# An Analysis of the Ping-Pong Protocol Operation in a Noisy Quantum Channel

Piotr Zawadzki

Institute of Electronics,
Silesian University of Technology,
Akademicka 16, 44-100 Gliwice, Poland
Piotr.Zawadzki@polsl.pl

**Abstract.** A generalized approach to Ping-Pong protocol analysis is introduced. The method is based on investigation of the density operator describing joint systems of communicating parties and an eavesdropper. The method is more versatile than approaches used so far as it permits on incorporation of different noise models in a unified way and make use of well grounded theory of quantum discrimination in estimation of eavesdropper's information gain. As the proof of the method usefulness an example of its application to the analysis of the protocol execution over depolarizing and dephasing channels is given.

**Keywords:** quantum direct communication, quantum cryptography.

## 1 Introduction

In the last two decades, we have witnessed several scientific discoveries which permitted to utilize quantum mechanical principles to enhance our abilities to compute and communicate [1]. Exploiting quantum nature of composite systems is of particular relevance in developing quantum technology for efficient computation [2–4] and secure communication [5] exceeding classical limits [6]. Non-locality and entanglement are the most prominent signatures of non-classicality [7]. In particular, entanglement of shared quantum states is the vital element for the success of Quantum Key Distribution (QKD) and Quantum Direct Communication (QDC) protocols, including the quantum dense information coding [8, 9] and quantum teleportation of states [10]. QKD schemes provide cryptographically secure keys [7] which are subsequently used to protect classical telecommunication links with methods known from classic cryptography [11]. In contrary, QDC protocols do not require prior key agreement and their security results from the laws of quantum mechanics [12].

The so called Ping-Pong protocol has attracted a lot of attention as it is asymptotically secure in lossless channels [13]. The theoretical success of the protocol has been closely followed by the experimental implementation and the proof on concept installation has been realized in the laboratory [14]. It has been also shown that protocol variants based on higher dimensional systems and

A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2013, CCIS 370, pp. 354–362, 2013.

exploiting dense information coding also share features of the seminal version when some improvements are introduced [15, 16].

The Ping-Pong protocol, similarly to other QDC protocols, operates in two modes: a message mode is designed for information transfer and a control mode is used for eavesdropping detection. Although the Ping-Pong protocol is asymptotically secure in perfect quantum channels, the situation looks worse in noisy environments when legitimate users tolerate some level of transmission errors and/or losses. If that level is too high compared to the quality of the channel, then an eavesdropper can peek some fraction of signal particles hiding himself behind accepted Quantum Bit Error Rate (QBER) threshold [17, 18]. But the possibility to intercept some part of the message without being detected renders the protocol insecurity. To cope with this problem an additional purely classical layer has been proposed [19]. However, estimation of security improvement offered by that layer heavily depends on observed QBER. Unfortunately the used so far methods of the protocol analysis do not offer mathematical apparatus capable to estimate QBER in noisy channels. The purpose of the following text is to fill in this gap.

The proposed method is based on the investigation of the properties of the density matrix describing the joint system of the communicating parties. This is in contrast with previous approaches in which probability distribution observed by the eavesdropper has been derived by manipulations on state vectors. The introduced approach is more general as it permits on easy incorporation of different models of noise in a unified way and make use of quantum states discrimination theory achievements [20–22] in estimation of eavesdropper's information gain and calculation of QBER observed by the receiver. As the proof of concept the example of method application to the analysis of the protocol operation over depolarizing channel is given.

## 2 Ping-Pong Protocol New Description

Let us consider the seminal version of the Ping-Pong protocol [13] in which the message and control mode are executed only in computational basis. The communication process is started by Bob, the recipient of information, who prepares an EPR pair

$$|\phi^+\rangle = \left(|0_\mathrm{B}\rangle|0_\mathrm{A}\rangle + |1_\mathrm{B}\rangle|1_\mathrm{A}\rangle\right)/\sqrt{2}\ . \tag{1}$$

At the same time eavesdropping Eve controls her own system, which is initially described by state $|\chi_\mathrm{E}\rangle$. As the states of Bob and Eve are separated, the density matrix of the whole system reads

$$\rho^{(0)}_{\mathrm{BAE}} = \rho^{(0)}_{\mathrm{BA}} \otimes \rho^{(0)}_{\mathrm{E}} = |\phi^+\rangle\langle\phi^+| \otimes |\chi_\mathrm{E}\rangle\langle\chi_\mathrm{E}|\ . \tag{2}$$

Next Bob sends a signal qubit A to Alice. This qubit on its way can be influenced by two factors: quantum noise because of channel imperfection and malicious activities of Eve who may entangle it with the system controlled by herself. Let us assume, that Eve is positioned close to Alice, so her action takes place on the

qubit modified by the noise. The density matrix of the system just before signal qubit enters environment controlled by Alice reads

$$\rho^{(1)}_{\mathrm{BAE}} = (\mathcal{N}_{\mathrm{BA}} \otimes \mathcal{I}_{\mathrm{E}}) \left( \rho^{(0)}_{\mathrm{BA}} \otimes \rho^{(0)}_{\mathrm{E}} \right) = \rho^{(1)}_{\mathrm{BA}} \otimes \rho^{(0)}_{\mathrm{E}} \ , \tag{3}$$

where it was explicitly highlighted that noise operator $\mathcal{N}$ acts only on the EPR pair ($\mathcal{I}$ denotes identity operation). Before signal qubit enters Alice's environment, Eve can entangle it with her own system

$$\rho^{(2)}_{\mathrm{BAE}} = (\mathcal{I}_{\mathrm{B}} \otimes \mathcal{E}_{\mathrm{AE}}) \, \rho^{(1)}_{\mathrm{BAE}} \ , \tag{4}$$

where entangling operator $\mathcal{E}_{\mathrm{AE}}$ acts only on qubit A of the EPR pair and system possessed by Eve. At that point of protocol execution Alice can select a control mode or continue in information mode.

In the former case she measures received qubit in computational basis, i.e. performs von Neumann measurement using projectors $M_{x,A} = \mathcal{I}_{\mathrm{B}} \otimes |x_{\mathrm{A}}\rangle\langle x_{\mathrm{A}}| \otimes \mathcal{I}_{\mathrm{E}}$, $x = 0, 1$. Probability that she finds qubit under investigation in state $|x\rangle$ (measures $\pm 1$) is given by

$$p_{\mathrm{A}}(x) = \mathrm{Tr}\left( \rho^{(2)}_{\mathrm{BAE}} M_{x,\mathrm{A}} \right) \ . \tag{5}$$

After measurement the state of the whole system collapses to

$$\sigma_{x\,\mathrm{BAE}}^{(2)} = \frac{M_{x,\mathrm{A}} \rho^{(2)}_{\mathrm{BAE}} M_{x,\mathrm{A}}}{\mathrm{Tr}\left( \rho^{(2)}_{\mathrm{BAE}} M_{x,\mathrm{A}} \right)} \ . \tag{6}$$

Subsequently Bob measures his qubit in computational basis using projectors $M_{y,\mathrm{B}} = |y_{\mathrm{B}}\rangle\langle y_{\mathrm{B}}| \otimes \mathcal{I}_{\mathrm{A}} \otimes \mathcal{I}_{\mathrm{E}}$, $y = 0, 1$. Probability that Bob finds his qubit in state $|y\rangle$ provided that Alice has found his qubit in state $|x\rangle$ is given by

$$p_{\mathrm{B|A}}(y|x) = \mathrm{Tr}\left( \sigma_{x\,\mathrm{BAE}}^{(2)} M_{y,\mathrm{B}} \right) \ . \tag{7}$$

It follows that errors in control mode appear with probability

$$P_{\mathrm{EC}} = p_{\mathrm{B|A}}(1|0) \, p_{\mathrm{A}}(0) + p_{\mathrm{B|A}}(0|1) \, p_{\mathrm{A}}(1) \ . \tag{8}$$

In information mode, Alice encodes classic bit $\mu$ applying ($\mu = 1$) or not ($\mu = 0$) operator $Z_{\mathrm{A}}$ to the possessed qubit. The system state after encoding is given by

$$\rho_{\mu\,\mathrm{BAE}}^{(3)} = (\mathcal{I}_{\mathrm{B}} \otimes Z_{\mathrm{A}}^{\mu} \otimes \mathcal{I}_{\mathrm{E}}) \, \rho^{(2)}_{\mathrm{BAE}} \left( \mathcal{I}_{\mathrm{B}} \otimes (Z_{\mathrm{A}}^{\mu})^{\dagger} \otimes \mathcal{I}_{\mathrm{E}} \right) \ . \tag{9}$$

The qubit A is sent back to Bob after encoding operation. Eve's task is to discriminate between states $\rho_{\mu\,\mathrm{AE}}^{(3)} = \mathrm{Tr}_{\mathrm{B}}\left( \rho_{\mu\,\mathrm{BAE}}^{(3)} \right)$ with maximal confidence. The system states after reception by Bob of a qubit A travelling back from Alice and in the absence of Eve measurements are given by

$$\rho_{\mu\,\mathrm{BAE}}^{(4)} = (\mathcal{N}_{\mathrm{BA}} \otimes \mathcal{I}_{\mathrm{E}}) \, \rho_{\mu\,\mathrm{BAE}}^{(3)} \ , \tag{10}$$

so Bob has to distinguish the states

$$\rho_{\mu\,\mathrm{BA}}^{(4)} = \mathrm{Tr}_{\mathrm{E}}\left(\rho_{\mu\,\mathrm{BAE}}^{(4)}\right) \quad . \tag{11}$$

When Eve performs measurements, the same quantum discrimination strategy is used but Bob is unconscious that measured states are of the form

$$\tau_{\mu,\alpha\,\mathrm{BA}}^{(4)} = \mathrm{Tr}_{\mathrm{E}}\left((\mathcal{N}_{\mathrm{BA}} \otimes \mathcal{I}_{\mathrm{E}})\,\frac{M_{\alpha,\mathrm{E}}\rho_{\mu\,\mathrm{BAE}}^{(3)}M_{\alpha,\mathrm{E}}}{\mathrm{Tr}\left(\rho_{\mu\,\mathrm{BAE}}^{(3)}M_{\alpha,\mathrm{E}}\right)}\right) \quad . \tag{12}$$

The analysis of the protocol should determine Eve's information gain $I_{\mathrm{E}}$ and probability of erroneous Bob's decoding $QBER$ as a functions of probability of error observed in control mode $P_{\mathrm{EC}}$ and, optionally, parameters describing noise operator $\mathcal{N}$.

## 3 Active Eavesdropping in the Noiseless Case

Ping-pong protocol active eavesdropping in perfect quantum channels has been analysed many times and protocol properties for this scenario are well known. The aim of this section is to show, that generalized approach presented in the previous section gives the same results. In the considered case noise operator is reduced to identity ($\mathcal{N} = \mathcal{I}$) and the most general entangling operation can be described as [13]

$$\mathcal{E}_{\mathrm{AE}}|0_{\mathrm{A}}\rangle|\chi_{\mathrm{E}}\rangle \to a|0_{\mathrm{A}}\rangle|0_{\mathrm{E}}\rangle + b|1_{\mathrm{A}}\rangle|1_{\mathrm{E}}\rangle \tag{13}$$

$$\mathcal{E}_{\mathrm{AE}}|1_{\mathrm{A}}\rangle|\chi_{\mathrm{E}}\rangle \to c|0_{\mathrm{A}}\rangle|2_{\mathrm{E}}\rangle + d|1_{\mathrm{A}}\rangle|3_{\mathrm{E}}\rangle \tag{14}$$

where map's coefficient are not independent: $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$, $|a| = |d|$, $|b| = |c|$. After some tedious calculations one gets $P_{\mathrm{EC}} = |b|^2$ and states accessible to Eve take form

$$\begin{aligned}\rho_{\mu\,\mathrm{AE}}^{(3)} = \frac{1}{2}\,[\;& |a|^2\,|0_{\mathrm{A}}\rangle|0_{\mathrm{E}}\rangle\langle 0_{\mathrm{A}}|\langle 0_{\mathrm{E}}| + (-1)^{\mu}a^*b|1_{\mathrm{A}}\rangle|1_{\mathrm{E}}\rangle\langle 0_{\mathrm{A}}|\langle 0_{\mathrm{E}}| + \\ &+ (-1)^{\mu}ab^*|0_{\mathrm{A}}\rangle|0_{\mathrm{E}}\rangle\langle 1_{\mathrm{A}}|\langle 1_{\mathrm{E}}| + |b|^2\,|1_{\mathrm{A}}\rangle|1_{\mathrm{E}}\rangle\langle 1_{\mathrm{A}}|\langle 1_{\mathrm{E}}| + \\ &+ |c|^2\,|0_{\mathrm{A}}\rangle|2_{\mathrm{E}}\rangle\langle 0_{\mathrm{A}}|\langle 2_{\mathrm{E}}| + (-1)^{\mu}dc^*|1_{\mathrm{A}}\rangle|3_{\mathrm{E}}\rangle\langle 0_{\mathrm{A}}|\langle 2_{\mathrm{E}}| + \\ &+ (-1)^{\mu}cd^*|0_{\mathrm{A}}\rangle|2_{\mathrm{E}}\rangle\langle 1_{\mathrm{A}}|\langle 3_{\mathrm{E}}| + |d|^2\,|1_{\mathrm{A}}\rangle|3_{\mathrm{E}}\rangle\langle 1_{\mathrm{A}}|\langle 3_{\mathrm{E}}|\;]\quad .\end{aligned} \tag{15}$$

At this point Holevo bound is usually used to estimate Eve's information gain

$$I_{\mathrm{E}}^{\mathcal{H}} = S\left(\frac{1}{2}\rho_{0\,\mathrm{AE}}^{(3)} + \frac{1}{2}\rho_{1\,\mathrm{AE}}^{(3)}\right) - \frac{1}{2}S\left(\rho_{0\,\mathrm{AE}}^{(3)}\right) I_{\mathrm{E}}^{\mathcal{H}} - \frac{1}{2}S\left(\rho_{1\,\mathrm{AE}}^{(3)}\right) = H\left(P_{\mathrm{EC}}\right) \tag{16}$$

where $S(\cdot)$ denotes von Neumann entropy and $H(\cdot)$ – entropy of a binary source. This result is in perfect agreement with data presented in literature [13, 15, 16]. However, the above estimate is an overkill in the considered scenario as it implicitly assumes that Eve has infinite number of $\rho_{\mu\,\mathrm{AE}}^{(3)}$ states and she can perform

a series of collective measurements. In practice, Eve can only mount an individual attack in which she has single copy of $\rho_{\mu\,\mathrm{AE}}^{(3)}$ for the given value of $\mu$ and she can perform only one measurement. It seems that unambiguous discrimination [20] is the most reasonable approach in such situation, although some other strategies are possible [21]. Eve's information gain is then equal to

$$I_{\mathrm{E}} = P_{\mathrm{s}} \log_2 N \ , \tag{17}$$

where $P_{\mathrm{s}}$ is a probability of successful measurement and $N$ denotes the number of discriminated states. In the considered protocol version $N = 2$ and the upper bound on $P_{\mathrm{s}}$ is given by [22]

$$P_{\mathrm{s}}^{\max} = 1 - F\left(\rho_0, \rho_1\right) \tag{18}$$

where $F\left(\rho_0, \rho_1\right) = \mathrm{Tr}\left|\sqrt{\rho_0}\sqrt{\rho_1}\right|$ denotes fidelity, $\mathrm{Tr}\left|\mathcal{A}\right| = \sum_k \left|\lambda_k\right|$ where $\lambda_k$ are eigenvalues of $\mathcal{A}$ and it was assumed that states $\rho_\mu$ are equally probable. Using (18) to states $\rho_{\mu\,\mathrm{AE}}^{(3)}$ specified in (15) one gets

$$F\left(\rho_0, \rho_1\right) = \left(1 - 2P_{\mathrm{EC}}\right)^2 \tag{19}$$

what leads to the following expression for an upper bound on Eve's information gain in individual attacks

$$I_{\mathrm{E}} = 4P_{\mathrm{EC}}\left(1 - P_{\mathrm{EC}}\right) \ . \tag{20}$$

The comparison of bounds (20) and (16) is shown on Fig. 1. It follows that in both cases undetectable attack ($P_{\mathrm{EC}} = 0$) provides Eve no information, and an attack providing maximal information ($I = 1\,\mathrm{bit}$) is detectable by control mode with probability 1/2. It is also visible that collective attacks provide only slight advantage compared to the individual ones.

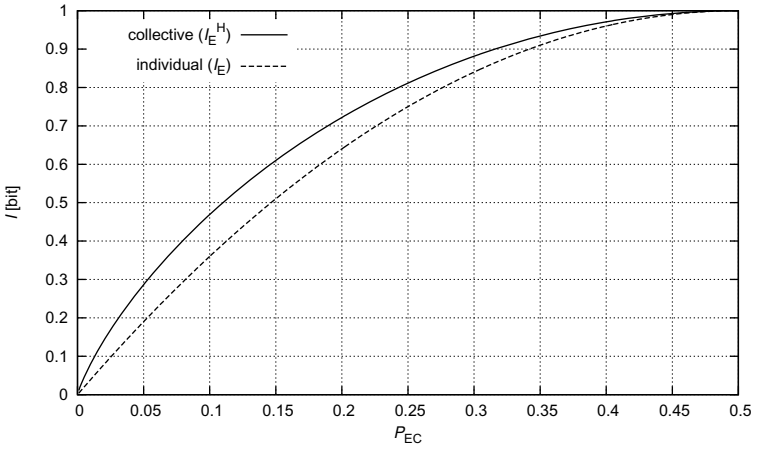


**Fig. 1.** Comparison of the eavesdropper's information upper bounds in collective ($I_{\mathrm{E}}^{\mathcal{H}}$) and individual ($I_{\mathrm{E}}$) attacks

## 4 Passive Eavesdropping in a Noisy Channel

Let us consider situation in which Eve does not entangle with a signal qubit i.e. $\mathcal{E}_{\mathrm{AE}} = \mathcal{I}_{\mathrm{A}} \otimes \mathcal{I}_{\mathrm{E}}$. Such assumption results in separation of the system controlled by Eve, so it is not taken into account in further expressions.

Any interaction with the environment observed from the perspective of the principal system only can be given in operator sum (Kraus) representation [1] as

$$\mathcal{N}\rho \to \sum_k E_k \rho E_k^\dagger \tag{21}$$

provided that $\sum_k E_k E_k^\dagger = \mathcal{I}$. Such an approach hides details of the interaction of the system under investigation with the environment. However, these details are not of immediate relevance in analysis of many quantum information processing related tasks. In such situations Kraus representation proved to be useful because it provides a unified description of many, seemingly different, physical processes.

A depolarizing channel used to model white noise [1]. is described by the following operators in the single qubit case

$$E_0 = \frac{\sqrt{1+3r}}{2}\mathcal{I} \ , \quad E_k = \frac{\sqrt{1-r}}{2}\sigma_k \ , \tag{22}$$

where $k = 1, 2, 3$, $\sigma_k$ are Pauli matrices and $r$ denotes channel reliability. As the noise affects only travelling qubit, the Kraus operators for the investigated system can be obtained by simple extension [23]

$$E_{\mathrm{BA}\,k} = \mathcal{I}_{\mathrm{B}} \otimes E_k \ . \tag{23}$$

With the help Equation (23) the map describing noise operator $\mathcal{N}_{\mathrm{BA}}$ can be constructed and the quantities given by (8) and (11) are easy to find numerically. If Bob uses unambiguous discrimination, the bits are lost (measurement fails) with a probability [22]

$$QLOSS = 1 - P_{\mathrm{s}}^{\max} = F\left(\rho_{0\,\mathrm{BA}}^{(4)}, \rho_{1\,\mathrm{BA}}^{(4)}\right) \ . \tag{24}$$

On the other hand, if Bob uses minimum error discrimination the observed bit error rate is equal to [24]

$$QBER = \frac{1}{2}\left(1 - \frac{1}{2}\mathrm{Tr}\left(\left|\rho_{0\,\mathrm{BA}}^{(4)} - \rho_{1\,\mathrm{BA}}^{(4)}\right|\right)\right) \ . \tag{25}$$

Quantities $QBER$ and $QLOSS$ as a function of control mode failure probability (8), which is a parameter directly accessible to communicating parties, are shown on Fig. 2. Both $QBER$ and $QLOSS$ do not scale linearly with $P_{\mathrm{EC}}$. Moreover, the functional form of the the obtained scaling heavily depends on parameters of the noise model used, thus the correct modelling of noise is of prime importance in the estimation of the protocol operation over non-perfect quantum channels.

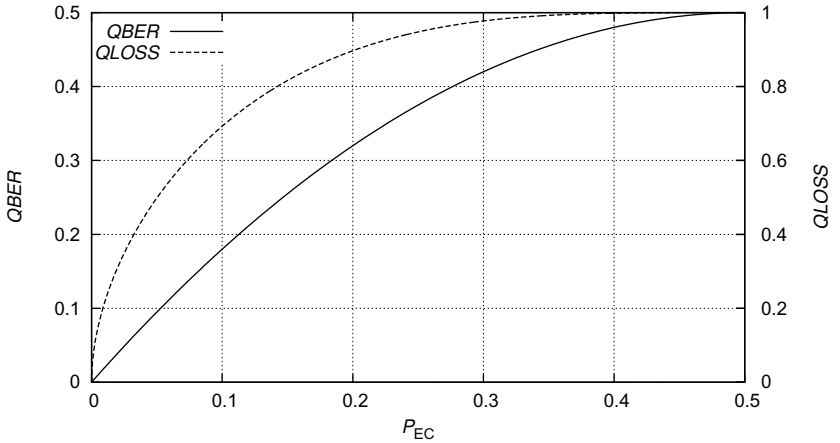


**Fig. 2.** Probabilities of a particle loss ($QLOSS$) or an erroneous decoding ($QBER$) as a function of control mode failure probability ($P_{\mathrm{EC}}$) in protocol operation over depolarizing channel

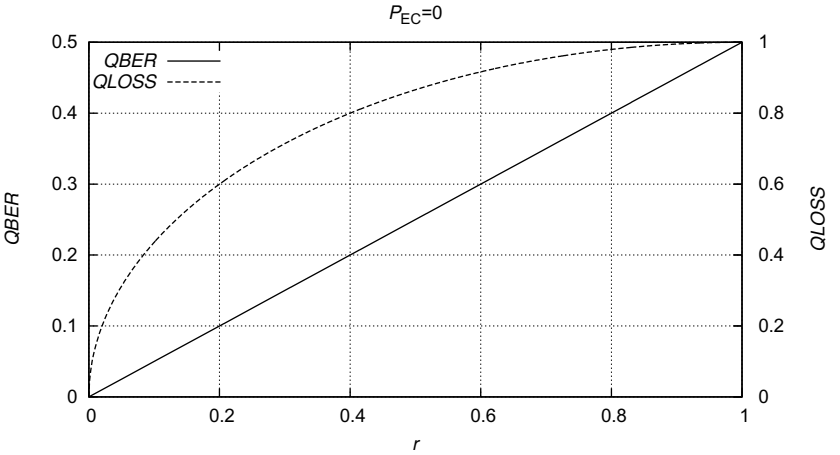


**Fig. 3.** Probabilities of a particle loss ($QLOSS$) or an erroneous decoding ($QBER$) as a function of dephasizig channel reliability $r$ (see (26) for explanation)

To emphasize the above stated thesis, let us consider protocol operation over dephasing channel, which is described by the following Kraus operators [1]

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-r} \end{bmatrix} \quad , \quad E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{r} \end{bmatrix} \tag{26}$$

where parameter $r \to 0$ for weak coupling and short interaction time and $r \to 1$ for strong coupling and/or long interaction time. Using definition (26) one can find that probability of error occurrence in control mode given by expression (8)

$$P_{\mathrm{EC}} \equiv 0 \tag{27}$$

independent of $r$. On the other hand probabilities of bit loss (24) or its detection error (25) are non-zero and vary, depending on $r$ value, in a range similar to the observed one for the depolarizing channel (see Fig. 3). It follows that some kinds of channel imperfections are not well detected by control mode, what implies, that it cannot universally (i.e. independent of occurring noise model) be used for estimation of QBER and/or QLOSS observed in information mode.

## 5 Conclusion

The usefulness of the general method based on density operator analysis for Ping-Pong protocol operation has been presented. As the proof of concept the example of its application to the analysis of the protocol execution over depolarizing and dephasing channels has been given. The analysis of a more complicated case of an active eavesdropping is left for future research. Although the method is more cumbersome than approach used so far, it is more versatile as it permits on incorporation of different models of noise in a unified way and make use of a well grounded theory of quantum discrimination in estimation of eavesdropper's information gain.

## References

1. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
2. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997)
3. Zawadzki, P.: A numerical simulation of quantum factorization success probability. In: Tkacz, E., Kapczyński, A. (eds.) Internet – Technical Developments and Applications. AISC, vol. 64, pp. 223–231. Springer, Heidelberg (2009)
4. Zawadzki, P.: A fine estimate of quantum factorization success probability. Int. J. Quant. Inf. 8(8), 1233–1238 (2010)
5. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of International Conference on Computers, Systems and Signal Processing, New York, pp. 175–179 (1984)
6. Izydorczyk, J., Izydorczyk, M.: Microprocessor scaling: What limits will hold? IEEE Computer 43(8), 20–26 (2010)
7. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74, 145–195 (2002)
8. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. 69, 2881–2884 (1992)
9. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A 71(4), 044305 (2005)
10. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70, 1895–1899 (1993)
11. Stinson, D.R.: Cryptography: Theory and Practice, 2nd edn. Chapman & Hall/CRC (2002)

12. Long, G.L., Deng, F.G., Wang, C., Li, X.H., Wen, K., Wang, W.Y.: Quantum secure direct communication and deterministic secure quantum communication. Front. Phys. China 2(3), 251–272 (2007)
13. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89(18), 187902 (2002)
14. Ostermeyer, M., Walenta, N.: On the implementation of a deterministic secure coding protocol using polarization entangled photons. Opt. Commun. 281(17), 4540–4544 (2008)
15. Vasiliu, E.V.: Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits. Quantum Inf. Process. 10, 189–202 (2011)
16. Zawadzki, P.: Security of ping-pong protocol based on pairs of completely entangled qudits. Quantum Inf. Process. 11(6), 1419–1430 (2012)
17. Wójcik, A.: Eavesdropping on the ping-pong quantum communication protocol. Phys. Rev. Lett. 90(15), 157901 (2003)
18. Zhang, Z., Man, Z., Li, Y.: Improving Wójcik's eavesdropping attack on the ping-pong protocol. Phys. Lett. A 333, 46–50 (2004)
19. Zawadzki, P.: The Ping-Pong protocol with a prior privacy amplification. Int. J. Quant. Inf. 10(3), 1250032 (2012)
20. Peres, A.: How to differentiate between non-orthogonal states. Phys. Lett. A 128(1-2), 19 (1988)
21. Herzog, U.: Optimal state discrimination with a fixed rate of inconclusive results: analytical solutions and relation to state discrimination with a fixed error rate. Phys. Rev. A 86, 032314 (2012)
22. Herzog, U., Bergou, J.A.: Distinguishing mixed quantum states: Minimum-error discrimination versus optimum unambiguous discrimination. Phys. Rev. A 70, 022302 (2004)
23. Miszczak, J.A.: Singular value decomposition and matrix reorderings in quantum information theory. Int. J. Mod. Phys. C 22(9), 897–918 (2011)
24. Fuchs, C.A., van de Graaf, J.: Cryptographic distinguishability measures for quantum-mechanical states. IEEE Trans. Inform. Theor. (4), 1216–1227 (1999)