BY BILL SCHWEBER • FORMER EXECUTIVE EDITOR

QUANTUM CRYPTOGRAPHY:

WHEN YOUR LINK HAS TO BE REALLY, REALLY SECURE

COMBINING QUANTUM THEORY AND SINGLE PHOTONS, SYSTEMS CAN ACHIEVE SECURITY THAT THE LAWS OF PHYSICS— RATHER THAN AN ALGORITHM'S COMPLEXITY—ASSURE.

Keeping data and communications secure is a hot topic. Hackers access systems through open ports, through secret programs, and through various ruses or aliases. As a result, data-security products and strategies are top priorities for both embedded and enterprise systems.

Another long-recognized weakness in any system is the physical link that connects users or system nodes. Although several ways, such as a private channel or a physically secured link, exist to minimize this risk, it is more common to use data encoded using a complex, mathematics-based approach, such as the RSA (Rivest/Shamir/Adleman) algorithm or a one-time key. Physically securing the link is often impractical and rules out wireless links; data encoding is susceptible to decoding by a determined eavesdropper. (Even the RSA algorithm may face this challenge as computers get more powerful.) And the one-time key, although absolutely secure in principle, has severe implementation problems in practice (see **sidebar** "Encryption basics" at the Web version of this article at www.edn.com/051216df1).

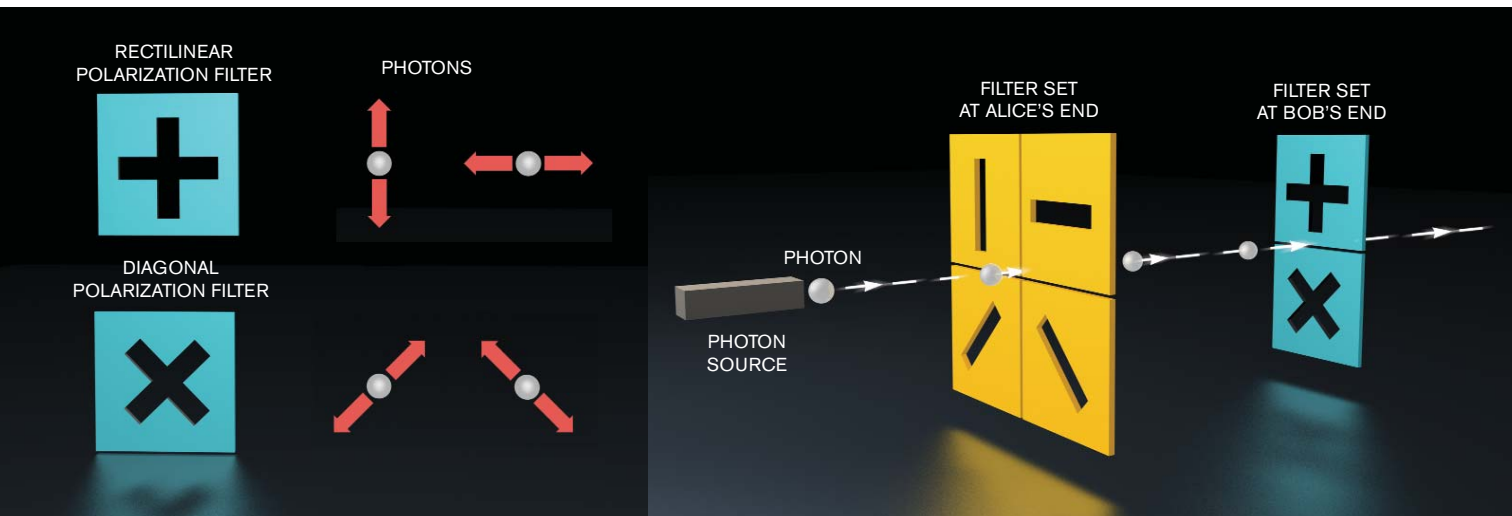But a technique now in use appears to offer

Figure 1 BBN and DARPA based the QC system on the random polarization of photons, followed by selective polarization filtering and polarization-direction detection.

the security of the one-time key without its key-management problems, and you can also use it for absolutely secure key exchange. QC (quantum cryptography) uses a string of individual photons and their quantum states as the bases of a link in which physicist Werner Heisenberg's often-cited, often-misunderstood uncertainty principle defeats any eavesdropper (**Reference 1**). Although IBM corporate researcher Charles Bennett and the University of Montreal's Giles Brassard first conceived quantum cryptography in the 1980s, it took many years for the needed optical components and associated technologies with the required performance to become available.

A fully operational QC system has been running in the Boston area since June 2004 over a 12-mile loop and with 10 nodes. BBN Technologies (www.bbn.com) developed the system with the cooperation of other labs and companies under a 2002 DARPA (Defense Advanced Research Projects Agency) grant. BBN, an R&D facility, aims to license the technology to others for commercialization. Although the system is not in regular commercial deployment, it is more than an academic proposal or lab curiosity: It runs 24 hours a day, seven days a week; is fully operational; and requires virtually no intervention to keep it going.

The QC system also includes an Internet gateway, so that its users can reach out and link beyond the QC-encrypted nodes, although they lose the QC once they cross the gateway. BBN has a long history of research and development in communications and networks; in the late 1960s,

the company—then better known as Bolt Beranek and Newman—led development of and launched the ARPAnet (Advanced Research Projects Agency network), the underlying structure of the Internet. BBN has the perspective of a telecom and networking organization, not an experimental-physics lab; it seeks to develop systems with near-100% uptime rather than "prima donna" operations that require constant care, attention, and restarts.

Vendors such as id Quantique (www.idquantique.com), MagiQ Technologies (www.magiqtech.com), and QinetiQ Ltd (www.qinetiq.com), offer commercially available QC products and subsystems.

QUANTUM IDEAS: NOT INTUITIVE

Before discussing how a QC system works, it's a good idea to review the quantum principles and orient yourself with some "out-of-the-box" thinking, compared with conventional signals, power, and observations (see **sidebar** "Think differently"). A QC system starts with a source of single photons and a pair of polarizing filters (**Figure 1**). (How you generate these photons is not trivial. One polarizing filter—the rectilinear filter—allows only photons having vertical or horizontal polarization to pass. The other filter—the diagonal-polarizing filter—allows only photons with polarization that is oriented at ±45° to the horizontal or vertical to pass. The frame of reference is arbitrary; just define one direction as the horizontal and use it as the baseline orientation for subsequent angles.)

For each photon that the source generates, the sender, which the relevant literature typically calls Alice, randomly passes it through either the rectilinear or the diagonal filter. If she uses the rectilinear filter, Alice records whether the photon that passes has horizontal or vertical polarization; if she uses the diagonal filter, she records whether the photon's polarization is tilted right 45° or left −45°. The photon, representing a bit of data, then travels through an optical fiber or free space.

At the receiving end, the receiver, which the relevant literature typically calls Bob, makes a random choice of whether to observe the incoming photon with a rectilinear or a diagonal filter, and he notes the filter he uses and the polarization value he sees—horizontal or ver-
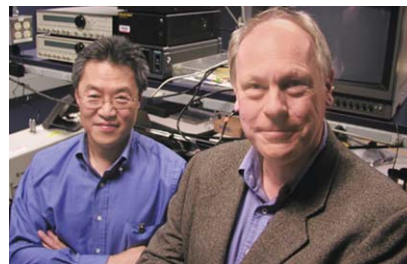

Figure 2 Henry Yeh (left) and Chip Elliott of BBN Technologies have led the DARPA-funded quantum-cryptography project.

tical, 45° or −45°. This number is his bit value. He repeats this procedure for all incoming photons. Bob then contacts Alice over an open, nonsecure channel and tells her the sequence of filters he used. He does not tell her the bit values, or "qubits," he recorded using this sequence.

Alice responds to Bob, again over an open channel, and tells him which of the filter orientations he used were correct. She doesn't comment on the bit values, because he has not given them to her. Alice and Bob use the instances in which the modes were correct as the key to encrypting and decrypting messages and ignore the positions in which the photons were not seen in the right mode.

What about the ever-hovering potential eavesdropper, which the relevant literature typically refers to as Eve? Due to the Heisenberg principle, she can't simultaneously measure the photons in both the rectilinear and the diagonal modes. Further, if Eve guesses, makes the measurements in the wrong mode, and resends the bits to Bob the way she measured them, she will introduce errors. Both Alice and Bob will detect the eavesdropper just by comparing selected bits and doing some error checking on their bit pairings.

The QC technique meets the needs of a secure link. You can use it either for sending a secure key from Alice to Bob or for creating and sending a one-time key along with the message bits. But it has limitations. First, it works over the distance of only a single, uninterrupted link, because any all-optical or electro-optical repeater or amplifier for the photons destroys their quantum states; no currently available opti-

cal-repeater design also preserves those states. A QC link employing the standard, low-loss fiber used for telecom can reach through about 100 km of fiber, and the free-space link with a carefully focused telescope at the receiver end achieves 20 km at night. (Daytime use is difficult due to the brightness of the sun.) Researchers believe that a link from a low-orbit satellite to a ground station is possible with suitable optical components, however.

Second, the data rate is relatively low, due to limitations of some of the optical components and the protocol complexity. When you use QC for sending a secure key, the link achieves rates of about 5 Mbps; when you use it for a one-time key, the system sends key material at 700 bps.

ONE PHOTON TO GO, PLEASE

Implementing a working QC system requires many functional blocks and pieces of equipment. Many are standard items; a few are not. Chip Elliott, principal engineer at BBN, and Henry Yeh, program manager, along with others did much of the work (**Figure 2**).

The system currently has nodes at BBN, Harvard University, and Boston University's Photonics Center, over a 12-mile loop of unused, commercial, dark optical fiber that is already in place. BBN, along with engineers at the NIST (National Institute of Standards and Technology, www.nist.gov), also developed a

free-space link from BBN to an adjacent building (**Figure 3**). The system is not just a simple point-to-point, single-protocol topology; it has electro-optical repeaters at each node to capture, recover, re-encrypt, and retransmit the data using QC, and it uses different data protocols.

A single-photon source and the corresponding single-photon detector are critical to a QC system. BBN's system has two methods of generating the single photons: One technique uses a laser and filters its output, and the other is an entangled-photon approach. In the first method, a filter drastically attenuates the output of a laser, or a phase-modulation path acts as the filter and separates the photons. This filtered-laser approach is the simpler of the two methods, in principle, but it is hard to precisely filter down to one photon. The attenuated, filtered output may comprise one, two, or even three photons, because, in the quantum world, the counting of photons implies an exactness that their probabilistic description cannot accept.

In the entangled-photon approach, a laser pump directs a stream of photons at a nonlinear crystal (**Figure 4**, **Reference 2**). The incoming photons stimulate the crystal, which then generates and ejects twin photons in opposite directions but having the same quantum states. The approach also involves some optical filtering and special mirror paths. The
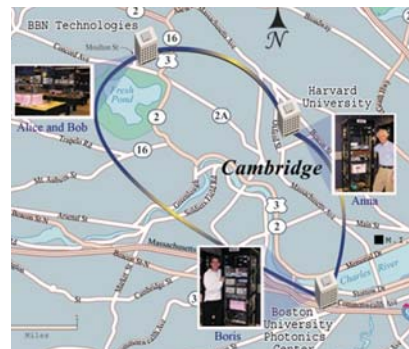

Figure 3 The QC system has two sites in Cambridge, MA—BBN (home to users "Alice" and "Bob") and Harvard University ("Anna")—and a site in Boston at Boston University ("Boris").

virtue of this system, which BBN also uses, is that, by observing one of the photons, you learn what you need to know about its twin. BBN's Elliott punches the point home with a comment that is familiar to quantum-physics researchers but not to conventional RF and telecom engineers. "You want to be pretty careful when you look at something; it is a conclusive action," he says.

SOURCING IS EASIER

Generating single photons may seem complicated, but it's the lesser of the complementary challenges. "Single-photon detectors are the real nightmares," notes Elliott, and they are currently the limiting factors in system implementation. The well-established silicon-based detector is adequate for visible photon wavelengths of the free-space link, even though you must cool them to −40°C to reduce random noise.

For fiber-based QC links, the BBN system uses an InGaAs/InP (indium-gallium-arsenide/indium-phosphide) photodetector cooled to −50°C. Unfortunately, this detector has low quantum efficiency, converting only 10 to 20% of the photons that hit it into an electrical pulse. To improve performance, Elliott says, the team is building a superconducting detector using niobium nitride, operating at 2 to 4°K. In this type of detector, an incoming photon momentarily kicks the crystal out of its superconducting mode, and the crystal produces a current glitch as a result. These detectors have the potential to run at 10 to 100 GHz, compared with a few megahertz for InGaAs/InP, thus removing one bottle-
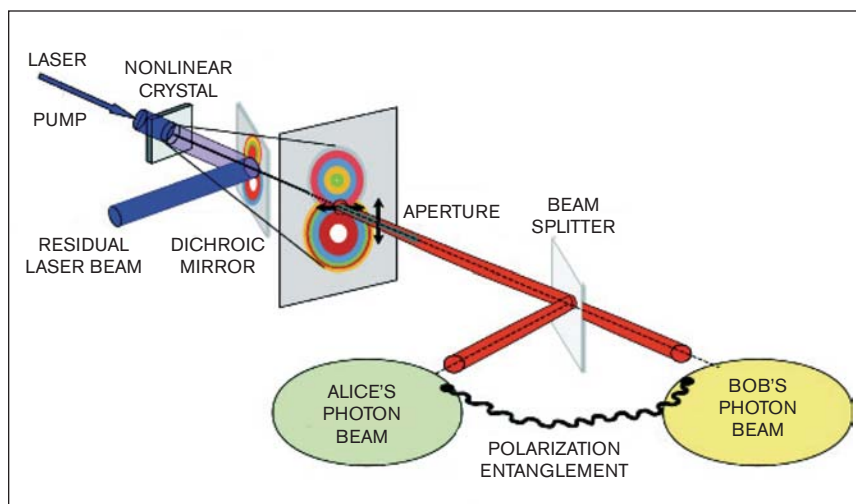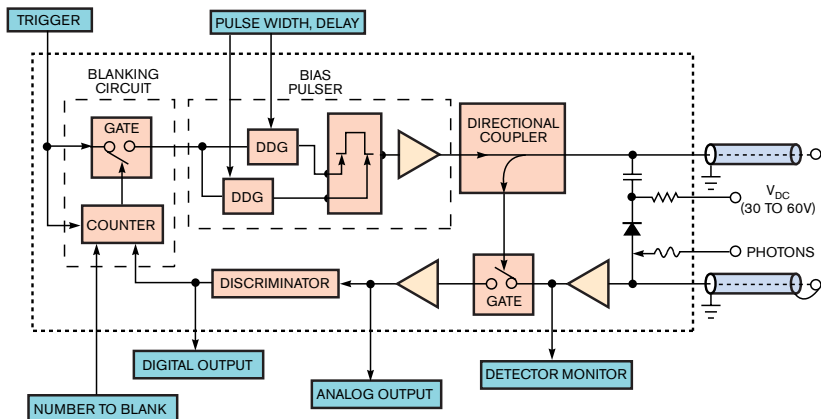

Figure 4 To generate a single photon with known quantum states, a laser's output stimulates a nonlinear crystal, which, in turn, generates twin photons with the same quantum states.

(a)

Figure 5 The custom-built, single-photon detector unit, which IBM Almaden built, has an optical-detector front end (a) and a considerable amount of support electronics (b).

(b)

neck to overall system throughput. Cooling the detector material to a few degrees Kelvin is not a problem because, Elliott notes, "It's amazing; you can get a pretty good chiller for $20,000."

A photon-detecting crystal is critical, but it is not the entire front end. The complete single-photon detector is a rackmount chassis with additional electronics (**Figure 5**); the DARPA Quantum Network built a dozen of these beautiful, handcrafted units at the IBM Almaden Research Center (San Jose, CA), and BBN has six of them. In October, IBM licensed this technology to Princeton Lightwave (www.princetonlightwave.com), to further commercialize QC.

Another pair of key elements of the fiber-based QC link is a set of interferometers—one at the BBN site and one at Harvard—to adjust and match optical-path phases. Their optical lengths must match to less than a fraction of a wavelength, which is a tight requirement. In the current design, a carefully controlled standard power supply applies subtle voltage changes across the lithium-niobate phase modulator that is part of the interferometer, and the piezoelectric effect produces a small but sufficient change in
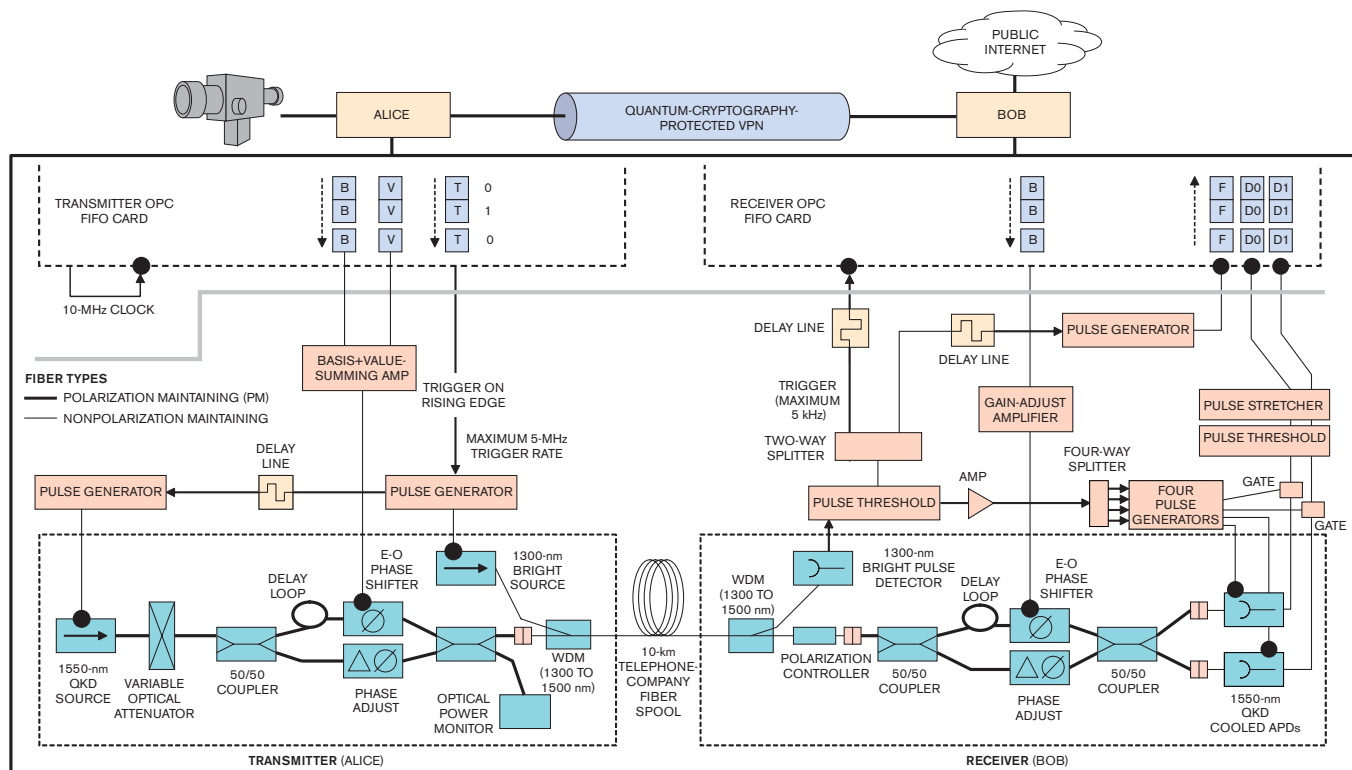

Figure 6 The complete link between Alice and Bob includes all-optical, electronic, and electro-optical elements, including sources, delay lines, phase shifters, couplers, splitters, and optical fibers. The optical fibers include both polarization-maintaining and -nonmaintaining fiber.

THINK DIFFERENTLY

For engineers used to thinking of signal power, decibels of attenuation, and meter-based measurement, the quantum world of photons can be a different place. When an optical engineer speaks about attenuating the signal energy or power, the process is not at all like it is for the case of conventional voltage and current signals. The only way to attenuate a photon stream's energy or power is to reduce the *number* of photons, because the energy of a photon is a function only of its wavelength or frequency.

Several quantum states, including polarization and characteristics, define each photon. The basic act of measuring a photon's quantum states may change the values of those parameters, following Werner Heisenberg's uncertainty principle, which states that you cannot simultaneously determine both the positions and the quantum states of particles such as photons. In short, the act of measurement affects the particle you are measuring. In the quantum-physics world, you are not dealing with certainties and absolutes; you are working with probabilities of where the photons are and what parameters they have. This situation contrasts with the well-defined and measurable world that engineers normally associate with their circuits and systems.

the crystal dimension. (A previous version used an independent piezoactuator, but the newer approach is simpler.) An absolutely light-tight box built of 3-in.-thick Styrofoam that you can purchase from Home Depot encloses the entire interferometer; it is the only part of the complete QC link insulated to minimize thermal effects (**Figure 6**).

The single-photon source and corresponding detector are custom-made, as is the interferometer and its box. Most of the remaining extensive setup is standard electronic or optical test, measurement, or processing equipment. As Elliott notes, "The rest is telecom equipment—fast and cheap." He adds, "Most of the equipment is off-the-shelf; you could just about get out your credit card and do it yourself in your basement." This statement is an exaggeration, because the design and implementation contain a tremendous amount of IP (intellectual property), but it does give a sense of how extensively the overall QC system takes advantage of moderate-cost, high-performance electronic- and optical-communication modules and units.

Despite the overall complexity of the system, it runs on its own with autocalibration, start-up mode, and self-test mode, and it supports continuous data throughput. From a power-up cold start, the entire QC link is ready to use in only about 30 seconds (not including the time for the various PCs used as controllers to boot up their operating systems and drivers), and aligning the interferometers takes up most of this time. The next step, says Elliott, is to put as many of the control functions as possible into FPGAs and reduce the use of PCs, which would make the systems smaller, cheaper, and more hardware-based.**EDN**

REFERENCES
1 Stix, Gary, "Best-kept secrets: Quantum cryptography has marched from theory to laboratory to real products," *Scientific American*, January 2005, www.sciam.com.
2 Schweber, Bill, "Going nonlinear can be a good thing," *EDN*, Sept 18, 2003, pg 36, www.edn.com/article/CA321808.

> **MORE** ❯ **AT EDN.COM** ▷
>
> ⊞ **Go to www.edn.com/051216df1 and click on Feedback Loop to post a comment on this article.**

Bill Schweber was Executive Editor of *EDN* until October 2005. We wish him well in his new endeavors.