A SECURE QUANTUM COMMUNICATION PROTOCOL USING INSECURE PUBLIC CHANNELS

I-Ming Tsai[1], Chia-Mu Yu[2], Wei-Ting Tu[1], and Sy-Yen Kuo[1]
[1]Department of Electrical Engineering; [2]Graduate Institute of Computer Science and Information Engineering; National Taiwan University, No.1, Sec. 4, Roosevelt Road, Taipei, 106, Taiwan

Abstract: Due to the discovery of Shor's algorithm[1], many classical crypto-systems based on the hardness of solving discrete log and factoring problem are theoretically broken in the presence of quantum computers. This means that some of the classical secret communication protocols are no longer secure and hence motivate us to find other secure crypto-systems. In this paper, we present a new quantum communication protocol which allows two parties, Alice and Bob, to exchange classical messages securely. Eavesdroppers are not able to decrypt the secret messages and will be detected if they do exist. Unlike classical crypto-systems, the security of this protocol is not based on the hardness of any unproven mathematic or algorithmic problem. Instead, it is based on the laws of nature.

Key words: Quantum Cryptography; Encrypted Communication; Quantum Entanglement

1. INTRODUCTION

Quantum information science is a highly interdisciplinary field of research and hence has applications in nearly every field of computer science and electrical engineering. Cryptography, most notably key distribution, is one example. Classical cryptography enables two parties, Alice and Bob, to exchange confidential messages such that the messages are illegible to any unauthorized third party. The problem is that it is difficult to distribute the

secret key securely through a classical channel. This is known as the key distribution problem. Classical key distribution protocols based on the hardness of mathematical or algorithmic problems[2,3] are conditionally secure *i.e.* theoretically insecure. However, quantum cryptography allows a number of applications that are not possible classically. An example is the Quantum Key Distribution (QKD) protocol -- a protocol dealing with secure key distribution using quantum mechanics.

Theoretical study and physical implementations of QKD have been developed rapidly after Bennett and Brassard proposed the standard BB84 protocol[4]. Basically, QKD schemes can be categorized into two classes -- non-deterministic QKD and deterministic QKD. For non-deterministic QKD, the sender and the receiver have no control over what bit string is used as the key. Typical non-deterministic QKD schemes include BB84, E91[5] and B92[6] protocols. In contrast, in a deterministic scheme, the sender and receiver have a total control of what bit string is used. This is actually, in classical cryptography terms, a secure communication, or an encryption/decryption process[7-10].

A secure communication protocol allows the sender (Alice) and the receiver (Bob) to exchange messages securely without running the risk of being decrypted by an eavesdropper (Eve). As a secure communication protocol, two requirements must be satisfied. First, upon a successful transmission process, the secret messages shall be able to be read out as its original form by the legitimate receiver. Second, in the presence of an eavesdropper, the encrypted message shall give her absolutely no information even if she may have total control of the channel. In the following sections, we present a protocol which not only fulfills these two requirements, but also can detect the eavesdroppers, if they do exist.

2. BACKGROUND

The state of a single quantum bit can be written as a linear combination of two states in a two-dimensional complex vector space as

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

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. The two orthonormal states $|0\rangle$ and $|1\rangle$ forms a computational basis of the system and the contribution of each basis state to the overall state (α and β in this case) is called the probability amplitude. According to quantum mechanics, when the system is measured, the state *collapses* to one of the basis states

($|0\rangle$ or $|1\rangle$). The probability of collapsing to a particular basis state is directly proportional to the square of the probability amplitude associated with it. More specifically, when a measurement is performed on a quantum state, the probability of getting a result of $|0\rangle$ is $|\alpha|^2$ and the probability of getting a result of $|1\rangle$ is $|\beta|^2$. Obviously, due to the rule of probability, $|\alpha|^2 + |\beta|^2 = 1$. The symbol for a quantum measurement is shown in Fig.1(a).

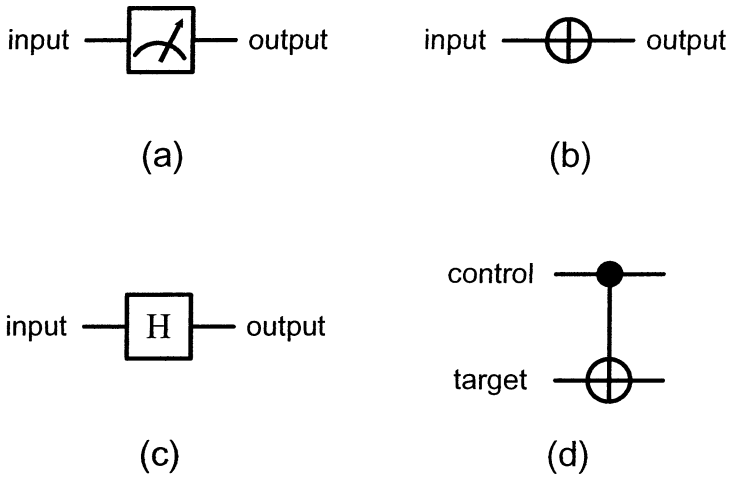

Figure 1. The symbols for quantum measurement and various quantum gates

The state described above exhibits a unique phenomenon called quantum *superposition*. When a particle is in such a state, it has a part corresponding to $|0\rangle$ and a part corresponding to $|1\rangle$, at the same time. However, when a measurement is performed, it collapses to one of the states in the basis (eigenstates). To distinguish the above system from a classical binary digit, such a unit is called a quantum binary digit, or *qubit*. An easy way to describe a qubit is to use column matrices. For example, Eq. (1) is equivalent to the notation

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{2}$$

Similar to classical bits manipulated by classical logic gates, a qubit can be manipulated using *quantum gates*. Like a qubit, a quantum gate can also be written in matrix form. In its matrix form, a quantum gate G must be unitary, *i.e.* satisfying $GG^+ = G^+G = I$, where G^+ stands for the

transpose conjugate of G. This is because any such gates can be pictorially described as a rotation on the Bloch sphere. When a qubit goes through some quantum gates, the state vector is rotated to another direction. An example of quantum gate is the quantum **NOT** gate, which has the matrix representation of

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3}$$

Using the matrix form, the new state after a quantum **NOT** gate can be calculated using matrix multiplication. For example, when a qubit $|\alpha|^2 + |\beta|^2 = 1$ goes through a quantum **NOT** gate, the state changes to

$$|\psi'\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}. \tag{4}$$

The symbol for a quantum **NOT** gate is shown in Fig.1(b). Another important quantum gate is the **HADAMARD (H)** gate. The matrix form of a **HADAMARD** gate is

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{5}$$

and is able to make the following state changes:

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

$$H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{7}$$

The symbol for a **HADAMARD** gate is shown in Fig.1(c).

The space of a multi-qubit system can be modeled by the tensor product of each individual space. For example, a two-qubit state is a linear combination of four basis states:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{8}$$

with α, β, γ, δ complex numbers and $|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1$. Similar to the single qubit case, a two-qubit system can be represented using a 4×1 column matrix and a two-qubit gate can be represented using a 4×4 matrix. An example of two-qubit gate is the **CONTROL-NOT (CN)** gate, as shown in Fig. 1(d). A **CN** gate consists of one *control* bit x and one *target* bit y. The target qubit will be inverted only when the control qubit is $|1\rangle$. Assuming x is the control bit, the gate can be written as **CN** $(|x,y\rangle)=|x,x\oplus y\rangle$, where $\oplus$ denotes exclusive-or. This actually performs a permutation on the basis as follows: $|00\rangle\rightarrow|00\rangle$, $|01\rangle\rightarrow|01\rangle$, $|10\rangle\rightarrow|11\rangle$, and $|11\rangle\rightarrow|10\rangle$. In column matrix, this is equivalent to

$$|\psi'\rangle=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\\\gamma\\\delta\end{pmatrix}=\begin{pmatrix}\alpha\\\beta\\\delta\\\gamma\end{pmatrix}. \tag{9}$$

An interesting phenomenon in quantum mechanics is *entanglement.* Imagine that Alice and Bob share a two-qubit system in the state

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{ab}, \tag{10}$$

where a and b denote Alice and Bob respectively. According to quantum mechanics, if Alice takes a measurement on qubit a, the state of the qubit will collapse to $|0\rangle$ with a probability of $\frac{1}{2}$. Moreover, Alice immediately knows that the state of the other qubit (qubit b) must be $|0\rangle$. In other words, once the measurement result of one qubit is decided, the state of the other one is perfectly correlated and can be instantaneously decided, no matter how far away Alice and Bob are separated. A similar result happens if the result of Alice's measurement is $|1\rangle$. This non-classical correlation among multiple quantum systems is called quantum entanglement, because they can not be written as separable states and are considered to be entangled. Studies of different types of entanglement and their applications are an important issue in quantum information science.

3. ENCRYPTED COMMUNICATION PROTOCOL

The proposed protocol uses one entangled qubit pair to transmit one encrypted classical bit, then an n-bit classical message can be transmitted

bit-by-bit via this protocol. At the end of the transmission, an error checking process is employed to check the integrity of the whole message.

3.1 Resource requirement

In this paper we assume Eve has unlimited technological and computational power. She can perform any operation on the transmitting qubit as long as it is allowed by the laws of nature. Under these circumstances, the propose protocol can protect both the privacy and integrity of the message using a classical public channel and a quantum channel. The natures of these channels are described in the following paragraphs.

A classical channel is a communication path that can be used to transmit classical information from a sender to a receiver. For example, an optical fiber which allows Alice to send her voice to Bob is a typical classical channel. Depending on whether the channel is readable or writable by an unauthorized third party, classical channels can be further categorized into classical private channels and classical public channels.

A classical private channel is a channel, together with some appropriate mechanisms, which are capable of maintaining the privacy and integrity of the messages transmitted via that channel. The term privacy refers to the fact that the data carried in the channel cannot be read or revealed by anyone without authorization. It involves mainly data encryption algorithms and secret keys. An encryption mechanism, together with a secret key, can be used to translate the message into a form that is unreadable without the secret key. The term integrity means the message from the source can not be either accidentally or maliciously modified, altered, or destroyed. In other words, the messages exchanged between Alice and Bob are identically maintained during the transmission process.

As a contrast, a classical public channel is a classical channel that maintains only the data integrity, regardless of the privacy. In other words, a classical public channel can be used to transmit classical information from Alice to Bob without being modified by eavesdroppers. However, anyone, including eavesdroppers, can read the original message. Radio broadcasting in a non-jamming environment is an example of a classical public channel. In general, a classical public channel is a weaker assumption compared to a classical private channel.

A quantum channel is a communication channel which can be used to transmit quantum information from a sender to a receiver, as opposed to a classical channel transmitting only classical information. In other words, a quantum channel can be used to transmit a quantum state as described in Eq. (1), from the sender to the receiver. An example of quantum channels is an

optical fiber that can be used to transmit and maintain the polarization of photons.

3.2 Bit encryption protocol

In the following paragraphs, we give the specific steps and associated examples of the encrypted quantum communication protocol. All the steps are illustrated in Fig. 2.

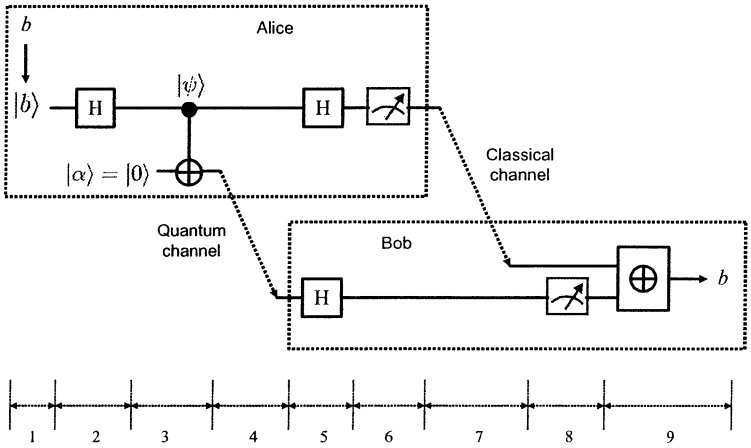

Figure 2. The encrypted quantum communication protocol with each step indicated

1. Assuming Alice has a classical secret bit $b \in \{0,1\}$ which she wants to send to Bob. To do this, Alice encodes her classical secret bit b into a quantum state $|0\rangle$ in case $b = 0$, or $|1\rangle$ in case $b = 1$.
2. Then Alice applies a **HADAMARD** gate on $|b\rangle$ to get a quantum state $|\psi\rangle$. Depending on the classical secret bit, the state will be

$$|\psi\rangle = H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{11}$$

if $b = 0$, or

$$|\psi\rangle = H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{12}$$

in case $b = 1$.

3. Alice then prepares an ancillary qubit $|\alpha\rangle = |0\rangle$ and applies a **CONTROL-NOT** gate $\mathbf{CN}(|\psi\rangle, |\alpha\rangle)$. The notation $\mathbf{CN}(|\psi\rangle, |\alpha\rangle)$ stands for a **CONTROL-NOT** gate with $|\psi\rangle$ as the control bit and $|\alpha\rangle$ as the target bit. This creates an entanglement between $|\psi\rangle$ and $|\alpha\rangle$, since

$$CN\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_{\psi}, |0\rangle_{\alpha}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\psi\alpha} \tag{13}$$

if $b = 0$, or

$$CN\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_{\psi}, |0\rangle_{\alpha}\right) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{\psi\alpha} \tag{14}$$

in case $b = 1$. The subscript ψ and α denote the order of the qubits.

4. Alice sends qubit $|\alpha\rangle$ to Bob through the quantum channel. After Bob gets qubit $|\alpha\rangle$, he tells Alice through the classical public channel that he has received the qubit.
5. Both Alice and Bob apply **HADAMARD** gates to their own qubits. If $b = 0$, this gives

$$\begin{aligned} & H \otimes H\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\psi\alpha}\right) \\ &= \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\psi\alpha} \end{aligned} \tag{15}$$

However, in case $b = 1$, it gives

$$\begin{aligned} & H \otimes H\left(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{\psi\alpha}\right) \\ &= \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle + |1\rangle}{\sqrt{2}} - \frac{|0\rangle - |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{\psi\alpha} \end{aligned} \tag{16}$$

6. Alice takes a measurement of her qubit with respect to $|0\rangle$ and $|1\rangle$. According to Eq.(15) and Eq.(16), she will get a result of either $|p\rangle = |0\rangle$ or $|p\rangle = |1\rangle$ with a probability of ½. Alice then translates the result $|p\rangle$ into the corresponding classical bit: $p = 0$ if $|p\rangle = |0\rangle$ or $p = 1$ if $|p\rangle = |1\rangle$.
7. Alice sends the result p to Bob through the classical public channel.
8. Similarly, Bob takes a measurement of his qubit with respect to $|0\rangle$ and $|1\rangle$. According to Eq.(15) and Eq.(16), he will get a result of either $|q\rangle = |0\rangle$ or $|q\rangle = |1\rangle$ with a probability of ½. Bob then translates the result $|q\rangle$ into the corresponding classical bit: $q = 0$ if $|q\rangle = |0\rangle$ or $q = 1$ if $|q\rangle = |1\rangle$.
9. Unlike Alice, who sends her result through the classical public channel, Bob keeps the result secret and performs

$$b = p \oplus q \tag{14}$$

to recover the classical message b.

3.3 Protocol description

In the protocol described above, the information of the secret bit b is encoded as the phase of the entanglement state after Alice applies the **CONTROL-NOT** gate. This can be seen from the phase (plus vs. minus sign) in Eq.(13) and Eq.(14). If Alice sends only one qubit to Bob, the information is shared between them and can not be retrieved via any local operation. In other words, the only qubit sent by Alice via the quantum channel does not contain enough information to recover the secret bit b.

To recover the original secret bit, either a joint operation (for example, a **CONTROL-NOT** gate) or classical message exchange between the two parties is necessary. In this protocol, Alice does not send both qubits to Bob, she keeps one qubit in her hand to avoid a joint operation performed by the eavesdropper. Instead, two **HADAMARD** gates are performed by Alice and Bob separately. Since after these operations, the measurement results of these qubits become perfectly correlated (as in Eq.(15) and Eq.(16)) and the secret bit can be deduced by a simple calculation over the two classical bits according to Eq.(17). However, one of the two classical bits is now in Bob's hand. All Alice has to do is to reveal her classical bit p to Bob. To do this, Alice can send her classical bit p to Bob via the classical public channel. Note that the result announced by Alice is completely random, so it does not contain enough information for Eve to deduce the secret bit. At the end of the protocol, Bob can count the number of '1's and decrypt the secret bit

according to Eq.(17). If the number of '1's is even, the message b is 0. On the other hand, if the number of '1's is odd, the message b is 1.

4. ANALYSIS OF THE PROTOCOL

In this section, we assume the existence of an eavesdropper and show that the protocol is secure as long as the qubit sent by Alice reaches Bob.

4.1 Analysis on eavesdropping

As described previously, step (1)-(3) are performed by Alice locally. Basically these steps prepare an entanglement state depending on the secret bit b. The only chance Eve can get information from the channel is step (4) and (7). A typical attack is shown in Fig. 3.

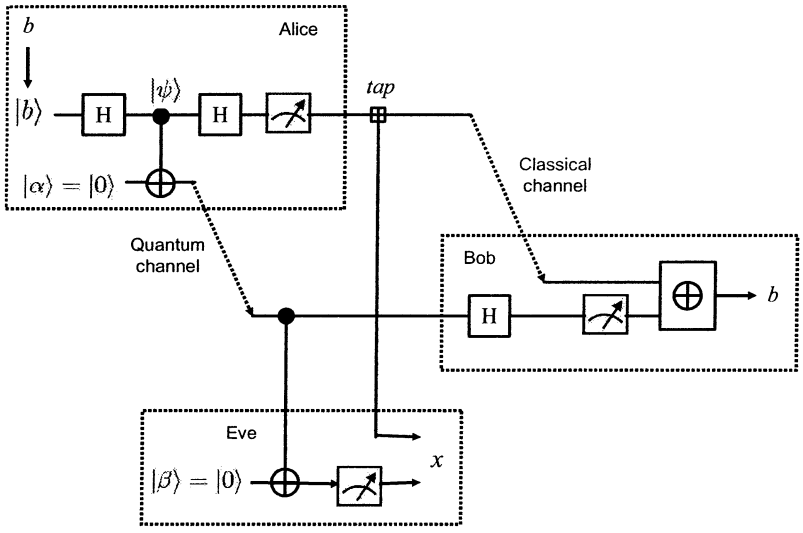

Figure 3. The encrypted quantum communication protocol with eavesdroppers

Since step (4) is the only chance for Eve to attack the quantum channel, we discuss this first. As Eve has the capability of performing quantum gates to that qubit, without lose of generality, we assume that Eve prepares an ancillary qubit $\beta = |0\rangle$ and performs a $\mathbf{CN}(\alpha, \beta)$ to get some information from the flying qubit.

The state is now

$$CN_{\alpha\beta}\left(\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{\psi\alpha},|0\rangle_{\beta}\right)=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{\psi\alpha\beta} \tag{18}$$

for $b=0$, and

$$CN_{\alpha\beta}\left(\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{\psi\alpha},|0\rangle_{\beta}\right)=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{\psi\alpha\beta} \tag{19}$$

in case $b=1$. The notation $CN_{\alpha\beta}$ stands for a **CN** gate with α as the control and β as the target. In the following steps, if Eve performs a **HADAMARD** gate as Alice and Bob do in step (5), the state will evolve as follows.

1. If $b=0$, it gives

$$\begin{aligned}&H\otimes H\otimes H\left(\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{\psi\alpha\beta}\right)\\&=\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\&=\frac{1}{2}(|000\rangle+|011\rangle+|101\rangle+|110\rangle)_{\psi\alpha\beta}\end{aligned} \tag{20}$$

2. if $b=1$, it becomes

$$\begin{aligned}&H\otimes H\otimes H\left(\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{\psi\alpha\beta}\right)\\&=\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}-\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\&=\frac{1}{2}(|001\rangle+|010\rangle+|100\rangle+|111\rangle)_{\psi\alpha\beta}\end{aligned} \tag{21}$$

From Eq.(20) and Eq.(21), we see this still makes the total number of '1's even in case $b=0$ and odd in case $b=1$. After Alice announces her measurement result in step (7), if Bob knew the result of all three qubits he could still count the total number of '1's to deduce the secret bit.

Assuming the secret bit $b = 0$, the total number of '1's is even ($|000\rangle, |011\rangle, |101\rangle, |110\rangle$). However, there is a probability of ½ ($|011\rangle$ and $|101\rangle$) that Eve has a '1' in her hand. The silent eavesdropper has no way to get rid of this bit and push this information back to Alice or Bob. This makes the total number of '1's belonging to Alice and Bob odd and will hence flip the secret bit. As for Eve's qubit, it carries no information because it can be either $|0\rangle$ or $|1\rangle$, each with a probability of ½. In summary, the intrusion introduces an error but gives Eve no information. Similar analysis holds for other unitary operations performed by Eve.

Since the existence of eavesdropping will inevitably introduce errors, Alice and Bob can detect the intrusion by appending an error checking code in the message. A simple error checking algorithm that allows two parties to perform message encryption is shown in the following section.

4.2 Message encryption protocol

The bit encryption protocol allows two parties to transmit one classical bit each time. The result is either a successful transmission or a bit-flip induced by eavesdropping. With the bit encryption protocol described above, an n-bit message can be sent using the following procedure to protect its integrity.

1. Alice sends the message bit-by-bit using the bit encryption protocol.
2. They negotiate publicly to decide a hash function.
3. Alice sends the hash result, bit-by-bit, using the bit encryption protocol.
4. Bob gets both the message and hash result. He can check the integrity of the message using the hash. If they don't match, the message is corrupted. Otherwise, the message is valid.

4.3 Channel analysis

In this protocol, two communication channels are used. One is a classical public channel; the other is a quantum channel. As described previously, the classical channel is a public channel, so the data is public readable. However, we did not discuss whether the channel can be publicly writable. Actually, if the classical public channel is contaminated, the result decrypted by Bob will be flipped and hence cause an error. From this point of view, the classical public channel is publicly writable, but any incorrect value inevitably causes an error. This is because an attack in the classical channel is protected by the quantum channel and will be detected. Moreover, this implies that the protocol still works even if a man-in-the-middle exists only in the classical channel. Similarly, the quantum channel is publicly writable as long as the classical channel is not contaminated. This is because even the flying qubit is

replaced by an uncorrelated new qubit, the eavesdropping will still be detected by the integrity checking process. However, if both classical and quantum channels are controlled by Eve, then she will be able to do whatever she likes as a man-in-the-middle. This becomes an authentication problem, which is outside the scope of this paper.

5. CONCLUSION

In this article, we propose a new cryptographic protocol based on a phase-encoding scheme. Local operation and classical communication can be used to achieve private communications between the sender and the receiver. In case eavesdroppers exist and have total control of the channel, the protocol not only gives absolutely no information but also can detect the existence of eavesdroppers. Unlike its classical counterpart, the security of the protocol does not depend on any unproven hard problems. It is based on the laws of physics.

REFERENCE

1. P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, *Proceeding of the 35th Annual IEEE Symposium on the Foundations of Computer Science*, 124-134(1994).
2. R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. (2) 21, pp. 120-126(1978).
3. W. Diffie, and M. E. Hellman, Multiuser Cryptogrphic Techniques, *Proceeding of AFIPS National Computer Conference*, 644-654(1976).
4. C. Bennett, and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, 175-179 (1984).
5. A. K. Ekert., Quantum Cryptography based on Bell's theorem, *Phys. Rev. Lett* 67(6), 661-663(1991).
6. C. Bennett, Quantum Cryptography: Uncertainty in the Service of Privacy, *Science* 257, 752-3 (1992).
7. K. Bostrom, and T. Felbinger, Deterministic Secure Direct Communication using Entanglement, *Phys Rev Lett.* 2002 Oct 28;89(18):187902.

8. Qing-Yu Cai, Deterministic Secure Direct Communication using Ping-Pong Protocol without Public Channel, http://xxx.lanl.gov/abs/quant-ph/0301048.
9. Qing-Yu Cai, Deterministic secure communication protocol without using entanglement, *Chin. Phys. Lett*, 21(4),601 (2004).
10. Z. Zhao, T. Yang, Z.-B. Chen, J.-F. Du, and J.-W. Pan, Deterministic and highly efficient quantum cryptography with entangled photon pairs, *Phys. Rev. Lett.*, http://xxx.lanl.gov/abs/quant-ph/0211098.