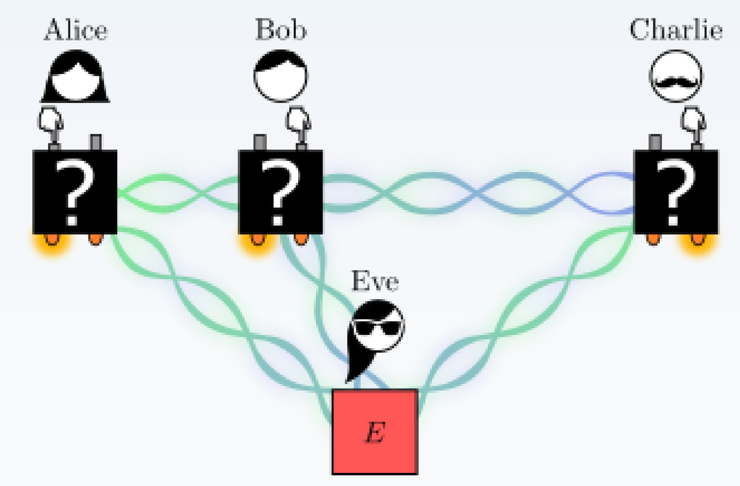
Entropic bounds for multiparty device-independent cryptography

F. Grasselli, Gláucia Murta, H. Kampermann, and D. Bruß

Heinrich-Heine-Universität Düsseldorf

arXiv:2004.14263

The device-independent scenario



- No assumptions on distributed system or measurements performed by the devices.
- Security certified by the statistics of inputs and outputs: $p(abc|xyz)$.

MABK test

Each party has 2 inputs with 2 outputs, $x, y, z \in \{0,1\}$ and $a, b, c \in \{0,1\}$.
They test for the MABK inequality[1]:

$$\mathcal{M} = \langle A_0 B_0 C_1\rangle + \langle A_0 B_1 C_0\rangle + \langle A_1 B_0 C_0\rangle - \langle A_1 B_1 C_1\rangle \leq 2,$$

A_x is the observable corresponding to Alice's measurement labeled by x, and similarly for B_y and C_z.

Figure of merit

The information available to an eavesdropper about the parties' outcome can be quantified by conditional entropies:

$$H(A|E), H(AB|E)$$

GOAL: estimate these entropies given that the MABK inequality is violated.

Result 1: 'Almost' GHZ-diagonal state

We can restrict the analysis to **almost GHZ diagonal states** and **rank-1 projective measurements**.

$$\rho = \begin{pmatrix} \lambda_{000} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_{100} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{001} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_{101} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_{010} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_{110} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{011} & is \\ 0 & 0 & 0 & 0 & 0 & 0 & -is & \lambda_{111} \end{pmatrix},$$

in the GHZ-basis: $\left|\psi_{ijk}\right\rangle = Z^i \otimes X^j \otimes X^k \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle);\, i,j,k \in \{0,1\}$.

For N parties:

$$\rho = \sum_{\vec{u}} \left[\lambda_{0\vec{u}} |\psi_{0\vec{u}}\rangle\langle\psi_{0\vec{u}}| + \lambda_{1\vec{u}} |\psi_{1\vec{u}}\rangle\langle\psi_{1\vec{u}}| + i s_{\vec{u}} \left(|\psi_{0\vec{u}}\rangle\langle\psi_{1\vec{u}}| - |\psi_{1\vec{u}}\rangle\langle\psi_{0\vec{u}}|\right)\right]$$

for $\vec{u} \in \{0,1\}^{\times N-1}$. Moreover N terms $s_{\vec{u}}$ can be set to zero and N pairs can be ordered as $\lambda_{0\vec{u}} \geq \lambda_{1\vec{u}}$.

Ingredients of the proof:

- Two binary measurements per party $\Rightarrow$ reduction to qubits and rank-1 projective measurements [2].
- Symmetrisation of marginals (can be enforced in the protocol): $\langle A_x B_y\rangle = \langle A_x C_z\rangle = \langle B_y C_z\rangle = \langle A_x\rangle = \langle B_y\rangle = \langle C_z\rangle = 0$.
- Use of extra degrees of freedom (local rotations).

Result 2: Maximal MABK violation

For arbitrary N-qubit state ρ and rank-1 projective measurements:

$$\mathcal{M}_\rho \leq 2\sqrt{u_1 + u_2}$$

where u_1 and u_2 are the largest and second-to-the-largest eigenvalues of $T_\rho^T T_\rho$, and T_ρ is the correlation matrix.

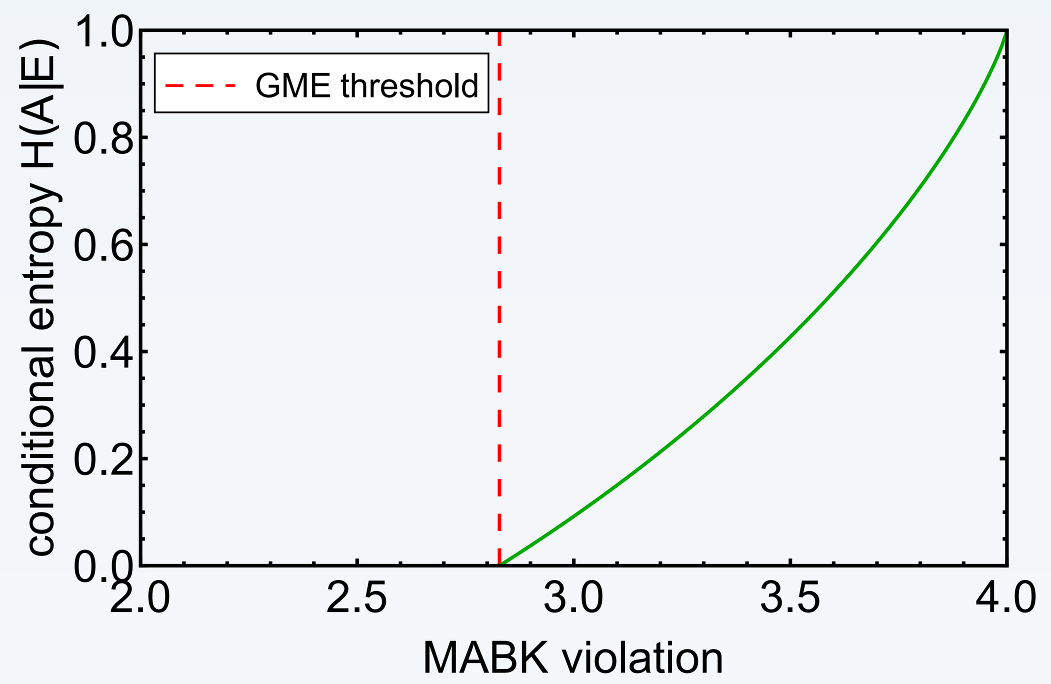
Correlation matrix for $N = 3$ is the 3×9 matrix defined by the elements

$$[T_\rho]_{ij} = \mathrm{Tr}\left(\sigma_\mu \otimes \sigma_\nu \otimes \sigma_\gamma \rho\right) \text{ s.t. } i = \mu \text{ and } j = 3(\nu - 1) + \gamma.$$

$$\sigma_1 = X,\, \sigma_2 = Y,\, \sigma_3 = Z$$

This generalizes the well known result for the CHSH inequality [3].
Our bound is tighter than the previously derived bound in Ref. [4].

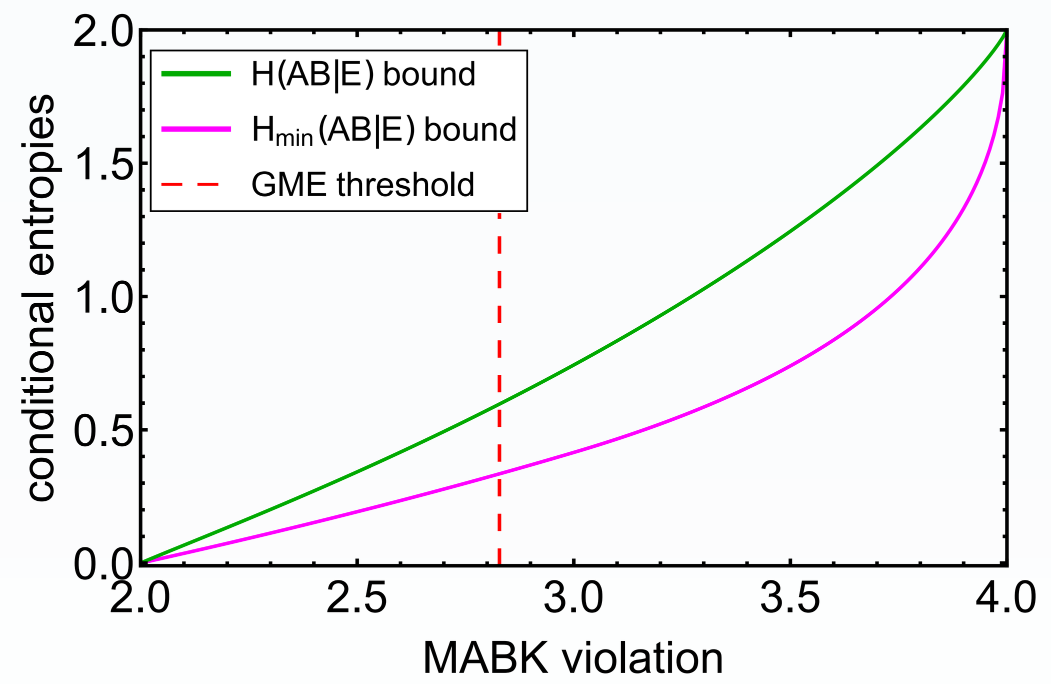
Results 3: Bounding Eve's information



- Using Results 1 and 2 we prove a lower bound on $H(A|E)$ as a function of the MABK value (green curve).
- The bound is tight and achieved for the family of states

$$\tau(\nu) = \nu\, |\Phi_{000}\rangle\langle\Phi_{000}| + (1-\nu)\, |\Phi_{011}\rangle\langle\Phi_{011}|, \quad \nu \in [0,1].$$

- Tight bound can be extended for arbitrary N.
- Our bound coincides with bound based on the MABK-CHSH correspondence [5] $\Rightarrow$ genuine multipartite entanglement is necessary for positive entropy.



- Our bound improves previous result [6] based on $H_{\min}$ $\Rightarrow$higher rates for randomness expansion protocols.

Applications and outlook:

Randomness expansion:

- $H(A|E) > 0 \Rightarrow$ Alice can extract secret randomness. A finite regime analysis can determine required parameters for an implementation.
- Next step: derive tight bounds to global randomness for more parties. Advantage in using many parties?

Conference key agreement (CKA):

- CKA also requires maximal correlation among the parties $\Rightarrow$ MABK inequality is not suitable for conference key agreement [7].
- Can we extend our method to derive tight bound on $H(A|E)$ when the parties test for Bell inequalities that are useful for CKA [8]?

References

[1] N. D. Mermin, PRL 65, 1838 (1990); M. Ardehali, PRA 46, 5375 (1992); A. V. Belinskiĭ and D. N. Klyshko, Physics-Uspekhi, 36(8) 653 (1993).

[2] S. Pironio *et al.* NJP 11, 045021 (2009).

[3] R. Horodecki, P. Horodecki, and M. Horodecki. Phys. Lett. A, 200, 340, (1995).

[4] M. A. Siddiqui and S. Sazim. Quantum Inf. Process. 18: 131 (2019).

[5] J. Ribeiro, G. Murta, and S. Wehner. PRA 97, 022307 (2018).

[6] E. Woodhead, B. Bourdoncle, and A. Acín. Quantum 2, 82 (2018).

[7] T. Holz, D. Miller, H. Kampermann, and D. Bruß. PRA 100, 026301 (2019).

[8] J. Ribeiro, G. Murta, and S. Wehner. PRA 100, 026302 (2019); T. Holz, H. Kampermann, D. Bruß. arXiv:1910.11360.