CHINA'S 2,000-KM QUANTUM LINK IS ALMOST COMPLETE

The Beijing–Shanghai project pushes the limits for "unhackable" links

XINHUA/ALAMY

QUANTUM SPACE LINK: Staff work on China's quantum research satellite, which launched in August. It is part of a larger effort in the country to push the limits of quantum key distribution.

By the end of this year, a team led by researchers from the University of Science and Technology of China, in Hefei, aims to put the finishing touches on a 2,000-kilometer-long fiber-optic link that will wind its way from Beijing in the north to the coastal city of Shanghai.

What will distinguish this particular stretch of fiber from myriad other long-distance links is its intended application: the exchange of quantum keys for secure communication—a sophisticated gambit to protect data from present and future hackers. If all goes according to plan, this Beijing-Shanghai line will connect quantum networks in four cities. And this large-scale terrestrial effort now has a partner in space: A quantum science satellite was launched in August with a research mission that includes testing the distribution of keys well beyond the country's borders.

With these developments, China is poised to vastly extend the reach of quantum key distribution (QKD), an approach for creating shared cryptographic keys—sequences of random bits—that can be used to encrypt and decrypt data. Thanks to the fundamental nature of quantum mechanics, QKD has the distinction of being, in principle, unhackable. A malicious party that attempts to eavesdrop on a quantum transmission won't be able to do so without creating detectable errors.

QKD has already made its way into the real world. In 2007, the scheme was used to secure the transmission of votes in a Swiss election. Several years ago, the U.S.-based firm Battelle began to use the approach to exchange information securely over kilometers of fiber between its corporate headquarters in Columbus, Ohio, and a production facility in Dublin, Ohio.

But despite great progress, there has been a stumbling block to wide distribution. "The problem we've got is »

RIVER OF SECRETS: A 2,000-kilometer-long backbone will connect quantum networks in four cities. The line uses a number of secured nodes as relays along the route.

distance," says Tim Spiller, director of the United Kingdom's Quantum Communications Hub, a nationally funded project that is building and connecting quantum networks in Bristol and Cambridge, in England.

The challenge is that QKD encodes information in the states of individual photons. And those photons can't travel indefinitely in fiber or through the air; the longer the distance, the greater the chance they will be absorbed or scattered.

This characteristic has a direct impact on how quickly a quantum key can be generated, explains physicist Jian-Wei Pan, who leads the Chinese projects. If researchers attempted to send signals directly down 1,000 kilometers of fiber, Pan says, "even using all the best technology, we would only manage to send 1 bit of secure key over 300 years."

Instead, QKD fiber links must have a way to refresh the signal every 100 km or so to maintain a reasonable bit rate. But this can't be done with conventional telecommunications equipment. The same rules that protect quantum transmission against eavesdropping also prohibit a quantum key from being copied without corrupting it. The solution has been to concatenate, creating a daisy chain of individual quantum links connected by physically secured spots, or "trusted nodes." Each intermediate node measures the key and then transmits it with fresh photons to the next node in the chain.

The Beijing–Shanghai line will use 32 trusted nodes to create the 2,000-km line. This approach isn't ideal for security. Because each trusted node has to convert the quantum key back into classical (nonquantum) information before passing it on, an eavesdropper at the node could potentially hack the data stream there undetected. "That's the drawback," Pan says. But the approach is "still much better than traditional communications... [where] there is the possibility of performing eavesdropping" at every point along the route, he says. Here, the problem is limited to 32 spots under lock and key.

"A long-distance chain link like this, [it's] really the first time it's been done," says Grégoire Ribordy of ID Quantique, based in Geneva, which makes hardware for QKD networks. "It's inspiring other people to try to do similar things around the world."

If you want to avoid even the small vulnerability of trusted nodes, Spiller says, long-distance QKD must use quantum entanglement, a property that can link the states of photons separated by great physical distance and that can be exchanged between photons. "Quantum repeaters," used in place of trusted nodes, could take advantage of this phenomenon to relay a quantum key without having to measure it. But this technology is still in an early stage of development, says Spiller; among other things, a quantum repeater will likely require a form of quantum memory to help coordinate communication.

"[If you] don't have to trust any of the nodes along the network, that will broaden the applicability of QKD," says Michele Mosca, cofounder of the Institute for Quantum Computing at the University of Waterloo, in Ontario, Canada. One reason to improve QKD's reach is to protect communications from tomorrow's quantum computers, which could make short work of the public-key cryptography that underpins Internet security and many other applications.

But Mosca notes that QKD is not the only possible way to address this threat; many cryptographers are exploring new "postquantum" algorithms to replace our existing public-key systems. QKD offers an "extra degree of assurance," he says, but improved conventional cryptography will be a cheaper and more practical solution for many applications. Both will likely have a role to play in the coming years. —RACHEL COURTLAND

ILLUSTRATION BY Erik Vrielink