BUT opens a unique laboratory of quantum security

As of today, the new laboratory with the so-called quantum communication infrastructure is available to experts from the Faculty of Electrical Engineering and Communication of the Brno University of Technology. The laboratory will enable scientists to work on next-generation computer networks that will also be protected from quantum computer attacks, to which the vast majority of current networks, including the Internet, are vulnerable.

Thanks to special equipment, experts will be able t**o work on the protection of sensitive data, even before the construction of a quantum computer,** for which the current level of security would be an easily overcome obstacle. **For example, data related to state security** or generally critical **infrastructure could fall into strange hands**. At the same time, it is necessary to protect the information passed between the Czech Republic and international institutions, such as the European Union or NATO.

"*One of the areas within the competence of the National Office for Cyber and Information Security is the protection of classified information in the information and communication systems and their cryptographic protection. For this reason, we welcome all activities leading to the research and development of the necessary technologies and to the training of experts in optical quantum communication and quantum cryptography. Academic workplaces have an irreplaceable role in this area, that is why cooperation with them is key for us*," Jaroslav Šmíd, the Deputy Director of the National Cyber and Information Security Agency says.

Part of the equipment, especially the elements for **quantum key determination, is purchased from the Swiss leader in quantum communication, ID Quantique. BUT develops other components of the laboratory itself**, especially high-speed cyphers capable of operating at speeds of up to 100 Gb per second, which is much more than most currently available devices can. The infrastructure is further supplemented by attackers' simulators, data traffic generators, high-speed traffic analysers or elements for simulating optical paths of various lengths.

In practice, **institutions requiring a high degree of data protection** should have a set similar to that in the BUT laboratory, i.e. namely a device for quantum key establishment and an encryptor, but they would send the data over existing optical networks.

At present, the laboratory serves mainly research activities within the Network Cybersecurity in Post-Quantum Era supported by the Ministry of the Interior of the Czech Republic in program IMPAKT. In the first phase, an encryptor resistant to quantum attacks will be developed, and then in the second phase, it will be tested in pilot

Bc. Tereza Kadrnožková, specialista komunikace
Vysoké učení technické v Brně / Antonínská 548/1 / 601 90 / Brno
T: 541 145 157 / M: 607 211 145 / www.vutbr.cz / tereza.kadrnozkova@vut.cz

operation in optical networks at a distance of up to several tens of kilometres. Close cooperation with the National Office for Cyber and Information Security and other universities is key in solving the project.

"*The aim is to verify the properties of the equipment in our laboratory, then increase the distances between the communicating parties to several tens of kilometres. We plan to achieve this through pilot connections between FEEC and FIT BUT or between BUT and Masaryk University. Active cooperation with partners across the Czech Republic is important*," the project leader Jan Hajný from BUT explains.

The opening of the laboratory responds to current trends abroad, especially in the EU, the USA and China, where similar infrastructures are already being built and interconnected into transnational networks. In the Czech Republic, the laboratory at the Brno University of Technology has the ambition to become **one of the first building blocks of the so-called National Quantum Network.** The results of measurements and experience with the deployment of quantum networks will be used in its construction under the banner of CyberSecurity Hub, of which BUT is a founding member, and then in connecting infrastructure with European partners, where the goal is to participate in a whole Europe initiative to build quantum communication infrastructure - EuroQCI.

In addition to scientific purposes, the laboratory aims to bring the issue of quantum networks to students in the Information Security programme and the general public, so it also includes demonstrators who present the basic principles of quantum cryptography in an understandable form.

Bc. Tereza Kadrnožková, specialista komunikace
Vysoké učení technické v Brně / Antonínská 548/1 / 601 90 / Brno
T: 541 145 157 / M: 607 211 145 / www.vutbr.cz / tereza.kadrnozkova@vut.cz