technologyreview.com

Inside Europe’s quest to build an unhackable quantum internet

11-14 minutes

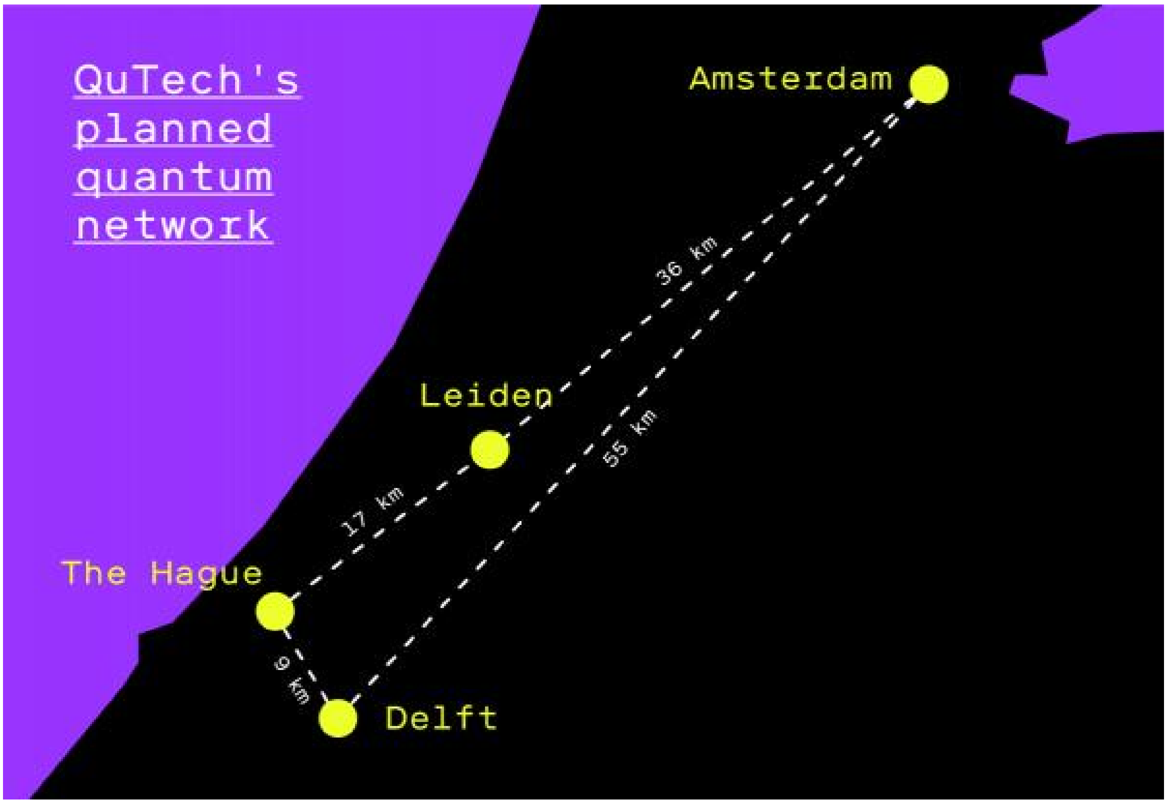
The fast train from Paris to Rotterdam was an hour late leaving the Gare du Nord. When it finally deposited me in the Dutch city, I discovered that the onward train to Delft had been suspended because of maintenance work on the tracks. It took two circuitous bus journeys and a taxi ride before I finally made it to my destination.

Given that I was there to learn about the future of communications, this seemed appropriate. My trip was a reminder that while shipping people from place to place is still fraught with unforeseen glitches, gargantuan amounts of data flow smoothly and swiftly all day, every day through the fiber-optic cables connecting cities, countries, and entire continents.

And yet these data networks have a weakness: they can be hacked. Among the secret documents leaked a few years ago by US National Security Agency contractor Edward Snowden were ones showing that Western intelligence agencies had managed to tap into communication cables and spy on the vast amounts of traffic flowing through them.

The research institute I was visiting in Delft, QuTech, is working on a system that could make this kind of surveillance impossible. The idea is to harness quantum mechanics to create a flawlessly secure communications network between Delft and three other cities in the Netherlands by the end of 2020 (see map below for the planned links).

The QuTech researchers, led by Stephanie Wehner and Ronald Hanson, still face a number of daunting technical challenges. But if they succeed, their project could catalyze a future quantum internet—in much the same way that Arpanet, which the US Department of Defense created in the late 1960s, inspired the creation of the internet as we know it today.



Inimitable qubits

The internet is vulnerable to the kind of hacking revealed by Snowden because data still travels over cables in the form of classical bits—a stream of electrical or optical pulses representing *1*s and *0*s. A hacker who manages to tap into the cables can read and copy those bits in transit.

The laws of quantum physics, on the other hand, allow a particle—for example, an atom, an electron, or (for transmitting along optical cables) a photon of light—to occupy a quantum state that represents a combination of *1* and *0* simultaneously. Such a particle is called a quantum bit, or qubit. When you try to observe a qubit, its state "collapses" to either *1* or *0*. This, explains Wehner, means that if a hacker taps into a stream of qubits, the intruder both destroys the quantum information in that stream and leaves a clear signal that it's been tampered with.

Because of this property, qubits have been used for quite some time to generate encryption keys in a process known as quantum key distribution (QKD). This involves sending data in classical form over a network, while the keys needed to decrypt the data are transmitted separately in a quantum state.

China has demonstrated some impressive applications of QKD. Last year, it used a satellite called Micius to transmit quantum keys to two ground stations, one in Beijing and the other in Vienna. The keys were then used to decrypt classical data for a secure video call between the two cities. Any attempt to intercept the communication containing the keys would have destroyed them, making it impossible for the spies (or anyone else) to decrypt the video call. China has also built a land-based QKD communications network from Beijing to Shanghai that banks and other companies are using to transmit sensitive commercial data.

However, the approach has limitations. Photons can be absorbed in the atmosphere or by materials in cables, which means they can typically travel for no more than a few tens of kilometers. The Beijing-Shanghai network gets around this by having 32 so-called "trusted nodes" at various points along it—similar to repeaters that amplify the signal in an ordinary data cable. At these nodes, keys are decrypted into classical form and then re-encrypted in a fresh quantum state for their journey to the next waypoint. But this means trusted nodes really shouldn't be trusted. A hacker who breaches their security could copy the classical keys undetected, as could a company or government running the nodes.

Quantum teleportation

Wehner, Hanson, and their colleagues at QuTech aim to overcome these limitations to build a completely secure quantum internet.

The approach they're using is called quantum teleportation. This may sound like science fiction, but it's an actual method of transmitting data. It relies on a phenomenon known as quantum entanglement.

Entanglement means creating a pair of qubits—photons of light, for this purpose—in a single quantum state, so that even if they travel off in opposite directions, they retain a quantum connection. Changing the state of one photon will instantaneously change the state of the other one in a predictable way, no matter how far apart they are. Albert Einstein called this "spooky action at a distance."

Quantum teleportation, then, requires first sending a pair of entangled photons to two people—call them Alice and Bob. Alice receives her entangled photon and lets it interact with a "memory qubit" that holds data she wants to transmit to Bob. This interaction changes the state of her photon, and thus changes the state of Bob's photon too. In effect, this "teleports" the data in Alice's memory qubit from Alice's photon to Bob's. The illustration below lays out the process in a little more detail.

Another way to think of it: the entangled pair of photons are like the two ends of a virtual, one-time-only data cable. Each time Alice and Bob want to send data, they first receive a new cable, and because each of them holds one end, only they can use it. That's what makes it secure from eavesdropping.

There are various ways in practice to create entangled qubits. Hanson, who heads the hardware side of QuTech's initiative, uses microscopic synthetic diamonds with a deliberate flaw in them known as a nitrogen vacancy defect. This defect can be manipulated using light and microwaves to emit photons that can be sent to distant locations.

Getting this to scale, however, is a massive scientific and engineering challenge, as Hanson readily acknowledges. "We can try to make long-distance entanglement, but it fails most of the time," he says. Given that fiber-optic cables sometimes take roundabout routes, the distances the photons will have to travel in the QuTech project will likely be longer than the direct ones shown on our map.

Still, there's been encouraging progress. Back in 2015, Hanson and a group of other researchers managed to entangle qubits 1.3 kilometers (0.8 miles) apart, but the connection could be established only once an hour and lasted for a fraction of a second. In June of this year, the researchers announced they had entangled two electrons a couple of meters apart 40 times per second. This made them the first in the world to show that entanglement on demand is possible.

Laser wave-maker

That experiment took place in a laboratory. Replicating it in the real world is another matter. The technical hurdles include not only speeding up entanglement and maintaining it over much longer distances, but also performing a delicate physics trick that uses laser pulses to increase photons' wavelengths so they can travel farther over fiber-optic cables.

While Hanson is focused on these challenges, Wehner has been leading the network design and software innovation needed to make the four-city linkup a reality. Software used to control classical communication networks can't cope with things like entanglement, so Wehner has been working on a novel architecture that will make it possible to control the new quantum network efficiently and build applications for it.

At a recent hackathon that QuTech organized jointly with Europe's regional internet registry, the applications suggested included secure voting, digital signatures, and even a quantum chat service.

The QuTech team seems determined to meet its target of completing the four-city network by the end of 2020, though Wehner admits that deadline is "super tight." What they learn will inform a recently launched European project, the Quantum Internet Alliance (QIA). Wehner is coordinating the alliance, whose goal is to "build a quantum internet that enables quantum communication applications between any two points on Earth."

That's ambitious, to say the least. While the Netherlands is a useful test bed, the distances between cities there are pretty small. Bigger networks are likely to require "quantum repeaters." Unlike the "trusted nodes" in China's network, which turn quantum information into classical form and then back again, these repeaters, or way stations with quantum processors, will be needed to extend entanglement over thousands of miles so that networks remain impervious to hackers.

Stephanie Wehner and Ronald Hanson

Various researchers, including a team at QuTech, are working on this idea, but it's still in its infancy. "There's a lot of beautiful theory out there," says Tracy Northup, a professor at the University of Innsbruck who's also involved with the QIA, "but there’s not even a proof of principle in the lab yet.”

Assuming a quantum internet becomes a reality, it will raise important questions. Will it be available to everyone, or will deep-pocketed companies and governments use quantum lanes while others are consigned to less secure classical ones? And will governments start insisting they need special access points into quantum networks, just as they agitate now for back doors into software and smartphones?

If the QuTech team can overcome the technical hurdles it faces, we’re going to get a big step closer. And the researchers in the Netherlands aren’t the only ones to keep an eye on. China is hatching a plan for a fully quantum communications network that would link the city of Zhuhai with Hong Kong. And with Micius and their existing land-based network, the Chinese have shown just how quickly they can advance. The race toward a quantum internet is well and truly on.