PERSPECTIVES: QUANTUM CRYPTOGRAPHY

Privacy in a Quantum World

Charles H. Bennett and Peter W. Shor

When information is stored in microscopic systems such as single atoms or photons, it obeys quantum rather than classical laws. Once regarded only as a nuisance, this fact has recently been used to devise novel and potentially useful forms of information processing that can only be carried out by quantum means. The most famous example is the quantum computer that could factor large numbers exponentially faster than any classical computer. In most areas of this field, theory far outpaces experiment: Reams of algorithms have been written for quantum computers, but existing laboratory realizations are mere toddlers, able to take only a few steps before they fall.

The one exception is quantum cryptography, which is poised to give, not only in principle but also in practice, a means of communication more private than any other. In this area, experiment has outpaced theory: There have been ambitious experimental realizations, extending many kilometers through commercial optical wires (*1*) and 1 km through the open air (*2*), but until recently only partial and incomplete proofs of their security. Recent advances, however, have led to success on two fronts. First, a new quantum cryptographic protocol and proof technique by Lo and Chau (*3*) gives a transparent and intuitive proof of security, although it requires a quantum computer for its implementation. Second, Mayers (*4*) and others (*5*) have proved the security of standard quantum cryptographic protocols, which do not require a quantum computer for their implementation but nevertheless should be proved secure against an adversary armed with one.

The problem these protocols solve is to enable two protagonists, "Alice" and "Bob," who share no secret information initially, to transmit a secret message x, for example, a cryptographic key, under the nose of an adversary "Eve," who is free to eavesdrop on all their communications (see left panel in the figure). If Alice and Bob are limited to classical communication, they cannot detect eavesdropping, nor can they prevent Eve from overhearing enough information to recover their entire secret. The best they can hope for is to make it computationally difficult for her to do so. But even that hope is vain if Eve has a quantum computer, because all widely used systems of classical public key cryptography, for example, those used to encrypt secure electronic commerce on the internet, depend on computations like factorization, which may be intractable classically but would be easy on a quantum computer.

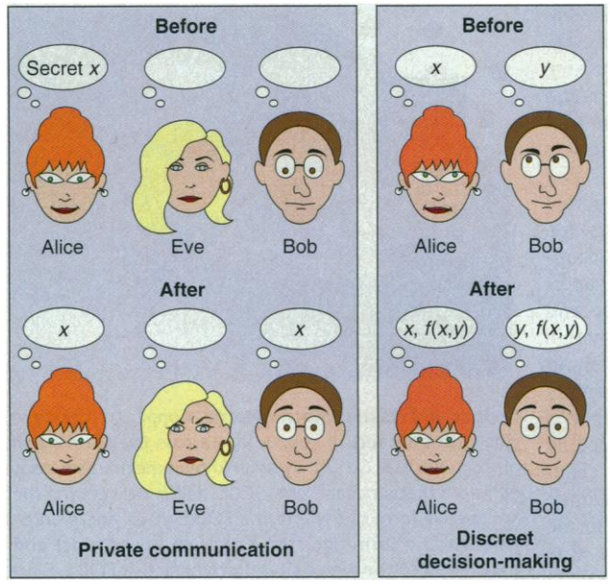
In quantum key distribution (QKD), Alice and Bob's classical public communication is supplemented by a quantum channel, which Eve is also free to eavesdrop on ... if she dares. Because of the fragile nature of quantum information, any eavesdropping disturbs the quantum transmission in a way likely to be detected by Alice and Bob. A quantum cryptographic protocol is considered secure if any eavesdropping strategy is almost certain either to be detected (causing Alice and Bob to abort the protocol and start over) or else to yield negligible information on the secret key, x, that Alice and Bob agree on.

To be useful as well as secure, a QKD protocol cannot simply quit at the first sign of trouble, because in a realistic setting quantum transmissions will usually be somewhat disturbed by channel and detector noise, even when there is no eavesdropping. Alice and Bob must devise a way to distill some amount of the highly secure key, x, even from a session partly compromised by noise or by eavesdropping masquerading as noise. This technique, called privacy amplification, is well understood in classical information theory; however, such classical techniques must be customized before they can be applied in a quantum setting.

Lo and Chau (*3*) have devised a QKD protocol that allows classical reasoning to be applied to error correction. Unfortunately, Alice and Bob each need a quantum computer in this approach. Mayers (*4*) avoids this requirement at the cost of much more complex reasoning, relying instead on the conjugacy of the local observables (such as rectilinear and circular polarization) used in traditional QKD protocols, that is, the fact that measuring either observable completely randomizes the other. Other researchers (*5*) have arrived independently at Mayers' conclusion by other means.

This current crop of full security proofs was preceded by a long train of proofs against more limited attacks, in which Eve, for example, was limited to measuring Alice's photons one at a time (*6*). However, QKD security research is far from finished. The proof of security for traditional protocols, not involving a quantum computer, so far depends on exact conjugacy of the transmitted states (*4*, *5*). This restriction can probably be lifted, and it will need to be to cover most current QKD implementations, which do not use single photons but rather dim coherent light pulses whose multiphoton contributions render the states nonconjugate and provide additional avenues for eavesdropping (*7*).

Private communication is just one of cryptography's goals. Another goal, especially important in the post–Cold War world, is discreet decision making (DDM) or secure two-party computation, the ability of two parties who do not entirely trust each other to reach a common decision based on private information they do not wish to reveal even to each other. This can be cast mathematically as evaluating an agreed-on function f of two private inputs x and y (see



Privacy and discretion. One traditional goal of cryptography (**left**), which quantum techniques help to fulfill, is to allow private communication between two parties, Alice and Bob, despite eavesdropping attempts by a third party, Eve. Another goal (**right**), for which quantum techniques are less helpful, is to allow discreet decision making by two parties who do not wish to share all their secrets.

C. H. Bennett is at the T. J. Watson Research Center, IBM, Yorktown Heights, NY 10598, USA. P. W. Shor is at AT&T Labs-Research, Florham Park, NJ 07932, USA. E-mail: bennetc@watson.ibm.com

right panel in the figure). It was once hoped that quantum mechanics would lead to an unconditionally secure protocol for DDM, as it does for QKD, but this hope was dashed 2 years ago (*8*), when it was shown that one prerequisite for DDM, called bit commitment, cannot be made unconditionally secure against quantum attacks. Conditionally secure DDM, based on classical bit commitments that are merely infeasibly hard, not impossible, for a quantum computer to break, remains a possibility.

References and Notes

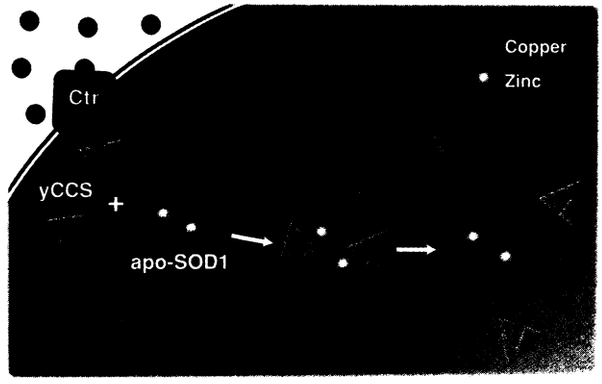
1. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, *Electron. Lett.* **34**, 2116 (1998); R. J. Hughes, G. L. Morgan, C. G. Peterson, in preparation (eprint available at xxx.lanl.gov/abs/quant-ph/9904038).
2. W. T. Buttler *et al.*, *Phys. Rev. Lett.* **81**, 3283 (1998).
3. H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
4. D. Mayers, eprint available at xxx.lanl.gov/abs/quant-ph/9802025 (September 1998). A very preliminary version appeared in D. Mayers and A. Yao, *Adv. Cryptol. Proc. Crypto* **96**, 343 (1996).
5. T. Mor and E. Biham (unpublished presentation at AQIP-99 Conference, DePaul University, Chicago, IL, 17 to 22 January 1999) gave an unconditional proof based on their previous proofs against more limited attacks; M. Ben-Or (private communication) has a proof based on communication complexity of the inner product function.
6. R. B. Griffiths and C.-S. Niu, *Phys. Rev. A* **56**, 1173 (1997); E. Biham, M. Boyer, G. Brassard, J. van de Graaf, T. Mor, *Phys. Rev. Lett.* **78** 2256 (1997), and references therein.
7. N. Lutkenhaus and T. Mor (presentations at AQIP-99 Conference, DeDaul University, Chicago, IL, 17 to 22 January 1999) cite dangers of multiphoton components in practical QKD sources; D. Mayers and A. Yao [in *IEEE Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 1999), p. 503] indicate an approach to dealing with such nonideal sources.
8. D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997); H.-K. Lo and H. F. Chau, *ibid.*, p. 3410.

PERSPECTIVES: BIOCHEMISTRY

Free Copper Ions in the Cell?

Stephen J. Lippard

Transition metal ions are essential for life (*1*). Cells regulate the traffic of transition metal ions (such as copper and iron), maintaining the amount necessary for biological function while avoiding excess levels that are toxic (*2*). Among the factors required to achieve such metal ion homeostasis are the metallochaperones, proteins that, like chaperones in ordinary life, guide and protect transition metal ions within the cell, delivering them safely to the appropriate protein receptors (*3*). One such metallochaperone is yCCS, a yeast protein encoded by the *LYS7* gene. This copper chaperone and its homologs in mice and humans deliver copper to the antioxidant enzyme copper-zinc superoxide dismutase (SOD1) and colocalize with SOD1 in vivo (*4*–*6*). SOD1 is mutated in people with an inherited form of familial amyotrophic lateral sclerosis, a fatal neurological disorder also known as Lou Gehrig's disease, that may be caused by aberrant effects of copper facilitated by improperly folded forms of the enzyme (*7*). Colocalization of CCS and SOD1 in mammalian tissue of the central nervous system is particularly intriguing and may yield clues for developing therapeutic strategies to treat this disease (*6*). On page 805 of this issue, Rae *et al.* show that yCCS directly inserts copper into SOD1 and is active at very low copper concentrations (*8*). In the course of their investigation, the authors made the remarkable discovery that the upper limit of so-called "free" pools of copper was far less than a single atom per cell. It had been commonly believed that metal ions were in equilibrium with metalloproteins. The implications of this finding are profound, especially if applicable to other physiologically important transition metals.



Copper and its metallochaperone. Copper trafficking in yeast begins with transport of copper ions across the plasma membrane by proteins such as Ctr (*9*). By an unknown mechanism, copper is loaded into a metallochaperone, yCCS, which delivers the metal ions to an inactive form of the enzyme SOD1. yCCS docks onto apo-SOD1 (the inactive form depicted as having bound zinc) and copper is transferred to the active sites, forming active SOD1. Once copper is loaded into its binding sites, yCCS molecules lacking copper are available for additional rounds of metal ion delivery to the enzyme. Although pools of free copper are available outside the cell, none are available within under normal growth conditions. (Metallochaperones that deliver copper to target proteins other than SOD1 are drawn in different colors and sizes. Proteins such as metallothionein that buffer total copper concentrations in the cell are not shown.)

A study of how SOD1 acquires copper in vivo resulted in the discovery of yCCS (*4*). Yeast is an excellent model system to investigate the trafficking of transition metal ions in eukaryotes. The Ctr family of membrane proteins facilitates the transport of copper ions across the yeast plasma membrane, and yCCS and two other copper metallochaperones assure its delivery to specialized compartments or enzymes in the cell (*9*) (see the figure).

Rae *et al.* considered three possible ways in which yCCS could mediate transfer of copper to apo-SOD1, an inactive form of SOD1, and so activate the enzyme: (i) yCCS could fold and stabilize the apoprotein into a conformation required to bind copper, (ii) it could itself modulate intracellular concentrations of copper, or (iii) it could directly insert copper into the enzyme. They now show that the third possibility is the correct one (*8*). They established through in vitro studies that, although several low molecular weight complexes of Cu(I) and Cu(II) could add copper to SOD1, only yCCS was capable of doing so in the presence of exceptionally strong copper-chelating agents that reduced available copper ions to very low concentrations. In a second line of evidence, they found no SOD1 activity in strains of yeast that lacked the *LYS7* gene and thus were deficient in yCCS (even though the yeast had normal concentrations of copper ions). In a further experiment, the authors looked at the ability of copper in the growth medium to activate SOD1 in yeast deficient in both yCCS and metallothionein (a protein that serves to buffer cellular copper ion concentrations). The levels of cellular copper increased tenfold and SOD1 activity was observed. Much larger (toxic) amounts of extracellular copper were required to activate SOD1 in the presence of metallothionein. Taken together, these results provide an indirect but persuasive case that CCS functions in vivo as a metallochaperone, specifically transferring copper to its target enzyme (see the figure).

The finding that the insertion of copper into apo-SOD in vivo requires CCS is interesting because the equilibrium constant for the dissociation of Cu(II) from the enzyme is in the femtomolar range (*10*). From this thermodynamic information and a measure of the number of SOD molecules in the cell, the investigators estimated an upper

SOURCE: FELICE FRANKEL

The author is in the Department of Chemistry, Massachusetts Institute of Technology, Cambridge, MA 02139, USA. E-mail: lippard@lippard.mit.edu