Stephanie Wehner is part of the team trying to build a true quantum network across Europe.

MARCEL WOGRAM FOR *NATURE*

THE ENTANGLED WEB

BY DAVIDE CASTELVECCHI

Quantum physics can already make communications super-secure. But exploiting some of its strangest properties could take these networks to the next level.

Before she became a theoretical physicist, Stephanie Wehner was a hacker. Like most people in that arena, she taught herself from an early age. At 15, she spent her savings on her first dial-up modem, to use at her parents' home in Würzburg, Germany. And by 20, she had gained enough street cred to land a job in Amsterdam, at a Dutch Internet provider started by fellow hackers.

A few years later, while working as a network-security specialist, Wehner went to university. There, she learnt that quantum mechanics offers something that today's networks are sorely lacking — the potential for unhackable communications. Now she is turning her old obsession towards a new aspiration. She wants to reinvent the Internet.

The ability of quantum particles to live in undefined states — like Schrödinger's proverbial cat, both alive and dead — has been used for years to enhance data encryption. But Wehner, now at Delft University of Technology in the Netherlands, and other researchers argue

that they could use quantum mechanics to do much more, by harnessing nature's uncanny ability to link, or entangle, distant objects, and teleporting information between them. At first, it all sounded very theoretical, Wehner says. Now, "one has the hope of realizing it".

Proponents say that such a quantum internet could open up a whole universe of applications that are not possible with classical communications, including connecting quantum computers together; building ultra-sharp telescopes using widely separated observatories; and even establishing new ways of detecting gravitational waves. Some see it as one day displacing the Internet in its current form. "I'm personally of the opinion that in the future, most — if not all — communications will be quantum," says physicist Anton Zeilinger at the University of Vienna, who led one of the first experiments on quantum teleportation[1], in 1997.

A team at Delft has already started to build the first genuine quantum network, which will link four cities in the Netherlands. The project, set to be finished in 2020, could be the quantum version of ARPANET, a communications network developed by the US military in the late 1960s that paved the way for today's Internet.

Wehner, who is involved in the effort, is also coordinating a larger European project, called the Quantum Internet Alliance, which aims to expand the Dutch experiment to a continental scale. As part of that process, she and others are trying to bring computer scientists, engineers and network-security experts together to help design the future quantum internet.

Many technical details still need to be sorted out, and some researchers caution that it is too early to say exactly how much a quantum internet might deliver. But by thinking about security early, Wehner says that she hopes to avoid the vulnerabilities that the Internet inherited from ARPANET. "Maybe we have a chance to do it all right from the start."

> "MAYBE WE HAVE A CHANCE TO DO IT ALL RIGHT FROM THE START."

QUANTUM KEYS

The first proposals for quantum modes of communication date back to around the 1970s. Stephen Wiesner, then a young physicist at Columbia University in New York City, saw potential in one of the most basic principles of quantum mechanics: that it is impossible to measure a property of a system without changing it.

Wiesner suggested that information could be encoded in the states of objects such as isolated atoms, whose 'spins' can point up or down — like the 0 and 1 of classical bits — but can also be in both states simultaneously. Such units of quantum information are now commonly called quantum bits, or qubits. Wiesner pointed out that because the properties of a qubit can't be measured without changing its state, it is also impossible to make exact copies or 'clones' of one[2]. Otherwise, someone could extract information about the state of the original qubit without affecting it, simply by measuring its clone. This prohibition later became known as quantum no-cloning, and it turns out to be a boon for security, because a hacker cannot extract quantum information without leaving a trace.

Inspired by Wiesner, in 1984, Charles Bennett, a computer scientist at IBM in Yorktown Heights, New York, and his collaborator Gilles Brassard, at the University of Montreal in Canada, came up with an ingenious scheme by which two users could generate an unbreakable encryption key that only they know[3]. The scheme depends on the fact that light can be polarized, so that the electromagnetic waves oscillate either in a horizontal or a vertical plane. One user converts a random sequence of 1s and 0s into a quantum key encoded in those two polarization states and sends it streaming to another person. In a sequence of steps, the recipient measures the key and establishes that the transmission was not disturbed by the measurements of an eavesdropper. Confident in the security of the key, the two parties can then scramble any message made up of classical bits — an image, for example — and send it just as they would any other encrypted message over the conventional Internet, or any other channel.

In 1989, Bennett led the team that first demonstrated this 'quantum key distribution' (QKD) experimentally[4]. Today, QKD devices that use similar schemes are commercially available and typically sold to financial or government organizations. ID Quantique, for example, a company founded in 2001 in Geneva, Switzerland, built a quantum link that has been protecting the results of Swiss elections for more than ten years.

Last year, China's Micius satellite, the brainchild of physicist Pan Jianwei of the University of Science and Technology of China in Hefei, made some of the flashiest demonstrations of the approach. Using a variant of Bennett and Brassard's protocol, the spacecraft created two keys, then sent one to a ground station in Beijing and another to Vienna as it passed overhead. An on-board computer then combined the two secret keys to create a new one, which it beamed down classically. Armed with their private keys, the Vienna and Beijing teams could unscramble that combined key by essentially subtracting their own, and so learn the other's secret key. With both keys, one team could decrypt a transmission that the other team encrypted with its key. Last September, Pan and Zeilinger used this approach to set up the first intercontinental video chat to be secured in part with a quantum key[5].

Satellites such as Micius could help to address one of the main challenges in making today's quantum communications secure: distance. The photons needed to create an encryption key can get absorbed by the atmosphere or — in the case of ground networks — by an optical fibre, which renders quantum transmission impractical after several tens of kilometres.

Because quantum states cannot be copied, it is not an option to send multiple copies of a qubit in the hope that at least one will arrive. So, at the moment, creating long-distance QKD links requires building 'trusted nodes' to act as intermediaries. If a person were to hack into a trusted node, which handles keys in both their quantum and classical forms, they would be able to copy the keys without being detected — and so, of course, could the government or company operating the node. This is true both for trusted nodes on the ground and for Micius. "The satellite knows everything," Pan says. But passing satellites could cut down on the number of trusted nodes that are needed to connect distant points.

Pan says that trusted nodes are already a step forward for some applications, because they reduce the number of spots where a network is vulnerable to attack. He has also led the creation of the extensive Beijing–Shanghai quantum-communication backbone. Launched in September, this connects 4 cities with 32 trusted nodes using more than 2,000 kilometres of optical fibre, and is being tested for banking and commercial communications, such as linking up the data centres of Internet-shopping giant Alibaba, Pan says.

QUANTUM CONNECTIONS

But networks that involve trusted nodes are only partly quantum. Quantum physics plays a part only in how the nodes create the encryption key; the subsequent encryption and transmission of information is entirely classical. A true quantum network would be able to harness entanglement and teleportation to transmit quantum information over long distances, without the need for vulnerable trusted nodes.

One of the main motivations for building such networks is to enable quantum computers to talk to each other, both between countries and across a single room. The number of qubits that can be packed into any one computing system may be limited, so networking the systems together could help physicists to scale them up. "At this point, it's fair to say that probably you'll be able to build a quantum computer with maybe a couple of hundred qubits," says Mikhail Lukin, a physicist at Harvard University in Cambridge, Massachusetts. "But beyond that, the only way to do this is use this modular approach, involving quantum communications."

On a larger scale, researchers envision a quantum-computing cloud,

NIK SPENCER/*NATURE*

with a few highly sophisticated machines that are accessible through a quantum internet from most university labs. "The extra cool thing is that such cloud quantum computing is also secure," says Ronald Hanson, an experimental physicist at Delft. "People at the server are unable to know what kind of program you're running and the data you have."

Researchers have come up with a plethora of other proposals for Internet applications — such as auctions, elections, contract negotiations and speed trading — that could exploit quantum phenomena to be faster or more secure than their classical counterparts.

But the biggest impact of a quantum internet could be on science itself. Synchronizing clocks using entanglement could improve the precision of Global Positioning System-like navigation networks from metres to millimetres, some researchers say. And Lukin and others have proposed using entanglement to combine distant atomic clocks into a single clock with vastly improved precision, which he says could lead to new ways of detecting gravitational waves, for example. In astronomy, quantum networks might link distant optical telescopes across thousands of kilometres, to effectively give them the resolution of one dish spanning the same distance. This process, called very long baseline interferometry, is applied routinely in radio astronomy, but operating in optical frequencies requires timing precision that is currently out of reach.

SPOOKY SECURITY

In the past decade or so, experiments pioneered by Christopher Monroe[6], a physicist at the University of Maryland in College Park, and others have demonstrated some of the fundamentals needed to build a truly quantum network, such as teleporting information encoded in qubits from one place to another (see 'Creating a quantum internet').

To see how teleportation (also proposed by Bennett and Brassard[7]) works, imagine two users: Alice and Bob. Alice holds a qubit, which could be a trapped ion or some other quantum system, and wants to transfer the information stored in it to Bob. As luck would have it, Alice and Bob come into possession of two 'proxy' particles — also qubits — that are entangled with each other. If Alice can entangle her qubit and proxy particle, the qubit will, by extension, also become entangled with Bob's particle. To do so, Alice performs a particular kind of joint measurement on her two particles. She then shares the results of that measurement (which are ordinary, classical data) with Bob. To complete the teleportation process, Bob then uses that information to manipulate his particle so that it ends up in the same state as Alice's qubit originally was.

For practical purposes, it doesn't matter how Alice and Bob obtain the entangled proxy particles. They could be individual atoms delivered in a briefcase, say, or photons beamed to the pair by a third party. (One of Micius's experiments last year sent entangled pairs of photons to two ground stations in China over a record distance of more than 1,200 kilometres.) Alice and Bob could also entangle the qubits they hold, by sending photons out to interact at a third location.

The beauty of quantum teleportation is that the quantum information does not technically travel along the network. The photons that do travel are just used to establish a link between Alice and Bob so that quantum information can then be transferred. If one pair of entangled photons fails to establish a connection, another pair will. This means that the quantum information is not lost if photons are.

LINK AND REPEAT

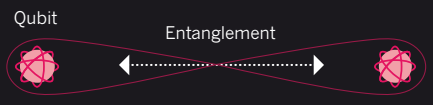
A quantum internet would be able to produce entanglement on demand between any two users. Researchers think that this will involve sending photons through both fibre-optic networks and satellite links. But connecting distant users will require a technology that can extend the reach of entanglement — relaying it from user to user and along intermediate points.

One way in which such a quantum repeater could work was proposed in 2001 by Lukin and his collaborators[8]. In their scheme, small quantum computers that can store qubits and do simple operations on them are used to entangle a qubit at an upstream station with one downstream.

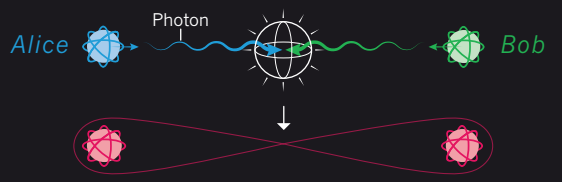
CREATING A QUANTUM INTERNET

Researchers expect that a fully quantum network will need to establish entangled links between any two users. Quantum information will then be teleported from one to the other, transferring the information without transmitting it over the network.

ESTABLISHING ENTANGLEMENT

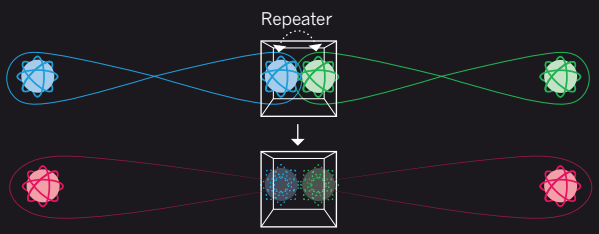


Entanglement links distant particles, so that if one changes state, so does the other. Entangled quantum bits, or qubits, effectively form a quantum communication channel that spans any distance.



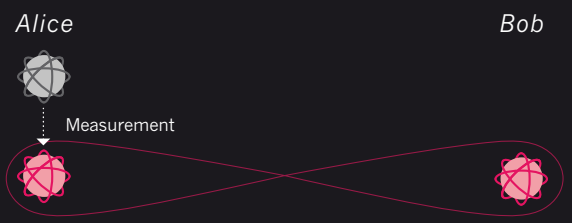
To create a link, Alice can emit a photon towards Bob from her qubit. Bob does the same towards Alice. Because the photons are entangled with their original qubits, when they interact, Alice's and Bob's qubits become entangled, too.

LONG-DISTANCE LINKS

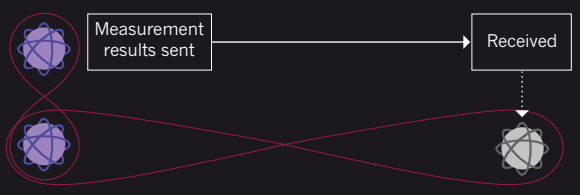


If Alice and Bob are far away from one another or not directly connected, one or more quantum repeaters will be needed to establish entanglement. Here, one qubit in the repeater is entangled with Alice's qubit, and the other with Bob's. By performing an operation on the two qubits it holds, the repeater creates entanglement between Alice's and Bob's qubits.

TELEPORTING INFORMATION



If Alice then wants to transmit quantum information over the connection, she can perform a particular kind of measurement on her entangled qubit (pink) and the qubit whose state she wants to teleport (grey). The grey qubit is now entangled with Alice's other particle and with Bob's.



Alice then sends information about the measurement to Bob, which can be done over the conventional Internet. With that information, Bob can perform an operation on his qubit that places it in the same state as Alice's second qubit was originally. The quantum state of Alice's particle — its quantum information — has been teleported.

MARCEL WOGRAM FOR *NATURE*

Part of an experiment to investigate diamond-based systems as quantum-internet nodes at Delft University of Technology in the Netherlands.

Repeated application of this 'entanglement swapping' process along a path in a network would eventually produce entanglement between any two users.

In 2015, Hanson and his collaborators showed how to build one leg of a network when they linked two qubits built from single-atom impurities in diamond crystals and separated by 1.3 kilometres[9]. Photons emitted by the two qubits travelled towards an intermediate station, where they then interacted, establishing entanglement. "It shows that one can really establish entanglement — strong, reliable entanglement — between two distant quantum-information processors," says Seth Lloyd, a physicist at the Massachusetts Institute of Technology in Cambridge.

Researchers are investigating other ways to construct and manipulate qubits, including using individual ions suspended in a vacuum — pioneered by Monroe and others — as well as systems that pair up atoms and photons bouncing between two mirrors inside a cavity.

Like Hanson's diamond system, these qubits could be used to build both quantum repeaters and quantum computers. Fortunately for people hoping to ramp up quantum communications, the requirements for a repeater may be less demanding than those for a fully fledged quantum computer. Iordanis Kerenidis, a quantum-computation researcher at the University of Paris Diderot, made this argument at a workshop on quantum repeaters in Seefeld, Austria, last September. "If you tell experimentalists that you need 1,000 qubits, they are going to laugh," he said. "If you tell them you need ten — well, they laugh less."

The prospect of creating a quantum internet is now becoming a problem of systems engineering. "From an experimental point of view, people have demonstrated various building blocks" for quantum networks, says Tracy Northup, a physicist at Austria's University of Innsbruck whose team works on cavity qubits and is part of Wehner's pan-European Quantum Internet Alliance. "But putting them together in one place — we all see how challenging it is," Northup says.

For the moment, Wehner's alliance is still at an early stage and looking for public funding as well as corporate partners. In the meantime, the Dutch demonstration network — which Wehner co-leads with Hanson and Erwin van Zwet, a joint systems engineer at the Dutch research organization, TNO — has been moving forward. Hanson and his colleagues have been improving the speed of their systems, which in the 2015 experiment entangled just 245 qubit pairs over the equivalent of about 9 days. Another crucial challenge has been to reliably convert photons from the visible wavelengths that come out of the diamond qubits to longer, infrared ones that can travel well along optical fibres; this is tricky because the new photon still has to carry the quantum information of the old one, but without the possibility of cloning it. Earlier this year, Hanson and his colleagues achieved this by making photons interact with a laser beam of longer wavelength[10]. That technique would enable qubits to be linked over distances of tens of kilometres over fibre.

Hanson's team is now building a link between Delft and The Hague, a good 10 kilometres away. By 2020, the researchers hope to have connected up four Dutch cities, with a station at each site acting as a quantum repeater. If successful, the project would be the world's first genuine quantum-teleportation network. The group aims to open it up to other teams interested in performing quantum-communications experiments remotely, much like IBM's Quantum Experience, which allows remote users access to a rudimentary quantum computer.

The network could be a test bed for researchers hoping to fix some of the Internet's flaws, not least the ease with which users can forge or steal identities. "The idea that you could join a network without establishing identity is a problem from early on," said Robert Broberg, a network engineer from the telecommunications equipment giant CISCO, at the Seefeld meeting. Wehner and others have proposed quantum techniques that would allow users to prove their identity by certifying that they own the correct secret code (a series of classical bits) without ever transmitting it. Instead, the user and the server use the code to create a sequence of qubits and send them to a 'black box' in between. The black box — which could be, say, a cash machine — can then compare the two sequences to see whether they match, without ever knowing the underlying code.

But some researchers caution against overselling the potential reach of the technology. "Today's Internet will never be entirely quantum, no more than computers will ever be all-quantum," says Nicolas Gisin, a physicist at the University of Geneva in Switzerland and a co-founder of ID Quantique. And it could be that many of the things people hope to achieve with quantum networks could be done with more conventional technologies. "Sometimes, something looks like a great idea at first, and then it turns out to be easily achievable without a quantum effect," says Norbert Lütkenhaus, a physicist at the University of Waterloo in Canada who is helping to develop standards for the future quantum internet.

Time will tell whether the promise of the quantum internet will materialize. As far as we know, teleportation is a phenomenon that, although physically possible, does not occur in nature, Zeilinger says. "So this is really new for humanity. It might take some time."

Wehner's familiarity with both physics and network security has made her a point of reference for people in the field. And after having done much work on hard-core quantum theory, she is relishing the opportunity to shape these future networks. "For me," she says, "this is really full circle." ■

Davide Castelvecchi *is a senior reporter for* Nature *in London.*

1. Bouwmeester, D. *et al. Nature* **390,** 575–579 (1997).
2. Wiesner, S. *SIGACT News* **15,** 78–88 (1983).
3. Bennett, C. H. & Brassard, G. *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* **1,** 175–179 (1984).
4. Bennett, C. H. & Brassard, G. *SIGACT News* **20,** 78–80 (1989).
5. Liao, S.-K. *et al. Phys. Rev. Lett.* **120,** 030501 (2018).
6. Moehring, D. L. *et al. Nature* **449,** 68–71 (2007).
7. Bennett, C. H. *et al. Phys. Rev. Lett.* **70,** 1895–1899 (1993).
8. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. *Nature* **414,** 413–418 (2001).
9. Hensen, B. *et al. Nature* **526,** 682–686 (2015).
10. Dréau, A., Tcheborateva, A., El Mahdaoui, A., Bonato, C. & Hanson, R. Preprint at https://arxiv.org/abs/1801.03304 (2018).

CORRECTION

The News Feature 'The Entangled Web' (*Nature* **554,** 289–292; 2018) misstated the leadership of the Dutch demonstration quantum network. The project is co-led by Ronald Hanson and Stephanie Wehner of Delft University of Technology in the Netherlands and Erwin van Zwet at the Dutch research organization TNO in The Hague.