Multi-million EU project to protect data against quantum computers

23 April 2015

Quantum-proof cryptosystems need to be in place before big quantum computers become a reality, which is expected some time after 2025. Even if the scientists win that race quantum computers can still decrypt communication that we encrypt today with current technologies if the attacker has retained this data.

At this moment all bets are off and it is unclear whether we will ever learn the outcome of this competition. Scientists at Eindhoven University of Technology (TU/e) and elsewhere are developing technology that can resist attacks using quantum computers. These cryptosystems need to be in place before big quantum computers become a reality, which is expected some time after 2025. Even if the scientists win that race quantum computers can still decrypt communication that we encrypt today with current technologies if the attacker has retained this data.

Tanja Lange, TU/e professor for Cryptology, is leading a research consortium consisting of eleven universities and companies which is funded with 3.9 million Euros by the European Commission under the H2020 program to develop cryptology that resists the unmatched power of quantum computers. The project PQCRYPTO was publicly announced by Lange at a meeting at the US-American standardization institute NIST on this topic.

The expectation is that large quantum computers will be built some time after 2025. Such computers surmount the abilities of current computers and enable new types of attacks. Currently used methods such as RSA and ECC use keys that will still be unbroken in 100 years with current computer technology - but if quantum computers live up to their promises they can break these systems in a matter of days, if not hours. "2025 seems still far away but we might already be too late", warns Eindhoven professor Lange, who has already worked on alternative cryptosystems since 2006. "It takes 15 to 20 years to introduce and standardize new cryptosystems and we are still in the research phase."

To make things worse, spy agencies are not expected to announce when they have successfully built quantum computers. They can even break encrypted messages from the past if they had the foresight to record all messages. Lange suggests to already now deploy post-quantum cryptography to encrypt data with confidentiality requirements of more than 10 years, such as health records or top-secret documents.

"We already have cryptosystems that resist quantum computers but they are demanding in power which makes them unsuitable for smart phones or contactless cards. The quest is thus to develop new techniques that are unnoticeable on current devices while resisting the power of quantum computers. The European PQCRYPTO consortium will work on this for the next three years. The core targets are small devices, secure data storage in the cloud, and secure Internet."

Provided by Eindhoven University of Technology