Ping-Pong Protocol Strengthening against Pavičić's Attack

Piotr Zawadzki

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

Abstract. A quantum circuit providing an undetectable eavesdropping of information encoded by bit flip operations in Ping-Pong protocol has been recently proposed by Pavičić [Phys. Rev. A, vol. 87, pp. 042326, 2013]. A modification of the protocol's control mode is proposed. The introduced improvement remedies deficiencies of the protocol seminal version and permits Pavičić's attack detection with overwhelming probability. The improved version is also immune to famous Wójcik's attack [Phys. Rev. Lett., vol. 90, pp. 157901, 2003]. As a result, the Ping-Pong protocol asymptotic security is restored both in perfect and lossy quantum channels.

Keywords: Ping-Pong protocol, quantum direct communication, quantum cryptography.

1 Introduction

Division of Telecommunication, a part of the Institute of Electronics and Faculty of Automatic Control, Electronics and Computer Science of Silesian University of Technology, for many years has been conducting research on advanced fields of telecommunication engineering [1–5]. Recently, it has been involved in investigation of quantum features of physical systems which can enhance our abilities to compute and communicate. Non-locality and entanglement, the most prominent signatures of non-classicality, form a foundation for developing a new computation technology which exceeds classical limits [6–9] and construction of novel cryptographic tools [10]. Quantum Key Distribution (QKD) protocols provide distribution of unconditionally secure random keys [10] which are subsequently used to protect classical telecommunication links with methods known from classic cryptography. In contrary, Quantum Direct Communication (QDC) protocols do not require prior key agreement and their security directly results from the laws of quantum mechanics [11].

The so called Ping-Pong [12] protocol has attracted a lot of attention as it is asymptotically secure in lossless channels [13]. The protocol has been recently reformulated to higher dimensional systems [14, 15] and security characteristics throughly analyzed [16, 17]. Also a proper joint usage of Ping-Pong protocol

A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2014, CCIS 431, pp. 205–212, 2014.

with primitives well known from classic cryptography can further improve its security [18, 19]. 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 [20]. 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. However, 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 using quantum circuit proposed by Wójcik [21]. Moreover, Pavičić proposed a quantum circuit capable to eavesdrop in undetectable manner also in lossless channels the information encoded via bit flipping [22]. In such situation quantum advantage of superdense coding is suppressed [23] and legitimate parties have to resort to phase flip encoding.

An improvement of the control mode is introduced and analyzed in the following paper. The proposal remedies diffidences of the seminal version which were exploited in the Wójcik's and Pavičić's attacks. Similar techniques for Ping-Pong protocol security improvement have been also proposed in [15, 24] but the attacks based on exploiting vacuum state properties were not addressed therein. The proposed countermeasures are also much simpler than the ones proposed in [17].

The paper is organized as follows. In Section 2 we review basic concepts of Pavičić's attack. In Section 3 a modification of the Ping-Pong protocol is proposed. It is also explained why it permits detection of the aforementioned attacks. Some general remarks are subject of the conclusion from Section 4.

2 Pavičić's Attack Summary

The Pavičić's attack applies to the Ping-Pong protocol variant in which communicating parties take the quantum advantage of superdense coding and transmit two classic bits per qubit transfer. The communication process is started by Bob, the recipient of information, who prepares two maximally entangled qubits. Without loss of generality it may be assumed that this is an Einstein-Podolsky-Rosen (EPR) pair

$$|\psi^-\rangle = \left(|0_t\rangle|1_h\rangle - |1_t\rangle|0_h\rangle\right)/\sqrt{2}\ . \tag{1}$$

One of the qubits, denoted as "home", is kept confidential, while the the second one, named the "travel", is sent to Alice via unprotected quantum channel. Alice randomly selects message or control mode. In message mode Alice sends information to Bob, while in control mode communicating parties check for the presence of the eavesdropper. In a former case she encodes a pair of classic bits by the application of one of Pauli operators $\mathcal{Z}$, $\mathcal{X}$, $i\mathcal{Y} = \mathcal{Z}\mathcal{X}$ or identity $\mathcal{I}$ to the received travel qubit. The entanglement of qubits causes that Alice's local operation causes non local effects. The state composed from the home and travel qubits is transformed into another EPR pair

$$\begin{aligned} \mathcal{Z}|\psi^-\rangle = |\psi^+\rangle &= (|0_t\rangle|1_h\rangle + |1_t\rangle|0_h\rangle)/\sqrt{2} \ , \\ \mathcal{X}|\psi^-\rangle = |\phi^-\rangle &= (|0_t\rangle|0_h\rangle - |1_t\rangle|1_h\rangle)/\sqrt{2} \ , \\ \mathcal{Z}\mathcal{X}|\psi^-\rangle = |\phi^+\rangle &= (|0_t\rangle|0_h\rangle + |1_t\rangle|1_h\rangle)/\sqrt{2} \end{aligned} \tag{2}$$

or left unchanged. In general, any set of four unitary transformations can be used for encoding as long as they are build around two complementary operators to fully explore the quantum advantage of superdense coding [23]. Next, the travel qubit is sent back to Bob, who performs collective measurement on both qubits. There exists one-to-one correspondence between encoded bits and the state detected by Bob, so Bob can decode information sent by Alice.

Alice switches to the control mode in some randomly selected protocol cycles. In this mode she measures the received travel qubit and the fact of switching is announced via public authenticated classic channel. This is equivalent to the assumption that classic information is available to Eve, but she cannot control its content. Bob subsequently measures the home qubit and reveals the value of measurement outcome. The result of Bob's measurement is fully determined by the value obtained by Alice because of the fragile entanglement of the EPR pair. Any deviation from that correlation indicates the presence of Eve.

Pavičić's has proposed the usage of quantum circuit shown on Fig. 1 for Ping-Pong protocol eavesdropping [22]. The circuit operates on three registers. Register "t" denotes travel qubit on its way forth and back between Alice and Bob. Registers "x" and "y" represent ancilla system controlled by Eve. The action of the circuit is described by the equation

$$\begin{aligned} \mathcal{Q} = &(\mathcal{I}_t \otimes \mathcal{H}_x \otimes \mathcal{H}_y)\ (\mathcal{CNOT}_{tx} \otimes \mathcal{I}_y)\,(\mathcal{CNOT}_{ty} \otimes \mathcal{I}_x) \times \\ &\times (\mathcal{I}_t \otimes \mathcal{PBS}_{xy})\ (\mathcal{CNOT}_{tx} \otimes \mathcal{I}_y)\,(\mathcal{CNOT}_{ty} \otimes \mathcal{I}_x) \ . \end{aligned} \tag{3}$$

The schematic illustration of the eavesdropping scenario is shown on Fig. 2. Please note that circuit is unitary thus $\mathcal{Q}^\dagger = \mathcal{Q}^{-1}$.

Let us consider in more details the action of the circuit under consideration. Initially Alice and Bob are decoupled from the ancilla. Eve leaves the register "x" empty and sets register "y" to $|0_y\rangle$. Thus the initial state of entire system (protocol's qubits plus ancilla) reads

$$|q_0\rangle = |\psi^-_{ht}\rangle|v_x\rangle|0_y\rangle \tag{4}$$

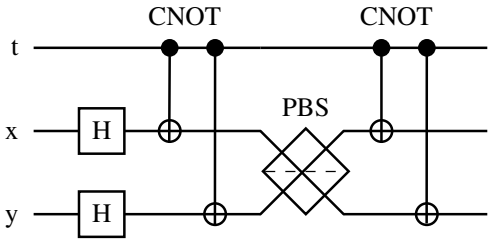

Fig. 1. Circuit proposed by Pavičić in [22] for Ping-Pong protocol eavesdropping

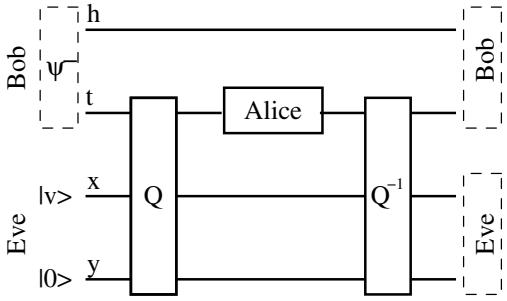

Fig. 2. Schematic illustration of the eavesdropping scenario (Q denotes device from Fig. 1)

where $|v\rangle$ denotes vacuum state. Taking into account (3) one can easily verify that system state when travel qubit arrives at Alice end is described by the expression

$$|q_A\rangle = \mathcal{Q}|q_0\rangle = |0_h\rangle|1_t\rangle\frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle}{2} - |1_h\rangle|0_t\rangle\frac{|0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle}{2} \quad . \tag{5}$$

The special attention is required in analysis of the Polarization Beam Splitter (PBS). It is assumed that state $|1\rangle$ is reflected and $|0\rangle$ transmitted

$$\begin{aligned}
\mathcal{PBS}_{xy}|v_x\rangle|0_y\rangle &= |0_x\rangle|v_y\rangle \ , \\
\mathcal{PBS}_{xy}|v_x\rangle|1_y\rangle &= |v_x\rangle|1_y\rangle \ , \\
\mathcal{PBS}_{xy}|0_x\rangle|v_y\rangle &= |v_x\rangle|0_y\rangle \ , \\
\mathcal{PBS}_{xy}|1_x\rangle|v_y\rangle &= |1_x\rangle|v_y\rangle \ .
\end{aligned} \tag{6}$$

It is equivalent to the assumption that $|1\rangle$ is encoded as photons with vertical polarization and $|0\rangle$ as horizontally polarized ones.

If Alice selects control mode then she measures travel qubit in computational basis. It is clear that (5) preserves anticorrelation required for successful protocol execution. As a result, Alice and Bob do not detect the presence of Eve's circuit.

If Alice decides to encode information then she does nothing or she applies one of the encoding operations (2). Application of $\mathcal{X}$ is equivalent to bit flipping of the travel qubit, while application of $\mathcal{Z}$ changes the relative phase of the travel and home qubits. The travel qubit is sent back to Bob. It enters again Eve's circuit, but this time it travels in opposite direction. If Alice applies no transformation then the system returns to initial state because $\mathcal{Q}^\dagger\mathcal{I}\mathcal{Q} = \mathcal{I}$

$$\mathcal{Q}^\dagger\mathcal{I}\mathcal{Q}|q_0\rangle = |\psi^-_{ht}\rangle|v_x\rangle|0_y\rangle \ . \tag{7}$$

Similarly, one can find system states after application of phase flip or bit flip operations

$$\mathcal{Q}^\dagger\mathcal{Z}\mathcal{Q}|q_0\rangle = |\psi^+_{ht}\rangle|v_x\rangle|0_y\rangle \ , \tag{8}$$

$$\mathcal{Q}^\dagger \mathcal{X} \mathcal{Q} |q_0\rangle = |\phi_{ht}^-\rangle |0_x\rangle |v_y\rangle \ , \tag{9}$$

$$\mathcal{Q}^\dagger \mathcal{Z} \mathcal{X} \mathcal{Q} |q_0\rangle = |\phi_{ht}^+\rangle |0_x\rangle |v_y\rangle \ . \tag{10}$$

It follows that Eve observes click in "x" register when $\mathcal{X}$ has been used in encoding or click in "y" register otherwise. Moreover, in each case, travel and home qubits are decoupled from Eve's ancilla. As a consequence, the presence of circuit is not detected by the control mode and introduces no errors in message mode.

3 Control Mode Improvement

A control mode improvement which removes above mentioned deficiency is presented in this section. Let us closely analyze expression (5) on system's global state at Alice end. It is clear that classic correlation of measurements' outcomes is preserved. But pairs $|0_t\rangle|1_h\rangle$ and $|1_t\rangle|0_h\rangle$ has lost their coherence as a result of Eve eavesdropping. Fortunately, coherence preservation can be checked with local measurements executed in mutually unbiased bases. Let us take into account dual basis

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \ , \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \ . \tag{11}$$

We have

$$|0_h\rangle|1_t\rangle = \frac{1}{2}\left[|+_h\rangle|+_t\rangle - |+_h\rangle|-_t\rangle + |-_h\rangle|+_t\rangle - |-_h\rangle|-_t\rangle\right] \ , \tag{12}$$

$$|1_h\rangle|0_t\rangle = \frac{1}{2}\left[|+_h\rangle|+_t\rangle + |+_h\rangle|-_t\rangle - |-_h\rangle|+_t\rangle - |-_h\rangle|-_t\rangle\right] \ , \tag{13}$$

and

$$|\psi^-\rangle = \left(|0_t\rangle|1_h\rangle - |1_t\rangle|0_h\rangle\right)/\sqrt{2} = \left(|-_t\rangle|+_h\rangle - |+_t\rangle|-_h\rangle\right)/\sqrt{2} \ . \tag{14}$$

It follows that anticorrelation between Alice's and Bob's measurements outcomes is preserved also in case of control mode executed in dual basis as long there is no eavesdropping. Let us investigate state (5) behavior under basis change

$$\begin{aligned} |q_A\rangle = {} & |+_h\rangle|+_t\rangle \frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle - |0_x\rangle|v_y\rangle - |v_x\rangle|1_y\rangle}{4} - \\ & - |+_h\rangle|-_t\rangle \frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle + |0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle}{4} + \\ & + |-_h\rangle|+_t\rangle \frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle + |0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle}{4} - \\ & - |-_h\rangle|-_t\rangle \frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle - |0_x\rangle|v_y\rangle - |v_x\rangle|1_y\rangle}{4} \ . \end{aligned} \tag{15}$$

It is clear that control measurement of travel qubit resulting in value "+1" (projection $|+_t\rangle\langle+_t|$) will induce home qubit collapse to states $|\pm_h\rangle$ with equal probability. In effect, Alice and Bob observe 50 % error rate in control mode executed in dual basis when travel qubit passes through eavesdropping circuit. Thus to detect eavesdropping Alice should interleave control measurements executed in

computational basis with the ones performed in the dual basis. As a result, the presence of eavesdropping circuit is detected with 25 % probability, what restores Ping-Pong protocol asymptotic security. The single cycle of the modified version of the Ping-Pong protocol is described by the following steps.

1. Bob creates an EPR pair $|\psi^-\rangle$ and sends one of its qubits to Alice.
2. Alice with some probability selects control mode or otherwise continues in message mode. If control mode is selected she goes to point 5.
3. Alice encodes information using one of unitary transformations (2) and then she sends signal qubit back to Bob.
4. Bob makes collective measurement on both qubits to identify encoding operation. This finishes message mode cycle.
5. Alice randomly selects computational or dual basis and measures received qubit in the selected basis.
6. She announces to Bob that control mode is activated and measurement basis.
7. Bob measures home qubit in a basis imposed by Alice and returns the outcome to Alice.
8. Alice checks for anticorrelation. This finishes control mode cycle.

The measurement basis selection in point 5 is the only postulated modification compared to the seminal version of the protocol.

The proposed improvement also permits detection of Wójcik's attack [21]. In this attack eavesdropper is able to detect phase flip encoding at the price of losses observed by Alice and Bob. Expression (16) describes the system state (legitimate qubits plus ancilla) when the travel qubit reaches Alice and Eve's eavesdropping circuit is enabled [21, Equation (4)]

$$|q_A\rangle = \frac{1}{2}|0_h\rangle|v_t\rangle|1_x\rangle|0_y\rangle + \frac{1}{2}|1_h\rangle|v_t\rangle|0_x\rangle|1_y\rangle + \\ + \frac{1}{2}|0_h\rangle|1_t\rangle|1_x\rangle|v_y\rangle + \frac{1}{2}|1_h\rangle|0_t\rangle|0_x\rangle|v_y\rangle \ . \tag{16}$$

The first two terms are responsible for losses observed by Alice, while the last two preserve the correlation of outcomes of control measurements although home and travel qubits are coupled with the ancilla registers. However, after transformation to dual basis the above expression takes the form

$$\begin{aligned} |q_A\rangle = {} & \tfrac{1}{2\sqrt{2}}\left(|+_h\rangle + |-_h\rangle\right)|v_t\rangle|1_x\rangle|0_y\rangle + \tfrac{1}{2\sqrt{2}}\left(|+_h\rangle - |-_h\rangle\right)|v_t\rangle|0_x\rangle|1_y\rangle + \\ & + \tfrac{1}{4}|+_h\rangle|+_t\rangle\left(|1_x\rangle|v_y\rangle + |0_x\rangle|v_y\rangle\right) + \\ & + \tfrac{1}{4}|+_h\rangle|-_t\rangle\left(-|1_x\rangle|v_y\rangle + |0_x\rangle|v_y\rangle\right) + \\ & + \tfrac{1}{4}|-_h\rangle|+_t\rangle\left(|1_x\rangle|v_y\rangle - |0_x\rangle|v_y\rangle\right) + \\ & + \tfrac{1}{4}|-_h\rangle|-_t\rangle\left(-|1_x\rangle|v_y\rangle - |0_x\rangle|v_y\rangle\right) \ . \end{aligned} \tag{17}$$

It follows, that the home qubit collapses to states $|+_h\rangle$ and $|-_h\rangle$ with equal probability independent on the outcome of the measurement in dual basis of a nonempty travel qubit. Thus similarly to the previous case, Alice and Bob will observe 50 % error rate in control modes executed in dual basis.

4 Conclusion

It has been shown that simple modification of the control mode make the Ping-Pong protocol immune to attacks which have been so far recognized as undetectable. Those attacks exploited the fact, that control mode in seminal version of the protocol does not detect coherence loss between travel and home qubits. Fortunately, decoherence can be detected when local projective measurements of entangled subsystems are conducted in mutually unbiased bases. The proposed modification is a direct consequence of this observation.

References

1. Kłosowski, P.: Speech processing application based on phonetics and phonology of the Polish language. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2010. CCIS, vol. 79, pp. 236–244. Springer, Heidelberg (2010)
2. Kucharczyk, M.: Blind signatures in electronic voting systems. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2010. CCIS, vol. 79, pp. 349–358. Springer, Heidelberg (2010)
3. Sułek, W.: Pipeline processing in low-density parity-check codes hardware decoder. B. Pol. Acad. Sci.-Tech. 59(2), 149–155 (2011)
4. Dustor, A., Kłosowski, P.: Biometric voice identification based on fuzzy kernel classifier. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2013. CCIS, vol. 370, pp. 456–465. Springer, Heidelberg (2013)
5. Dziwoki, G., Kucharczyk, M., Sulek, W.: OFDM transmission with non-binary LDPC coding in wireless networks. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2013. CCIS, vol. 370, pp. 222–231. Springer, Heidelberg (2013)
6. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997)
7. Zawadzki, P.: A numerical simulation of quantum factorization success probability. In: Tkacz, E., Kapczynski, A. (eds.) Internet – Technical Development and Applications. AISC, vol. 64, pp. 223–231. Springer, Heidelberg (2009)
8. Zawadzki, P.: A fine estimate of quantum factorization success probability. Int. J. Quantum Inf. 8(8), 1233–1238 (2010)
9. Izydorczyk, J., Izydorczyk, M.: Microprocessor scaling: What limits will hold? IEEE Computer 43(8), 20–26 (2010)
10. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74, 145–195 (2002)
11. 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)
12. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89(18), 187902 (2002)
13. Boström, K., Felbinger, T.: On the security of the ping-pong protocol. Phys. Lett. A 372(22), 3953–3956 (2008)
14. Vasiliu, E.V.: Non-coherent attack on the Ping-Pong protocol with completely entangled pairs of qutrits. Quantum Inf. Process. 10, 189–202 (2011)
15. Zawadzki, P.: Security of Ping-Pong protocol based on pairs of completely entangled qudits. Quantum Inf. Process. 11(6), 1419–1430 (2012)

16. Jahanshahi, S., Bahrampour, A., Zandi, M.H.: Security enhanced direct quantum communication with higher bit-rate. Int. J. Quantum Inf. 11(2), 1350020 (2013)
17. Jahanshahi, S., Bahrampour, A., Zandi, M.H.: Three-particle deterministic secure and high bit-rate direct quantum communication protocol. Quantum Inf. Process. 12(7), 2441–2451 (2013)
18. Zawadzki, P.: Improving security of the Ping-Pong protocol. Quantum Inf. Process. 12(1), 149–155 (2013)
19. Zawadzki, P.: The Ping-Pong protocol with a prior privacy amplification. Int. J. Quantum Inf. 10(3), 1250032 (2012)
20. Ostermeyer, M., Walenta, N.: On the implementation of a deterministic secure coding protocol using polarization entangled photons. Opt. Commun. 281(17), 4540–4544 (2008)
21. Wójcik, A.: Eavesdropping on the Ping-Pong quantum communication protocol. Phys. Rev. Lett. 90(15), 157901 (2003)
22. Pavičić, M.: In quantum direct communication an undetectable eavesdropper can always tell ψ from ϕ Bell states in the message mode. Phys. Rev. A 87, 042326 (2013)
23. Coles, P.J.: Role of complementarity in superdense coding. Phys. Rev. A 88, 062317 (2013)
24. Zawadzki, P., Puchała, Z., Miszczak, J.: Increasing the security of the Ping-Pong protocol by using many mutually unbiased bases. Quantum Inf. Process. 12(1), 569–575 (2013)