Steganalysis and improvement of a quantum steganography protocol via a GHZ_4 state*

Xu Shu-Jiang(徐淑奖)[a)b)c)], Chen Xiu-Bo(陈秀波)[a)c)†], Niu Xin-Xin(钮心忻)[a)], and Yang Yi-Xian(杨义先)[a)]

[a)] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[b)] *Shandong Provincial Key Laboratory of Computer Network, Shandong Computer Science Center, Jinan* 250014, *China*

[c)] *State Key Laboratory of Information Security, (Institute of Information Engineering, Chinese Academy of Sciences), Beijing* 100093, *China*

(Received 7 November 2012; revised manuscript received 24 December 2012)

Quantum steganography that utilizes the quantum mechanical effect to achieve the purpose of information hiding is a popular topic of quantum information. Recently, El Allati *et al.* proposed a new quantum steganography using the GHZ_4 state. Since all of the 8 groups of unitary transformations used in the secret message encoding rule change the GHZ_4 state into 6 instead of 8 different quantum states when the global phase is not considered, we point out that a 2-bit instead of a 3-bit secret message can be encoded by one group of the given unitary transformations. To encode a 3-bit secret message by performing a group of unitary transformations on the GHZ_4 state, we give another 8 groups of unitary transformations that can change the GHZ_4 state into 8 different quantum states. Due to the symmetry of the GHZ_4 state, all the possible 16 groups of unitary transformations change the GHZ_4 state into 8 different quantum states, so the improved protocol achieves a high efficiency.

Keywords: quantum steganography, GHZ_4 entangled state, quantum cryptography, quantum communication

PACS: 03.67.Dd, 03.67.–a, 03.65.–w, 03.67.Hk **DOI:** 10.1088/1674-1056/22/6/060307

1. Introduction

Quantum steganography, known as the quantum vision of classical steganography, has become a popular topic in the field of quantum cryptography. As an alternative method for privacy protection, quantum steganography employs quantum mechanical effects, including quantum communication and quantum computation, to achieve quantum or classical information hiding tasks. Due to Heisenberg's uncertainty principle, any attempt to measure a quantum system will disturb it, so the disturbance inevitably alerts legitimate users to the eavesdropper's presence. Therefore, quantum steganography, as well as other quantum cryptography schemes, such as quantum key distribution (QKD),[1–5] quantum secret sharing (QSS),[6–10] quantum secure direct communication (QSDC),[11–16] and so on, can achieve unconditional security without being eavesdropped. In a steganography scheme, both the secret message and its existence should be imperceptible. In fact, the imperceptibility of quantum steganography has some inborn advantages in comparison with classical steganography due to Heisenberg's uncertainty principle and the no-cloning theorem.

Similar classical information hiding, quantum information hiding can be classified into three basic categories: quantum steganography (QS), quantum covert channels (QCCs), and quantum watermarking (QW). QS is the most important subdiscipline of quantum information hiding. There are four types of QS schemes according to the embedding methods. The first one is quantum data hiding (QDH),[17–23] which employs some physical properties of quantum states to embed and recover the secret message by local operations and classical communication (LOCC). For example, Terhal *et al.*[17] proposed a QDH scheme in 2001 based on the fact that $|\Psi^-\rangle$ is just a spin singlet while the other three of the four Bell states are spin triplets. The second one, which is based on the quantum error-correcting code (QECC), is called QECC-based QS.[24–27] For instance, a QS protocol was presented to hide quantum information via disguising it as noise in a codeword of a QECC by Shaw *et al.*[25] in 2011. The third one, which is based on classical or quantum image processing techniques, is called image-based QS. In 2008, Mogos[28,29] expanded the field of applicability of steganography from the classical image informatics to the quantum one by describing a qutrit as a linear combination of the projections on a three coordinate axes. The last one, which makes a minor revision of quantum communication protocols or quantum cryptography protocols to hide secret messages, is protocol-based QS.[30–33] For example, Martin[31] proposed a steganography strategy to successfully transmit a bit of information in each round of procedure of QKD between the two correspondents.

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61170272, 61272514, 61003287, and 61070163), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20100005120002), the Fok Ying Tong Education Foundation (Grant No. 131067), the Natural Science Foundation of Shandong Province, China (Grant No. ZR2011FM023), the Outstanding Research Award Fund for Young Scientists of Shandong Province, China (Grant No. BS2011DX034), and the Fundamental Research Funds for Central Universities of China (Grant No. BUPT2012RC0221).

†Corresponding author. E-mail: flyover100@163.com (Chen Xiu-Bo)

© 2013 Chinese Physical Society and IOP Publishing Ltd

However, Gao *et al.*[34] pointed out that the quantum cryptography protocols QKD, QSS, and QSDC are not suitable for steganography since each of them can be used for deterministic secure communication. Covert channels are distinct from a legitimate channel using steganography that disguises secret message inside legitimate information objects. The legitimate channel misuse by steganography schemes is especially not a covert channel and can be prevented by ultra-high-assurance secure operation systems, while covert channels can tunnel through secure operating systems and require special measures to control them. The quantum covert channel,[35–37] which usually establishes a subliminal channel within a quantum communication protocol or a quantum cryptography protocol, can be defined as a quantum communications channel that transfers some kinds of information using a method originally not intended to transfer this kind of information. The idea of building an imperceptible channel for sending secret messages in quantum communication is really interesting and was first proposed by Qu *et al.*[35,36] using entanglement swapping of quantum states. There is only one real quantum watermarking scheme in quantum fields so far, but this is a hopeful and useful topic in quantum information. In 2012, Iliyasu *et al.*[38] proposed a secure, keyless and blind watermarking and authentication strategy for images based on restricted geometric transformations of a quantum image.

Recently, Allati *et al.*[39] proposed a new QS protocol using GHZ_4 state, where the GHZ_4 state can be rewritten into four different forms by two groups of different orthogonal basis. After applying unitary transformations to his own two particles, a sender can transmit a 3-bit secret message by transmitting 2 particles to the recipient based on the novel correlation of four particle GHZ_4 states. We analyze this protocol and show the reason why a 2-bit instead of a 3-bit secret message can be encoded by one group of the given unitary transformations. To encode a 3-bit secret message by applying a group of unitary transformations to the GHZ_4 state, we give another 8 groups of unitary transformations that can change the GHZ_4 state into 8 different quantum states.

The rest of this paper is organized as follows. Section 2 gives the brief introduction of the original protocol. The steganalysis is shown in Section 3. We present the improved protocol in Section 4. Section 5 concludes this paper.

2. Review of AMH protocol

In this section, we will briefly introduce the quantum steganography protocol,[39] which can be called the AMH protocol for simplicity.

A maximally entangled GHZ_4 state is defined as:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0000\rangle_{1234} + |1111\rangle_{1234}). \tag{1}$$

The four unitary transformations σ_I, σ_x, σ_y, and σ_z are:[40]

$$\begin{aligned}
\sigma_I &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\
\sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\
\sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \\
\sigma_y &= |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix},
\end{aligned} \tag{2}$$

where $\mathrm{i}^2 = -1$. Only applying one of the four local unitary transformations to a particle of a quantum state, the quantum state can be changed into another state.[40] The eigenstates of the Pauli operators in Eq. (2), $X = \{|x_+\rangle, |x_-\rangle\}$ and $Y = \{|y_+\rangle, |y_-\rangle\}$, form two different groups of orthonormal basis for one-particle space. Here

$$|x_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \ |x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{3}$$

$$|y_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}|1\rangle), \ |y_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle). \tag{4}$$

Using the two groups of orthonormal basis, the entangled GHZ_4 state (1) can be rewritten into four different forms:[39]

$$\begin{aligned}
|\Psi\rangle = \frac{1}{2\sqrt{2}}[&(|x_+\rangle_1|x_+\rangle_2 + |x_-\rangle_1|x_-\rangle_2)(|x_+\rangle_3|x_+\rangle_4 \\
&+ |x_-\rangle_3|x_-\rangle_4) + (|x_+\rangle_1|x_-\rangle_2 + |x_-\rangle_1|x_+\rangle_2) \\
&\times (|x_+\rangle_3|x_-\rangle_4 + |x_-\rangle_3|x_+\rangle_4)] = |\Psi_1\rangle,
\end{aligned} \tag{5}$$

$$\begin{aligned}
|\Psi\rangle = \frac{1}{2\sqrt{2}}[&(|y_+\rangle_1|y_+\rangle_2 + |y_-\rangle_1|y_-\rangle_2)(|y_+\rangle_3|y_+\rangle_4 \\
&+ |y_-\rangle_3|y_-\rangle_4) + (|y_+\rangle_1|y_-\rangle_2 + |y_-\rangle_1|y_+\rangle_2) \\
&\times (|y_+\rangle_3|y_-\rangle_4 + |y_-\rangle_3|y_+\rangle_4)] = |\Psi_2\rangle,
\end{aligned} \tag{6}$$

$$\begin{aligned}
|\Psi\rangle = \frac{1}{2\sqrt{2}}[&(|x_+\rangle_1|y_+\rangle_2 + |x_-\rangle_1|y_-\rangle_2)(|x_+\rangle_3|y_-\rangle_4 \\
&+ |x_-\rangle_3|y_+\rangle_4) + (|x_+\rangle_1|y_-\rangle_2 + |x_-\rangle_1|y_+\rangle_2) \\
&\times (|x_+\rangle_3|y_+\rangle_4 + |x_-\rangle_3|y_-\rangle_4)] = |\Psi_3\rangle,
\end{aligned} \tag{7}$$

$$\begin{aligned}
|\Psi\rangle = \frac{1}{2\sqrt{2}}[&(|y_+\rangle_1|x_+\rangle_2 + |y_-\rangle_1|x_-\rangle_2)(|y_+\rangle_3|x_-\rangle_4 \\
&+ |y_-\rangle_3|x_+\rangle_4) + (|y_+\rangle_1|x_-\rangle_2 + |y_-\rangle_1|x_+\rangle_2) \\
&\times (|y_+\rangle_3|x_+\rangle_4 + |y_-\rangle_3|x_-\rangle_4)] = |\Psi_4\rangle.
\end{aligned} \tag{8}$$

With the correlation among the four particles shown in Eqs. (5)–(8), one can encode 2^4 different 4-bit codewords. For instance, the tensor product $|x_+\rangle_1|x_+\rangle_2|x_+\rangle_3|x_+\rangle_4$ can be encoded into 0000.

By applying the unitary transformations $\sigma_I\sigma_I$, $\sigma_x\sigma_x$, $\sigma_I\sigma_z$, $\sigma_y\sigma_y$, $\sigma_I\sigma_x$, $\sigma_x\sigma_y$, $\sigma_I\sigma_y$ or $\sigma_y\sigma_x$ on the second and the fourth particles of $|\Psi_i\rangle$ $(i = 1,2,3,4)$, one can encode a 3-bit secret message, then the secret message encoding rule can be derived which is shown in Table 1.[39]

Table 1. The correlation between unitary transformations and all possible cases of code.

Alice's unitary transformations	Code	Alice's unitary transformations	Code
$\sigma_I\sigma_I$	000	$\sigma_x\sigma_x$	100
$\sigma_I\sigma_z$	001	$\sigma_y\sigma_y$	101
$\sigma_I\sigma_x$	010	$\sigma_x\sigma_y$	110
$\sigma_I\sigma_y$	011	$\sigma_y\sigma_x$	111

The AMH protocol procedure is as follows.[39]

(i) **Preparation of the initial entangled quantum states** The receiver of the protocol, Bob, prepares a sequence of GHZ_4 entangled states $|\Psi\rangle^{\otimes n} = |\Psi\rangle_1|\Psi\rangle_2\ldots|\Psi\rangle_n$ and respectively takes one particle from each state to form four ordered particle sequences: Si: $[P_1^i, P_2^i, \ldots, P_n^i]$ $(i = 1,2,3,4)$, here P_j^i means the i-th particle of the j-th GHZ_4 entangled state $|\Psi\rangle_j$. He keeps particle sequences S1 and S3, and sends the particles in sequences S2 and S4 to the sender of the protocol, Alice.

(ii) **Eavesdropping check** After receiving the particles, Alice and Bob perform an eavesdropping check by choosing sample particles from the four sequences. Here we do not describe the eavesdropping check processes in detail.

(iii) **Secret message encoding** If the quantum channel is secure, Alice randomly chooses many pairs of particles from S2 and S4 and encodes the secret message according to the secret message encoding rule, then she sends the encoded particles to Bob.

(iv) **Secret message decoding** Bob measures the corresponding particles in S1 and S3 based on Eqs. (5)–(8) and performs a measurement on the travel particles that Alice has sent to him. With the measurement results, Bob can distinguish the unitary transformations used by Alice and decode the secret message according to Table 1.

3. Steganalysis of AMH quantum steganography

In this section, we will show that the 8 groups of unitary transformations $\sigma_I\sigma_I$, $\sigma_x\sigma_x$, $\sigma_I\sigma_z$, $\sigma_y\sigma_y$, $\sigma_I\sigma_x$, $\sigma_x\sigma_y$, $\sigma_I\sigma_y$, and $\sigma_y\sigma_x$, which are used in Table 1, change the GHZ_4 state into 6 instead of 8 different quantum states when the global phase is not considered. Thus, a 2-bit instead of a 3-bit secret message can be obtained by performing one group of the given 8 groups of unitary transformations.

Let us see the result states after respectively applying the four unitary transformations, which is shown in Eq. (2), to the four quantum states in Eqs. (3) and (4):[40]

$$\begin{aligned}
&\sigma_I|x_\pm\rangle = |x_\pm\rangle\,,\ \ \sigma_I|y_\pm\rangle = |y_\pm\rangle\,,\\
&\sigma_z|x_\pm\rangle = |x_\mp\rangle\,,\ \ \sigma_z|y_\pm\rangle = |y_\mp\rangle\,, \qquad (9)\\
&\sigma_x|x_+\rangle = |x_+\rangle\,,\ \ \sigma_x|x_-\rangle = -|x_-\rangle\,,\\
&\sigma_x|y_+\rangle = \mathrm{i}|y_-\rangle\,,\ \ \sigma_x|y_-\rangle = -\mathrm{i}|y_+\rangle\,, \qquad (10)\\
&\sigma_y|x_+\rangle = -\mathrm{i}|x_-\rangle\,,\ \ \sigma_y|x_-\rangle = \mathrm{i}|x_+\rangle\,,
\end{aligned}$$

$$\sigma_y|y_+\rangle = |y_+\rangle\,,\ \ \sigma_y|y_-\rangle = -|y_-\rangle\,. \qquad (11)$$

Suppose that the given unitary transformations are respectively applied to the second and the fourth particles, according to Eqs. (9)–(11), we can obtain

$$\sigma_I\sigma_I|\Psi_i\rangle = |\Psi_i\rangle = \sigma_z\sigma_z|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,, \qquad (12)$$

$$\sigma_I\sigma_z|\Psi_i\rangle = \sigma_z\sigma_I|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,, \qquad (13)$$

$$\sigma_I\sigma_x|\Psi_i\rangle = -\mathrm{i}\sigma_z\sigma_y|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,, \qquad (14)$$

$$\sigma_I\sigma_y|\Psi_i\rangle = \mathrm{i}\sigma_z\sigma_x|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,. \qquad (15)$$

$$\sigma_x\sigma_x|\Psi_i\rangle = -\mathrm{i}\sigma_y\sigma_y|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,, \qquad (16)$$

$$\sigma_x\sigma_y|\Psi_i\rangle = \sigma_y\sigma_x|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,. \qquad (17)$$

If the global phase is not considered, all the given unitary transformations used in Table 1 can change the GHZ_4 entangled state into 6 instead of 8 different forms. As a result, Bob fails to exactly decode the 3-bit secret message that Alice has sent to him. In fact, Alice can send a 2-bit secret message by performing the given unitary transformations on a GHZ_4 state.

4. An improved quantum steganography protocol based on a GHZ_4 state

In this section, we will give another 8 groups of unitary transformations to encode a 3-bit secret message. There are 16 groups of different two-particle unitary transformations, 8 of them are adopted in Table 1. We first show which states can be changed into by applying another 4 groups of unitary transformations to the GHZ_4 state. Similar to Eqs. (12)–(17), we can obtain

$$\sigma_x\sigma_I|\Psi_i\rangle = -\mathrm{i}\sigma_y\sigma_z|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,, \qquad (18)$$

$$\sigma_x\sigma_z|\Psi_i\rangle = -\mathrm{i}\sigma_y\sigma_I|\Psi_i\rangle\,,\ \ i = 1,2,3,4\,. \qquad (19)$$

Obviously, all the possible 16 groups of unitary transformations change the GHZ_4 state into 8 different quantum states due to the symmetry of the GHZ_4 state. Thus, a 3-bit secret message at most can be encoded by applying a group of unitary transformations to two particles of the GHZ_4 state.

According to Eqs. (12)–(19), the 8 unitary transformations $\sigma_I\sigma_I$, $\sigma_I\sigma_z$, $\sigma_I\sigma_x$, $\sigma_I\sigma_y$, $\sigma_x\sigma_I$, $\sigma_x\sigma_z$, $\sigma_x\sigma_x$, and $\sigma_x\sigma_y$ can change the GHZ_4 state into 8 different quantum states. Based on the unitary transformations $\sigma_I\sigma_I$, $\sigma_I\sigma_z$, $\sigma_I\sigma_x$, $\sigma_I\sigma_y$, $\sigma_x\sigma_I$, $\sigma_x\sigma_z$, $\sigma_x\sigma_x$, and $\sigma_x\sigma_y$, we obtain an improved secret message encoding rule that is shown in Table 2. Using the improved rule, a 3-bit secret message can be encoded successfully.

Table 2. The improved correlation between unitary transformations and all possible cases of code.

Alice's unitary transformations	Code	Alice's unitary transformations	Code
$\sigma_I\sigma_I$	000	$\sigma_x\sigma_I$	100
$\sigma_I\sigma_z$	001	$\sigma_x\sigma_z$	101
$\sigma_I\sigma_x$	010	$\sigma_x\sigma_x$	110
$\sigma_I\sigma_y$	011	$\sigma_x\sigma_y$	111

5. Conclusion

In summary, we point out that the receiver fails to exactly decode a 3-bit secret message in the AMH protocol because all the given 8 groups of unitary transformations that the sender applied can change the GHZ_4 state into 6 instead of 8 different states when the global phase is not considered. In order to send a 3-bit secret message by one group of unitary transformations, we give another 8 groups of unitary transformations that can change the GHZ_4 state into 8 different states.

The GHZ_4 state is a special state in the graph state family which has many interesting features,[41] such as the thought-provoking theoretical structure, nonlocality, and decoherence. Especially, many or their entanglement properties are closely related to their underlying graphs. Nowadays, the GHZ states including 3-particle, 4-particle, 5-particle, and 6-particle states have been achieved experimentally.[41–45] Because the unitary transformations by quantum circuits and the von Neumann measurement on single-photon could be implemented with high-efficiency,[46] it is believed that the improved scheme can be realized by experiment easily. Quantum steganography can be adopted for covert exchange of information and copyright protection with unconditional security, the implementability of the improved scheme will make quantum steganography more practical.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, 12–19 December, 1984, Bangalore, India, p. 175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Zhu C H, Pei C X, Quan D X, Gao J L, Chen N and Yi Y H 2010 *Chin. Phys. Lett.* **27** 090301

[4] Zhou Y Y and Zhou X J 2011 *Acta Phys. Sin.* **60** 100301 (in Chinese)

[5] Zhou N R, Wang L J, Gong L H, Zuo X W and Liu Y 2011 *Opt. Commun.* **284** 4836

[6] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648

[7] Chen X B, Yang S, Su Y and Yang Y X 2012 *Phys. Scr.* **86** 055002

[8] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev. A* **72** 044301

[9] Zhang Z R, Liu W T and Li C Z 2011 *Chin. Phys. B* **20** 050309

[10] Chen X B, Niu X X, Zhou X J and Yang Y X 2012 *Quantum Inf. Process.* **12** 365

[11] Bostrom K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[12] Cai Q Y and Li B W 2004 *Phys. Rev. A* **69** 054301

[13] Chen X B, Wang T Y, Du J Z, Wen Q Y and Zhu F C 2008 *Int. J. Quantum Inf.* **6** 543

[14] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305

[15] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev. A* **78** 064304

[16] Chen X B, Wen Q Y, Guo F Z, Sun Y, Xu G and Zhu F C 2008 *Int. J. Quantum Inf.* **6** 899

[17] Terhal B M, DiVincenzo D P and Leung D W 2001 *Phys. Rev. Lett.* **86** 5807

[18] Eggeling T and Werner R F 2002 *Phys. Rev. Lett.* **89** 097905

[19] DiVincenzo D P, Leung D W and Terhal B M 2002 *IEEE Trans. Inf. Theory* **48** 580

[20] Guo G C and Guo G P 2003 *Phys. Rev. A* **68** 044303

[21] Hayden P, Leung D and Smith G 2005 *Phys. Rev. A* **71** 062339

[22] Chattopadhyay I and Sarkar D 2007 *Phys. Lett. A* **365** 273

[23] Matthews W, Wehner S and Winter A 2009 *J. Commun. Math. Phys.* **291** 813

[24] Gea-Banacloche J 2002 *J. Math. Phys.* **43** 4531

[25] Shaw B A and Brun T A 2011 *Phys. Rev. A* **83** 022310

[26] Cao D and Song Y L 2011 *J. Inf. Comput. Sci.* **8** 1793

[27] Cao D and Song Y L 2011 *J. Inf. Comput. Sci.* **8** 2703

[28] Mogos G 2008 *International Symposium on Computer Science and Its Applications*, 13–15 October, 2008, Hobart, Australia, p. 187

[29] Mogos G 2009 *Int. J. Multimedia Ubiquitous Eng.* **4** 13

[30] Worley III G G 2004 arXiv: 0401041v2 [hep-ph]

[31] Martin K 2007 *LNCS* **4567** 32

[32] Zhang D X and Liao X Y 2007 *Wseas Trans. Comput.* **5** 757

[33] Liao X, Wen Q Y, Y Sun and J Zhang 2010 *The Journal of Systems and Software* **83** 1801

[34] Gao F, Liu B, Zhang W W, Wen Q Y and Liu H 2013 *Quantum Inf. Process.* **12** 625

[35] Qu Z G, Chen X B, Niu X X and Yang Y X 2010 *Opt. Commun.* **283** 4782

[36] Qu Z G, Chen X B, Niu X X and Yang Y X 2011 *Opt. Commun.* **284** 2075

[37] Fatahi N and Naseri M 2012 *Int. J. Theor. Phys.* **51** 2094

[38] Iliyasu A M, Le P Q, Dong F Y and Hirota K 2012 *Inf. Sci.* **186** 126

[39] El Allati A, Ould Medeni M B and Hassouni1 Y 2012 *Commun. Theor. Phys.* **57** 577

[40] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[41] Lu C Y, Zhou X Q, Gühne O, Gao W B, Zhang J, Yuan Z S, Goebel A, Yang T and Pan J W 2007 *Nat. Phys.* **3** 91

[42] Sackett C A, Kielpinski D, King B E, Langer C, Meyer V, Myatt C J, Rowe M, Turchette Q A, Itano W M, Wineland D J and Monroe C 2000 *Nature* **404** 256

[43] Pan J W, Daniell M, Gasparoni S, Weihs G and Zeilinger A 2001 *Phys. Rev. Lett.* **86** 4435

[44] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J and Pan J W 2004 *Nature* **430** 54

[45] Leibfried D, Knill E, Seidelin S, Britton J, Blakestad R B, Chiaverini J, Hume D B, Itano W M, Jost J D, Langer C, Ozeri R, Reichle R and Wineland D J 2005 *Nature* **438** 639

[46] Kim J, Takeuchi S, Yamamoto Y and Hogue H 1999 *Appl. Phys. Lett.* **74** 902