A. Quantum Key Distribution

The purpose of QKD is to establish a string of random bits (the "key") shared by Alice and Bob, where Alice and Bob can be highly confident that eavesdropper Eve knows almost nothing about the key. Then the key can be used by Alice and Bob as a one-time pad for enciphering and deciphering a message. Because the key is random and unknown by Eve, she can't learn anything about the message by intercepting the ciphertext.

The promise of quantum cryptography was first glimpsed by Stephen Wiesner, [1] who proposed a quantum realization of unforgeable bank notes in the early 1970s. A decade later, Charles Bennett and Gilles Brassard [2] proposed the first QKD scheme, which was published in 1984 and became known as the "BB84" protocol. In BB84, Alice repeatedly sends to Bob one of four possible states of a qubit, and Bob measures each signal in one of two complementary

bases. This protocol was reinvented a few years later by Douglas Wiedemann, [3] who was unaware at the time of the work of Bennett and Brassard.

In 1990, Artur Ekert, also initially unaware of the earlier work, began developing a different approach to quantum cryptography that ultimately proved very fruitful. Ekert proposed a key-distribution protocol [4] in which entangled pairs of qubits are distributed to Alice and Bob, who then extract key bits by measuring their qubits. Bennett, Brassard, and Mermin [5] then noted that a simplified version of entanglement-based QKD can be cast in a form closely resembling BB84, where each party measures the qubit in one of two complementary bases. Many other variations on QKD were proposed later, such as

- a "six-state protocol" [6], in which Alice sends each qubit in one of six possible states;
- Bennett's B92 protocol [7], in which Alice sends one of two nonorthogonal states;
- the "time-reversed" EPR protocol [8], in which Alice and Bob send the BB84 states to a central switching station (where their shared key is established via an entangled measurement); and
- protocols using continuous quantum variables [9], in which Alice sends a squeezed state or a coherent state of a harmonic oscillator.

In their original paper and in subsequent work with other collaborators [10], Bennett and Brassard analyzed "individual" attacks on BB84, in which Eve attacks the quantum signals one at a time. However, a complete proof of information-theoretic security is more challenging. In principle, Eve could attack all of the signals sent by Alice to Bob collectively, entangling the qubits with an ancilla that she controls. Eve could then monitor the public classical communication between Alice and Bob, in which they reveal their basis choices and exchange further information to correct errors in their shared key and to amplify its privacy. The information Eve learns from this public discussion might help her decide how to measure her ancilla to optimize her information about the key.

New techniques for analyzing collective attacks by the eavesdropper were developed by Andrew Yao [11] in 1995, and the first complete proof of information-theoretic security for BB84 was obtained by Dominic Mayers [12] in 1996. Around the same time, Bennett, Brassard, Popescu, Schumacher, Smolin, and Wootters [13] discovered that noisy quantum entanglement can be distilled, and Deutsch, Ekert, Jozsa, Macchiavello, Popescu, and Sanpera [14] noted that if Alice and Bob have reliable quantum computers, they can use an entanglement-distillation protocol to achieve a secure version of entanglement-based key distribution. This observation was developed into a formal proof of security by Lo and Chau [15] in 1998. The approaches of Mayers and of Lo and Chau were united in 2000 by Shor and Preskill, [16] who showed that entanglement distillation can be invoked to formulate a relatively simple proof of the security of the original BB84 protocol.

The Shor-Preskill analysis relies on the idea that Alice and Bob could use a quantum error-correcting code to prevent Eve from becoming entangled with the protected qubits that are used to generate the key. Furthermore, this code can be chosen to have the property that bit-flip error correction and phase error correction can be performed separately. However, for the final key to be private, it is not necessary to actually perform the phase error correction—it is enough to know, based on the verification test included in the protocol, that phase error correction would

have succeeded *if it had been done*. By this reasoning based on *virtual quantum error correction*, a protocol invoking quantum error correction reduces to BB84 augmented by classical error correction and classical privacy amplification, which is therefore provably secure against any possible eavesdropping strategy.

Another novel approach to proving the security of BB84 (long in gestation but still unpublished) has been pursued by Ben-Or [17]. In Ben-Or's proof, one uses the results of the verification test to infer that the quantum state of Eve's ancilla is highly compressible. Then results regarding the quantum-communication complexity of the binary inner product function are cited to establish that Eve cannot possibly have enough information to compute the final key generated by Alice and Bob. Quite different technical tools were developed by Biham, Boyer, Boykin, Mor, and Roychowdhury [18], who were the first after Mayers to obtain a complete proof of security.

The formal security proofs establish that, if the bit error rate (BER), δ, observed in the verification test is low enough, then the secure final key can be extracted from the sifted key at a nonzero asymptotic rate. For example, in the case where error correction and privacy amplification are carried out using only one-way communication from Alice to Bob, the ratio of the length k of the final key (after error correction and privacy amplification) to the length n of the sifted key satisfies

$$R = \lim_{n\to\infty} k/n \geq 1-2H_2(\delta), \qquad \text{(Equation A-1)}$$

where $H_2(\delta) \equiv -\delta\log_2\delta - (1-\delta)\log_2(1-\delta)$ is the binary Shannon entropy function. Hence, secure key exchange can be achieved for any $\delta < 11\%$. The proof shows the following: Suppose Eve uses a strategy that passes the verification test with a probability that is not exponentially small. For *any* such attack by Eve, if the verification test succeeds then Alice and Bob agree with high probability on a final key that is nearly uniformly distributed, and Eve's information about the final key is exponentially small. Here "exponentially small" means bounded above by (e^{-Ck}) where k is the length of the final key and C is a positive constant, "high probability" means exponentially close to 1, and "nearly uniformly distributed" means exponentially close to a uniform distribution. Informally, for any attack, either Alice and Bob are almost certain to catch Eve, or else Eve knows almost nothing about the final key.

The Shor-Preskill method was adapted by Lo [19] to prove the security of the six-state protocol for BERs up to 12.7%, and by Tamaki, Koashi, and Imoto [20] to prove the security of B92. Gottesman and Lo [21] have shown that if Alice and Bob use two-way communication to correct errors and amplify privacy, then secure key distribution is still possible in BB84 for BERs up to 18.9%, and in the six-state protocol for BERs up to 26.4%. On the other hand, it is known that information-theoretically secure key distribution is impossible if the BER is above 25% in BB84 or 33% in the six-state protocol—these are the error rates that arise if Eve measures each signal in a randomly selected basis and then sends onto Bob the state resulting from her measurement ("intercept/resend attack"). If Alice and Bob are limited to one-way communication, then secure key distribution is impossible if the BER is above 14.6% in BB84 or 16.7% in the six-state protocol—these are the error rates that arise if an optimal approximate cloner diverts to Eve a state identical to that received by Bob. It is an interesting challenge to close the gaps between the best known upper and lower bounds on the BER.

The Shor-Preskill method was also applied by Gottesman and Preskill [22] to a continuous-variable key-distribution protocol, in which Alice sends a squeezed state and Bob performs a homodyne measurement. This scheme is information-theoretically secure if Alice's signals are squeezed sufficiently. Protocols in which Alice's signals are coherent states have been shown to be secure against certain types of individual attacks [23], but whether information-theoretic security can be established for a coherent-state protocol remains an important open question.

QKD has also been called *quantum key expansion*, emphasizing that Alice and Bob must share a short private key at the start of the protocol, which expands to a much longer key when key distribution is successful. The initial key is used for *authentication*; Alice and Bob need a way to guarantee that they are really talking to one another. Otherwise, Eve could pretend to be Alice when talking to Bob and pretend to be Bob when talking to Alice ("man-in-the-middle attack"). Information-theoretically secure classical protocols for authentication are known, but these require Alice and Bob to share the initial secret key. Suppose that the initial key used for authentication was in fact generated during a previous round of quantum key expansion—might the eavesdropper exploit this feature to sharpen her attack? This subtle question was answered recently by Ben-Or and Mayers, [24] who showed that QKD can be safely composed with authentication without compromising security. This work also highlights the importance of formulating careful definitions of security that are amenable to composability.

Information-theoretic security has also been called "unconditional security," to emphasize that there are no assumptions about the technological sophistication or computational power of the adversary. But of course there are conditions that must be satisfied for security proofs to apply—in any analysis of security we have to decide what to trust and what to mistrust. For example, in discussions of QKD, we typically accept that Alice's random number generator is reliable, and that Eve has no *a priori* knowledge of the bases chosen by Alice and Bob in the protocol. Furthermore, assumptions are needed about the performance of the equipment used in the protocol, and these should be carefully considered to assess whether QKD is really secure in realistic implementations.

In the original BB84 security proof by Mayers, it is assumed that Alice's source is perfect, but Bob's detector can be completely uncharacterized; the flaws in the detector cannot fool Alice and Bob into accepting a key that Eve knows, and the rate of key generation R for a given BER Q is independent of the detector's performance. Koashi and Preskill [25] showed that an analogous result holds if the detector is perfect and the source is uncharacterized, as long as the source does not leak to Eve any information about Alice's basis choice.

The security analysis is more delicate if the faulty performance of the source *does* reveal some information about the basis choice. Of particular practical importance is the case where the source emits weak coherent states rather than single photons, and Alice's qubit is encoded in the photon polarization. The source occasionally emits more than one photon in the same polarization state, and Eve can skim off the extra photon(s), wait until Alice and Bob announce their bases, and then measure in the correct basis, obtaining perfect polarization information at no cost in disturbance. The privacy-amplification scheme must be sufficiently powerful (and the coherent states sufficiently weak), to nullify this advantage. Inamori, Lütkenhaus, and Mayers [26] proved the information-theoretic security of BB84, where Alice's source emits weak

coherent states and Bob's detector is uncharacterized, establishing that secure final key can be extracted from sifted key at an asymptotic rate

$$R \geq (1 - \square) - H_2(\square) - (1 - \square) H_2(\square / (1 - \square)); \qquad \text{(Equation A-2)}$$

here $\square$ is the BER observed in the verification test, and $\square = p_M / p_D$, where p_M is the probability that the source emits multiple-photons, and p_D is the probability that a photon emitted by the source is detected by Bob.

More generally, if we trust a characterization of the equipment ensuring that the flaws in the source and detector are sufficiently small, then in many cases information-theoretic security can be proven, and lower bounds on the asymptotic key generation rate established; various examples have been analyzed by Gottesman, Lo, Lütkenhaus, and Preskill [27]. Furthermore, Mayers and Yao [28] have formulated the concept of a "self-testing" source and detector, which can be reliably characterized even if we do not trust the devices used to test the equipment. However, we are still lacking a complete proof of security that applies to arbitrary attacks by the eavesdropper and fully realistic implementation.

Another difficulty for the implementation of QKD using polarization encoding is that optical fibers rotate the polarization, and the amount of rotation may fluctuate over time. Boileau, Gottesman, Laflamme, Poulin, and Spekkens [29] proposed a means of overcoming this difficulty, in which the key bits are encoded in a noiseless subsystem. Their scheme requires Alice to have a source of entangled photons.

A serious limitation on practical QKD is that losses in optical fibers limit the range over which a secure key can be established. In principle, the range could be extended dramatically using "quantum repeaters" that implement quantum error correction; this might be an important application for quantum computers of modest scale. For example Dür, Briegel, Cirac, and Zoller, [30] among others, have described how, with reasonable resources, a nested cascade of entanglement distillation protocols can establish high-fidelity entangled pairs over long distances, which could then be used for key distribution. Further theoretical work aimed at optimizing the efficiency of quantum repeaters may prove fruitful.

Let us summarize the current status of the theory of QKD. The designer of a cryptographic system should ensure that the security of the system rests on a firm foundation. It is reckless to underestimate the ingenuity of the adversary and inherently risky to assume that the eavesdropper will use a particular strategy, even if that assumption seems to be warranted by apparent technological limitations. Therefore, theorists have focused primarily on establishing the security of QKD against unrestricted attacks by the eavesdropper ("information-theoretic" or "unconditional" security). Satisfactory proofs of security have been found for protocols executed under ideal conditions. However, existing quantum cryptosystems are far from ideal, and the demanding criteria that these systems must meet to provide genuine security pose new challenges for the system designer, quite distinct from the problems encountered in classical cryptography. Recent results show that information-theoretic security can be maintained in the presence of certain kinds of system faults. An important goal for future research is to sharpen our understanding of the conditions that ensure adequate security, so that practitioners of QKD can achieve high confidence in the reliability of their systems.

8. Quantum-computational security

References

[1] Wiesner, S., "Conjugate coding," originally written *c.* 1970 but unpublished until *Sigact News* **15**(1), 78–88 (1983).

[2] Bennett, C.H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179.

[3] Wiedemann, D., "Quantum cryptography," *Sigact News* **18**(2), 48–51 (1987); Bennett, C.H. and G. Brassard, "Quantum public key distribution reinvented," *Sigact News* **18**(4), 51–53 (1987).

[4] Ekert, A.K., "Quantum cryptography based on Bell's theorem," *Physical Review Letters* **67**, 661–663 (1991).

[5] Bennett, C.H., G. Brassard, and N.D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters* **68**, 557–559 (1992).

[6] Bruss, D., "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters* **81**, 3018–3021 (1998), [preprint *quant-ph/9805019*].

[7] Bennett, C.H., "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters* **68**, 3121–3124 (1992).

[8] Biham, E., B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Physical Review A* **54**, 2651–2658 (1996), [preprint *quant-ph/9604021*].

[9] Ralph, T.C., "Continuous variable quantum cryptography," *Physical Review A* **61**, 010303 (2000), [preprint *quant-ph/9907073*].
Hillery, M., "Quantum cryptography with squeezed states," *Physical Review A* **61**, 022309 (2000), [preprint *quant-ph/9909006*].
Reid, M.D., "Quantum cryptography with a predetermined key, using continuous variable Einstein-Podolsky-Rosen correlations," *Physical Review A* **62**, 062308 (2000), [preprint *quant-ph/9909030*].
Pereira, S.F., Z.Y. Ou, and H.J. Kimble, "Quantum communication with correlated nonclassical states," *Physical Review A* **62**, 042311 (2000), [*quant-ph/0003094*].

[10] Bennett, C.H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology* **5**(1), 3–28 (1992).

[11] Yao, A.C.-C., "Security of quantum protocols against coherent measurements," in *Proc. 27th ACM Symposium on the Theory of Computing* (ACM press, New York, 1995), pp. 67–75.

[12] Mayers, D., "Unconditional security in quantum cryptography," *Journal of the ACM* **48**(3), 351–406 (2001), [preprint *quant-ph/9802025*].

[13] Bennett, C.H., G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters* **76**(5), 722–725 (1996), [preprint *quant-ph/9511027*], Erratum: *Physical Review Letters* **78**(10), 2031 (1997).

[14] Deutsch, D., A.K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Physical Review Letters* **77**(13), 2818–2821 (1996), [preprint *quant-ph/9604039*], Erratum: *Physical Review Letters* **80**(9), 2022 (1998).

[15] Lo, H.-K. and H.F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science* **283**(5410), 2050–2056 (1999), [preprint *quant-ph/9803006*].

[16] Shor, P.W. and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters* **85**(2), 441–444 (2000), [preprint *quant-ph/0003004*].

[17] Ben-Or, M., "Simple security proof for quantum key distribution," (presentation available at URL: http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html).

[18] Biham, E., M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," in the *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing* (ACM press, New York, 2000), pp. 715–724, [preprint *quant-ph/9912053*].

[19] Lo, H.-K., "Proof of unconditional security of six-state quantum key distribution scheme," *Quantum Information and Computing* **1**(2), 81–94, (2001), [preprint *quant-ph/0102138*].

[20] Tamaki, K., M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Physical Review Letters* **90**, 167904 (2003), [preprint *quant-ph/0210162*].

[21] Gottesman, D. and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Transactions on Information Theory* **49**(2), 457–475 (2003), [preprint *quant-ph/0105121*].

[22] Gottesman, D. and J. Preskill, "Secure quantum key distribution using squeezed states," *Physical Review A* **63**, 022309 (2001), [preprint *quant-ph/0008046*].

[23] Grosshans, F. and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters* **88**, 057902 (2002), [preprint *quant-ph/0109084*].

[24] Mayers, D. and M. Ben-Or, "Composing quantum protocols," (presentation available at URL: http://www.msri.org/publications/ln/msri/2002/qip/mayers/1/index.html).

[25] Koashi, M. and J. Preskill, "Secure quantum key distribution with an uncharacterized source," *Physical Review Letters* **90**, 057902 (2003), [preprint *quant-ph/0208155*].

[26] Inamori, H., N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," preprint available at http://arxiv.org/abs/quant-ph/0107017.

[27] Gottesman, D., H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," preprint available at http://arxiv.org/abs/quant-ph/0212066.

[28] Mayers, D. and A. Yao, "Self testing quantum apparatus," preprint available at http://arxiv.org/abs/quant-ph/0307205.

[29] Boileau, J.-C., D. Gottesman, R. Laflamme, D. Poulin, and R.W. Spekkens, "Robust polarization-based quantum key distribution over collective-noise channel," preprint available at http://arxiv.org/abs/quant-ph/0306199.

[30] Dür, W., H.-J. Briegel, J.I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Physical Review A* **59**(1), 169–181 (1999), [preprint *quant-ph/9808065*], Erratum: *Physical Review A* **60**(1), 725 (1999).

[31] Mayers, D., "Unconditionally secure quantum bit commitment is impossible," *Physical Review Letters* **78**(17), 3414–3417 (1997), [preprint *quant-ph/9605044*].

[32] Lo, H.-K. and H.F. Chau, "Is quantum bit commitment really possible?" *Physical Review Letters* **78**(17), 3410–3414 (1997), [preprint *quant-ph/9605026*].

[33] Kent, A., "Unconditionally secure bit commitment," *Physical Review Letters* **83**(7), 1447–1450 (1999), [preprint *quant-ph/9810068*].

[34] Spekkens, R.W. and T. Rudolph, "Degrees of concealment and bindingness in quantum bit commitment protocols," *Physical Review A* **65**, 012310 (2002), [preprint *quant-ph/0106019*].

[35] Hardy, L. and A. Kent, "Cheat sensitive quantum bit commitment," preprint available at http://arxiv.org/abs/quant-ph/9911043;
Aharonov, D., A. Ta-Shma, U.V. Vazirani, and A.C. Yao, "Quantum bit escrow," in the *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 705–714, [preprint *quant-ph/0004017*].

[36] Ambainis, A., "Lower bound for a class of weak quantum coin flipping protocols," preprint available at http://arxiv.org/abs/quant-ph/0204063.

[37] Spekkens, R.W. and T. Rudolf, "A quantum protocol for cheat-sensitive weak coin flipping," *Physical Review Letters* **89**, 227901 (2002), [preprint *quant-ph/0202118*].