Contribution ID: **15** Type: **Talk**

High-dimensional quantum key distribution rates for multiple measurement bases

Monday 5 May 2025 17:15 (30 minutes)

High-dimensional quantum key distribution rates for multiple measurement bases Quantum key distribution (QKD) protocols take at least two advantages from high-dimensional (HD) systems: the secret key rate scaling as the dimension and the opportunity of exploiting more than two mutually-
unbiased bases (MUBs). Indeed, if the dimension d of the system is a prime power, then d + 1 MUBs exist. Here, we retrieve analytic key rates for a BBM92-like protocol where the dimension of the Hilbert space is generic and different numbers m of MUBs are considered. A similar task has been addressed in Ref. [1], where the authors optimized the key rate for generic dimension and m = 3. We extend their analysis by considering every allowed number of MUBs and identify the optimal number of MUBs providing the larger secure key rate.
In the limit of infinite number of rounds, we find the analytic expression for the asymptotic key rate with m = d + 1 MUBs and provide a numeric evaluation for m <d +1. We show that, as one may expect, both the key rate and the maximum tolerable error rate increase as m increases. In the finite-key scenario, we retrieve upper bounds on the key rate in the presence of collective and coherent attacks. In particular, we compare the rates obtained by using a specific entropic uncertainty relation (EUR) with the ones obtained from the asymptotic equipartition property (AEP). The EUR al-
lows to achieve a tighter bound for small numbers of rounds (< 106), but can be exploited just for m = 2, while the AEP can be used for every choice of m, up to m = d + 1. This is shown in Fig. 1, where we set d = 5 and plotted the key rates as a function of the number of rounds N. Here, we
also compare the rates obtained from different choices of m. Surprisingly, we find that for N < 106 the highest key rate is obtained by exploiting just three MUBs.

Presenter: CHESI, Giovanni (University of Pavia)