Optical Realization of Quantum Gambling Machine

Yong-Sheng Zhang, Chuan-Feng Li, Wan-Li Li, Yun-Feng Huang, and Guang-Can Guo*

Laboratory of Quantum Communication and Quantum Computation and Department of Physics, University of Science and Technology of China, Hefei 230026, P. R. China

Quantum gambling — a secure remote two-party protocol which has no classical counterpart — is demonstrated through optical approach. A photon is prepared by Alice in a superposition state of two potential paths. Then one path leads to Bob and is split into two parts. The security is confirmed by quantum interference between Alice's path and one part of Bob's path. It is shown that a practical quantum gambling machine can be feasible by this way.

As a kind of game, gambling plays an important role in the society and nature which are full of conflict, competition and cooperation. Up to now, game theory has been investigated with mathematical methods [1] and applied to study economy, psychology, ecology, biology and many other fields [2, 3].

One might wonder why games like gambling can have anything to do with quantum physics. After all, game theory is about numbers that entities are efficiently acting to maximize or minimize. However, if linear superpositions of the actions are permitted, games will be generalized into quantum domain [4, 5]. Quantizing games may be interesting in several fields [4], such as foundation of game theory, games of survival and quantum communication [6]. Moreover, quantum mechanics may assure the fairness in remote gambling [7].

In this letter, we present a quantum gambling machine composed of optical elements.

We may firstly investigate the simplest classical gambling machine: one particle and two boxes A and B. During a game, the casino (Alice) stores the particle in A or B randomly, then the player (Bob) guesses which box the particle is in. For the two parties do not trust each other, even a third party, a remote classical gambling is impossible. Whereas in the quantum domain, Alice may prepare the particle in a superposition state of $|a\rangle$ (the particle in A) and $|b\rangle$ (the particle in B). If she generate the equal superposition state

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\left(|a\rangle + |b\rangle\right) \tag{1}$$

and a prescribed box (e.g. B) is sent to Bob, a remote fair gambling may be carried out. For simplicity, the bet in a single game is taken to be one coin. If Bob finds the particle in box B (state $|b\rangle$), he wins one coin, otherwise he loses the bet. Obviously, the probability for Bob to win is exactly 50%. Moreover, Bob cannot cheat by claiming that he found the particle when he did not, for Alice can verify by opening box A.

In order to decrease the probability for the particle in box B, Alice may prepare a biased superposition state (she gets no advantage using an ancilla or other complex strategy [7])

$$|\Psi_0'\rangle = \sqrt{\frac{1}{2}+\epsilon}\,|a\rangle + \sqrt{\frac{1}{2}-\epsilon}\,|b\rangle \tag{2}$$

instead of $|\Psi_0\rangle$, where ϵ is the preparation parameter, with $0 \leq \epsilon \leq \frac{1}{2}$. However, the quantum principle assures that Bob has a chance to find out the difference and win her R coins, which is the punishment the two parties agree on before the game.

Bob's strategy is to split out part of the state $|b\rangle$ and convert it to state $|b'\rangle$ by performing a unitary operation, *i.e.*,

$$|b\rangle \rightarrow \sqrt{1-\eta}\,|b\rangle + \sqrt{\eta}\,|b'\rangle\,, \tag{3}$$

Where $|b'\rangle$ is orthogonal to $|a\rangle$ and $|b\rangle$ and η is the splitting parameter. After the splitting, if

*Electronic address: gcguo@ustc.edu.cn

Bob does not find the particle in box B, Alice will send box A to him for verification. In this case the state of the particle is reduced to $|\phi_a\rangle = \sqrt{\frac{1}{1+\eta}}\left(|a\rangle + \sqrt{\eta}\,|b'\rangle\right)$, if Alice prepare the particle in the equal superposition state $|\Psi_0\rangle$. Therefore, the verification of Bob is to measure the particle under the basis $|\phi_a\rangle$ and its orthogonal basis $|\phi_b\rangle$. If Alice prepare the biased superposition state $|\Psi_0'\rangle$, he may find the particle in state $|\phi_b\rangle$ with a certain probability and win R coins.

There exists an equilibrium for the two parties in this protocol [7]. Alice can ensure her expected gains no less than zero by preparing the equally distributed state $|\Psi_0\rangle$. Bob can ensure his expected gains no less than a particular value only depending on R by selecting an optimal splitting parameter $\eta = \tilde{\eta}(R)$. In fact, this protocol is a zero-sum game, and the strategies of Alice and Bob are represented by different choices of ϵ and η, respectively.

In the experiment, a linear-polarized photon is employed as the particle. Similar to the simulation of quantum logic [8], two potential paths of the photon may serve as boxes A and B. $|b'\rangle$ are distinguished from $|a\rangle$ and $|b\rangle$ by the polarization of the photon.

Figure 1

The setup of the optical quantum gambling machine is shown in Figure 1. A virtue of this machine is that all the detections are carried out automatically by the machine, which may help to eliminate the classical communication between the parties and prevent their cheating.

Initially, the photon is generated in a definite linear polarization state (such as vertical $|V\rangle$ or horizontal $|H\rangle$) by a polarizer. Then the state is transferred to a superposition state of $|V\rangle$ and $|H\rangle$ with half waveplate (HWP) a according to the preparation parameter ϵ chosen by Alice. The preparation is accomplished by swapping the location and polarization states of the photon with polarizing beamsplitter (PBS) 1 and the fixed HWP σ_x. After the state swapping, the polarization is horizontal while the location is prepared in the required state $|\Psi_0'\rangle$.

Bob's splitting is realized by adjusting the HWP b_1 according to the parameter η he selects. Then $|b'\rangle$ (split out by Bob) is separated from $|b\rangle$ via PBS 2 and superposed with $|a\rangle$ via PBS 3. The verification is implemented with HWP b_1 and PBS 4. HWP b_1 is adjusted according to η so as to assure that $|\phi_a\rangle$ and $|\phi_b\rangle$ are transmitted and reflected by PBS 4 respectively. In order to obtain the result of the gambling, three detectors D_1, D_2 and D_3 are adopted to detect the photon in the state $|b\rangle$, $|\phi_a\rangle$ and $|\phi_b\rangle$, respectively.

A single game of gambling with this machine is described as follows. After Bob put in his bet — one coin, the machine will inform Alice and Bob to select the parameter ϵ (adjusting HWP a) and η (adjusting HWP b_1 and b_2 simultaneously). Then a photon is generated from the polarizer and distributed to three parts. If the detector D_1 or D_3 responds, Bob win one or R coins; if D_2 responds, Bob loses the bet (then the bet will be conserved for Alice automatically).

To demonstrate the performance of the optical gambling machine, a beam (composed of independent identical photons) is generated instead of a single photon during the experiment, namely, a well polarized He-Ne laser (3mW at 632.8nm) is utilized as the light source. The results are shown in Figure 2, where P_1 and P_3 denote the probabilities that Bob win one and R coins, P_2 denotes the probability that Bob lose the bet. The probabilities are determined by the relative light intensities measured by the three detectors.

Figure 2

In order to illustrate Bob's strategies, we suppose that Alice and Bob agree on $R = 5$ at the beginning of the gambling. The expected gains of Bob are shown in Figure 3. Obviously, there exists an optimal splitting parameter $\tilde{\eta}(5) \doteq 0.27$ to assure his expected gains no less than a particular value despite Alice's choice.

Figure 3

Optical approach has many advantages. By making use of two different freedom degrees of the photon (location and polarization), an optical quantum gambling machine may be realized conveniently with several HWPs, PBSes and detectors. Particularly, the decoherence of all-optical system is relatively low [9], while the protocol is very sensitive to the errors caused by the device and environment. As discussed by Goldenberg *et* *al.* [7], for a successful realization of quantum gambling, the error rate has to be lower than $\sqrt{2/R^3}$. Since the error rate in the experiment is only about $\frac{1}{40}$, a practical quantum gambling may be carried out with this optical machine under the condition $R < 14.4$.

Our experiment has shown that quantum gambling and quantum games have real physical counterpart, and a practical quantum gambling machine can be realized with simple optical devices. It can be expected that quantum mechanics may bring other interesting results in game theory.

This work was supported by the National Natural Science Foundation of China and the Doctoral Education Fund of the State Education Commission of China.

---

[1] J. Von Neumann and O. Morgenstern, *The theory of Games and Economic Behavior* (Princeton University Press, Princeton, 1947).

[2] R. B. Myerson, *Game Theory: An Analysis of Conflict* (MIT Press, Cambridge, 1991).

[3] R. Axelrod, *The Evolution of Cooperation* (Basic Books, New York, 1984); R. Dawkins, *The Selfish Gene* (Oxford University Press, Oxford, 1976).

[4] J. Eisert, M. Wilkens, M. Lewenstein, *Phys. Rev. Lett.* **83**, 3077 (1999).

[5] D. A. Meyer, *Phys. Rev. Lett.* **82**, 1052 (1999).

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smonlin, *J. Crypto.* **5**, 3 (1992).

[7] L. Goldenberg, L. Vaidman, S. Wiesner, *Phys. Rev. Lett.* **82**, 3356 (1999).

[8] N. J. Cerf, C. Adami, P. G. Kwiat, *Phys. Rev. A* **57**, 1447 (1998).

[9] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, A. G. White, quant-ph/**9905086** at http://xxx.lanl.gov.

Figure captions:

Figure 1. The optical setup for quantum gambling machine.

The PBSes transmit the horizontal and reflect the vertical component of the photons. HWP σ_x is fixed at 45°. HWP a is used for Alice to adjust ϵ for preparation. HWP b_1 is adopted for Bob to adjust η for splitting. HWP b_2 is utilized to accomplish the verification. The phase difference between the two paths from PBS 1 to PBS 3 are tuned to zero in advance. If the photon is detected by D_1 or D_3, Bob wins one or R coins, respectively. If it is detected by D_2, Bob loses one coin.

Figure 2. Performance of the machine.

P_1, P_2 and P_3 denote the probabilities that Bob wins one, loses one and wins R coins, respectively. With a certain preparation parameter ϵ, the probabilities vary with the splitting parameter η. The experimental data are denoted by scattered dots. The solid diamond, open downtriangle, solid uptriangle, solid circle and open square represent the cases that $\epsilon = 0$, 0.19, 0.34, 0.47 and 0.5, respectively. The corresponding lines are theoretical predictions.

Figure 3. Expected gains of Bob varying with ϵ and η.

Experimental results are denoted by scattered dots. The cross ($\times$), downtriangle, cross ($+$), diamond, square represent the case that $\epsilon = 0$, 0.19, 0.34, 0.47 and 0.5, respectively. The corresponding lines are theoretical predictions. The lower bound of all possible values is denoted by the dashed line. It is shown that the optimal parameter $\tilde{\eta}(5) \doteq 0.27$ because at this value the maximum of the lower bound is accessed.

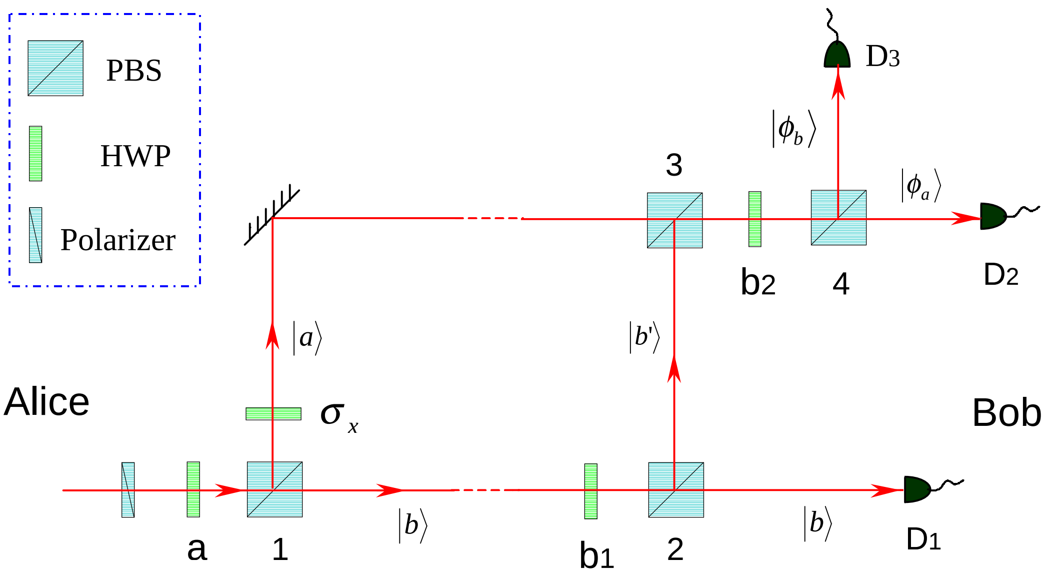

Figure 1, Zhang

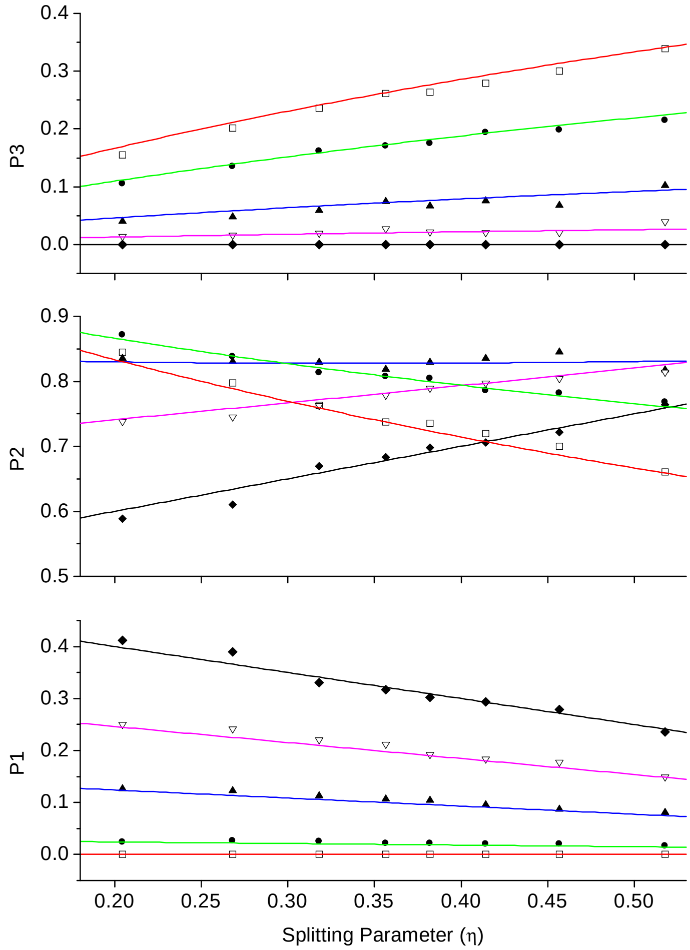

Figure 2, Zhang

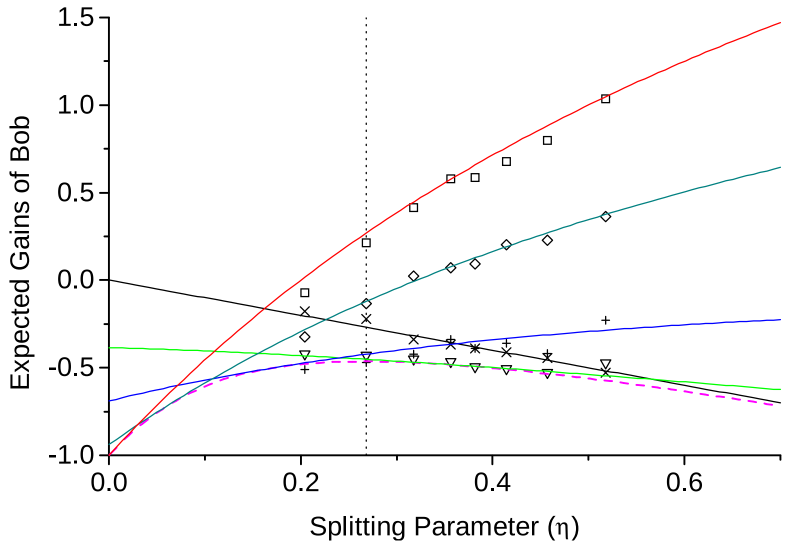

Figure 3, Zhang