Ping-Pong Protocol Eavesdropping in Almost Perfect Channels

Piotr Zawadzki(✉)

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

Abstract. An undetectable eavesdropping of the entanglement based quantum direct communication in lossy quantum channels has already been demonstrated by Zhang et al. (Phys Lett A 333(12):46–50, 2004). The circuit proposed therein induces losses at a constant 25 % rate. Skipping of some protocol cycles is advised in situations when the induced loss rate is too high. However, such policy leads to a reduction in information gain proportional to the number of skipped cycles.

The entangling transformation, parametrized by the induced loss ratio, is proposed. The new method permits fine-tuning of the loss ratio by a modification of coupling coefficients. The proposed method significantly improves efficiency of the attack operated in the low loss regime. The other properties of the attack remain the same.

Keywords: Ping-pong protocol · Quantum direct communication

1 Introduction

The ping-pong protocol [1] aims to provide confidentiality without encryption. It has been proven that it is asymptotically secure in lossless channels [2–6]. Unfortunately, the existence of the losses is a rule in a quantum world and their exclusion from the analysis is an oversimplification. Zhang et al. [7] presented a circuit than permits successful eavesdropping of 0.311 bits per protocol cycle at the price of loosing one quarter of control photons. The attack targets the only practical implementation [8] of the protocol, so its further analysis and deeper understanding is scientifically justified.

To exemplify the power of the attack, it is frequently argued that the existing quantum channel can be replaced with a better one to mask the presence of the circuit. Although in practice this is usually not the option, the attack still cannot be excluded completely. Legitimate parties usually monitor the average loss ratio of the channel and they assume some safety margin to avoid false alarms. The presence of an adversary is hidden as long as the additional losses stay below that margin, which is usually much lower than 25 % rate. The typical policy of an eavesdropper is to skip some protocol cycles to reduce induced losses. Linear reduction of average information gain with the number of skipped cycles is the price he pays.

P. Gaj et al. (Eds.): CN 2016, CCIS 608, pp. 260–268, 2016.
DOI: 10.1007/978-3-319-39207-3_23

It follows that impact of the attack on practically deployed systems is determined by its properties in the low-loss regime. The new method of an attack that outperforms known solutions in this area is proposed. It permits fine-tuning of the loss ratio by a modification of coupling coefficients of the entangling transformation. The other properties of the attack remain the same.

The paper is constructed as follows. A brief reclaim the ping-pong protocol and the analysis of the Zhang's circuit is provided in Sect. 2. An alternative entangling transformation and key results are introduced in Sect. 3. Concluding remarks are made in the last section.

2 Analysis

The message mode of the ping-pong protocol is composed of three phases: an entanglement distribution, a message encoding and its subsequent decoding. Its further description adheres to the standard cryptographic personification rules: Alice and Bob are the names of the communicating parties, the malevolent eavesdropper is referred as Eve.

Bob starts the communication process through the creation of an EPR pair

$$|\psi_{\text{init}}\rangle = |\psi^+\rangle = \left(|0_B\rangle|1_A\rangle + |1_B\rangle|0_A\rangle\right)/\sqrt{2}. \tag{1}$$

The qubits that constitute the pair are further referred to as home and travel/signal qubits, respectively. Bob sends the signal qubit to Alice. Alice applies a phase flip operator $\mathcal{Z}_\mathcal{A} = |0_A\rangle\langle 0_A| - |1_A\rangle\langle 1_A|$ to the received qubit to encode a single classic bit

$$|\psi^\nu\rangle = \mathcal{Z}_\mathcal{A}|\psi_{\text{init}}\rangle = (\mathcal{Z}_A)^\nu|\psi^+\rangle = \left((-1)^\nu|0_B\rangle|1_A\rangle + |1_B\rangle|0_A\rangle\right)/\sqrt{2}. \tag{2}$$

The signal particle is sent back to Bob, who identifies the transformation that has been applied through the measurement of both qubits (Fig. 1).

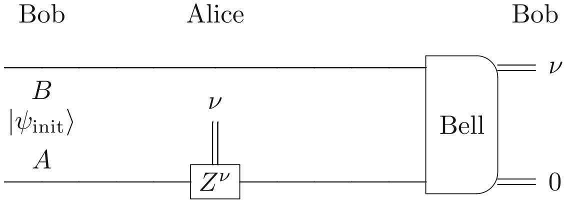

Fig. 1. The schematic diagram of a message mode in the ping-pong protocol

Unfortunately, such a communication scenario is vulnerable to the intercept-resend attack. As a countermeasure, Alice measures the received qubit in randomly selected protocol cycles and asks Bob over an authenticated classic channel to do the same with his qubit (Fig. 2). Her measurement causes the collapse of the shared state. The correlation of the outcomes is preserved only if the qubit measured by Alice is the same one that was sent by Bob. That way Alice and Bob can convince themselves with the confidence approaching certainty that the quantum channel is not spoofed provided that they have executed a sufficient number of control cycles. The above scheme is asymptotically secure in the absence of losses and/or transmission errors i.e., in a perfect quantum channel.

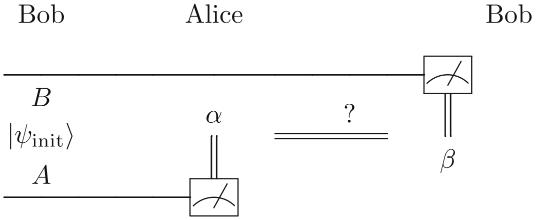

Fig. 2. The schematic diagram of a control mode in the ping-pong protocol

Further, we will consider individual (incoherent) attacks in which Eve attacks each protocol cycle independently. The signal particle travelling back and forth between Alice and Bob can be the subject of any quantum action $\mathcal{Q}$ introduced by Eve, as depicted in Fig. 3. Eve's activity can be described as a unitary operation acting on the signal qubit and two additional qubit registers, as follows from Stinespring's dilation theorem.

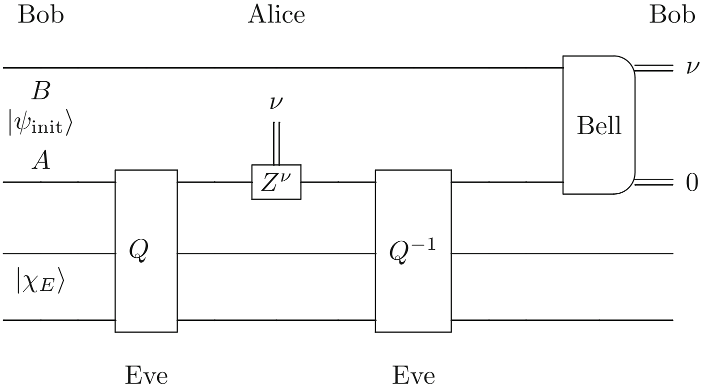

Fig. 3. A schematic diagram of an individual attack

The efficiency of the eavesdropping detection depends on the properties of the control mode. In the seminal version of the protocol, the reliability of quantum communication is estimated by the measurements in the computational basis. The probability of verification failure p_C (the specific form of the operator depends on the assumed initial state) and the probability of a non-conclusive control cycle p_L (it is assumed that Bob's qubit is never lost) can be found as

$$\mathcal{P}_C = |0_B\rangle|0_A\rangle\langle 0_A|\langle 0_B| + |1_B\rangle|1_A\rangle\langle 1_A|\langle 1_B|, \tag{3}$$

$$\mathcal{P}_L = \mathcal{I}_B \otimes |v_A\rangle\langle v_A|, \tag{4}$$

$$p_{C,L} = \mathrm{Tr}_{x,y}\left(\left(\mathcal{P}_{C,L} \otimes \mathcal{I}_E\right)\left(\mathcal{I}_B \otimes \mathcal{Q}\right)|\psi_{\mathrm{init}}\rangle|\chi_E\rangle\right). \tag{5}$$

where $|v\rangle$ denotes vacuum state and $|\chi_E\rangle$ is the initial state of the ancilla system.

Zhang's attack [7] addresses the violation of the protocol security in the presence of losses in a quantum channel. The clever circuit permits the detection of phase flip operations at the price of introducing some losses. The expected correlation of outcomes of the conclusive measurements made in the control mode (3) is also preserved so the attack is undetectable.

The Zhang's circuit is composed of two modules [7, Eq. (2)]: the coupling unit $\mathcal{C}_{\mathrm{U}}$ followed by the selective swap $\mathcal{C}_{\mathrm{SWAP}}$ (Fig. 4). The first one entangles the signal qubit from register A with the ancilla registers x and y. The second module swaps the contents of the A and x registers exclusively for signal qubit being in state $|1_A\rangle$. If qubit in register A is equal to $|0_A\rangle$ then no swapping occurs. Both modules are build around Controlled Polarization Beam Splitter (CPBS) originally proposed by Wójcik [9].

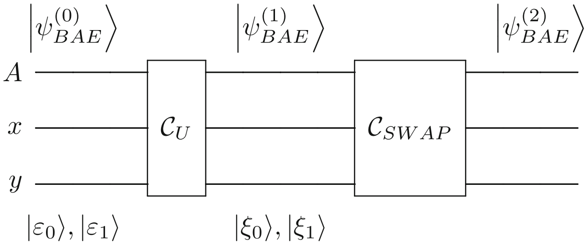
$\left|\psi^{(0)}_{BAE}\right\rangle$
$\left|\psi^{(1)}_{BAE}\right\rangle$
$\left|\psi^{(2)}_{BAE}\right\rangle$
A
x
y
$\mathcal{C}_U$
$\mathcal{C}_{SWAP}$
$|\varepsilon_0\rangle, |\varepsilon_1\rangle$
$|\xi_0\rangle, |\xi_1\rangle$

Fig. 4. The block diagram of the Zhang's circuit

Polarization Beam Splitter (PBS) is a two qubit gate which conditionally swaps the port of the input based on its value – the qubit $|0\rangle$ arriving on port x (y) appears on port y (x) of output, but the qubit set to $|1\rangle$ does not change its port. The CPBS acts as normal PBS for control qubit is set to $|0\rangle$. In the complementary situation, i.e., for the control register set to $|1\rangle$, we have the opposite behaviour: $|1\rangle$ ($|0\rangle$) is swapped (hold). The CPBS can be realized as PBS preceded and followed by double CNOT gates (Fig. 5).

The coupling module $\mathcal{C}_{\mathrm{U}}$ is realized as a circuit from Fig. 5. The quantum state of the whole system is given as

$$|\psi^{(0)}_{BAE}\rangle = |\psi_{\mathrm{init}}\rangle|\chi_E\rangle = \frac{1}{\sqrt{2}}\left(|0_B\rangle|1_A\rangle + |1_B\rangle|0_A\rangle\right)|v_x\rangle|0_y\rangle, \tag{6}$$

where it was assumed that the ancilla is initially in the state $|\chi_E\rangle = |v_x\rangle|0_y\rangle$. The $\mathcal{C}_{\mathrm{U}}$ actions are as follows

$$\mathcal{C}_{\mathrm{U}}|0_A\rangle|v_x\rangle|0_y\rangle = \frac{1}{\sqrt{2}}|0_A\rangle\left(|0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle\right) = |0_A\rangle|\alpha^+\rangle, \tag{7a}$$

$$\mathcal{C}_\mathrm{U}|0_A\rangle|v_x\rangle|1_y\rangle = \frac{1}{\sqrt{2}}|0_A\rangle\left(|0_x\rangle|v_y\rangle - |v_x\rangle|1_y\rangle\right) = |0_A\rangle|\alpha^-\rangle, \tag{7b}$$

$$\mathcal{C}_\mathrm{U}|1_A\rangle|v_x\rangle|0_y\rangle = \frac{1}{\sqrt{2}}|1_A\rangle\left(|v_x\rangle|0_y\rangle + |1_x\rangle|v_y\rangle\right) = |1_A\rangle|\beta^+\rangle, \tag{7c}$$

$$\mathcal{C}_\mathrm{U}|1_A\rangle|v_x\rangle|1_y\rangle = \frac{1}{\sqrt{2}}|1_A\rangle\left(|v_x\rangle|0_y\rangle - |1_x\rangle|v_y\rangle\right) = |1_A\rangle|\beta^-\rangle. \tag{7d}$$

so the resulting state of the system takes the form (compare with Fig. 4)

$$|\psi^{(1)}_{BAE}\rangle = \frac{1}{\sqrt{2}}\left(|1_B\rangle|0_A\rangle|\alpha^+\rangle + |0_B\rangle|1_A\rangle|\beta^+\rangle\right). \tag{8}$$

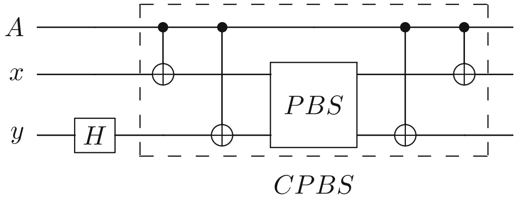

Fig. 5. The coupling circuit $\mathcal{C}_\mathrm{U}$

It enters the $\mathcal{C}_\mathrm{SWAP}$ circuit (Fig. 6) which is also build on the CPBS basis, but this time the y register serves as the control.

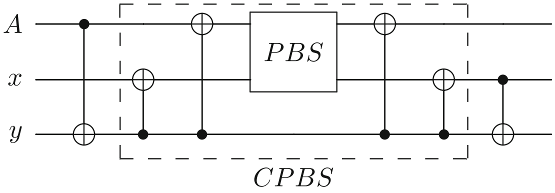

Fig. 6. The selective swap circuit $\mathcal{C}_\mathrm{SWAP}$

The circuit does nothing for signal qubit set to $|0_A\rangle$. Otherwise, i.e., for signal qubit equal to $|1_A\rangle$, it swaps the contents of A and x registers:

$$\mathcal{C}_\mathrm{SWAP}|0_A\rangle|\alpha^+\rangle = \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_x\rangle|v_y\rangle + |0_A\rangle|v_x\rangle|1_y\rangle\right) = |0_A\rangle|\alpha^+\rangle, \tag{9a}$$

$$\mathcal{C}_\mathrm{SWAP}|1_A\rangle|\beta^+\rangle = \frac{1}{\sqrt{2}}\left(|v_A\rangle|1_x\rangle|0_y\rangle + |1_A\rangle|1_x\rangle|v_y\rangle\right). \tag{9b}$$

In effect, the state of the system at Alice's end reads (see Fig. 4)

$$|\psi^{(2)}_{BAE}\rangle = \frac{1}{\sqrt{2}}|1_B\rangle|0_A\rangle|\alpha^+\rangle + \frac{1}{\sqrt{2}}|0_B\rangle\left[\frac{1}{\sqrt{2}}\left(|v_A\rangle|1_x\rangle|0_y\rangle + |1_A\rangle|1_x\rangle|v_y\rangle\right)\right]. \tag{10}$$

Her encoding affects only the term in square brackets

$$\mathcal{Z}_A^{\nu}\left(|v_A\rangle|1_x\rangle|0_y\rangle + |1_A\rangle|1_x\rangle|v_y\rangle\right) = \left(|v_A\rangle|1_x\rangle|0_y\rangle + (-1)^{\nu}|1_A\rangle|1_x\rangle|v_y\rangle\right). \tag{11}$$

The photons that "carry" encoded information and travel back to Bob are affected by $\mathcal{C}_{\mathrm{SWAP}}^{-1}$. The component with $|\alpha^+\rangle$ is not changed again but the term (11) sensitive to Alice's encoding operation is transformed to

$$\frac{1}{\sqrt{2}}|1_A\rangle\left(|v_x\rangle|0_y\rangle + (-1)^{\nu}|1_x\rangle|v_y\rangle\right) = |1_A\rangle|\beta^{\pm}\rangle. \tag{12}$$

Thus the forward and backward application of the $\mathcal{C}_{\mathrm{SWAP}}$ circuit to the state (8) caused that Alice's encoding is effectively applied to the x register. The states visible at this cross-section after applied encoding read (Fig. 4)

$$\nu = 0 \qquad |\xi_0\rangle = \frac{1}{\sqrt{2}}\big(|1_B\rangle|0_A\rangle|\alpha^+\rangle + |0_B\rangle|1_A\rangle|\beta^+\rangle\big), \tag{13a}$$

$$\nu = 1 \qquad |\xi_1\rangle = \frac{1}{\sqrt{2}}\big(|1_B\rangle|0_A\rangle|\alpha^+\rangle + |0_B\rangle|1_A\rangle|\beta^-\rangle\big), \tag{13b}$$

where $|\beta^{\pm}\rangle = (|v_x\rangle|0_y\rangle \pm |1_x\rangle|v_y\rangle)$. These states are transformed by the $\mathcal{C}_{\mathrm{U}}^{-1}$ to

$$|\varepsilon_0\rangle = \mathcal{C}_{\mathrm{U}}^{-1}|\xi_0\rangle = \frac{1}{\sqrt{2}}\left(|1_B\rangle|0_A\rangle|v_x\rangle|0_y\rangle + |0_B\rangle|1_A\rangle|v_x\rangle|0_y\rangle\right), \tag{14a}$$

$$|\varepsilon_1\rangle = \mathcal{C}_{\mathrm{U}}^{-1}|\xi_1\rangle = \frac{1}{\sqrt{2}}\left(|1_B\rangle|0_A\rangle|v_x\rangle|0_y\rangle + |0_B\rangle|1_A\rangle|v_x\rangle|1_y\rangle\right), \tag{14b}$$

where expressions (7) have been taken into account. Eve has to discriminate between states

$$\rho_0 = \mathrm{Tr}_{BA}\left(|\varepsilon_0\rangle\langle\varepsilon_0|\right) = |v_x\rangle|0_y\rangle\langle v_x|\langle 0_y|, \tag{15}$$

$$\rho_1 = \mathrm{Tr}_{BA}\left(|\varepsilon_1\rangle\langle\varepsilon_1|\right) = \frac{1}{2}|v_x\rangle|0_y\rangle\langle v_x|\langle 0_y| + \frac{1}{2}|v_x\rangle|1_y\rangle\langle v_x|\langle 1_y|. \tag{16}$$

The information she can draw is limited by the Holevo bound [10]

$$I_{AE} = S\left(\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1\right) - \frac{1}{2}S\left(\rho_0\right) - \frac{1}{2}S\left(\rho_1\right) \tag{17}$$

where $S\left(\cdot\right)$ denotes von Neumann entropy. The straightforward analysis shows that Eve's information gain is equal to $I_{AE} = 0.311$ bits per single message mode cycle. However, the information is intercepted at the price of an induction of a 25 % loss rate in the control mode (10). As long as legitimate parties accept losses above that threshold, the quantum channel can be in theory replaced with a perfect one and the attack can be applied without modification. But the replacement of the quantum channel is impossible in typical real-life scenarios. Moreover, the communicating parties monitor the average losses occurring in the link they use and any abrupt change and/or excess value can trigger an alarm.

However, to avoid false alarms, the estimation procedure cannot be exact and some safety margin have to be assumed. This opens a gap for mounting the attack as long as the induced losses are below that margin. It is advised that Eve should skip some protocol cycles to keep average induced losses below the required threshold. But this decreases her information gain proportionally to the number of omitted cycles. Further, it is shown that such a policy is not optimal. The entangling transformation that provides fine-tuning of the induced loss rate via the control of the coupling coefficients, is proposed. It provides better results than a linear decrease in information gain while reducing losses. The proposed enhancement can be considered as the generalization of the Zhang's attack.

3 Results

The map (7) that defines coupling of the signal qubit with the ancilla has straightforward generalization

$$\mathcal{W}|0_A\rangle|v_x\rangle|0_y\rangle = |0_A\rangle\left(a|0_x\rangle|v_y\rangle + f|v_x\rangle|1_y\rangle\right) = |0_A\rangle|\alpha^+\rangle, \tag{18}$$
$$\mathcal{W}|1_A\rangle|v_x\rangle|0_y\rangle = |1_A\rangle\left(a|1_x\rangle|v_y\rangle + f|v_x\rangle|0_y\rangle\right) = |1_A\rangle|\beta^+\rangle, \tag{19}$$

where $|a|^2 + |f|^2 = 1$. The transformation $\mathcal{W}$ is unitary when

$$\mathcal{W}|0_A\rangle|v_x\rangle|1_y\rangle = |0_A\rangle\left(f|0_x\rangle|v_y\rangle - a|v_x\rangle|1_y\rangle\right) = |0_A\rangle|\alpha^-\rangle, \tag{20}$$
$$\mathcal{W}|1_A\rangle|v_x\rangle|1_y\rangle = |1_A\rangle\left(f|1_x\rangle|v_y\rangle - a|v_x\rangle|0_y\rangle\right) = |1_A\rangle|\beta^-\rangle, \tag{21}$$

$fa^* = f^*a$ and

$$\mathcal{W}|0_A\rangle|0_x\rangle|v_y\rangle = |0_A\rangle|v_x\rangle|0_y\rangle, \qquad \mathcal{W}|0_A\rangle|1_x\rangle|v_y\rangle = |0_A\rangle|1_x\rangle|v_y\rangle, \tag{22}$$
$$\mathcal{W}|1_A\rangle|0_x\rangle|v_y\rangle = |1_A\rangle|0_x\rangle|v_y\rangle, \qquad \mathcal{W}|1_A\rangle|1_x\rangle|v_y\rangle = |1_A\rangle|v_x\rangle|1_y\rangle. \tag{23}$$

The state (10) used for control measurements then takes the form

$$|\psi^{(1)}_{BAE}\rangle = \frac{1}{\sqrt{2}}|1_B\rangle|0_A\rangle|\alpha^+\rangle + \frac{1}{\sqrt{2}}|0_B\rangle\left(f|v_A\rangle|1_x\rangle|0_y\rangle + a|1_A\rangle|1_x\rangle|v_y\rangle\right). \tag{24}$$

The average loss rate observed in control measurements is related to coefficient f as

$$p_L = \frac{1}{2}|f|^2 \tag{25}$$

and Eve is now able to fine-tune induced losses by an appropriate selection of this coupling parameter. However, the above capability does not come without a price. Alice's encoding is still effectively applied to the x register when the system state is observed at the $\mathcal{C}_{\mathrm{SWAP}}$-$\mathcal{C}_{\mathrm{U}}$ cross-section. But this time information encoding does not transform $|\beta^+\rangle$ into $|\beta^-\rangle$ as in (13) but instead into the state

$$|\beta^z\rangle = \left(-a|1_x\rangle|v_y\rangle + f|v_x\rangle|0_y\rangle\right). \tag{26}$$

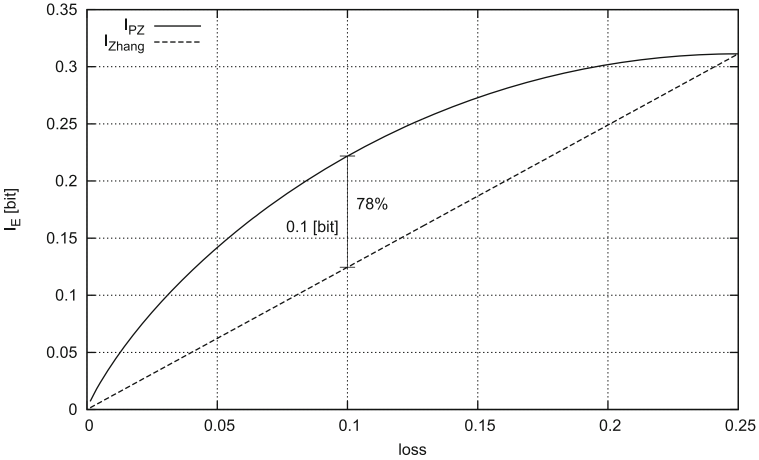

Fig. 7. Eve's information gain as a function of the average loss rate

so the information-encoded states take the form

$$\nu = 0 \qquad |\xi_0\rangle = \frac{1}{\sqrt{2}}\left(|1_B\rangle|0_A\rangle|\alpha^+\rangle + |0_B\rangle|1_A\rangle|\beta^+\rangle\right), \tag{27a}$$

$$\nu = 1 \qquad |\xi_1\rangle = \frac{1}{\sqrt{2}}\left(|1_B\rangle|0_A\rangle|\alpha^+\rangle + |0_B\rangle|1_A\rangle|\beta^z\rangle\right), \tag{27b}$$

Consequently, disentangling $\mathcal{W}^{-1} = \mathcal{W}^\dagger$ leads to states

$$|\varepsilon_0\rangle = \mathcal{W}^\dagger|\xi_0\rangle = \frac{1}{\sqrt{2}}\left(|1_B\rangle|0_A\rangle|v_x\rangle|0_y\rangle + |0_B\rangle|1_A\rangle|v_x\rangle|0_y\rangle\right), \tag{28a}$$

$$|\varepsilon_1\rangle = \mathcal{W}^\dagger|\xi_1\rangle, \tag{28b}$$

and Eve's information gain is determined by the distinguishability of states

$$\rho_0 = \mathrm{Tr}_{BA}\left(|\varepsilon_0\rangle\langle\varepsilon_0|\right) = |v_x\rangle|0_y\rangle\langle v_x|\langle 0_y|, \tag{29}$$

$$\rho_1 = \mathrm{Tr}_{BA}\left(\mathcal{W}^\dagger|\varepsilon_1\rangle\langle\varepsilon_1|\mathcal{W}\right). \tag{30}$$

Figure 7 presents Eve's information gain for the two policies of total induced loss reduction. A key "Zhang" denotes the information gain when the losses are reduced by the plain skipping of protocol cycles. The curve marked as "PZ" illustrates the same quantity computed with the introduced technique and obtained for real-valued coefficient f. The improvement $\Delta I = I_{\mathrm{PZ}} - I_{\mathrm{Zhang}}$ expressed in bits does not first appear to be impressive as it does not exceed $\Delta I_{\max} = 0.1$ bit. However, the ratio of the additional eavesdropped information to the one received with the traditional technique better exhibits the strength of the contribution. As the graph illustrates, the new way of eavesdropping can be almost 80 % better than methods proposed so far. The other features of the new method remain unchanged compared to Zhang's method. Numerical simulations have shown that maximal information gain is obtained for $a = f = 1/\sqrt{2}$ i.e., for values hard encoded in Zhang's circuit. At the same time, the maximal loss ratio is observed for these coupling constants.

4 Conclusion

The entangling transformation, parametrized by the induced loss ratio, is proposed. In the new method, the eavesdropper's information gain exceeds values offered by other methods. The other key properties of the attack remain the same. The proposed method significantly improves efficiency when attack is operated in low loss regime. It follows, that instead of skipping some protocol cycles, a better policy based on the modification of the entangling transformation parameters should be used to fine tune induced losses.

Acknowledgement. Author acknowledges the support by the Polish Ministry of Science and Higher Education under research project 8686/E-367/S/2015.

References

1. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
2. Boström, K., Felbinger, T.: On the security of the ping-pong protocol. Phys. Lett. A **372**(22), 3953–3956 (2008)
3. Jahanshahi, S., Bahrampour, A., Zandi, M.H.: Security enhanced direct quantum communication with higher bit-rate. Int. J. Quantum Inf. **11**(2), 1350020 (2013)
4. Vasiliu, E.V.: Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits. Quantum Inf. Process. **10**, 189–202 (2011)
5. Zawadzki, P.: Security of ping-pong protocol based on pairs of completely entangled qudits. Quantum Inf. Process. **11**(6), 1419–1430 (2012)
6. 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)
7. Zhang, Z., Man, Z., Li, Y.: Improving wójcik's eavesdropping attack on the ping-pong protocol. Phys. Lett. A **333**(1–2), 46–50 (2004)
8. Ostermeyer, M., Walenta, N.: On the implementation of a deterministic secure coding protocol using polarization entangled photons. Opt. Commun. **281**(17), 4540–4544 (2008)
9. Wójcik, A.: Eavesdropping on the ping-pong quantum communication protocol. Phys. Rev. Lett. **90**(15), 157901 (2003)
10. Holevo, A.S.: Bounds for the quantity of information transmitted by a quantum communication channel. Probl. Inform. Transm. **9**(3), 177–183 (1973)