Vol 14 No 11, November 2005
1009-1963/2005/14(11)/2164-06

Chinese Physics

© 2005 Chin. Phys. Soc.
and IOP Publishing Ltd

A realizable quantum encryption algorithm for qubits*

Zhou Nan-Run(周南润)† and Zeng Gui-Hua(曾贵华)

The State Key Laboratory on Fiber-Optic Local Area Networks and Advanced Optical Communication Systems, Electronic Engineering Department, Shanghai Jiaotong University, Shanghai 200030, China

(Received 15 October 2004; revised manuscript received 20 May 2005)

A realizable quantum encryption algorithm for qubits is presented by employing bit-wise quantum computation. System extension and bit-swapping are introduced into the encryption process, which makes the ciphertext space expanded greatly. The security of the proposed algorithm is analysed in detail and the schematic physical implementation is also provided. It is shown that the algorithm, which can prevent quantum attack strategy as well as classical attack strategy, is effective to protect qubits. Finally, we extend our algorithm to encrypt classical binary bits and quantum entanglements.

Keywords: quantum encryption algorithm, quantum computation, cryptography
PACC: 0365, 4250, 4230Q

1. Introduction

The strength of our current popular encryption systems is based on cryptographic keys and complex mathematics algorithms. By using a sufficiently long cryptographic key, a mathematical algorithm transfers (locks) plaintext into ciphertext in such a way as to make it computationally infeasible for a cryptanalyst to determine either the enciphered message or the underlying key. Classical cryptosystems come in two main classes depending on whether communicators, e.g. Alice and Bob use the same key. Asymmetrical systems, whose security is based on computational complexity, involve the use of different keys for encryption and decryption. Symmetrical ciphers require the use of a single key for both encryption and decryption. The Vernam algorithm (also called "one-time pad") belongs to this category.[1]

The rapid progress in quantum information theory poses a threat to classical cryptosystems, such as quantum factoring algorithm which can break the condition for many cryptographic protocols.[2] However, quantum cryptography[3−6] has been of particular interest since the initial proposal of unconditionally secure quantum key distribution protocol in 1984[7] and its experimental demonstration in 1992.[8] Recently, quantum cryptographic (encryption) algorithms have also been investigated extensively. Leung has investigated the quantum Vernam cipher using entanglement as the key to encrypt quantum information sent through an insecure quantum channel, and especially, followed that the quantum key can be reused securely.[9] Boykin and Roychowdhury have devised a quantum one-time pad using a secret-key shared between Alice and Bob in advance to control the X and Z gates applying to qubits and discussed the characterization and optimality of quantum one-time pads at length.[10] Through designing keys in the non-orthogonal quantum states, a quantum cryptographic algorithm to encrypt classical binary bits has been presented by Zeng.[11] Motivated by the method in Ref.[11], we has proposed a novel quantum encryption algorithm for classical binary information, which can be realized with current technology.[12] On the other hand, the attempts to construct quantum public-key cryptographic algorithms, or rather, quantum asymmetric-key cryptographic algorithms, have

*Project supported by the National Natural Science Foundation of China (Grant Nos 60472018 and 90104005) and by the Doctoral Programs Foundation of the Ministry of Education of China (Grant No 20020247063).
†Corresponding author. E-mail: znr21@sjtu.edu.cn

been made from different aspects.[13−15] In particular, Patrick Navez *et al* have developed a "quantum public key" scheme similar to the classical one for continuous variables, in which the q-private and q-public keys consist in each of the two entangled photon beams of squeezed light respectively. An analogue message is enciphered by modulating the phase of the beam sent in public, and the knowledge of the degree of non-classical correlation between the beam quadratures measured in private and in public allows only the receiver to decrypt the message.[15]

The goals of quantum encryption algorithms and classical encryption algorithms are consistent, i.e. to protect secret information or keep communications private. The difference between quantum and classic cryptographic algorithms is as follows: the former is based on quantum laws while the latter is based on pure mathematic principles. In quantum encryption algorithms, some are used to protect classical messages; the others aim at quantum messages. To our knowledge, most proposed algorithms are difficult to be implemented with current technology due to the problem of storing quantum states of long duration. It has to be said that almost all previously proposed quantum encryption algorithms do not make good use of the ingenious and mature methods used in the classical cryptography.

The purpose of the present paper is to design a realizable quantum encryption algorithm to protect qubits, each of which is a simplest quantum mechanical system and has a two-dimensional state space. We introduce the system extension, permutation, quantum error and H transformation into our algorithm. The new idea allows us to make the qubits confusable and undistinguishable and gives a larger ciphertext space to the eavesdroppers. Without loss of generality, we assume that the set of all possible quantum computations or operations Alice can choose from are known to everyone, involving Eve. The index of the exact operations performed by Alice and Bob on their qubits is the secret key shared between them at some point.

This paper is organized as follows. We give a detailed description of the realizable quantum encryption algorithm in Section 2, including encryption process, decryption process and physical realization. In Section 3, we analyse the security of the proposed algorithm from different aspects. Finally, we make a brief discussion and conclusion in Section 4.

2. Realizable quantum encryption algorithm

A qubit can be expressed as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, where α and β are complex numbers, although for many purposes not much is lost by thinking of them as real numbers. In the following, we will introduce our quantum encryption algorithm in detail, which involves four groups of keys during the process of encryption and decryption. The first three groups of keys are to disturb and confuse the secret messages. The fourth group of key is to make the ciphertext quantum states non-orthogonal. So if the fourth group of key is insecure, then the ciphertext states transmitted through the channel can be eavesdropped by the attacker. To guarantee the absolute security of the keys, it is advisable to employ quantum key distribution technology.[3]

2.1. Encryption process

Step 1 System extension. All previously presented quantum encryption algorithms do not involve this operation; however, system extension is a basic issue both in cryptography and in real-life physical systems. The goal of the system extension is to expand the ciphertext space. Suppose the ith element of the first group of key is k_{1i}, then we prepare the tensor product state

$$\begin{aligned}|\psi_{1i}^{\mathrm{C}}\rangle =& |k_{1i}\rangle|\psi_i\rangle = |k_{1i}\rangle \otimes |\psi_i\rangle \\ =& \alpha_i|k_{1i}0_{\mathrm{q}}\rangle + \beta_i|k_{1i}1_{\mathrm{q}}\rangle, \end{aligned} \tag{1}$$

where q denotes the quantum bits in order to distinguish them from the key bits. So after the extension of the system, one original state corresponds to two states: $\alpha_i|00_{\mathrm{q}}\rangle + \beta_i|01_{\mathrm{q}}\rangle$ when $k_{1i} = 0$, and $\alpha_i|10_{\mathrm{q}}\rangle + \beta_i|11_{\mathrm{q}}\rangle$ when $k_{1i} = 1$. It is worth pointing out that the state in Eq.(1) is not entangled since it is expressed in the form of a tensor product.

Step 2 Permutation. As is well known, permutation is a fundamental means in classical cryptography, and most real popular cryptosystems unavoidably involve it. However, permutation has seldom been seen in quantum cryptography although it shows up frequently in quantum computation and can be realized easily. This step will extend the ciphertext space and confuse the attackers. Under the control of the ith element k_{2i} of the second group of key k_2, permuting two qubits can be implemented by the bit-swapping circuit, which is shown in Fig.1. The function of the bit-swapping circuit can be written as $|A\rangle|B\rangle \to |B\rangle|A\rangle$

and its matrix representation is

$$U_{\text{swap}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2}$$

After permutation, the possible quantum state can be written as

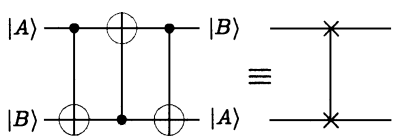


Fig.1. Circuit swapping two qubits.

$$\begin{aligned} |\psi_{2i}^{\text{C}}\rangle =& \delta_{0,k_{2i}} (\alpha_i |k_{1i}0_{\text{q}}\rangle + \beta_i |k_{1i}1_{\text{q}}\rangle) \\ & + \delta_{1,k_{2i}} (\alpha_i |0_{\text{q}}k_{1i}\rangle + \beta_i |1_{\text{q}}k_{1i}\rangle) \\ =& U_{\text{swap}}^{k_{2i}} |\psi_{1i}^{\text{C}}\rangle . \end{aligned} \tag{3}$$

From Eq.(3) we can derive all possible states for different k_{1i} and k_{2i}, i.e. $\alpha_i |00_{\text{q}}\rangle + \beta_i |01_{\text{q}}\rangle$, $\alpha_i |10_{\text{q}}\rangle + \beta_i |11_{\text{q}}\rangle$, $\alpha_i |0_{\text{q}}0\rangle + \beta_i |1_{\text{q}}0\rangle$ and $\alpha_i |0_{\text{q}}1\rangle + \beta_i |1_{\text{q}}1\rangle$.

Step 3 Quantum error. In order to disturb the quantum information further, Alice can insert some errors into it. For a state in the form of $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, all errors can fall into four types, such as I, X, Z and Y, which represent no error, bit flip, phase flip, and both bit flip and phase flip, respectively. I, X, Z and Y are applied to the quantum state if their respective classical control bits are 00, 01, 10 and 11 according to the key element k_{3i}. The resulting state is given by

$$\begin{aligned} |\psi_{3i}^{\text{C}}\rangle =& (\delta_{00,k_{3i}} I + \delta_{01,k_{3i}} X + \delta_{10,k_{3i}} Z + \delta_{11,k_{3i}} Y) \\ & [\delta_{0,k_{2i}} (\alpha_i |k_{1i}0_{\text{q}}\rangle + \beta_i |k_{1i}1_{\text{q}}\rangle) \\ & + \delta_{1,k_{2i}} (\alpha_i |0_{\text{q}}k_{1i}\rangle + \beta_i |1_{\text{q}}k_{1i}\rangle)], \end{aligned} \tag{4}$$

or

$$\begin{aligned} |\psi_{3i}^{\text{C}}\rangle =& X^{\delta_{01,k_{3i}}} Z^{\delta_{10,k_{3i}}} Y^{\delta_{11,k_{3i}}} |\psi_{2i}^{\text{C}}\rangle \\ =& X^{\delta_{01,k_{3i}}} Z^{\delta_{10,k_{3i}}} Y^{\delta_{11,k_{3i}}} U_{\text{swap}}^{k_{2i}} |\psi_{1i}^{\text{C}}\rangle. \end{aligned} \tag{5}$$

From Eq.(4) or Eq.(5), any ciphertext state in step 2 corresponds to four different states, so one can obtain 16 different states for one qubit according to different keys.

Step 4 H transformation. Alice applies H gate to the states derived from Step 3 under the control of the key element k_{4i}, thereby obtaining the non-orthogonal ciphertext states. The function of H gate can be written as

$$H = \frac{1}{\sqrt{2}} [(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|], \tag{6}$$

or expressed in the matrix form

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} (X + Z). \tag{7}$$

It is easy to obtain $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Therefore, the final ciphertext state is

$$\begin{aligned} |\psi_{4i}^{\text{C}}\rangle =& (\delta_{0,k_{4i}} + \delta_{1,k_{4i}} H)(\delta_{00,k_{3i}} I + \delta_{01,k_{3i}} X \\ & + \delta_{10,k_{3i}} Z + \delta_{11,k_{3i}} Y) \\ & \times [\delta_{0,k_{2i}} (\alpha_i |k_{1i}0_{\text{q}}\rangle + \beta_i |k_{1i}1_{\text{q}}\rangle) \\ & + \delta_{1,k_{2i}} (\alpha_i |0_{\text{q}}k_{1i}\rangle + \beta_i |1_{\text{q}}k_{1i}\rangle)], \end{aligned} \tag{8}$$

or

$$\begin{aligned} |\psi_{4i}^{\text{C}}\rangle =& H^{\delta_{1,k_{4i}}} |\psi_{3i}^{\text{C}}\rangle \\ =& H^{\delta_{1,k_{4i}}} X^{\delta_{01,k_{3i}}} Z^{\delta_{10,k_{3i}}} Y^{\delta_{11,k_{3i}}} U_{\text{swap}}^{k_{2i}} |\psi_{1i}^{\text{C}}\rangle. \end{aligned} \tag{9}$$

One can acquire 32 different states from Eq.(8) or Eq.(9) according to different keys. The possible states in Step 4 are non-orthogonal, which makes the states undistinguishable for the eavesdropper. For n qubits, the ciphertext can be written as

$$|\psi_{\text{C}}\rangle = |\psi_4^{\text{C}}\rangle = |\psi_{4n}^{\text{C}}\rangle \otimes ... |\psi_{4i}^{\text{C}}\rangle \otimes ... |\psi_{42}^{\text{C}}\rangle \otimes |\psi_{41}^{\text{C}}\rangle \tag{10}$$

After executing the four steps of operations, the encryption process is finished. It can be seen in Section 3 that the security would be intimidated without performing the H transformation.

2.2. Decryption process

Note that the set of operations that Alice performs are reversible and, hence, unitary. The sequence of decryption process is right inverse of the sequence of encryption process. Because the above quantum operations are unitary, the decryption operations can be executed easily under the guidance of the pre-shared keys. The decryption process is as follows.

Firstly, Bob decrypts the state $|\psi_4^{\text{C}}\rangle$ upon receiving it under the control of the key k_4. If k_{4i} is equal to 1, Bob applies H gate to $|\psi_{4i}^{\text{C}}\rangle$, or else Bob keeps it alone. Thus Bob obtains the state $|\psi_3^{\text{C}}\rangle$.

Secondly, Bob unlocks the state $|\psi_3^{\text{C}}\rangle$ according to the key k_3. If k_{3i} is 00, Bob lets $|\psi_{3i}^{\text{C}}\rangle$ alone, or if k_{3i} is 01, he applies X gate to $|\psi_{3i}^{\text{C}}\rangle$, or if k_{3i} is 10, he

applies Z gate to $|\psi_{3i}^{\mathrm{C}}\rangle$, or else if k_{3i} is 11, he applies Y gate to $|\psi_{3i}^{\mathrm{C}}\rangle$. After this process, Bob obtains the state $|\psi_2^{\mathrm{C}}\rangle$.

Thirdly, Bob continues to swap the qubits in $|\psi_2^{\mathrm{C}}\rangle$. When the key element k_{2i} is equal to 1, Bob swaps the qubits in $|\psi_{2i}^{\mathrm{C}}\rangle$, otherwise, he leaves it alone. After the above operations, Bob obtains the tensor product state as follows

$$|\psi_{1i}^{\mathrm{C}}\rangle = U_{\mathrm{swap}}^{k_{2i}} X^{\delta_{01,k_{3i}}} Z^{\delta_{10,k_{3i}}} Y^{\delta_{11,k_{3i}}} H^{\delta_{1,k_{4i}}} |\psi_{4i}^{\mathrm{C}}\rangle. \tag{11}$$

Finally, Bob separates the tensor product state and then obtains the anticipated qubits. Thus, Bob achieves the anticipated quantum state sent from Alice.

Without the guidance of the keys, Bob's operations will necessarily modify the ciphertext and he acquires no useful results.

2.3. Physical implementation

So far, we have provided a quantum encryption algorithm based on bit-wise quantum computation. Now we show the physical realization of the proposed algorithm. The physical implementation of the proposed algorithm is shown in Fig.2. In the figure, S_1 is a quantum switch under the control of k_2. When the key k_{2i} is 0, S_1 switches onto 1, otherwise S_1 switches onto 2. For Alice, i.e. the encryption procedure, time runs from left to right, while for Bob, i.e. the decryption procedure, time runs right to left. X, Z, Y and H are applied to the quantum state if their respective classical control bits are 01, 10, 11 and 1.

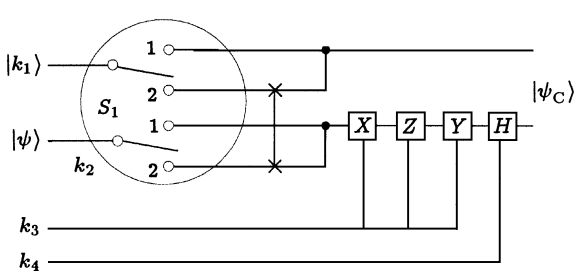


Fig.2. Schematic of physical implementation for the quantum encryption algorithm.

From Fig.2, one can see that the quantum encryption algorithm only involves simple quantum logic gates, which can be realized physically, for example, modulation and demodulation between two dim laser-pulses. Furthermore, the keys adopted while encrypting are all classical. The ciphertext states are directly sent to Bob through an optical fibre channel or via air after the encryption process is finished by Alice. Upon receiving the ciphertext state, Bob decrypts it in time and it is not necessary to store the quantum states. Most important of all, the algorithm can be realized with current technology and may have wide use with the quantum error-correcting technology to enhance its performance.

3. Security analyses

To analyse the security of the proposed algorithm, we firstly introduce Theorem 1, on which Theorem 2 is based. Then we discuss the ciphertext-only attack, known-plaintext attack and chosen-plaintext attack in Theorem 3. Finally we analyse the aspect of the Trojan horse attack strategy.[16]

Theorem 1 Unitary operation cannot alter the density matrix of quantum states.

Proof Assume U and $|\psi\rangle$ to be a unitary operation and a quantum state, if $|\psi\rangle\langle\psi| = I$, then

$$U|\psi\rangle\langle\psi|U^{+} = UIU^{+} = I. \tag{12}$$

Theorem 2 Ciphertext state shows no plaintext information.

Let $|\psi_{1i}\rangle$ be the linear combinations of all the possible quantum states with equal probability in the ciphertext set C_t (t=1, 2, 3, 4), which corresponds to the ith qubit. For example, $|\psi_{1i}\rangle = \frac{1}{2}(\alpha_i|00_{\mathrm{q}}\rangle + \beta_i|01_{\mathrm{q}}\rangle + \alpha_i|10_{\mathrm{q}}\rangle + \beta_i|11_{\mathrm{q}}\rangle)$. One can calculate the density matrix

$$|\psi_{1i}\rangle\langle\psi_{1i}| = I. \tag{13}$$

Since all encryption operations are unitary, it follows from Theorem 1 that the ciphertext is homogeneous and the proposed algorithm is perfect privacy. Due to

$$\begin{aligned}\langle\psi_{4i}|\psi_{4i}\rangle =& \frac{1}{64}[(6+2\sqrt{2}) + (1+\sqrt{2})\alpha_i\beta_i \\ &+ (4+2\sqrt{2})(\alpha_i^2 - \beta_i^2)],\end{aligned} \tag{14}$$

different ciphertext states are undistinguishable according to the no-cloning theorem.[17] The no-cloning theorem is the basic idea from which one can prove that the transmission of information encoded by non-orthogonal quantum states is secure against an eavesdropper (Eve). The impossibility of reproduction prevents Eve from having access to any quantum state without disturbing or modifying it. Such a disturbance or modification makes her results random and meaningless. Finally, if we do not reuse the used keys, the ciphertext states are random and independent of qubits when the key is random and unknown.

Theorem 3 The ciphertext-only attack, known-plaintext attack and chosen-plaintext attack are impossible.

In classical cryptography, Eve can duplicate the ciphertext without modifying it through intercepting the channel or illegitimately accessing to the ciphertext bank, thus she can attempt to decrypt it time after time. While in quantum encryption algorithm, the information is encoded by non-orthogonal quantum states, so Eve can perform one set of operations on each enciphered state just one time. Since she does not know the key, her measured results must be random. From this point of view, one can see that the ciphertext-only attack strategy is impossible. Likewise, from the encryption process of our algorithm, the known-plaintext and chosen-plaintext attack strategies are unfeasible because Eve could not know without the key what the ciphertext corresponding to the known-plaintext is. This property results from the uncertainty principle in quantum mechanics.

Theorem 4 The Trojan horse attack strategy can not obtain useful information.

The Trojan horse attack strategy (THAS) may be generated from the drawback of construction of the system (e.g. device, program, algorithm or protocol). When a Trojan horse can be lurked in a system without easy detection, attackers can make use of this kind of strategy to obtain useful information and then break the system. This attack strategy is not only popular in classical cryptography but also available in the recently proposed quantum cryptography.[16,18,19]

From Refs.[11,12], due to the non-orthogonality of different ciphertext states, the Trojan horse will feedback no meaningful information even if the attacker has pre-lurked a Trojan horse in the encryption or decryption apparatus, therefore our algorithm can counteract the Trojan horse attack strategy. For example, the Trojan horse will feedback available information 0 and 1 when the ciphertext is in state $|0\rangle$ or $|1\rangle$. However when the ciphertext is in states $|+\rangle$ or $|-\rangle$, there is no determined feedback information.

The security is intrinsic to the non-orthogonal quantum cipher-text, rather than due to using classical bits or something else (qubits or entanglements) as the key. Here we choose classical bits as the key in order to make our algorithm implemented with current technology. To lessen the burden of key management, we can recycle the first three groups of keys. As long as the fourth group of key is secure, the above security analyses are still valid. If there is an eavesdropper, Bob's result must be obscure. Therefore, the presence of an attacker can be detected. If there is no eavesdropper, Alice and Bob can reuse the shared key, therefore the proposed algorithm takes the form of block encryption.

4. Discussion and conclusion

The proposed algorithm can be applied to encrypting binary classical bits with minor modification. We denote binary classical bits 0 and 1 by single qubits $|0\rangle$ and $|1\rangle$, respectively. Recalling the equations $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\alpha|^2 + |\beta|^2 = 1$, one knows that classical bit 0 corresponds to the quantum state where $|\alpha|^2 = 1$, and that classical bit 1 corresponds to the quantum state where $|\beta|^2 = 1$. Thus, the encryption of binary classical bits can be treated as a particular case of the quantum context, however, its physical implementation will be simpler, and the number of key bits used during encryption and decryption cuts down greatly.

Entanglement, an important resource for quantum information processing, is one of the most prominent nonclassical properties in quantum theory. Entanglement can exhibit a nonlocal correlation between quantum systems that have no classical interpretation. For an arbitrary entanglement state $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$, one can encrypt it in the same way with minor modification to its physical implementation.

In summary, we have proposed a quantum encryption algorithm in order to protect qubits by introducing quantum computation into quantum cryptography. The security of the algorithm is discussed at length and a schematic implementation diagram is given. It is shown that the algorithm, which can prevent quantum attack strategy as well as classical attack strategy, is effective to protect qubits, and can be extended to encrypt binary classical bits and entanglement states. Therefore our quantum encryption algorithm has a good extension and potential applications.

References

[1] Schneier B 1994 *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (New York: Wiley)

[2] Shor P W 1994 Proc. 35th *Annual Symposium on Foundation of Computer Science* (Los Alamitos CA: IEEE Computer Society Press) p124

[3] Zhou N, Zeng G and Xiong J 2004 *Electron. Lett.* **40** 1149

[4] Wu X S 2004 *Chin. Phys.* **13** 173

[5] Liang C, Fu D H, Liang B *et al* 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese)

[6] Miao E L, Mo X F, Gui Y Z *et al* 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese)

[7] Bennett C H and Brassard G 1984 *Advances in Cryptology: Proceedings of Crypto'84* 475 (Berlin: Springer)

[8] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Crypto.* **5** 3

[9] Leung D W 2001 *Quantum Inform. Comp.* **1** 1

[10] Boykin P O and Roychowdhury V 2003 *Phys. Rev.* A **67** 042317

[11] Zeng G H 2004 *Chin. J. Electronics* **13** 651

[12] Zhou N R and Zeng G H 2004 *Progress on Cryptography—25 Years of Cryptography in China* The Kluwer International Series in Engineering and Computer Science (Boston: Kluwer) p195

[13] Tatsuaki Okamoto, Keisuke Tanaka and Shigenori Vchiyama 2000 *Proceedings of Crypto 2000 Lecture Notes In Computer Science* (Berlin: Springer) p147

[14] Brown M S 2004 quant-ph/0404061

[15] Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimure *et al* 2004 quant-ph/0403069

[16] Gisin N, Ribcrdy G, Tittel W *et al* 2002 *Rev. Mod. Phys.* **74** 145

[17] Wooters W K and Zurek W H 1982 *Nature* **299** 802

[18] Wiesner S 1983 *Sigact News* **15** 78

[19] Lo H K and Chau H F 1999 *Science* **283** 2050