High-dimensional quantum key distribution rates for multiple measurement bases

N. Wyderka[1], G. Chesi[2], H. Kampermann[1], C. Macchiavello[2] and D. Bruß[1]

[1]Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany
[2]Dipartimento di Fisica, Università degli Studi di Pavia, Via Agostino Bassi 6, 27100 Pavia, Italy

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. Surprisingly, in the *finite-key* scenario, we find that the highest key rate is obtained by exploiting just *three* MUBs.

Protocol

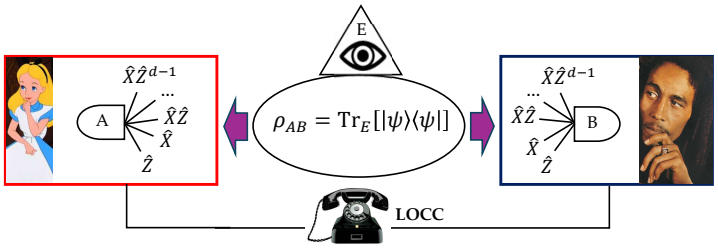
Preparation

$|\psi\rangle \in \mathcal{H}_{ABE}$

$|\phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle$

$|\phi_{\alpha,\beta}\rangle = (I \otimes \hat{X}^\alpha \hat{Z}^\beta)|\phi^+\rangle$

$\rho_{AB} = \sum_{\alpha,\beta} \lambda_{\alpha,\beta} |\phi_{\alpha,\beta}\rangle\langle\phi_{\alpha,\beta}|$



Measurement

$\hat{X} \equiv \sum_j |j\rangle\langle j-1|$

$\hat{Z} \equiv \sum_j e^{\frac{2\pi i}{d} j} |j\rangle\langle j|$

error rates

$Q_Z \equiv 1 - \sum_j \langle jj|\rho_{AB}|jj\rangle = 1 - \sum_{\alpha=0}^{d-1} \lambda_{0,\alpha}$

$Q_{XZ^k} = 1 - \sum_{\alpha=0}^{d-1} \lambda_{\alpha,k\alpha}$

Asymptotic key rates

Von Neumann entropy: $H(A)_\rho = -\mathrm{Tr}[\rho_A \log(\rho_A)]$

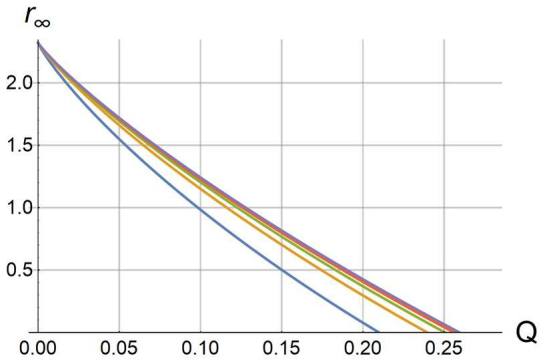
Conditional entropy: $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$

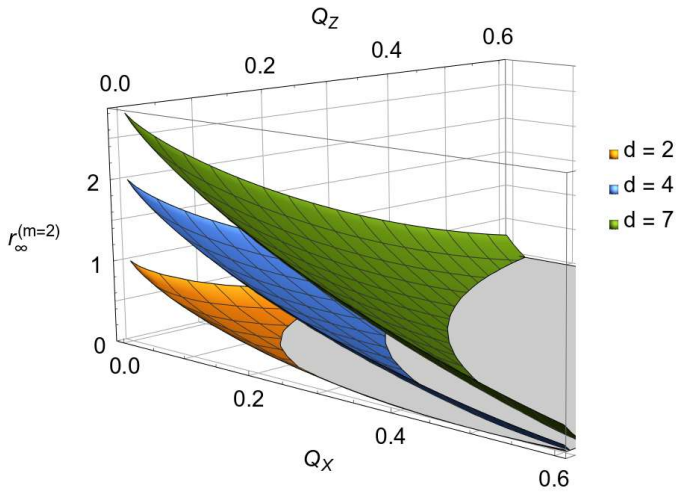
Devetak-Winter rate: $r_\infty = H(R_A|E) - H(R_A|R_B)$

$\min_{\rho_{AB}} \log d - H(A,B)_{\rho_{AB}}$ subject to Q_i as observed, $i \in \{X, Z, XZ, \dots\}$

$$r_\infty^{(m=d+1)} = \log(d) + (1-q)\log(1-q) - q\log(d-1) + (q - Q_Z)\log(q - Q_Z) + \sum_{k=0}^{d-1} (q - Q_{XZ^k})\log(q - Q_{XZ^k})$$

$$q \equiv \left(Q_Z + \sum_{k=0}^{m-2} Q_{XZ^k}\right)/(m-1)$$





Finite key rates

Bound from the *entropic uncertainty relation* ($m = 2$):

$$r \leq C - h(\bar{Q} + \mu_\varepsilon) - (\bar{Q} + \mu_\varepsilon)\log(d-1) - \frac{1}{n}\left[\mathrm{leak}_{EC} + \log\left(\frac{2}{\varepsilon_{EC}}\right) + 2\log\left(\frac{1}{2\varepsilon_{PA}}\right)\right]$$

C: incompatibility; $\bar{Q} + \mu_\varepsilon$: max error tolerance; μ_ε: statistical uncertainty; leak_{EC}: leakages; ε_{EC}, ε_{PA}: security parameters

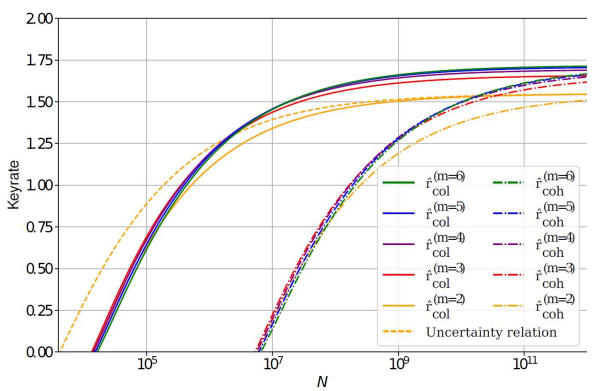
Bounds from the *asymptotic equipartition property*:

$$r_{\mathrm{col}} \leq \frac{n}{N} r_\infty^{(m)}(\bar{Q} + \mu_\varepsilon) - \frac{1}{N}\left[\log\left(\frac{1}{\varepsilon_{EC}\varepsilon_{PA}^2}\right) + 4\sqrt{n}\log(2+\sqrt{d})\sqrt{\log\left(\frac{2}{\varepsilon^2}\right)}\right]$$

collective attacks

$$r_{\mathrm{coh}} = r_{\mathrm{col}} - \frac{2(d^4-1)}{N}\log(N+1)$$

coherent attacks



N. Wyderka, G. Chesi, H. Kampermann, C. Macchiavello and D. Bruß, "*High-dimensional quantum key distribution rates for multiple measurement bases*", arXiv:2501.05890 [quant-ph].