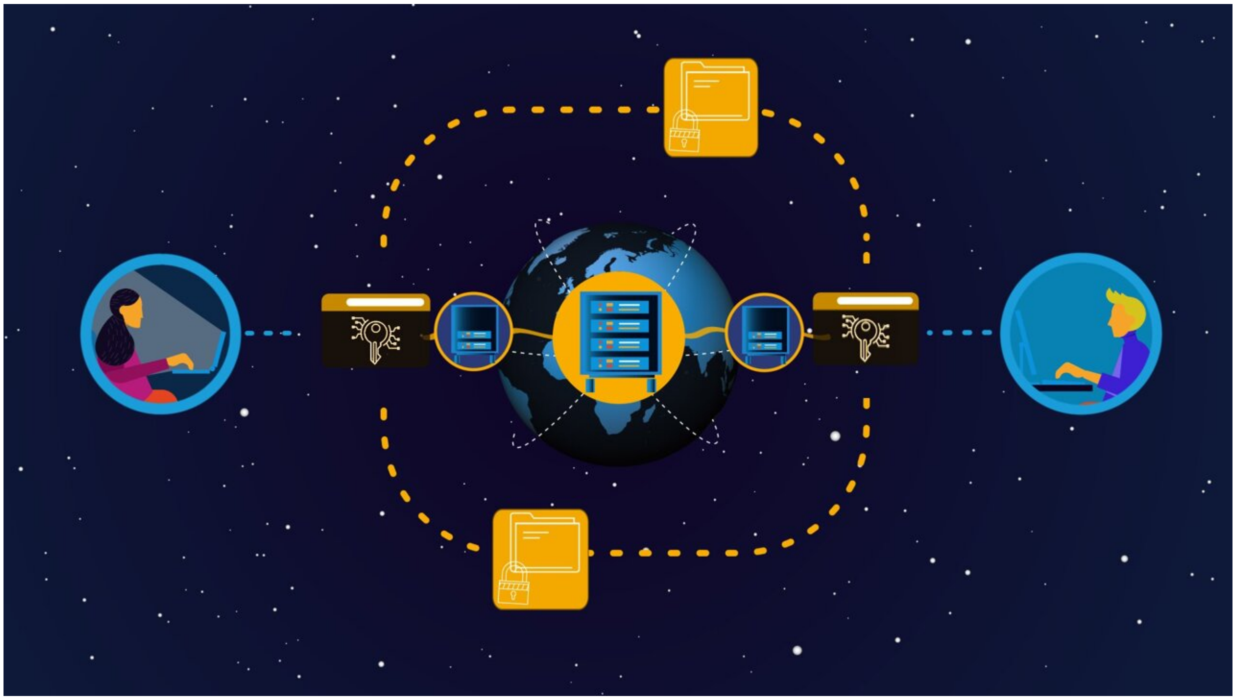
Untappable communication becomes practical with new system in future quantum internet

July 7 2021, by Gerd de Smyter



Alice & Bob can use quantum keys to communicate and send files securely using an MDI-QKD key. Credit: QuTech (Vincent de Mees, Slim Plot)

Engineers from QuTech (a collaboration between TU Delft and TNO) can provide untappable communication that is cost-scaling to many users by using measurement-device independent (MDI) quantum key distribution (QKD). A notable side-feature is that, courtesy of Cisco, conventional internet operaltes in parallel, on the same optical fiber from Dutch telecom provider KPN. MDI-QKD is an important step towards an accessible quantum internet.

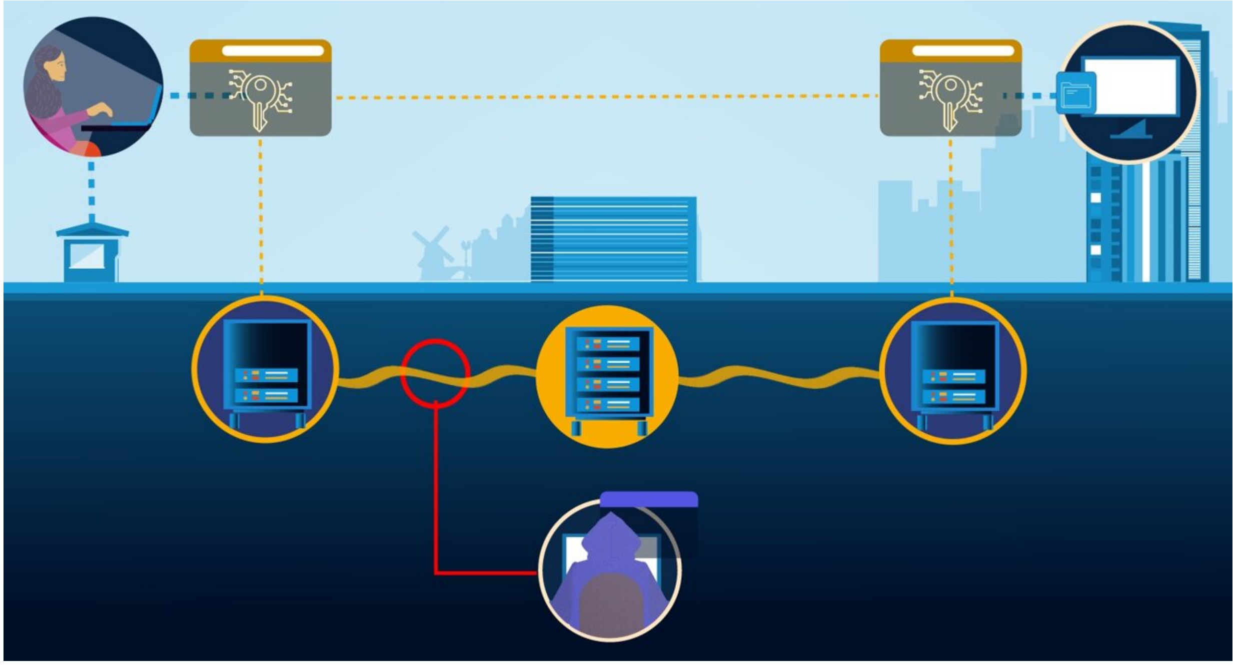
Presently secure communication is based on the fact that breaking cryptography is slow using conventional computers. This includes communication between datacentres, inter-governmental communication, or critical infrastructure like banking, energy and airports. Some communication lines require secrecy by law or by the user. Any attacker could be recording these messages and then decrypting them later. Unfortunately, computers are becoming faster, even more so with the impending introduction of quantum computers.

Ultimate defense against eavesdropping

Joshua Slater, team lead of the MDI-QKD project: "Important conventional cryptographic methods rely on, for example, a public and a private key. These two keys are essentially two large numbers that belong together. Their security is based on the fact that the private key is difficult and slow to calculate with knowledge of only the public key. Unfortunately, with the introduction of very powerful computers (such as quantum computers), calculating the private key becomes trivially easy and then encryption can become insecure."

A solution to eavesdropping—now and in the future—is the use of quantum key distribution (QKD). In quantum communication, eavesdropping on a message disturbs transmission of the quantum key. Slater: "If the quantum signals are disturbed, the users know not to use the generated key for their secure communication line. Once the quantum key is successfully shared with the intended recipient, the rest of the secure communication benefits from 'forward secrecy': the assurance that the key distribution cannot be cracked now or in the future."

"Unfortunately, current commercially available QKD systems are difficult to scale in a network," Slater explained. "To solve all these problems, we've built a measurement-device independent (MDI) QKD system, in which multiple users can be connected via a central node that operates like a typical telephone switch board operator. Importantly, the central node does not need to be trusted. The entire system is designed such that hacking attacks against the central node cannot break the security of the protocol."



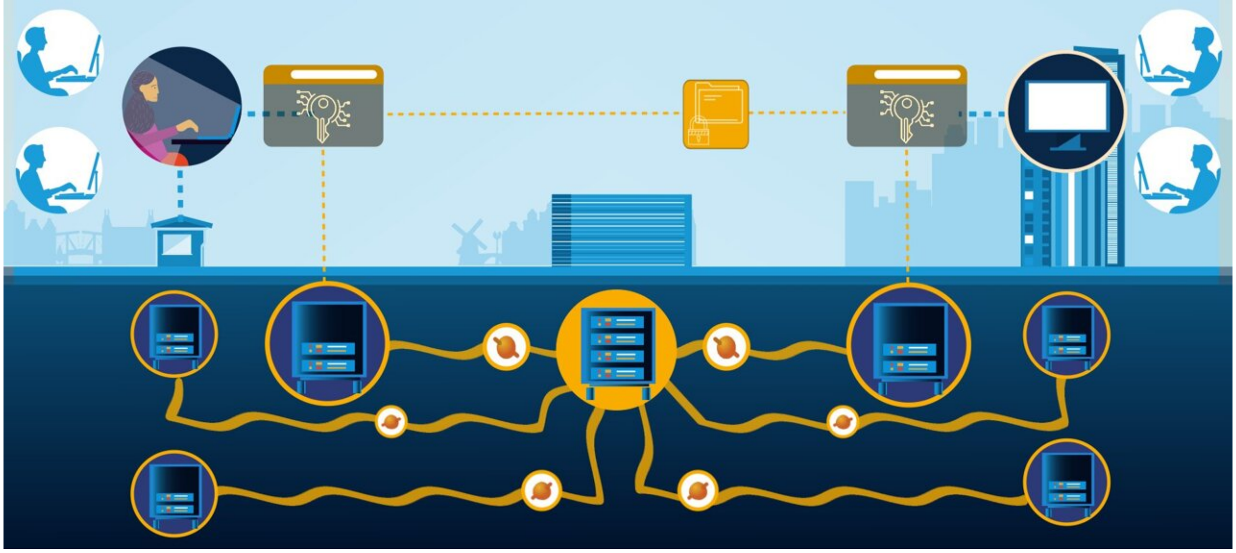
Because of the quantum key distribution (QKD) used by Alice & her bank, a hacker cannot eavesdrop on them. Also, the central node doesn't have to be trusted for Alice & her bank to communicate securely. Credit: QuTech (Vincent de Mees, Slim Plot)

Scalable quantum networks

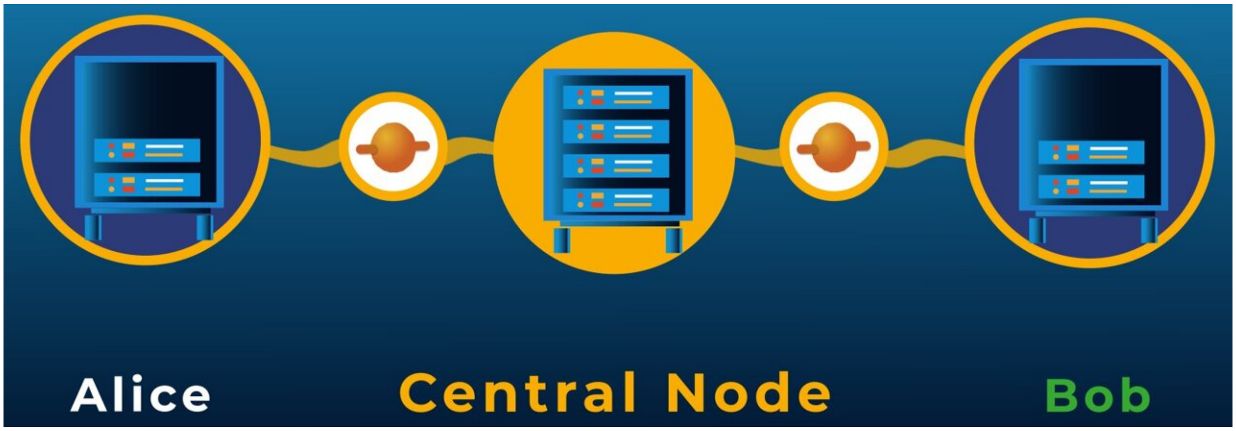
Slater: "A major advantage of our system over other QKD systems is its scaling to many users. Our MDI-QKD can be used in a star-type physical network. Researchers at QuTech have already previously performed the first proof-of-principle demonstration of MDI-QKD, the first demonstration over deployed fibers, and the first demonstration using cost-effective, off-the-shelf hardware."

"A significant achievement that we're demonstrating here for the first time, is that our quantum signals are transmitted over the same fiber as conventional internet traffic," said Slater. "Using standard equipment that Cisco supplied and configured with us, we established two multiplexed internet networks between the locations over the same optical fibers. The existence of these two networks do not impact the performance of our quantum system. Essentially, we've shown how our systems can coexist, in parallel"

"This is an important development in guaranteeing the security of internet traffic in the future," said Babak Fouladi, Chief Digital and Technology Officer and member of the Executive Board at KPN. "I am pleased that we can contribute towards making this insight practical using the network of the Netherlands. Solutions like MDI-QKD should not only protect users today, but also make communication as future-proof as possible."



Because of the measurement-device independent (MDI) system the whole network is rather easy to scale up to many users. Credit: QuTech (Vincent de Mees, Slim Plot)



Alice is a standard telco rack located at the Delft University of Technology (the Netherlands), the central node in a neighbouring city Rijswijk, and Bob is at KPN in The Hague. Credit: QuTech (Vincent de Mees, Slim Plot)

Demonstration in Delft–Rijswijk–The Hague

The current system consists of three standard telco racks, each in a different city in the Netherlands. The first 'user' connected to the demo setup is code-named Alice and resides in Delft. The second user, called Bob, sits in a KPN building in The Hague. The central node, Charlie, is located in between. Every user is connected to the center node by a standard optical fiber. Furthermore, the users and the central node are able to communicate over the normal internet, either directly via the (same) optical fiber, or indirectly via any internet connection.

Finally, the MDI-QKD deployment represents an important step towards a future quantum internet. The network is designed to be upgradable in the future: users like Alice and Bob can upgrade their functionality (with e.g. quantum processors, quantum repeaters, quantum entanglement, quantum memory, quantum computers, whatever), while the central node and the rest of the network remains the same. The network is future-proof and ready to be upgraded for the quantum future.

"This is a great milestone, and an important foundation for the deployment of a national quantum network infrastructure in the Netherlands. That is one of the main goals of the Netherlands' National Agenda Quantum Technology, which is being executed by Quantum Delta NL," said Jesse Robbers, director of Quantum Delta NL—which received €615 million from the Dutch government in April of this year.

Provided by Delft University of Technology

Citation: Untappable communication becomes practical with new system in future quantum internet (2021, July 7) retrieved 24 April 2024 from https://phys.org/news/2021-07-untappable-future-quantum-internet.html