New Horizons in Mathematical Physics, Vol. 1, No. 2, September 2017
https://dx.doi.org/10.22606/nhmp.2017.12005

Quantum direct communication with quasi Bell states

Piotr Zawadzki[1*]

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

Abstract The variant of ping-pong protocol initialised with a non-orthogonal quantum states is being analysed. The impact of the non-orthogonality of the signal states on occurrence of false alarms in the control mode, level of the bit error rate in the message mode and uncontrolled leakage of the sensitive data is analysed. It is shown that only anti-symmetrical quasi Bell states enable confidential communication.

Keywords: ping-pong protocol, quantum direct communication, quasi Bell states.

1 Introduction

Quantum direct communication (QDC) aims to provide confidentiality of information transferred in open communication channel with no need for use of encryption – a task impossible to carry out with making use of classical techniques. The principles of quantum mechanics have been exploited to propose many flavours of QDC. An extensive review of the applied techniques can be found in [1]. One of the first QDC protocols [2,3] was based on the ping-pong communication scheme and it exploited an entanglement of EPR pairs in order to limit capabilities of the eavesdropper. That protocol has been further extended to multidimensional signal particles [4,5] and thoroughly analysed in different configurations [6,7,8,9]. The adoption of orthogonal initial states is a common denominator of all ping-pong protocol analyses used so far. However, it has been shown that non-orthogonal entangled quantum states [10] can be successfully employed while performing the quantum teleportation [11,12,13,14] – the another communication task with no classical counterpart either. An applicability of the quasi Bell states – a subclass of bipartite non-orthogonal entangled states – to the quantum direct communication is investigated in this contribution. The study analyses the impact of imperfect initial state preparation on the protocol operation and, in particular, it aims to determine whether the aforementioned non-orthogonality has an impact on the security and performance. In consequence, the analysis is limited to small deviations from the perfect setting. To the best of our knowledge, this paper is the first study of this aspect of ping-pong protocol operation. Section 2 introduces notation and explains basic concepts. The main contribution is presented in Section 3. The impact of the obtained results and directions of future research are summarised in Section 4.

2 Analysis

The following description of protocol operation adheres to standard cryptographic personification rules: Alice and Bob are eligible parties of the communication protocol and the malevolent intruder is referred to as Eve. The communication process in ping-pong protocol can be decomposed to the following steps:

1. Bob, the recipient of information, prepares an EPR pair $|\psi_{\text{init}}\rangle_{\text{BA}}$ – this can be any state from eq. (1). Then he sends one of the qubits to Alice.
2. Alice, in order to encode a single bit of the message, applies or not a phase flip operation $\mathcal{Z}_{\text{A}} = |0_{\text{A}}\rangle\langle 0_{\text{A}}| - |1_{\text{A}}\rangle\langle 1_{\text{A}}|$ to the received qubit and then she sends the qubit back to Bob.
3. Bob discriminates between states $|\psi_{\text{init}}\rangle_{\text{BA}}$ and $(\mathcal{I}_{\text{B}} \otimes \mathcal{Z}_{\text{A}})\,|\psi_{\text{init}}\rangle_{\text{BA}}$ in order to decode the value of the bit posted by Alice.

The above steps are referred to as a message mode of the protocol. Eve has no chances to identify the value of the encoded bit as long as she is passive. Due to maximal entanglement of the shared quantum state, she always (i. e., before and after encoding operation) sees the travel qubit as a mixed state of the form $\rho_{\mathrm{A}} = \left(|0_{\mathrm{A}}\rangle\langle 0_{\mathrm{A}}| + |1_{\mathrm{A}}\rangle\langle 1_{\mathrm{A}}|\right)/2$. However, she can mount a man-in-the-middle attack or entangle the travel qubit with her probe $|\chi_{\mathrm{E}}\rangle$ just before it reaches Alice's site (see Figure 1). Actions of legitimate

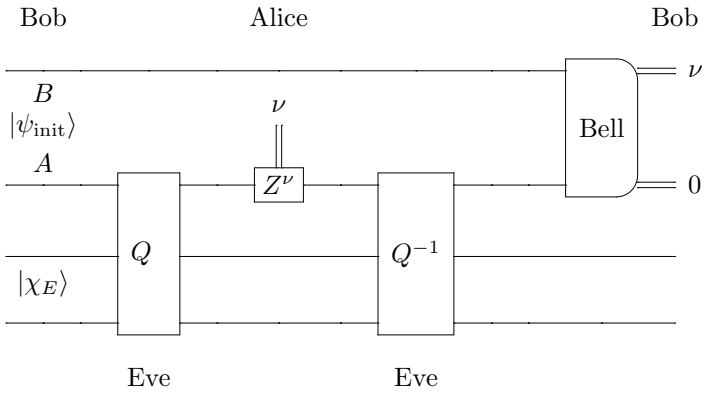

Figure 1. The incoherent attack.

parties aimed at detection of the active eavesdropping are referred to as a control mode. Alice and Bob perform local measurements of the possessed qubits in randomly selected protocol cycles. If the measured qubits really belong to the shared EPR pair, then communicating parties expect to observe a perfect correlation of the outcomes. Any deviation from this rule means that Alice's qubit is not genuine and/or it is affected by Eve's malevolent activity. The protocol is quasi-secure as any entangling transformation $\mathcal{Q}$ that provides non-zero information to Eve is detected with non-zero probability [2]. Alice and Bob can be sure that their communication is not tampered with after sufficient number of control cycles.

Bob, in seminal protocol formulation, can initiate the protocol operation with any EPR pair

$$|\Psi^{\pm}\rangle = \frac{|0_{\mathrm{B}}\rangle|1_{\mathrm{A}}\rangle \pm |1_{\mathrm{B}}\rangle|0_{\mathrm{A}}\rangle}{\sqrt{2}} \qquad |\Phi^{\pm}\rangle = \frac{|0_{\mathrm{B}}\rangle|0_{\mathrm{A}}\rangle \pm |1_{\mathrm{B}}\rangle|1_{\mathrm{A}}\rangle}{\sqrt{2}} \tag{1}$$

and his choice does not affect the protocol security and efficiency. This study responds to the question whether this feature holds for the imperfectly prepared initial state. The quasi Bell states introduced in [10]

$$|\psi^{\pm}\rangle = \frac{|\alpha_{\mathrm{B}}\rangle|\beta_{\mathrm{A}}\rangle \pm |\beta_{\mathrm{B}}\rangle|\alpha_{\mathrm{A}}\rangle}{N_{\pm}^{\psi}} \qquad |\phi^{\pm}\rangle = \frac{|\alpha_{\mathrm{B}}\rangle|\alpha_{\mathrm{A}}\rangle \pm |\beta_{\mathrm{B}}\rangle|\beta_{\mathrm{A}}\rangle}{N_{\pm}^{\phi}} \tag{2}$$

are non-orthogonal analogues of EPR pairs, i. e., $\langle\alpha|\beta\rangle \neq 0$ and $N_{\pm}^{\psi} \neq \sqrt{2} \neq N_{\pm}^{\phi}$ in generic case. These states have been successfully used to study the impact of non-orthogonality of the components of the entangled state on quantum teleportation efficiency [13,14]. However, no similar studies in the context of quantum direct communication have been carried out.

3 Results

This section is devoted to numerical simulations of the protocol operation. It is assumed that Alice and Bob operate in orthogonal basis related to the imperfect initial state in the following way

$$|0\rangle = |\alpha\rangle \tag{3a}$$

$$|1\rangle = N\left(|\beta\rangle - \langle\alpha|\beta\rangle|\alpha\rangle\right) \tag{3b}$$

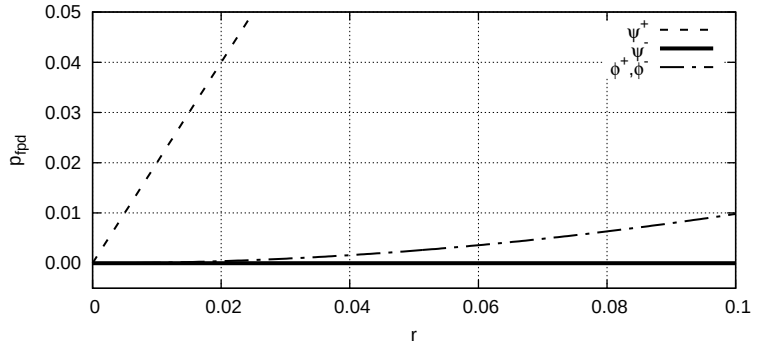

Figure 2. Probability of false positive detection of Eve's presence for non-orthogonal initial states.

The non-orthogonality can be characterised by two real parameters $\langle\alpha|\beta\rangle = re^{j\theta}$ and the reduction to the seminal formulation of the protocol [2] is achieved for $r = 0$. The impact of the imperfect preparation of the initial state is analysed, so the small values of r are considered further.

The form of the initial state and the non-orthogonality level may have the impact on the protocol operation even in the absence of Eve. The malfunction can manifest itself as the additional bit error rate in the message mode or as the false positive detection of an attack in the control mode. Let us focus on the latter issue. The protocol operation has been simulated for $\mathcal{Q} = \mathcal{I}_\mathrm{A} \otimes \mathcal{I}_\mathrm{E}$, i. e., for the completely decoupled Eve. The probability p_fpd of false positive detection of Eve is the probability of finding the shared entangled state in error space. The respective projection operators for $|\psi^\pm\rangle$ and $|\phi^\pm\rangle$ are given as

$$\Pi_\psi = |0_\mathrm{B}0_\mathrm{A}\rangle\langle 0_\mathrm{B}0_\mathrm{A}| + |1_\mathrm{B}1_\mathrm{A}\rangle\langle 1_\mathrm{B}1_\mathrm{A}| \qquad \Pi_\phi = |0_\mathrm{B}1_\mathrm{A}\rangle\langle 0_\mathrm{B}1_\mathrm{A}| + |1_\mathrm{B}0_\mathrm{A}\rangle\langle 1_\mathrm{B}0_\mathrm{A}| \tag{4}$$

The probability p_fpd has been computed as a function of parameters r, θ for different forms of initial states given in (2). The probability p_fpd does not depend on θ and its dependency on r for different initial states is plotted on Figure 2. Only the state $|\psi^-\rangle$ does not induce false positive detections. For the state $|\psi^+\rangle$, the probability p_fpd increases linearly with r and it is much larger than that for $|\phi^\pm\rangle$. The lack of dependency on θ is understandable, as legitimate parties perform local measurements in control mode, so the relative phase of the components of the shared state $|\psi_\mathrm{init}\rangle$ is irrelevant.

The non-orthogonality of the $|\psi_\mathrm{init}\rangle$ also induces errors in the message mode. This time the relative phase of the components is significant, as Bob performs collective measurement on both qubits. The states $|\psi_\mathrm{init}\rangle$ and $\mathcal{Z}_A|\psi_\mathrm{init}\rangle$ are perfectly distinguishable (i. e., orthogonal) for the maximally entangled $|\psi_\mathrm{init}\rangle$. Otherwise, states $|\psi_\mathrm{init}\rangle$ and $\mathcal{Z}_A|\psi_\mathrm{init}\rangle$ can be non-orthogonal, what in turn induces non-zero bit error rate (BER) in message mode. The results of computer simulations for $r < 0.1$ and $0 \leq \theta < 2\pi$ are shown on Figure 3. Again, BER does not appear only for the state $|\psi^-\rangle$. For other types of initial states BER is non-zero and two orders of magnitude higher for $|\psi^+\rangle$ than for $|\phi^\pm\rangle$. It follows that only imperfectly prepared states of type $|\psi^-\rangle$ have no impact on protocol efficiency. The legitimate users have to fight with false positive detection and experience non-zero BER for the remaining three types of protocol initialisation.

Eve was decoupled form the signal qubit so far. However, imperfections of the initial state can also affect the protocol security. It follows from Stinespring's dilation theorem, that the most generic incoherent attack can be described with some unitary transformation $\mathcal{Q}$ that entangles qubit under attack with two qubits controlled by Eve. It can be modelled as a matrix of size $2^3 \times 2^3$ that cannot be decomposed as $\mathcal{Q}_\mathrm{A} \otimes \mathcal{Q}_\mathrm{E}$, i. e., it must provide coupling between signalling system and the probe. However, the optimal form of the coupling transformation $\mathcal{Q}$ is not known. Instead, the Monte-Carlo simulations have been used to gain some insight into the protocol behaviour. The extensive numerical study for different types of initial states and different values of (r, θ) revealed that only the quality of $|\psi^+\rangle$ impacts the protocol security. No dependence on θ has been identified. The Figure 4 illustrates the results of simulations for $r = 0.1$. The solid line represents an upper bound of Eve's information gain in an ideal setting (EPR pair as an initial state, perfect quantum channel, etc.)

$$I_\mathrm{E}^\mathrm{upper} = \mathrm{H}(p) = -p\log_2 p - (1-p)\log_2(1-p) \tag{5}$$

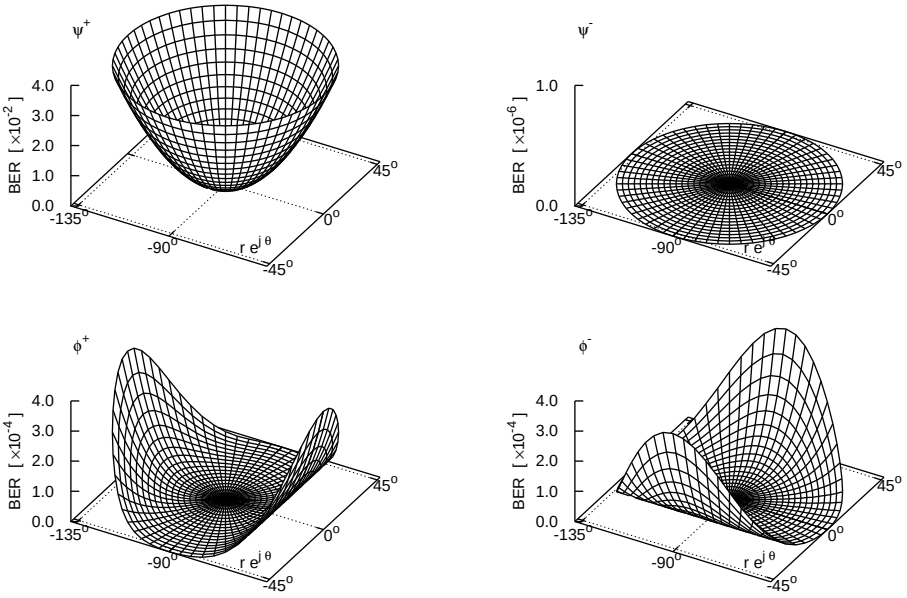

Figure 3. Bit error rate (BER) in message mode for non-orthogonality parameter $r < 0.1$ and different initial states.

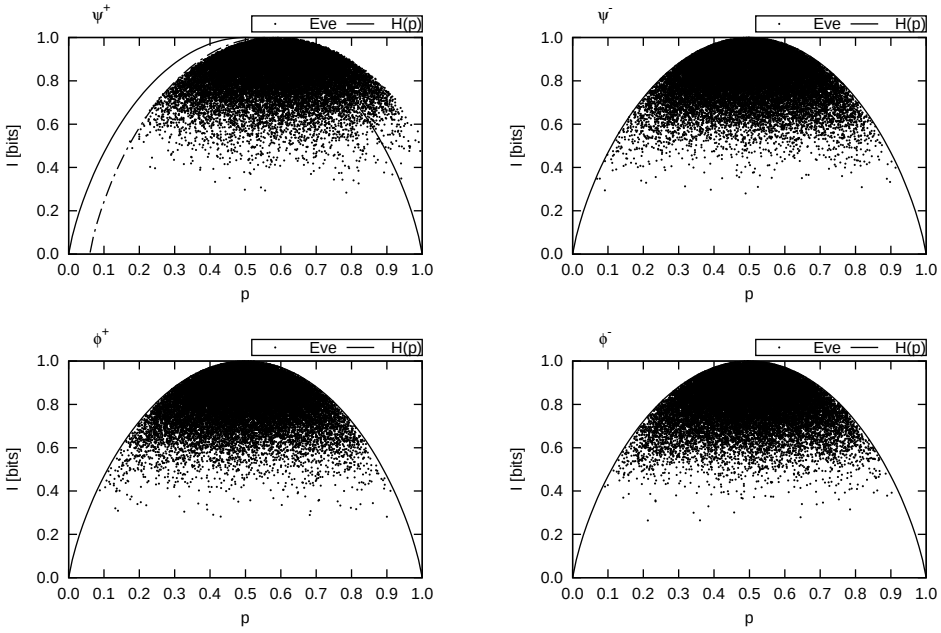

Figure 4. Eavesdropper's information gain in bits per protocol cycle for randomly selected coupling transformation and different initial states.

where p is detection probability. Dots illustrate the information gain for some random coupling $\mathcal{Q}$. Each graph is a result of simulation of 25000 random attacks. The simulations do not reveal security loopholes for $|\psi^-\rangle$ and $|\phi^\pm\rangle$, as the graphs resemble the ones received in an ideal setting [5]. Results for $|\psi^+\rangle$ are interesting. At first it seems that $|\psi^+\rangle$ is advantageous compared to remaining cases as non-zero information gain starts for $p \approx 0.06$ (as follows from the interpolation of simulation data). In other words, the dots representing the attacks are shifted to the right side of the graph. However, as discussed in the preceding paragraph, the usage of $|\psi^+\rangle$ is inevitably related with the false alarms in normal operation. For the $|\psi^+\rangle$ and $r = 0.1$ that happens with probability $p_{\text{fpd}} = 0.2$ (not shown on Figure 2 because of the excessive growth). As a consequence, legitimate parties have to ignore up to 20% errors in control mode and attacks that induce $p < 0.2$ will come unnoticed. It may be estimated from graph that such attacks provide about 0.5 bits per protocol cycle. Similar reasoning applies to $|\phi^\pm\rangle$, but this time $p_{\text{fpd}} = 0.01$ is much less (Figure 2), so the Eve's information gain decreases to approximately 0.1 bits per protocol cycle. As a consequence, only the states of the form $|\psi^-\rangle$ do not imply a security threat.

4 Conclusion

In most analyses it is assumed that ping-pong protocol is initialised with a perfect EPR pair and, as a consequence of this assumption, the obtained results do not depend on the particular form of the initial state. As follows from the presented numerical study, this is no longer true for quasi Bell states – a non-orthogonal analogues of EPR pairs. Only initial states of the form $|\psi^-\rangle = |\alpha\rangle|\beta\rangle - |\beta\rangle|\alpha\rangle$ (normalisation skipped for simplicity) guarantee normal protocol operation without induction of additional bit error rate and erroneous signalling of Eve's presence. The non-zero level of false alarms pose a security threat as the legitimate parties simply do not know whether the event is a feature of the protocol or it is caused by the activity of the eavesdropper. As a result, rarely occurring alarms are simply being ignored. If Eve is able to construct an attack detectable with probability below their threshold, then she can gain some information without being detected. Unfortunately, this is the case for the ping-pong protocol. Thus the form of the initial state has impact on both protocol efficiency and security as long as imperfectly prepared states are allowed. The bottom line is that the form of the initial state is significant as the considered imperfections of its preparation are inevitable in the practical implementation of the protocol.

Acknowledgements

Author acknowledges support by the Ministry of Science and Higher Education funding for statutory activities and Rector of Silesian University of Technology grant number 02/030/RGJ17/0025 in the area of research and development.

References

1. G.-l. Long, F.-g. Deng, C. Wang, X.-h. Li, K. Wen, and W.-y. Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Front. Phys. China*, vol. 2, no. 3, pp. 251–272, 2007.
2. K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," vol. 89, no. 18, p. 187902, 2002.
3. F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," vol. 68, p. 042317, 2003.
4. E. V. Vasiliu, "Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits," vol. 10, no. 2, pp. 189–202, 2010.
5. P. Zawadzki, "Security of ping-pong protocol based on pairs of completely entangled qudits," vol. 11, no. 6, pp. 1419–1430, 2012.
6. Q.-y. Cai and B.-w. Li, "Improving the capacity of the Boström-Felbinger protocol," vol. 69, p. 054301, May 2004.
7. C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," vol. 71, p. 044305, Apr 2005.
8. P. Zawadzki, Z. Puchała, and J. Miszczak, "Increasing the security of the ping-pong protocol by using many mutually unbiased bases," vol. 12, no. 1, pp. 569–575, 2013.

9. P. Zawadzki, "An improved control mode for the ping-pong protocol operation in imperfect quantum channels," vol. 14, no. 7, pp. 2589–2598, 2015.
10. O. Hirota, S. J. V. Enk, K. Nakamura, M. Sohma, and K. Kato, "Entangled nonorthogonal states and their decoherence properties," 2001. [Online]. Available: https://arxiv.org/pdf/quant-ph/0101096.pdf
11. A. K. Pati and P. Agrawal, "Probabilistic teleportation of a qudit," vol. 371, no. 3, pp. 185–189, 2007.
12. Y.-Y. Nie, Z.-H. Hong, Y.-B. Huang, X.-J. Yi, and S.-S. Li, "Non-maximally entangled controlled teleportation using four particles cluster states," vol. 48, no. 5, pp. 1485–1490, 2009.
13. S. Adhikari, A. S. Majumdar, D. Home, A. K. Pan, and P. Joshi, "Quantum teleportation using non-orthogonal entangled channels," vol. 85, no. 4, p. 045001, 2012.
14. H. Prakash and V. Verma, "Minimum assured fidelity and minimum average fidelity in quantum teleportation of single qubit using non-maximally entangled states," vol. 11, no. 6, pp. 1951–1959, 2012.

