

Quantum Cryptography
STEVEN J. VAN ENK
Bell Laboratories, Lucent Technologies
Murray Hill, New Jersey

Cryptography has a very long history (Singh, 2000). The ancient civilizations of the Chinese, Egyptians, Greeks, Romans, and Arabs all developed methods of keeping messages secret. Early on, often all that was necessary was hiding the *existence* of a message (steganography). A method developed in China, for instance, involved shaving the head of a messenger, writing the message there, and waiting for the hair to grow back. This method was obviously both inconvenient and time consuming. But the main drawback of steganography is that once the hiding place of a message has been discovered, all of the information in the message is revealed at once. Thus, cryptography, the art of hiding the *meaning* of a message, was born.

There are two basic methods of encrypting a message—transposition and substitution. In transposition, the order of the letters is changed; in substitution, each character (or sometimes a whole word) is replaced by another character (or word), according to certain procedures known to both sender and receiver. Over the course of thousands of years, increasingly complicated versions of encryption protocols have been designed, but in the end, almost every one has been broken.

Every language contains structure—particularly certain letters or letter combinations that appear more often than others—and, if one is not careful, encrypted texts reveal the same structure. Nowadays we know that the only secure way of encrypting a text is by shifting each letter by a random amount. In modern terminology, each bit must be XOR-ed with a random bit. Only then does the encrypted text itself contain no information.

The remaining problem is key distribution, how to get the sender and receiver to agree on the random sequence of bits to be used. Modern methods, the ones used for encryption of Internet communications for instance, all rely on so-called one-way functions—functions that are easy to calculate (roughly speaking, with resources that scale polynomially with the number of bits of the numbers involved) but very hard (scaling exponentially) to invert. For example, public key cryptography (particularly, the well known RSA encryption scheme) is based on the difficulties of factoring large numbers and of taking the discrete logarithm.

This type of protocol has two weaknesses. First, neither of these two tasks has been proven to be exponentially hard. Indeed, a quantum computer can solve both problems in polynomial time (Ekert and Jozsa, 1996; Shor, 1997). Second, with increasingly powerful classical computers and algorithms, or with a powerful quantum computer, a code that cannot be cracked now may be cracked in the future. Therefore, if the encrypted message is stored, it could eventually be deciphered. For most messages this may not be important, but for certain military messages, it may be essential, especially if the time span turns out to be short. Perhaps surprisingly, both problems can be solved with quantum mechanics, which provides an unconditionally secure protocol that relies only on the laws of physics and not on unproven mathematical assumptions (Bennett and Brassard, 1984; Bennett et al., 1992).

Here is how quantum key distribution (QKD) works. Alice (the sender) and Bob (the receiver) wish to create a shared random key. Alice sends Bob a series of polarized photons. First she tosses her coin many times to produce two random sequences of 0's and 1's. One sequence determines which bit she is going to send, the other which polarization basis she will use, either horizontal/vertical polarization, or left-hand/right-hand circular polarization. An eavesdropper cannot find out with certainty which bit was sent. For example, a polarization filter set to block vertical polarization will make no distinction at all between the two circular polarizations because both will be blocked 50

percent of the time. Moreover, if Alice uses such a filter, even a circularly polarized photon that passes through will have vertical polarization. The disturbance of the quantum state caused by measurements is what Alice and Bob will notice.

Let's say Bob chooses a basis too randomly for his polarization measurement. In the absence of errors and eavesdroppers, Bob would find the correct polarization if he happened to choose the same basis as Alice (which occurs with 50 percent probability). To detect the presence of an eavesdropper, they can check a small subset of the bits that should be the same. The fraction of errors they find is the upper bound on how much information an eavesdropper may have gathered. It is only an upper bound, however, because errors may also be caused by other, innocent effects. Once they have an upper bound, Alice and Bob can distill, by purely classical privacy amplification techniques, a shorter random key that is secure to an arbitrary degree. In a simplified example, let's suppose Alice and Bob share two random bits, but they know an eavesdropper knows at most one. If they simply take the sum (XOR) of their two bits, they will have a perfectly secure new random bit.

I have just sketched the ideal protocol. In practice, single photons are very hard to generate. Instead, faint laser pulses are used (the number of photons in a pulse is not fixed but distributed according to a Poisson distribution). The laser light is attenuated so strongly that the average number of photons is only about 0.1 to 0.01. Despite these differences, and despite all kinds of other inevitable imperfections (e.g., losses in fibers, misalignments of optical elements, etc.), such protocols have been proven secure (Inamori, 2002). Because the total number of errors is limited (otherwise the upper bound on the information the eavesdropper has would indicate she knows everything!), and because the main errors are caused by losses inside optical fibers, QKD is possible only over a limited distance.

The state of the art in QKD (Gisin et al., 2002; Townsend, 1998) is as follows: the world record in distance for free-space QKD is 23 km (Kurtsiefer et al., 2002). To avoid turbulence, the communication line was between two mountaintops in Germany. The secure bit rate was about 300 to 400 bits/sec. For QKD over standard optical telecom fibers, the record is 67 km with a secure bit rate of about 60 bits/sec (Stucki et al., 2002). It is important to note that these numbers refer to a protocol with conditional, rather than unconditional, security. The security is based on relaxed, but realistic, assumptions—the eavesdropper cannot store photons, cannot measure the number of photons in a pulse without destroying them, and cannot replace the channel by a channel with no losses.

Secure distances for the unconditional security promised by the original protocols are limited to about 15 to 20 km for fibers, less for free-space QKD. Nevertheless, because no one knows at this moment how to store quantum data for a substantial amount of time, QKD does provide a new type of protection against eavesdropping. In effect, today's QKD messages are safe against tomorrow's technology, which cannot be said of RSA-encrypted data.

As the state-of-the-art experiments have shown, QKD has been advanced beyond proof-of-principle demonstrations in physics laboratories. In fact, the devices developed for QKD are available as commercial products (Stucki et al., 2002), and a whole QKD setup, including the software to perform the classical calculations for privacy amplification, may soon be available. Does this mean a quantum computer is around the corner? Unfortunately, the answer is no, because two requirements for quantum computing are very hard to achieve, although they are not necessary for quantum communication. First, in a quantum computer the quantum states of many qubits, the quantum counterpart of the classical bit, must be stored for roughly as long as the computation runs; for QKD, qubits may be measured and destroyed as soon as they have reached the receiver. Second, the many qubits of a quantum computer must interact with each other in a carefully controlled way; in QKD, the qubits can be sent separately and never have to interact with each other.

Future research will focus on two aspects of QKD—miniaturization of the devices

and improved secure bit rates and longer distances for secure key distribution. The latter will require the development of better single-photon detectors and true single-photon generators. In addition, until “lossless” fibers are developed, the only technique for overcoming fiber losses is quantum error correction, which is a challenging task, comparable in difficulty to building a small quantum computer (van Enk et al., 1998). Despite the challenges that lie ahead, quantum mechanics will someday make communications more secure.

REFERENCES

- Bennett, C.H., and G. Brassard. 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing. Pp. 175-179 in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. New York: IEEE.
- Bennett, C.H., G. Brassard, and A. Ekert. 1992. Quantum cryptography. *Scientific American* 269(4): 26-33.
- Ekert, A., and R. Jozsa. 1996. Quantum computation and Shor’s factoring algorithm. *Review of Modern Physics* 68(3): 733-753.
- Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden. 2002. Quantum cryptography. *Review of Modern Physics* 74(1): 145-195.
- Inamori, H., N. Lutkenhaus, and D. Meyers. 2002. Unconditional Security of Practical Quantum Key Distribution. Available online at: <http://xxx.lanl.gov/abs/quant-ph/0107017>.
- Kurtsiefer, C., P. Zarda, M. Halder, H. Weinfurter, P.M. Gordon, P.R. Tapster, and J.G. Rarity. 2002. A step towards global key distribution. *Nature* 419(6906): 450.
- Shor, P.W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* 26(5): 1484-1509.
- Singh, S. 2000. *The Code Book*. New York: Anchor Books.
- Stucki, D., N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. 2002. Quantum key distribution over 67km with a plug&play system. *New Journal of Physics* 4(41): 1-8. Available online at: <http://www.idquantique.com/qkd.html>.
- Townsend, P.D. 1998. Quantum cryptography on optical fiber networks. *Optical Fiber Technology* 4(4): 345-370.
- van Enk, S.J., J.I. Cirac, and P. Zoller. 1998. Photonic channels for quantum communication. *Science* 279(5348): 205-208.

Copyright © 2003 National Academy of Sciences. All rights reserved.

Unless otherwise indicated, all materials in this PDF File provided by the National Academies Press (www.nap.edu) for research purposes are copyrighted by the National Academy of Sciences. Distribution, posting, or copying is strictly prohibited without written permission of the NAP.

Generated for robsons@univates.br on Tue Aug 19 15:24:09 2003