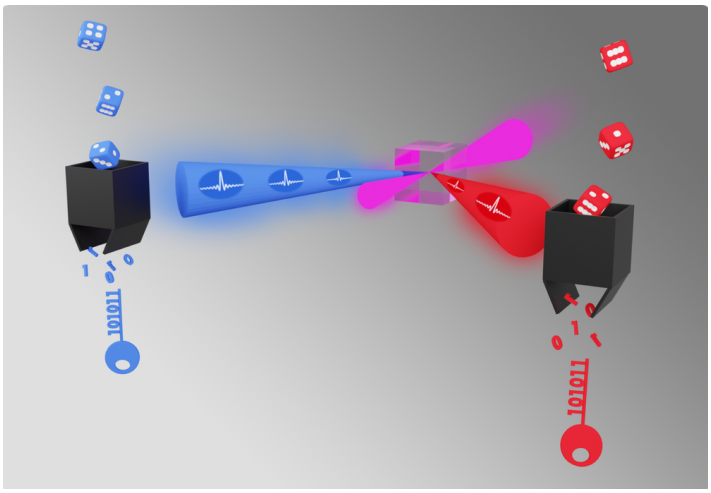
Hiding Secrets Using Quantum Entanglement

Three experiments demonstrate the key elements of a quantum cryptographic scheme that predictions indicate should be unhackable, bringing the promise of quantum encryption technologies a step closer to reality.

By **Sophia Chen**

In the 1980s, physicists began proposing quantum-based encryption methods that would scramble data to guarantee its security. The methods exploit a particular quirk of quantum systems: that measurements of those systems inherently change the systems' properties. Specifically, the protocols involve serial measurements of quantum objects, the statistics of which should reveal any eavesdropper. However, researchers have struggled to build devices that work exactly as the protocols specify. Now three research groups, one based in Germany, one in the UK, and one in China, have independently performed proof-of-principle experiments of a quantum encryption method that can secure information even if the devices used do not behave exactly as predicted [**1**–**3**]. The demonstrations are "a major breakthrough for cybersecurity," says Charles Lim of the National University of Singapore, who was involved in the Germany-based experiments.



Device-independent quantum key distribution methods sidestep the vulnerabilities of other quantum encryption techniques, as they work even if the devices used to create and detect the needed quantum particles behave differently from predictions.
Credit: W. Z. Liu and C. Wu/University of Science and Technology of China

The three experiments each demonstrate aspects of an encryption method known as device-independent quantum key distribution (DIQKD). In DIQKD, a device repeatedly generates pairs of entangled quantum particles. Two parties, Alice and Bob, each take one particle from every pair. Alice and Bob then create a "key"—a string of 1's and 0's that can encode and decode messages—in part by making a series of measurements of a two-outcome property of their particles. If the particle is a photon, this property might be its polarization, which can be horizontal or vertical. For an atom, it might be the atom's state (ground or excited). Because the outcome of a measurement on one particle is correlated with that of its entangled counterpart, Alice and Bob can generate a single shared key after some postprocessing.

As Alice and Bob make these measurements, they intermittently verify the security of their channel using a test based on a quantum rule known as Bell's theorem. According to Bell's theorem, if two particles are entangled, measurements of those particles must exhibit specific statistical correlations. For the test, Alice and Bob use a subset of the measurements for

generating the key. They then check that the measurements follow the prescribed statistics. If there is a mismatch, Alice and Bob know that their particles are no longer entangled, indicating that they can no longer guarantee the security of the channel. They then discard their measurements and restart the process.

Researchers have mathematically proven the security of DIQKD. No such proof exists for standard classical encryption methods, which rely on the computational difficulty of factoring large numbers. Researchers anticipate that future quantum computers will be able to quickly factor these numbers, rendering current classical encryption obsolete. On the other hand, DIQKD provides security "against an adversary with arbitrary processing power or even a quantum computer," says Jean-Daniel Bancal of the French National Center for Scientific Research (CNRS).

For the DIQKD methods used in the new experiments, Alice and Bob require no information about the device that generated their particles, meaning that researchers "don't need to model [their] devices," says Antonio Acín of the Institute of Photonic Sciences in Spain, who was not involved in any of the experiments. "You can treat them as black boxes." Thus, the methods sidestep the vulnerabilities of other quantum encryption protocols, some of which have been implemented in commercially available technologies, such as one available from the Swiss company ID Quantique. In 2007, the Swiss government used ID Quantique's encryption devices to secure the votes in their national election. But by 2010, two teams of researchers had successfully hacked ID Quantique's device using discrepancies between its operation and its theoretical description. One team, for example, intercepted an encryption key without either Alice or Bob noticing by exploiting a time gap in the machine's production of successive photons, which theory requires be produced without delay.

"A real device is different from a mathematical model," says Qiang Zhang of the University of Science and Technology of China, a member of the China-based team. "Without full knowledge of that difference, it may leave a backdoor open to an attack."

While the three experiments used similar DIQKD methods, they have notable differences. The China-based experiments used entangled photons; the UK ones, entangled strontium ions; and the German ones, entangled rubidium atoms. "Each has its own advantage," Zhang says. When using atoms and ions, for example, researchers can keep track of both particles in an entangled pair, he says. They have no way of tracking two entangled photons. When one photon in a pair gets lost, this raises other experimental requirements for security, which Zhang's team was able to meet. However, photons are used in many exisiting communications technologies, for example, potentially making it easier and quicker to implement quantum techniques with photons, Zhang says.

Only the UK-based experiment completed an entire DIQKD protocol, generating a 95,000-bit encryption key over about 8 hours. The Germany-based experiment produced a few thousand bits over two days, enough for a small fraction of a key, but it did not complete the key because of time constraints. The China-based experiment also did not generate a complete key because their detector could not keep track of enough entangled photon pairs to do so. Once they improve their detection efficiency, the team says that their system should only take a few minutes to make a key.

In all the experiments, Alice and Bob were much less than a kilometer apart. In China they were 20 to 220 m apart, in Germany 400 m apart, and in the UK they were separated by only 2 m. Because of those distance limitations, the demonstrations do not yet show that DIQKD can be a practical technology, says Acín. For that to happen, researchers will need to demonstrate the viability of the methods over kilometer-scale distances. They also need the methods to generate keys faster, Lim says.

Given these engineering challenges, Zhang thinks that commercial DIQKD encryption tools are unlikely anytime soon. But he still thinks that the new demonstrations have value. "It [seems like] a ridiculous thing," he says. But these experiments show that "you can use a device that you don't trust, and you can still generate a secure key."

Sophia Chen is a freelance science writer based in Columbus, Ohio.

REFERENCES

1. W. Z. Liu *et al.*, "Toward a photonic demonstration of device-independent quantum key distribution," **Phys. Rev. Lett.**

129, 050502 (2022).

2. D. P. Nadlinger *et al.*, "Experimental quantum key distribution certified by Bell's theorem," **Nature 607, 682 (2022).**
3. W. Zhang *et al.*, "A device-independent quantum key distribution system for distant users," **Nature 607, 687 (2022).**