Theoretical and Applied Informatics
ISSN 1896–5334
Vol.23 (2011), no. 2
pp.85–95
DOI: 10.2478/v10179-011-0006-8

Security of the quantum direct communication based on pairs of completely entangled qudits

PIOTR ZAWADZKI

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

Received 26 April 2011, Revised 20 June 2011, Accepted 28 June 2011

Abstract: Quantum secure direct communication protocols offer confidential transmission of classic information over the quantum channel without a prior key agreement. The ping-pong based protocols provide asymptotic security and detailed analysis of the security level provided by each variant of the protocol is required. The paper presents a general method of calculation of the eavesdropped information as a function of the attack detection probability. The method is applied to the ping-pong protocol based on completely entangled pairs of qudits. The lower and upper bound on the amount of the leaked information is provided.

Keywords: quantum cryptography, quantum secure direct communication, ping-pong protocol

1. Introduction

Quantum cryptography is extensively developed since the seminal paper of Bennet and Brassard [1]. The interest in this area is motivated by the promise of provable security based on the laws of physics. The first protocols [1, 2] addressed the problem of quantum key distribution (QKD). They are supposed to fill in the gap which appeared after the publication of the Shor's algorithm [3], which is able to break Rivest, Shamir, Adleman (RSA) [4] cryptosystem in polynomial time [5, 6]. However, the information resulting from QKD execution is not determined by either of parties but is settled by the protocol completion itself. Thus QKD protocols cannot be used directly for the exchange of deterministic information. Moreover, quantum communication must be assisted by classic algorithms of privacy amplification which diminish the eavesdropper knowledge about the key under agreement. In effect the information throughput in QKD protocols is low.

Quantum secure deterministic communication (QSDC) protocols are designed for transfer of deterministic classic information over the quantum channel. They provide unidirectional communication in which information content is specified by the sender. Similarly to QKD, QSDC protocols offer asymptotic security in that sense, that there exists a finite probability that the eavesdropper can successfully intercept some part of the message without being detected. The protocol design should provide the possibly low probability of non-detection and the eavesdropper's information gain.

The first QSDC protocol, based on a single photon transmission, was proposed by Beige *et. al.* [7]. Later, Boström et. al. [8] proposed the ping-pong protocol based on EPR pairs. Since then many enhancements and modifications of the ping-pong protocol paradigm have been published including the superdense coding [9], the usage of GHZ states for two [10] and multiparty [11] communication, and variants based on higher dimensional systems i.e. qutrits [12, 13] and qudits [14]. The original protocol is provably secure in case of a perfect quantum channel [8], and although it has been successfully attacked in presence of a noise [15, 16], there exist simple countermeasures that restore its security [17]. The security of the ping-pong protocol based on GHZ states [18] and qutrits [19] also has been studied. It has been shown that their security properties are very similar to the original version although multiparty variants are vulnerable to double CNOT attack [20].

Although the version of the ping-pong protocol based on pairs of maximally entangled qudits is relatively old, its security has not been analyzed [21] in depth. The aim of this paper is to fill in this gap. The approach presented here is a generalization of the methods presented in [8, 19]. It is applied to the protocol variant with superdense coding and the eavesdropping detection performed in the computational base. The analysis of the protocol in which the eavesdropper detection is performed in mutually unbiased bases [22] is left for the future work.

2. The ping-pong protocol in short

In the provided protocol description Alice and Bob are legitimate parties while Eve is a malicious eavesdropper. The ping-pong protocol operates in two modes. In the message mode Alice sends information to Bob, while in the control mode the communicating parties check for presence of an eavesdropper. The operation is started by Bob, the recipient of information, who prepares two maximally entangled qudits. Without loss of generality it may be assumed that it is in the state [23]

$$|\psi_{0,0}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle_h |k\rangle_t \tag{1}$$

One of the qudits, denoted as "home", is kept confidential, while the the second one, named the "travel", is sent to Alice. Alice randomly selects either the message mode or the control mode. In the message mode she applies one of the unitary transformations to the travel qudit [24, 25]

$$U_{\alpha,\beta} = \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{\alpha k}{N}\right) |k+\beta\rangle_t \langle k|_t \tag{2}$$

where summation within kets is performed $(\mathrm{mod} N)$ and $\alpha, \beta = 0, \ldots, N-1$. The message is encoded in α and β so Alice can encode $2\log_2(N)$ bits per one protocol cycle. The entanglement of qudits causes that Alice's local operations have non local effects. The state composed from home and travel qudits is transformed into another maximally entangled state $|\psi_{\alpha,\beta}\rangle$. Next, the transformed qudit is sent back to Bob, who a performs collective measurement on both qudits. There exists one-to-one correspondence between the state detected by Bob and the values of α and β, so Bob can decode information sent by Alice.

However, such a scheme can be attacked by eavesdropping Eve. Although the travel qudit looks for her as maximally mixed, she can attach, according to the dilation theorem [26], an ancilla system of dimension N^2 that purifies the travel qudit. She can then entangle the travel qudit with the ancilla by some unitary operation E. Because of the introduced entanglement the encoding operations $U_{\alpha,\beta}$ also transform the ancilla system. Then Eve can infer some information about Alice encoding by measuring the travel qudit and the ancilla. However, Eve's eavesdropping introduces transmission errors as a side effect, which are perceived by Alice and Bob as a noise. Thus Alice and Bob have to take additional countermeasures to detect Eve's operations.

The special control mode is used for the eavesdropping detection. Alice switches to the control mode in some randomly selected protocol cycles. In this mode she measures the received travel qudit. The fact of switching into control mode is then announced via the public classic channel. It is assumed that although public information is accessible to Eve, she can't control its content. Bob subsequently measures the home qudit in the same base and asks Alice to reveal the value of her measurement. Because of the fragile entanglement of the two-qudit system the result of Bob's measurement is fully determined by the value obtained by Alice. Any deviation from that correlation indicates the presence of Eve.

3. Security analysis

Eve observes the travel qudit as a maximally mixed state

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{3}$$

where the subscript "t" has been omitted as further only the travel qudit will be considered. The best she can do is to entangle the qudit with the ancilla system and infer some information about encoding transformation from the measurement of the accessible part of the resulting quantum system. However, any mixed state in the the space of $\dim(\mathcal{H})$ may be treated as the partial trace of the pure state living in the space with attached ancilla of size $\dim(\mathcal{H}_E) \leq (\dim(\mathcal{H}))^2$.

The entanglement operation is unitary and may be described as

$$|\psi^{(x)}\rangle = E|x\rangle|\phi\rangle = \sum_{l=0}^{N-1} e_{l,x}|l\rangle|\phi_{x,l}\rangle \tag{4}$$

where $|x\rangle$ and $|x\rangle$ denote the state of the travel qudit before and after transformation. Similarly, $|\phi\rangle$ and $|\phi_{x,l}\rangle$ denote the states of the ancilla. There exist exactly N such states for each x so Eve has to use N^2 probes.

The state of the travel qudit and the attached ancilla after Alice's encoding operation takes the form

$$\begin{aligned} &|\psi^{(x)}_{\alpha,\beta}\rangle = U_{\alpha,\beta}|\psi^{(x)}\rangle = \left(\sum_{k=0}^{N-1} \exp\left(2\pi i\tfrac{\alpha k}{N}\right)|k+\beta\rangle\langle k|\right)\left(\sum_{l}^{N-1} e_{l,x}|l,\phi_{x,l}\rangle\right) = \\ &= \sum_{k=0}^{N-1} \exp\left(2\pi i\tfrac{\alpha k}{N}\right) e_{k,x}|k+\beta\rangle|\phi_{x,k}\rangle \end{aligned} \tag{5}$$

Lets us assume that encoding operations used by Alice are equally probable and consider the attack on state $x = 0$. The resulting density matrix has the form

$$\begin{aligned} &\rho^{(0)} = \tfrac{1}{N^2}\sum_{\alpha,\beta=0}^{N-1}|\psi^{(0)}_{\alpha,\beta}\rangle\langle\psi^{(0)}_{\alpha,\beta}| = \tfrac{1}{N^2}\sum_{\alpha,\beta=0}^{N-1} U_{\alpha,\beta}|\psi^{(0)}\rangle\langle\psi^{(0)}|U^{\dagger}_{\alpha,\beta} = \\ &= \tfrac{1}{N^2}\sum_{\alpha,\beta=0}^{N-1}\left(\sum_{k=0}^{N-1}\exp\left(2\pi i\tfrac{\alpha k}{N}\right)e_{k,0}|k+\beta\rangle|\phi_{0,k}\rangle\right)\times \\ &\times\left(\sum_{l=0}^{N-1}\exp\left(-2\pi i\tfrac{\alpha l}{N}\right)e^{*}_{l,0}\langle\phi_{0,l}|\langle l+\beta|\right) = \\ &= \tfrac{1}{N^2}\sum_{\alpha,\beta=0}^{N-1}\left(\sum_{k,l=0}^{N-1}\exp\left(2\pi i\tfrac{\alpha(k-l)}{N}\right)e_{k,0}e^{*}_{l,0}|k+\beta\rangle|\phi_{0,k}\rangle\langle\phi_{0,l}|\langle l+\beta|\right) = \\ &= \tfrac{1}{N^2}\sum_{\beta=0}^{N-1}\left(\sum_{k,l=0}^{N-1}\left(\sum_{\alpha=0}^{N-1}\exp\left(2\pi i\tfrac{\alpha(k-l)}{N}\right)\right)e_{k,0}e^{*}_{l,0}|k+\beta\rangle|\phi_{0,k}\rangle\langle\phi_{0,l}|\langle l+\beta|\right) \end{aligned} \tag{6}$$

But $\sum_{\alpha=0}^{N-1}\exp\left(2\pi i\frac{\alpha(k-l)}{N}\right) = N\delta_{k,l}$ and

$$\rho^{(0)} = \frac{1}{N}\sum_{\beta=0}^{N-1}\sum_{k=0}^{N-1} e_{k,0}e^{*}_{k,0}|k+\beta\rangle|\phi_{0,k}\rangle\langle\phi_{0,k}|\langle k+\beta| \tag{7}$$

There exist N^2 base vectors $|k+\beta\rangle|\phi_{0,k}\rangle$, but fixing β selects the subspace spanned by N vectors. It follows that density matrix of size $N^2 \times N^2$ may be factorized into N identical[1] submatrices of size $N \times N$. Moreover, each of those matrices is diagonal

$$\begin{aligned}\rho^{(0)} &= \tfrac{1}{N}\sum_{k=0}^{N-1} e_{k,0}e_{k,0}^{*}|k\rangle|\phi_{0,k}\rangle\langle\phi_{0,k}|\langle k|+ \\ &+\tfrac{1}{N}\sum_{k=0}^{N-1} e_{k,0}e_{k,0}^{*}|k+1\rangle|\phi_{0,k}\rangle\langle\phi_{0,k}|\langle k+1|+\ldots \\ &+\tfrac{1}{N}\sum_{k=0}^{N-1} e_{k,0}e_{k,0}^{*}|k+N-1\rangle|\phi_{0,k}\rangle\langle\phi_{0,k}|\langle k+N-1|\end{aligned} \tag{8}$$

The maximal mutual information $I_{A,E}$ between Alice and Eve is limited by the Holevo bound

$$I_{A,E} \leq \chi = S\left(\rho^{(0)}\right) - \frac{1}{N^2}\sum_{\alpha,\beta=0}^{N-1} S\left(|\psi_{\alpha,\beta}^{(0)}\rangle\langle\psi_{\alpha,\beta}^{(0)}|\right) \tag{9}$$

where $S(\rho)$ denotes the von Neumann entropy of the system described by the density matrix ρ. But, by the assumption about the construction of the ancilla system, the states $|\psi_{\alpha,\beta}^{(0)}\rangle$ are pure and $S\left(|\psi_{\alpha,\beta}^{(0)}\rangle\langle\psi_{\alpha,\beta}^{(0)}|\right) = 0$ so

$$I_{A,E}^{(0)} \leq S\left(\rho^{(0)}\right) = -\mathrm{Tr}\rho^{(0)}\log_2\rho^{(0)} = -\sum_{k=0}^{N^2-1}\lambda_k\log_2\lambda_k \tag{10}$$

However, each eigenvalue is N-fold degenerate and

$$S\left(\rho^{(0)}\right) = -N\sum_{k=0}^{N-1}\lambda_k\log_2\lambda_k = \log_2 N - \sum_{k=0}^{N-1}|e_{k,0}|^2\log_2|e_{k,0}|^2 \tag{11}$$

where identity $\sum_{k=0}^{N-1}|e_{k,0}|^2 = 1$ has been used. It is worth noting, that $p_{nd}^{(0)} = |e_{0,0}|^2$ is a non-detection probability when the control mode is executed in the computational basis. Similarly for other x

$$I_{A,E}^{(x)} \leq S\left(\rho^{(x)}\right) = \log_2 N - \sum_{k=0}^{N}|e_{k,x}|^2\log_N|e_{k,x}|^2 \tag{12}$$

and non-detection probability equals to $p_{nd}^{(x)} = |e_{x,x}|^2$. The states $|x\rangle$ looks for Eve as maximally mixed ensemble and total information equals to

$$I_{A,E} = \frac{1}{N}\sum_{x=0}^{N} I_{A,E}^{(x)} \tag{13}$$

[1]This results from the assumption that coding transformations $U_{\alpha,\beta}$ are equally probable.

Similarly the non-detection probability should be averaged on the ensemble

$$p_{nd} = \frac{1}{N} \sum_{x=0}^{N} p_{nd}^{(x)} \tag{14}$$

The above equations represent opposed interests of the Eve: she has to choose the attack operation such that p_{nd} is kept possibly small while the mutual information $I_{A,E}$ is maximized.

4. Results

A Monte-Carlo analysis of the protocol security was performed. For a set of randomly selected attack operations intercepted information and a non-detection probability were computed using (13) and (14). The considered operations are represented as points on Fig. 1. on results for the qudit dimension $N = 3, 4, 5$ are plotted.

But before delving into the analysis of the numerical results it is helpful to consider two canonical attack operations. Let us suppose that Eve is able to construct the unitary transformation such that

$$|e_{m,n}|^2 = \begin{cases} p_{nd} & m = n \\ 1 - p_{nd} & n = (m+1) \bmod N \end{cases} \tag{15}$$

where p_{nd} represents the non-detection probability. In this case the mutual information between Alice and Eve equals to

$$I_{AE}^{\min} = \log_2 N - p_{nd} \log_2 (p_{nd}) - (1 - p_{nd}) \log_2 (1 - p_{nd}) \tag{16}$$

In the second scenario let the detection probability will be equally spread over all probe states

$$|e_{m,n}|^2 = \begin{cases} p_{nd} & m = n \\ \frac{1-p_{nd}}{N-1} & m \neq n \end{cases} \tag{17}$$

In such a situation

$$I_{AE}^{\max} = I_{AE}^{\min} - (1 - p_{nd}) \log_2 (N - 1) \tag{18}$$

The curves (16) and (18) are also shown on Fig. 1. It is immediately visible that they represent lower and upper bound of information accessible to the eavesdropper. The maximal information available to Eve is equal to the channel capacity $2 \log_2 N$. Moreover, for larger N the attack providing maximal possible information is detected with higher probability. If Eve implements attacks that are harder to detect then mutual information is diminished. In the limiting case when Eve is totally hidden ($p_{nd} = 1$) she has knowledge about half of the transmission content. It is also visible that randomly

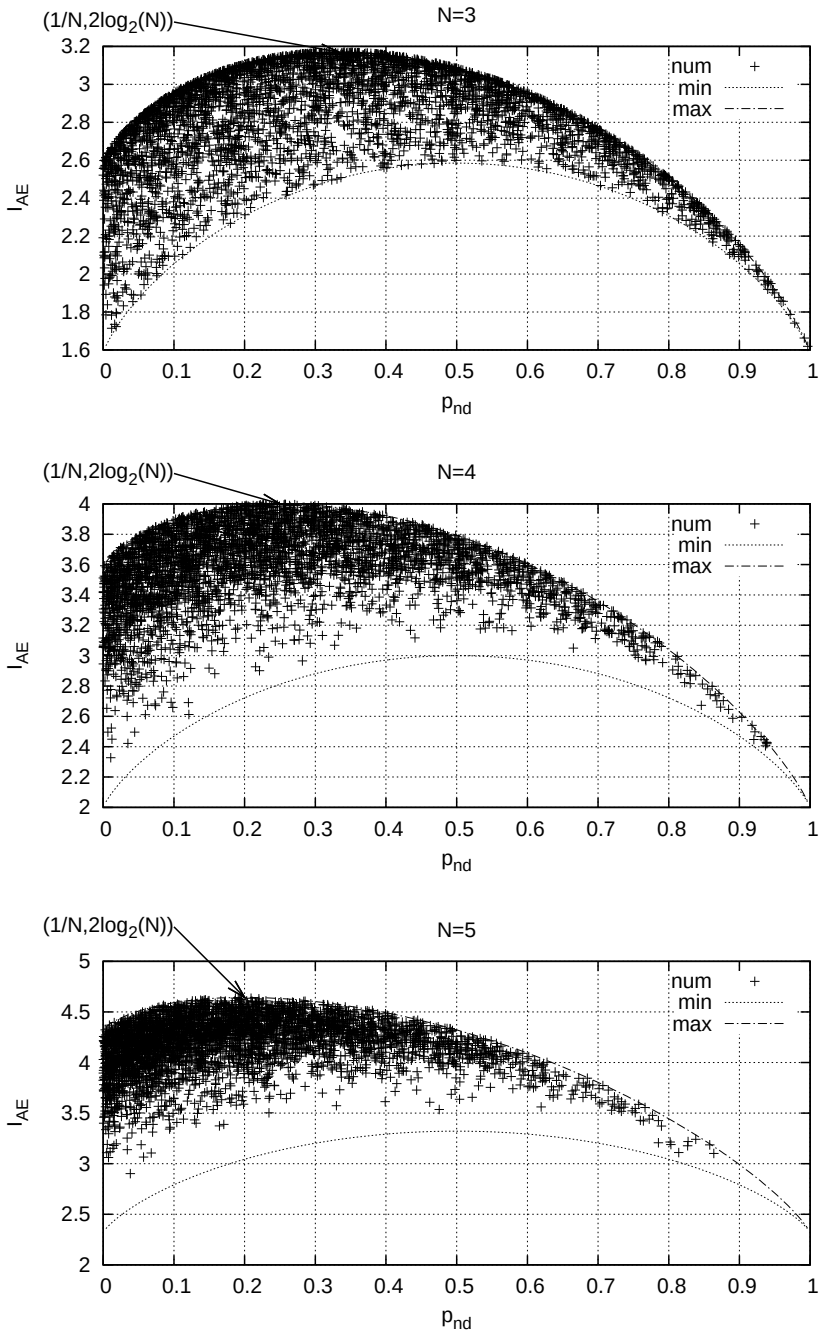

Fig. 1: Information accessible to the eavesdropper in the qudits based ping-pong protocol versus a non-detection probability

selected attack transformations are concentrated around the point in which Eve gets most information but is easily detected. The results presented herein are in the perfect agreement with the analysis of the qutrit based protocol presented in [19]. It immediately follows that all qudit based ping-pong protocols that use the superdense coding and the eavesdropping detection only in the computational base are not secure. Eve intercepts at least a half of the message content and in such conditions even privacy amplification cannot restore protocol security. It is also worth noting that the usage of privacy amplification together with the QSDC protocols is unreasonable as the latter ones were devised to avoid necessity of such postprocessing.

5. Conclusion

The numerical experiments and theoretical analysis reveal a tradeoff between the eavesdropper detectability and the information leakage. The maximal amount of information obtained by the eavesdropper is equal to the total channel capacity. However, as the number of states of the signal particle gets larger, the probability of non-detection is diminished. Moreover, the control mode using only the computational base is not sufficient, as in this case Eve can intercept a half of the message and stay undetected.

The examination of the eavesdropper detection based on mutually unbiased bases will be the subject of future research. Fortunately, the proposed general approach to the security analysis of the ping-pong protocols also may be used in such a case. The presented method can be applied not only to variants when one qudit particle is used for signaling, but also, almost without any modifications, it can be applied to analyze protocols based on multiple qubits and GHZ states. Thus it seems to be very fruitful, as the QSDC protocols are one of the most actively developed branches of quantum cryptography. Moreover, protocols conforming to the ping-pong paradigm, in which signal particle travels forth and back between the recipient and the sender of information, are the most popular [27].

References

1. C. H. Bennett and G. Brassard: *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.

2. A. K. Ekert: *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., vol. 67, pp. 661–663, Aug 1991.

3. P. W. Shor: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Sci. Statist. Comput., vol. 26, pp. 1484–1509, 1997.

4. R. Rivest, A. Shamir, and L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

5. P. Zawadzki: *Numerical estimation of the quantum factorization effectiveness*, Theor. Appl. Inf., vol. 22, no. 1, pp. 63–72, 2010.

6. P. Zawadzki: *A fine estimate of quantum factorization success probability*, Int. J. Quant. Inf., vol. 8, no. 8, pp. 1233–1238, 2010.

7. A. Beige, E. B. G., C. Kurtsiefer, and W. H: *Secure communication with a publicly known key*, Act. Phys. Pol., vol. 101, no. 3, pp. 357–368, 2002.

8. K. Boström and T. Felbinger: *Deterministic secure direct communication using entanglement*, Phys. Rev. Lett., vol. 89, p. 187902, Oct 2002.

9. Q. Y. Cai and B. W. Li: *Improving the capacity of the boström-felbinger protocol*, Phys. Rev. A, vol. 69, p. 054301, May 2004.

10. T. Gao, F. L. Yan, and Z. X. Wang: *Deterministic secure direct communication using ghz states and swapping quantum entanglement*, J. Phys. A: Math. Gen., vol. 38, no. 25, p. 5761, 2005.

11. A. Chamoli and C. Bhandari: *Secure direct communication based on ping–pong protocol*, Quant. Inf. Proc., vol. 8, pp. 347–356, 2009. 10.1007/s11128-009-0112-2.

12. 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*, Phys. Rev. A, vol. 71, p. 044305, Apr 2005.

13. H. Bechmann-Pasquinucci, A. Peres: *Quantum cryptography with 3-state systems*, Phys. Rev. Lett., vol. 85, pp. 3313–3316, Oct 2000.

14. T. Durt, D. Kaszlikowski, J.-L. Chen, L. C. Kwek: *Security of quantum key distributions with entangled qudits*, Phys. Rev. A, vol. 69, p. 032313, Mar 2004.

15. A. Wójcik: *Eavesdropping on the "Ping-Pong" quantum communication protocol*, Phys. Rev. Lett., vol. 90, p. 157901, 4 2003.

16. Z. Zhang, Z. Man, Y. Li: *Improving Wójcik's eavesdropping attack on the ping–pong protocol*, Phys. Lett. A, vol. 333, pp. 46–50, 2004.

17. K. Boström, T. Felbinger: *On the security of the ping-pong protocol*, Phys. Lett. A, vol. 372, no. 22, pp. 3953–3956, 2008.

18. E. V. Vasiliu: *Asymptotic security of the ping-pong quantum direct communication protocol with three-qubit greenberger–horne–zeilinger states*, Georgian Elec. Sci. J. Comput. Sci. Telecomm., vol. 3, no. 20, pp. 3–15, 2009.

19. E. V. Vasiliu: *Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits*, Quant. Inf. Proc., vol. 10, pp. 189–202, 2011.

20. Y.-G. Yang, Y.-W. Teng, H.-P. Chai, Q.-Y. Wen: *Revisiting the security of secure direct communication based on ping-pong protocol*, Quant. Inf. Proc., 09 2010.

21. C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, G. L. Long: *Quantum secure direct communication with high-dimension quantum superdense coding*, Phys. Rev. A, vol. 71, p. 044305, 2005. QSDC for qudits with superdense coding.

22. I. Bengtsson: *Three ways to look at mutually unbiased bases*. quant-ph/0610216v1, 2006.

23. T. Durt, D. Kaszlikowski, J.-L. Chen, L. C. Kwek: *Security of quantum key distributions with entangled qudits*, Phys. Rev. A, vol. 69, p. 032313, Mar 2004.

24. C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, G. L. Long: *Quantum secure direct communication with high-dimension quantum superdense coding*, Phys. Rev. A, vol. 71, p. 044305, Apr 2005.

25. X. S. Liu, G. L. Long, D. M. Tong, and F. Li: *General scheme for superdense coding between multiparties*, Phys. Rev. A, vol. 65, p. 022304, Jan 2002.

26. M. Keyl: *Fundamentals of quantum information theory*, Phys. Rep., vol. 369, no. 5, pp. 431–548, 2002.

27. M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

28. 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.

Ocena bezpieczeństwa bezpośredniej komunikacji kwantowej wykorzystującej pary całkowicie splątanych quditów

Streszczenie

Kryptografia kwantowa jest jednym z najintensywniej rozwijanych praktycznych zastosowań kwantowego przetwarzania informacji. Pierwsze zaproponowane protokoły kryptograficzne dotyczyły problemu uzgodnienia klucza za pomocą otwartego łącza telekomunikacyjnego [1, 2]. Niestety protokoły te okazały się mało wydajne i nie umożliwiają przesyłania klasycznej informacji za pomocą kanału kwantowego. Problem ten rozwiązują protokoły bezpośredniej deterministycznej komunikacji kwantowej (QSDC). Pierwszy protokół tego typu wykorzystujący pojedyncze fotony został zaproponowany przez Beige et. al. [7]. Nieco później Boström et. al. [8] zaproponował protokół ping-pong wykorzystujący pary EPR. Protokół ten stał się pierwowzorem dla wielu protokołów pracujących według tego samego paradygmatu. Odbiorca posiada stan splątany, którego część przekazuje nadawcy. Nadawca wykonując operacje kwantowe na cząstce sygnałowej w takt kodowanej informacji zmienia stan całego stanu splątanego. Nadawca następnie odsyła cząstkę sygnałową do odbiorcy, a ten wykonuje kolektywny pomiar na stanie splątanym dekodując tym samym nadaną informację [9, 10, 11, 12, 13].

Protokoły QSDC oferują bezpieczeństwo asymptotyczne, w tym sensie, że istnieje niezerowe prawdopodobieństwo nie wykrycia napastnika mimo iż uzyska on dostęp do

części przesyłanej informacji. Dlatego też istotne jest systematyczne przebadanie właściwości protokołów QSDC w tym zakresie. Jak dotąd do badania protokołów stosowano metody wykorzystujące ich szczególne właściwości i dopiero w pracach [18, 19] dokonano tego w sposób systematyczny dla par qutritów oraz stanów GHZ.

Mimo, że wersja protokołu ping-pong dla par maksymalnie splątanych quditów jest stosunkowo stara [21] to nie doczekała się systematycznej analizy pod kątem poziomu zapewnianej ochrony. W niniejszym artykule zaproponowano uogólnienie podejścia zaproponowanego w [8, 19] i zastosowano je do wspomnianego wyżej wariantu protokołu. W pracy przedstawiono wyniki obliczeń numerycznych oraz zaproponowano wyrażenia na kres dolny i górny informacji uzyskanej przez napastnika, przy czym wartości kresów zależne są od prawdopodobieństwa wykrycia podsłuchu. Z przedstawionych rezultatów wynika, że napastnik może uzyskać dostęp do $\log_2 N$ bitów informacji, co stanowi połowę pojemości kanału, a w szczególnym przypadku może przejąć całość transmisji, jednak wiedza ta okupiona jest stosunkowo dużym prawdpodobieństwem wykrycia jego obecności ($p = (N-1)/N$). W świetle zaprezentowanych wyników odmiany protokołu ping-pong wykorzystujące supergęste kodowanie i wykrywanie podsłuchu tylko w bazie pomiarowej należy uznać za mało bezpieczne. Zaproponowana metoda analizy może być również zastosowana, praktycznie bez żadnych modyfikacji, do badania protokołów wykorzystujących stany splątane GHZ.