G. Zeng

Modern information processing laboratory (MIPL),
Department of Electronic Engineering, Shanghai Jiaotong University,
Shanghai 200030, China.
Theoretische Quantendynamik,
Fakultät für Physik, Universität Freiburg,
H.-Herder-Strasse 3, D-79104 Freiburg, Germany.
E-mail: guihuazeng@hotmail.com

Trojan Horse Attacking Strategy on Quantum Cryptography

Received March 31, 2003

Trojan horse attacking strategy on quantum cryptography is investigated, three aspects are involved. First, the mechanism for the Trojan horse attacking strategy on quantum cryptography as well as classic cryptography is studied. Then the fragility of the quantum cryptographic algorithm employing EPR pairs as key against the Trojan horse attacking strategy is analyzed. To prevent the Trojan horse attacking strategy, an improvement scheme which makes use of non-orthogonal entangled states is proposed, results show the improvement scheme is robust to the Trojan horse attacking strategy without reducing the security on other kinds of attacking strategies.

1. Introduction

In private communication and data security attackers (e.g., adversary and/or ragger) will try to break the employed confidential system for their benefits. To prevent effectively the attacks from obtaining the legitimate information, cryptography has arisen and is employed to prevent the attacks. Cryptography is a subject which is employed for rendering the message secret and creating a cipher by making use of algorithms and protocols so that the attackers can not or can not easily acquire the private information. It plays a very important role in the modern information protection. However, as virtue rises one foot, vice rises ten feet. To break the algorithms and protocols provided in the cryptography, a concomitant subject called cryptoanalysis has also arisen [1].

The so called cryptoanalysis is a science and study of methods of breaking ciphers. Many attacking strategies for converting encrypted messages into plaintext without initial knowledge of the key employed in the encryption have been investigated and used in practice. But, any successes of these strategies completely depend on the drawbacks of the cryptographic system, i.e., cryptosystem. These drawbacks arose from two major causes, i.e., the inappropriate fundamentals, which are employed as a foundation for the scheme, and the imperfection of the cryptosystem's construction. Actually, any improper design will create drawbacks in the cryptosystem and subsequently the attacker can break in principle the scheme by means of these drawbacks. Of course, an absolutely perfect cryptosystem is not possible and not necessary in practice, since such kind of system leads to a huge cost.

Trojan horse attacking strategy (THAS) arose from the drawbacks of construction of the system (e.g., device, computer program, algorithm or protocol *et al.*). When a Trojan horse can be hidden without easy detection in a system, an attacker can make use of this kind of strategy to break the system and then obtain useful information. Unfortunately, this strategy is not only available in classic cryptography but also in the recently proposed quantum cryptography [2]–[9]. This strategy on the quantum key distribution has been analyzed in [10, 6, 11], and a scheme for preventing this strategy was proposed in [11].

In this paper we consider the THAS on the quantum cryptographic algorithm, which employs EPR pairs as the symmetrical key. Three aspects will be investigated in this work, including the mechanism, the attacking way on the quantum cryptographic algorithm, and the preventing approach for this attacking strategy. Especially the improvement scheme will be investigated in detail.

This paper is arranged as follows. In Sec. 2, the mechanism for the THAS will be analyzed first. Then in Sec. 3 we will investigate the THAS on the quantum cryptographic algorithm which employs EPR pairs as the key. An improvement scheme for preventing the THAS will be presented in Sec. 4. After these a simple remark will be presented in Sec. 5. Finally a conclusion will be drawn in Sec. 6.

2. Mechanism for Trojan horse attacking strategy

Let us firstly investigate the mechanism for the THAS on cryptography in this section. In essential, all attacking approaches proposed in cryptoanalysis (including classic cryptoanalysis and quantum cryptoanalysis) can be categorized mainly as three kinds of attacking strategies, i.e., the strategy based on fundamentals drawbacks (SFD), the strategy based on obtained information (SOI), and the strategy based on assistant systems (SAS). In the SFD the attacker makes use of fundamentals drawbacks to break the cipher and obtain useful information. As an example, the classic cryptosystem is based on the complexity assumption which has not been proven, thus usually containing a fundamentals drawback. With the development of the mathematics these drawbacks become a means for breaking the cryptosystem [1]. Another example is the attacking approaches presented in quantum cryptography, by far most attacking strategies such as the individual and collective attacks [8] are based on the fundamentals, i.e., quantum laws. Fortunately all proofs are advantaged to the quantum cryptography but not to the cryptoanalysis. While in the SOI the attacker makes use of the leaked information of the cryptosystem, the ciphertext, and/or the obtained parts of plaintext to break the cryptosystem [1]. However, we would like to stress here the SAS, which relies on assistant systems to break the cryptosystem. One of the typical approaches in this situation is the THAS.

To study the mechanism for THAS let us firstly consider what is the Trojan horse in the information protection, since the Trojan horse is the important base in the THAS. In data security the Trojan horse is defined as a small program inserted by an attacker in a computer system. It performs functions not described in the program specifications, taking advantage of rights belonging to the calling environment to copy, misuse or destroy data not relevant to its stated purpose. For example, a Trojan horse in a text editor might copy confidential information in a file being edited to a

file accessible to another. More generally, the so-called Trojan horse is a 'robot horse' which can become a part of the legitimate users' systems. Then the 'robot horse' can be surreptitiously exploited by the legitimate authorizations of operation (e.g., measurement, detection et al.) to the detriment of security. For example, break the system via feeding back information to the attacker (e.g., the dishonest manufacturer or even the adversary) or directly destroying the legitimate data. To the legitimate users' system the Trojan horse is actually an additional system with passive effects. Many things, such as devices and small programs inserted in the users' system, probing signals entering the users' system through a public channel et al, or even the attacker, can become a Trojan horse. However, we must emphasize that it is impossible for any Trojan horse to play the same role as legitimate users because the Trojan horse is only a small part of the legitimate system.

There are mainly two kinds of Trojan horses, i.e., the pre-lurked Trojan horse and the online Trojan horse. The pre-lurked Trojan horse is a 'robot horse' which is pre-inserted in the legitimate users's system, e.g., programs, apparatuses or even offices. At an appropriate condition the lurked Trojan horse is activated automatically by the legitimate system, and then it feeds back the available information to the attackers, even destroying the users' system. The online Trojan horse is actually a probing signal which may enter the legitimate system without awareness and then back-reflect to the attacker. Both kinds of Trojan horses may be classic as well as quantum. In addition, the Trojan horse may also be a combination of the 'quantum horse' and 'classic horse'.

If a Trojan horse can be inserted successfully in the users' system, the attacker can break the employed cryptosystem and obtain available information by means of the feedback information of the 'robot horse'. This attacking strategy is called THAS. Corresponding to the kinds of the Trojan horses there are two kinds of THAS's, i.e., the strategy relying on a pre-lurked Trojan horse and the strategy depending on the probing signal. While the attacking ways may be classic approaches or quantum approaches determined by the features of the employed Trojan horses. For example, if employing a pointer state of the legitimate system as the Trojan horse, or a preinserted tiny device as a Trojan hose, which is exploited to detect the quantum state of the qubits as the key, the attacker can obtain useful messages by analyzing the feedback information of the Trojan horses. If sending light pulses (probing signal) into the fiber entering legitimate users's apparatuses, then the attacker can analyze the backreflected light [10]. Of course, without the Trojan horse this strategy can do nothing since the feedback information of the Trojan horse is very important in this attacking strategy. Obviously this strategy is completely different from the strategies which are always involved in the quantum cryptography, e.g., the intercept/resend attack and the entanglement attack [3, 5, 8, 7], where the attacker can directly obtain the information for attacking.

3. Trojan horse attacking strategy on quantum cryptographic algorithm

In this section we consider the THAS on the quantum cryptographic algorithm which employs EPR pairs as the key. Recently, two interesting quantum vernam algorithms based on EPR pairs have been proposed. These algorithms employ EPR pair(s) as the symmetrical keys of the algorithm. In [12] the message is encrypted by means of a quantum controlled-NOT with employment of a symmetrical key which consisted of one EPR pair and one bilateral rotation. In [13] the message is encrypted with a key which consisted of two EPR pairs. A common feature of the above quantum vernam algorithms is that EPR pairs are applied as a sharing key between the two legitimate users called Alice and Bob. These algorithms are provably secure for the SFD and the SOI. However, they can not circumvent the THAS. In the following we investigate the fragility of these algorithms against the THAS which employs prelurked Trojan horse (in this section and the following section we suppose the Trojan horse is a tiny device pre-inserted in Alice's or Bob's apparatus).

To show the fragility of the quantum cryptographic algorithm employing EPR pair(s) as the key against the THAS, we first give a simple description for this kind of algorithm. In general, this kind of algorithm can be summarized generally as follows. Suppose Alice and Bob sharing n EPR pairs as the key $\mathcal{K} = \{|k_1\rangle, |k_2\rangle, \cdots, |k_n\rangle\}$. Each EPR pair can be expressed as,

$$|\Phi_i^+\rangle = \frac{1}{\sqrt{2}} \left(|0_a^i 0_b^i\rangle + |1_a^i 1_b^i\rangle \right) = |k_i\rangle, \tag{3.1}$$

where subscripts a, b denote Alice's particles \mathcal{P}_a and Bob's \mathcal{P}_b of each EPR pair, $|k_i\rangle$ denotes the i^{th} key element, and $i = 1, 2, \dots, n$. Denote the plaintext (message) by,

$$|\psi^m\rangle = \alpha|0\rangle + \beta|1\rangle,\tag{3.2}$$

the corresponding particle is expressed as \mathcal{P}_m , where $|\alpha|^2 + |\beta|^2 = 1$. Suppose Alice is the sender, then Alice encrypts the qubit $|\psi^m\rangle$ by making use of the quantum controlled-NOT operations on both her EPR particle \mathcal{P}_a (key particle) and the message particle \mathcal{P}_m . After that, Alice obtains the ciphertext $|\Psi^c\rangle$, which can be denoted as,

$$|\Psi^c\rangle = C_{mk}^n |k_n\rangle \left\{ C_{mk}^{n-1} |k_{n-1}\rangle \left\{ \cdots \left\{ C_{mk}^1 |k_1\rangle |\psi^m\rangle \right\} \right\} \right\}, \tag{3.3}$$

where C_{mk}^i denotes the i^{th} quantum controlled-NOT gate on \mathcal{P}_m and \mathcal{P}_a , the subscript mk denotes the quantum gate operating on the key particle and the message particle. Then Alice sends the ciphertext to Bob via a quantum channel. After receiving the ciphertext $|\Psi^c\rangle$ Bob decrypts the ciphertext by making use of an inverse process controlled under the key. Finally Bob gets the message.

Now let us investigate THAS on the above quantum algorithm. First, we consider the situation of using only one EPR pair as the key. In this case, the key is just the EPR pair, i.e, $|K\rangle = |\Phi^{+}\rangle$, which can be denoted as,

$$|\Phi^{+}\rangle = \frac{1}{\sqrt{2}} \left(|0_a 0_b\rangle + |1_a 1_b\rangle \right). \tag{3.4}$$

Then ciphertext can be expressed as,

$$|\Psi^c\rangle = C_{ma}|\Phi^+\rangle|\psi^m\rangle = |0_a0_b\rangle \otimes |\psi^m\rangle + |1_a1_b\rangle \otimes X_m|\psi^m\rangle. \tag{3.5}$$

where X_m denotes the quantum X-gate on the particle \mathcal{P}_m . Eq. (3.5) illustrates that when Alice's and Bob's EPR particles are in the states $|0_a0_b\rangle$ then the message particle is in the state $|\psi^m\rangle$, otherwise, the state of the message particle is in $X_m|\psi^m\rangle$.

Obviously, if Alice's and Bob's EPR particles can not be disturbed by the attacker, the above algorithm is secure. However, if the attacker can pre-lurk a Trojan horse in Alice's or Bob's apparatus, the legitimate communicators Alice and Bob will not be lucky since the attacker can obtain their useful information through the THAS. This can be done very easily. Suppose the attacker puts successfully a Trojan hose, Υ , e.g., a set of tiny devices which can distinguish the eigenstates states $|0\rangle$ and $|1\rangle$ (for example a device can recognize the 'bright' and 'dark' pulse) and send feedback information, in Alice's apparatus (this is available since in practice the users are not experts so that they can not easily find the 'robot horse' which is pre-lurked ulteriorly by the dishonest manufacturers), then the key can be written as $|\Phi^+(\Upsilon)\rangle$. Subsequently Alice's encrypting transformation by making use of controlled-NOT yields a ciphertext state, which can be written as,

$$|\Psi_h^c\rangle = |0_a(h_{\parallel})0_b\rangle \otimes |\psi^m\rangle + |1_a(h_{\perp})1_b\rangle \otimes X_m|\psi^m\rangle, \tag{3.6}$$

where h_{\shortparallel} and h_{\perp} are the feedback information of the Trojan horse. After Alice has encrypted her message $|\psi^{m}\rangle$ using the EPR pair, the Trojan horse is activated automatically. For example, if the attacker pre-lurks measurement bases for the eigenstates states $|0\rangle$ and $|1\rangle$, the Trojan horse only needs to measure Alice's EPR particle. Now the 'horse' feeds back the result h_{\perp} when the measurement result is $|0\rangle$, otherwise the 'horse' feeds back the result h_{\perp} . Then, what the attacker needs to do is to wait for Alice's ciphertext $|\Psi^{c}\rangle$ and the feedback information of the Trojan horse. If the attacker can successfully intercept the ciphertext particle \mathcal{P}_{m} which is sent to Bob, then the attacker can obtain completely the qubit $|\psi_{m}\rangle$ by making use of the feedback information h_{\shortparallel} and h_{\perp} , and the intercepted particle \mathcal{P}_{m} . For example, if the feedback information shows that Bob's key bit is $|0\rangle$, attacker gets $|\psi^{m}\rangle$. If the feedback information shows that Bob's key bit is $|1\rangle$, attacker gets $X_{m}|\psi^{m}\rangle$. With this knowledge, the attacker can completely obtain the plaintext (message).

In the above we have analyzed the Trojan horse attacking strategy for the situation which makes use of only one EPR pair as a key. For the case of making use of two EPR pairs $|\Phi_1^+\rangle$ and $|\Phi_2^+\rangle$ as the key (see Ref. [13]), the Trojan horse attacking strategy can also be successful. In this case the key can be denoted as,

$$|k_1\rangle = |\Phi_1^+\rangle = \frac{1}{\sqrt{2}} \left(|0_a^1 0_b^1\rangle + |1_a^1 1_b^1\rangle \right),$$
 (3.7)

and

$$|k_2\rangle = |\Phi_2^+\rangle = \frac{1}{\sqrt{2}} \left(|0_a^2 0_b^2\rangle + |1_a^2 1_b^2\rangle \right).$$
 (3.8)

Suppose the attacker pre-lurks successfully two 'horse' Υ_1 and Υ_2 into Alice's or Bob's devices using the similar ways described above. After Alice's encryption using controlled-X and controlled-Z gates on the key particle and message particle, the

ciphertext state can be written as,

$$\begin{split} |\Psi_{h}^{c}\rangle &= C_{a_{2}m}^{Z}\{(C_{a_{1}m}^{X}(|\Phi^{+}_{1}(\Upsilon_{1})\rangle|\psi^{m}\rangle))|\Phi^{+}_{2}(\Upsilon_{2})\rangle\} = \\ &= \frac{1}{2}|0_{a}^{1}0_{b}^{1}(h_{\shortparallel}^{1})\rangle\left\{|0_{a}^{2}0_{b}^{2}(h_{\shortparallel}^{2})\rangle\otimes|\psi^{m}\rangle + |1_{a}^{2}1_{b}^{2}(h_{\perp}^{2})\rangle\otimes Z_{m}|\psi^{m}\rangle\right\} + \\ &+ \frac{1}{2}|1_{a}^{1}1_{b}^{1}(h_{\shortparallel}^{1})\rangle\left\{|0_{a}^{2}0_{b}^{2}(h_{\shortparallel}^{2})\rangle\otimes X_{m}|\psi^{m}\rangle + |1_{a}^{2}1_{b}^{2}(h_{\perp}^{2})\rangle\otimes X_{m}Z_{m}|\psi^{m}\rangle\right\} \quad (3.9) \end{split}$$

where the superscripts '1' and '2' refer to the particles in the pairs $|\Phi^+_1\rangle$ and $|\Phi^+_2\rangle$, h_{\shortparallel}^1 and h_{\perp}^1 are feedback information of the Trojan horse Υ_1 , h_{\shortparallel}^2 and h_{\perp}^2 are feedback information of the Trojan horse Υ_2 . Υ_1 and Υ_2 are associated with Bob's particles. It is clear that the attacker can get the message by the similar way of employing one EPR pair as the key. Therefore, the quantum cryptographic algorithms based on the EPR pairs as keys are fragile against the THAS, although they are provably secure against the other attacking strategies.

Actually, if the possible states of Alice's key particles \mathcal{P}_a (or Bob's key particle \mathcal{P}_b) are orthogonal states, any quantum cryptographic algorithm which employs directly such kind of key is not robust to the THAS. Because in such a situation the successful Trojan horse can recognize the possible states of the key particle. For example, while Alice and Bob employ the EPR pair as the key then Alice's or Bob's key particle takes the state $|0\rangle$ or $|1\rangle$. Then a proper Trojan horse, e.g., a device which can distinguish the eigenstates $|0\rangle$ and $|1\rangle$, can recognize exactly the state of the key particle as described above. Thus the available feedback information can be obtained by the attacker. Therefore, to prevent the THAS one should use the non-orthogonal states as a sharing key in the symmetrical quantum cryptographic algorithm.

4. Prevent Trojan horse attacking strategy

In this section we will show that the above THAS can be prevented by making use of the non-orthogonal entanglement state as the key. The process is as follows. The legitimate users Alice and Bob create a set of EPR pairs, each pair can be denoted as,

$$|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|0_{a}0_{b}\rangle + |1_{a}1_{b}\rangle) = \frac{1}{\sqrt{2}}(|+_{a}+_{b}\rangle + |-_{a}-_{b}\rangle),$$
 (4.1)

where $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. Then Alice or Bob randomly choose a operator from $\{\mathcal{I},H\}$ to apply on her (his) EPR particles until all EPR pairs have been operated, where \mathcal{I} and H are respectively the unit operation and the Hadamard gate. This operation yields,

$$|\psi_1\rangle = \mathcal{I}|\Phi^+\rangle = |\Phi^+\rangle,$$
 (4.2)

and

$$|\psi_2\rangle = \mathcal{H}|\Phi^+\rangle. \tag{4.3}$$

In bases $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle, |\psi_2\rangle$ can be expressed as,

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|1_a + b\rangle + |0_a - b\rangle) = \frac{1}{\sqrt{2}}(|+_a 1_b\rangle + |-_a 0_b\rangle).$$
 (4.4)

After these operations, Alice and Bob obtain a random sequence which consists of $\{|\psi_1\rangle, |\psi_2\rangle\}$. Finally Alice and Bob take this sequence as the key. Since $|\langle\psi_1|\psi_2\rangle|^2 \neq$ = 0 which means that the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are non-orthogonal, any quantum attacking strategies can not be available [14]. This point is guaranteed by the nocloning theorem [15]. In the following we will show these properties can also be employed to prevent the Trojan horse attacking strategy.

To the attacker the key $|K\rangle$ is a superposition of $|\psi_1\rangle$ and $|\psi_2\rangle$, i.e.,

$$|K\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle. \tag{4.5}$$

Then the ciphertext state can be written as,

$$|\Psi_e^c\rangle = C_{am}|K\rangle|\psi^m\rangle = \left(\tilde{\alpha}_k^c|0_a0_b\rangle + \tilde{\beta}_k^c|0_a - b\rangle\right) \otimes |\psi^m\rangle + \left(\tilde{\alpha}_k^c|1_a1_b\rangle + \tilde{\beta}_k^c|1_a + b\rangle\right) \otimes X_m|\psi^m\rangle, \quad (4.6)$$

where $\tilde{\alpha}_k^c = c_1/\sqrt{2}$, $\tilde{\beta}_k^c = c_2/\sqrt{2}$. After the encrypting transformation, Alice obtains the ciphertext, i.e., Eq. (4.6). Then Alice sends the particle \mathcal{P}_m to Bob,

Now let us show how to prevent the Trojan horse attacking strategy. Suppose the attacker lurks successfully a 'horse', Υ , in Bob's apparatus, then the ciphertext state takes,

$$|\Psi^{c}(\Upsilon)\rangle = C_{am} \left(\alpha^{c} |\Psi^{+}(\Upsilon)\rangle + \beta^{c'} |\psi^{+}(\Upsilon)\rangle\right) |\psi^{m}\rangle =$$

$$= \left(\tilde{\alpha}_{k}^{c} |0_{a}0_{b}(h_{\shortparallel})\rangle + \tilde{\beta}_{k}^{c} |0_{a} - {}_{b}(h_{?})\rangle\right) \otimes |\psi^{m}\rangle +$$

$$+ \left(\tilde{\alpha}_{k}^{c} |1_{a}1_{b}(h_{\perp})\rangle + \tilde{\beta}_{k}^{c} |1_{a} + {}_{b}(h_{?}')\rangle\right) \otimes X_{m} |\psi^{m}\rangle, \quad (4.7)$$

where $h_{?}$ and $h'_{?}$ denote the inconclusive feedback information. Although the key is a superposition state (see Eq. (4.5)), in each encrypting operation Alice and Bob only choose one state from $\{|\psi_{1}\rangle, |\psi_{2}\rangle\}$ as the key element. Accordingly, if the attacker pre-lurks one Trojan horse, e.g., Υ_{1} (for $\{|0\rangle, |1\rangle\}$), in Bob's apparatus, then another states, i.e., $\{|+\rangle, |-\rangle\}$ can not be recognized exactly. If the attacker employs two Trojan horses, e.g., 'robot horse' Υ_{1} and 'robot horse' Υ_{2} (for $\{|+\rangle, |-\rangle\}$), the attacker can find it impossible to get the useful feedback information. Because Alice and Bob's choices for the key are completely random, this makes it impossible for the Trojan horses Υ_{1} and Υ_{2} to follow completely the changes of the key elements. In other terms, because there are two pairs random bases, i.e., $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ in Alice's and Bob's apparatuses, it is impossible for the the attacker's 'horse' to recognize these bases. Subsequently, the 'horses' are blind and can not give correct feedback information. The security is the same as the BB84 protocol [3].

5. Remark

In the above we have analyzed the fragility of the quantum cryptographic algorithm against the Trojan horse strategy, where the EPR pair(s) are employed as a key. However, we here would like to stress that the quantum key distribution protocols which are implemented by making use of the EPR pair(s) do not suffer this kind of drawbacks. Since in the quantum key distribution the EPR pair carries initially no information. Especially the users's measurement for obtaining the final key is completely random. This random feature leads the Trojan horse employed in the above section to be of no use [4].

6. Conclusion

In this work, the fragility of the THAS on the quantum cryptographic algorithm implemented by the EPR pairs as the key has been analyzed in detail. It is found that any quantum cryptographic algorithm exploiting set of orthogonal states as the symmetrical key can not circumvent the THAS. To prevent this kind of attacking strategy we proposed a new approach which makes use of the non-orthogonal entangled states. The improvement scheme is robust to the THAS. In addition, the mechanism for the THAS on the quantum cryptography as well as the classic cryptography is also investigated. In any THAS the Trojan horse is very important.

Acknowledgement

This work was supported by the Alexander von Humboldt-Stiftung foundation (Grant no. IV CHN 1069575 STP) and the National Natural Science Foundation of China (Grant no. 60102001).

References

- [1] B. Schneier, Applied Cryptography: protocols, algorithms, and source code in C (John Wiley & Sons, Inc., 1994).
- [2] S. Wiesner, Sigact News. 15, 78, (1983).
- [3] C. H. Bennett, and G. Brassard. Advances in Cryptology: Proceedings of Crypto'84, August 1984, Springer-Verlag, 475 (1984).
- [4] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
- [5] C. H. Bennett et al., J. Crypto. 5, 3 (1992); W. T. Buttler et al., Phys. Rev. Lett. 84, 5652 (2000).
- [6] H.-K. Lo and H.F. Chau, Science, 283, 2050 (1999).
- [7] M. Hillery, V. Buzek and A. Berthiaume, Phys. Rev. A 59,1829 (1999); R. Cleve, D. Gottesman, H. -K. Lo, Phys. Rev. Lett. 83, 648 (1999).
- [8] P. W. Shor, and J. Preskill, Phys. Rev. Lett. 85, 441 (2000); D. S. Naik et al., ibid 84, 4733 (2000).

- [9] G. Zeng, and W. Zhang, Phys. Rev A 61, 032303 (2000).
- $[10]\,$ N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, arXiv: quant-ph/0101098, 19, Jan 2001.
- [11] J. Larsson, arXiv: quant-ph/0111073, 13 Nov 2001.
- [12] Y. Zhang, C. Li and G. Guo, Phys. Rev. A 64, 024302 (2001).
- [13] D.W. Leung, Quantum information and computation **2** no.1, (2001). See also arXiv: quant-ph/0012077, newest version, 9 Oct 2001.
- [14] A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A 59, 162 (1999).
- [15] W. K. Wooters and W. H. Zurek, Nature 299, 802 (1982).