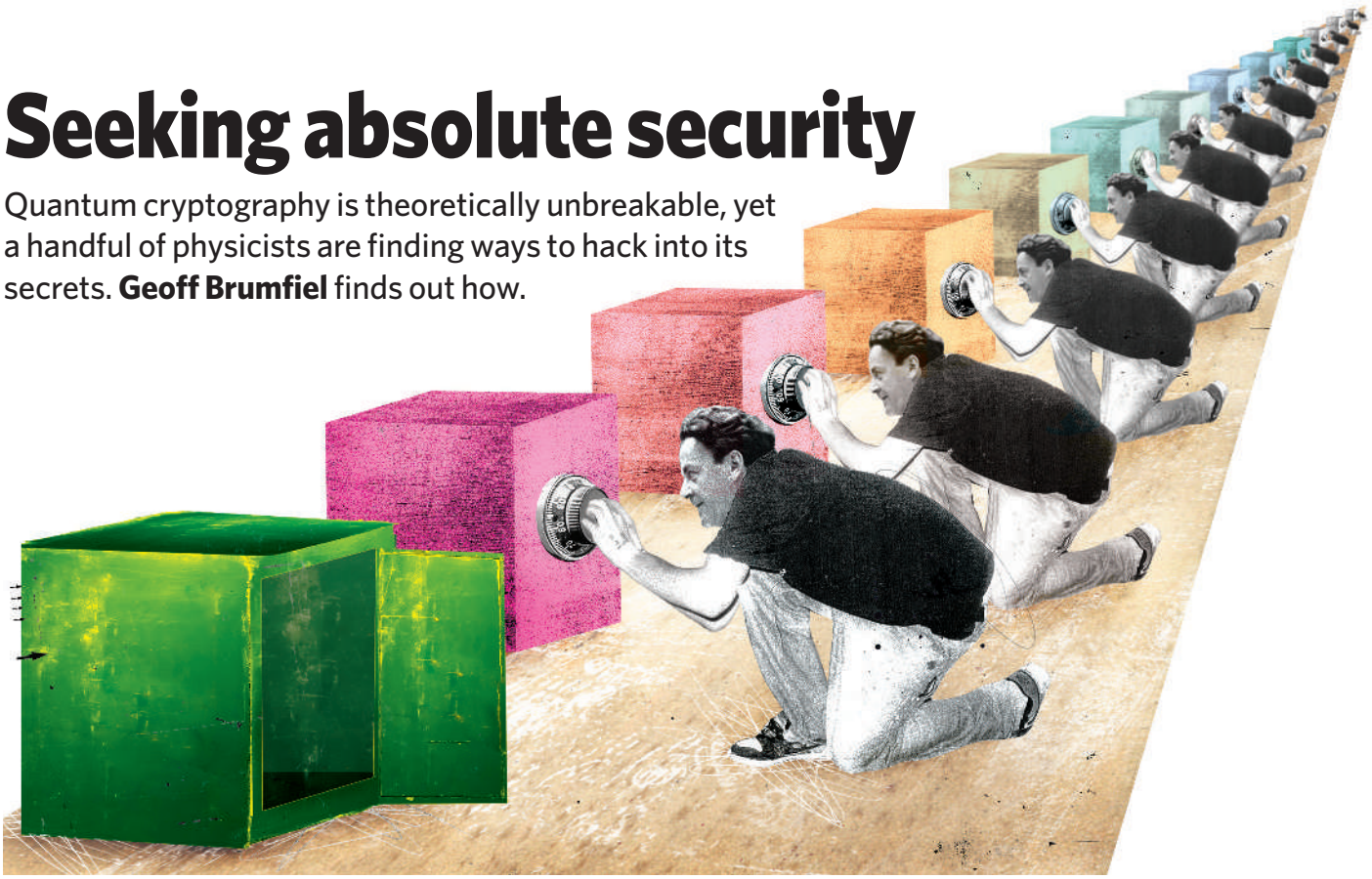
# Seeking absolute security

Quantum cryptography is theoretically unbreakable, yet a handful of physicists are finding ways to hack into its secrets. **Geoff Brumfiel** finds out how.



D. ALLISON; L. DUNCAN/UNIV. ROCHESTER/AIP EMILIO SEGRE VISUAL ARCHIVES

On an otherwise quiet Saturday evening in 1946, Frederic de Hoffman briefly thought he had lost the secrets of the atomic bomb. De Hoffman was a physicist at Los Alamos National Laboratory in New Mexico. As part of his job, he kept the design for the weapon in nine filing cabinets in his office. When he came into work and opened one, he found an enigmatic note: "When all the combinations are the same, one is no harder to open than another — same guy."

De Hoffman thought that the 'same guy' was the person who had tried to break into the lab's secure facility earlier that summer, but, as it turned out, the thief was standing next to him. It was Richard Feynman (pictured above), a leading quantum theorist who had a reputation as an incorrigible prankster. He had broken into de Hoffman's filing cabinets earlier that day to grab a few documents he needed to write a report.

Security has come a long way since 1946, but some things never change. Quantum physicists are now learning how to crack what is arguably the most secure form of data transmission ever conceived: quantum cryptography. This encryption method is theoretically unbreakable, but nevertheless, groups are finding weaknesses that may require rethinking the design of commercial systems. The work, says Seth Lloyd, a physicist at the Massachusetts Institute of Technology (MIT) in Cambridge, is a cautionary tale. "Nothing is unassailable," he warns.

Quantum cryptography uses the fundamental laws of physics to encode information in the quantum states of particles, usually photons. Most existing systems use a protocol known as Bennett–Brassard 1984, or BB84, which generates a secure quantum 'key' that can be used to encode messages sent between parties. BB84 works like this: the sender transmits an encoded key by polarizing single photons along one of two axes — up and down or tilted at 45° — and sending them along a fibre-optic cable to the receiver (see diagram). The receiver then randomly chooses an up-and-down or tilted filter to read each photon. If the filter they choose is aligned with the sender's original polarization, the receiver will be able to read one bit of the sender's data, but if they choose the wrong alignment, then the photon, by virtue of quantum mechanics, will pass through the filter in a random orientation.

**"Not enough attention has been paid to vulnerabilities."**
— Daniel Gottesman

After the original key has been transmitted, the sender and receiver compare the filters they used for each photon. They throw away the random bits and keep the rest as part of a new, secure shared key, which is then used to encode a longer message sent over regular channels.

At first glance, the BB84 protocol may seem complicated and highly inefficient. But the method behind it means that it can't be intercepted without the sender and receiver finding out. Suppose an eavesdropper were to try to listen in on their conversation. As she reads each photon with her own two filters, she passes it along to the receiver, but not necessarily in the same orientation as it was originally sent. Therefore, when the sender and receiver compare their keys, they will find a lot more random bits created by the eavesdropper and they can immediately cut off their communication or try to send a fresh key through a different channel.

What sets the BB84 protocol apart from other forms of cryptography is that the code should be impossible to crack. Most of today's keys are encrypted with a mathematical technique that depends on large prime numbers. Security hinges on the idea that large numbers are hard to factor into primes, but there is no way to be sure of that assumption, says Daniel Gottesman, who studies quantum cryptography at the Perimeter Institute in Waterloo, Canada. "We don't think there's a way to do it on a classical computer in any reasonable amount of time, but there is no way to prove that," he says. By contrast, the security of BB84 and other quantum protocols hinges on the immutable laws of physics: "Given that quantum mechanics is correct, then we can mathematically prove that this idealized BB84 protocol is actually secure."

But if the idealized version of the BB84 protocol is secure, the real version can be anything but, according to Charles Bennett, a computer scientist at IBM Research in Yorktown Heights, New York. Bennett is one of the 'B's in the BB84 name, and he and other researchers built the first demonstration unit in 1989. In that very first quantum-cryptographic system, Bennett recalls, the polarization of the photon was switched by use of

a high-voltage power supply. "The power supply hummed differently depending on whether or not the voltage was being applied," Bennett says. "If you listened, you could hear it."

## No escape from reality

Nobody was planning on sending state secrets over the experimental set-up in Bennett's office. But while showing that quantum cryptography could work, he and his collaborators inadvertently demonstrated something else: idealizations are often far from reality. "It's hard to ensure that any box that you build is entirely secure," he says.

Such real-world security is the key to moving quantum cryptography from the lab to the commercial sector, and it has been a slow process. BB84 protocols require sending single photons, but early technology often sent more than one photon at a time, raising the possibility that an eavesdropper could read one without disturbing the others. Single-photon systems became commercially available a few years ago, but they remain modest in their capabilities. Error rates can be high, data speeds slow, and they can only be transmitted as far as a single photon can travel along a commercial fibre-optic line.

Meanwhile, researchers are stepping up their attacks on quantum cryptography. The most scientifically sophisticated strike was conducted earlier this year by MIT physicists led by Jeffery Shapiro and Franco Wong[1]. The team stole information from a passing photon by entangling its polarization with its own momentum. This quantum-mechanical entanglement allowed the team to read about 40% of the key while leaving the polarization relatively untouched. But Shapiro and Wong both admit that an eavesdropper would be defeated just by increasing the length of the key. Commercial systems already use long keys to deflect such attacks.

Other vulnerabilities could be even more dangerous because they have been overlooked by theorists. For instance, theoretical physicists assume that the sender and receiver will have absolute control over their equipment. But the real world is less precise, says Nicolas Gisin of the University of Geneva in Switzerland. Gisin and his colleagues have shown that an eavesdropper could learn a sender's polarizations by shining a light down the fibre and into the sender's set-up[2]. Because the cryptographic protocol assumes that light will only come from the sender, it doesn't take into account such dirty tricks.

And still other attacks can take advantage of simple flaws in individual components. Earlier this year, Hoi-Kwong Lo and his colleagues at the University of Toronto in Canada showed that they could steal a commercial system's quantum secrets by exploiting a small defect in the receiver's photodetectors. The protocol under attack was different from BB84 in that it required two photons. The system switched on the two highly sensitive detectors only when it was expecting photons from the sender to avoid false alarms. But the detectors switched on at slightly different times. By delaying photons so that they arrived just as a detector was turning on or off, Lo showed that an eavesdropper could modify the measurement, which blinds the receiver to the eavesdropper's presence.

**"It's hard to ensure that any box that you build is entirely secure."**
— Charles Bennett

Not everyone agrees on how serious the threats are to commercial systems. "We are quite confident that our system will remain impervious," says Robert Gelfond, chief executive of MagiQ, a quantum-cryptography company in Somerville, Massachusetts. Gelfond says MagiQ's government and military customers regularly try to breach their systems' security. "They want to see it and test for themselves," he says. So far, MagiQ has not had to modify any of its cryptographic technology.

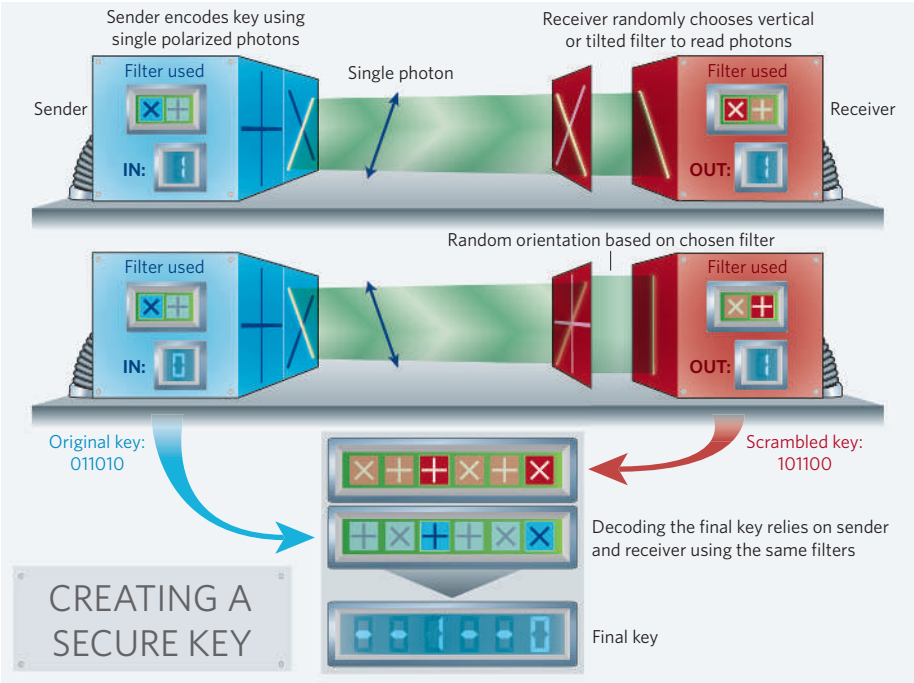
## Weak spots

But others think that more needs to be done to ensure that the systems live up to their theoretical reputation. "There's been a lot of lip service," says Gottesman. "But I don't think enough attention has been paid to vulnerabilities." The researchers are more concerned with getting their set-up to work than they are with finding ways to cheat the system, he says.

That may be changing. Gisin thinks that the number of studies on potential attacks has risen over the past few years. "The entire field is getting more mature," he says. "Now is really the time to think about these things." As quantum cryptographic networks grow in size and complexity, they are also at risk from new kinds of attacks. Gisin would like to see the industry develop standards for detectors, transmission lines and other equipment that would help to close future gaps in security.

But there will always be a dirty trick to try, as the quantum-theorist-turned-safecracker Richard Feynman knew all too well. Feynman didn't rely on his theoretical brilliance to open the safes holding America's atomic secrets. He simply guessed the combination. He knew that his friend, a physicist, would undoubtedly choose a number he already had memorized, and the sly theorist got it on the second try: 27-18-28, the first six digits of the mathematical constant *e*. ■

**Geoff Brumfiel is *Nature*'s physical sciences reporter in Washington DC.**




1. Kim, T., Stork, I., Wong, F. N. C. & Shapiro, J. H. *Phys. Rev. A* **75,** 042327 (2007).
2. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. *Phys. Rev. A* **73,** 022320 (2006).
3. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Loh, H.-K. Preprint at http://lanl.arxiv.org/abs/0704.3253 (2007).

## G8 leaders make progress towards Kyoto successor

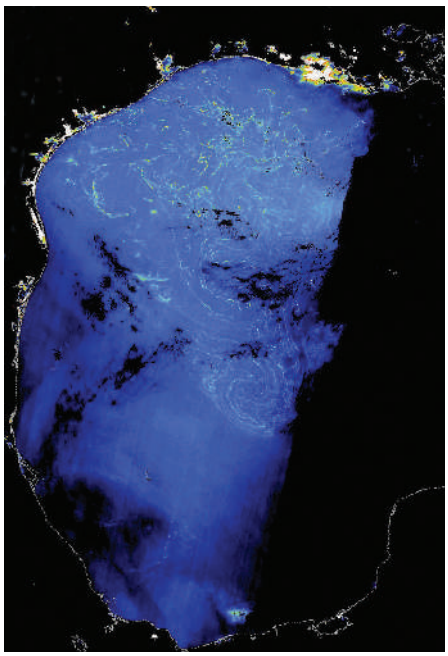
A climate agreement reached by world leaders at last week's G8 summit in Germany has "re-energized" the process to find a successor to the Kyoto treaty, says Yvo de Boer, executive secretary of the United Nations body that oversees the Kyoto protocol. De Boer, who will lead the negotiations in Bali in December, says that the deal sends "an important signal to developing countries" ahead of the climate-change summit.

G8 leaders, including US President George W. Bush, have agreed to "consider seriously" the decision made by the European Union, Canada and Japan to at least halve global emissions by 2050. Although some environmental groups have criticized the agreement's lack of hard targets, the G8 communiqué notes it is "vital" that major emitters agree to a detailed global framework by 2009 (see http://tinyurl.com/28xyta). This, says de Boer, raises the likelihood that a follow-on agreement for Kyoto will be in place before the current treaty expires in 2012.

## Satellite detects invasive seaweed's fluorescence

Sargassum, a dense floating brown seaweed famous for entangling ships in the Sargasso Sea, has been detected from space for the first time, thanks to the European Space Agency's Envisat. The satellite's Medium Resolution Imaging Spectrometer (MERIS) detects fluorescence emission from chlorophyll, and is unique among ocean-observing satellites in being able to pick up emissions at 709 nanometres. This allowed scientists at the Institute of Ocean Sciences in British Columbia, Canada, and the University of South Florida in Tampa to detect lines of the seaweed in the Gulf of Mexico. Being able to measure sargassum from space should improve estimates of ocean primary productivity; the alga has spread as an invasive species to many spots around the world.

ESA



Sargassum in the Gulf of Mexico, seen from space.

## Kamchatkan mudslide wipes out study sites

I. SHPILENOK

A massive mudslide on 3 June in the Valley of Geysers, on the Kamchatka Peninsula in the far east of Russia, has loosed an estimated 4.5 million cubic metres of rock, gravel, snow and ice onto the World Heritage site.

Scientists have been sent to investigate the extent of the damage. Juergen Wiegel, a microbiologist at the US University of Georgia in Athens, who has previously worked in the region, says the slide will "definitely" affect future research into unique extremophiles living in the vents. The loss "is very sad", he says.

Botanists worry for rare plants in the valley, and wildlife officials are concerned about salmon — an important food source for other animals in the region. Geologists add that mud caps over the geysers could cause explosions.

## Transit of Earth-like planet eludes astronomers

Astronomers who had been anxiously keeping an eye on the dwarf star Gliese 581, in hopes of observing an Earth-like planet pass in front of it, have been met with disappointment so far. The star's light, as viewed by the Canadian Space Agency's MOST space satellite, has been remarkably constant — meaning the recently spotted planet 581c has not passed between the star and Earth. Data collected from such a pass would have allowed a precise determination of the planet's size and composition.

Astronomers have not yet had time to check whether another planet, 581d, passes between the star and Earth, but say the odds for this are very slim. Some say that 581d, which is cooler than 581c, may have more promising conditions for the possible formation of complex life in that system.

## US House votes to free up federal stem-cell funding

The US House of Representatives voted on 7 June to loosen restrictions on federal stem-cell funding. The bill, passed by the Senate in April (see *Nature* **446**, 842; 2007), allows US funding for research on stem cells derived from left-over embryos at fertility clinics. But President Bush quickly made clear he would again veto the measure, which he first quashed last July (see *Nature* **442**, 335; 2006).

Speaking at the G8 summit in Germany, Bush highlighted research published last week showing that adult mouse cells can be reprogrammed to an early embryonic state without the need for eggs or embryos (see *Nature* **447**, 618–19; 2007). "These reports give us added hope that we may one day enjoy the potential benefits of embryonic stem cells without destroying human life," he said. The Senate may succeed in mustering the two-thirds majority needed to override a veto; its vote in April was 63–34, with three absentees. At 247–176, the House remains dozens of votes short of a veto-proof majority.

## EU ministers fail to agree on Galileo rescue plan

Galileo, the EU's proposed satellite navigation rival to the US's global positioning system, has an uncertain future. The partnership set up between the public sector and European aerospace companies to develop the project was pronounced dead at a meeting of EU transport ministers in Luxembourg last Friday.

Progress had stalled mainly because the companies couldn't agree on the sharing of costs. The ministers said they would come up with a new funding plan by this autumn, in which the EU or governments may end up picking up the €2.4-billion (US$3.6-billion) bill for completing the 30-satellite system.

**Correction**

The News Feature 'Seeking absolute security' (*Nature* **447,** 372–373; 2007) incorrectly stated that Hoi-Kwong Lo and his colleagues hacked into a quantum-cryptographic system that did not use the standard BB84 protocol for quantum security. In fact, the system did use BB84.