Recent Progress in Quantum Communications Networks

Mohsen Razavi
(University of Leeds, UK)

Data security in the quantum era can be one of the key challenges that telecom operators will face in the coming years. With the recent trend in advanced quantum computing machines, the need for implementing alternative solutions for secure communications—those that do not rely on computational complexity assumptions—has become more urgent. This would be of special interest in scenarios that forward secrecy, or long-term security, is a requirement. Fortunately, there is a possible solution to this problem, known as quantum key distribution (QKD), whose security relies on the laws of physics as we understand them by quantum mechanics. QKD enables two users to securely exchange a secret key. This can, in principle, resolve the security issues that threatens the public-key cryptography schemes. In practice, however, a large-scale deployment of QKD in our current infrastructure will face certain challenges. This will nevertheless provide many opportunities for engineers and scientists alike to harness the power of quantum mechanics for our daily applications. In this talk, I will give an overview of this technology and how it has evolved over the past few decades. I will also describe how the backbone networks could be upgraded, in multiple phases, to accommodate a global quantum communications network.