A simple proof of the unconditional security of quantum key distribution

2001 J. Phys. A: Math. Gen. 34 6957

(http://iopscience.iop.org/0305-4470/34/35/321)

Institute of Physics Publishing Journal of Physics A: Mathematical and General

J. Phys. A: Math. Gen. **34** (2001) 6957–6967 PII: S0305-4470(01)18252-1

A simple proof of the unconditional security of quantum key distribution

Hoi-Kwong Lo

MagiQ Technologies, Inc., 275 Seventh Avenue, 26th Floor, New York, NY 10001-6708, USA

E-mail: hoi_kwong@magiqtech.com

Received 20 October 2000
Published 24 August 2001
Online at stacks.iop.org/JPhysA/34/6957

Abstract
Quantum key distribution is the best known application of quantum cryptography. Previously proposed proofs of security of quantum key distribution contain various technical subtleties. Here, a conceptually simpler proof of security of quantum key distribution is presented. The new insight is the invariance of the error rate of a teleportation channel: we show that the error rate of a teleportation channel is independent of the signals being transmitted. This is because the non-trivial error patterns are permuted under teleportation. This new insight is combined with the recently proposed quantum-to-classical reduction theorem. Our result shows that assuming that Alice and Bob have fault-tolerant quantum computers, quantum key distribution can be made unconditionally secure over arbitrarily long distances even against the most general type of eavesdropping attacks and in the presence of all types of noises.

PACS numbers: 03.67.−a, 03.65.Ta

1. Introduction

Perfectly secure communication between two users can be achieved if they share beforehand a common random string of numbers (a key). A big problem in conventional cryptography is the key distribution problem: in classical physics, there is nothing to prevent an eavesdropper from monitoring the key distribution channel passively, without being caught by the legitimate users. Quantum key distribution (QKD) [1, 12] has been proposed as a new solution to the key distribution problem. In quantum mechanics, there is a well-known 'quantum no-cloning theorem' which states that it is impossible for anyone (including an eavesdropper) to make a perfect copy of an unknown quantum state [9, 24]. Therefore, it is generally thought that eavesdropping on a quantum channel will almost surely produce detectable disturbances. For a survey on quantum cryptography, see, for example, [13, 14].

1.1. Prior work on security of QKD

A proof of security of QKD turned out to be a hard problem: an ingenious eavesdropper, Eve, can adopt many different eavesdropping strategies. Instead of measuring the quantum signals sent by Alice one by one, Eve may perform subtle quantum attacks in which she entangles all the quantum signals with her ancilla. A proof of security should defeat all possible eavesdropping strategies of Eve and take into account the imperfection of Alice and Bob's apparatus and the lossy nature of the quantum channel between Alice and Bob. While many partial results had been reported in various earlier papers (for a review, see, for example, [17]), complete proofs of security did not appear until the last few years.

Roughly speaking, there are two alternative approaches to proving the unconditional security of QKD. The first approach by Mayers [22] (earlier versions of [22] have appeared as [20] but they are less definite) deals with the best-known QKD scheme BB84 proposed by Bennett and Brassard [1]. The advantage of this approach is that it does not require the deployment of quantum computers by Alice and Bob. However, Mayers' proof is rather complex.

The second approach deals with QKD schemes that employ subtle quantum mechanical correlations—known as 'entanglement'–which have no classical analogue. This approach was first suggested by Deutsch *et al* in [10], which, however, assumes perfect quantum devices. A more recent paper by Lo and Chau [19] addresses this issue of imperfect devices using the idea of fault-tolerant quantum computation and quantum repeaters (i.e., relay stations) [8]. It also derives a rigorous bound on Eve's information under the assumption of reliable local quantum computations. Note that the second approach requires Alice and Bob to possess quantum computers, which are well beyond current technology. However, the second approach, as rigorously developed in [19], has the advantage of being conceptually simpler. The idea of commuting observables plays a key role in the second approach. By considering only commuting observables, one can apply directly *classical* arguments to tackle a *quantum* problem.

1.2. Significance of our results

It has to be said that all previously proposed proofs of security of QKD involve various technical subtleties. Here we present a simple proof of the unconditional security of QKD. The proof, based on the second approach, not only enjoys all the fundamental advantages mentioned above of the recently proposed proof [19], but also is conceptually simpler.

Furthermore, our proof gives us an interesting new insight into the well known 'teleportation' channel [2]: with a classical random sampling method, one can assign a set of *classical* probabilities to the various error patterns of a *quantum* teleportation channel. Besides, the error rate (the probability of having a non-trivial error pattern) for each signal is independent of the identity of the signal being transmitted. This is highly non-trivial because the well known Einstein–Podolsky–Rosen (EPR) paradox demonstrates that applications of classical arguments to a quantum problem often lead to fallacies [11].

2. Security requirement and ideas towards a proof

Definition. A QKD scheme is said to be unconditionally secure if, for any security parameters $k, l > 0$ chosen by Alice and Bob, they can follow the protocol and construct a verification test such that, for *any* eavesdropping attack by Eve that will pass the test with a non-negligible amount of probability (i.e., more than e^{-k}) the two following conditions are satisfied: (i) Eve's mutual information with the final key is always negligible (i.e., less than e^{-l}) and (ii) the final key is, indeed, essentially random.

Remark. The security parameters k and l depend on how hard Alice and Bob are willing to work towards perfect security (e.g., the size of the messages exchanged between Alice and Bob and the number of rounds of authentication between them) and are, at least in principle, computable from a protocol.

2.1. A simple idea, its problems and our solution

Consider the following simple idea of proof of security of QKD. Alice prepares r quantum signals and encodes their state into a quantum error-correcting code (QECC) (see, for example, [3]) of length n which corrects say t errors. In addition, she also prepares m other quantum signals which will be used as test signals. She then *randomly* permutes the $N = n + m$ signals and sends them to Bob via a noisy channel controlled by an eavesdropper. Bob publicly announces that he has received all the N signals from Alice. Upon Bob's confirmation of the receipt, Alice publicly announces the location of the m test signals and their specific state. Next Bob measures the m test signals and computes their error rate, e_1. Using the error rate e_1, Alice and Bob apply classical random sampling theory in statistics to establish confidence levels for the error rate of the n remaining (i.e., untested) signals and, hence, produce a probabilistic bound on the amount of the eavesdropper's information on the encoded r quantum signals. (The point is that, unless there are more than t errors in the QECC, Eve knows absolutely nothing about the encoded state.) If Alice and Bob are satisfied with the degree of security, they measure the r quantum signals to generate an r-bit key.

This raw idea looks simple, but it is essentially classical. It will work if the following three requirements are satisfied. (1) Each error pattern can be assigned with a classical probability. (2) The error rates of the signals are independent of the actual signals being transmitted (i.e., Eve cannot somehow change a non-trivial error operator to a trivial one depending on which signals are transmitted). (3) The quantum error correction and key generation can be done fault-tolerantly.

Since applications of classical arguments could be fallacious, it would be naïve to assign a probability distribution to the set of error patterns without a rigorous mathematical justification. In fact, rather disappointingly, we are unable to establish requirements (1) and (2) for the most general quantum channel.

Nonetheless, we manage to complete our proof of security of QKD by the following line of arguments. We notice that requirement (1) has already been established in [16] for the special case of the transmission of some standard states (halves of so-called EPR pairs). Moreover, it is well known in quantum information theory that the transmission of any general quantum state can be reduced to that of the standard state and classical communication via a process called *teleportation* [2] (which will be discussed in subsection 4.1).

Our line of attack is thus to establish requirements (1) and (2) for the special case of a teleportation channel only. In other words, we show that, by using teleportation to transmit quantum states through a noisy quantum channel (which may be controlled by an eavesdropper), the error rate (i.e., the probability of having a non-trivial error operator, or Pauli matrix, acting on the transmitted signal, as can be estimated by a classical random sampling procedure) is independent of the quantum state being transmitted. This invariance result ensures that, for a quantum teleportation channel, even an ingenious eavesdropper cannot change its underlying error rate and make it dependent on the identity of the quantum signals being transmitted. This new insight of ours—the 'invariance of the error rate of a quantum teleportation channel'—will be stated as proposition 5 and discussed in subsequent sections.

2.2. Einstein–Podolsky–Rosen pairs

Readers who are unfamiliar with quantum information should refer to appendix A. One can measure a quantum bit (or qubit) along any direction and each measurement can give two possible outcomes. An Einstein–Podolsky–Rosen pair of qubits has the following interesting property. If two members of an EPR pair are measured along *any* common axis, each member will give a random outcome, and yet the outcomes of the two members will always be anti-parallel. This is so even when the two members are distantly separated. Such an action at a distance is at the core of the EPR paradox and it defies any simple classical explanation.

Now, if two persons, Alice and Bob, share R EPR pairs, they can generate a common random string of numbers (an R-bit key) by measuring each member along some common axis. The laws of quantum mechanics guarantee that, provided that the R pairs are of almost perfect fidelity, the key generated will be almost perfectly random and that Eve will have a negligible amount of information on its value. In fact, we have

Lemma 1. (*Note* 28 *of* [19].) *If Alice and Bob share R EPR pairs of fidelity at least* $1 - 2^{-k}$, *for a sufficiently large k, and they generate an R-bit key by measuring these pairs along any common axis, then Eve's mutual information on the final key will be bounded by* $2^{-c} + 2^{O(-2k)}$ *where* $c = k - \log_2 \left[2R + k + (1/\log_\varepsilon 2)\right]$.

Proof. In supplementary material of [19]. □

So, the Holy Grail of the second approach to secure QKD is to construct a scheme for distributing R almost perfect EPR pairs even in the presence of noise and Eve.

3. Quantum-to-classical reduction theorem

3.1. Theory

A proof of security of QKD can be simplified greatly if one can apply well known powerful techniques in classical probability theory and statistical theory to the problem. However, applications of classical arguments to a quantum problem require careful justifications. A key ingredient of our current proof is, therefore, a quantum-to-classical reduction theorem proven in [19], which justifies the usage of classical arguments.

Let us recapitulate this quantum-to-classical reduction theorem from the viewpoint of 'commuting observables': conceptually, classical arguments work because all the observables O_i under consideration are diagonal with respect to a *single* basis, which we shall call $\mathcal{B}$. More concretely, let M be the observable that represents the complete von Neumann measurement along the basis $\mathcal{B}$. Since the O_i and M are all diagonal with respect to the basis $\mathcal{B}$, they clearly commute with one another. Therefore, the measurement M along basis $\mathcal{B}$ will in no way change the outcome of subsequent measurements O_i. Without loss of generality, we can imagine that such a measurement M is always performed before the measurement of the subsequent O_i. Consequently, the initial state is always a classical mixture of eigenstates of M. Therefore, one can safely assign classical probabilities to those simultaneous eigenstates and apply directly classical probability theory or statistical theory to deduce the values of those classical probabilities. In this sense, the quantum problem has a classical interpretation[1]. Mathematically, this quantum-to-classical reduction theorem can be stated as the following theorem.

Theorem 2. [19] *Consider a mixed quantum state described by ρ and a set of one-dimensional non-commuting projection operators Q_j on it. Suppose there exists a complete set of coarse-grained observables O_i of Q_j such that all the O_i commute with one another.* (*Here, by coarse-graining, one means that each O_i can be written as a sum of a set of orthogonal projectors Q_j and by completeness, one means that $\sum_i O_i = I$.*) *Let us consider a complete von Neumann measurement M which commutes with all O_i.* (*Because of the commutativity of the O_i, such M must exist.*) *Let $|v_k\rangle$ be the basis vectors of M. Then, for all* i, *we have*

$$\mathrm{Tr}(O_i\rho) = \mathrm{Tr}\left(O_i \sum_k |v_k\rangle\langle v_k|\rho|v_k\rangle\langle v_k|\right). \tag{1}$$

Remark. Physically, theorem 2 says that the probability of all the coarse-grained outcomes O_i are unchanged by a prior complete von Neumann measurement M. The full power of theorem 2 will be demonstrated in proposition 3.

Proof. Sketch by construction, for each O_i there exists a coefficient λ_i and a set K_i such that $O_i = \lambda_i \sum_{l\in K_i} |v_l\rangle\langle v_l|$. From the definition of TrA as $\sum_m \langle v_m|A|v_m\rangle$, it is now a simple exercise to establish equation (1). □

3.2. Application to random sampling

Consider the following example (example (i) on p 2054 of [19]). Suppose two distant observers, Alice and Bob, share a large number, say N, pairs of qubits, which may be prepared by Eve. Those pairs may thus be entangled with one another in an arbitrary manner and also with the external universe, for example, an ancilla prepared by Eve. How can Alice and Bob estimate the number of singlets in those N pairs? (By the number of singlets, here we mean the expected number of 'yes' answers if a singlet-or-not measurement were made on each pair individually.)

The solution is the following random sampling procedure and proposition.

Procedure. Suppose Alice and Bob randomly pick m of the N pairs and, for each pair, choose randomly one of the three (x, y and z) axes and measure the two members along it. They publicly announce their outcomes. Let k be the number of anti-parallel outcomes obtained in this random sampling procedure.

Proposition 3. (*From section VI of supplementary material of* [19].) *The fraction of singlets, f_s, in the N pairs can be estimated as $(3k - m)/2m$. Furthermore, confidence levels can be deduced from classical statistical theory for a finite population* (*of N objects*).

[1] This quantum-to-classical reduction theorem is rather subtle. First, the observables O_i under consideration are coarse-grained observables (i.e., observables with degenerate eigenvalues) rather than fine-grained ones (i.e., observables with non-degenerate eigenvalues). It is *a priori* surprising that coarse-graining as a mathematical technique will give a classical interpretation to a quantum problem. Second, the eigenstates of M employed in [19] are, in fact, the so-called Bell states (see subsection 3.2 and appendix B) which exhibit non-local quantum mechanical correlations. It is *a priori* surprising that such a non-local (or quantum mechanical) Bell basis can have a classical interpretation.

Proof. This is a direct application of theorem 2. Let us order the N pairs. Consider, for the ith pair, the projection operations $P^i_{\|,a}$ and $P^i_{\text{anti-}\|,a}$ for the two coarse-grained outcomes (parallel and anti-parallel) of the measurements on the two members of the pair along the a axis where $a = x, y$ or z. A simple but rather important observation is that each of these projection operators can be mathematically re-written as a linear combination of projection operators along a single basis, namely the Bell basis (see appendix B for details). A basis for N ordered pairs of qubits (what we shall call the N-Bell basis) consists of products of Bell basis vectors, each of which is described by a $2N$-bit string. Now, let us consider the operator M_B that represents the action of a complete von Neumann measurement along an N-Bell basis. Since M_B, $P^i_{\|,a}$ and $P^i_{\text{anti-}\|,a}$ are diagonal with respect to a single basis (N-Bell basis), they clearly commute with each other. Thus, a pre-measurement M_B by Eve along an N-Bell basis will in no way change the outcome for $P^i_{\|,a}$ and $P^i_{\text{anti-}\|,a}$. With no loss of generality, we can assume that such a pre-measurement is always performed before the subsequent measurement of $P^i_{\|,a}$ and $P^i_{\text{anti-}\|,a}$. In other words, we have a classical mixture of N-Bell basis vectors, and classical probability theory referring only to the N-Bell basis vectors is, thus, valid. For this reason, estimation of the number of singlets as well as confidence levels of such an estimation can be done by classical statistical theory. □

4. Our secure QKD scheme

We remark that the fraction of singlets, f_s, in proposition 3 has the significance of being the fraction of uncorrupted qubits in a quantum communication channel shared between Alice and Bob in the following situation. Suppose Alice prepares N EPR pairs locally and, afterwards, sends a member of each pair to Bob via a noisy quantum channel controlled by Eve. As a result of channel noises and eavesdropping attack, some of the N EPR pairs may be corrupted. Proposition 3 gives us a mathematical estimate of the number of uncorrupted qubits in the actual transmission, based on the random sampling of a small number of transmitted signals.

Since quantum error-correcting codes (QECCs) exist, it is tempting to construct a secure QKD scheme by, first, using the random sampling procedure to estimate the error rate of the transmission and, second, using a QECC to correct the appropriate number of errors. To ensure that the sampling procedure is indeed random, Alice should mix up the test pairs with the pairs in the actual QECC randomly.

However, as briefly noted in the introduction, the above idea implicitly assumes that the following conjecture is true. Let us consider the four error operators I, σ_x, σ_y and σ_z for each quantum signal transmitted (see appendix A for notations).

Conjecture 4. *The error rate of a quantum communication channel is independent of the signals being transmitted. More precisely, in the current case, one can safely assign a probability for each error pattern in analyzing the security issue of a QKD scheme.*

While such a conjecture is intuitively plausible, we are unaware of any rigorous proof for a general quantum channel. To address this problem, we prove a related but perhaps weaker result concerning a teleportation channel. We make use of the well known fact that, any quantum signals can always be transmitted to a quantum communication channel via teleportation.

4.1. Teleportation

In teleportation [2] a quantum signal is transported via a dual usage of prior ‘entanglement’ (i.e., standard EPR pairs shared between the sender, Alice, and the receiver, Bob) and a classical communication channel. The quantum signal in Alice's hand is destroyed by her local measurement, which generates a classical message. This message is then transmitted to Bob via a classical communication channel. Depending on the content of this message, Bob can then re-construct the destroyed quantum signal by applying one of the unitary transformations I, σ_x, σ_y and σ_z to each of his members of the EPR pairs originally shared with Alice.

Two points are noteworthy. First, in teleportation the same prior entanglement is shared by Alice and Bob, independent of the actual quantum signal that will subsequently be transported. Now, since Alice always sends the same standard quantum signal to Bob during the prior sharing part of the teleportation process, the discussion of classical random sampling theory in subsection 3.2 can be applied directly. Second, the re-construction step in teleportation, if done with reliable quantum computers, will not introduce new errors into the quantum system. Indeed, if Alice and Bob use a *noisy* quantum state shared between them for teleportation, for each transmitted signal, the three types of errors σ_x, σ_y and σ_z are simply permuted to one another during the re-construction process. This idea is true even for a quantum superposition of error patterns and entanglement with an external universe (as specified by the original noisy quantum state shared between them).

Let us formulate this result mathematically. Consider the teleportation of a system $\mathcal{S}$ consisting of N qubits from Alice to Bob with the most general mixed state ρ_u. Without loss of generality, a system decribed by a mixed state can be equivalently described by a pure state of a larger system consisting of the original system and an ancilla. (John Smolin has coined the name 'the Church of the larger Hilbert space' for this simple but useful observation, which has recently been extensively used [10, 21, 18, 16]. For instance, the generality of the recent proofs of the impossibility of bit commitment [21, 18] and one-out-of-two oblivious transfer [16] follows from this idea.) Applying this idea to our current case, the state of original system $\mathcal{S}$ (plus an ancilla $\mathcal{R}$ with which it is entangled) can be written in the following form (the so-called Schmidt decomposition):

$$|v\rangle_{\mathcal{RS}} = \sum_m c_m |w_m\rangle_{\mathcal{R}} |v_m\rangle_{\mathcal{S}} \tag{2}$$

where c_m are some complex coefficients, and $|w_m\rangle_{\mathcal{R}}$ and $|v_m\rangle_{\mathcal{S}}$ are some basis vectors of the two systems $\mathcal{R}$ and $\mathcal{S}$ respectively. The initial state ρ_u of the N pairs shared by Alice and Bob can also be *purified* in 'the Church of the larger Hilbert space' as

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

where i_k denotes the state of the kth pair and it runs from $\tilde{0}\tilde{0}$ to $\tilde{1}\tilde{1}$, the $|j\rangle$ form an orthonormal basis for the environment (or an ancilla prepared by Eve), and $\alpha_{i_1, i_2, \ldots, i_N, j}$ are some complex coefficients. Each state $|u\rangle$ represents a particular mixed state. Note that $|u\rangle$ can be re-written as an entangled sum of a linear superposition of various error patterns, i.e.,

$$|u\rangle = \sum_{i_1, i_2, \ldots, i_N} \sum_j \alpha_{i_1, i_2, \ldots, i_N, j} \left(\prod_k \sigma_{i_k}^{(k)} \right) |\Psi^-\rangle^N \otimes |j\rangle \tag{4}$$

where $\sigma_{i_k}^{(k)}$ acts on Bob's member of the kth pair as either I, σ_x, σ_y or σ_z depending on the value of i_k, and $|\Psi^-\rangle$ denotes an EPR pair. With such notation, one can prove our main proposition.

Proposition 5. Invariance of error rate under teleportation. *In the above notation, suppose the system* $\mathcal{S}$ (*described by* $|v\rangle_{\mathcal{RS}} = \sum_m c_m |w_m\rangle_{\mathcal{R}} |v_m\rangle_{\mathcal{S}}$ *of the combined system* $\mathcal{R}$ *and* $\mathcal{S}$ *in equation* (2)) *is teleported using the N pairs shared by Alice and Bob* (*described by* $|u\rangle$ *of the combined system of the N pairs and Eve's ancilla in equation* (4)). *Suppose further that the* *classical outcome of Alice's measurements is $\{j_k\}$, i.e., she informs Bob to use the operator $\prod_k \sigma_{j_k}^{(k)}$ for the re-construction process. Then Bob's re-constructed state for the combined system $\mathcal{R}$, $\mathcal{S}$ and $\mathcal{E}$ can be described by*

$$\sum_m c_m |w_m\rangle_{\mathcal{R}} \sum_{i_1,i_2,\ldots,i_N} \sum_j \alpha_{i_1,i_2,\ldots,i_N,j} \left[\prod_k \left(\sigma_{j_k}^{(k)} \sigma_{i_k}^{(k)} \sigma_{j_k}^{(k)} \right) \right] |v_m\rangle_{\mathcal{S}} \otimes |j\rangle. \quad (5)$$

Remark. The set of complex coefficients $c_m \alpha_{i_1,i_2,\ldots,i_N,j}$ remains totally unchanged under teleportation. For each teleportation outcome labelled by $\{j_k\}$, the only real change lies in the conjugation action in the error operator acting on the subsystem $\mathcal{S}$, i.e., $\sigma_{i_k}^{(k)} \rightarrow \sigma_{j_k}^{(k)} \sigma_{i_k}^{(k)} \sigma_{j_k}^{(k)}$ for each k. (Recall that $\sigma_{j_k}^{(k)}$ is always its own inverse.) Since under such conjugation the trivial error operator (i.e., the identity I) is invariant and the three non-trivial error operators σ_x, σ_y and σ_z are permuted with one another, the error rate of the teleported signal is exactly the same as the original N EPR pairs.

Proof of proposition 5. This is a straightforward exercise in quantum information theory [2], which we will skip here. □

4.2. Procedure of our secure QKD scheme

Having established proposition 5, we now present the procedure of our secure QKD scheme. Note that the procedure itself is simple. The non-trivial thing that we have done is to prove that it is actually secure.

(1) Alice prepares N EPR pairs and sends a member of each pair to Bob through a noisy channel. (In theory, quantum repeaters [8] and two-way schemes for so-called entanglement purification [1] (a generalization of quantum error correcting codes) could be used in this step. The error rate here can, therefore, be made to be very small and the scheme works even for arbitrarily long distances.)

(2) Bob publicly announces his receipt of the N quantum signals.

(3) Alice *randomly* picks m of the N EPR pairs for testing. She publicly announces her choice to Bob. For each pair, Alice and Bob randomly pick one of the three (x, y, and z) axes and perform a measurement on the two members along it.

(4) Alice and Bob publicly announce their measurement outcomes and use classical sampling theory to estimate the error rate in the transmission.

Remark. Proposition 3 allows Alice and Bob to apply classical sampling theory to the quantum problem at hand to estimate the error rate of the untested particles. Alice and Bob then proceed with quantum error correction in the next step.

(5) Alice prepares, say, R EPR pairs and encodes the R halves of the pairs (i.e., one member from each pair) by a quantum error-correcting code (QECC) into $N - m$ qubits.

Remark. The requirement of QECC will be discussed in subsection 4.3.

(6) Alice teleports the $N - m$ qubits to Bob via the remaining $N - m$ pairs that they share.

Remark. Proposition 5 guarantees the invariance of error rate under teleportation. So, the estimate done by Alice and Bob in step (4) remains valid.

(7) Alice and Bob perform fault-tolerant quantum computation to generate a random R-bit key by measuring the state of the R encoded EPR pairs along a prescribed common axis (say the z axis).

4.3. Fault-tolerant quantum computation

From propositions 3 and 5 it is quite clear that, assuming reliable local quantum computers, our scheme works perfectly. However, since local quantum computations may be imperfect, errors may be generated during the teleportation and key generation, i.e., steps (6) and (7). One can easily take those local errors into account by a choice of QECC with generous error-correcting and fault-tolerant capabilities. The point is that we have a very specific and short computation in mind (measurement along the z axis only and no unitary computation at all). Based on any realistic error model for quantum computers and concrete choice of QECC, one can give a generous upper bound on the number of local errors due to imperfect quantum computation. With a fault-tolerant implementation the total number of errors in the whole process (transmission, teleportation and key generation) can be bounded. Therefore, provided that our QECC has sufficiently generous error-correcting and fault-tolerant capabilities, security is guaranteed. (To be precise, in step (5), the R EPR pairs should be prepared fault-tolerantly in an *encoded* form rather than in an unencoded form.) We remark that, since the required quantum computation here is much simpler than in [19], the present QKD scheme may be more efficient than the one there.

5. Concluding remarks

In summary, we have presented a simple proof of the unconditional security of quantum key distribution, i.e., ultimate security against the most general eavesdropping attack and the most general types of noises. Our scheme allows secure QKD over arbitrarily long distances, but it requires Alice and Bob to have reliable quantum computers, which is far beyond current technology. However, to put things in perspective, all proposed proofs of security of QKD involve assumptions (such as ideal sources) that are beyond current technologies.

Notice that some of the techniques developed here and in [19] have applications. For example, note 21 of [19] shows that teleportation is a powerful technique against the quantum Trojan Horse attack. A new application—using random sampling and random teleportation to prove the feasibility of a general two-party fault-tolerant quantum computation even in the presence of eavesdroppers—will be discussed in appendix C. In fact, some of the results are applicable even to the case when Alice and Bob do not have a quantum computer. A good example is a quantitative statement on the trade-off between information gain and disturbance in BB84 [19].

Acknowledgments

We particularly thank P W Shor for inspiring discussions and patient instruction. Very helpful comments from C H Bennett, H F Chau, and John Smolin are also gratefully acknowledged. The research and the write-up of the first version of this paper was done while the author was with Hewlett-Packard Laboratories, Bristol, UK.

Notes added in revised version. Biham *et al* [6] and Ben-Or [4] have also provided proofs of security of BB84. A simple proof of security of BB84 has been given by Shor and Preskill [23], who combined the ingredients in the proofs of Mayers [22] and Lo and Chau [19]. Finally, a proof of security of BB84 with two-way classical communications has recently been given by Gottesman and Lo [15].

Appendix A. Physics background: Einstein–Podolsky–Rosen pairs

The fundamental unit of quantum information is called a quantum bit or ‘qubit’. Physically, it is often represented by a two-level microscopic system such as an atom or nuclear spin or a polarized photon. Mathematically, a pure quantum state of a qubit is simply given by a unit vector in a two-dimensional Hilbert space $\mathcal{H}^2$: let us consider any basis $|0\rangle$ and $|1\rangle$. A single qubit in a pure state can be in any superposition of the two basis vectors, i.e., $a|0\rangle + b|1\rangle$ where a and b are complex coefficients with the normalization $|a|^2 + |b|^2 = 1$. A pair of qubits is described by a unit vector in the tensor product space $\mathcal{H}^4 = \mathcal{H}^2 \otimes \mathcal{H}^2$. with the basis states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. Consider the state $|\Psi^-\rangle = \sqrt{1/2}(|01\rangle - |10\rangle)$. The important point to note is that it is impossible to re-write $|\Psi^-\rangle$ into the form of a direct product $|u\rangle \otimes |v\rangle$. The state $|\Psi^-\rangle$ is called *entangled* because it is impossible to assign a definite state to the individual subsystems. And $|\Psi^-\rangle$ is called an Einstein–Podolsky–Rosen (EPR) pair.

It is common to write $a|0\rangle + b|1\rangle$ also as a column vector $\binom{a}{b}$. The non-trivial error operators (or Pauli matrices) are defined as $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$, and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Appendix B. Bell basis

The basis vectors of the Bell basis are $\Psi^{\pm}$ and $\Phi^{\pm}$, where

$$\Psi^{\pm} = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle) \tag{B1}$$

and

$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle). \tag{B2}$$

With the convention in [3], Bell basis vectors are represented by two classical bits:

$$\begin{aligned} \Phi^{+} &= \tilde{0}\tilde{0} \\ \Psi^{+} &= \tilde{0}\tilde{1} \\ \Phi^{-} &= \tilde{1}\tilde{0} \\ \Psi^{-} &= \tilde{1}\tilde{1}. \end{aligned} \tag{B3}$$

Since Bell basis vectors are highly entangled, one should not think of them as direct product states.

Appendix C. Two-party fault-tolerant quantum computation in the presence of an eavesdropper

Here we show that random sampling and random teleportation can be used to prove the feasibility of a general two-party fault-tolerant quantum computation even in the presence of eavesdroppers. This may look hard because the usual requirements of fault-tolerant quantum computation demand that the errors of different signals are independent and that the error rate for each error to happen is smaller than some threshold value. In contrast, an eavesdropper can introduce collective noises into the system.

Proposition 6. *In the large-N limit, the procedure in proposition* 3 *can be used to establish that, with a very high confidence level, the error rates of the transmitted signals are well below* *the threshold value required for a general fault-tolerant quantum computation and that the error rates for different signals are essentially independent*.

Proof. Suppose N quantum signals are teleported via N EPR pairs such that each signal is teleported by a *random* pair (without replacement, of course) chosen by Alice and Bob. By propositions 3 and 5, we can apply classical sampling theory to our current quantum problem. Now, since the signals are *randomly* sampled, in the large-N limit of classical sampling theory, they have *identical* and *independent* error probabilities. Therefore, by random sampling and random teleportation, Alice and Bob can establish confidence levels for the smallness and independence of the error rates of different signals, thus allowing subsequent fault-tolerant quantum computations. □

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE) p 175

[2] Bennett C H, Brassard C H, Crepeau C, Jozsa R, Peres A and Wootters W 1993 *Phys. Rev. Lett.* **70** 1895

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

[4] Ben-Or M 2001 in preparation

[5] Biham E and Mor T 1997 *Phys. Rev. Lett.* **78** 2256

[6] Biham E, Boyer M, Boykin P, Mor T and Roychowdhury V 2000 *Proc. 32nd Ann. ACM Symp. on Theory of Computing (STOC)* (New York: ACM Press) p 715

[7] Biham E, Boyer M, Brassard G, van de Graaf J and Mor T 1998 *Preprint* quant-ph/9801022

[8] Dür W, Briegel H-J, Cirac J I and Zoller P 1999 *Phys. Rev.* A **59** 169

[9] Dieks D 1982 *Phys. Lett.* A **92** 271

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

[11] Einstein A, Podolsky B and Rosen N 1935 *Phys. Rev.* **47** 777

[12] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[13] Gisin N, Ribordy G, Tittel W and Zbinden H 2001 *Preprint* quant-ph/0101098

[14] Gottesman D and Lo H-K 2000 *Phys. Today* **53** (November) 22

[15] Gottesman D and Lo H-K 2000 *Preprint* quant-ph/0105121

[16] Lo H-K 1997 *Phys. Rev.* A **56** 1154

[17] Lo H-K 1998 *Introduction to Quantum Computation and Information* ed H-K Lo, S Popescu and T Spiller (Singapore: World Scientific) p 76

[18] Lo H-K and Chau H F 1997 *Phys. Rev. Lett.* **78** 3410

[19] Lo H-K and Chau H F 1999 *Science* **283** 2050 (supplementary material available at www.sciencemag.org/feature/data/984035.shl)

[20] Mayers D 1996 *Advances in Cryptology: Proceedings of Crypto'96* (*Lecture Notes in Computer Science* vol 1109) (Berlin: Springer) p 343

[21] Mayers D 1997 *Phys. Rev. Lett.* **78** 3414

[22] Mayers D 1998 *Preprint* quant-ph/9802025

[23] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[24] Wootters W K and Zurek W 1982 *Nature* **299** 802