Quantum Inf Process (2015) 14:2589–2598
DOI 10.1007/s11128-015-0989-x

An improved control mode for the ping-pong protocol operation in imperfect quantum channels

Piotr Zawadzki[1]

Received: 16 October 2014 / Accepted: 7 April 2015 / Published online: 21 April 2015

Abstract Quantum direct communication (QDC) can bring confidentiality of sensitive information without any encryption. A ping-pong protocol, a well-known example of entanglement-based QDC, offers asymptotic security in a perfect quantum channel. However, it has been shown (Wójcik in Phys Rev Lett 90(15):157901, 2003. doi:10.1103/PhysRevLett.90.157901) that it is not secure in the presence of losses. Moreover, legitimate parities cannot rely on dense information coding due to possible undetectable eavesdropping even in the perfect setting (Pavičić in Phys Rev A 87(4):042326, 2013. doi:10.1103/PhysRevA.87.042326). We have identified the source of the above-mentioned weaknesses in the incomplete check of the EPR pair coherence. We propose an improved version of the control mode, and we discuss its relation to the already-known attacks that undermine the QDC security. It follows that the new control mode detects these attacks with high probability and independently on a quantum channel type. As a result, an asymptotic security of the QDC communication can be maintained for imperfect quantum channels, also in the regime of dense information coding.

Keywords Quantum cryptography · Quantum direct communication · Ping-pong protocol

The Author acknowledges support by the Polish National Science Centre (NCN) under the Grant Number DEC-2011/03/D/ST6/00413.

✉ Piotr Zawadzki
Piotr.Zawadzki@polsl.pl

[1] Institute of Electronics, Akademicka 16, 44-100 Gliwice, Poland

1 Introduction

An entanglement, a physical property unique to quantum systems, can bring a new dimension to communication schemes [4]. Security of such schemes results from the fundamental property that eavesdropper having an access to a part of the entangled state cannot draw deterministic conclusions about the whole system. That feature has been used as a foundation of the quantum direct communication (QDC) protocols in which, unlike the quantum key distribution (QKD) systems, sensitive information is sent directly in the quantum channel. In consequence, the confidentiality of that information results directly from the laws of physics and no classic encryption algorithm has to be applied.

The ping-pong protocol is a QDC scheme founded on the fragility of the entanglement of the EPR pairs [1]. It is composed of two, randomly interwoven, operation modes. The message mode used for sensitive information exchange is supported with the control mode in which legitimate parties using local measurements and classic communication verify whether they share components of the same EPR pair. Protocol offers the capacity of a single classic bit per message cycle and an asymptotic security in perfect quantum channels. Many enhancements of the seminal proposal or quite new schemes exploring entanglement of Bell states have been proposed since its publication [5]. The offered capacity per signal particle has been enhanced by various protocol modifications: introduction of a dense information coding [8], increase in the dimensionality of the signal particle [7,11], and usage of a multi-particle entanglement [3]. However, serious deficiencies can be identified in the ping-pong protocol and its derivatives.

1. *Perfect channel* The dense coding cannot be directly used to securely increase the capacity of the protocol. Eve can mount an undetectable attack in which she can correctly eavesdrop a half of the sent bits [8,11].
2. *Noisy channel* The asymptotic security can be attained only if legitimate parties know exactly the reliability of the error-prone channel. However, such an assumption is equally unrealistic as that of the existence of a perfect quantum channel. To cope with this problem, the protocol can be combined with an additional layer based on a careful classic information preprocessing [10,12]. The security of that layer directly depends on a QBER occurring in the message mode. However, the control mode in its present formulation does not permit to estimate a QBER as it is sensitive only to bit flip errors, while information is encoded in the relative phase of the EPR pair components [1].
3. *Lossy channel* An eavesdropper can mount an undetectable attack with a nonzero information gain at the price of induction of losses [6,9]. If legitimate parties tolerate a too high level of losses, then such an attack may be passed unnoticed. Some countermeasures have been given in [2]. However, the approach proposed therein does not address problems (1) and (2).

We have identified an incomplete check of the coherence of the shared entangled system as the source of the above weaknesses. We propose a method to overcome the aforementioned deficiencies. It is based on the observation that coherence of the distant parts of the entangled system can be verified with a nonzero probability with a

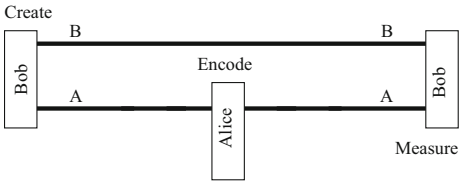

Fig. 1 A schematic diagram of a message mode in the entanglement-based QDC

scheme founded on classic communication and local measurements. In the improved protocol, legitimate parties perform control measurements in mutually unbiased bases in subsequent protocol cycles. As a result, the asymptotic security of QDC is restored because attacks mentioned in points 1) and 3) are detected with a finite probability. Also the QBER can be reliably estimated as the new control mode is sensitive to both phase flip and bit flip errors.

The following text adheres to standard cryptographic personification rules: Alice, Bob, and Eve are the names of the message sender, recipient, and malevolent eavesdropper, respectively. It explains our improved control mode and consequences of its introduction on a basis of the seminal version of the protocol [1]. Such presentation form stems from the fact that main threats have been also formulated in the context of this protocol [6,9,13]. Section 2 presents the ping-pong protocol in its seminal version and fixes notation used further. The idea of our improvement and its relation to the mentioned threats is discussed in Sect. 3. Some general remarks and conclusions sum up the paper.

2 Ping-pong protocol

A message mode of the EPR-based QDC is composed of three phases: the entanglement distribution, a message encoding, and its decoding. Bob starts the communication process by a creation of an EPR pair $|\psi^+\rangle = (|0_B\rangle|1_A\rangle + |1_B\rangle|0_A\rangle)/\sqrt{2}$. Then, he sends one of the qubits, further referred as a signal one, to Alice. An unitary transformation applied to the qubit possessed by Alice is used to encode a one classic bit μ

$$|\psi^\mu\rangle = (Z_A)^\mu|\psi^+\rangle = \left((-1)^\mu|0_B\rangle|1_A\rangle + |1_B\rangle|0_A\rangle\right)/\sqrt{2}\ . \tag{1}$$

The signal particle is sent back to Bob, who detects applied transformation by a collective measurement of both qubits (Fig. 1).

Unfortunately, such a communication scenario is vulnerable to the intercept-resend attack. As a result, legitimate parties have to implement countermeasures to make sure that the qubit processed by Alice is really the same qubit which was sent by Bob. In seminal version of the protocol, Alice measures the received qubit in a computational basis in some randomly selected protocol cycles and asks Bob over an authenticated classic channel to do the same with his qubit (Fig. 2). As the Alice's measurement comes first, it fully determines the state accessible to Bob and the result of his measurement. The parties can verify the correlation of the outcomes by a public discussion over a classic channel and a probability $p_C^{(Z)}$ of an error occurrence results from the projection

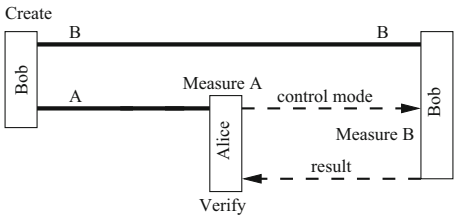

Fig. 2 A schematic diagram of a control mode in the entanglement-based QDC

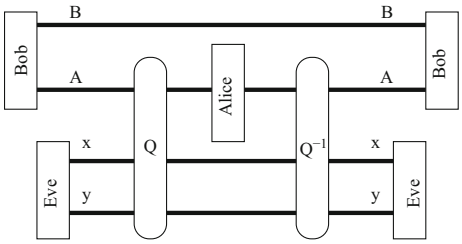

Fig. 3 A schematic diagram of an incoherent attack on the entanglement-based QDC

$$\Pi_C^{(Z)} = I_{BA} - |0_B\rangle|1_A\rangle\langle 1_A|\langle 0_B| - |1_B\rangle|0_A\rangle\langle 0_A|\langle 1_B| \ . \tag{2}$$

The above scheme is asymptotically secure in a perfect quantum channel, i.e., an eavesdropper is detected with a probability close to certainty after a sufficiently large number of control cycles. However, this feature is valid in a lossy and/or noisy channel as long as legitimate parties know exactly the loss ratio and/or quantum bit error rate. Otherwise, some information may leak out in an undetectable manner [9,13]. Moreover, Alice cannot rely on a dense coding to encode two classic bits ν, μ per protocol cycle

$$|\psi^{\nu,\mu}\rangle = (X_A)^{\nu}(Z_A)^{\mu}|\psi^{+}\rangle \ , \tag{3}$$

because of attacks described in [6,11].

Let us now summarize in more detail the security of the protocol in the presence of losses in a quantum channel. Capabilities of the eavesdropper can be then enhanced with quantum circuits which exploit properties of the vacuum state. Two attacks, which follow the scheme depicted on the Fig. 3, have been demonstrated so far [6,9]. The signal qubit in its way to Alice is entangled via the transformation Q with Eve's registers initialized to the state $|v_x\rangle|0_y\rangle$, where $|v\rangle$ denotes the vacuum state. That way, due to introduced coupling, Alice's encoding operations affect the state of x and y registers. The ancilla is next decoupled from the signal qubit on its way back to Bob. The clever design of the circuit Q permits detection of phase flip operations at the price of an introduction of some losses [9] or bit flip operations with no additional losses [6]. In both cases, the expected correlation of outcomes of conclusive measurements in the seminal control mode (2) is preserved so the aforementioned attacks are considered to be undetectable. Controlled Polarization Beam Splitter (CPBS) depicted on the Fig. 4 is a central element of both devices. It is responsible for a signal qubit coupling with the Eve's registers. The Eqs. (4) and (5)

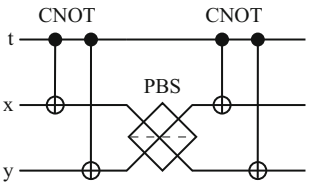

Fig. 4 Controlled polarization beam splitter

describe quantum circuits detecting phase flip or bit flip encoding operations, respectively

$$Q_{txy}^{(\text{phase})} = SWAP_{tx}CPBS_{txy}H_y \tag{4}$$

$$Q_{txy}^{(\text{bit})} = CPBS_{txy}H_xH_y \tag{5}$$

where H_α denotes the Hadamard gate applied to register α and $SWAP_{\alpha\beta}$ swaps the contents of registers α and β. In fact, these devices differ only the way in which the inputs for the $CPBS$ are prepared and the output states are collected. One should keep in mind that attacks (4) and (5) were aimed at two different flavors of the ping-pong protocol. The device (4) targets the seminal formulation of the protocol and shows that losses can be used to mask the presence of the eavesdropper. On the other hand, the device (5) demonstrates that dense coding cannot be used to increase protocol's capacity per cycle because all information encoded as bit flips of the signal particle can be eavesdropped without detection as long as the control mode is left intact.

3 Improved protocol

Security problems of the communication scenario described in the previous section come from the fact that the control mode (2) does not check the coherence of the EPR components, but only classic correlation of local measurements in the computational basis. The coherence can be checked in a deterministic way only by the collective measurement, but within the protocol definition this is not feasible as the control mode is performed by remote parties. However, remote control measurements of an EPR pair components performed in mutually unbiased bases can be used to detect the coherence loss in a probabilistic manner. Based on this observation, we propose the following amendment of the seminal control mode:

1. Alice switches into the control mode in randomly selected protocol cycles.
2. *She randomly selects a basis from a set of two mutually unbiased bases composed from the eigenvectors of Z and X operators* and measures the received qubit. The aggregated probability of the new control mode failure is now given as

$$p_C = \left(p_C^{(Z)} + p_C^{(X)}\right)/2, \tag{6}$$

where $p_C^{(X)}$ now comes from the projection

Table 1 Error detection table

Shared state	Basis	
	Z	X
$\|\psi^+\rangle$	$\|0_B 1_A\rangle + \|1_B 0_A\rangle$	$\|+_B +_A\rangle - \|-_B -_A\rangle$
No error	Anticorrelation	Correlation
$Z_A\|\psi^+\rangle = \|\psi^-\rangle$	$\|1_B 0_A\rangle - \|0_B 1_A\rangle$	$\|+_B -_A\rangle - \|-_B +_A\rangle$
Phase flip		Detected
$X_A\|\psi^+\rangle = \|\phi^+\rangle$	$\|0_B 0_A\rangle + \|1_B 1_A\rangle$	$\|+_B +_A\rangle + \|-_B -_A\rangle$
Bit flip	Detected	
$Z_A X_A\|\psi^+\rangle = \|\phi^-\rangle$	$\|0_B 0_A\rangle - \|1_B 1_A\rangle$	$\|+_B -_A\rangle + \|-_B +_A\rangle$
Phase and bit flip	Detected	Detected

$$\Pi_C^{(X)} = I_{BA} - |+_B\rangle|+_A\rangle\langle+_A|\langle+_B| - |-_B\rangle|-_A\rangle\langle-_A|\langle-_B| \tag{7}$$

where the form of $\Pi_C^{(X)}$ results from the first row of the Table 1 and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

3. The fact of the control mode selection and *the basis of the control measurement* are sent to Bob over an authenticated classic channel (Fig. 2).
4. Bob measures the possessed qubit in a basis selected by Alice. He communicates the outcome to Alice.
5. Alice verifies whether an expected correlation holds. She can also estimate the QBER in the message mode as the failures in computational basis are related to bit flip errors, while failures in dual basis are related to phase flip errors.
6. The decision on a communication termination is taken after the sufficient number of control cycles.

It follows from the Table 1 that operators (2) and (7) are sufficient to detect all types of errors. Quantities $p_C^{(Z)}$ and $p_C^{(X)}$ may be used for the QBER estimation depending on the nature of information encoding in the message mode. For instance, $p_C^{(X)}$ determines the expected QBER in the seminal version of the protocol.

Let us investigate whether the improved control mode detects devices (4) and (5). The expression (8) describes the system state (legitimate qubits plus ancilla) when the signal qubit reaches Alice and Eve's phase flip detection circuit is enabled (see [9, equation (4)])

$$\begin{aligned} |q_{\text{phase}}\rangle = &\frac{1}{2}|0_B\rangle|v_A\rangle|1_x\rangle|0_y\rangle + \frac{1}{2}|1_B\rangle|v_A\rangle|0_x\rangle|1_y\rangle \\ &+ \frac{1}{2}|0_B\rangle|1_A\rangle|1_x\rangle|v_y\rangle + \frac{1}{2}|1_B\rangle|0_A\rangle|0_x\rangle|v_y\rangle\,. \end{aligned} \tag{8}$$

The first two terms are responsible for the induction of losses observed by Alice in the control mode. The last two ones preserve the correlation of outcomes of control measurements although home and signal qubits are coupled with the ancilla registers. Similarly, the system state takes the form (9) (see [6, equation(3)])

$$|q_{\text{bit}}\rangle = \frac{1}{2}|0_B\rangle|1_A\rangle\left(|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle\right) - \frac{1}{2}|1_B\rangle|0_A\rangle\left(|0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle\right). \quad (9)$$

when the signal qubit arrives at Alice's site and the bit flip detection circuit is enabled. Also in this case, the nature of a quantum measurement guarantees that Alice's and Bob's outcomes are perfectly anticorrelated.

However, there is a big difference between the states (8) or (9) and the state of the system when Eve is decoupled

$$|q_{\text{sep}}\rangle = \left(|0_A\rangle|1_B\rangle + |1_A\rangle|0_B\rangle\right)|\chi_{x,y}\rangle/\sqrt{2}\,, \quad (10)$$

where $|\chi_{x,y}\rangle$ denotes a state of the ancilla. In the latter case, qubits A and B are in the coherent state, while in the former two cases they are not. The coherence loss can be detected with the control measurements in the dual basis. The states (8)–(10) in X basis take the form:

$$\begin{aligned}|q'_{\text{phase}}\rangle = {} & \frac{1}{2\sqrt{2}}\left(|+_B\rangle + |-_B\rangle\right)|v_A\rangle|1_x\rangle|0_y\rangle + \frac{1}{2\sqrt{2}}\left(|+_B\rangle - |-_B\rangle\right)|v_A\rangle|0_x\rangle|1_y\rangle \\ & + \frac{1}{4}|+_B\rangle|+_A\rangle\left(|1_x\rangle|v_y\rangle + |0_x\rangle|v_y\rangle\right) + \frac{1}{4}|+_B\rangle|-_A\rangle\left(-|1_x\rangle|v_y\rangle + |0_x\rangle|v_y\rangle\right) \\ & + \frac{1}{4}|-_B\rangle|+_A\rangle\left(|1_x\rangle|v_y\rangle - |0_x\rangle|v_y\rangle\right) + \frac{1}{4}|-_B\rangle|-_A\rangle\left(-|1_x\rangle|v_y\rangle - |0_x\rangle|v_y\rangle\right), \end{aligned} \quad (11)$$

$$\begin{aligned}|q'_{\text{bit}}\rangle = {} & |+_B\rangle|+_A\rangle\,\frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle - |0_x\rangle|v_y\rangle - |v_x\rangle|1_y\rangle}{4} \\ & - |+_B\rangle|-_A\rangle\,\frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle + |0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle}{4} \\ & + |-_B\rangle|+_A\rangle\,\frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle + |0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle}{4} \\ & - |-_B\rangle|-_A\rangle\,\frac{|1_x\rangle|v_y\rangle + |v_x\rangle|0_y\rangle - |0_x\rangle|v_y\rangle - |v_x\rangle|1_y\rangle}{4}\,, \end{aligned} \quad (12)$$

$$|q'_{\text{sep}}\rangle = \left(|+_A\rangle|+_B\rangle - |-_A\rangle|-_B\rangle\right)|\chi_{x,y}\rangle/\sqrt{2}\,. \quad (13)$$

In a dual basis, the (anti)correlation between Alice's and Bob's outcomes is preserved only when qubits A and B are in coherent state (13). Otherwise, i.e., when hostile circuits are enabled, the control measurement of a signal qubit resulting in value "+1" (projection $|+_A\rangle\langle+_A|$) will induce the home qubit collapse to states $|\pm_B\rangle$ with an equal probability as follows from (11) and (12). In effect, Alice and Bob observe 50 % of the error rate in the control mode executed in a dual basis for travel qubits passing through the hostile circuit. In consequence, the net probability of the Eve's presence detection is on average equal to 25 % when only successful measurements are taken into account. The above observation restores protocol's asymptotic security.

For instance, let us reconsider an attack with the device (4) and compare the eavesdropper's information gain and detection capabilities of the seminal and proposed control modes. Let the quantum channel be perfect, but legitimate users tolerate losses on the level *QLOSS*. This is the limiting case of the situation in which Eve replaces

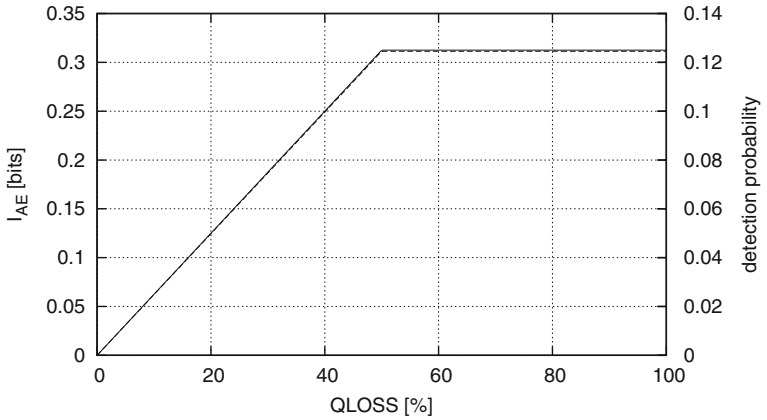

Fig. 5 Eve's information gain and detection probability of hostile circuit (4) detection as a functions of accepted losses

the original imperfect quantum channel with a better one, or Alice and Bob underestimate the quality of the channel they have already been using. The amount of leaked information depends on the message mode properties and the specific features of the hostile circuit. The improvement is limited to the control mode, and thus, new results related to this aspect of protocol operation do not occur. The eavesdropper may gain at most $I_{AE}^{(\max)} = \frac{3}{4}\log_2\frac{4}{3}$ bits per a message cycle (see [9, equation (8)]) at the price of the induction of losses in the control mode at the level $QLOSS_{ind} = 50\,\%$ (see [9, equation (4)]). Thus, Eve can eavesdrop $I_{AE}^{(\max)}$ bits without risking a detection as long as Alice and Bob tolerate $QLOSS \geq QLOSS_{\text{ind}}$. Otherwise, she has to resign from the eavesdropping of some protocol cycles to stay undetected. That way, the level of induced losses is kept below the value accepted by legitimate parties, but, at the same time, Eve's information gain decreases linearly with the percentage of skipped cycles. It is worth noting that the eavesdropper can be detected only by monitoring a level of losses as the projection (2) applied to the state (8) always gives $p_C^{(Z)} = 0$. Although our improvement does not influence the amount of leaked information, it qualitatively changes the detectability of the hostile circuit. Let us replace seminal control mode with the improved one. If Eve attacks all protocol cycles and her device is the sole cause of losses, then the presence of the hostile circuit is revealed with a probability $p_C = 1/8$ under the assumption that all control modes are taken into its calculation. Again, she can disable the eavesdropping on some cycles to limit the level of induced losses at the price of diminishing her information gain. But Eve cannot be revealed when the hostile circuit is idle so p_C also decreases linearly with the percentage of skipped cycles. In consequence, both Eve's information gain and the probability of eavesdropping detection are given by the functions of the same shape (Fig. 5).

Similar considerations for the device (5) are more simple. The attack targets the ping-pong protocol with the dense coding (3) enabled. It has been shown (see [6, equation(5)]) that Eve can always distinguish the classic bit responsible for the bit flip operation on the signal particle. At the same time, the device does not induce losses

in the control mode and it preserves the correlation expected in the seminal control mode (9). Thus, Eve's information gain is equal to $I_{AE} = 1$ bit per the message cycle and $p_C^{(Z)} = 0$. However, the improved control mode reveals the presence of the circuit with probability $p_C = 1/4$ per the control cycle. As a result, Eve gains a half of sent bits at the price of being detected with a finite probability in a single control mode cycle, and, in consequence, she risks detection with a probability close to certainty after a sufficiently large number of control cycles.

4 Conclusion

The control mode is used to detect eavesdroppers in an entanglement-based QDC. Formerly, its purpose has been limited to the verification of the authenticity of the components of the shared entangled state. However, the control mode has to estimate the QBER observed in the message mode in noisy environments as well as it should provide a reliable authentication in lossy quantum channels. The seminal version of the control mode fails to fulfill these additional tasks as local measurements in a computational basis cannot reliably verify the coherence of the distant components of the EPR pair.

We propose a simple method to overcome the aforementioned deficiencies. The improved control mode detects with a nonzero probability the loss of coherence of the EPR pair components by the verification of bit or phase coincidence. In consequence, the presence of the hostile circuits can be revealed because they inevitably break the coherence of the legitimate Bell state. Communicating parties can also estimate the expected QBER with the help of the improved control mode. The proposed amendment closes security loopholes which have been revealed so far, and it restores an asymptotic security of the entanglement-based QDC.

References

1. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002). doi:10.1103/PhysRevLett.89.187902
2. Boström, K., Felbinger, T.: On the security of the ping-pong protocol. Phys. Lett. A **372**(22), 3953–3956 (2008). doi:10.1016/j.physleta.2008.03.048
3. Chamoli, A., Bhandari, C.: Secure direct communication based on ping-pong protocol. Quantum Inf. Process. **8**, 347–356 (2009). doi:10.1007/s11128-009-0112-2
4. Hsieh, M.H., Wilde, M.M.: Entanglement-assisted communication of classical and quantum information. IEEE Trans. Inform. Theory **56**(9), 4682–4704 (2010). doi:10.1109/TIT.2010.2053903
5. 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). doi:10.1007/s11467-007-0050-3
6. 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**(4), 042326 (2013). doi:10.1103/PhysRevA.87.042326

7. Vasiliu, E.V.: Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits. Quantum Inf. Process. **10**(2), 189–202 (2011). doi:10.1007/s11128-010-0188-8
8. 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). doi:10.1103/PhysRevA.71.044305
9. Wójcik, A.: Eavesdropping on the ping-pong quantum communication protocol. Phys. Rev. Lett. **90**(15), 157901 (2003). doi:10.1103/PhysRevLett.90.157901
10. Zawadzki, P.: The ping-pong protocol with a prior privacy amplification. Int. J. Quantum. Inform. **10**(03), 1250032 (2012). doi:10.1142/S0219749912500323
11. Zawadzki, P.: Security of ping-pong protocol based on pairs of completely entangled qudits. Quantum Inf. Process. **11**(6), 1419–1430 (2012). doi:10.1007/s11128-011-0307-1
12. Zawadzki, P.: Improving security of the ping-pong protocol. Quantum Inf. Process. **12**(1), 149–155 (2013). doi:10.1007/s11128-012-0363-1
13. Zawadzki, P.: Effective noise estimation for secure quantum direct communication over imperfect channels. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) Computer Networks, Communications in Computer and Information Science, vol. 431, pp. 197–204. Springer International Publishing, Switzerland (2014). doi:10.1007/978-3-319-07941-7