

A Hybrid E91-based QKD Protocol with PNS-Resistance and Location-Based Authentication

Hamza Abaakil¹, Abdallah Slaoui^{1, 2}, and Hanane El Hadfi²

¹ LPHE-Modeling and Simulation, Faculty of Sciences,
Mohammed V University in Rabat, Rabat, Morocco

² Centre of Physics and Mathematics (CPM), Faculty of Sciences,
Mohammed V University in Rabat, Rabat, Morocco

Abstract

We propose a hybrid quantum key distribution protocol based on the E91 entanglement scheme that combines sifting-less reverse reconciliation with quantum position verification (QPV). The protocol removes both the classical sifting step and the need for pre-shared authentication keys, enabling a more self-contained QKD architecture. We derive a composable security bound $\epsilon_{\text{total}} \approx 2 \times 10^{-5}$ and an analytical expression for the secret key rate under collective attacks. Numerical results show that the protocol outperforms standard E91 in high-loss regimes, achieving a key rate scaling of approximately $K_{\text{opt}} \propto T^{1.5}$ compared to T^2 in the conventional case. These results demonstrate that integrating entanglement-based QKD with sifting-less processing and position-based authentication provides a viable route toward scalable, long-distance quantum communication.

Keywords: Quantum Key Distribution, E91 Protocol, Sifting-less Reconciliation, Quantum Position Verification, PNS Attack, Composable Security