Quantum Computers Render Quantum Key Distribution Unconditionally Secure Over Arbitrarily Long Distances

Hoi-Kwong Lo[1*] and H. F. Chau,[2†]

[1] Hewlett-Packard Labs, Filton Road, Stoke Gifford, Bristol BS34 8QZ, U. K.
[2] Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong

(May 22, 1998)

Abstract

Quantum cryptography has long been claimed to be useful for achieving many tasks that are impossible from the perspective of conventional cryptography. Arguably, the most important problem in quantum cryptography has been a rigorous proof of the security of quantum key distribution, the most well-known application. This notoriously hard problem has eluded researchers for years and has become even more important after the recent surprising demonstration of the insecurity of many other quantum cryptographic schemes including quantum bit commitment. Here, we solve this long standing problem by showing that, given quantum computers, quantum key distribution over an *arbitrarily long* distance of a realistic noisy channel can be made unconditionally secure. The novel technique we use is reduction from a quantum scheme to a classical scheme. The security in realistic noisy environments is then proven by using the recent theory of fault-tolerant quantum computation.

PACS numbers: 03.65.Bz, 89.70.+c, 89.80.+h

Keywords: Quantum Key Distribution, Quantum Cryptography, Quantum To Classical Reduction, Unconditional Security

*e-mail: hkl@hplb.hpl.hp.com

†e-mail: hfchau@hkusua.hku.hk

I. INTRODUCTION

A. Quantum Cryptography

Quantum cryptography [1–4] has received much recent attention. The most well-known application of quantum cryptography is quantum key distribution (QKD) [1–3]. The goal of key distribution is to allow two users to share a secure key which can then be used to render their subsequent communication unintelligible to a wiretapper. Unfortunately, there is, in principle, nothing in *conventional* cryptography to prevent an eavesdropper from passively wiretapping. In contrast, thanks to the uncertainty principle in quantum mechanics, any eavesdropping attack against a quantum channel will almost surely lead to detectable disturbance to the signals. The two users can, therefore, test part of their quantum signals. Only when the error rates are acceptable, will they use the quantum signals to generate a key. Consequently, the two users have the confidence that if a key is generated, it is almost surely secure. We remark on passing that various quantum key distribution experiments have been performed [5–10].

B. Security of Quantum Key Distribution

1. Definition

The most important question in quantum cryptography is arguably how secure it really is. What do we mean by security? Suppose that Alice and Bob are given imperfect devices and a noisy channel and that Alice would like to send Bob a key of length N. They choose any security parameter $k > 0$. A quantum key distribution scheme is said to be secure only if it specifies a procedure for Alice and Bob such that the amount of information that Eve can have on the final key is less than e^{-k} (provided that the classical communications between Alice and Bob are perfectly authenticated). [Other requirements are that the final key is nearly random and that Alice and Bob have the same key.] Notice that, by choosing k to be as large as they like, Alice and Bob are supposed to be able to construct a procedure to reduce Eve's information to as little as they like, even though they are using imperfect devices and a noisy channel.

2. Prior Work

Indeed, a rigorous proof of the security of QKD over a noisy channel has been a long-standing open problem. Much work has been done on the security of QKD [11–15]. Early studies were restricted to simple attacks such as the intercept-resend attacks and individual particle attacks. More recently, the security of QKD against a restricted class of joint attacks — the so-called collective attacks — has been discussed [12]. There are also claims of proofs of ultimate security of QKD [16–18], but there has been no consensus in the scientific community regarding the validity of those proofs.

The absence of a widely accepted proof of security of quantum key distribution leaves the whole foundation of quantum cryptography in shaky ground. The problem has become more acute after the recent surprising demonstration of the insecurity of many other quantum cryptographic schemes such as quantum bit commitment [19–22] and quantum one-out-of-two oblivious transfer [23]. Therefore, it is important for us to settle the basic and provocative question: Is quantum key distribution really secure?

3. Difficulty of the Problem

We remark that a proof of security of QKD is a very hard problem. A big challenge is to demonstrate security against the most general type of attacks, namely *joint attacks*: Instead of measuring the particles in transit from Alice to Bob one by one, an eavesdropper may regard all the quantum particles as a single entity. She then couples this entity with her ancilla and evolves the combined system. Afterwards, she sends the particles to Bob and keeps the ancilla herself. After hearing the public discussion (for error correction and *privacy amplification*) between Alice and Bob, Eve extracts from her ancilla information about the key distilled by Alice and Bob. Notice that Eve tries to disguise her presence from Alice and Bob by the channel noises during the normal transmission. Since, after Eve's interception, the signals are no longer independent of each other, one would expect classical intuition (such as the law of large numbers) to be invalid. This is why joint attacks are so hard to analyze and defeat.

C. Our Contributions

In this paper, we present an alternative approach to the proof of security. Instead of working with standard schemes, we construct a new entanglement-based quantum key distribution scheme and establish its unconditional security (i.e. security against the most general type of attacks and the most general type of noises).

Roughly speaking, we consider the following verification problem. Suppose two widely separated observers Alice and Bob share N pairs of spin-1/2 particles, which may be prepared by Eve. Those pairs are supposed to be singlets. How can they verify this fact with a sequence of only *local* operations and classical communications? Our solution: we have devised a verification scheme which sacrifices m of those pairs for testing such that, upon passing the verification test, the remaining $N-m$ particles have a very high fidelity as $N-m$ singlets. The above statement is valid for *any* eavesdropping strategy that passes the test with a non-negligible probability. (Of course, strategies that pass the test with negligible probabilities are uninteresting.) Moreover, using the random hashing technique devised by Bennett *et al.* [24], we show that the fidelity can be made to be exponentially close to 1, i.e., $1-O(e^{-cm})$ for some $c>0$. Therefore, upon passing the test, Alice and Bob can confidently use the remaining pairs to generate a shared key.

Apart from solving the long-standing problem of the security of quantum key distribution, the techniques employed are novel and interesting in their own right. The most important technical contribution of this paper is a reduction theorem. It reduces the proof of security of the noiseless quantum scheme mentioned above to that of a *classical* verification scheme. [More specifically, we show that, with respect to projections onto the Bell basis, our scheme has a classical interpretation.] This is non-trivial and may even seem paradoxical: It is a well-known result (the Einstein-Podolsky-Rosen paradox) [25–27] that entangled quantum mechanical systems generally exhibit subtle correlations which have no classical analog. It cannot be over-emphasized that the general philosophy and techniques behind this reduction theorem may have wide-ranging applications outside quantum key distribution.

Yet another contribution of ours is fault-tolerance. All sorts of noises or errors (e.g. channel noises, storage errors) can occur. Besides, the manipulations of quantum information are usually imperfect. It is *a priori* a non-trivial matter to demonstrate the security of a quantum key distribution scheme being operated with imperfect elementary quantum gates in a *noisy* environment. Here we argue that the general theory of fault-tolerant quantum computation [28–32] can be applied to our problem to reduce the noisy case to the noiseless case. Subtleties in applying this general theory to our problem at hand are also discussed.

Our result has an important implication on the power of quantum cryptography. We show that, given quantum computers, quantum key distribution over an arbitrarily long distance of a realistic noisy channel can be made unconditionally secure.

D. Organization of this paper

We proceed as follows. First of all, we will ignore all sources of errors and consider the security of quantum key distribution in an error-free setting. We propose a quantum key distribution in this setting and prove its security. Finally, we generalize our proof to include all types of errors.

To prove the security of quantum key distribution it turns out to be useful to ask the conceptual question: What types of experiments have classical explanations? This question will, therefore, be the subject of section II.

II. WHAT TYPE OF EXPERIMENTS HAVE CLASSICAL EXPLANATIONS

A. The Einstein-Podolsky-Rosen (EPR) Paradox

In the well-known Einstein-Podolsky-Rosen (EPR) paradox [26], photons of a so-called EPR pair always give opposite polarizations upon measurement, no matter how far apart they are. This spooky action at a distance is a counter-intuitive feature of quantum mechanics that defies any simple classical explanation and puzzled Einstein [26]. However, it has proven to be correct by experiments [27]. In summary, the Einstein-Podolsky-Rosen (EPR) paradox demonstrates that *some* (but not all) quantum mechanical experiments do not have simple classical explanations. In fact, 'entanglement' in quantum mechanics defies local explanations.

B. Evading the EPR Paradox

The natural question to ask is: What types of experiments *do* have simple classical explanations? To answer this question, it is important to notice that the Einstein-Podolsky-Rosen paradox can be observed only if measurements along *more than one* basis is performed.

A simple example of an experiment that evades the EPR paradox is one in which a complete measurement with one-dimensional projection operators along a *single* basis is performed.

C. A quantum verification scheme for spin-$1/2$ particles

For instance, suppose Peggy (the prover) gives N spin-$1/2$ objects to Vergy (the verifier) and claims that they are all spin ups along the agreed z-axis. Vergy's job is to verify that this is indeed the case. However, a cheating Peggy may prepare these N spins in a state where they are all entangled with each other, as well as with an ancilla in her hand. Of course, Vergy may verify the value of the spins perfectly by measuring the spins of all particles along the z-axis. However, suppose Vergy is unwilling to do that. She may decide to measure the spins of all but one (randomly chosen) particles along the z-axis. She then accepts the last particle as spin-up along the z-axis if all the $N-1$ tested particles give spin 'up' upon her measurement. Is this verification scheme secure?

1. Corresponding classical scheme

The above quantum verification scheme is highly reminiscent of a simple classical verification scheme based on the cut-and-choose method. Peggy prepares N blinded messages that she claims to satisfy certain constraints and presents them to Vergy. Vergy asks Peggy to open all but one of the N messages. If Peggy can indeed demonstrate that each of the $N-1$ opened messages satisfies the required constraints, Vergy will assume that the unopened message satisfies the constraints too. She will, therefore, sign it without the opening.

2. Reduction from the quantum scheme to the classical scheme

Now, if one regards a spin 'up' as a valid message and a spin 'down' as an invalid message, the quantum problem is *exactly* the same as the classical problem: Indeed, any strategy for Peggy to cheat Vergy in the quantum case can be mapped into a strategy for Peggy to cheat Vergy in the classical scheme. All Peggy has to do to reduce the quantum problem to the classical problem is for her to perform a measurement on each spin along the z-axis. Given any quantum cheating strategy, the probabilities of passing the test successfully, $p_1 = P(\text{passing})$, and of cheating successfully, $p_2 = P(\text{passing and the remaining spin being down})$, for the quantum problem remain unchanged under such a measurement. This is because those two probabilities refer to measurement outcomes performed on the spins along a *single* basis. Clearly, a measurement on the state along *this particular basis* will not change those probabilities. For this reason, the probabilities of passing the test successfully, $P(\text{passing})$, and of cheating successfully, $P(\text{passing and the remaining spin being down})$, for the quantum problem are exactly the same as the ones for the corresponding classical problem.

In particular, suppose that in the quantum verification scheme there existed a useful cheating strategy by Peggy which gives a probability greater than $1/N$ of cheating successfully. If Peggy performs a measurement along the z-axis, this would map this cheating strategy against the quantum scheme into a strategy that cheats successfully with a probability greater than $1/N$ against the *classical* scheme. On the other hand, one can apply classical probability theory to prove rigorously that no cheating strategy against the classical scheme can cheat successfully with a probability greater than $1/N$. This leads to a contradiction. Therefore, we conclude that no quantum cheating strategy can defeat the quantum verification scheme with a probability greater than $1/N$ as well.

In summary, we have proven that the proof of security of a quantum verification scheme for spin-1/2 particles can be reduced to the proof of security of a corresponding classical verification scheme. We emphasize that the classical interpretation given above for a complete measurement is a very general concept. Whenever all the probabilities involved refer to measurement outcomes along a *single basis* and a complete measurement is performed along such a basis, a quantum mechanical experiment has a classical interpretation. In this case, classical statistical techniques such as sampling theories can be directly applied to those quantum mechanical experiments.

D. Incomplete Measurements

Consider the following problem. Eve prepares N pairs of spin-1/2 particles and gives a member of each pair to Alice, the other to Bob. She claims that they are singlets. Alice and Bob's job is to devise a verification scheme which sacrifices a small number say m pairs for measurements such that, upon passing the test, they can feel confident that the remaining $N - m$ untested pairs are, indeed, singlets. Here let us imagine in our thought experiment that at a later time Alice and Bob will finally come together to measure their $N - m$ remaining pairs to see if they are really singlets. Therefore, they will know if their verification scheme is good or not. Now, the big question is: how can such a test be devised?

The problem is trivial if Alice and Bob get together for the initial testing of the m pairs. In this case, they can perform a measurement say along the so-called *Bell* basis $\Psi^{\pm}$ and $\Phi^{\pm}$ where $\Psi^{\pm} = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$ and $\Phi^{\pm} = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle)$. Here, Ψ^{-} represents the singlet state and the rest are the three triplet states. As a complete measurement is performed, the security of this verification scheme follows from the discussion in the last subsubsection (i.e., subsubsection II C 2).

Now suppose that Alice and Bob are distant observers who prefer not to get together to test the m pairs. (However, we assume that they finally come together to measure their remaining $N - m$ pairs.) We shall state with proof that there is no local procedure (local operations plus classical communications) that will allow them to distinguish a singlet from a triplet with certainty. Now the question is the following: Is there any way for them to devise a secure quantum verification scheme? We claim that, perhaps rather surprisingly, the answer is yes. The point is that they can still distinguish between a singlet and a triplet with a *substantial* probability. Given any N pairs of particles shared between them, they randomly pick all but one pairs to perform testing (i.e. leave only one pair untested). For each pair, they randomly choose to perform one of the following three measurements. Type 1 measurement: they measure the spin of each member of a pair along the x-axis. Type 2 measurement: they measure the spin of each member of a pair along the y-axis. Type 3 measurement: they measure the spin of each member of a pair along the z-axis. Now they accept that the only remaining pair is a singlet if and only if the measurement outcomes for all the tested pairs are anti-parallel. Recall that the two members of a singlet will always give anti-parallel results upon measurements along the same axis. Consequently, if the N pairs are indeed singlets, they will always pass the above verification test.

What about a general state? A non-singlet has only a probability 1/3 of passing the test. Let us consider the above three possible types of measurements more carefully. (See Ref. [24] for details.) Measurements along the x-axis will give an anti-parallel result for the pair if its initial state is in the two-dimensional subspace spanned by Φ^- and Ψ^-. They give a parallel result for the two-dimensional subspace spanned by the other two states Φ^+ and Ψ^+. Similarly, measurements along the y-axis will give an anti-parallel result for the pair if its initial state is in the two-dimensional subspace spanned by Φ^+ and Ψ^-. They give a parallel result for the two-dimensional subspace spanned by the other two states Φ^- and Ψ^+. Also, measurements along the z-axis will give an anti-parallel result for the pair if its initial state is in the two-dimensional subspace spanned by Ψ^+ and Ψ^-. They give a parallel result for the two-dimensional subspace spanned by the other two states Φ^+ and Φ^-.

Since, for *any* of the three possible types of measurements, one can always describe the two coarse-grained (i.e. classes of) outcomes — parallel or anti-parallel — in terms of a two-dimensional projection operator along a fixed basis, it is highly tempting to give a probabilistic interpretation to those measurements. In what follows, we shall argue that this probabilistic interpretation is valid for the quantum verification scheme that we are considering. It is important to note that this interpretation works even for quantum mechanically correlated (i.e., entangled) pairs.

1. Corresponding classical scheme

Consider the following classical verification problem. Peggy has prepared N objects, each of which can be of either type W, X, Y or Z. Peggy claims that they are all of type W. Vergy's job is to verify this claim. More concretely, she would like to go through a procedure of testing all but one of Peggy's objects so that at the end she either a) rejects Peggy's claim, or 2) has the confidence that, in some sense, the untested object is almost surely of type W. Furthermore, we suppose that, for each object, Vergy can perform *one and only one* of the following three types of measurements.

Measurement type I: Distinguish $\{W, X\}$ from $\{Y, Z\}$. i.e., Vergy gets the yes/no answer to the question: Is this object of type W or X (but not of type Y or Z)?

Measurement type II: Distinguish $\{W, Y\}$ from $\{X, Z\}$.

Measurement type III: Distinguish $\{W, Z\}$ from $\{X, Y\}$.

Now consider the following procedure. Vergy randomly picks all except one objects to perform testing (and leaves one object untested): The testing is done as follows. On each object, Vergy randomly chooses one of the above three types of measurements to perform. She accepts the result if and only if *all* the measurement outcomes indicate that the tested samples are consistent with their identity being of type W. Only in this case, will she assume the only remaining untested object to be of type W.

We now show that no cheating strategy by Peggy can allow her to cheat successfully with a probability greater than $1/N$. Suppose only $N - e$ of the objects prepared by Peggy are of type W and Vergy goes through the above random testing scheme on all except one objects. Let us use the notation 'bad' to refer to the fact that the remaining (i.e., untested) object is not of type W. Now,

$$
\begin{aligned}
& P(\text{cheating successfully in the classical scheme}) \\
\equiv\ & P(\text{bad and passing the test}) \\
=\ & P(\text{bad})P(\text{passing the test} \mid \text{bad}) \\
=\ & \frac{e}{N}(\frac{1}{3})^{e-1},
\end{aligned} \tag{1}
$$

which attains the maximum value of $1/N$ when $e = 1$. (Recall that e out of the N objects are bad and that any object not of type-W has only a probability $1/3$ of passing a random test.)

2. Reduction from the quantum scheme to the classical scheme

We now claim that the security of the quantum verification scheme reduces to the classical scheme. Briefly stated, the reasoning is as follows: Given any cheating strategy against the quantum verification scheme by Eve, she can map it into a cheating strategy against the classical verification scheme by Peggy. Eve does this by performing measurements along Bell basis. Perhaps more importantly, the resulting classical cheating strategy is equally successful as the original quantum cheating strategy. Now suppose there exists a highly successful quantum cheating strategy, then after the mapping, it becomes a highly successful classical cheating strategy. But we have just seen in the last subsubsection that this is impossible. Therefore, we conclude that the quantum verification scheme must be secure.

We must emphasize that this reduction argument works because all the probabilities involved refer to a single basis — Bell basis. Consequently, the quantum verification scheme has a classical interpretation. We also remark that basis vectors of Bell basis are all maximally entangled. It is a priori surprising that a quantum mechanical experiment (involving local operations and classical communication only) will acquire a classical interpretation with respect to such a highly non-local basis.

We shall now discuss our reasoning in more detail. Recall that we assume that, after performing the verification test described in subsection II D on the $N-1$ pairs, Alice and Bob actually come together to determine if the remaining pair is a singlet or not. This is, in principle, a doable experiment. Notice that, the most general cheating strategy by the eavesdropper Eve in the quantum scheme is for her to prepare an entangled state of the system consisting the N pairs and an ancilla (of arbitrarily high dimension) under her control. Since any mixed state can be represented by a pure state by including the quantum die explicitly, we shall, without loss of generality, consider that Eve prepares a pure state only. Using the convention of Ref. [24], two classical bits are used to label each of the Bell states.

$$
\begin{aligned}
\Phi^+ &= 00 = 0 \\
\Psi^+ &= 01 = 1 \\
\Phi^- &= 10 = 2 \\
\Psi^- &= 11 = 3.
\end{aligned} \tag{2}
$$

Eve prepares a pure state

$$|u\rangle = \sum_{i_1,i_2,\cdots,i_N} \sum_j \alpha_{i_1,i_2,\cdots,i_N,j} |i_1, i_2, \cdots, i_N\rangle \otimes |j\rangle, \tag{3}$$

where i_j denotes the state of the j-th pair and it runs from 0 to 3, and $|j\rangle$'s form an orthonormal basis for the ancilla. Each state $|u\rangle$ represents a particular cheating strategy chosen by Eve.

For any state $|u\rangle$ (and hence any cheating strategy by Eve) in this experiment, we define the following probability:

$$\begin{aligned} & P(\text{cheating successfully in the quantum scheme}) \\ \equiv\ & P(\text{bad and passing the test}) \\ =\ & \frac{1}{\binom{N}{1} 3^{N-1}} \sum_{S_1} \sum_{S_2} \sum_{S_3} \sum_{i_1,i_2,\cdots,i_N}{}' \sum_j |\alpha_{i_1,i_2,\cdots,i_N,j}|^2, \end{aligned} \tag{4}$$

where S_i's are disjoint subsets of the set $\{1, 2, \cdots N\}$ such that their union $S_1 \cup S_2 \cup S_3$ contains $N-1$ elements and the sum $\sum'_{i_1,i_2,\cdots,i_N}$ is a sum over $i_1, i_2, \cdots, i_N$ such that, for each i_l, (a) if $l \in S_1$, the sum is over $i_l = 2$ or 3, (b) if $l \in S_2$, the sum is over $i_l = 0$ or 3, (c) if $l \in S_3$, the sum $i_l = 1$ or 3, and (d) if $l \notin S_1 \cup S_2 \cup S_3$, the sum is over $i_l = 0$ or 1, or 2. Here, for pairs in S_1 (i.e., case (a)), Alice and Bob measure the spins along the x-axis. For pairs in S_2 (i.e., case (b)), Alice and Bob measure the spins along the y-axis. For pairs in S_3 (i.e., case (c)), Alice and Bob measure the spins along the z-axis. For the remaining pair (which does not belong to $S_1 \cup S_2 \cup S_3$, i.e., case (d)), we imagine that Alice and Bob finally come together to measure it to see if it is a singlet. Conditions (a), (b) and (c) taken together are equivalent to the requirement that $N-1$ tested pairs pass the verification test. In other words, each of them gives anti-parallel results upon measurement. Condition (d) is equivalent to the requirement that the remaining pair (the l-th pair such that $l \notin S_1 \cup S_2 \cup S_3$) is 'bad' (i.e. not a singlet) upon measurement.

Notice that in Eq. (4) we are expressing the probability of cheating successfully in Bell basis (with bases vectors $\Psi^\pm$ and $\Phi^\pm$) for the N pairs and in any orthonormal basis say $|a_i\rangle$'s for the ancilla. In this basis, this probability is a sum of squared moduli of the coefficients of the terms satisfying the requirements of being bad (i.e. the remaining pair is not a singlet) and passing the verification test in the classical sense. Indeed, whether a state passes the test and whether the remaining object is good could be *totally* determined if a complete measurement along Bell basis for the N pairs and a measurement along $|a_i\rangle$'s for the ancilla were performed.

Since the measurement outcomes refer to this single basis, we conclude that this quantum mechanical experiment has simple classical explanations: Recall that any cheating strategy of Eve (or Peggy) corresponds to the preparation of a pure state $|u\rangle$ for the system consisting of the N pairs and the ancilla. Now, given *any* quantum state of the N pairs of spin-1/2 particles prepared by Eve, suppose Eve *measures* it along Bell basis for the pairs and $|a_i\rangle$'s for the ancilla. After the measurement, the N pairs become 'classical' with respect to Bell basis. To be more precise, their state in Bell basis is now fully described by a *diagonal* density operator:

$$\rho_{\text{measured}} = \sum_{i_1,i_2,\cdots,i_N} \sum_{a_i} |\alpha_{i_1,i_2,\cdots,i_N,j}|^2 |i_1\rangle\langle i_1||i_2\rangle\langle i_2| \cdots |i_N\rangle\langle i_N||a_i\rangle\langle a_i|. \tag{5}$$

This reduces the quantum verification problem into a classical verification problem.

More importantly, the probability, as defined in Eq. (4), of cheating successfully in the quantum verification scheme by using the original state $|u\rangle$ will be precisely the same as the probability, as in Eq. (1), of cheating successfully in the classical verification scheme using the state ρ_{measured} resulting from measuring the state $|u\rangle$ along Bell basis and $|a_i\rangle$'s. Indeed, the operator for cheating successfully, P_{ch}, is a *diagonal* projection operator in Bell basis, i.e., a diagonal operator with entries 1's and 0's only. Therefore, for a measurement along Bell basis, we have $\text{Tr}(|u\rangle\langle u|P_{\text{ch}}) = \text{Tr}(\rho_{\text{measured}} P_{\text{ch}})$ and there is no change in the probability of cheating successfully due to the measurement.

We now argue that no cheating strategy against the quantum scheme can defeat it with a probability larger than $1/N$. We prove it by contradiction. Suppose there exists a wonderful cheating strategy against the quantum scheme which gives a probability of cheating successfully larger than $1/N$, using the above reduction theorem it can be mapped into a wonderful cheating strategy against the corresponding classical scheme with a probability of cheating successfully larger than $1/N$. However, we have proven in the subsubsection II D 1 that no cheating strategy can defeat the classical scheme with a probability larger than $1/N$. This leads to a contradiction. Therefore, we conclude that no cheating strategy against the quantum scheme can defeat it with a probability larger than $1/N$. i.e.,

$$
\begin{aligned}
& P(\text{cheating successfully in the quantum scheme}) \\
\equiv\ & P(\text{bad and passing the test}) \\
\leq\ & 1/N.
\end{aligned}
\tag{6}
$$

3. Coarse graining

An important remark is in order. The classical interpretation discussed above refers only to the coarse-grained probabilities, i.e., for each pair, the sum of probabilities of some outcomes, e.g. the probability for anti-parallel outcomes which include 'up, down' and 'down, up'. Unlike the coarse-grained probabilities, the fine-grained probabilities (i.e., those of complete measurement outcomes, 'up, up', 'up, down', 'down, up' and 'down, down') are *changed* by Eve's measurements.

Recall that vectors in Bell basis are maximally entangled. As remarked earlier, it is perhaps surprising at first sight that the coarse-grained probabilities of a quantum mechanical experiment involving only local operations and classical communications can have a classical interpretation with respect to such a highly non-local basis.

III. SECURITY OF QUANTUM KEY DISTRIBUTION: ERROR-FREE CASE

We will now show that the above verification scheme is sufficient for proving the security of a one-bit key generated by quantum key distribution in the error-free case. Here, by error-free we assume a) that the channel is *noiseless* and b) that there are no storage errors and c) that all operations (preparation, unitary transformations and measurements by Alice and Bob) can be performed perfectly.

In this case, Alice simply prepares N EPR pairs and sends a member of each pair to Bob. They then go through the quantum verification scheme described in subsection II D: That is to say, they randomly pick $N-1$ pairs to test (and leave one pair untested). For each of the $N-1$ pairs, they randomly choose to measure along either the x-axis, the y-axis or the z-axis. They demand that the two members of each pair always give anti-parallel results. When this happens, they accept the remaining pair as secure. i.e., they will assume it to be a singlet and hence be unentangled with Eve. Otherwise, they discard the remaining pair. If they accept the remaining pair, then they randomly pick from x-, y- or z-axis to measure the spins of the two members.

A. Two important statements for proving security of quantum key distribution

We divide the proof of the security of the generated key into two steps. Firstly, given any $1 > p > 1/N$, we show that *any* cheating strategy by Eve that passes the verification test with *a priori* probability greater than p must give a fidelity greater than $1 - \frac{1}{pN}$ for the remaining pair as a singlet when the verification step is passed. Secondly, we prove that a high fidelity is a sufficient condition for the security of quantum key distribution. In particular, high fidelity implies low entropy. The proofs of these two statements are given in appendix A.

B. A subtlety

There is, in fact, an important subtlety that we must take into account in our proof of security of quantum key distribution. Recall that the actual complete measurement outcome for each pair, say 'up, down' or 'down, up' for a successful verification step is publicly announced. One might wonder if Eve could gain additional information about the generated key from this announcement. If this were possible, it would be a total disaster. We remark that the answer is no.

To understand our argument, let us divide the system into two parts: the remaining pair(s) and 'the rest' (i.e., the tested pairs plus Eve's system). The key observation is that the measurements on the verification step are performed on the tested pairs, which are part of 'the rest', *rather than* the remaining pair(s). Now once we have shown that the entropy of the *remaining pair(s)* is small, no local measurements on 'the rest' can possibly increase this entropy [24]. More importantly, by Kholevo's theorem [33] this entropy provides an upper bound on the amount of classical mutual information between the remaining pair(s) and 'the rest'. Since Eve's system is only part of 'the rest', this entropy provides a rigorous bound on her information about the generated key.

IV. RANDOM HASHING

For simplicity, in our above discussion we have only introduced a simple verification scheme. In actual applications, we suggest employing a verification scheme based on random hashing proposed by Bennett *et al.* [24]. This scheme requires only a very number of tested pairs to achieve exponential security and is, thus, much more efficient than the simple scheme that we have discussed. This random hashing scheme requires non-trivial quantum computations on the pairs before the actual verification. This, however, does not create any problem. See appendix B for details. This completes our discussion on the error-free case of the security of our quantum key distribution scheme.

V. NOISY CHANNEL, STORAGE ERRORS AND COMPUTATION ERRORS

In this section, we will introduce errors into the system and briefly discuss how they can be overcome. There are many sources of errors in a quantum key distribution scheme. First of all, the quantum communication channel between Alice and Bob is unavoidably noisy. Moreover, errors (decoherence) will occur during the storage of quantum information. Furthermore, errors may also occur during quantum computation: There are two types of computational errors, namely gate errors and measurement errors. The reason is that the elementary gates used for quantum computation and all real measurements are imperfect. In what follows, we will argue that the general theory of fault-tolerant quantum computation (and quantum error correction) can be used to overcome all sources of errors.

A general theory of fault-tolerant quantum computation [29–32] has been developed. For a review, see, for example, Ref. [28]. In particular, assuming an independent noise model, once the probability of error for each primitive computational gate and that for each time step of storage become smaller than a threshold value, it has been argued that arbitrarily large quantum computations can be done with an arbitrarily high fidelity using fault-tolerant quantum computation.‡§ The quantum information is in an encoded form during the computation.

Our basic philosophy is to extend this threshold theorem for fault-tolerant *local* quantum computation to *distributed* quantum computation. More precisely, we shall argue that by encoding quantum signals before the transmission through quantum channels and if necessary by setting up 'relay stations' to manipulate the signals *during the transmissions*, any procedure of distributed quantum computation can be done fault-tolerantly. We remark that useful procedures for entanglement purification have already been discussed in the literature [37–39] and are widely accepted.

In the special case of quantum key distribution, our global strategy is as follows. We argue that one can devise a quantum key distribution scheme through a noisy channel such that at the end each of Alice and Bob's systems can be written as a block of a fault-tolerant quantum error correcting code. They can then apply the recovery procedure to their state.

---

‡Fault-tolerant quantum computation developed after the discovery of quantum error correcting codes [34–36] by Shor and independently by Steane.

§Indeed, heuristic calculations suggest that an *exponentially* small error rate, i.e. fidelity $1 - e^{-n}$ for some large n, for the *encoded* quantum information, can be achievable through concatenated coding. Eq. (36) of Ref. [28] says that, roughly speaking, if the threshold gate error rate is ϵ_0, and the actual elementary gate error rate is $\epsilon < \epsilon_0$, then concatenating the code L times will reduce the error rate to $\epsilon^{(L)} \sim \epsilon_0 \left(\frac{\epsilon}{\epsilon_0}\right)^{2^L}$.

Alice and Bob can now go through the verification step as discussed in subsubsection II D 2. The difference is that the verification is now done on the *encoded* state using fault-tolerant quantum computation.

Our Trust Model: In the most general eavesdropping strategy Eve prepares the state of Alice and Bob. i.e., Eve has complete control over the relay stations as well as the quantum communication channel. Alice and Bob only trust their own quantum computers and authenticated classical messages from each other.

To understand the security of our scheme, it is convenient to consider the problem in the mathematical basis where the physical qubits are written as a tensor product of the logical qubits (which contain the actual quantum information) and the ancilla qubits (which contain the error syndromes). Fault-tolerant quantum computation tells us that the logical qubits will, with a very high fidelity $(1 - O(e^{-l}))$, remain unchanged, provided that the storage and gate error rates are smaller than some critical values. Besides, the verification and subsequent key generation steps can be thought of as being performed *solely* on the logical qubits. The ancilla qubits are irrelevant for those steps, despite their usefulness in the error correction steps. Now, our discussion of the reduction theorem in subsubsection II D 2 carries over completely except that it refers to the logical qubits rather than the physical ones.

As in subsubsection II D 2, the verification step will ensure that Eve's entanglement with the logical qubits is most likely to be negligible. Consequently, Eve has very little information about the generated key. However, notice that Eve's system can be significantly entangled with the ancilla qubits. So Eve may learn as much as she likes about the error syndrome found by Alice and Bob in their recovery procedure. Fortunately, by the virtue of quantum error correction, the error syndrome tells her nothing about the logical qubits. Consequently, Eve most likely has a negligible amount of information about Alice and Bob's generated key *whenever* the verification step is passed. See Appendix B 4 for our rigorous bound on Eve's information. Therefore, our key distribution scheme is secure against all types of errors and all types of attacks — including joint attacks. A more detailed discussion of the fault-tolerant procedure can be found in appendix C.

VI. CONCLUDING REMARKS

The most important conceptual point of this paper is that a quantum mechanical experiment has a classical interpretation whenever probabilities referring to *only one* basis are considered. More specifically, given an experiment involving measurements along a basis chosen randomly from a set of possible bases, one may, nevertheless, perform *coarse-graining* (i.e., a grouping) of the measurement operators. If the coarse-grained operators for such a measurement can be re-written as the projection operators along a single basis, then the coarse-grained probabilities associated with those coarse-grained operators have classical interpretations. It may seem paradoxical that it is with respect to the highly non-local Bell basis that our verification scheme acquires a classical interpretation. We emphasize that this quantum to classical reduction technique can potentially have many applications.

We have proceeded as follows. We first introduce a quantum verification scheme together with a corresponding classical verification scheme. We then show that, rather paradoxically, the quantum verification scheme has a classical interpretation. i.e., Given a cheating strategy against the *quantum* scheme, one can map it into a cheating strategy against the *classical* scheme with the *same* probability of success. The mapping is done by the cheater Eve's performing a measurement along a *single* basis, namely Bell basis. Consequently, its security is reduced to the security of the corresponding classical scheme, which can be established by simple classical probability theory.

Afterwards, we show that this quantum verification scheme can be used as a proof of security of a quantum key distribution scheme in an error-free environment.

Noises and errors (channel noises, storage errors and computational errors) are then taken in account. Specifically, we show that the general theory of fault-tolerant quantum computation and fault-tolerant quantum error correction can be used to overcome all types of errors. We consider the most general eavesdropping strategy by Eve, in which Eve prepares the state to be tested by Alice and Bob. By integrating out all the computations and communications performed by the intermediate connection points, each of Alice and Bob at the end should have some state in the encoded form of a quantum error correcting code. They perform the recovery procedure to correct errors.

One can mathematically re-express Alice (or Bob)'s state as a tensor product of the logical (i.e. informational) qubits and the ancilla qubits (which contain the error syndromes). Our discussion for error-free case carries over completely to the noisy case except that the verification and key generation steps now refer *solely* to the logical qubits. *Upon passing* the verification step, we are almost sure that Eve has very little entanglement with the logical qubits and, hence, has very little information about the generated key. This is so, even though she can have as much entanglement as she likes with the ancilla qubits.

We remark that our proof of security applies not only to entanglement-based schemes, but also to *encoded* versions of single-particle-based schemes such as BB84.[**] (The encoding is used simply for quantum error correction and is not directly related to the security analysis.) Indeed, in our scheme Alice is allowed to perform measurements on her part of the system before sending out Bob's part. This is fine provided that Alice withholds the information on the bases of her measurements until Bob has acknowledged the receipt of all the quantum signals.

Our result puts the whole subject of quantum key distribution on solid foundation. An important implication of our result is that, given quantum computers, (both entanglement-based and single-particle-based schemes of) quantum key distribution over an arbitrarily long distance of a realistic noisy channel can be made unconditionally secure.

Now that we have learnt that quantum key distribution is unconditionally secure and that quantum bit commitment is impossible, the natural questions for future investigations are: What is the boundary to the power of quantum cryptography? And why is there such a boundary?

ACKNOWLEDGMENTS

H.-K. Lo particularly thanks A. Ekert for pressing him to investigate the security of quantum key distribution. We thank C. H. Bennett, G. Brassard, D. P. DiVincenzo, D.

[**]We thank C. H. Bennett for pointing this out to us.

Gottesman, E. Knill, D. W. C. Leung and T. Spiller for invaluable conversations and suggestions. One of us (H. F. C.) is supported by the Hong Kong Government RGC grant HKU 7095/97P.

Notes Added: After the completion and circulation of a preliminary version of this paper, we have learnt that Mayers and Yao [40] have also written a new preprint on the subject.

APPENDIX A: PROOFS OF THE TWO IMPORTANT STATEMENTS

Here we present the proofs of the two important statements used in subsection III A.
Statement 1: Consider the error-free case of our quantum key distribution scheme. Given any $1 > p > 1/N$ and any cheating strategy by Eve that passes the verification test with a probability greater than p, the fidelity of the remaining pairs as a singlet *conditional* on passing the test is greater than $1 - \frac{1}{pN}$
Proof: Given any strategy, we know from Eq. (6) that

$$\begin{aligned} & P(\text{cheating successfully in the quantum scheme}) \\ \equiv\, & P(\text{bad and passing the test}) \\ \leq\, & 1/N. \end{aligned} \tag{A1}$$

Here 'bad' means that the remaining pair fails the yes/no test of being a singlet upon measurement. Now suppose that a cheating strategy gives

$$\begin{aligned} & P(\text{passing the test}) \\ =\, & P(\text{bad and passing the test}) + P(\text{good and passing the test}) \\ >\, & p, \end{aligned} \tag{A2}$$

where 'good' means that the remaining pair passes the yes/no test of being a singlet upon measurement. Notice that Eve should only be interested in cheating strategies which give non-negligible value for p. But then $P(\text{good and passing the test}) > p - 1/N$. Therefore, for any strategy satisfying Eq. (A2), the fidelity of the remaining pair as a singlet *conditional* on passing the test:

$$\begin{aligned} & F \\ =\, & P(\text{good} \mid \text{passing the test}) \\ =\, & \frac{P(\text{good and passing the test})}{P(\text{passing the test})} \\ >\, & \frac{p - \frac{1}{N}}{p} = 1 - \frac{1}{pN}. \end{aligned} \tag{A3}$$

Now we should think of p as a security parameter for the test. Given any fixed p, by increasing N, we can increase the *conditional* fidelity of the remaining pair, which is used to generate the key. □

Now we come to the second statement — that a high fidelity of the remaining pair is a sufficient condition for security. We first note that security is guaranteed if the following three conditions are fulfilled: (a) Alice and Bob almost surely generate the same key; (b) The generated key is almost random; and (c) Eve has little information about the key.

Now it is quite clear that a high fidelity implies the first two conditions. What about the last condition? The following lemma shows that it is also satisfied.

Lemma 1: (High fidelity implies low entropy) If $\langle R \text{ singlets}|\rho|R \text{ singlets}\rangle > 1-\delta$ where $\delta \ll 1$, then $S(\rho) < -(1-\delta)\log_2(1-\delta) - \delta \log_2 \frac{\delta}{(2^{2R}-1)}$.

Proof: If $\langle R \text{ singlets}|\rho|R \text{ singlets}\rangle > 1-\delta$, then the largest eigenvalue of the density matrix ρ must be larger than $1-\delta$, the entropy of ρ is, therefore, bounded above by that of $\rho_0 = \text{diag}\,\{1-\delta, \frac{\delta}{(2^{2R}-1)}, \frac{\delta}{(2^{2R}-1)}, \cdots, \frac{\delta}{(2^{2R}-1)}\}$. That is, ρ_0 is diagonal with a large entry $1-\delta$ and with the remaining probability δ equally distributed between the remaining $2^{2R}-1$ possibilities. □

To apply the above lemma to our problem, take ρ to be the reduced density matrix of the remaining $N-m$ pairs and R to be $N-m$. Now a very high fidelity of the remaining pairs as singlets implies that the entropy of the remaining pairs tends to 0. But then the entropy provides a bound on the amount of classical information that Eve may have on the key. We have, thus, proven that a very high fidelity is a sufficient condition for the security of quantum key distribution.

APPENDIX B: SECURITY OF A QUANTUM KEY DISTRIBUTION SCHEME BASED ON RANDOM HASHING

Here we shall discuss a more efficient quantum verification scheme. It is based on a one-way hashing scheme for entanglement purification developed by Bennett *et al.* [24]. In Ref. [24], a Bell state is represented by two classical bit (see Eq. (2)). A $2N$-bit string x_0 forms a basis for the state of the N pairs. The parity of a string is a modulo-2 sum of its bits. Now the parity of a subset s of the bits in a string x can be expressed as a Boolean inner product $s \cdot x$ which is the modulo sum of the bitwise AND of the strings s and x. In the most general eavesdropping strategy, the state of the N pairs and Eve's ancilla can be written as an entangled state of the two subsystems. The important observation made by Bennett *et al.* [24] is that, by applying *local* operations (which include BXOR bilateral $\pi/2$ rotations and unilateral Pauli rotations), followed by local measurement of one of the pairs, one can measure the parity of an arbitrary chosen subset s of the unknown x.

Notice that, for any two distinct strings $x \neq y$, the probability that they give the same parity for a random subset, i.e., $s \cdot x = s \cdot y$ is exactly 1/2. This is because $(s \cdot x) \oplus (s \cdot y) = s \cdot (x \oplus y)$.

Suppose m rounds of hashing are performed. After each round of the hashing, the tested pair is discarded from our consideration and, therefore, each of the basis state is mapped into a shorter string. More concretely, suppose initially the N pairs are described by a basis of $2N$-bit long strings. Suppose Alice and Bob measure the parity of the set s_0. In round one, an initial $2N$-bit string x_0 is mapped into a $(2N-2)$-bit string $x_1 = f_{s_0}(x_0)$. Similarly, in the second round, x_1 is mapped into a $(2N-4)$-bit string $x_2 = f_{s_1}(x_1)$. Given any two initial strings x_0 and y_0, it is then shown in [24] that the probability that the remaining strings are different and yet the random parities computed in the first m rounds are the same, i.e. $P((x_m \neq y_m)$ and$(s_k \cdot x_k = s_k \cdot y_k)$ for $0 \leq k \leq m-1)$ is at most 2^{-m}.

In our quantum verification scheme, Alice and Bob are given N pairs of spin-1/2 particles. Only *after* their confirmation of the receipt of their quantum particles, Alice and Bob iteratively select m random subsets of the string and perform m rounds of random hashing by using local operations and (one-way) classical communications. They demand that each round gives the correct parity as what they would expect starting from N singlets. If the test is passed, they expect the remaining $N-m$ pairs as secure and use them to generate an $(N-m)$-bit key. The key generation is done by measuring the spin of each pair randomly along x-, y- or z-axes.

1. Classical scheme

In the classical case, the input is a string of length $2N$. Each round of the hashing reduces the string length by 2 bits. m rounds of hashing are applied and this is used to verify that the remaining string is, in fact, $11\cdots1$. i.e., a $(2N-2m)$-bit string made up of 1's only. From the above discussion, we learn that no cheating strategy can defeat such a verification scheme with probability larger than 2^{-m}.

2. Reduction in the random hashing scheme

Notice that the above probability refers to a single basis, namely Bell basis. Being so, we now argue the following important fact: such a random hashing scheme has a classical interpretation. In particular, we argue that there exists no cheating strategy that can pass the random hashing test and yet produce a 'bad' state for remaining pair with a probability greater than 2^{-m}.

The proof of this reduction is essentially as in subsubsection II D 2. Suppose that there exists a cheating strategy that succeeds with a probability larger than 2^{-m} against the quantum scheme. Now let Eve performs a measurement along Bell basis. This measurement will collapse the wavefunction into a diagonal density operator in Bell basis. Such a state can be used in a cheating strategy that succeeds with a probability greater than 2^{-m} against the classical scheme. But this has just been proven to be impossible in the last subsection.

3. Security of quantum key distribution

With the above reduction theorem, one can now establish rigorously the security of a quantum key distribution scheme based on the random hashing verification step. The discussion there parallels that in appendix A.

Given any cheating strategy against the quantum verification scheme by Eve, let p_1 ($p_2 = 1 - p_1$ respectively) be the total probability for the state of the N pairs to be N singlets (to be something else respectively), under the measurement along Bell basis. The case of N singlets (Case A), which happens with a probability p_1, will automatically pass the verification test and give $N-m$ singlets as the remaining pair. This case is perfectly fine and secure. What about the other case? Upon a random hashing verification scheme that sacrifices m pairs, the other case (which happens with probability p_2) will be further divided into three cases. Either (B1) it passes the verification and gives a residual state for the $N - m$ pairs that *are* singlets, or (B2) it passes the verification and gives a residual state for the remaining $N - m$ pairs which are *not* N singlets, or (B3) it fails the verification test and is, therefore, rejected. Let us assign probabilities a, b and $p_2 - a - b$ to these three cases.

Notice that the cases (A) and (B1) are secure because the remaining pairs are $N - m$ singlets. On the other hand, case (B2) is insecure because the remaining pairs are not singlets, even though the verification test is passed. Now, from arguments in section IV, we learn that the probability of passing and being bad is not more than 2^{-m}. i.e.,

$$b \leq 2^{-m} p_2 \leq 2^{-m}. \tag{B1}$$

Since only cases (A), (B1) and (B2) pass the test, the probability that a strategy passes the verification test is given by

$$P(\text{passing}) = p_1 + a + b. \tag{B2}$$

Eve would better be interested in a cheating strategy that passes the test with a non-negligible probability, say at least 2^{-r} where we assume that $r \ll m$. Therefore, we demand that

$$P(\text{passing}) = p_1 + a + b \geq 2^{-r}. \tag{B3}$$

Now, the fidelity of the $N - m$ pairs as singlets is given by

$$F' = \frac{p_1 + a}{p_1 + a + b} \geq \frac{p_1 + a}{p_1 + a + 2^{-m}} \tag{B4}$$

where Eq. (B1) has been used.

The numerator of Eq. (B4) is

$$\begin{aligned} p_1 + a &= p_1 + a + b - b \\ &\geq 2^{-r} - b \\ &\geq 2^{-r} - 2^{-m} \\ &= 2^{-m}(2^{m-r} - 1), \end{aligned} \tag{B5}$$

where Eqs. (B3) and (B1) are used in getting the second and third lines respectively.

Therefore, we find, from Eqs. (B4) and (B5) that

$$\begin{aligned} F' &\geq \frac{p_1 + a}{p_1 + a + 2^{-m}} \\ &\geq \frac{2^{-m}(2^{m-r} - 1)}{2^{-m}(2^{m-r} - 1) + 2^{-m}} \\ &= \frac{(2^{m-r} - 1)}{2^{m-r}} \\ &= 1 - 2^{-(m-r)} \end{aligned} \tag{B6}$$

for any cheating strategy that passes the verification test with a probability at least 2^{-r} where $r \ll m$. Therefore, given any security parameter r, one can increase the conditional fidelity in Eq. (B6) by increasing the number m of random parities computed.

Now, by a similar proof of lemma 1 in appendix A, a high fidelity is a sufficient condition for the security of quantum key distribution.

a. A subtlety

Actually, there is a subtlety in the above discussion. The subtlety is that non-trivial quantum computation is performed during the computation of the parity of a random subset. This quantum computation generally *changes* the density matrix of the remaining pairs. For instance, in the case of having two pairs in the initial state

$$|u_i\rangle = a|0000\rangle + b|0011\rangle. \tag{B7}$$

Suppose the random string s is chosen to be 0101. The density matrix of the second pair is computed from the partial trace over the first pair:

$$\rho_i = \mathrm{Tr}_{\text{first two qubits}}|u_i\rangle\langle u_i| = (a|00\rangle + b|11\rangle)(a^*\langle 00| + b^*\langle 11|). \tag{B8}$$

Let us collect the parity of the subset s in the second bit of the first pair. After the quantum computation, the final state becomes

$$|u_f\rangle = a|0000\rangle + b|0111\rangle. \tag{B9}$$

Now, the density matrix of the second pair becomes

$$\rho_f = \mathrm{Tr}_{\text{first two qubits}}|u_f\rangle\langle u_f| = |a|^2|00\rangle\langle 00| + |b|^2|11\rangle\langle 11|, \tag{B10}$$

which is generally different from Eq. (B8). This shows that the density matrix of the remaining pairs are changed by the quantum computation of the random parity. Naively, one might think that this will be a problem to our reduction argument from a quantum to a classical scheme.

However, this is not really a problem because we are not interested in the density matrix of the remaining pairs itself. All we care about is the fidelity of the remaining pairs in Bell basis. Unlike the density matrix, this fidelity is *not* changed by the computation of the random parity. Therefore, our reduction argument remains valid. This can be seen in the above example by computing the fidelity before the computation from

$$F_i = \langle 11|\rho_i|11\rangle = |b|^2, \tag{B11}$$

and that after the computation,

$$F_f = \langle 11|\rho_f|11\rangle = |b|^2. \tag{B12}$$

The fidelities F_i and F_f before and after the measurement are exactly the same. This fact — that (up to a reordering of basis) the fidelity of the remaining pairs as singlets remains unchanged during the computation of the parity of a random subset — is true for any initial state of the N pairs.

4. Bound on Eve's information

For completeness, we now derive a bound on Eve's information for any eavesdropping strategy that passes an m-round random hashing verification scheme with a probability at least 2^{-r} (where $m \gg r$). From Eq. (B6), upon passing the test, the conditional fidelity of the remaining $N-m$ pairs as singlets is at least $1-2^{-(m-r)}$. Putting $\delta = 2^{-(m-r)}$ in Lemma 1 of Appendix A, we find that the entropy of the remaining pairs

$$S < -[1-2^{-(m-r)}]\log_2[1-2^{-(m-r)}] - 2^{-(m-r)}\log_2[\frac{2^{-(m-r)}}{2^{2(N-m)}-1}]. \tag{B13}$$

Let us first consider the first term in Eq. (B13). Noting that $log_2(1-\delta) = log_e(1-\delta)/log_e 2 = \frac{1}{log_e 2}(-\delta + O(\delta^2))$, the first term is equal to $\frac{1}{log_e 2}(\delta + O(\delta^2))$ where $\delta = 2^{-(m-r)}$. We now turn to the second term in Eq. (B13). It is bounded above by $-2^{-(m-r)}\log_2[\frac{2^{-(m-r)}}{2^{2(N-m)}}] = 2^{-(m-r)}[2N-m-r]$. Combining these two results together, we find an upper bound on the entropy

$$S < 2^{-(m-r)}[\frac{1}{log_e 2} + 2N - m - r] + O(2^{-2(m-r)}). \tag{B14}$$

For instance, if the number m of rounds satisfies

$$m > \log_2(2N) + k + r \tag{B15}$$

where $k > 0$, then the entropy

$$S < c \times 2^{-k} \tag{B16}$$

for some constant $c > 0$. Therefore, given any $k > 0$, one can guarantee that the entropy of the remaining pairs (and hence Eve's information on the generated key) is bounded above by $c \times 2^{-k}$ simply by choosing $m > \log_2(2N) + k + r$. This statement is valid for any eavesdropping strategy that gives at least a probability 2^{-r} of passing the verification test performed by Alice and Bob. This completes our proof of security of our random-hashing based quantum key distribution scheme.

Incidentally, our scheme remains secure even when its efficiency $\frac{N-m}{N}$ exceeds 50%. For a discussion on the efficiency of quantum key distribution, see Ref. [41].

APPENDIX C: ERRORS

Here we discuss the procedure of fault-tolerant quantum key distribution in more detail.

1. Storage Errors

When the error rates of the quantum gates and of the elementary storage devices are below the accuracy threshold, it is possible to maintain an *unknown* quantum state an indefinitely long time. If the probability of a storage error per computational time step is ϵ, then the initial encoding and hence the final decoding of the state can be performed with a fidelity no better than $F = 1 - O(\epsilon)$.[††]

Now suppose we are given a quantum channel with an error rate $\delta < \delta_0$ where δ_0 is the threshold value for fault tolerant quantum computation but with a *limited* transmission rate, say one quantum signal at each time step. We remark that the bottleneck in waiting in the queue for the transmission does not create much problem. Suppose we would like to send P qubits through such a channel. In the input and output queues, decoherence in the waiting period is prevented by putting each qubit in an encoded form of a quantum error correcting code. Each qubit should be in its bare form only during the actual transmission. i.e., it should be decoded just before the transmission and encoded again immediately after the transmission. By doing so, we can effectively convert the quantum channel into one with an error rate $e = O(\delta + \epsilon)$ (assuming independent errors) but with an unlimited transmission rate.

For ease of discussion, we shall, therefore, ignore all storage errors and focus only on the channel errors. We also assume that the channel has an unlimited transmission rate.

2. fault-tolerant distributed quantum computations over noisy channels

a. channel error rate less than the threshold value

Let us first consider the case that the channel error rate is less than the threshold value $e < \epsilon_0$ for fault-tolerant quantum computation. Suppose Alice picks a fault-tolerant quantum error correcting code that encodes N qubits into $K > N$ qubits. Alice prepares two blocks of K qubits with each block representing the encoded form of N qubits in the spin up. She performs fault tolerant quantum computation to change the state into the encoded form of N EPR pairs. The two blocks, if separated, represent the encoded state of N EPR pairs shared between two observers. She now sends one of the two blocks through the noisy quantum channel to Bob. Bob then corrects the errors due to the transmission. Assuming that the channel noises are independent and are below the threshold value, fault-tolerant quantum error correction can be applied to correct all likely channel noises. Therefore, Alice and Bob will end up to share the encoded form of N EPR pairs.

b. channel error rate greater than the threshold value

Suppose Alice and Bob are separated by an arbitrarily long distance. The channel error rate may now exceed the threshold value. A naive application of the threshold theorem will not work. However, as discussed by Briegel *et al.* [37], Alice and Bob can still overcome the channel noises by the following method: They can divide up the transmission process by setting up intermediate connection points (or relay stations). In those connection points,

---

[††]See, for example, section 3.5 of Ref. [28] for a discussion on the encoding process. Notice that, for many block coding schemes, the decoding process is just the inverse of the encoding process. Therefore, it can be done with a similar fidelity.

they are now allowed to perform quantum computations. ".. In the context of fault-tolerant quantum computing, using concatenated quantum codes, Knill and Laflamme have discussed an important scheme that allows (one), in principle, to transmit a qubit over arbitrary long distances with a polynomial overhead in the resources. The method requires (one) to encode a single qubit into an entangled state of a large number of qubits, and to operate on this code repeatedly *during the transmission process.* The tolerable error probabilities for transmission are less than 10^{-2}, whereas for local operations, they are less than 5×10^{-2}. This seems to be outside the range of any practical implementation in the near future." [37]

Briegel *et al.* [37] also presented a model of quantum repeater that, they claimed, allows one to create an entangled EPR pair over arbitrarily large distance with a polynomial overhead in the resources and with the tolerable error rate in the percent region. We also remark that the issue of distributed quantum computation over noisy channels has also been investigated by others, for example, van Enk, Cirac and Zoller [38] and Ekert *et al.* [39].

3. The most general eavesdropping strategy

Suppose Alice and Bob would like to share the encoded state of N EPR pairs. Let us be so generous as to give Eve complete control of all the intermediate connection points. Notice that this is the most general eavesdropping strategy by Eve. We shall prove that even in this case, our key distribution scheme is still secure.

Consider the moment that Alice and Bob have already received all the classical and quantum communication from the intermediate connection points and that they have acknowledged each other of the receipt of all those signals. Alice and Bob applies the recovery procedure of the error correcting code to his/her block.

Let us re-express each of Alice and Bob's state *mathematically* in terms of the tensor product of the logical qubits (which actually contain the quantum information) and the ancilla qubits (which contain the error syndromes). The essence of fault-tolerant quantum computation is that while the state of the ancilla qubits will evolve randomly over time, the state of the logical qubits will, with a very high $(1 - O(e^{-l}))$ fidelity, remain unchanged. Moreover, fault-tolerant quantum computation ensures that, as long as the gate error rate and storage error rate are sufficiently small, the subsequent verification and key generation steps can be thought of as being performed *solely* on the logical qubits. i.e., the ancilla qubits decouple from the verification step. Therefore, Eq. (3) and its accompanying discussion are perfectly valid except that they now refer to the logical qubits rather than the physical qubits. In summary, by performing the verification process and the key generation process on the *encoded* quantum information contained in the logical qubits, the whole argument in subsubsection II D 2 carries over completely.

Finally, we remark that the above idea of 'integrating out' the intermediate computation and communication steps is general. It applies not only to the connection points procedure but to any method of correcting errors in a noisy quantum channel between Alice and Bob. The essence is that one should not be concerned with the details of the quantum error correcting procedure in the intermediate steps. It is only the resulting output state shared between Alice and Bob that counts.

4. Computational errors during the final recovery and the verification step

In reality, the elementary gates used for quantum computation and all real measurements for the *final* recovery procedure and the verification step for security are imperfect. To ensure security, we once again use the general theory of *fault-tolerant* quantum computation [28–32] developed over the last few years. By implementing quantum error correction in a fault-tolerant manner, we argue that one can guarantee that the quantum verification scheme that we are considering works even in the presence of computational errors in the final recovery procedure.

In more detail, let us consider a fault-tolerant implementation of the final recovery and verification step such that, for *all* input states, the fidelity of the output (as compared to the output in the error-free case) is $1 - e^{-k}$, where $k \gg 1$ is the security parameter. This security parameter only depends on the effectiveness of the fault-tolerant scheme and can be made independent of any parameter in the original verification scheme. It is precisely because of this independence that a rigorous proof of security is possible. More concretely, compare the following two situations. Situation 1: a highly *fault-tolerant* final recovery and verification scheme on the m tested pairs followed by an error-free measurement on the remaining $N - m$ pairs to determine if they are all singlets. Situation 2: an *error-free* final recovery and verification scheme on the m tested pairs followed by an error-free measurement on the remaining $N - m$ pairs to determine if they are all singlets. By making the security parameter k of the fault-tolerant verification scheme arbitrarily large, one can ensure that the probability of Eve cheating successfully — i.e., passing the verification test and yet upon measurements the state of the remaining pairs are not $(N-m)$ singlets — against the fault-tolerant verification scheme is arbitrarily close to that of cheating successfully against an error-free recovery and verification scheme. But then, in the same manner as in situation 2, one can argue in situation 1 that the conditional fidelity of the remaining pairs as a product of singlets can be made very high. Now a high fidelity implies low entropy. (Lemma 1 in appendix A.) This proves that Eve has very limited information about the final key even in situation 1 — i.e., in the case of a highly fault-tolerant final recovery and verification scheme.

5. Summary

We have by now introduced all the three types of possible errors — channel noises, storage errors, and computational errors — in our discussion and showed that they can all be overcome by using a quantum error correcting scheme, followed by a quantum verification scheme and quantum measurements all performed in a fault-tolerant manner. This completes our proof of security for our quantum key distribution scheme.

6. What can an eavesdropper learn

Notice that we have given the eavesdropper complete freedom in preparing the state shared between Alice and Bob but yet we show that there is no way for Eve to find a state that will defeat Alice and Bob's verification step with a non-negligible probability. The reason can be best understood by again re-expressing the state of Alice or Bob in terms of the tensor product of the logical qubits and the ancilla qubits. For any state that passes the verification step with a non-negligible probability, conditional on passing the verification step, Eve has very little entanglement with the logical qubits. However, Eve's system can be highly entangled with the ancilla qubits. Therefore, she is free to learn a lot about the error syndromes found by Alice and Bob. Fortunately, by the very definition of quantum error correcting codes, those error syndromes tell Eve nothing about the state of the encoded quantum information and, hence, Alice and Bob's generated key.

REFERENCES

[1] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett. **68**, 3121–3124 (1992).

[2] C. H. Bennett, and G. Brassard, "Quantum key distribution and coin tossing", *Proceedings of IEEE Int. Conf. on Computers, Systems, and Signal Processing*, Bangalore, India (1984), 175–179.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. **67**, 661–664 (1991).

[4] S. Wiesner, "Conjugate coding", SIGACT News **15**, 77–88 (1983). Manuscript written in the 1970s.

[5] J. D. Franson, and H. Ilves, "Quantum cryptography using optical fibers", Appl. Opt. **33**, 2949–2954 (1994).

[6] R. J. Hughes, *et al.*, "Secure communications using quantum cryptography", *Proceedings of SPIE* **3076** (1997), 2–11.

[7] A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre", Europhys. Lett. **33**, 335–339 (1996).

[8] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, " 'Plug and play' systems for quantum cryptography", Appl. Phys. Lett. **70**, 793–795 (1997).

[9] P. D. Townsend, "Secure key distribution system based on quantum cryptography", Electronics Lett. **30**, 809–811 (1994).

[10] P. D. Townsend, "Quantum cryptography on multi-user optical fibre networks", Nature (London) **385**, 47–49 (1997).

[11] C. H. Bennett, T. Mor, and J. A. Smolin, "Parity bit in quantum cryptography", Phys. Rev. A **54**, 2675–2684 (1996).

[12] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, "Security of quantum key distribution against all collective attacks", Los Alamos preprint archive `quant-ph/9801022` (1998).

[13] E. Biham, and T. Mor, "Bounds on information and the security of quantum cryptography", Phys. Rev. Lett. **79**, 4034–4037 (1997).

[14] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy", Phys. Rev. A **56**, 1163–1172 (1997).

[15] R. B. Griffiths, and C.-S. Niu, "Optimal eavesdropping in quantum cryptography. II. A quantum circuit", Phys. Rev. A **56**, 1173–1176 (1997).

[16] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels", Phys. Rev. Lett. **77**, 2818–2821 (1996).

[17] D. Mayers, "On the security of the quantum oblivious transfer and key distribution protocols", *Advances in Cryptology: Proceedings of Crypto'95*, Lecture Notes in Comp. Sci., Vol. 963, (Springer-Verlag, 1995), 124–135.

[18] D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channel", *Advances in Cryptology: Proceedings of Crypto'96*, Lecture Notes in Comp. Sci., Vol. 1109, (Springer-Verlag, 1996), 343–357.

[19] Mayers, D., "Unconditionally secure quantum bit commitment is impossible", Phys. Rev. Lett. **78** 3414–3417 (1997).

[20] H.-K. Lo, and H. F. Chau, "Is quantum bit commitment really possible?", Phys. Rev. Lett. **78**, 3410–3413 (1997).
[21] H.-K. Lo, and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible", *Proceedings of PHYSCOMP96* (New England Complex System Inst., Boston, 1996), pp. 76–81. Also available on Los Alamos preprint archive `quant-ph/9605026`.
[22] H. F. Chau, and H.-K. Lo, "Making an empty promise with a quantum computer", Fort. de Phys. , to appear (1998). Also available on Los Alamos preprint archive `quant-ph/9709053`.
[23] H.-K. Lo, "Insecurity of quantum secure computations", Phys. Rev. A **56**, 1154-1162 (1997).
[24] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction", Phys. Rev. A **54**, 3824–3851 (1996).
[25] J. S. Bell, "On the Einstein Podolsky Rosen paradox", Physics **1**, 195–200 (1964); reprinted in *Quantum Theory and Measurement* (Princeton Univ. Press, Princeton, 1983), eds.: J. A Wheeler and W. H. Zurek, pp. 403–408.
[26] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", Phys. Rev. **47**, 777–780 (1935); reprinted in *Quantum Theory and Measurement* (Princeton Univ. Press, Princeton, 1983), eds.: J. A. Wheeler and W. H. Zurek, pp. 145–151.
[27] S. J. Freedman, and J. F. Clauser, "Experimental test of local hidden-variable theories", Phys. Rev. Lett. **28**, 938–941 (1972).
[28] J. Preskill, "Fault-tolerant quantum computation", in *Introduction to Quantum Information and Computation*, eds. Lo, H.-K., Popescu, S., and Spiller, T., (World Scientific, to be published) Los Alamos preprint archive `quant-ph/9712048` (1998).
[29] P. W. Shor, "Fault-tolerant quantum computation", *Proceedings of the Sym. on Found. Comp. Sci.* (Los Alamitos, CA, IEEE Press, 1996), 56-65.
[30] A. Yu. Kitaev, "Quantum error correction with imperfect gates", preprint (1996).
[31] E. Knill, R. Laflamme, and W. Zurek, "Resilient quantum computation", Science **279**, 342–345 (1998).
[32] D. Aharonov, and M. Ben-Or, "Fault-tolerant quantum computation with constant error", *Proceedings of the 29th Annual ACM Symposium on the Theory of Computing.* Also available in Los Alamos preprint archive `quant-ph/9611025`.
[33] A. S. Kholevo, "Bounds for the quantity of information transmitted by a quantum communication channel", Probl. Inf. Transm. (USSR) **9**, 117-183 (1973).
[34] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", Phys. Rev. A **52**, 2493-2496 (1995).
[35] A. M. Steane, "Error correcting codes in quantum theory", Phys. Rev. Lett. **77**, 793-797 (1996).
[36] For a review, see for example, A. M. Steane, in *Introduction to Quantum Information and Computation*, eds. Lo, H.-K., Popescu, S., and Spiller, T., (World Scientific, to be published).
[37] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters for communication", Los Alamos preprint archive `quant-ph/9803056`.
[38] S. J. van Enk, J. I. Cirac, and P. Zoller, "Ideal quantum communication over noisy

channels", Phys. Rev. Lett. **78**, 4293–4296 (1997).
[39] A. K. Ekert, S. F. Huelga, C. Macchiavello, and J. I. Cirac, "Distributed quantum computation over noisy channels", Los Alamos preprint archive `quant-ph/9803017` (1998).
[40] D. Mayers, and A. C. C. Yao, "Unconditional security in quantum cryptography", Los Alamos preprint archive `quant-ph/9802025`.
[41] M. Ardehali, G. Brassard, H. F. Chau, and H.-K. Lo, "Efficient quantum key distribution", Los Alamos preprint archive `quant-ph/9803007`.