Evento organizzato nell'ambito di Engineering Physics Colloquia

Ca' Foscari University of Venice

Department of Molecular Sciences and Nanosystems

Emerging quantum key distribution networks

24 maggio 2024 , ore 11.00
Conference Room Orio Zanetto, Alfa Building
ed in videoconferenza al link: **https://unive.zoom.us/j/84345725884**
password: **seminar1**

The organizers will offer coffee & cookies to participants

Prof. **Miroslav Vozňák**
VŠB-Technical University of Ostrava (Czech Republic)

Abstract

Conventional encryption algorithms are expected to be broken in a large-scale quantum computer. It is not a question of yes or no, we don't know when it will happen, whether within this or the following decade. If you ask how we can deal with the coming threats to the cryptography currently in use, fortunately, we have a response. There are two ways, post-quantum cryptography (PQC) and quantum key distribution (QKD). The PQC standardization process began in 2016 and it's still open, within the process, the world's cryptographic experts were called to submit candidate algorithms, now we have selected four and we expect the next three this year. Another approach is not based on mathematical algorithms but on quantum physics principles, which is the idea of quantum key distribution (QKD). The speech will briefly introduce the principles of cryptography in the beginning, then will continue with the Open Quantum Safe project and the major part will be devoted to the QKD. A substantial part will be about issues of QKD networks and the speaker will share his experience from recently finished H2020 OpenQKD and NATO Quantum5 projects.