Quantum Information and Computation, Vol. 1, No. 2 (2001) 81–94

PROOF OF UNCONDITIONAL SECURITY OF SIX-STATE QUATUM KEY DISTRIBUTION SCHEME

Hoi-Kwong Lo
MagiQ Technologies Inc., 275 Seventh Avenue, 26th Floor
New York, NY 10001, USA

Received March 5, 2001
Revised July 12, 2001

We prove the unconditional security of the standard six-state scheme for quantum key distribution (QKD). We demonstrate its unconditional security up to a bit error rate of 12.7 percents, by allowing only one-way classical communications in the error correction/privacy amplification procedure between Alice and Bob. This shows a clear advantage of the six-state scheme over another standard scheme—BB84, which has been proven to be secure up to only about 11 percents, if only one-way classical communications are allowed. Our proof technique is a generalization of that of Shor-Preskill's proof of security of BB84. We show that a advantage of the six-state scheme lies in the Alice and Bob's ability to establish rigorously from their test sample the non-trivial mutual information between the bit-flip and phase error patterns. A modified version of the degenerate quantum codes studied by DiVincenzo, Shor and Smolin is employed in our proof.

Keywords: Quantum key distribution, quantum cryptography, security, six-state scheme

Communicated by: R Cleve and H Zbinden

1. BB84

Whereas conventional cryptography is often based on some unproven computational assumptions, the security of quantum key distribution [1,2,3,4] *is guaranteed by the fundamental laws (particularly the uncertainty principle) of quantum mechanics. The best-known quantum cryptographic application is quantum key distribution (QKD) whose goal is to allow two persons, Alice and Bob, to communicate in perfect security in the presence of an eavesdropper, Eve.

A number of years had passed before rigorous and convincing proofs of security against the most general attack finally appeared. Mayers [8] and subsequently others [9] have proven the security of the standard Bennett and Brassard's BB84 scheme [1], a scheme that is closer to a realistic experimental situation. Unfortunately, those proofs are rather complex. A proof by Lo and Chau [10] has the advantage of being conceptually simple,

*Quantum cryptography, but not quantum key distribution per se, was invented by Stephen Wiesner around 1970 in a paper that remained unpublished until 1983 [5]. Quantum key distribution is experimentally the most advanced subfield of quantum information processing. Photons have been transmitted over about 50km of commercial Telecom fibers [6] and over 1km of open air [7].

but it requires a quantum computer to implement. Their proof built on earlier work on quantum privacy amplification [11] and has subsequently been further simplified [12]. Recently, Shor and Preskill [13] have proposed a simple proof of security of BB84 by combining and generalizing the insights in Lo and Chau's [10] and Mayers' [8] proofs. Their proof also extends the tolerable error rate of BB84 from about 7 percents set by Mayers' proof to about 11 percents.[†]

Other QKD schemes have also been proposed.[‡] A notable example is the six-state scheme proposed by Bruss [16]. Recently, a proof of security of the six-state scheme has been proposed by Inamori [17], which, unlike Shor and Preskill's proof of security of BB84, requires two-way classical communications between Alice and Bob.

Until now, it was not obvious how to generalize the proof technique of Shor-Preskill's proof, which requires only one-way classical communications, to the six-state scheme. The main goal of this paper is to provide precisely such a simple proof of security for the six-state using Shor and Preskill's approach. Our result shows that, using only one-way classical communication, six-state QKD scheme can be made secure up to an error rate of about 12.7 percents. This is higher than the value of about 11 percents in the case of Shor-Preskill's result in BB84, thus demonstrating the advantage of the six-state scheme over BB84. Our proof also clarifies the symmetry structure employed in Shor and Preskill's proof.

A key idea of Shor-Preskill's proof is reduction: Instead of tackling the security of BB84 directly, they took an indirect path. They constructed a QKD scheme that employs entanglement purification (i.e., it requires a quantum computer to implement) and showed that such a scheme is secure. Then, they showed that the security of such an entanglement-purification-based QKD scheme implies the security of BB84. In their proof, the bit-flip and phase errors of the underlying entanglement purification protocol may be totally uncorrelated. Therefore, in the worst case situation, the bit-flip error syndromes tell the two users nothing about the phase errors.

In this paper, we will follow Shor-Preskill's approach for the case of a six-state QKD scheme. We see a clear advantage of the six-state scheme over BB84: As will be discussed in subsequent sections, for the six-state scheme, one can show that in the corresponding underlying entanglement-purification-based QKD scheme, the bit-flip and phase errors are *correlated*.[§] In other words, the bit-flip error syndromes can be used to reduce the conditional entropy of the phase error pattern. This reduction in conditional entropy makes the task of entanglement purification easier and allows us to establish the security of the six-state scheme up to an error rate of 12.7 percents.

This paper is organized as follows. In Section 2, we review Shor-Preskill's proof. In Section 3, we study the differences between BB84 and the six-state scheme, emphasizing

[†] Mayers' proof also permits the same extension.

[‡] For instance, an efficient four state scheme has been proposed and its unconditional security was proven in [14]. Besides, the security of a continuous variable (squeezed state) QKD scheme has been proven by Gottesman and Preskill [15] using the same approach of Shor and Preskill's proof.

[§] As shown in subsequent sections, the six-state QKD scheme can be made symmetric with respect to all three bases, X, Y and Z. In the language of entanglement purification, this corresponds to a so-called depolarizing channel. Therefore, the bit-flip and phase errors are, indeed, correlated.

the ability by Alice and Bob to establish the correlations between the bit-flip and phase error patterns in the six-state scheme, but *not* in BB84. In Section 4, our protocol for secure six-state QKD scheme is given. Section 5 contains various concluding remarks.

2. Shor-Preskill's proof

In this section, we shall recapitulate briefly Shor and Preskill's proof [13] of security of BB84. A nice review of Shor and Preskill's proof can be found in the early sections of [15]. Readers who are familar with the subject can skip this section. Before we go to the specifics, we should first review the three major ingredients of their proof: entanglement purification, classicalization (i.e., quantum to classical reduction) and CSS codes.

2.1. *Entanglement purification*

Entanglement purification was first studied by Bennett, DiVincenzo, Smolin and Wootters[18] and its usage in QKD was first proposed by Deutsch *et al.* [11]. Suppose Alice prepares n EPR pairs and sends the half of each pair to Bob through a channel controlled by Eve. Because of Eve's interference, the n EPR pairs are now noisy. However, Alice and Bob can purify from the n imperfect pairs a smaller number, say m, perfect EPR pairs, *provided that* the channel is not too noisy.

2.2. *Classicalization*

A key question remains: how can one *verify* that the channel is, indeed, not too noisy? This is not entirely trivial because noise pattern of the channel is controlled by Eve and does not have to be independent. Moreover, the Einstein-Podolsky-Rosen paradox tells us that it would be too naive to apply classical arguments blindly to a quantum problem. This is where the classicalization (quantum to classical reduction) idea of Lo and Chau [10] comes in.

The key idea is "commuting observables", i.e., one should focus on observables that commute with each other. For those observables, it is consistent to assign probabilities to their *simultaneous* eigenstates and study those probabilities by classical probability theory, particularly classical random sampling theory. This leads to substantial simplification of the original quantum problem. [This "commuting observables" idea is the essence of the stabilizer formalism of Gottesman [19] and Calderbank *et al.* [20].]

More concretely, Alice and Bob can figure out the error rate of the two (rectilinear or diagonal) bases by random sampling. That is to say that, for each basis, Alice and Bob select a random subset of test EPR pairs and compare their polarizations of the two halves of a pair to see if they agree. Mathematically, this is equivalent to measuring the either operator XX and ZZ, where X and Z are respectively the Pauli matrices, σ_x and σ_z. The key observation here is that XX commutes with ZZ. Therefore, the commuting observables idea indeed applies and probabilities to the simultaneous eigenstates can be assigned to Alice and Bob's state.

With the above two ingredients—entanglement purification and classicalization, one can prove the security of QKD by intuitive classical argument [10]. Nonetheless, the resulting protocols still require quantum computers to implement. This is because a general entanglement purification protocol requires a quantum computer for its implementation. It is the following insight of Shor and Preskill [13] that allows one to implement a secure QKD scheme without a quantum computer.

2.3. *CSS codes*

Their proof makes essential use of the Calderbank-Shor-Steane (CSS) code. The CSS code has the useful property that the error correction procedure for the phase error is decoupled from that for the bit-flip error. Clearly, bit-clip error correction is important to ensure that Alice and Bob do share a common key. However, Shor and Preskill made the following important observation: Since phase errors will not change the bit value of their final key anyway, Alice and Bob have the liberty of dropping the whole phase error correction procedure altogether. This is the fundamental reason why they can implement a CSS code-based QKD scheme without a quantum computer. General quantum error correcting codes can also be used for QKD, but it is unclear how to implement those QKD schemes without a quantum computer.

Even though the phase error correction procedure is dropped in BB84, it is, nonetheless, important that the phase error is, in principle, correctable by the underlying quantum error correcting code because only then can security be guaranteed by the quantum no-cloning theorem. In other words, Alice and Bob do not need to perform phase error correction. The very fact that Alice and Bob *could* perform phase error correction (if they had quantum computers) would be enough to guarantee security of QKD. The phase error correction procedure reduces the eavesdropper's information on the key to an exponentially small amount in terms of some security parameters. In other words, the phase error correction is used for privacy amplification, whereas the bit-flip error correction is used for error correction. The remenant of the phase error correction procedure is a "coset extraction" procedure. This point has been emphasized in [13] and will be recapitulated below.

2.4. *Notation*

Having introduced the above three major ingredients, we shall give more specifics of the Shor-Preskill's proof. We shall mostly use the notations in [13]. For each qubit, we use a canonical basis, $|0\rangle$ and $|1\rangle$. Define also the basis, $|+\rangle$ and $|-\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The Hadamard transform, H, is a single qubit unitary transformation of the form:

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

in the canoncial basis. It interchanges the bases $|0\rangle$, $|1\rangle$ and $|+\rangle$, $|-\rangle$.

Let us also introduce Pauli matrices,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2}$$

In what follows, we may simplify our notation and denote the three Pauli matrices simply by X, Y and Z.

The Bell basis is an orthogonal basis for the quantum state of two qubits. It has basis vectors,

$$\Psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{3}$$

$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle). \tag{4}$$

2.4.1. *CSS codes*

Let us consider two classical binary codes, C_1 and C_2, such that,

$$\{0\} \subset C_2 \subset C_1 \subset F_2^n, \tag{5}$$

where F_2^n is the binary vector space of the n bits and that both C_1 and $C_2^{\perp}$, the dual of C_2 can correct up to t errors. A basis for the CSS code can be found as follows. For each $v \in C_1$, define the vector

$$v \rightarrow \frac{1}{|C_2|^{1/2}} \sum_{w \in C_2} |v + w\rangle. \tag{6}$$

Notice that v_1 and v_2 give the same vector whenever $v_1 - v_2 \in C_2$. In other words, the codeword of the CSS code corresponds to the coset of C_2 in C_1. Let H_1 be the parity check matrix for the code C_1 and H_2 for $C_2^{\perp}$.

2.5. *Secure QKD based on entanglement purification*

Let us recapitulate the key point of Shor-Preskill's proof. As a starting point of their paper, they [13] proved the security of the following QKD scheme:

Protocol 1 (in [13]): **Modified Lo-Chau**

(0) Alice and Bob decide on a large positive integer n, a CSS code and a maximal number e_{max} of check bit errors that they tolerate in the protocol.

(1) Alice prepares $2n$ EPR pairs in the state $(\Phi^+)^{2n}$.

(2) Alice picks a random $2n$-bit string b and applies a Hadamard transform H on the second half of each EPR pair for which (the component of) b is 1.

(3) Alice sends the second halves of the EPR pairs to Bob.

(4) Bob receives the qubits and publicly acknowledges the completion of his reception.

(5) Alice selects randomly n of the $2n$ EPR pairs to serve as check bits to test for the eavesdropper, Eve,'s eavesdropping.

(6) Alice announces the bit string b and which n EPR pairs are to be used as check bits.

(7) Bob performs a Hadamard transform on the qubits where (the component of) b is 1.

(8) Alice and Bob each measure their halves of the n check EPR pairs in the $|0\rangle$, $|1\rangle$ basis and broadcast their results. If more than e_{max} check bits disagree, they abort. Otherwise, they proceed to the next step.

(9) Alice and Bob each measure $\sigma_z^{[r]}$ for each row $r \in H_1$ and $\sigma_x^{[r]}$ for each row $r \in H_2$. They broadcast their results. Bob transforms his state accordingly to obtain m nearly perfect EPR pairs.

(10) Alice and Bob measure the EPR pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

Remark: As discussed by Shor and Preskill, Alice should also scramble the qubits by a random permutation before sending them to Bob. Such a scrambling extends the tolerable error rate from about 7 percents set by Mayers [8] to about 11 percents in Shor-Preskill's proof. We shall assume that this is done.

The above protocol consists of two steps: a) verification and b) privacy amplification/error correction. In step a), Alice and Bob verify by *random* sampling that the error rate of the transmission is smaller than some prescribed value. Otherwise, they abort. In step b), Alice and Bob employ the property of CSS code to correct up to t errors and obtain privacy.

One can calculate the probability that the test on the check bits is passed and yet the entanglement purification procedure on the code bit fails. Since Eve does not know which qubits are used as check bits and which as code bits, she cannot treat them differently. In other words, the check bits provide a random sample of all the bits. Moreover, since all relevant measurements refer to the Bell-bases and thus commute with each other, one can apply a *classical* random sampling argument to estimate the number of errors. By choosing an appropriate CSS code and e_{max}, one can ensure that this probability is exponentially small in n. The readers should refer to [13,15] for details.

2.6. *Reduction to a quantum error-correcting code protocol*

Now, the above entanglement purification protocol only involves one-way communication from Alice to Bob. It has been shown [18] that any one-way purification protocol can be reduced to a quantum error-correcting code protocol. i.e., Instead of Alice preparing EPR pairs and sending halves to Bob, Alice prepares an encoded quantum state with a quantum error correcting code and sends it to Bob.

More concretely, suppose Alice and Bob start with n perfect EPR pairs. Suppose in step (9) Alice measures the eigenvalues of $\sigma_z^{[r]}$ for each row $r \in H_1$ and $\sigma_x^{[r]}$ for each row $r \in H_2$ and obtains the results, x and z respectively. Her measurement will project the state of Bob into the CSS codespace $Q_{x,z}$, which has basis vectors indexed by the coset of C_2 in C_1. For $v \in C_1$, the corresponding codeword is given by

$$v \to \frac{1}{|C_2|^{1/2}} \sum_{w \in C_2} (-1)^{z \cdot w} |x + v + w\rangle. \tag{7}$$

The index, x, and z, defines a family of CSS codes, $Q_{x,z}$, with equivalent error correcting capability. In other words, each of them can correct up to t phase errors and t bit-flip errors.

Also, Alice may measure her half of the EPR pair before or after transmission. If she measures first, it will be the same as she has chosen a random raw key k and encoded it by $Q_{x,z}$ (i.e., take $v = k$ in Eq. (7)).

2.7. *Reduction to BB84*

The property of CSS codes is used in the reduction from a quantum error correcting code protocol to BB84. Recall that the bit-flip and phase error correction procedures decouple in a CSS code. What if Alice and Bob simply drop the phase error correction procedure? The resulting protocol is essentially BB84!

More concretely, since Bob does not really need the phase error syndrome z to extract the value of the shared key, there is no reason for Alice to send it. Let us now consider the case when Alice has obtained a value k for the raw key and does not send z. We can take the average density matrix of Bob, over all values of z, thus obtaining:

$$\begin{aligned} & \tfrac{1}{2^n|C_2|} \sum_z \sum_{w_1,w_2 \in C_2} (-1)^{(w_1+w_2)\cdot z} \\ & \quad \times |k + w_1 + x\rangle\langle k + w_2 + x| \\ = \; & \tfrac{1}{|C_2|} \sum_{w \in C_2} |k + w + x\rangle\langle k + w + x|. \end{aligned} \tag{8}$$

This gives rise to a classical mixture of the states, $|k+w+x\rangle$ with w randomly chosen from C_2. Mathematically, the key extraction procedure is the same as the following *classical* error correction/privacy amplification procedure: Alice sends a random string v to Bob and later broadcasts $u + v$ where u is a random string in C_1. The key is then the coset, $u + C_2$, of C_2 in C_1. Bob receives a corrupted string $v + e$. He then substracts Alice's broadcast string $u + v$ from his string to obtain $u + e$. He corrects errors to find u in C_1. He then finds the final key to be $u + C_2$, which is a coset of C_2 in C_1.

3. BB84 vs six-state scheme

Let us look at Shor-Preskill's proof of security of BB84 more closely by re-examining their underlying entanglement purification protocol (EPP), Protocol 1. Recall from subsection that one can employ the commuting observable idea and only be concerned with probabilities of their simultaneous eigenstates. In such a description, one only considers the *diagonal* entries of the density matrix with respect to the Bell-basis. Furthermore, in the large N limit (where N is the number of pairs of qubits), by random sampling, one should only be concerned with the *average* density matrix. Therefore, one can reduce the whole problem of purification of a general N-pair state in QKD to the problem of purification of an ensemble of N *identical Bell-diagonal* states. In what follows, we will see that the four entries in the density matrix have interpretations in terms of the probabilities of a) no error, b) a bit-flip error, but no phase error, c) a phase error, but no bit-flip error and d) both bit-flip and phase errors. A natural question to ask is: What are the correlations between the bit-flip and phase errors?

We will now show that in Protocol 1, the bit-flip and phase errors can be totally uncorrelated. In the language of commuting observables and in the limit of large number of pairs, let us denote the effective density matrix by:

$$diag(a, b, c, d). \tag{9}$$

Here, we use the Bell-basis as in the notations of [18]. (See also Eqs. (3) and (4).) Now, the action of the Hadamard transform in Eq. (1) will permute the four matrix elements of Eq. (9) into:

$$diag(a, c, b, d). \tag{10}$$

In Step 2 of Protocol 1, one applies randomly either the identity or the Hadamard. Averaging over the two cases: a) Identity and b) Hadamard, we find that the effective average density matrix shared by Alice and Bob after Step is of the form:

$$diag(a, (b+c)/2, (b+c)/2, d) = diag(a, e, e, d), \tag{11}$$

where we define $e = (b+c)/2$.

As remarked earlier, the four entries represent, for each shared pair between Alice and Bob, the four physical possibilities respectively: a) No error; b) bit-flip error, but no phase error; c) phase error, but no bit-flip error; and d) both bit-flip error and phase error. See, for example, [18] for details. In the random sampling procedure—Steps (5)-(8), the sample bit error rate found by Alice and Bob will be approximately $e + d$. ¶This leaves d unconstrained in Shor-Preskill's proof of security of BB84 scheme. The implication is that Alice and Bob cannot possibly know of the correlations between the bit-flip and the phase error. This is a serious limitation of the BB84 scheme. In the worst case situation, the bit-flip and phase error are independent. This corresponds to the values, $e = (b+c)/2 = p(1-p)$ and $d = p^2$ for some $0 < p < 1$.‖

Let us now consider the six-state scheme. We will now show that the situation there is completely different. Indeed, we will establish that, for the six-state scheme, the density matrix is that given by a depolarizing channel and as such *does* have correlations between bit-flip and phase errors. It is this correlations between bit-flip and phase errors that will give the six-state scheme an advantage over BB84.

As an analog of the Hadamard transform, which symmetrizes between the two bases—X and Z—in BB84, in the six-state scheme we look for a symmetry operator that will symmetrize between the three bases—X, Y and Z. We find the operator (see, e.g., Eq. (15) of [21].)

$$T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \tag{12}$$

¶We remark that, owing to the symmetry between the two bases, only a single bit error rate of the sample is required to establish the security of the Shor-Preskill's procedure. In other words, there is no need to employ a refined data analysis studied in [14].

‖Owing to symmetrization by the Hadamard transform, two of the diagonal entries in Eq. (11) are the same. This means that the probability of having a bit-flip error but no phase error is the same as that of having a phase error but no bit-flip error. Now, suppose the two types of errors are independent. They must occur independently with the same probability p. This means that $e = p(1-p)$ and that $d = p^2$, as stated in the main text.

which cyclically permutes the three bases. i.e.,

$$T : X \to Y \to Z \to X. \tag{13}$$

Suppose we apply either i) the identity operator; or ii) T; or iii) T^2 with equal probability to the density matrix shown in Eq. 9. The average density matrix becomes

$$diag(a, (b+c+d)/3, (b+c+d)/3, (b+c+d)/3), \tag{14}$$

which is totally symmetric with respect to the three bases, X, Y and Z. This shows that the channel is effectively a depolarizing channel [18]. More importantly, the above four entries again represent the four possibilities: a) No error; b) bit-flip error, but no phase error; c) phase error, but no bit-flip error; and d) both bit-flip error and phase error. This implies that there are non-trivial correlations between bit-flip and phase errors.

Such non-trivial correlations can be exploited to design a six-state error correction/privacy amplification protocol that tolerates a higher error rate than Shor-Preskill's protocol for BB84. The key point is that, the bit-flip error pattern and the phase error pattern are no longer independent in the six-state scheme. Therefore, given the same bit error rate, the actual entropy of the density matrix is smaller in the case of the six-state scheme, as compared to the worst case situation in BB84.

More concretely, for the n imperfect EPR pairs shared by Alice and Bob, let us denote by the variable $\mathcal{X}$, the phase error pattern and by $\mathcal{Z}$, the bit-flip error pattern. Now, the entropy of the whole error pattern is given by

$$H(\mathcal{X}, \mathcal{Z}) = H(\mathcal{X}) + H(\mathcal{Z}) - I(\mathcal{X}; \mathcal{Z}). \tag{15}$$

The fact that the phase and bit-flip error patterns are correlated means that $I(\mathcal{X}; \mathcal{Z}) > 0$. Consider now the following strategy of quantum error correction.

Subrountine A: Modified "random" hashing procedure with CSS codes

(I) Alice and Bob apply a random hashing code on the $\mathcal{Z}$ variable only to identify the bit-flip error pattern. Note that (slightly more than) $H(Z)$ rounds of random hashing is needed.

(II) Alice and Bob use the information on the bit-flip error pattern to reduce their ignorance on the phase error pattern from $H(\mathcal{X})$ to $H(\mathcal{X}|\mathcal{Z}) = H(\mathcal{X}) - I(\mathcal{X}; \mathcal{Z}) = H(\mathcal{X}, \mathcal{Z}) - H(\mathcal{Z})$.

(III) Alice and Bob apply a random hashing code on the $\mathcal{X}$ variable only to identify the phase error pattern. Note that only (slightly more than) $H(\mathcal{X}, \mathcal{Z}) - H(\mathcal{Z})$ rounds of random hashing is needed.

Remark: Bennett, DiVincenzo, Smolin and Wootters (BDSW) [18] have studied a random hashing scheme in entanglement purification. Our random hashing code is analogous, except that we restrict our attention to CSS codes. Therefore, in (I), all the operators are chosen to be tensor products of Z operators only and in (III), X operators only. Nonetheless, in the asymptotic limit of large number of pairs, our scheme is equally efficient as the original random hashing scheme by BDSW. In BDSW, it was shown that the scheme gives non-zero rate of distilled entanglement when the fidelity $f > 0.81071$. Since $f = 1 - 3p/2$ for a depolarizing channel, this corresponds to a bit error rate of about 12.6 percents.

Remark: By adopting a modified version of the DiVincenzo-Shor-Smolin code [22], a slightly higher error rate of about 12.7 percents can be tolerated in the six-state scheme. DSS code consists of the concatenated of a non-random (cat) code with random hashing code. It is one of the few examples of a so-called degenerate code and gives better performance than any known non-degenerate code. Note that the non-random (cat) code is a CSS-code. Since we have given a modified version of the random hashing code that is a CSS code, the concatenated code can, therefore, also be modified into a CSS code. While the actual improvement—12.7 percents vs 12.6 percents—is quite small, the result is conceptually interesting because it shows that a degenerate code can be employed in the underlying entanglement purification protocol in i) establishing a secure error-correction/privacy amplification protocol for the six-state QKD scheme and ii) tolerating a higher error rate than any known non-degenerate codes.

4. Protocol for secure six-state QKD scheme

Following our discussion in the last section, we now give the details of our procotol for secure six-state QKD scheme. We claim the following modified QKD scheme is secure. For conciseness, we omit the steps that are identical to Protocol 1. We replace some of the steps of Protocol 1 by the following.

Protocol 1': QKD based on entanglement purification

(0') Alice and Bob decide on a large positive integer n and a maximal number e_{max} of check bit errors that they tolerate in the protocol.

(2') Alice selects a random $2n$-trit t, and performs I, T or T^2 on the second half of each EPR pair if (the component of) t is 0, 1 or 2 respectively.

(6') Alice announces the trit string t and which n EPR pairs to be check bits.

(7') Bob performs I, T^{-1} or T^{-2} on the qubits depending on the value of (the component of) t.

(9') Alice and Bob apply Subrountine A (the modified random hashing procedure with CSS codes discussed in the last section) to correct the (correlated) bit-flip and phase errors. They broadcast their results. Bob transforms his state accordingly to obtain m nearly perfect EPR pairs (which are shared with Alice).

The proof of security is analogus to Shor-Preskill's proof.

4.1. *Reduction to six-state protocol*

Furthermore, the various reduction arguments of Shor-Preskill directly carry over and reduce Protocol 1' to a six-state protocol. From the security of Protocol 1', we have proven the security of the six-state protocol.

More specifically, the quantum key distribution Protocol 1', which is based on a one-way entanglement purification protocol, is mathematically equivalent to a protocol based on a class of CSS code. Furthermore, by the virtue of CSS codes, the phase error-correcting procedure is essentially decoupled from the bit-flip error-correcting procedure. Since the phase errors do not affect the value of the final key, the phase error correction procedure can be simply dropped. Put in another way, Alice could have done the procedure with *any* CSS code in the same family (they are all related by phase errors to one another). Mathematically, the mixture of the CSS codes in the family is equivalent to a classical code (with the corresponding error correction and privacy amplification procedure). Therefore, the protocol can be reduced to the a simple "prepare and measure" protocol, namely the six-state scheme. The maximal tolerable bit error rate of the six-state scheme with our error-correction/privacy amplification procedure is 12.6 percents for modified random hashing with CSS codes (and 12.7 percents if we employ a modified DSS code described in the last Section).

Inamori [17] has recently proposed a proof based on a different approach which gives a higher tolerable error rate of about 13%. However, unlike the present proof, Inamori's proof requires two-way communications between Alice and Bob.

In conclusion, we have proven the security of the six-state quantum key distribution up to a bit error rate of 12.7 percents.

5. Concluding remarks

We shall conclude with a few remarks.

5.1. *Efficient six-state scheme and proof of its unconditional security*

In the six-state scheme, Alice and Bob independently and randomly choose between three bases. Therefore, two-thirds of the times they disagree and have to throw away their polarization data. We remark that they can improve the efficiency of scheme substantially by choosing the three bases with different probabilities, say ϵ, ϵ and $1 - 2\epsilon$. This ensures that the efficiency is greater than $(1 - 2\epsilon)^2$. As $\epsilon \to 0$, the efficiency asymptotically goes to 100%.

Whereas in the standard six-state scheme the computation of only a single error rate is required for its proof of security, for this efficient scheme to be secure, it is now necessary to use a refined data analysis [14]. One should divide up the data according to the various bases in which they are transmitted and received and compute the error rate for each basis *separately* and demand that all the error rates are small.

Note that the scheme is insecure when ϵ is exactly zero. The constraint on ϵ has been discussed. Basically, it is necessary that $N\epsilon^2 > m$ where N is the total number of photons transmitted from Alice to Bob and m is the minimal number of photons needed for an accurate estimation of the error rate of the data. The numerical value of m must scale at least as $\log N$. But, it is a priori unnecessary for it to scale linearly with N. We remark that the unconditional security of the efficient four-state scheme has been proven in [14]. It is straightforward to apply the techniques developed there to prove the unconditional security of the efficient six-state scheme up to the same error rate of 12.7 percents.

5.2. *Security of other QKD schemes*

The security of some other QKD schemes remains to be explored. In particular, it would be interesting to study the security of the B92 scheme [23] with noises. It is not entirely obvious to us how the Shor-Preskill's techniques can be applied to B92.

5.3. *Real life issues*

Our result only applies to an idealized situation. In a real experiment, the source of EPR pairs are imperfect; the channel is lossy and the detector efficiency is far from perfect. It would be interesting to explore the security of the six-state in a real world situation. For BB84, some works along those lines have been done by researchers including Lütkenhaus [24,25].

In a recent preprint, Inamori, Lütkenhaus and Mayers [26] have proposed a proof of security of a weak coherent state implementation of the BB84 scheme. A key assumption is that, given any quantum signal, independent of the basis of measurement chosen by Bob, Bob's detection efficiency stays the same. (One can imagine that Bob chooses his measurement basis by pushing a button. Then, independent of which button his pushes, it is assumed that the measurement will with the same probability be successful. In other words, the signals *cannot* behave differently according to the basis chosen by Bob. Cf. Trojan Horse attack in the next subsection.) This assumption is closely related to the detectors' loophole problem in the testing of Bell's inequalities. Given rather imperfect detectors, testing of Bell's inequalities often assumes that the detected sample provides a fair representation of all the signals, detected or not.

The Shor-Preskill's proof is a fine theoretical result. However, if one would like to apply the result, one needs to make sure that the amount of computing power required is reasonable. It is not entirely clear to us that this is the case. Some discussion has been made in [25].

5.4. *Trojan Horse problem*

In proofs of security of QKD schemes, it is often assumed that the signals transmitted from Alice to Bob lives in a two-dimensional space. How can one be sure that there is no hidden Trojan Horse in the signal? For instance, the signal may, in principle, be made up of two parts, one is the usual quantum signal, the other is a robot that will explore Alice or Bob's system and tell the first part of the signal to behave differently according to, for example, the basis of measurement actually employed by Bob. Notice that the Trojan Horse can break the quantum crypto-system without directly leaking out information from Bob's laboratory to Eve!

One might naively think that QKD provides more room for the Trojan Horse attack. Fortunately, it has been pointed out (Note 21 of [10]) that this Trojan Horse problem in quantum cryptography is no worse than in classical cryptography: By using teleportation, any quantum signal can be reduced to classical one. Therefore, Alice and Bob only need to receive classical signals anyway. This teleportation trick requires only the experimental implementation of teleportation, rather than a full-blown quantum computer.

5.5. *Bell's inequality with untrusted imperfect apparatus*

Another question is whether Alice and Bob can buy their quantum cryptographic devices from untrusted vendors and verify their security by doing some simple testing themselves. By assuming that Alice and Bob's laboratory can be sufficiently shielded from the environment, a procedure to prove security based only on input/output probabilities (that corresponds to a choice of several local measurements by Alice and Bob and the corresponding measurement outcomes) has been provided for the case of perfect EPR pairs [27]. It would, thus, be interesting to generalize the result to the case of imperfect EPR sources and measuring apparatus. (See also Subsection 5.3). This line of research can also be re-phrased as a generalization of Bell's inequality to the case of a limited amount of entanglement. The question there becomes: given a fixed amount of entanglement, how far can Bell's inequality be violated? Conversely, given some experimental violations of Bell's inequality on some random sample, can one deduce the minimal amount of entanglement shared by Alice and Bob? Interesting questions include what type of privacy amplication/error correction procedures can be employed to prove unconditional security in this untrusted situation.

In summary, there is no doubt in our mind that QKD provides a fertile real-life playground for the various concepts in quantum information theory. Moreover, these interactions between theory and practice will most likely inspire new research avenues on both sides.

Notes Added: Recently, Gottesman and Lo [28] have proven the security of the six-state scheme up to a bit error rate of about 23 percents. However, their method employs two-way classical communications between Alice and Bob. They also show that, by allowing two-way classical communications, BB84 scheme can be made unconditionally secure up to an error rate of 17 percents.

6. Acknowledgments

We thank helpful discussions with various colleagues including Charles Bennett, David DiVincenzo, Nicolas Gisin, Daniel Gottesman, Hitoshi Inamori, John Preskill, Peter Shor, John Smolin and Barbara Terhal. We particularly thank Debbie Leung for pointing out some minor errors in the earlier version of this paper, Gerard Gilbert for bringing Ref. [25] to our attention and Norbert Lütkenhaus for helpful suggestions and critical comments.

References

1. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE press, 1984, p. 175.
2. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
3. For a survey, see, for example, D. Gottesman and H.-K. Lo, Physics Today **53**, No. 11, p. 22.
4. For a review, see, for example, N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/0101098
5. S. Wiesner, Sigact News, vol. 15, no. 1, 1983, pp. 78 - 88.
6. R. J. Hughes, G. L. Morgan, C. G. Peterson, J. Mod. Opt. **47**, 533 (2000); P. Townsend, Optical Fiber Technology **4**, 345 (1998)and references therein.

7. W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, Phy. Rev. Lett. **84**, 5652 (2000); B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996).
8. D. Mayers, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/9802025, to appear in J. of Assoc. Comp. Mach. A preliminary version in D. Mayers, *Advances in Cryptology—Proceedings of Crypto' 96* (Springer-Verlag, New York, 1996), p. 343.
9. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing* (STOC) (ACM Press, New York, 2000), p. 715; M. Ben-Or, to appear.
10. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
11. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996); **80**, 2022 (1998) (errata).
12. H.-K. Lo, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/9904091, to appear in a special issue of J. of Physics A.
13. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
14. H.-K. Lo, H. F. Chau and M. Ardehali, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/0011056.
15. D. Gottesman and J. Preskill, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/0008046
16. D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
17. H. Inamori, "Security of EPR-based Quantum Key Distribution using three bases", Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/0008076.
18. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. **A54**, 3824 (1996).
19. D. Gottesman, Phys. Rev. **A54**, 1862 (1996).
20. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
21. D. Gottesman, Phys. Rev. **A57**, 127 (1998).
22. D. P. DiVincenzo, P. W. Shor and J. A. Smolin, "Quantum Channel Capacity of Very Noisy Channels", Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/9706061
23. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
24. N. Lütkenhaus, Phys. Rev. **A61**, 52304 (2000); G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
25. G. Gilbert and M. Hamrick, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/0009027
26. H. Inamori, N. Lütkenhaus and D. Mayers, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/0107017
27. D. Mayers and A. Yao, in *IEEE Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 1999) p. 503.
28. D. Gottesman and H.-K. Lo, Los Alamos preprint archive http://xxx.lanl.gov/abs/quant-ph/0105121