Security issues of Key Recycling in Quantum Key Distribution

Irene Di Muzio

November 15, 2024

Quantum Key Distribution (QKD) is a cryptographic technique that leverages the laws of quantum physics to create an ITS key exchange process. However, its unconditional security is contingent upon unconditionally secure classical authentication. In order to enhance their combination, the key recycling approach has shown promise. We will investigate the security of such scenario, after an high-level overview of QKD.