Quantum Cryptography

Chip Elliott
BBN Technologies

Einstein wrote, "I cannot believe that God plays dice with the cosmos."[1] But quantum mechanics has proved him wrong, and a remarkable crop of new cryptographic systems takes full advantage of those dice that Einstein found so troubling. Though most people think they are science fiction, quantum cryptography systems are now operational, with prototypes protecting Internet traffic across metropolitan areas. These systems are so novel that we can consider quantum cryptography—or, more properly, quantum key distribution (QKD)—as the third and final insight to transform cryptography in the 20th century.

In the 1940s, Claude Shannon provided the information-theoretic basis for secrecy; the amount of uncertainty that can be introduced into an encoded message can't be greater than that of the cryptographic key used to encode it.[2] To achieve perfect secrecy, the key must be at least as long as the message and never reused, that is, we must use Vernam ciphers,[3] also known as "one-time pads." Unfortunately, in practice, it is difficult to distribute completely secret, completely random, one-time pads needed for Vernam ciphers, so they haven't been widely adopted.

In the early 1970s, or possibly earlier, several researchers, including Whitfield Diffie, Martin Hellman, Ralph Merkle, Ron Rivest, Adi Shamir, Leonard Adleman, James Ellis, Clifford Cocks, and Malcolm Williamson, invented cryptographic techniques based on computational complexity. Today, these public-key techniques are ubiquitous; probably the most well known are the Diffie-Hellman key-exchange and RSA prime-factor algorithms. Unlike Shannon, who assumed that adversaries had unlimited mathematical prowess, public-key techniques assume that certain mathematical functions are one way—easy to do in one direction but too difficult for an adversary to undo in a reasonable time. For example, the RSA algorithm assumes that it is simple to multiply two large prime numbers to get their product, but quite hard to factor that product into the two original primes. (However, no one has proved these assumptions.)

Invented by Charles Bennet and Giles Brassard in 1984,[4] QKD begins with a radically different premise: we should base security on known physical laws rather than on mathematical complexities. Physical devices with specialized cryptographic protocols can conjure up ever-flowing streams of random bits whose values will remain unknown to third parties. When we use these bits as key material for Vernam ciphers, we can achieve Shannon's ideal of perfect secrecy—cheaply and easily. In contrast with the unproven foundations of public-key techniques, QKD provides information-theoretic secrecy firmly based on the laws of physics.

How does it work?

QKD lets two parties—for example, Alice and Bob—agree on secret keys. More formally, it's a technique for agreeing on a shared random bit sequence within two distinct devices, with a very low probability that other eavesdroppers will be able to make successful inferences as to those bits' values. We use the random bit sequences as secret keys for encoding and decoding messages between the two devices. Thus, QKD is not, in itself, a full cryptosystem. Rather, we should compare it to other key-distribution techniques, such as trusted couriers, the Diffie-Hellman key exchange, and so on.

QKD can be an intensely confusing field: there are many approaches, the schemes are complex, and it helps to have a working knowledge of quantum optics, which is fundamental to the technology. I recommend Nicholas Gisin's article[5] for a detailed review. However, the basic idea is simple, as Figure 1 illustrates.

Alice sends a series of single photons to Bob, each modulated with a random *basis* (here, a two-sided card) and a random value. Alice chooses a card side at random, writes a random 0 or 1 on that side, and sends the card to Bob. Bob also chooses a side at random and reads that side's value. When Alice and Bob choose the same side, Bob reads exactly what Alice wrote. Otherwise, he reads a 0 or 1 completely at random.

After Bob reads all the photons, he performs a *sifting* transaction with Alice to discard all cases where he read the wrong side (basis). He sends

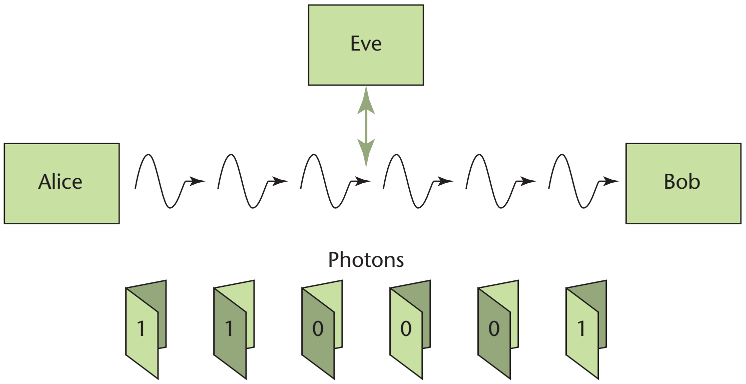

Figure 1. The basic idea of quantum cryptography. Alice sends a series of single photons to Bob, each modulated with a random basis. Bob demodulates them with a random basis. Any noise in Bob's detection is assumed to have been added by an eavesdropper, Eve, who guessed the basis wrong in her eavesdropping. Alice and Bob can use those bits where they randomly selected the same basis, provided that the detection noise is low.

Figure 2. BBN quantum cryptography system (Anna and Boris). A full-featured quantum cryptography system now operating in the world's first quantum cryptographic network, under the streets of Cambridge, Massachusetts.

the random basis settings list that he used to Alice, and she tells him which ones were correct. Then Alice and Bob discard all values where they disagreed on the basis and keep the remaining values for raw key material.

Now, what about an eavesdropper, who we shall call Eve? At first, Eve is in a situation similar to Bob's. She must guess which side of the card to read; half the time she will be able to read what Alice sent, and the other half she'll get a random value. But she can't surreptitiously siphon off a little bit of a single photon because when she reads it, she demolishes it. But if Bob doesn't get that photon, it's no loss; the sifting process will discard that photon and Alice and Bob won't use that bit in their key material.

A clever Eve might try to regenerate a demolished photon and send a copy to Bob but she can't. Quantum physics' no-cloning theorem says that she can't copy values from both sides of the card—only from the side she read. The other side will have a random value. If that's a side that Alice and Bob agree on during sifting, any Eve-generated random values will appear as small noise bursts in the communicated values. Hence, eavesdropping always produces QKD noise, and a cautious Alice and Bob interpret all noise as evidence of active eavesdropping.

In a perfect world, that would end the story. However, in real systems, some channel noise is always present, and a cryptographic system must operate with some noise levels even if they imply eavesdropping activities. To address this, we employ relatively elaborate error-detection and -correction protocols to find and correct bit errors and *privacy amplify* the result so that Eve has a vanishingly small knowledge of the resultant bit values Alice and Bob use. Operating on bits in computer memory, privacy amplification is a classical algorithm that smears out the value of each initial shared bit across the shorter resulting set of bits; that is, it distributes its value via a universal hash across the resulting bits.

Current systems

Bennet and Brassard built the first primitive QKD apparatus in 1992[6] (eight years after their first paper); several systems followed since then, including systems built by Los Alamos, British Telecom, Johns Hopkins University, and IBM Almaden Research Center. Most were component parts, typically only optics. In the past year, two fully-operational systems emerged from Los Alamos and BBN,[7,8] and two companies (ID Quantique, www.idquantique.com and Magiq Technologies, www.magiqtech.com) announced commercial systems but haven't provided public demonstrations.

QKD can work through telecommunications fiber or through the atmosphere. Although these systems differ greatly in their technical details, researchers have demonstrated both approaches. Today's systems generate very high-grade key material at rates approaching 5,000 bits/s at distances of up to 50 km through telecom fiber or 10 to 20 km through atmosphere. While these rates are not fast enough to protect useful traffic with one-time pads, they do allow very rapid rekey-

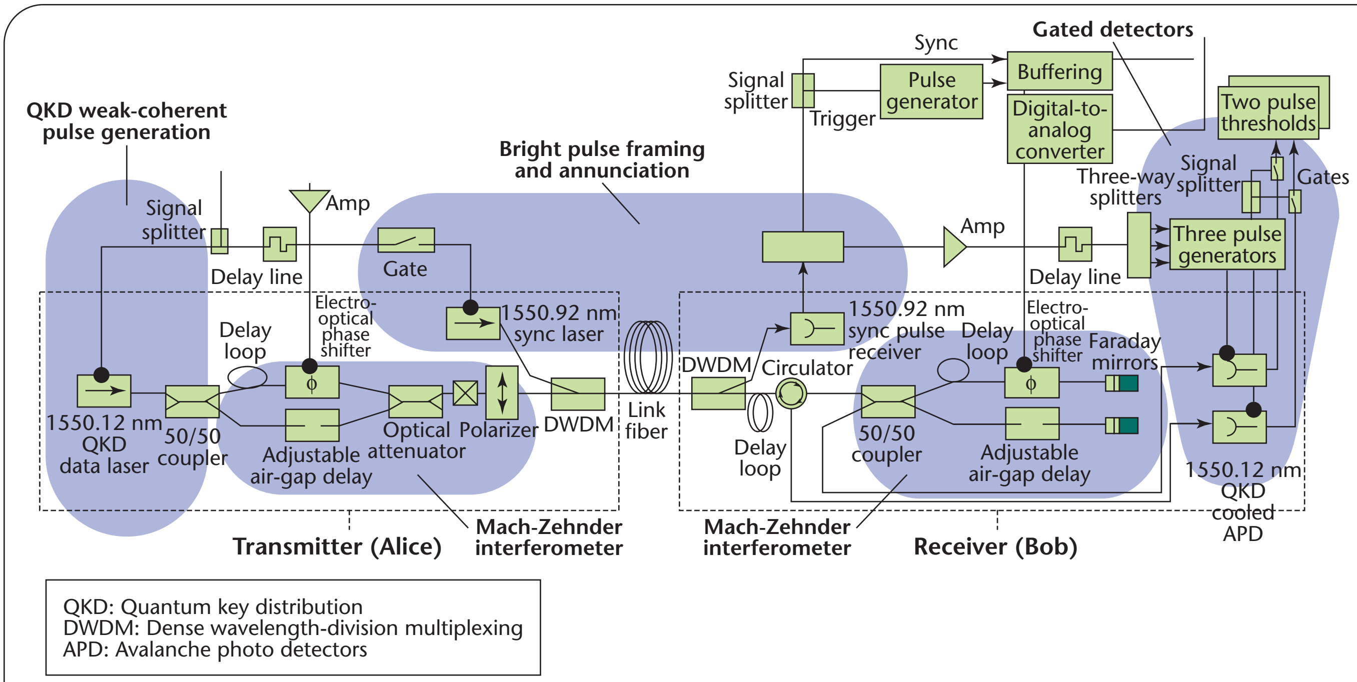

Figure 3. Functional decomposition of BBN quantum cryptography system. Alice produces single photons and phase-modulates them via a Mach-Zehnder interferometer for transmission over standard telecommunication fiber to Bob. Bob demodulates them with an identical interferometer and detects the values that Alice transmitted with his thermo-electrically cooled and electrically gated detectors.

ing of conventional cryptographic algorithms, for example, the Advanced Encryption Standard (AES). Fortunately, there is a relatively clear, though challenging, technology path toward much faster systems. Today's QKD systems are severely limited by the rates at which they can detect single photons; exotic new detectors based on cryogenic superconductors might remove this limit or, perhaps, even more conventional indium–gallium arsenide detectors tailored to the single-photon regime.

As real-world implementation examples, I'll describe Anna and Boris (see Figure 2), two systems BBN Technologies (www.bbn.com) built as part of the DARPA Quantum Network project (http://quantum.bbn.com), which recently began to operate the world's first quantum cryptographic network under the streets of Cambridge, Massachusetts. We now have six QKD nodes running in our laboratory. Four of them became operational in October 2003, replacing our first-generation system, which started continuous operation in December 2002. These systems continuously generate key material, and then use it to protect Internet traffic. (We extended standard Internet Protocol security [IPsec] protocols to support the rapid rekeying of conventional encryption algorithms.)

Each system uses a highly attenuated "single-photon" telecommunications laser operating at a standard wavelength (1550.12 nanometers) with phase modulation via unbalanced Mach-Zehnder interferometers and thermo-electrically cooled avalanche photo detectors (APDs), which are capable of detecting single photons. We implemented most of the electronics using discrete components (such as pulse generators), though we could integrate all necessary electronics onto a small custom printed circuit board.

In May 2004, we deployed Anna at Harvard University and will shortly install Boris at Boston University. Alice and Bob remain at BBN. They are linked by the Cambridge dark fiber network (optical telecommunications fiber without amplifiers or electronics). The longest fiber length (between Boston University and BBN) is about 22 km.

Figure 3 highlights the systems' major features. The transmitter at Alice sends data using 0.1 mean photon number laser pulses. Each pulse passes through a Mach-Zehnder interferometer, which randomly modulates it to one of four phases, encoding a basis and a value in that photon's self interference. The receiver at Bob contains another Mach-Zehnder interferometer, randomly set to one of two phases to select the demodulation basis. The received single photons pass through Bob's interferometer to strike one of the two APDs to present a received value. Alice also transmits bright pulse—typical telecommunications

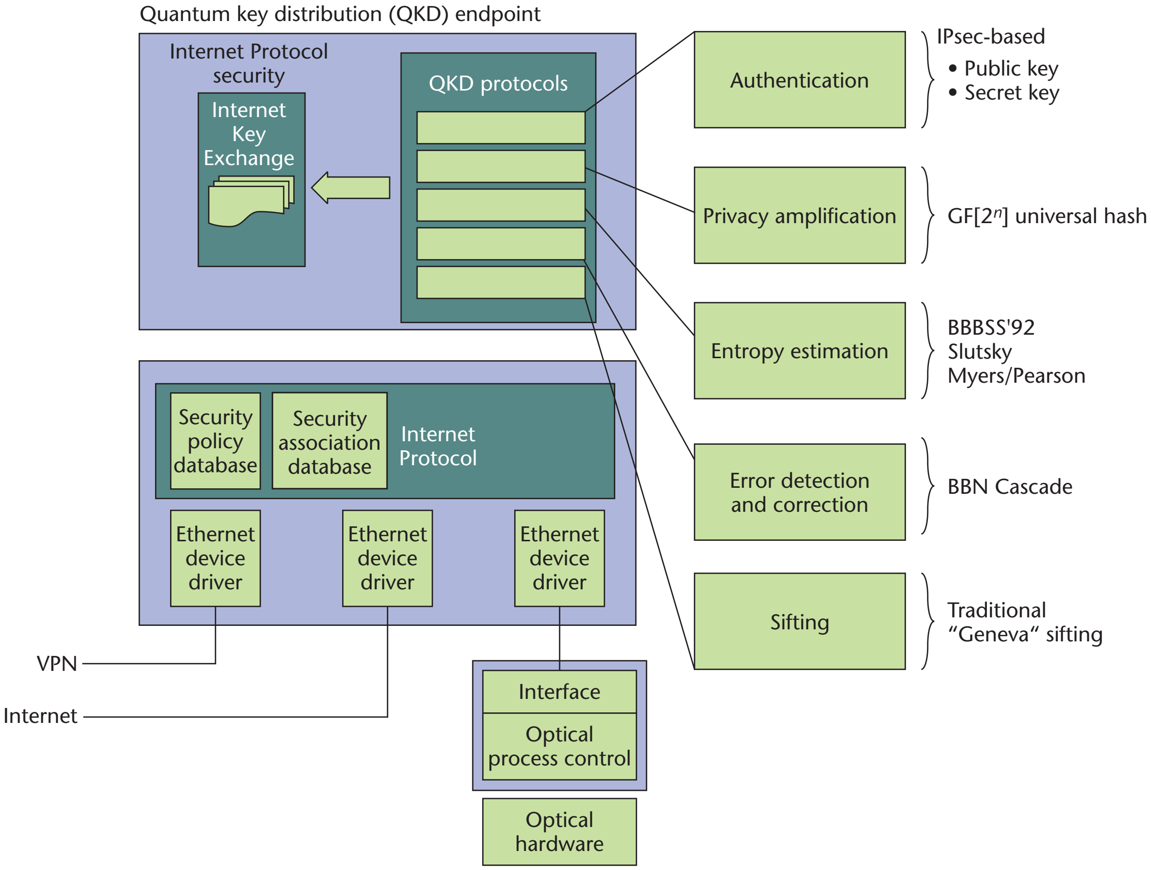

Figure 4. BBN quantum cryptography protocols. Quantum cryptography protocols form a "stack," somewhat like conventional communications protocols. There are many possible variants for the different stack layers. BBN has implemented a full suite of quantum cryptography protocols, including the variants shown here.

power level—multiplexed over the same fiber, to send timing and framing information to Bob.

QKD protocols

Although a detailed discussion of QKD protocols is beyond this article's scope, QKD systems contain a surprising amount of sophisticated software. While developing our systems, we observed that QKD optics is perhaps the easiest part; the electronics are more difficult than the optics; and, for a practical functional system, the software is harder than the electronics.

Figure 4 illustrates how QKD protocols might integrate into a Unix operating system to provide key material to its indigenous Internet Key Exchange (IKE) daemon for use in cryptographically protecting Internet traffic via standard IPsec protocols and algorithms. BBN's QKD protocol stack is written in C for portability to embedded real-time systems. David Pearson, Gregory Troxel (both at BBN Technologies) and I present a more detailed discussion of this implementation and how QKD interacts with IKE and IPsec elsewhere.[8]

As I previously mentioned, once Alice and Bob agree on sifted bits, they must perform error correction to find and eliminate any bits damaged (or compromised by Eve) in transmission, for example, bits sent as a 1s but received as 0s. There are many ways to perform error correction but each has two important consequences:

- Error correction is always probabilistic unless all bits are revealed during the process, and thus there is a small possibility that Alice and Bob believe that they share identical bit sets, but, in fact, they do not.
- Error correction requires communications between Alice and Bob, and inevitably—assuming that Eve can obtain plain-text versions of all such public communications—the process of error correction reveals sifted-bit information to Eve.

Thus, the error correction's end results are that Alice and Bob will—with high probability—have in their local memories identical copies of a set of error-corrected bits and Eve will have some knowledge of these bits' values, which Alice and Bob must reduce through privacy amplification.

Privacy amplification lets Alice and Bob reduce Eve's knowledge of their error-corrected bit values to an arbitrarily low fraction of the total number of bits. At its core, it occurs via randomized algorithms in Alice and Bob and public communication between them regarding the results of these algorithms.

Finally, authentication gives Alice and Bob reasonable assurance that they are communicating with each other. In most modern cryptographic systems, this function occurs via some kind of one-way function, for example, digital signatures implemented by public-key techniques. In classic QKD literature, authentication relies on shared secret keys, such as in universal hash functions.

QKD networks

The DARPA Quantum Network consists of two transmitters, Alice and Anna, and two compatible receivers, Bob and Boris, with quantum channels directly interconnected using fiber via a 2 × 2 optical switch. Either transmitter can negotiate a mutual key with either receiver. The switch is optically passive; that is, it does not detect or amplify any photons passing through it, so it doesn't disturb the quantum state of the photons that encode key bits.

When two QKD endpoints don't share a direct or switched channel but there is a path between them over channels through trusted relays, our networking protocols let them agree on a shared key by choosing a path through the network, creating a new random number *R*, and, essentially, sending an *R* one-time-pad encrypted across each link. We call this process *key relay*, and the resulting network a *trusted network* because this scheme's chief characteristic is that the key's secrecy depends on the endpoints and intermediate nodes being trustworthy.

The BBN key relay protocols have been operating continuously in the DARPA Quantum Network since October 2003. Even though Alice and Anna are transmitters, the protocols let Alice build up a reservoir of shared key material with Anna via a trusted relay at Bob or Boris. Similarly, Bob and Boris continuously build up shared key material via trusted relays at Alice or Anna.

What's next? QKD's next generation will be even stranger than today's because it will draw key material from pairs of entangled photons. In some ways, this is the most satisfying of all forms of QKD because it directly exploits the universe's underlying randomness and strangeness. Such cryptographic systems create, and derive their keys from, highly unusual "Siamese twin," or entangled, photons:

> The entangled state contains no information on the individual particles; it only indicates that two particles will be in opposite states. The important property of an entangled pair is that as soon as a measurement on one particles projects it, say, onto [a horizontal polarization], the state of the other one is determined to be [vertical], and vice versa. How could a measurement on one of the particles instantaneously influence the state of the other particle, which can be arbitrarily far away? Einstein, among many other distinguished physicists, could simply not accept this "spooky action at a distance." But this property of entangled states has been demonstrated by numerous experiments.[9]—Dik Bouwmeester

One of these systems is taking shape in BBN's Cambridge laboratory. Other teams, such as those at Bristol and Vienna universities, are proposing even wilder, space-based systems with entangled photon pairs transmitting between Earth and orbiting satellites. It is remarkable that Einstein's "spooky action at a distance" consideration provides the engineering core for the next generation of cryptographic systems! □

References

1. A. Einstein, "Sayings of the Week," *London Observer*, 5 Apr. 1964.
2. C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical J.*, vol. 28, no. 4, 1949, pp. 656–715.
3. G.S. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," *J. Am. Inst. Electrical Eng.*, vol. 45, 1926, pp. 109–115.
4. C.H. Bennet and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proc. Int'l Conf. Computers, Systems & Signal Processing*, CS Press, 1984, pp. 175–179.
5. N. Gisin et al., "Quantum Cryptography," *Rev. Modern Physics*, vol. 74, no. 1, 2002, pp. 145–195.
6. C.H. Bennett et al., "Experimental Quantum Cryptography," *J. Cryptology*, vol. 5, no. 1, 1992, pp. 3–28.
7. R.J. Hughes et al., "Practical Free-Space Quantum Key Distribution Over 10 km in Daylight and at Night," *New J. Physics*, vol. 4, 2002, pp. 43.1–43.14.
8. C. Elliott, D. Pearson, and G. Troxel, "Quantum Cryptography in Practice," *Proc. ACM SIGCOMM 2003*, ACM Press, 2003, pp. 227–238.
9. D. Bouwmeester et al., "Experimental Quantum Teleportation," *Nature*, vol. 390, 1997, pp. 577–579.

***Chip Elliott** is principal engineer for BBN Technologies. His research interests include quantum cryptography and mobile ad hoc networking. He has a BA in mathematics from Dartmouth College. He is a senior member of the IEEE, a member of the American Association for the Advancement of Science, the ACM, and the American Institute of Aeronautics and Astronautics, and has been nominated for a World Technology Award for his work in quantum cryptography. Contact him at celliott@bbn.com.*