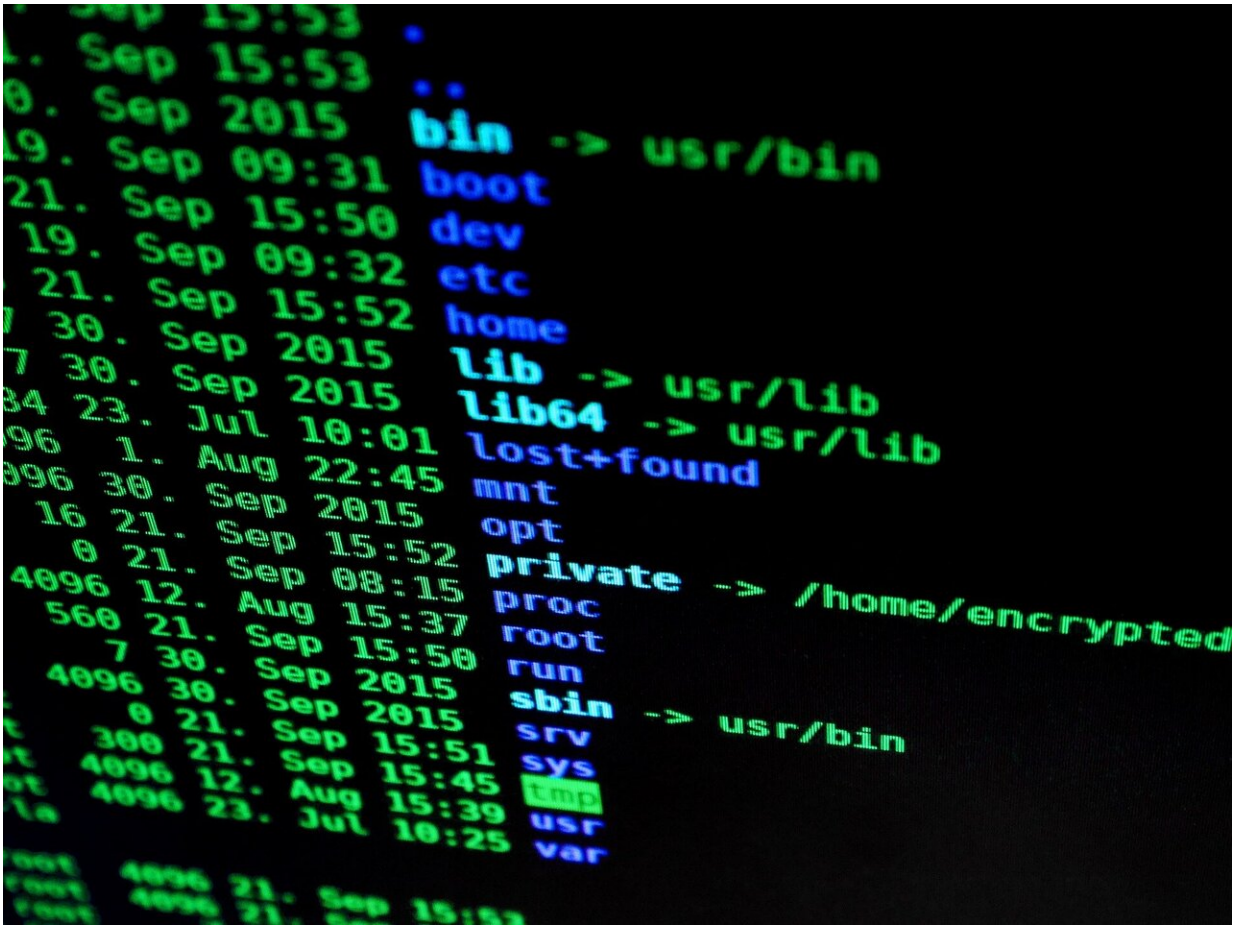
Quantum—a double-edged sword for cryptography

June 11 2019, by Jon Cartwright, From Horizon Magazine



Cryptography that would be impossible for a regular computer to crack, would take a quantum computer just seconds. Credit: Pixabay/ joffi, licensed under pixabay license

Quantum computers pose a big threat to the security of modern communications, deciphering cryptographic codes that would take regular computers forever to crack. But drawing on the properties of quantum behaviour could also provide a route to truly secure cryptography.

Defence, finance, social networking—communications everywhere rely on cryptographic security. Cryptography involves jumbling up messages according to a code, or key, that has too many combinations for even very powerful computers to try out.

But quantum computers have an advantage. Unlike regular computers, which process information in 'bits' of definite ones and zeros, quantum computers process information in 'qubits," the states of which remain uncertain until the final calculation.

The result is that a quantum computer can effectively try out many different keys in parallel. Cryptography that would be impenetrable to regular computers could take a quantum computer mere seconds to crack.

Practical quantum computers that can be used to break encryption are expected to be years, if not decades, away. But that should not be of any reassurance: even if a hacker cannot decipher confidential information now, they could save it and simply wait until a quantum computer is available.

"The problem already exists," said Professor Valerio Pruneri of the Institute of Photonic Sciences in Barcelona, Spain, and the coordinator of a quantum security project called CiViQ. "A hacker can take what is stored now, and break its key at a later date."

The answer, says Prof. Pruneri, is another quantum technology. Known

as quantum key distribution (QKD), it is a set of rules for encrypting information—known as a cryptography protocol—that is almost impossible to crack, even by quantum computers.

Eavesdrop

QKD involves two parties sharing a random quantum key, according to which some separate information is encoded. Because in quantum theory it is impossible to observe something without corrupting it, the two parties will know whether someone else has eavesdropped on the key—and therefore whether it is safe, or not, to share their coded information.

Until now, QKD has usually involved specialist technology, such as single-photon detectors and emitters, which are difficult for people outside labs to implement. In the CiViQ project, however, Prof. Pruneri and his team are developing a variant of QKD that works with conventional telecommunications technology.

They have already created prototypes, and performed some field demonstrations. Now, the researchers are working with industry telecoms clients including Telefónica in Spain, Orange in France and Deutsche Telekom in Germany to create systems that work to their respective requirements, with the hope that the first systems could be online within three years.

Prof. Pruneri's hope is to create highly secure communication systems up to 100 km in size suitable for governmental, finance, medical and other high-risk sectors within cities. It could even be used by everyday consumers, although Prof. Pruneri says that QKD currently reaches shorter distances and lower speed than regular communication.

Random

Like normal cryptography, QKD needs random keys—strings of numbers—to be generated in the first place. The more random these keys are, the greater the security of the system, as there is less chance of the keys being guessed. But the problem is that the numbers generated with traditional methods often aren't totally random.

Here, quantum mechanics can again come to the rescue. The behaviour of atoms, photons and electrons is believed to be truly random and this can be used as a way of generating numbers that cannot be predicted.

Professor Hugo Zbinden of the University of Geneva in Switzerland said: "Quantum random-number generators profit from the intrinsic randomness of quantum physics, whereas classical true random number generators are based on chaotic systems, which are deterministic and, in theory, to some extent predictable."

Quantum random-number generators already exist, but to make them more widely applicable Prof. Zbinden and his colleagues working on a project called QRANGE are improving their speed and reliability, as well as reducing their cost. Currently, they are trying to develop prototypes with a 'high technology readiness level' – in other words, prototypes that demonstrate that the technology is ripe for use in the real world.

The work is an important step in ensuring that, while being a threat to the security of our current communications, quantum approaches also provide a path to more secure systems.

Quantum computers threaten classical cryptography," says Prof. Zbinden. "Quantum cryptography can be a solution, (but) it needs high-quality random numbers."

Provided by Horizon: The EU Research & Innovation Magazine