Coherent One-Way protocol: study of possible variants

Abstract

Distributed-phase reference coding protocols stem from a wish to implement quick and easy Quantum Key Distribution schemes. In effect, from an experimental point of view, both the Differential-Phase Shift DPS and the Coherent One-Way COW protocols are composed with few standard telecom devices. However, since all coherent pulses that Alice sends to Bob constitute a quantum signal where individual qubits cannot be distinguished, "conventional" security proofs do not apply. Different variants of the historical COW protocol and also known attacks are reviewed, in the perspective of finding improvements for its the implementation and security. We also propose and study a new kind of attack, the Attenuated-Beam Attack ABA, which Eve can perform on two variants. Furthermore, we compare all variants of the historical COW protocol.