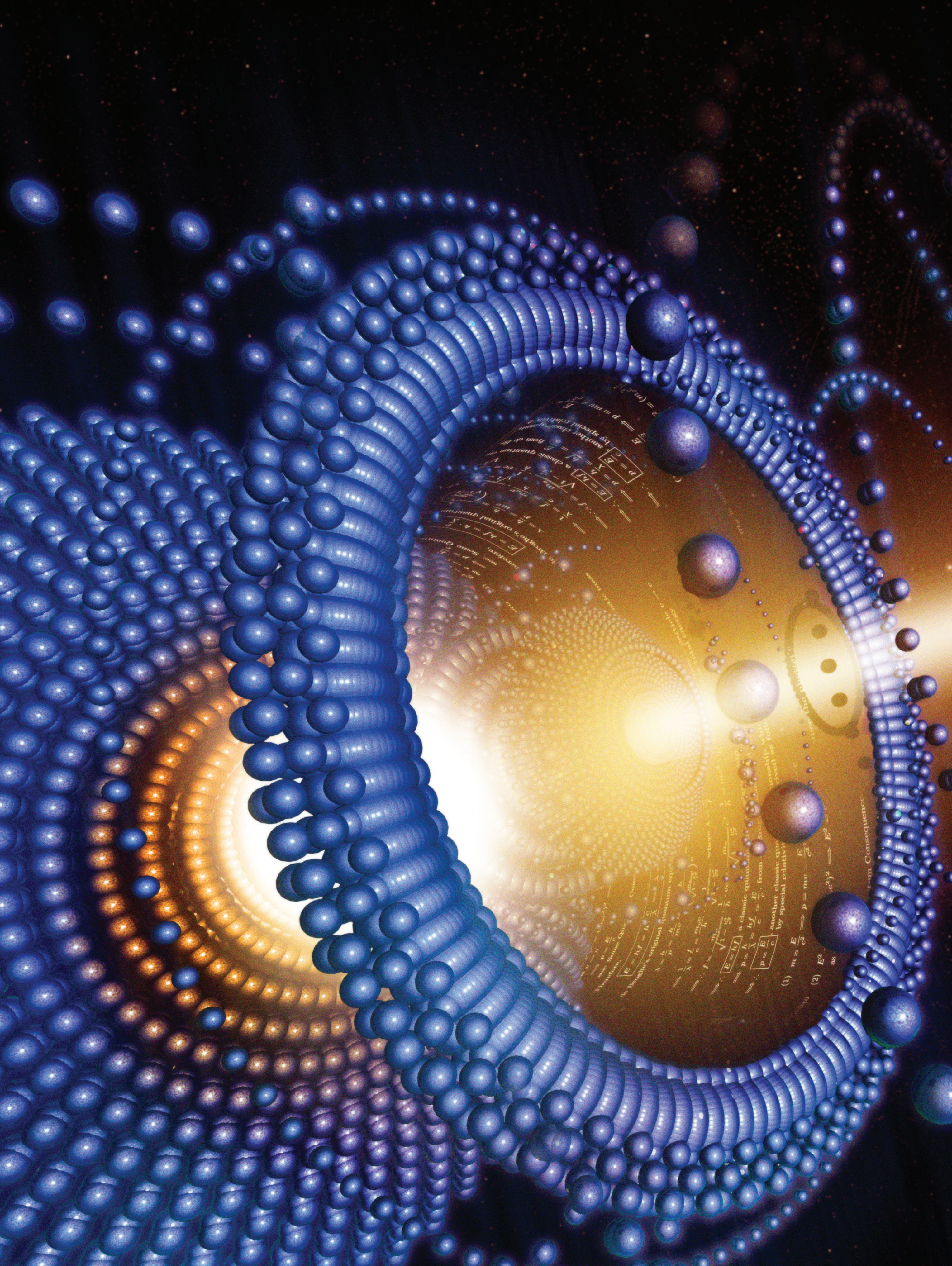
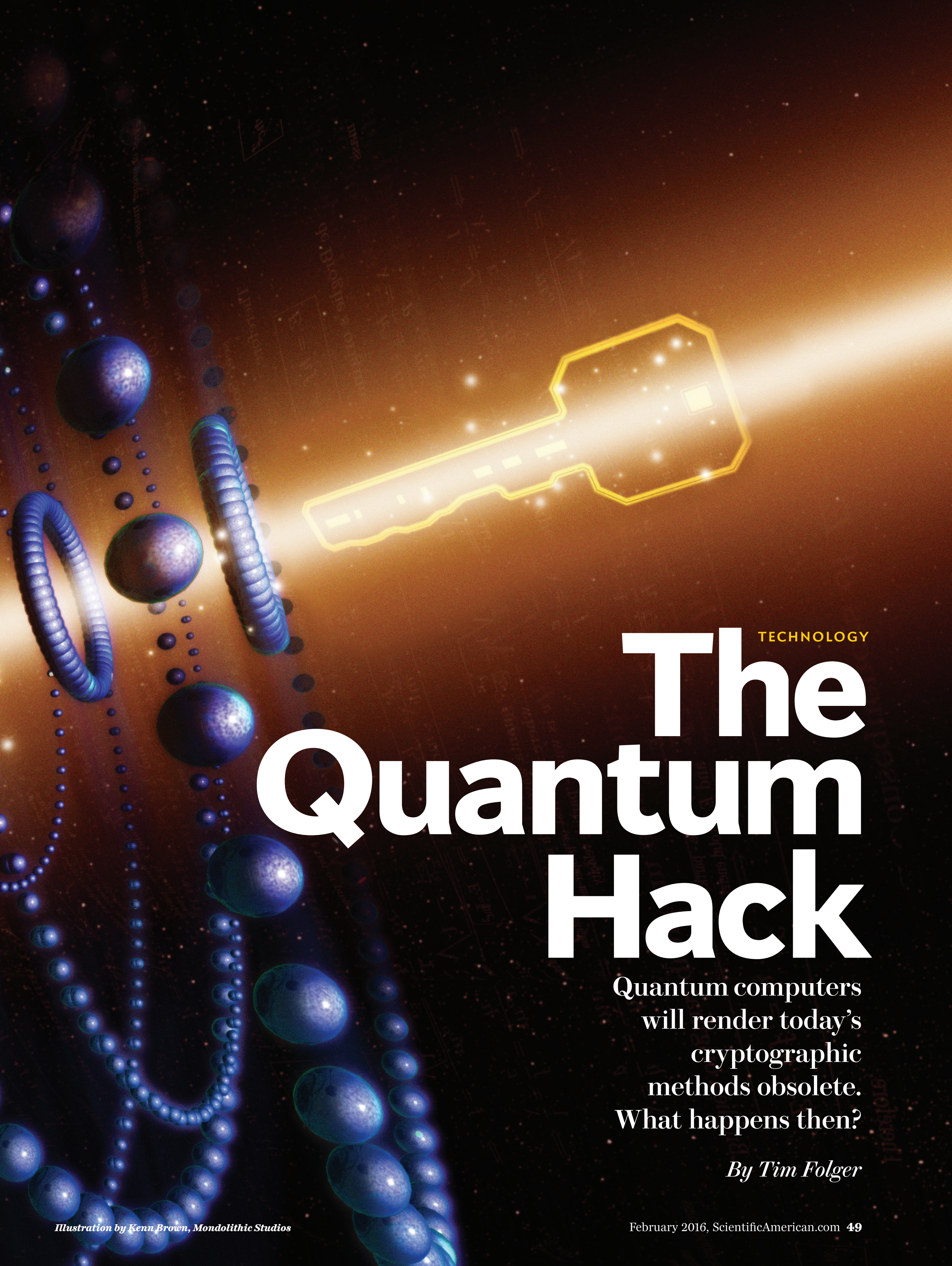




TECHNOLOGY

The Quantum Hack

Quantum computers will render today's cryptographic methods obsolete. What happens then?

By Tim Folger

Illustration by Kenn Brown, Mondolithic Studios

Tim Folger writes for *National Geographic, Discover* and other national publications. He is also the series editor for *The Best American Science and Nature Writing*, an annual anthology published by Houghton Mifflin Harcourt.

ONE BRIGHT OCTOBER AFTERNOON ON A BEACH IN SAN JUAN, PUERTO RICO, two scientists found the solution to a problem that didn't yet exist. It was 1979. Gilles Brassard, then a newly graduated Ph.D. from Cornell University, was immersed in the warm Caribbean water when someone swam toward him. The dark-haired stranger launched into a pitch about how to make a currency that could not be counterfeited. The scheme, invented several years earlier by a Columbia University graduate student named Stephen Wiesner, involved embedding photons—particles of light—in banknotes. By the laws of quantum mechanics, any attempt to measure or copy the photons would instantaneously change their properties. Each bill would have its own string of photons, a quantum serial number that could never be duplicated.

"I was surprised, of course," says Brassard, now a professor of information science at the University of Montreal, "but I listened politely." The conversation, he says, turned out to be a life-changing experience. His new acquaintance was Charles Bennett, a research physicist at IBM. Bennett had recognized Brassard from a conference they were attending. Although they were both intrigued by the quantum-banknote idea, they knew it was technically infeasible. Even today no one knows how to capture, immobilize and store photons in a piece of paper. Light particles, after all, tend to move rather quickly.

"We're better now but still nowhere close to anything that would be remotely practical for quantum banknotes," Brassard says. "But it was a starting point as a thought experiment. It's a beautiful example of an idea that is completely ridiculous in terms of being practical but at the same time turns out to be totally seminal. Because it was from there that Bennett and I had the idea for what is now known as quantum-key distribution."

Quantum-key distribution, or QKD, is a technique to encode and transmit data using photons. In principle, it provides a completely unbreakable form of cryptography. After that day on the beach, Bennett and Brassard began a five-year collaboration that produced the first cryptographic method in history to rely not on mathematical complexity but on the laws of physics. When Bennett and Brassard finally published their work in 1984, few researchers took the idea seriously or even noticed it. "It was considered a fringe pursuit," Brassard says. "And that was for those who paid any attention. I don't think we took ourselves very seriously either."

That is no longer the case. Thirty years ago hardly anyone outside of government intelligence agencies used cryptographic technology. Now it has become essential to routine transactions on the Internet. Whenever someone enters a password or credit-card number online, sophisticated programs built into all Web browsers work behind the scenes to keep that information safe from cyberthieves. "This is a technology that everyone needs but that no one is aware of," says Vadim Makarov, a researcher at the Institute for Quantum Computing at the University of Waterloo in Ontario. "It just works."

But it might not work for much longer. Nearly every encryption scheme now in use is likely to become obsolete with the advent of quantum computers—machines capable of cracking the elaborate codes that protect everything from Amazon purchases to power grids. Although no one has yet built a full-blown quantum computer, researchers in academic, corporate and government laboratories around the world are trying. Among the documents released by whistle-blower Edward Snowden was a description of a secret National Security Agency project called

IN BRIEF

Conventional computers have been ill equipped to crack the encryption schemes, often based on large prime numbers, at the core of everyday online commerce and communication.

Quantum computers, however, could break today's encryption schemes by exploiting the strange rules of the subatomic world and trying all solutions to a code simultaneously.

No one has built a full-scale quantum computer, but academic, government and private researchers are trying, and some experts say they could succeed in as little as 10 years.

That is why researchers are racing to perfect and deploy technology for quantum encryption, which uses quantum uncertainty to create nearly unbreakable codes.

Penetrating Hard Targets—a $79.7-million effort to build a quantum computer. "It's hard to say with any confidence that one won't exist in 10 or 15 years," says Ray Newell, a physicist at Los Alamos National Laboratory.

If or when that first quantum computer boots up, the most effective counter to its code-breaking powers may turn out to be another kind of quantum wizardry: cryptographic networking technology based on the theory Bennett and Brassard devised 32 years ago. Quantum encryption—a method of encoding transmissions that exploits the strange properties of single particles of light—has, it turns out, been an easier problem than building a quantum computer. Indeed, some small quantum-encryption projects are already up and running. There is just one problem: replacing the world's encryption systems with quantum versions will probably take longer than developing quantum computers. "If you think this problem might exist in 10 to 15 years, we need to be doing this *yesterday,*" Newell says. "We're probably already too late."

VERY BIG NUMBERS

HIDDEN BEHIND THE EFFORTLESS mouse clicks and screen taps of Web commerce stands an elegant and complex mathematical scaffolding of two distinct forms of cryptography: symmetric encryption, in which the same secret key is used to encrypt and decrypt data, and asymmetric encryption, in which one key encodes the message and a different key deciphers it. Every exchange of secure information on the Internet requires both methods.

A typical session between someone's home computer and an online retailer's Web server starts with the creation of a symmetric key that the customer and merchant will share over the Internet to encode credit-card numbers and other private information. A key is essentially a set of instructions for how to encode information. A ridiculously simple key might specify that every digit in a credit-card number be multiplied by three. In the real world, of course, keys are far more complex mathematically. Whenever someone purchases something on the Internet, the Web browser on the home computer exchanges a key with the server of the online retailer. But how is the key itself kept private during that initial exchange? A second layer of security—an asymmetric one—encrypts the symmetric key.

Invented independently in the 1970s by the British secret service and academic researchers, asymmetric encryption uses two different keys: a public key and a private key. Both are necessary for any encrypted transaction. During an online purchase, a merchant's server sends its public key to a customer's computer. The customer's computer then uses the merchant's public key—which is openly available to all customers—to encrypt a shared symmetric key. After receiving the encrypted symmetric key from a customer, the merchant's server decrypts it with a private key, which no one else possesses. Once the symmetric key is safely shared, it encrypts the rest of the transaction.

The public and private keys used in asymmetric encryption are derived from the factors of very large numbers—specifically, prime numbers, integers divisible only by 1 and themselves. The public key consists of a number generated by multiplying two

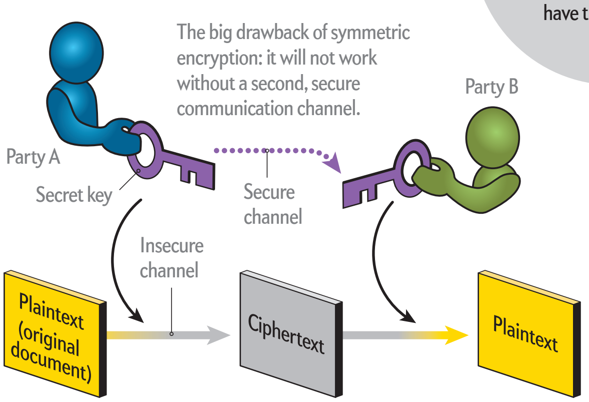
TODAY

How Encryption Works—for Now

Every time you buy something online, your browser and the seller's Web site exchange a secret code—a key for encrypting the information they are about to exchange. Because both parties use the same key, this process is known as symmetric encryption. To securely share that key, however, both parties rely on a second form of encryption—asymmetric encryption. This two-step system works well, but if working quantum computers arrive, it could become instantly obsolete.

Symmetric Encryption

Faced with an insecure communication channel, Party A encodes a message before sending it to Party B over an insecure channel. If someone intercepts the message, no problem: the encoded message will be gibberish. Party B, however, *can* read the message because Party A has sent Party B a secret key through a secure back channel.

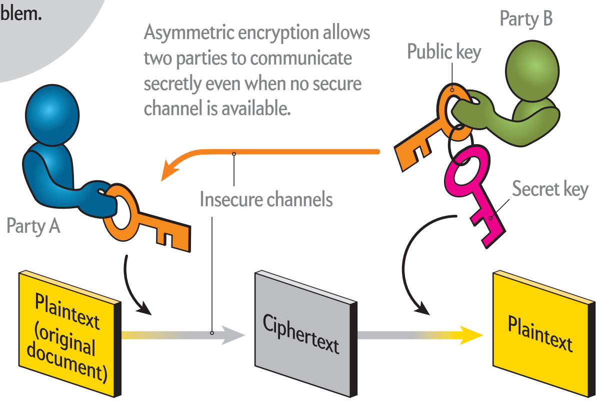

The big drawback of symmetric encryption: it will not work without a second, secure communication channel.

Vulnerabilities

Asymmetric encryption works because it is extremely difficult for classical computers to factor very large numbers. Quantum computers do not have this problem.

Asymmetric Encryption

Party B—the recipient—selects a pair of keys: one that explains how to encode a message and one that explains how to decode it. Party B publishes instructions for encoding messages. This is the "public" key. Party A encodes her messages according to the public key. When Party B gets the encoded message, she decodes it using the second, secret key.


Asymmetric encryption allows two parties to communicate secretly even when no secure channel is available.

Illustrations by Jen Christiansen

large prime numbers together; the private key comprises the two prime factors that create the public key. Even children can multiply two primes, but the reverse operation—splitting a large number into two primes—taxes even the most powerful computers. The numbers used in asymmetric encryption are typically hundreds of digits long. Finding the prime factors of such a large number is like trying to unmix the colors in a can of paint, Newell says: "Mixing paint is trivial. Separating paint isn't."

The most widely used asymmetric encryption method is known as RSA, after its creators: Ron Rivest, Adi Shamir and Leonard Adleman, who developed the idea in the late 1970s at the Massachusetts Institute of Technology. Key lengths have been increasing steadily to keep them safe from hackers with faster computers and better skills; longer keys require more computing power to break. Asymmetric keys now are typically 1,024 bits long, but even leaving aside the prospect of quantum computers, that might not be enough to foil future cyberattacks. "The National Institute of Standards and Technology is actively recommending that RSA key sizes be upgraded to 2,048 bits," says Richard Hughes, a physicist at Los Alamos. "But the increase in key size comes at a performance cost. That annoying time lag when you click 'purchase' and things hang for a moment or two—that's the public-key cryptography working. And the bigger the key size, the longer the time delay." The problem is that the processors in our computers are not improving quickly enough to keep up with the decrypting algorithms that are driving the need for increasingly long keys. "That gets to be a concern for a lot of reasons," Hughes says. "If you're running a cloud system with many public-key sessions at once or if you're running something like the electric grid, you just can't have that kind of time lag."

Even NIST's recommended upgrade will become obsolete if quantum computers come on the scene. "I think there's a one-in-two chance that a quantum computer will be able to break RSA-2048 by 2030," says Michele Mosca, co-founder of the Institute for Quantum Computing, in reference to RSA's forthcoming 2,048-bit keys. "We've certainly seen a lot of advances in the past five years that lead us to think we need to be prepared in case we do see quantum computers," says Donna Dodson, chief cybersecurity adviser for NIST. "We're of the mind-set that they're probable."

OF CODES AND QUBITS

WHY WOULD A QUANTUM computer be so powerful? In a conventional computer, any single bit of information can assume only one of two values: 0 or 1. A quantum computer, however, takes advantage of a weird property of the subatomic world, where individual particles can exist in many states at once. Like Erwin Schrödinger's cat in a box—existing both alive and dead until someone opens the box for a look—a quantum bit, or qubit, of information can be a 1 and a 0 at the same time. (Physically, a qubit might be a single electron held in two spin states simultaneously.) A quantum computer with 1,000 qubits would contain $2^{1,000}$ different possible quantum states, exceeding by far the total number of particles in the universe. That does not mean a quantum computer could store limitless amounts of data: any attempt to observe the qubits would immediately cause them to assume a single 1,000-bit value. Yet with clever programming, the vast number of possible qubit states could be harnessed while *unobserved* to perform calculations that are impossible with conventional computers.

In 1994 Peter Shor, a mathematician then at AT&T Bell Laboratories, proved that a quantum computer could factor the kinds of large numbers that are used in RSA encryption—the asymmetric encoding scheme that protects the exchange of symmetric keys during Internet transactions. In effect, Shor wrote the first program for a quantum computer. Unlike a normal computer, where calculations proceed sequentially, one step at a time, a quantum computer performs all its operations simultaneously, a property Shor exploited. "Shor's algorithm would shatter RSA," Mosca says. But symmetric encryption methods—the most common being the Advanced Encryption Standard (AES), approved by NIST in 2001—would still be safe from quantum computers. That is because symmetric encryption programs such as AES do not use prime numbers to encode keys. Instead symmetric keys

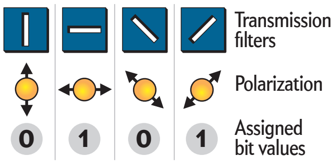
TOMORROW

The Quantum Future of Cryptography

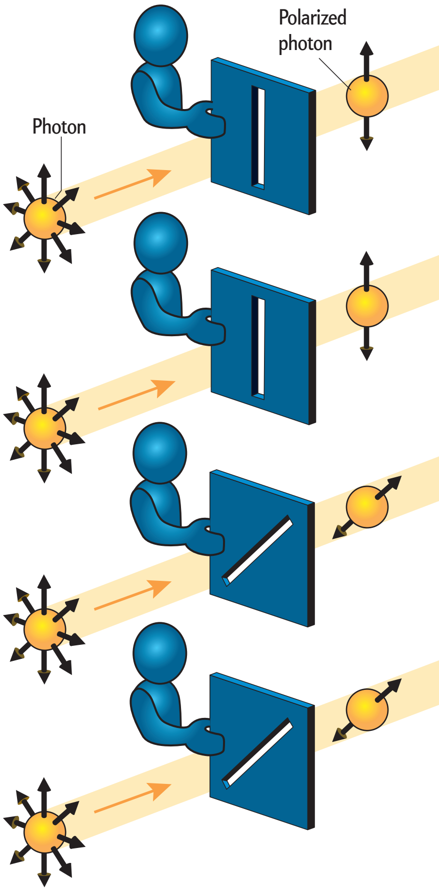
Quantum-key distribution is a way of securely sharing a cryptographic key using a stream of light particles, or photons, that are polarized. If an eavesdropper measures those photons while they are in transit, the act of measurement will change the polarization of some of those photons, and the sender and recipient will know that their message has been tampered with.

Sending and Receiving Polarized Photons

The sender (*blue*) transmits a series of photons; each passes through one of four polarizing filters. Each filter—and therefore polarization direction—is assigned a bit value of 0 or 1 (*below*). The sender writes down the bit value of each photon. The recipient (*green*) can only determine the bit value of each photon after it has passed through a receiving filter.



Transmitter has four polarizing filters. Each bit (as encoded by the photon's orientation) is recorded as it is transmitted.



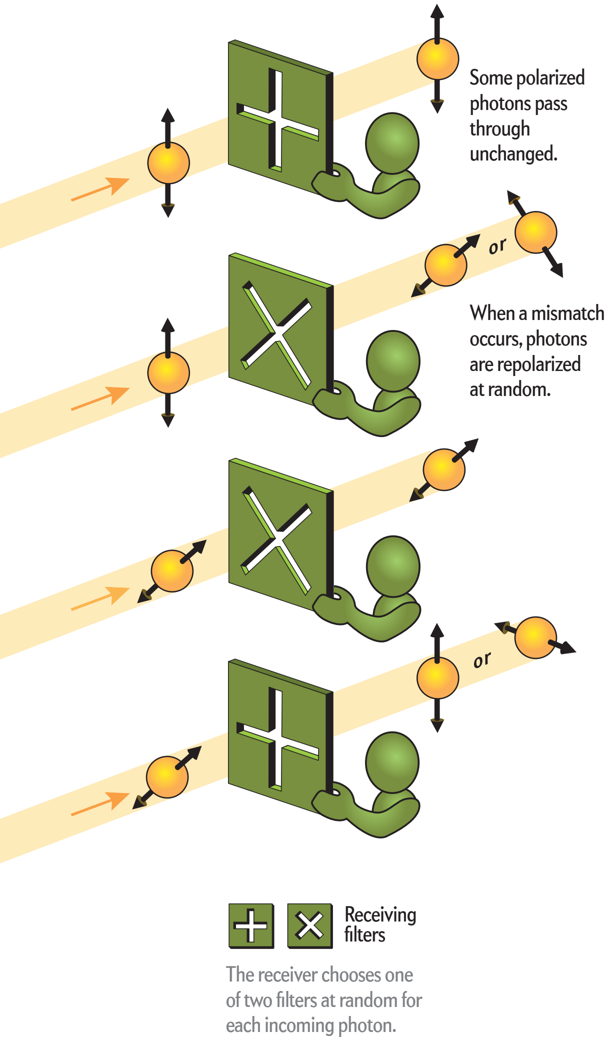
consist of randomly generated strings of 0s and 1s, typically 128 bits long. That makes for 2^{128} different possible key choices, which means a hacker would have to sort through some billion billion billion billion key combinations. The world's fastest computer—China's Tianhe-2, which can blaze through 33.8 quadrillion calculations per second—would need more than a trillion years to search all the key options. Even a quantum computer would not help hackers *directly* crack such huge numbers. But again, those enormous *symmetric* keys are encrypted during Internet transactions with *asymmetric* programs such as RSA, which *are* vulnerable to Shor's factoring method.

Before Shor's program can dismantle RSA, though, it first needs a quantum computer of sufficient power on which to run. Within the next year Mosca predicts that a number of labs around the world will have developed rudimentary systems consisting of a few tens of qubits. "If you're trying to factor a 2,048-bit RSA key," he says, "you probably need at least 2,000 qubits." The leap from tens of qubits to thousands might take a decade, but he sees no insurmountable obstacles. "Right now we meet most of the performance criteria to build a large-scale quantum computer," he says, "just not necessarily in the same place at the same time in a system that can be made larger."

QUANTUM NETWORKING

THE GOOD NEWS is that so far progress in quantum-encryption technology has outstripped efforts to build a working quantum computer. Quantum encryption began to take off in 1991, when Artur Ekert, a physicist at the University of Oxford, published a paper on quantum cryptography in the prestigious *Physical Review Letters.* Ekert, who at the time was unaware of the earlier work by Bennett and Brassard, described an alternative method of using quantum mechanics to encrypt information. His work eventually brought new recognition to Bennett and Brassard's idea, which turned out to be more practical than Ekert's own scheme.

It was not until the early 2000s, however, that quantum-encryption technology began to move out of the lab and into the commercial world. By then, physicists had found ways to cool photon detectors—the essential and most expensive component of any quantum-encryption device—using electric currents instead of liquid nitrogen. "When I started my Ph.D. in 1997, you cooled them



Some polarized photons pass through unchanged.

When a mismatch occurs, photons are repolarized at random.

Receiving filters

The receiver chooses one of two filters at random for each incoming photon.

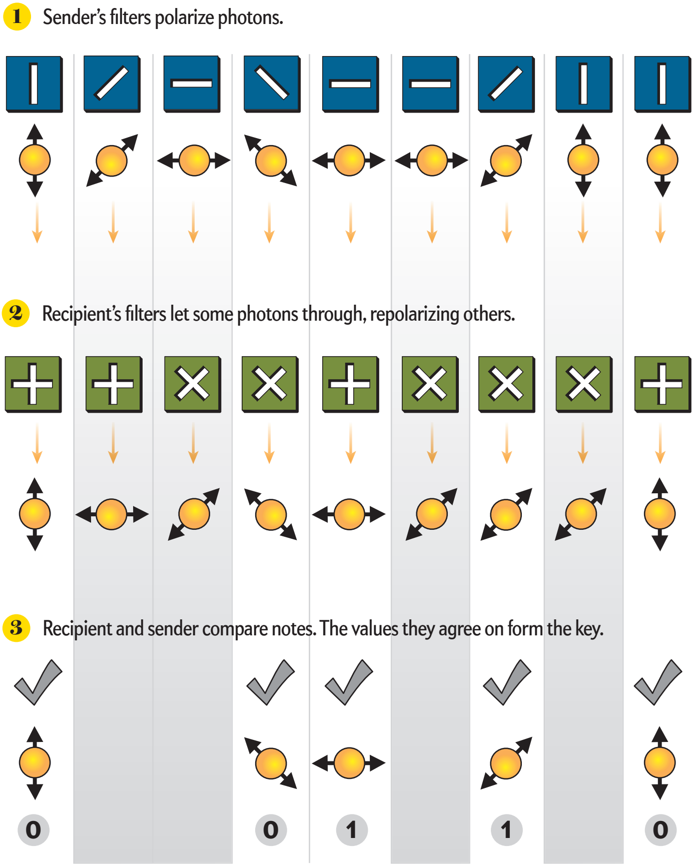
Retrieving the Key

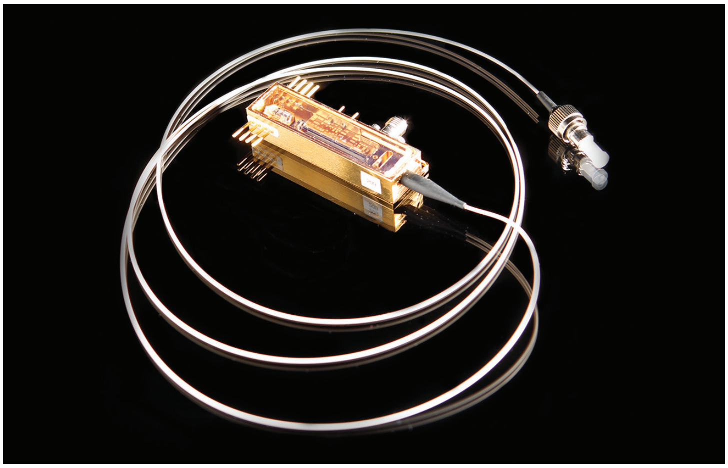
The recipient records the bit values of the photons coming through the receiving filters, then compares notes with the sender, who reveals which filters the recipient chose correctly. The string of bit values that both the sender and recipient share becomes the quantum key.

1 Sender's filters polarize photons.

2 Recipient's filters let some photons through, repolarizing others.

3 Recipient and sender compare notes. The values they agree on form the key.





QUANTUM ROUTER: The QKarD, developed by researchers at Los Alamos National Laboratory, would allow any number of computers, cell phones and other gadgets to exchange quantum keys through a secure, central server.

COURTESY OF LOS ALAMOS NATIONAL LABORATORY

by dipping the detectors into a dewar of liquid nitrogen, which is okay in the lab but not very practical if you want to use them in a data center," says Grégoire Ribordy, CEO of ID Quantique, a Swiss firm that in 2007 developed one of the first commercial quantum-encryption systems, which the Swiss government bought to protect data centers. The company has since sold its wares to Swiss banks and is now working with Battelle Memorial Institute in Columbus, Ohio, to build a network that will eventually link the company's Ohio offices with a branch in Washington, D.C.

On an overcast summer day Nino Walenta, a physicist at Battelle, shows me one of the encryption devices. "All we need is on this shelf," he says. "All the quantum optics, and everything we need to generate keys and distribute them, is right here." Walenta is standing next to a two-meter-high cabinet in a basement lab at Battelle's Columbus facility. On one shelf of the cabinet is a metal box about the size of a large briefcase. Within it lies the physical realization of the quantum-coding scheme first proposed by Bennett and Brassard more than three decades ago.

The hardware consists of a small laser diode, similar to those used in DVD players and bar-code scanners, that aims pulses of light at a glass filter. The filter absorbs nearly all the photons, allowing, on average, the passage of only a single particle of light at a time. Those individual photons are then polarized in one of two directions, each direction corresponding to a bit value of 1 or 0. Once filtered and polarized, the photons become the basis for a secret key that is then transmitted along a fiber-optic cable to the intended recipient, whose own hardware decodes the key by measuring the photons' polarizations.

Unlike a conventional secret key, the photon key is nearly tamper-proof. (More on that "nearly" in a bit.) Any eavesdropper who tries to intercept the photons will disturb them, altering their values. By comparing parts of the key, the legitimate sender and receiver can check whether the transmitted photons match the originals. If they detect signs of spying, they can scrap the key and start again. "Today keys are often used for years," Walenta says. "But with quantum-key distribution, we can change the key every second or every minute, which is why it is so secure."

Battelle has already set up a quantum network to exchange financial reports and other sensitive material between its Columbus headquarters and one of its manufacturing facilities in Dublin, Ohio, with a 110-kilometer loop of fibers connecting them. That distance, it turns out, approaches the upper limit for sending quantum-encrypted messages. Beyond that, the signal deteriorates because of the absorption of photons by the fiber-optic cable.

To get around that limitation and extend their network to cover more of Columbus—and, in the near future, to cover Washington, D.C.—the researchers at Battelle are working with ID Quantique to deploy "trusted nodes," relay boxes that receive and resend quantum transmissions. The nodes would be encased in sealed, insulated units to protect the sensitive photon detectors inside, which are cooled to −40 Celsius. If someone tried to break into one of the nodes, the device inside would shut down and erase itself. "Key generation would stop," says Don Hayford, a physicist who directs quantum-encryption research at Battelle.

If the chain of trusted nodes works smoothly, Hayford says, the technology could be deployed on a larger scale. He hands me a brochure with a map illustrating a future quantum network extending across large parts of the country. "That is our vision of a quantum network that protects all the Federal Reserve banking systems," he says. "If you get all the Federal Reserve banks, you've done pretty well. To go across country, you would need 75 nodes, roughly, which sounds like a lot, but when you do any conventional fiber networking, you have repeaters at about the same intervals."

The Chinese government has embraced similar technology. Construction has begun on a 2,000-kilometer quantum network between Shanghai and Beijing for use by the government and financial institutions. Whereas the projects envisioned by Hayford and under way in China might be used to protect banks and other organizations with private networks, they would not be practical for the Internet. The trusted nodes link one computer to the next in a linear chain rather than in a branching network where any machine can easily communicate with another. To Beth Nordholt, a physicist who recently retired from Los Alamos, such point-to-point connections recall the chaotic beginnings of the telephone industry in the late 19th century, when dark thickets of cables overhung city streets. "In those days you had to have a separate wire for everybody you wanted to talk to," she says. "That doesn't scale well."

Nordholt and her husband, Richard Hughes, and their Los Alamos colleagues Newell and Glen Peterson are working to make quantum encryption more scalable. For that purpose, they have built a device about the size of a memory stick that would allow any number of networked gadgets—cell phones, home computers or even televisions—to exchange quantum keys by connecting to a secure, centralized server. They call their invention the QKarD, a play on quantum-key distribution.

"The expensive parts of quantum cryptography are the single photon detectors and all the things to cool them and make them happy," Nordholt says. So she and her colleagues placed the complicated, costly components in one computer at the hub of a network. Client computers, each equipped with a QKarD, connect to

SCIENTIFIC AMERICAN ONLINE For more on the quantum-encryption race, go to ScientificAmerican.com/feb2016/crypto

the hub—but not directly to one another—by fiber-optic cables. The QKarD itself is a transmitter, with a small laser that allows it to send photons to the hub.

The QKarD works something like a telephone switchboard. Each computer on the network uploads its own symmetric keys encoded as streams of photons to the hub. This quantum encryption replaces the RSA encoding that would typically be used to protect the transmission of symmetric keys. Once the keys have been exchanged between the various client computers and the hub, the hub uses the keys and AES to relay conventional, nonquantum messages among any clients in the network that need to share sensitive data.

Nordholt's team has been running a model QKarD. Even though the entire system sits in one small lab at Los Alamos, a 50-kilometer length of fiber-optic cable, spooled in a bucket underneath a lab bench, connects the system's components and simulates real-world distances. The QKarD technology has been licensed for commercial development to Whitewood Encryption Systems. If the device does make it to market, Hughes estimates that a central hub capable of linking 1,000 QKarD-equipped clients might cost $10,000. If mass-produced, the QKarDs themselves could sell for as little as $50.

"I would like to see a QKarD built into phones or tablets so you can have a secure connection to a server," Nordholt says. "Or you could put one in a base station in your office and upload keys [to a server]. You could organically build out networks."

A QUANTUM FUTURE?

OVERHAULING THE WORLD'S encryption infrastructure could take more than a decade. "The more broadly deployed something is, the harder it is to fix," Mosca says. "Even if we could fix this at a technological level, everyone would have to agree on how to do this and have it all be interoperable for one global telecommunications system. We don't even have a common electrical system—we have to get adapters every time we travel."

The very difficulty of the challenge only adds to the urgency, Nordholt says: "This isn't just about protecting credit-card numbers. It's getting really serious." A few years ago, she says, Idaho National Laboratory conducted a study showing that hackers could blow up generators by feeding bad data into the networks that control the power grid. "I don't want to bring up doomsday scenarios," she says, "but this makes a real difference in people's lives."

The first target of a quantum computer, though, probably will not be a power grid. Many researchers in the field of cryptography believe that the NSA and other intelligence agencies around the world are storing huge quantities of encrypted data from the Internet that cannot be cracked with today's technology. The data are being saved, the reasoning goes, with the expectation that the NSA will be able to decrypt them when the agency has a quantum computer. In that scenario, it will not be only the private transactions of citizens a few decades from now that are at risk. It will be our own communications from today—communications that we naively consider to be secure.

"It would be completely crazy to think that there is not someone—maybe many someones—out there taking down all the traffic, just waiting for the technology to break it all retroactively," Brassard says. "So even if a quantum computer is not yet available, and even if one is not developed for the next 20 years, as soon as one *is* available, all the traffic that you've sent from day one of using these classical [encryption] techniques is compromised."

And even when widespread quantum encryption arrives, the cat-and-mouse game of encryption will continue. If the history of conventional cryptography is any guide, there is inevitably a gap between theoretical perfection and real-world implementation. When RSA encryption was first introduced, it was considered completely secure, says Zulfikar Ramzan, chief technology officer of RSA, the company that Rivest, Shamir and Adleman created to commercialize their invention. But in 1995 then Stanford University undergraduate Paul Kocher discovered that he could crack RSA's encryption simply by observing how long it took a computer to encode a small amount of data.

"It turns out that if the key has more 1s than 0s, it takes a bit more time to compute an RSA encryption," Ramzan says. "And then repeating that observation over and over again and measuring the timing, you can actually derive the entire RSA key, purely by looking at the amount of time the computation took." The work-around was fairly simple—engineers managed to camouflage the calculation times by adding some randomness to the procedure. "But again, it was the kind of attack that nobody conceived of until someone came up with it," Ramzan says. "So there may be similar attacks within the context of quantum computing."

In fact, the first quantum hack attack has already occurred. Five years ago a team led by Makarov, then at the Norwegian University of Science and Technology, connected a suitcase packed with optical equipment to a fiber-optic communications line linked to a quantum-encryption system built by ID Quantique. By using laser pulses to temporarily blind the encryption device's photon detectors, Makarov's team was able to successfully decrypt a supposedly secure quantum transmission.

Such an attack would be beyond the reach of an ordinary hacker, Makarov says. "You need to be a bit older than a teenager," he says. "And you need to have access to an optic lab. You don't have this technology in basements—yet." Although ID Quantique has since patched its device so that it is no longer vulnerable to the same type of attack, Makarov's successful hack popped the bubble of invincibility that surrounded quantum cryptography. "Breaking is easier than building," he says.

For Brassard, there is no doubt that the crackpot idea he and Bennett hatched on a beach all those years ago—even if it is imperfect—will be crucial to the future security of the world's many networks. "It requires the will to do it," Brassard says. "It will be expensive, just like fighting climate change will be expensive. But it's an expense that is minuscule compared to what will be lost if we don't do it—in both cases." SA

MORE TO EXPLORE

The Cost of the "S" in HTTPS. David Naylor et al. in *Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies,* pages 133-140; 2014.

NSA Seeks to Build Quantum Computer That Could Crack Most Types of Encryption. Steven Rich and Barton Gellman in *Washington Post;* January 2, 2014.

FROM OUR ARCHIVES

Quantum Cryptography. Charles H. Bennett, Gilles Brassard and Artur K. Ekert; October 1992.

Best-Kept Secrets. Gary Stix; January 2005.

scientificamerican.com/magazine/sa