From Quantum Cheating to Quantum Security

For thousands of years, code-makers and code-breakers have been competing for supremacy. Their arsenals may soon include a powerful new weapon: quantum mechanics.

Daniel Gottesman and Hoi-Kwong Lo

Cryptography—the art of code-making—has a long history of military and diplomatic applications, dating back to the Babylonians. In World War II, the Allies' feat of breaking the legendary German code Enigma contributed greatly to their final victory. Nowadays, cryptography is becoming increasingly important in commercial applications for electronic business. Sensitive data such as credit card numbers and personal identification numbers (PINs) are routinely transmitted in encrypted form. Quantum mechanics is a new tool for both code-breakers and code-makers in their eternal arms race. It has the potential to revolutionize cryptography both by creating perfectly secure codes and by breaking standard encryption schemes.

The best-known application of cryptography is secure communication,[1] illustrated in figure 1. Suppose Alice would like to send a message to Bob, but there is an eavesdropper, Eve, who is wiretapping the channel. To prevent Eve from knowing the message, Alice may perform encryption—that is, transform the message to something that is unintelligible to Eve—during the communication. On receiving the message, Bob inverts the transformation and recovers the message.

Bob's advantage over Eve lies in his knowledge of a secret, commonly called the key, that he shares with Alice. The key tells him how to decode the message. Consider this example (in the style of cold-war espionage thrillers):

> *The rumble of Soviet tanks shook the Prague hotel room (number 117) as secret agent John Blond finished decoding his orders from his superior, N. He tore the used page from the codebook and immediately burned it with his lighter.*

Blond is using a perfectly unbreakable cipher, a "one-time pad." The secret codebook allows N and Blond to share a long secret binary string—the key—before Blond leaves on his mission. Whenever N would like to send a message to Blond, she first converts it to binary. She then takes the exclusive-OR (XOR) between each bit of the message and the corresponding key bit to generate the encrypted message, which is transmitted over a public channel. An enemy can intercept the encrypted message, but without the key, it is incomprehensible gibberish, offering no clue to the contents of the original message. On the other hand, Blond, by looking up the key in the codebook, can recover the original message by taking the XOR between the encrypted message and the key. Blond immediately burns the used page of the codebook to prevent it from falling into enemy hands in the future.

Daniel Gottesman *(gottesma@microsoft.com) is a postdoctoral fellow in the theory group at Microsoft Corp in Richmond, Washington.* **Hoi-Kwong Lo** *(hoi_kwong@magiqtech.com) is chief scientist and senior vice president for research and development at MagiQ Technologies Inc (http://www.magiqtech.com) in New York, New York.*

Key distribution problem

> *John Blond finally snapped shut the codebook and sighed. He had been on duty in Czechoslovakia for so long that his codebook was getting thin. He knew his days in Prague would soon be over: N would have to recall him before he used up his whole codebook. Blond recalled master cryptographer R's remonstration: "This is no joking matter, double-one seven.* Never *reuse the one-time pad."*

R was serious for a good reason. The reuse of keys by the Soviet Union (due to the manufacturer's accidental duplication of one-time-pad pages) enabled US cryptanalysts to unmask the atomic spy Klaus Fuchs in 1949.[2] When the key for a one-time pad is used more than once, enemy cryptanalysts have the opportunity to look for patterns in the encrypted messages that might reveal the key. Nevertheless, excellent cryptosystems (known as symmetric cryptosystems) that reuse the key have been developed. The longer the key, the more secure the system. For instance, a widely used system is the Data Encryption Standard (DES), which has a key length of 56 bits. No method substantially more efficient than trying all 2^{56} values of the key is known for breaking DES. It is still conceivable, however, that some yet unknown clever algorithm could defeat DES and its cousins.

For top-secret applications, therefore, the one-time pad is preferable. Blond's predicament illustrates the drawback of the one-time pad: When the secret key is used up, the code cannot be used until the sender and receiver get together to share a new secret key. Sending a courier with a new codebook into the Prague Spring is a dangerous and unreliable business. Even if the courier arrives, Blond and N can never be sure that the codebook was not copied during its journey.

This issue is known as the "key distribution problem." A possible solution is public key cryptography. Instead of a single long key shared between the sender and receiver,

© 2000 American Institute of Physics, S-0031-9228-0011-010-5

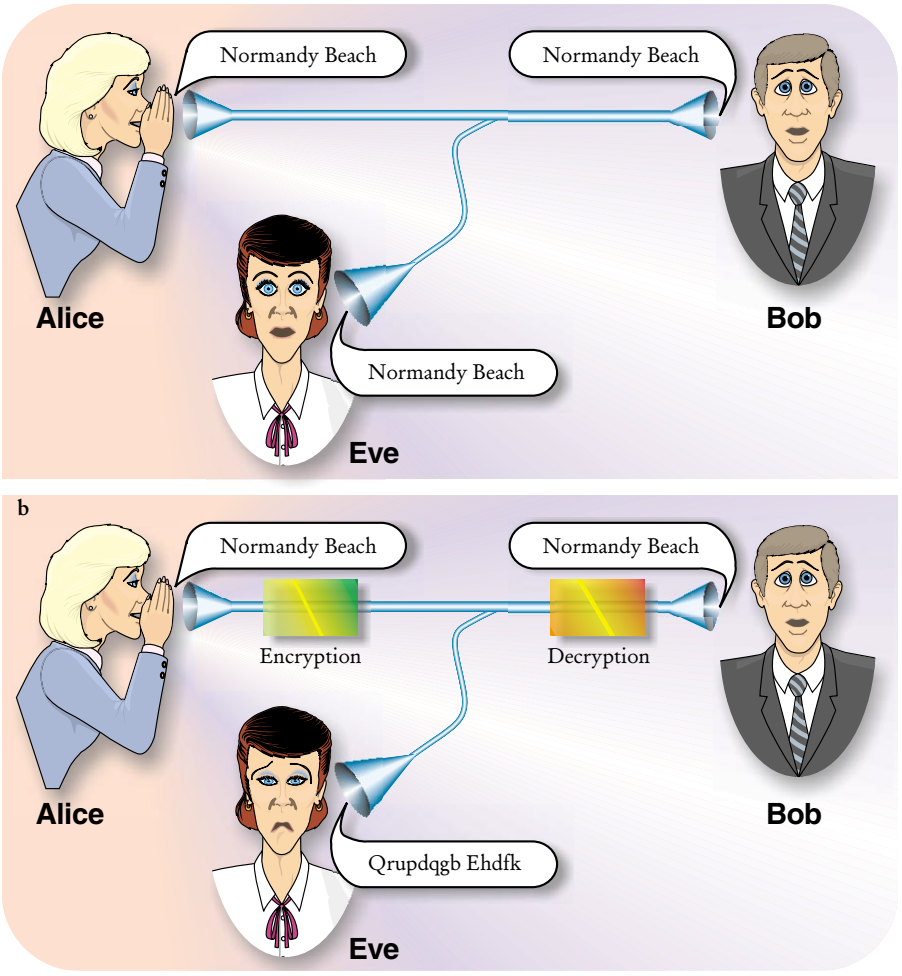

FIGURE 1. COMMUNICATION security. **(a)** Alice sends a message to Bob through a communication channel, but an eavesdropper, Eve, is wiretapping. **(b)** A message is encrypted by Alice using an encryption key. The encrypted message, the *ciphertext*, is now unintelligible to Eve. Bob, who has the same key as Alice, can decrypt the ciphertext and recover the original message. (The code used in this figure is not very secure. Try breaking it yourself; the solution is at the end of the article.)

public key cryptography uses two sorts of keys: one public key, which is known to the world, and one private key, known only to the receiver. Anyone with the public key can send secret messages, but only someone who knows the private key can read them. The important defining feature of public key cryptography is that, even knowing the encryption key, there is no known *computationally efficient* way of working out what the decryption key really is. As an example, the security of the best-known public key cryptosystem, RSA, relies on the difficulty of factoring large integers (see figure 2).

Public key cryptography can be used for another important task: digital signatures. A digital signature exchanges the role of the keys used in public key cryptography: The private key is used to generate a signature and the public key is used to verify it. Only someone with the private key could have created the signature.

Quantum code-breaking

Both DES and RSA rely on an unproven assumption: There is no fast algorithm to determine the secret key. For instance, RSA is believed to be secure because mathematicians throughout the world have worked very hard to break it, steadily producing modest improvements in factoring algorithms, but without groundbreaking success. With only modest increases in key size, users of RSA can easily keep ahead even of the exponential growth in computing power over the years.

Quantum mechanics changed this. In 1994, Peter Shor of AT&T Laboratories invented a *quantum* algorithm for efficient factoring of large numbers.[3] The state of a quantum computer is a superposition of exponentially many basis states, each of which corresponds to a state of a classical computer of the same size. By taking advantage of interference and entanglement in this system, a quantum computer can perform in a reasonable time some tasks that would take ridiculously long on a classical computer. Shor's discovery propelled the then-obscure subject of quantum computing into a dynamic and rapidly developing field, and stimulated scores of experiments and proposals aimed toward building quantum computers.

Another remarkable discovery was made by Lov Grover of Bell Laboratories, Lucent Technologies, who in 1996 invented a quantum searching algorithm[4] (see PHYSICS TODAY, October 1997, page 19). To find one particular item among N objects requires checking $O(N)$ items classically. With Grover's algorithm, a quantum computer need only look up items $O(\sqrt{N})$ times. It can be used to radically speed up the exhaustive key search of DES (that is, trying all 2^{56} possibilities).

If a quantum computer is ever constructed in the future, much of conventional cryptography will fall apart! To provide the same security, the key lengths of symmetric schemes like DES would have to be doubled due to Grover's algorithm. The most commonly used public key schemes are RSA and others based on discrete logarithms or elliptic curves; Shor's algorithm breaks all of them. Even if it is decades until a sufficiently large quantum computer can be built, this is a matter of current concern: Some data, such as nuclear weapons designs, will still need to remain secret, and it is important that today's secret messages cannot be decoded tomorrow.

Quantum code-making

Even if DES and RSA do fall apart, the one-time pad remains a perfectly unbreakable cipher even against a quantum computer. However, as previously discussed, it has a serious catch: the key distribution problem. It presupposes that Alice and Bob share a key that is secret and as long as the message. There is no way to guarantee that

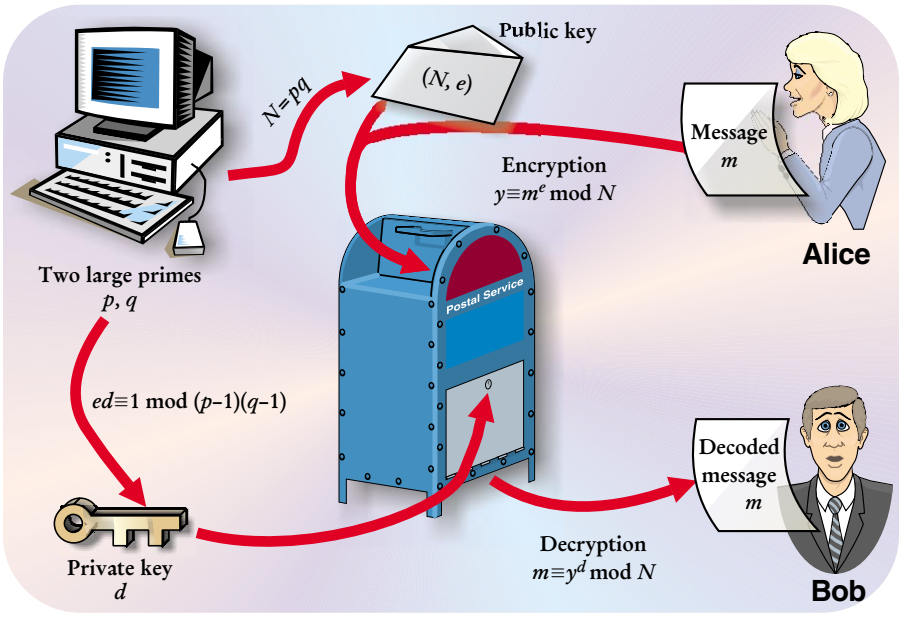

FIGURE 2. THE RSA PUBLIC KEY cryptosystem. The best-known public key system is called RSA, after its inventors Ronald Rivest, Adi Shamir, and Leonard Adleman. It is based on modular arithmetic over a large base N that is the product of two large primes p and q. If x is relatively prime to N, the Euler–Fermat theorem tells us that $x^r \equiv 1 \bmod N$, where $r = (p-1)(q-1)$. The public key is a pair of numbers (N, e), and the private key is d, with $ed \equiv 1 \bmod r$ (that is, $ed = kr + 1$ for some integer k). To encrypt a message m, the sender (Alice) computes $y \equiv m^e \bmod N$. To decrypt the message y, the receiver (Bob) computes $y^d \bmod N \equiv m^{ed} \bmod N \equiv m$. For this step, Bob has to know the private key d. Anyone can send Bob an encrypted message, but only Bob can decrypt it.

in practice. Trusted couriers can be bribed or even intercepted without their knowledge. More generally, classical signals are distinguishable. An eavesdropper can reliably read the signals without changing them. Therefore, in classical physics there is nothing, in principle, to prevent an eavesdropper from wiretapping the key distribution channel passively.

Fortunately, quantum mechanics helps to make codes as well as break them.[5] (See also Charles Bennett's article, "Quantum Information and Computation," PHYSICS TODAY, October 1995, page 24.) The Heisenberg uncertainty principle dictates that it is fundamentally impossible to know the exact values of complementary variables such as a particle's momentum and its position. This apparent limitation imposed by quantum mechanics can be a powerful tool in catching eavesdroppers. The central idea is to use nonorthogonal quantum states to encode information. More concretely, the essence of quantum cryptography can be understood in a single question: Given a single photon in one of four possible polarizations (↔, ↕, ↗, or ↖), can one determine its polarization with certainty? Surprisingly, the answer is no. The rectilinear basis (↔ and ↕) and the diagonal basis (↗ and ↖) are incompatible, so the Heisenberg uncertainty principle forbids us from simultaneously measuring both. More generally, experiments distinguishing nonorthogonal states, even if only partially reliable, will disturb the states.

The key distribution problem can be partially solved by quantum mechanics using the idea of quantum key distribution (QKD). The first and best-known protocol, usually called "BB84" because it was published in 1984 by Charles Bennett and Gilles Brassard,[6] is described in the box below. In a prototypical QKD protocol, Alice sends some nonorthogonal quantum states to Bob, who makes some measurements. Then, by talking on the phone (which need not be secure), they decide if Eve has tampered with the quantum states. If not, they have a shared key that is guaranteed to be secret. Note that Alice and Bob must share some authentication information to begin with; otherwise, Bob has no way to know that the person on the phone is really Alice, and not a clever mimic. The key generated by QKD can subsequently be used for both encryption and authentication, thus achieving two major goals in cryptography.

Experimental QKD

QKD is an active experimental subject. The first working prototype, constructed in 1989 at IBM in Yorktown Heights, New York, transmitted quantum signals over 32 cm of open air.[7] Since then, various groups—including

The BB84 Protocol

In the best-known quantum key distribution (QKD) scheme, BB84, Alice sends Bob a sequence of photons, each independently prepared in one of four polarizations (↔, ↕, ↗, or ↖). For each photon, Bob randomly picks one of the two (rectilinear and diagonal) bases to perform a measurement. He keeps the measurement outcome secret. Now Alice and Bob publicly compare their bases. They keep only the polarization data for which they measured in the same basis. In the absence of errors and eavesdropping by Eve, these data should agree.

To test for tampering, they now choose a random subset of the remaining polarization data, which they publicly announce. From there they can compute the error rate (that is, the fraction of data for which their values disagree). If the error rate is unreasonably high—above, say, 10%—they throw away all the data (and perhaps try again later). If the error rate is acceptably small, they perform error correction and also "privacy amplification" to distill a shorter string that will act as the secret key. These steps essentially ensure that their keys agree, are random, and are unknown to Eve.

Other QKD schemes have also been proposed. For example, Artur Ekert of the University of Oxford suggested one based on quantum mechanically correlated (that is, entangled) photons, using Bell inequalities as a check of security. In 1992, Charles Bennett of IBM proposed a simple QKD scheme, called B92, that uses only two nonorthogonal states.

those led by Paul Townsend at the British Telecommunications Photonics Technology Research Centre (now part of Corning), Jim Franson of Johns Hopkins University, Nicolas Gisin and Hugo Zbinden of the University of Geneva, and Richard Hughes of Los Alamos National Laboratory—have made important contributions. A primary focus has been a series of impressive experiments over commercial optical fibers. The world record distance for QKD,[8] at the time of writing, is about 50 km. One of the long-distance experiments, performed at Los Alamos, is depicted in figure 3.

Most experiments to date have used variants of either the BB84 or B92 schemes (see the box), although recently three groups—one led by Paul Kwiat of Los Alamos, Gisin and Zbinden's group at Geneva, and a collaboration led by Anton Zeilinger of the University of Vienna and Harald Weinfurtur of the University of Munich—have independently implemented protocols based on entangled pairs of particles, also known as Einstein-Podolsky-Rosen or EPR states. In the BB84 and B92 schemes, typically a single-photon source is simulated using attenuated coherent states—on average, only a fraction of a photon is actually sent. With additional losses in the fiber, very few arriving laser pulses actually contain a photon. This low yield does not interfere much with key distribution, however, since only the photons that reach Bob are used in the protocol. The key is generally encoded in either the polarization or the phase of the photon. Error rates in the photons actually received are usually a few percent.

For commercial applications in, say, a local area network environment, it is useful for a quantum cryptographic system to be integrated into a passive multiuser optical fiber network and its equipment to be miniaturized. Townsend's group has done much work in this area.[9] For point-to-point applications, the Geneva group has devised a so-called "plug and play" system that automatically compensates for polarization fluctuations.[10] Such systems might someday convey secret information between government agencies around Washington, DC, or connect bank branches within a city.

QKD has also been performed in open air,[11] during daylight, with a current range of about 1.6 km. Ambitious schemes to perform a ground-to-satellite QKD experiment have been proposed. If successful, quantum cryptography may be used to ensure the security of command control of satellites from control centers on the ground.

Future experiments will aim to make QKD more reliable, to integrate it with today's communications infrastructure, and to increase the distance and rate of key generation. Another ambitious goal is to produce a quantum repeater using techniques of quantum error correction. Such an accomplishment will require substantial technical breakthroughs, but would allow key distribution over arbitrarily long distances.

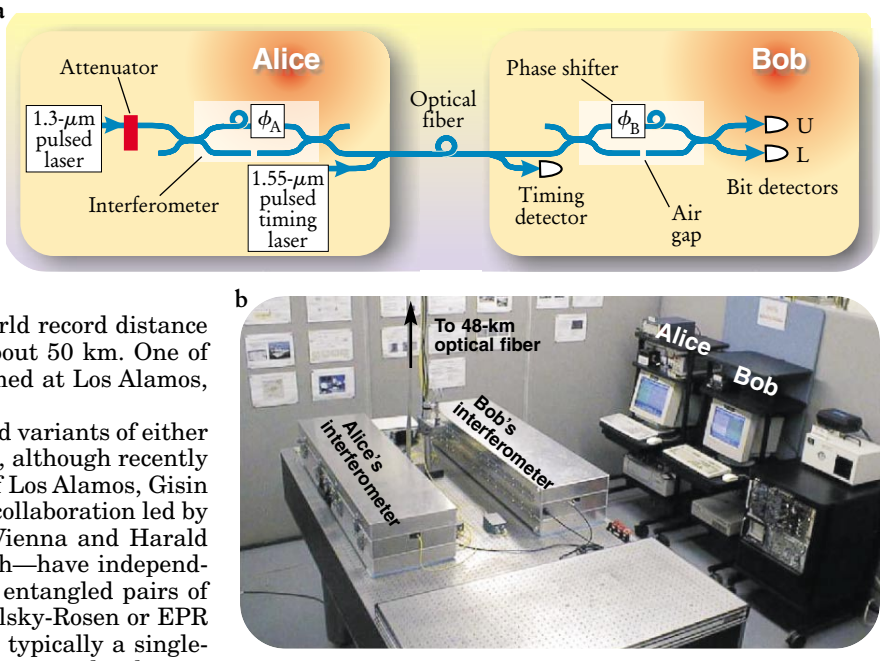

FIGURE 3. EXPERIMENTAL QUANTUM KEY DISTRIBUTION. **(a)** Schematic of the experiment at Los Alamos[8] that implements the protocol known as B92 (see the box on page 24) over 48 km of optical fiber. A laser with a wavelength of 1.3 μm, attenuated to approximate a single-photon source, is the source of the key bits. Its output is passed through Alice's interferometer. The two nonorthogonal quantum states used in the B92 protocol are realized as two possible settings for the phase delay ϕ_A in one branch of the interferometer. To measure the state, Bob passes the photon through his interferometer, adding one of two possible phase shifts ϕ_B, and detects the photon in one of the two bit detectors. A bright pulse from a second laser tells Bob when to expect a photon from Alice. Air gaps in both interferometers allow Alice and Bob to tweak the optical path lengths to keep properly synchronized. **(b)** The actual setup of the experiment. The two boxes in the foreground are the interferometers, connected to each other only through 48 km of optical fiber. (Figure courtesy of Richard Hughes.)

Is QKD secure?

While experiments in QKD forged ahead, the theory developed more slowly. A clever Eve can adopt many possible strategies to fool Alice and Bob, including subtle quantum attacks entangling all of the particles sent by Alice. Taking all possibilities into account, as well as the effects of realistic imperfections in Alice and Bob's apparatus and channel, has been difficult. A long series of partial results has appeared over the years, addressing restricted sets of strategies by Eve,[12] but only in the past few years have complete proofs appeared.

One class of proofs, by Dominic Mayers[13] and subsequently by others, including Eli Biham and collaborators and Michael Ben-Or,[14] attacks the problem directly and proves that the standard BB84 protocol is secure. Another approach, by one of us (HKL) and H. F. Chau,[15] proves the security of a new QKD protocol that uses quantum error-correcting codes.[5] (For more on quantum error correction, see John Preskill, "Battling Decoherence: The Fault-Tolerant Quantum Computer," PHYSICS TODAY, June 1999, page 24.) This approach allows one to apply *classical* probability theory to tackle a *quantum* problem directly. It works because the relevant observables all commute with each other. While conceptually simpler, this protocol requires a quantum computer to implement. The two approaches have been unified by Peter Shor and John Preskill,[16] who showed that a quantum error-correcting protocol could be modified to become BB84 without compromising its security.

The proof of the security of QKD is a fine theoretical result, but it does not mean that a real QKD system would be secure.[17] Some known and unknown security loopholes might prove to be fatal. Apparently minor quirks of a system

can sometimes provide a lever for an eavesdropper to break the encryption. For instance, instead of producing a single photon, a laser may produce two; Eve can keep one and give the other to Bob. She can then learn what polarization Alice sent without revealing her presence. There are various possible solutions to this particular problem; it is the unanticipated flaws that present the greatest security hazard. Ultimately, we cannot have confidence that a real-life quantum cryptographic system is secure until it has withstood attacks from determined real-life adversaries. Traditionally, breaking cryptographic protocols has been considered to be as important as making them—the protocols that survive are more likely to be truly secure. The same standard will have to be applied to QKD.

Post-cold-war applications

There are many problems beyond secure communication that can be addressed by cryptography.

> *Alice and Bob are considering going on a date, but neither is willing to admit their interest unless the other is also interested. How can they decide whether or not to date without letting slip any unnecessary information?*

This dating problem can be phrased as the problem of computing a function $f(a, b) = ab$, where a and b are single bits held respectively by Alice and Bob (0 = not interested, 1 = interested). Problems like this can be solved classically using variants of public key cryptography, which we know might be rendered insecure by quantum computers. By exchanging quantum states, can Alice and Bob solve the above dating problem with absolute security?

There are many possible functions f that two people might wish to compute together, too many to consider each of them individually. Instead, cryptographers rely on a suite of primitive operations that can be combined to build more complex functions. One important protocol is called bit commitment, and it is the electronic equivalent of a locked box. Alice chooses a bit, 0 or 1, and writes it on a piece of paper, which she deposits in the box. She gives the box to Bob but keeps the key. She cannot change what she wrote, and without the key, Bob cannot open the box. But at some later point, Alice can give Bob the key and reveal her bit. By itself, bit commitment is useful mostly for debunking professional psychics, but it serves as a useful building block for more interesting functions.

Consider the following bit commitment scheme[6] proposed by Bennett and Brassard: If Alice wishes to commit to a 0, she sends Bob a polarized photon in the rectilinear basis; if she wishes to commit to a 1, she sends Bob a polarized photon in the diagonal basis. In either case, Alice flips a coin to decide which of the two polarizations to send. Bob has no way to tell which basis Alice used; no matter which bases Alice and he choose, Bob would measure a random value. But when Alice unveils her bit, telling Bob which of the four states she sent, Bob can measure in the appropriate basis to verify that Alice is telling the truth. If she lies about which basis she used, Bob has a 50% chance of finding out. If the protocol is repeated many times, Alice's chance of successfully cheating is abysmally small.

This protocol is secure against a classical cheater, who does not have much ability to store and manipulate quantum states. But as Bennett and Brassard recognized, a *quantum* cheater can break the protocol. Suppose that instead of picking a specific state and sending it to Bob, Alice creates an entangled pair of photons, $(|{\leftrightarrow}{\updownarrow}\rangle - |{\updownarrow}{\leftrightarrow}\rangle)/\sqrt{2}$ (an EPR pair), and sends the second photon to Bob, keeping the first one. She stores the quantum state

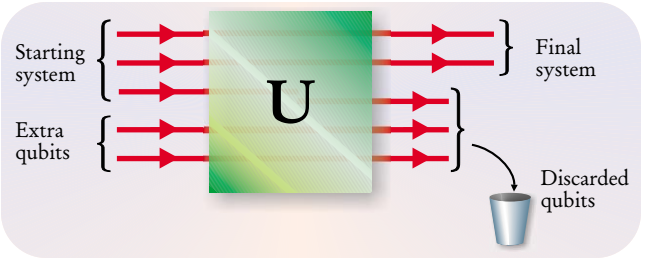

FIGURE 4. THE CHURCH OF THE LARGER HILBERT SPACE. In cryptography—and other areas—the quantum mechanical description of explicitly quantum aspects (such as single-photon polarizations) can be expanded to include other parts as well, including measurements and random number generation. This alternative treatment consists of three steps. First, the original quantum system—which might consist of two-level quantum bits (called "qubits"), for example—is augmented with an additional system. In this expanded Hilbert space, all operations are unitary and can be combined into a single quantum mechanical step (here denoted by "U"). Part of the output of the transformation is thrown away, leaving only the final quantum system of interest. Using quantum mechanics to simulate classical computations and working with pure quantum states allows the most generalized treatment of a problem and simplifies the task of determining whether a given protocol is secure. Describing a protocol in the Church of the Larger Hilbert Space does not change the protocol in any way; it merely provides a new and sometimes simpler way of looking at the system.

of the first photon and delays measuring it. Suppose that when the time comes for Alice to open the commitment, she decides she would like the committed bit to read 0, which requires her to specify a state in the rectilinear basis. Because of the entanglement, Alice knows that if she and Bob measure in the same basis, they will get opposite results. Therefore, she can measure her photon in the rectilinear basis and tell Bob he has the opposite polarization, and she will always be right.

If Alice instead wishes the committed bit to read 1, she needs a state in the diagonal basis. But $(|{\leftrightarrow}{\updownarrow}\rangle - |{\updownarrow}{\leftrightarrow}\rangle)/\sqrt{2} = (|{\nearrow}{\nwarrow}\rangle - |{\nwarrow}{\nearrow}\rangle)/\sqrt{2}$. So Alice can measure her particle in the diagonal basis and again be sure that Bob's measurement outcome will be opposite to hers. Quantum cheating allows Alice to change her mind at the last minute without being caught by Bob, thus totally defeating the purpose of bit commitment.

Nonetheless, more sophisticated schemes for quantum bit commitment were proposed, and for a long time were believed to be secure. Eventually, the bubble burst and it was shown that the above quantum cheating strategy, which uses EPR nonlocality and delayed measurements, can be generalized to break all two-party quantum bit commitment schemes.[18] If Alice and Bob hold one of two pure quantum states that are indistinguishable to Bob, then Alice, acting unilaterally, can change one to the other. Therefore, the two basic requirements of bit commitment—that Bob does not know the bit and that Alice cannot change it—are fundamentally incompatible with quantum mechanics.

The strength of the proof lies in its generality. The idea is to treat the whole system as if it were quantum mechanical, extending the part that was originally quantum to include any dice, measuring devices, and classical computations that appear in the protocol. From this point of view, the original protocol is equivalent to a purely quantum one, with some of the output being thrown in the trash

(see figure 4). Note that throwing something away can never help a cheater, so we might as well assume that the state shared by Alice and Bob is the pure quantum state that is completely determined by the protocol. That assumption substantially reduces the complexity of the problem. It is not difficult to show that when Alice and Bob hold a pure state, quantum bit commitment is impossible.

Following the fall of quantum bit commitment, other important basic quantum cryptographic protocols have also been proven to be insecure by one of us (HKL), thus leaving the field in a shambles. What is left?

Some potential applications in cryptography are too similar to bit commitment and cannot be done at all quantum mechanically. Others have more modest goals and *can* be solved by quantum protocols. For instance, Lior Goldenberg, Lev Vaidman, and Stephen Wiesner of Tel Aviv University have proposed a method of "quantum gambling," in which a cheater must pay a large fine if caught. The majority lie in a middle ground—we do not know whether they can be solved. The dating problem is an example. Many approaches to it tread too near bit commitment and are doomed to failure, but it's possible there are others, as yet undiscovered, that do not.

Physics today, cryptology tomorrow

Quantum computers are still on the drawing boards, and quantum cryptographic systems are only prototypes. Still, there are a number of reasons for thinking about quantum cryptology today. Unlike other cryptosystems, the security of QKD is based on fundamental principles of quantum mechanics, rather than unproven computational assumptions. QKD eliminates the great threat of unanticipated advances in algorithms and hardware breaking a widely used cryptosystem. Small-scale QKD systems are well within the capabilities of today's technology, and commercial systems could be available within a few years (although whether such systems are widely adopted depends on many nonacademic factors, including cost).

Furthermore, grappling with the problems posed by quantum protocols can give us insight into more general questions about quantum mechanical systems in many fields of physics. For instance, one reason it is hard to analyze protocols and attacks is that they frequently involve a combination of quantum and classical behaviors. In considering bit commitment, though, it was possible to replace classical parts of the protocol with a quantum description, an approach that is useful for many problems inside and outside the field of quantum cryptography. This fully quantum treatment is sometimes called the Church of the Larger Hilbert Space, following John Smolin of IBM. All quantum operations, including measurements, are unitary when considered as acting on a larger Hilbert space (figure 4).

Finally, quantum mechanics changes the world of cryptology, and it is important to know what the new terrain will look like to decide on cryptographic standards that may last for decades. In a world where quantum computers and communication are commonplace, today's most widespread public key cryptosystems would no longer work; in the worst case, perhaps *no* public key cryptosystem will work. If so, symmetric cryptosystems and QKD would partially fill the gap, allowing secure communication. Unfortunately, digital signatures would fail as well, meaning important communications would need to be notarized by a trusted third party.

Of course, QKD and symmetric cryptosystems are not useful in situations in which Alice and Bob have never met. Solving this problem would probably require a quantum cryptographic center, which could verify the identity of both of them. The center would have to be known and trusted by both Alice and Bob.

Problems beyond secret communication and digital signatures are a mixed bag. Many, such as bit commitment and perhaps the dating problem, would be impossible, whereas others, such as quantum gambling, could be carried out with complete security.

This is just one of a number of possible futures. Perhaps some new or existing public key cryptosystems will survive quantum computation, or perhaps new public key systems will be developed that can only run on a quantum computer. Perhaps quantum computers will always remain difficult to build (we believe that this is unlikely), and public key cryptography will remain widespread, despite its potential flaws. Only time will tell who benefits more from quantum cryptology: the code-makers or the code-breakers.

Decoding the message in Figure 1

The code is a "Caesar's cipher," in which each letter is shifted by a fixed number of places in the alphabet. In this case, the shift is three places.

References

1. B. Schneier, *Applied Cryptography*, 2nd ed., Wiley, New York (1996).
2. http://www.odci.gov/csi/books/venona/preface.htm, the section "What made Venona possible?"
3. P. W. Shor, in *Proc. 35th Annual Symposium on Foundations of Computer Science* (FOCS), S. Goldwasser, ed., IEEE Press, Los Alamitos, Calif. (1994), p. 124.
4. L. K. Grover, in *Proc. 28th Annual ACM Symposium on the Theory of Computing* (STOC), ACM Press, New York (1996), p. 212.
5. H.-K. Lo, S. Popescu, T. Spiller, eds., *Introduction to Quantum Computation and Information*, World Scientific, Singapore (1998).
6. C. H. Bennett, G. Brassard, in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE Press, Los Alamitos, Calif. (1984), p. 175. The first paper on quantum cryptography was written by Stephen Wiesner around 1970, but it remained unpublished until 1983: S. Wiesner, Sigact News **15** (1), 78 (1983).
7. C. H. Bennett *et al.*, J. Cryptology **5**, 3 (1992).
8. R. J. Hughes, G. L. Morgan, C. G. Peterson, J. Mod. Opt. **47**, 533 (2000). P. D. Townsend, Opt. Fiber Technol. **4**, 345 (1998) and references therein.
9. P. D. Townsend, Nature **385**, 47 (1997).
10. A. Muller *et al.*, Appl. Phys. Lett. **70**, 793 (1997).
11. B. C. Jacobs, J. D. Franson, Opt. Lett. **21**, 1854 (1996). W. T. Buttler *et al.*, Phys. Rev. Lett. **84**, 5652 (2000).
12. For a review, see C. H. Bennett, P. W. Shor, Science **284**, 747 (1999) and references therein.
13. D. Mayers, http://xxx.lanl.gov/abs/quant-ph/9802025, J. Assoc. Comput. Mach. (in press). A preliminary version appeared in D. Mayers, *Advances in Cryptology—Proc. Crypto '96*, N. Koblitz, ed., Springer-Verlag, New York (1996), p. 343.
14. See, for example, E. Biham *et al.*, in *Proc. 32nd Annual ACM Symposium on the Theory of Computing* (STOC), ACM Press, New York (2000), p. 715.
15. H.-K. Lo, H. F. Chau, Science **283**, 2050 (1999). This paper built on earlier work on quantum privacy amplification: D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996); **80**, 2022 (1998) (erratum).
16. P. W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
17. G. Brassard, N. Lütkenhaus, T. Mor, B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
18. D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997). H.-K. Lo, H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997). ■