INTRODUCTION

Discrete-modulated continuous-variable (CV) quantum key distribution (QKD) can be a cost-effective solution to distributing secret keys in the quantum-secured networks since it uses a setup nearly identical to modern telecommunication equipment.

PROTOCOL DESCRIPTION

SECURITY PROOF METHOD

Source-replacement scheme:

\[ |\Psi_{AB}^A = \sum_{x} \sqrt{\beta(x)} |x\rangle_A |x\rangle_B \]

where Alice prepares \(|a_x\rangle\) with a priori probability \(p_x\) and \(|x\rangle\) is an orthonormal basis for the register. \(P_{AB} = \langle \sum x \beta(x) \rangle |\Psi_{AB}^A \rangle \rangle, \) where \(\beta(x)\) is a positively trace preserving (CPTP) map.

Asymptotic key rate (reverse reconciliation):

\[ R'' = P_{\text{pass}} \beta I(X:Z) - \text{max } \chi(Z:E) \]

\[ = P_{\text{pass}} \text{min } H(Z|E) - H(Z) + \beta I(X;Z) \]

\[ = \min_{\rho_{AB}} \langle G(\rho_{AB})|Z|G(\rho_{AB})\rangle - P_{\text{pass}} H(Z) + P_{\text{pass}} \beta I(X;Z) \]

\[ \text{Ref. [4]} \]

The cost of error correction per signal is \(H(Z) - \beta I(X;Z)\).

DETECTOR MODEL

Trusted Detector Noise

Untrusted Detector Noise

\[ \rho_{AB} \text{ is characterized by a parameter } \delta \text{, the parameter } \delta \text{ is optimized via a search over a discrete set of values.} \]

KEY RATE OPTIMIZATION PROBLEM

\[ P(\psi) = Tr(\pi_{\omega} M_{\omega}) \]

\[ f^{(1)}(x',y') \text{ is a real-valued function such that the integral converges.} \]

\[ \text{minimize } D(G(\rho_{AB}))|Z|G(\rho_{AB})\rangle \]

\[ \text{subject to: } \]

\[ Tr[\rho_{AB} (\{x\}A \otimes \bar{O}_2) ] = p_x \langle 0|X \rangle \]

\[ Tr[\rho_{AB}] = \sum \rho_i \|p_i\| (|x_i\rangle |x_i\rangle) / |0\rangle \langle 0| A \]

\[ \rho_{AB} \geq 0, Tr[\rho_{AB}] = 1 \]

for \(x \in \{0,1,2,3\}\) and some choices of \(\bar{O}_2\)

Photon-number cutoff assumption

\[ \rho_{AB} = (\lambda |\Theta\rangle \langle \Theta| \lambda) \rho_{AB} \text{ for a sufficiently large integer } N. \]

REFERENCES