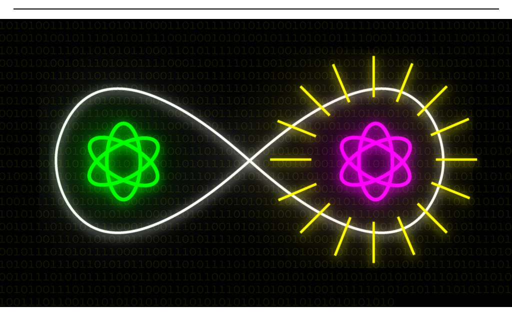
Computing / Quantum Computing

Explainer: What is quantum communication?

Researchers and companies are creating ultra-secure communication networks that could form the basis of a quantum internet. This is how it works.

by Martin Giles

Feb 14, 2019



***This is the second in a series of explainers on quantum** technology. The other two are on quantum computing and post-quantum cryptography.*

Barely a week goes by without reports of some new mega-hack that's exposed huge amounts of sensitive information, from people's credit card details and health records to companies' valuable intellectual property. The threat posed by cyberattacks is forcing governments, militaries, and businesses to explore more secure ways of transmitting information.

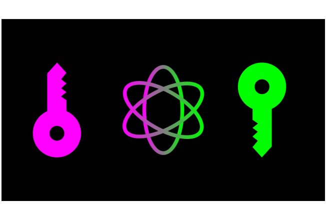
Sign up for **The Download** — your daily dose of what's up in emerging technology
Enter your email | Sign up
Also stay updated on MIT Technology Review initiatives and events? Yes No

Today, sensitive data is typically encrypted and then sent across fiber-optic cables and other channels together with the digital "keys" needed to decode the information. The data and the keys are sent as classical bits—a stream of electrical or optical pulses representing *1*s and *0*s. And that makes them vulnerable. Smart hackers can read and copy bits in transit without leaving a trace.

Quantum communication takes advantage of the laws of quantum physics to protect data. These laws allow particles—typically photons of light for transmitting data along optical cables—to take on a state of superposition, which means they can represent multiple combinations of *1* and *0* simultaneously. The particles are known as quantum bits, or qubits.

The beauty of qubits from a cybersecurity perspective is that if a hacker tries to observe them in transit, their super-fragile quantum state "collapses" to either *1* or *0*. This means a hacker can't tamper with the qubits without leaving behind a telltale sign of the activity.

Some companies have taken advantage of this property to create networks for transmitting highly sensitive data based on a process called quantum key distribution, or QKD. In theory, at least, these networks are ultra-secure.



What is quantum key distribution?

QKD involves sending encrypted data as classical bits over networks, while the keys to decrypt the information are encoded and transmitted in a quantum state using qubits.

Various approaches, or protocols, have been developed for implementing QKD. A widely used one known as BB84 works like this. Imagine two people, Alice and Bob. Alice wants to send data securely to Bob. To do so, she creates an encryption key in the form of qubits whose polarization states represent the individual bit values of the key.

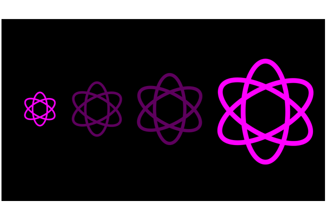
The qubits can be sent to Bob through a fiber-optic cable. By comparing measurements of the state of a fraction of these qubits—a process known as "key sifting"—Alice and Bob can establish that they hold the same key.

As the qubits travel to their destination, the fragile quantum state of some of them will collapse because of decoherence. To account for this, Alice and Bob next run through a process known as "key distillation," which involves calculating whether the error rate is high enough to suggest that a hacker has tried to intercept the key.

If it is, they ditch the suspect key and keep generating new ones until they are confident that they share a secure key. Alice can then use hers to encrypt data and send it in classical bits to Bob, who uses his key to decode the information.

We're already starting to see more QKD networks emerge. The longest is in China, which boasts a 2,032-kilometer (1,263-mile) ground link between Beijing and Shanghai. Banks and other financial companies are already using it to transmit data. In the US, a startup called Quantum Xchange has struck a deal giving it access to 500 miles (805 kilometers) of fiber-optic cable running along the East Coast to create a QKD network. The initial leg will link Manhattan with New Jersey, where many banks have large data centers.

Although QKD is relatively secure, it would be even safer if it could count on quantum repeaters.



What is a quantum repeater?

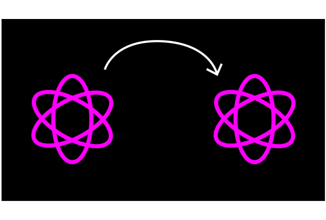
Materials in cables can absorb photons, which means they can typically travel for no more than a few tens of kilometers. In a classical network, repeaters at various points along a cable are used to amplify the signal to compensate for this.

QKD networks have come up with a similar solution, creating "trusted nodes" at various points. The Beijing-to-Shanghai network has 32 of them, for instance. At these waystations, quantum keys are decrypted into bits and then reencrypted in a fresh quantum state for their journey to the next node. But this means trusted nodes can't really be trusted: a hacker who breached the nodes' security could copy the bits undetected and thus acquire a key, as could a company or government running the nodes.

Ideally, we need quantum repeaters, or waystations with quantum processors in them that would allow encryption keys to remain in quantum form as they are amplified and sent over long distances. Researchers have demonstrated it's possible in principle to build such repeaters, but they haven't yet been able to produce a working prototype.

There's another issue with QKD. The underlying data is still transmitted as encrypted bits across conventional networks. This means a hacker who breached a network's defenses could copy the bits undetected, and then use powerful computers to try to crack the key used to encrypt them.

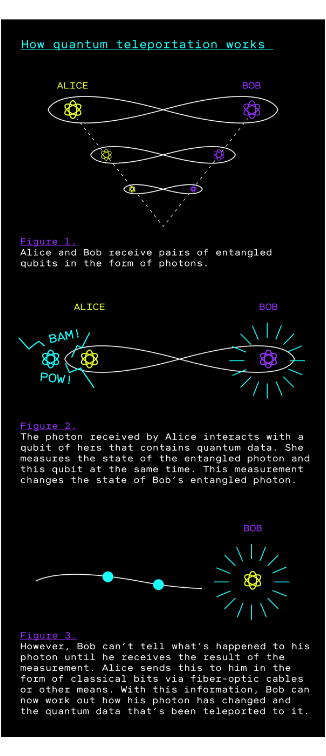
The most powerful encryption algorithms are pretty robust, but the risk is big enough to spur some researchers to work on an alternative approach known as quantum teleportation.



What is quantum teleportation?

This may sound like science fiction, but it's a real method that involves transmitting data wholly in quantum form. The approach relies on a quantum phenomenon known as entanglement.

Quantum teleportation works by creating pairs of entangled photons and then sending one of each pair to the sender of data and the other to a recipient. When Alice receives her entangled photon, she lets it interact with a "memory qubit" that holds the data she wants to transmit to Bob. This interaction changes the state of her photon, and because it is entangled with Bob's, the interaction instantaneously changes the state of his photon too.

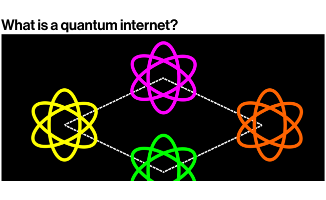


In effect, this "teleports" the data in Alice's memory qubit from her photon to Bob's. The graphic below lays out the process in a little more detail:

Researchers in the US, China, and Europe are racing to create teleportation networks capable of distributing entangled photons. But getting them to scale will be a massive scientific and engineering challenge. The many hurdles include finding reliable ways of churning out lots of linked photons on demand, and maintaining their entanglement over very long distances—something that quantum repeaters would make easier.

Still, these challenges haven't stopped researchers from dreaming of a future quantum internet.

What is a quantum internet?



Just like the traditional internet, this would be a globe-spanning network of networks. The big difference is that the underlying communications networks would be quantum ones.

It isn't going to replace the internet as we know it today. Cat photos, music videos, and a great deal of non-sensitive business information will still move around in the form of classical bits. But a quantum internet will appeal to organizations that need to keep particularly valuable data secure. It could also be an ideal way to connect information flowing between quantum computers, which are increasingly being made available through the computing cloud.

China is in the vanguard of the push toward a quantum internet. It launched a dedicated quantum communications satellite called Micius a few years ago, and in 2017 the satellite helped stage the world's first intercontinental, QKD-secured video conference, between Beijing and Vienna. A ground station already links the satellite to the Beijing-to-Shanghai terrestrial network. China plans to launch more quantum satellites, and several cities in the country are laying plans for municipal QKD networks.

Some researchers have warned that even a fully quantum internet may ultimately become vulnerable to new attacks that are themselves quantum based. But faced with the hacking onslaught that plagues today's internet, businesses, governments, and the military are going to keep exploring the tantalizing prospect of a more secure quantum alternative.

Share | Link
Tagged Computing, Quantum Communications, Quantum Computing
Author Martin Giles

Popular
01. The AI technique that could imbue machines with the ability to reason
02. Explainer: What is post-quantum cryptography?
03. Facebook's new poker-playing AI could wreck the online poker industry—so it's not being released

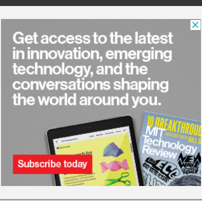
Special issue: space July/August 2019
Who gets to send radio waves in space?
Satellites aren't much use if they can't communicate

Humans and Technology 2h
A biotech startup is making cow-free ice cream. Would you eat it?
Perfect Day says it's figured out how to make ice cream that's creamy without any animal protein.
A company called Perfect Day has announced that after five years and $60 million in venture backing, it's created ice cream made of whey protein harvested from genetically modified yeast....
Expand

Artificial Intelligence 2h
Watch this robot do the Bottle Cap Challenge—and show a new way to control machines
It isn't quite a roundhouse kick, but check out the robot above in a simpler version of the "Bottle Cap Challenge." (If you haven't come across this yet, it consists of people trying to kick the top...
Expand

Artificial Intelligence 3h
The AI technique that could imbue machines with the ability to reason
Read more

TR 35 2019
Innovators Under 35 | 2019
It's part of our ethos that technology can and should be a force for good. In these profiles you'll find people employing innovative methods to treat disease, to fight online harassment, and to create the next big battery breakthrough.
Rediet Abebe — She uses algorithms and AI to fight socioeconomic inequality
Tim Ellis — He developed a massive 3D metal printer—for building an entire rocket
Ritu Raman — She's develope[d] robots made [of] tissue and mus[cle]



SPONSORED
Excelling in the new data economy
Effectively managing the massive influx of data is a matter of rethinking data management tactics and technologies.
Read more
Produced in association with Intel

Silicon Valley Jul 12
Humans might be listening to your Google Assistant recordings
Google's privacy policy page makes no mention of the fact human contractors listen to some of the recordings....
Expand

Libra backlash Jul 12
Even Donald Trump is dumping on Facebook's digital-currency dreams
Read more