QUANTUM INNOVATION 2021

CC-01-01

Bringing QKD to real-world digital infrastructures

Michele Mosca

evolutionQ, and IQC, University of Waterloo, Canada

Abstract

For the advent of large-scale fault-tolerant quantum computers to represent a positive milestone in human history, we must first evolve critical digital infrastructures to be safe from quantum-enabled attacks.
However, the current status quo in cryptography is already not good enough anymore. With connected industrial devices, driverless cars, 5G, and more, the stakes are already far higher than they were a decade or more ago, and they keep getting higher.
The emerging “quantum internet” further amplifies the positive impacts of quantum computation and quantum sensing, and also offers a fundamentally new suite of tools for protecting digital platforms from a range of cyber attacks. Quantum key establishment (known as Quantum Key Distribution, QKD) is one such tool that is already commercially available and will continue to improve as quantum technologies continue to advance.
It is already time to design QKD into real-world digital infrastructures, alongside other quantum-safe methods. I will overview our work facilitating robust scalable real-world deployment of QKD.