Capacity Optimization of Channel Models for a Pragmatic QKD Protocol Based on Spatial Entanglement of Twin Beams in PDC

M Mondin[1], F Daneshgaran[2], I P Degiovanni[3], M Genovese[3], and I Ruo Berchera[3]

[1]*DET, Politecnico di Torino, Corso Duca degli Abruzzi 24, I-10129, Turin, Italy*
[2]*ECE, California State University, 5151 State University Dr., 90032, Los Angeles CA, USA*
[3]*Istituto Nazionale di Ricerca Metrologica, Strada delle Cacce 91, I-10135, Turin, Italy*
Contact Email: marina.mondin@polito.it

One of the key issues in QKD is the rather limited data rate at which the secret key can be generated. This paper explores the use of twin beams in a PDC process for imaging CCD devices whose photon counts in symmetric pixel positions can be used to generate secret keys. The fundamental reason is that the two beams are entangled in the photon number state and measurements of the correlation statistics should theoretically expose the presence of the eavesdropper. Via a binning approach the photon counts at Alice and Bob who each image one of the two beams, can be turned into discrete labels that represent elements of the raw key that needs further reconciliation and privacy amplification. Discrepancies between the photon counts can be modeled via a fictitious discrete memoryless channel. Furthermore, the use of multi-pixels images allows to create a number of parallel channels for generation of secret keys, thus significantly boosting the achievable key rate.

This work explores the derivation of proper channel models for this application starting from measured data and the optimization of the secret key rate. Trade-offs between error probability and key rate are analyzed, with the final goal of maximizing the system Shannon capacity.