3].

Quantum key distribution (QKD)[4] offers secure communication based on the fundamental laws of physics—namely, that measurement of a quantum system being used to transmit information must necessarily disturb that system, and that this disturbance is detectable [5].

The first QKD scheme was proposed by Bennett and Brassard in 1984 (BB84) [6] and is based on generating a secure key between the sender, Alice and the receiver, Bob by sending a random bit string encoded and measured in one of two randomly chosen bases.

In this paper, we concentrate on providing a mathematical framework for studying the BB84 protocol. We formulate it as a three player- Alice, Bob and Eve- static game.

Alice's strategy is to choose between the two bases, eigenbasis of x or eigenbasis of z to encode the each data bit, in the qubit. Bob's and Eve's strategy is to choose between these two bases to measure the qubits.

We will describe how game theory can be used to find strategies for the basis choice for Alice, Bob and Eve and show his strategy is to choose randomly, as what is assumed in the protocol.

The organization of the paper is as follows. In section II, a brief review of game theory is introduced. In section III a review of BB84 quantum key distribution protocol is described. In section IV, our game model to analysis the strategies is presented. Section V concludes the paper.

II. BRIEF REVIEW OF GAME THEORY

Game theory [7-11] is a collection of mathematical models formulated to study situations of conflict and cooperation, in those an individual's success in making choices depends on the choices of others. It is concerned with finding the best actions for individual decision makers in these situations and recognizing stable outcomes.

The object of study in game theory is the game, defined to be any situation in which:

- There are at least two *players*. A player may be an individual, a firm, a nation, or even a biological species.
- Each player has a number of possible *strategies*, courses of action he or she may choose to follow.
- The strategies chosen by each player determine the *outcome* of the game.
- Associated with each possible outcome of the game is a collection of numerical *payoffs*, one to each player. These payoffs represent the value of the outcome to the different players [7, 12].

The pioneering analysis of game theory was the study of a duopoly by Cournot in 1838; however, game theory was not established as a

978-0-7695-4020-7/10 $26.00 © 2010 IEEE
DOI 10.1109/IITSI.2010.135

field in its own right until the monumental *Theory of Games and Economic Behavior* [13] by von Neumann and Oskar Morgenstern in 1944 [7, 12]. A few years later, John Nash made a number of additional contributions [14, 15], the cornerstone of which is the famous *Nash equilibrium*. Since then, many other researchers have contributed to the field, and game theory has been widely recognized as an important tool in many fields.

III. REVIEW OF BB84 QUANTUM KEY DISTRIBUTION PROTOCOL

BB84 protocol is a secure way of distributing a cryptographic key using a sequence of individual qubits [16].

In this protocol, Alice generates two random sequences of bits, *a* and *b*, each *n* bits long. She then encodes these two sequences as a sequence of *n* qubits:

$$|\varphi\rangle = \bigotimes_{k=1}^{n} |\varphi_{a_k b_k}\rangle$$

Where a_k, b_k are the *k*th bit of *a* and b, respectively. Each qubit is one of four states:

$$|\varphi_{00}\rangle = |0\rangle$$

$$|\varphi_{10}\rangle = |1\rangle$$

$$|\varphi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\varphi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The effect of this procedure is to encode *a* in the eigenbasis of *x* or eigenbasis of *z* as determined by *b*. Then Alice sends $|\varphi\rangle$ over a public quantum channel to Bob. Bob generates a sequence of random bits *b*' of the same length as *b*, which determines the basis of measurement, then measures the string *a'*. At this point, Bob announces publicly that he has received Alice's transmission. Alice then announces *b*. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the qubits in *a* and *a*' where *b* and *b*' do not match. From the remaining *n* bits where both Alice and Bob measured in the same basis, Alice randomly chooses *n* / 2 bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see if more than a certain number of them agree. If too few of the check bits agree, the incorrect rate is above some threshold, then with high probability, an eavesdropper, Eve has disturbed the transmission. Alice and Bob must abort the protocol.

In the most common eavesdropping strategy, intercept-resend, Eve individually intercepts each qubit sent by Alice, measures the qubit state and immediately sends Bob her results in order to hide her presentence. For each qubit, Eve chooses at random between the two measurement bases: eigenbasis of *x* or eigenbasis of *z*. If Eve uses the eigenbasis of *z* in a measurement, result 0 means that Eve sends $|0\rangle$, and result 1 means that she sends $|1\rangle$ to Bob. If Eve's measurement basis is eigenbasis of *x*, she resends $|+\rangle$ if the result is 0, and $|-\rangle$ if the result is 1 [16-18].

Suppose Eve makes measurement on the *k*th qubit after choosing one of the two bases randomly. If her choice is the same as the basis used by Alice to encode a_k, her measurement does not make any change in the qubit and with probability equal to unity Alice and Bob will not detect Eve's intercept of this qubit. If her choice is different from the basis, due to principles in quantum mechanics it is easy to show with the probability of $\frac{1}{2}$ Bob's measurement outcome is the same as a_k, and with this probability Eve's intercept remains undetected.

IV. STATIC GAME

A. Game Model

A static game is one in which a single decision is made by each player, and each player has no knowledge of the decision made by the other players before making their own decision [8]. Since in the BB84 protocol bases are chosen by Alice, Bob and Eve independently, we can analyze each basis choice separately. So we formulate the problem as a three player-Alice, Bob and Eve- static game. Alice's strategy is to choose between eigenbasis of *x* or eigenbasis of *z* to encode each bit of *a*. Bob's and Eve's strategy is to choose between eigenbasis of *x* or the eigenbasis of *z* to measure each qubit. In our game model, Alice's and Bob's objective is to maximize the probability of detecting Eve's intercept on each qubit, while Eve's objective is to minimize this probability. Therefore we fill the payoff tables with the probabilities of undetecting Eve's intercept on each qubit, as payoffs to Eve, and their negatives as payoffs to Alice and Bob, for each strategy combination.

The qubits for which the bases Alice and Bob have chosen do not match, are discarded. So we

consider the payoffs of 0 for Alice, Bob, and Eve in these cases. As discussed in the last paragraph of section III, When Alice, Bob and Eve choose the same bases; Eve's intercept on the qubit remains undetected with the probability equal to unity. So we assign the payoff -1 to Alice and Bob in these cases and 1 to Eve. When Alice and Bob choose the same bases and Eve chooses the other one, Eve's intercept on the qubit remains undetected with the probability of $\frac{1}{2}$. Therefore we assign the payoff $-\frac{1}{2}$ to Alice, Bob in these cases and $\frac{1}{2}$ to Eve.

Table I illustrates the payoff matrices of the game in normal form.

TABLE I. NORMAL FORM OF STATIC GAME

Payoffs to Alice

Alice chooses *x* basis

	Eve chooses *x* basis	Eve chooses *z* basis
Bob chooses *x* basis	-1	$-\frac{1}{2}$
Bob chooses *z* basis	0	0

Alice chooses *z* basis

	Eve chooses *x* basis	Eve chooses *z* basis
Bob chooses *x* basis	0	0
Bob chooses *z* basis	$-\frac{1}{2}$	-1

Payoffs to Bob

Bob chooses *x* basis

	Eve chooses *x* basis	Eve chooses *z* basis
Alice chooses *x* basis	-1	$-\frac{1}{2}$
Alice chooses *z* basis	0	0

Bob chooses *z* basis

	Eve chooses *x* basis	Eve chooses *z* basis
Alice chooses *x* basis	0	0
Alice chooses *z* basis	$-\frac{1}{2}$	-1

Payoffs to Eve

Eve chooses *x* basis

	Alice chooses *x* basis	Alice chooses *z* basis
Bob chooses *x* basis	1	$\frac{1}{2}$
Bob chooses *z* basis	0	0

Eve chooses *z* basis

	Alice chooses *x* basis	Alice chooses *z* basis
Bob chooses *x* basis	0	0
Bob chooses *z* basis	$\frac{1}{2}$	1

B. Nash equilibrium Analysis

In a well defined game, there is a generic assumption that all players are rational, so the objective of all players is to maximize their expected payoffs.

We suppose Alice, Bob and Eve choose eigenbasis of *x* with the probabilities *p*, *q* and *r*, respectively. The expected payoffs for the players, when they choose eigenbasis of *x* or the eigenbasis of *z*, are as follows.

E u_{Alice}(choosing eigenbasis of *x*)=
$-qr - \frac{1}{2}q(1-r)$
E u_{Alice}(choosing eigenbasis of *z*)=
$-\frac{1}{2}(1-q)r - (1-q)(1-r)$
E u_{Bob}(choosing eigenbasis of *x*)=
$-pr - \frac{1}{2}p(1-r)$
E u_{Bob}(choosing eigenbasis of *z*)=
$-\frac{1}{2}(1-p)r - (1-p)(1-r)$
E u_{Eve}(choosing eigenbasis of *x*)=
$qp + \frac{1}{2}q(1-p)$
E u_{Eve}(choosing eigenbasis of *z*)=
$\frac{1}{2}(1-q)p + \frac{1}{2}(1-q)(1-p)$

Nash equilibrium is an action profile with the property that no player can do better by changing her action, given the other players' actions.

In the generalization of the notion of Nash equilibrium that models a stochastic steady state of a strategic game, each player is allowed to choose a probability distribution over her set of actions rather than restricting her to choose a

single deterministic action. Such a probability distribution is referred as a mixed strategy.

The mixed strategy profile $\alpha*$ is a mixed strategy Nash equilibrium if and only if $\alpha*i$ is in $B_i(\alpha*-i)$ for every player i, where a_i is the action of player i and $a-i$ is the list of others' action [7]. Denoting by $B_{Alice}(q,r)$ the set of probabilities Alice assigns to choose the eigenbasis of x in best responses to q, r, we have

$$B_{Alice}(q,r)=\begin{cases}\{1\} & if\ \left(\frac{3q}{2}+\frac{r}{2}\right)<1\\ \{p:0\le p\le 1\} & if\ \left(\frac{3q}{2}+\frac{r}{2}\right)=1\\ \{0\} & if\ \left(\frac{3q}{2}+\frac{r}{2}\right)>1\end{cases}$$

The best response function of Bob is similar:

$$B_{Bob}(p,r)=\begin{cases}\{1\} & if\ \left(\frac{3p}{2}+\frac{r}{2}\right)<1\\ \{q:0\le q\le 1\} & if\ \left(\frac{3p}{2}+\frac{r}{2}\right)=1\\ \{0\} & if\ \left(\frac{3p}{2}+\frac{r}{2}\right)>1\end{cases}$$

The best response function of Eve is as follows:

$$B_{Eve}(p,q)=\begin{cases}\{0\} & if\ \left(\frac{3p}{2}+\frac{q}{2}\right)<1\\ \{r:0\le r\le 1\} & if\ \left(\frac{3p}{2}+\frac{q}{2}\right)=1\\ \{1\} & if\ \left(\frac{3p}{2}+\frac{q}{2}\right)>1\end{cases}$$

Best response functions are illustrated in Fig. 1.

The set of mixed strategy Nash equilibria of the game corresponds to the set of intersections of the best response functions in this figure; we see that there is one intersection, corresponding to the Nash equilibrium each player assigns probability $\frac{1}{2}$ to choose eigenbasis of x; and illuminates the result taken by mathematical calculations.

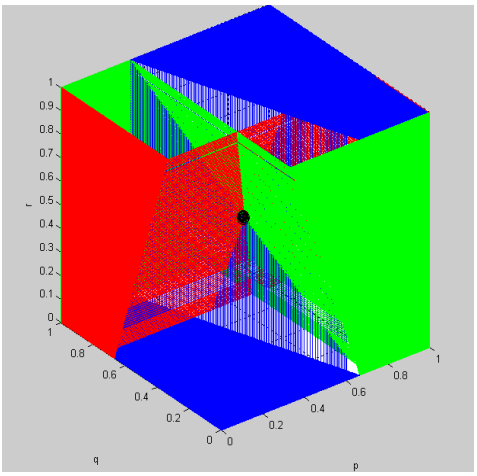

Figure 1. The players' best response functions. The probabilities assigned by Alice, Bob, and Eve to choose eigenbasis of x are p, q and r respectively. The best response function of Alice is blue, that of Bob is green, and Eve's is red. The black point indicates unique Nash equilibrium.

V. CONCLUSION AND FUTURE WORK

In this paper we presented a game theory model to view the BB84 protocol. In our model Alice, Bob, and Eve are the three players. Alice and Bob cooperate each other and try to maximize the probability of detecting Eve, while Eve is against them and tries to minimize this probability. Mixed strategy Nash equilibrium analysis assigns the probability of $\frac{1}{2}$ to Alice, Bob and Eve for choosing between eigenbasis of x and eigenbasis of z.

In our further research, we will notice more parameters, like the efficiency of the protocol, to present a more comprehensive model.

REFERENCES

[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution protocols," *Phys. Rev. A* vol. 73, 2006.

[2] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," Karlsruhe, Germany: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications 2003..

[3] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology* vol. 18, pp. 133 - 165 2005.

[4] W. Y. Hwang, I. G. Koh, and Y. D. Han, "Quantum cryptography without public announcement of bases," *Phys Letters A,* vol. 244, pp. 489-494, 1998.

[5] O. Ahonen, M. Möttönen, and J. L. O'Brien, "Entanglement-enhanced quantum key distribution," *Phys. Rev. A* vol. 78, 2008.

[6] G. B. Charles. H Bennet, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceeding of IEEE International Conference on Computer System and Signal Processing*, New York, 1984, pp. 175-179.

[7] M. J. Osborne, *An Introduction to Game Theory*: Oxford University Press, 2003.

[8] J. N. Webb, *Game Theory, Decisions, Interactions and Evolution*, 1 ed.: Springer, 2006.

[9] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA: The MIT Press, 1994.

[10] D. Fudenberg and J. Tirole, *Game Theory*: MIT Press, 1991

[11] R. Gibbons, *A Primer in Game Theory*: Prentice Hall, 1992.

[12] Y. XIAO, X. SHAN, and Y. REN, "Game Theory Models for IEEE 802.11 DCF in Wireless Ad Hoc Networks," in *IEEE Radio Communications*, 2005.

[13] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton, N.J: Princeton Univ. Press, 1944.

[14] J. Nash, "Equilibrium points in *n*-person games," *Proceedings of the National Academy of Sciences*, vol. 36, pp. 48–49, 1950.

[15] ——, "Non-cooperative games," *The Annals of Mathematics*, vol. 54, no. 2, pp. 286–295, 1951.

[16] M. Nakahara and T. Ohmi, *Quantum Computing: From Linear Algebra to Physical Realizations*, 1 ed.: Taylor & Francis, 2008.

[17] G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Compuation and Information* vol. 1: Basic concepts: World Scientific Publishing, 2004.

[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*: Cambridge university press, 2001.