Error Correction and Security in Quantum Cryptography

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

July 10, 2002

Abstract

Quantum key distribution (QKD) allows perfectly secure communications in the presence of an eavesdropper. Quantum error correction (QEC) allows reliable quantum computations in the presence of environmental noises. Recently, the deep connection between QEC and the security of QKD has been demonstrated: Experimental QKD, which is feasible with current technology, can provide one of the first arenas for the applications of the abstract concepts in QEC and, more generally, entanglement purification. Moreover, concepts in QEC/entanglement purification allow QKD to operate in an unconditionally secure manner in a much larger parameter region than previously known. Here, I survey these exciting developments.

1 Introduction

QKD allows two parties to communicate in absolute privacy in the presence of an eavesdropper. Unlike conventional schemes of key distribution that rely on unproven computational assumptions, the security of QKD is guaranteed by the Heisenberg uncertainty principle of quantum mechanics. Much of the interest in QKD arises from the possibility of near-term real-life applications, whereas most other potential uses of quantum information remain remote.

Today's technologies fall short of full control and manipulation of quantum states, so practical QKD protocols must use a much more restricted set of operations. The best-known QKD protocol, which is nearly practical, was published by Bennett and Brassard in 1984 [1]. BB84 is a simple "prepare-and-measure" protocol that can be implemented without a quantum computer, but it requires a perfect single-photon source. In a "prepare-and-measure" protocol, Alice simply prepares a sequence of single-photon signals and transmits them to Bob. Bob immediately measures those signals. Thus, no quantum computation or long-term storage of quantum information is necessary. Only the transmission of single-photon states, which can be performed through Telecom optical fibers, is required.

Proofs of security of QKD against the most general attack allowed by quantum mechanics turned out to be very hard problem. Mayers [2] provided the first proof of the unconditional security of BB84.

2 Entanglement Purification Approach

Here, I will focus on another approach by myself and Chau, who built on earlier works by Deutsch *et al.* and Bennett *et al.* This second approach is based on "entanglement purification". Suppose two distant observers, Alice and Bob, share N imperfect EPR pairs. They can apply local operations and classical communication to distill out a smaller number, say k, of EPR pairs of higher fidelity. This distillation process is called entanglement purification. Entanglement purification protocols that involve only one-way classical communications between Alice and Bob have been shown to be equivalent to quantum error-correcting codes. They are useful for both communication and storage of quantum information. On the other hand, entanglement purification protocols that involve two-way classical communications can generally tolerate higher noise levels than those involving only one-way classical communications. They are useful for the communication of quantum information, but not its storage.

Now, assuming that entanglement purification is successful, Alice and Bob will share k almost perfect EPR pairs. By measuring those k EPR pairs along say the Z-axis, they can obtain a secure key. To ensure that entanglement purification will be successful with high confidence, Alice and Bob should perform some verification test. For instance, Alice can prepare $2N$ EPR pairs and send halves of those pairs to Bob. They randomly pick N of those EPR pairs

and measure each pair along a random basis, X or Z. They can then compute the error rates of the two bases. Since a random sample is used for the verification test, the error rate of the tested sample, with high confidence, provides an estimate of the error rate of the untested sample, which is used for entanglement purification. This can be done by using classical probability theory and statistical theory.

A key non-trivial insight in Lo-Chau's proof is a "quantum to classical reduction argument", which showed that it is, indeed, consistent to assign *classical* probabilities to the $2N$-Bell basis states. Each basis vector of the $2N$-Bell basis is the tensor product of Bell states $\Psi^{\pm}$ and $\Phi^{\pm}$, for a pair of qubits, where $\Psi^{\pm} = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$, and $\Phi^{\pm} = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle)$.

As noted in the Einstein-Podolsky-Rosen paradox, it is generally naive and inconsistent to assign classical probability theory to a quantum problem. The key reason why classical probability theory does apply here is the "commuting observables" idea. Provided that all the relevant observables of interest commute with each other, it is consistent to assign classical probability theory to a quantum problem. The hard part of Lo-Chau's proof is to construct such commuting observables. The proof has the advantage of being conceptually simple, but requires a quantum computer to implement.

Recently, Shor and Preskill [4] provided a simple proof of security of BB84 using the entanglement purification approach, thus removing the requirement of having quantum computers. A key insight is that it is sufficient for the security of QKD to show that Alice and Bob *could have performed* entanglement purification, if they had had quantum computers. It is un-necessary for Alice and Bob to actually perform entanglement purification.

Incidentally, Shor and Preskill's proof makes use of a specific and well-known class of codes—so-called CSS codes, which have the nice property that its error correction procedure can be decoupled into two pieces, namely "bit-flip" and "phase" error correction. Since phase errors do not affect the value of the final key, there is no need for Alice and Bob to announce the phase error syndrome. For this reason, Alice and Bob can perform secure QKD without quantum computers. Shor-Preskill's proof is important because it shows that the machinery in entanglement purification can be applied to a near-practical QKD protocol like BB84.

More recently, Gottesman and I [4] have generalized Shor and Preskill's result to prove the security of BB84 at a much higher bit error rate of about 18.9 percents. (Shor-Preskill's proof works only up to a bit error rate of about 11 percents.) Our protocols require two-way classical communications between Alice to Bob and are related to entanglement purification protocols with two-way classical communications. We also showed that the six-state scheme can be made unconditionally secure up to an error rate of 26.8 percents. Since BB84 is known to be insecure at an error rate of 25 percents by a simple intercept and resend strategy, our result showed that the six-state can intrinsically tolerate a higher bit error rate than BB84.

In summary, entanglement purification has proven to be a fruitful avenue in the investigation of security of QKD. It showed clearly that QKD can be made unconditionally secure in a much larger parameter space than previously known. Moreover, QKD provides a concrete arena for the applications of the abstract concepts of entanglement purification. I expect that this interplay between theory and practice will remain an important theme in future.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE press, 1984, p. 175.

[2] D. Mayers, "Unconditional security in Quantum Cryptography," Journal of ACM, vol. 48, Issue 3, p. 351-406. Also [Online] Available: http://xxx.lanl.gov/abs/quant-ph/9802025 A preliminary version is D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," *Advances in Cryptology—Proceedings of Crypto' 96* (Springer-Verlag, New York, 1996), p. 343.

[3] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999). Also, [Online] Available: http://xxx.lanl.gov/abs/quant-ph/9803006.

[4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, p. 441, 2000. Also, [Online] Available: http://xxx.lanl.gov/abs/quant-ph/0003004.

[5] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, available at http://xxx.lanl.gov/abs/quant-ph/0105121