Quantum Key Distribution with Two-Qubit Quantum Codes

Xiang-Bin Wang*

Imai Quantum Computation and Information Project, ERATO, Japan Science and Technology Agency,
Daini Hongo White Building 201, 5-28-3, Hongo, Bunkyo, Tokyo 113-0033, Japan

(Received 9 September 2003; published 20 February 2004)

We propose a prepare-and-measure scheme for quantum key distribution with two-qubit quantum codes. The protocol is unconditionally secure under all types of intercept-and-resend attack. Given the symmetric and independent errors to the transmitted qubits, our scheme can tolerate a bit of an error rate up to 26% in four-state protocol and 30% in six-state protocol, respectively. These values are higher than all currently known threshold values for the prepare-and-measure protocols. Moreover, we give a practically implementable linear optics realization for our scheme.

DOI: 10.1103/PhysRevLett.92.077902 PACS numbers: 03.67.Dd, 03.67.Pp

Introduction.—Quantum key distribution (QKD) is different from classical cryptography in that an unknown quantum state is, in principle, not known unless it is disturbed, rather than the conjectured difficulty of computing certain functions. The first published protocol, proposed in 1984 [1], is called BB84 (Bennett and Brassard). For a history of the subject, one may see, e.g., Ref. [2]. Since then, studies on QKD are extensive. Strict mathematical proofs for the unconditional security have been given already [3–5]. It is greatly simplified if one connects this with the quantum entanglement purification protocol (EPP) [3,6–10]. Very recently, motivated for higher bit error rate tolerance and higher efficiency, Gottesman and Lo [11] studied the classicalization of EPP with two way communications (2-EPP). Their protocol has increased the tolerable bit error rate of the channel to 18.9% and 26.4% for four-state QKD and six-state QKD, respectively. Very recently, these values have been upgraded to 20% and 27.4% by Chau [12].

This type of prepare-and-measure QKD schemes is particularly interesting because it does not need the very difficult technique of quantum storage. In this Letter, we propose a new prepare-and-measure scheme with the assistance of two-qubit quantum codes. The linear optical realization is shown in Figs. 1 and 2). In our scheme, Alice sends both qubits of the quantum codes to Bob; therefore, they do not need any quantum storage. Bob first checks the parity of the two qubits by the polarizing beam splitter (PBS) and then decodes the code with postselection. The two-qubit code is produced by the SPDC (spontaneous parametric down conversion) process [13]; see Fig. 1.

We use the representation of $|0\rangle = \binom{1}{0}; |1\rangle = \binom{0}{1}$. We denote

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

These operators represent a bit-flip error only, a phase-flip error only, and a combination of both errors, respectively. The detected bit (or phase) flip error rate is the summation of the σ_x (or σ_z) error rate and the σ_y error rate. The Z, X, Y bases are defined by the bases of $\{|0\rangle, |1\rangle\}$, $\{|0\rangle \pm |1\rangle\}$, $\{|0\rangle \pm i|1\rangle\}$, respectively.

Main idea.—We propose a revised 2-EPP scheme which is unconditionally secure and which can further increase the thresholds of error rates given the independent channel errors. We propose to let Alice send Bob the quantum states randomly chosen from $\{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), |00\rangle, |11\rangle\}$. As we shall see, these states are just the quantum phase-flip error-rejection (QPFER) code for the BB84 state $\{|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$.

In our four-state protocol, the tolerable channel bit-flip and phase-flip rate is raised to 26% for the symmetric channel with independent noise. (A symmetric channel is defined as the one with an equal distribution of errors of $\sigma_x, \sigma_z, \sigma_y$.) Note that the theoretical upper bound of 25% [11] holds only for those four-state schemes where Alice and Bob test the error rate *before* any error removing steps. However, this is not true with the *delay* of the error test. Considering the standard purification protocol [7] with symmetric channels, one may distill the maximally entangled states out of the raw pairs whose initial bit-flip error and phase-flip error are 33.3%. In our four-state protocol, we delay the error test by one step of purification with a two-qubit QPFER code. This raises the tolerable channel flipping rates.

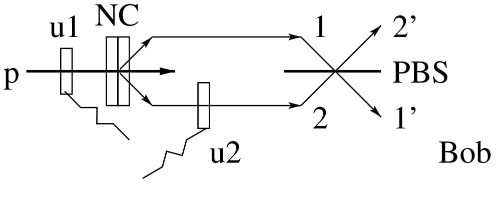

FIG. 1. QKD scheme with two-qubit quantum codes. PBS: polarizing beam splitter; NC: nonlinear crystals used in SPDC process; p: pump light in horizontal polarization; u1: unitary rotator; u2: phase shifter. The u1 takes the value of 0, $\pi/2$, $\pi/4$ to produce emission state $|11\rangle$, $|00\rangle$, $|\phi^+\rangle$, respectively. u2 can be either I or σ_z.

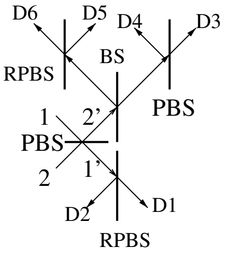

FIG. 2. Bob's action in the QKD scheme of Fig. 1. RPBS: Rotated polarizing beam splitter which transmits the state $|+\rangle$ and reflects state $|-\rangle$. BS: 50:50 beam splitter. D represents a photon detector. With RPBS, one may measure the incident beam in the $\{|+\rangle, |-\rangle\}$ basis.

The QPFER code.—We use the following QPFER code:

$$\begin{aligned} |0\rangle|0\rangle &\rightarrow (|00\rangle + |11\rangle)/\sqrt{2}, \\ |1\rangle|0\rangle &\rightarrow (|00\rangle - |11\rangle)/\sqrt{2}. \end{aligned} \tag{1}$$

Here the second qubit in the left side of the arrow is the ancilla for the encoding. This code is not assumed to reduce the errors in all cases. But in the case that the channel noise is uncorrelated or nearly uncorrelated, it works effectively. Consider an arbitrary state $\alpha|0\rangle_1 + \beta|1\rangle_1$ (qubit 1) and an ancilla state $|0\rangle_2$ (qubit 2). Taking unitary transformation of Eq. (1), we obtain the following unnormalized state:

$$\alpha(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2) + \beta(|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2). \tag{2}$$

This can be regarded as the encoded state for $\alpha|0\rangle_1 + \beta|1\rangle_1$. Alice then sends both qubits to Bob. In receiving them, Bob first takes a parity check; i.e., he compares the bit values of the two qubits in the Z basis. Note that this *collective* measurement does not destroy the code state itself. Specifically, the parity check operation can be done by the PBS in Fig. 2: there, states $|0\rangle$ and $|1\rangle$ are for horizontal and vertical polarization photon states, respectively. Since a PBS transmits $|0\rangle$ and reflects $|1\rangle$, if incident beams (beams 1 and 2) of the PBS are both horizontally polarized or vertically polarized, there must be one photon on each output beam (beams $1'$ and $2'$); if the polarizations of two incident beams are one horizontal and one vertical, one of the output beams must be empty. After the parity check, if bit values are different, Bob discards the whole two-qubit code; if they are same, Bob decodes the code. In decoding, he measures qubit 1 in X basis, and if he obtains $|+\rangle$, he takes a Hadamard transformation $H = (1/\sqrt{2})\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to qubit 2; if he obtains $|-\rangle$ for qubit 1, he takes the Hadamard transformation to qubit 2 and then flips qubit 2 in the Z basis. Suppose the original channel error rates of the σ_x, σ_y, σ_z types are p_{x0}, p_{y0}, p_{z0}, respectively. Let $p_{I0} = 1 - p_{x0} - p_{y0} - p_{z0}$. One may easily verify the probability distribution and error type for the surviving and decoded states (qubit 2) in Table I. The first column lists the various types of joint channel errors (JCE) before decoding. $\{\alpha \otimes \beta\}$ denotes both $\alpha \otimes \beta$ and $\beta \otimes \alpha$. According to Table I, the error rate distribution for the surviving raw pairs after decoding is

$$\begin{cases} p_I = \frac{p_{I0}^2 + p_{z0}^2}{(p_{I0}+p_{z0})^2 + (p_{x0}+p_{y0})^2}, \\ p_z = \frac{p_{x0}^2 + p_{y0}^2}{(p_{I0}+p_{z0})^2 + (p_{x0}+p_{y0})^2}, \\ p_y = \frac{2p_{x0}p_{y0}}{(p_{I0}+p_{z0})^2 + (p_{x0}+p_{y0})^2}, \\ p_x = \frac{2p_{I0}p_{z0}}{(p_{I0}+p_{z0})^2 + (p_{x0}+p_{y0})^2}. \end{cases} \tag{3}$$

With this formula, the phase-flip error to the decoded states is obviously reduced. Note that this formula does not hold for the correlated channel errors. Even though the noise of the physical channel is uncorrelated, in carrying out the QKD task, we should not use this formula to *deduce* the flipping rates of the decoded qubits based on our knowledge of the physical channel noise, i.e., the values of p_{I0}, p_{x0}, p_{y0}, p_{z0}. But we can choose to directly test the error rate of the surviving and decoded qubits and to *see* whether formula (3) indeed holds, based on our prior knowledge of physical channel noise.

Our protocol with linear optical realization.—In the BB84 protocol, there are only four different states. Therefore, Alice may directly prepare random states from the set of $\{(1/\sqrt{2})(|00\rangle + |11\rangle), (1/\sqrt{2})(|00\rangle - |11\rangle), |00\rangle, |11\rangle\}$ and sends them to Bob. This is equivalent to first preparing the BB84 states and then encoding them by Eq. (1). We propose the following four-state protocol with implementation of linear optics in Figs. 1 and 2: (1) Alice prepares N two-qubit quantum codes with $N/4$ of them being prepared in $|00\rangle$ or $|11\rangle$ with equal probability and $3N/4$ of them being prepared in $(1/\sqrt{2})(|00\rangle \pm |11\rangle)$ with equal probability. All codes are put in random order. She records the "preparation basis" as the X basis for code $|00\rangle$ or $|11\rangle$; and as the Z basis for code $(1/\sqrt{2})(|00\rangle \pm |11\rangle)$. And she records the bit value of 0 for the code $|00\rangle$ or $(1/\sqrt{2})(|00\rangle + |11\rangle)$ and the bit value of 1 for the code $|11\rangle$ or $(1/\sqrt{2})(|00\rangle - |11\rangle)$. She sends each two-qubit code to Bob. In Fig. 1, any of the above four states can be produced from the nonlinear crystal by appropriately setting the polarization of the pump light [14]. (2) Bob checks the parity of each two-qubit code in the Z basis. He discards the codes whenever the two-qubits have different values and he takes the following measurement if they have the same values: he measures

TABLE I. Probabilities of joint channel errors (JCE) and the results after decoding.

JCE	Probability	Decoded state	Error type
$I \otimes I$	p_{I0}^2	$\alpha\vert 0\rangle + \beta\vert 1\rangle$	I
$\{I \otimes \sigma_z\}$	$2p_{I0}p_{z0}$	$\alpha\vert 1\rangle + \beta\vert 0\rangle$	σ_x
$\sigma_z \otimes \sigma_z$	p_{z0}^2	$\alpha\vert 0\rangle + \beta\vert 1\rangle$	I
$\sigma_y \otimes \sigma_y$	p_{y0}^2	$\alpha\vert 0\rangle - \beta\vert 1\rangle$	σ_z
$\sigma_x \otimes \sigma_x$	p_{x0}^2	$\alpha\vert 0\rangle - \beta\vert 1\rangle$	σ_z
$\{\sigma_x \otimes \sigma_y\}$	$2p_{x0}p_{y0}$	$\alpha\vert 1\rangle - \beta\vert 0\rangle$	σ_y

qubit 1 in X basis and qubit 2 in either the X basis or the Z basis with equal probability. If Bob has measured qubit 2 in the X (Z) basis, he records the "measurement basis" as the Z (X) basis [15], and we simply call the qubit a Z-bit (or X-bit) later on. If he obtains $|+\rangle|+\rangle$, $|+\rangle|0\rangle$, $|-\rangle|-\rangle$, or $|-\rangle|0\rangle$, he records the bit value 0 for that code; if he obtains $|-\rangle|+\rangle$, $|-\rangle|1\rangle$, $|+\rangle|-\rangle$, or $|+\rangle|1\rangle$, he records the bit value 1 for that code. In our linear optical realization, Bob's detections are done by postselection in Fig. 2: If beam $1'$ and beam $2'$ each contain one photon, beam 1 and beam 2 must have the same bit values. Otherwise, their bit values must be different. This requires Bob to accept only the events of twofold clicking with one clicked detector from {D1, D2} and the other clicked detector from {D3, D4, D5, D6}. All other types of events must be discarded. Moreover, according to the above-mentioned corresponding rule, to those accepted events, clicking of D3 or D4 means measurement in the Z basis to beam $2'$, corresponding to the "X basis" for his record; also, clicking of D5 or D6 means measurement in the X basis to beam $2'$, corresponding to "Z basis" for his record. The twofold clicking of (D1, D6), (D1, D3), (D2, D5), or (D2, D3) corresponds to the bit value of 0; the twofold clicking of (D2, D6), (D2, D4), (D1, D5), or (D1, D3) corresponds to bit value 1. (3) Bob announces which codes have been discarded. Alice and Bob compare the preparation basis and the measurement basis of each bit decoded from the surviving codes by classical communication. They discard those bits whose measurement basis disagrees with "preparation basis." Bob announces the bit value of all X-bits. He also randomly chooses the same number of Z-bits and announces their values. If too many of them disagree with Alice's record, they abort the protocol. (4) Now they regard the tested error rates on Z-bits as the bit-flip rate and the tested error rate on X-bits as the phase-flip rate. They reduce the bit-flip rate in the following way: they randomly group all their unchecked bits with each group containing two-qubit. They compare the parity of each group. If the results are different, they discard both bits. If the results are the same, they discard 1 bit and keep the other. They repeatedly do so for a number of rounds until they believe that both the bit-flip rate and the phase-flip rate can be reduced to less than 5% with the next step being taken. (5) They then randomly group the remaining bits with each group containing r bits. They use the parity of each group as the new bits. (6) They use the classical CSS code [6] to distill the final key.

Note that in this protocol, since formula (3) is not unconditionally true, Alice and Bob check the bit errors *after* decoding the two-qubit quantum codes. If the detected errors are significantly larger than the expected values calculated from Eq. (3), they will abort the protocol. That is to say, if formula (3) really works, they continue; if it does not work, they abort it. After any round of bit-flip error rejection in step (4), the error rate is iterated by Eq. (1) in Ref. [12]. After the phase error correction in step (5), the new error rate satisfies the inequality of formula (3) of Ref. [12] provided that $p_I > 1/2$. The above steps to remove the bit-flip error and the phase-flip error are unconditionally true since Alice and Bob have paired the qubits *randomly.* Even though the errors of the decoded qubits are arbitrarily correlated, the above steps always work as theoretically expected.

Given p_x, p_y, p_z, if there exits a finite number k, after k rounds of bit-flip error rejection, we can find an r which satisfies

$$r(p_x + p_y) \leq 5\%, \qquad e^{-2r(0.5-p_z-p_y)^2} \leq 5\%; \qquad (4)$$

one can then obtain the unconditionally secure and faithful final key with a classical CSS code [6].

In the four-state protocol, we do not detect the σ_y error for the states decoded from the surviving codes; therefore, we have to assume $p_y = 0$ after the quantum parity check and decoding. But we do not have to assume $p_{y0} = 0$, and actually Alice and Bob never test any error rate before decoding in the protocol. However, *if the* channel noise is symmetric and uncorrelated, after the quantum decoding, both the σ_z error (p_z) and the σ_y error (p_y) are reduced; i.e., the detectable phase error rate has been reduced in a rate as it should be [see Eq. (3)]. We then start from the unsymmetric error rate with assumption $p_y = 0$ and p_x, p_z being the detected bit-flip rate and phase-flip rate, respectively. After the calculation, we find that the tolerable error rate of bit-flip or phase-flip is 26% for the four-state protocol. Moreover, in the case that the channel error distribution itself is $p_{y0} = 0$; $p_{x0} = p_{z0}$, the tolerable channel error rate for our protocol is $p_{x0} = p_{z0} \leq 21.7\%$. The above protocol is totally equivalent to the one based on entanglement purification; therefore, it is unconditionally secure [16]. Here we give a simple security proof.

Security proof.—Consider two protocols, protocol P0 and protocol P. In protocol P0, Alice directly sends Bob each individual qubit. In protocol P, Alice first encodes each individual qubit by a certain error-rejection code and then sends each quantum code to Bob. We denote the encoding operation as $\hat{E}$ and the parity check and decoding operation by $\hat{D}$. Bob first checks the parity of each code and decodes the surviving codes. After decoding, Alice and Bob continue the protocol. Suppose except for the operations of $\hat{D}$ and $\hat{E}$ everything else in protocol P0 and protocol P is identical and operation $\hat{D}$ or $\hat{E}$ do not require any information of the original qubit itself, then we have the following theorem.

Theorem: If protocol P0 is secure with arbitrary lossy channel, then protocol P is also secure. The proof of this theorem is very simple. Suppose P is insecure. Then Eve must be able to attack the final key with a certain operation. Eve's attack during the period that all codes are transmitted from Alice to Bob is denoted as $\hat{A}$. Eve may obtain significant information of the final key with operation $\hat{A}$ and other operations ($\hat{Q}$) after Bob receives the qubits. If this is true, then in protocol P0, Eve may take the operation of $\hat{D}\hat{A}\hat{E}$ in the same period and then send the decoded states to Bob, with all other operations identical to those in protocol P. (The time order is from right to left.) To Alice and Bob, it looks like they are carrying out protocol P0 with a lossy channel now, because Eve has to discard some of the two-qubit quantum codes after the parity check in decoding. All final results from protocol P0 with attack $\hat{Q}\hat{D}\hat{A}\hat{E}$ must be identical to protocol P with attack $\hat{Q}\hat{A}$, since everything there with the two protocols is now the same. This completes our proof of the theorem.

Our QKD protocol in the previous section is just the modified Chau protocol [12] with encoding and decoding added. We can regard our protocol as P and Chau protocol as P0 in applying our theorem. Since the Gottesman-Lo protocol [11] and the Chau protocol [12] are all unconditionally secure with arbitrary lossy channel, we conclude that our protocol must also be unconditionally secure.

Six-state protocol.—Our protocol can obviously be extended to the six-state protocol [17]. In doing so, Alice changes only the initially random codes by adding $N/4$ codes from $\{\frac{1}{2}[(|00\rangle + |11\rangle) \pm i(|00\rangle - |11\rangle)]\}$. This is equivalent to $(1/\sqrt{2})(\{|00\rangle \mp i|11\rangle)\}$. She regards all these types of codes as Y-bits. In decoding the codes, Bob's measurement basis is randomly chosen from three bases, X, Y, and Z. All decoded X-bits, Y-bits, and the same number of randomly chosen decoded Z are used as the check bits. Since the Hadamard transform switches the two eigenstates of σ_y, after decoding, whenever Bob measures qubit two in the Y basis, he needs to flip the measurement outcome so that to obtain everything the same as that in the 2-EPP with quantum storages [16]. In such a way, if the channel is symmetric, Bob will find $p_y \neq 0$. And he will know p_x, p_y, p_z exactly instead of assuming $p_y = 0$. This increases the tolerable error rate accordingly. In the case of the symmetric physical channel, our six-state protocol tolerates the flipping rate up to 30%.

Subtlety of the "conditional advantage."—Although the advantage of a higher threshold is conditional, the security of our protocol is *unconditional*. That is to say, whenever our protocol produces any final key, Eve's information to that key must be exponentially close to zero, no matter whether Eve uses a coherent attack or an individual attack. *Our protocol is totally different from the almost useless protocol which is secure only with uncorrelated channel noise.* There are two conditions for the error threshold advantage: (1) The noise of the physical channel should be the type where Eq. (3) holds; (2) Eve is not detected in the error test; i.e., the result of error test must be in agreement with the expected result given by Eq. (3).

Both conditions here are verifiable by the protocol itself. The second condition is a condition for *any* QKD protocol. The first condition is on the *known* physical channel rather than Eve's channel in QKD. In our protocol, Eve's attack must not affect the error rates detected on the decoded qubits if she wants to hide her presence. That is to say, if Eve hides her presence, all results about the final key of our protocol can be correctly estimated based on the known properties of the physical channel, no matter what type of attack she has used. *Given a physical channel with its noise being uncorrelated, symmetric, and higher than the thresholds of all other prepare-and-measure protocols but lower than that of our protocol, our protocol is the only one that works.* In practice, one may simply separate the two qubits of the quantum code substantially to guarantee the uncorrelation of the physical channel noise. This is to say, *the error threshold advantage of our protocol is actually unconditional in practice.*

Loose ends in practice.—Multipair emission in SPDC and dark counting of detectors have not been considered. We believe these issues can be resolved along the similar lines in the case of BB84 implemented with a weak coherent light source.

I thank Professor Imai H for support. The extended version of this work has been submitted to the QIT-EQIS workshop (Kyoto) [16]. I thank C. H. Bennett and H.-K. Lo for their encouragement and enlightening discussions. I thank Dr. B. S. Shi for discussions on the source design.

*Email address: wang@qci.jst.go.jp

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE Press, Los Alamitos, CA, 1984), pp. 175–179; IBM Technical Disclosure Bulletin **28**, 3153 (1985).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[4] D. Mayers, J. ACM **48**, 351 (2001).

[5] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)* (ACM Press, New York, 2000), p. 715.

[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[8] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996); **80**, 2022(E) (1998).

[9] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 22309 (2001).

[10] A. R. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996); A. M. Steane, Proc. R. Soc. London A **452**, 2551 (1996).

[11] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).

[12] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).

[13] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. H. Shih, Phys. Rev. Lett. **75**, 4337 (1995).

[14] P. G. Kwiat *et al.*, Phys. Rev. A **60**, R773 (1999).

[15] Here Bob has omitted the Hadamard transformation as appeared in the EPP.

[16] One may see details in X. B. Wang, quant-ph/0306156.

[17] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).