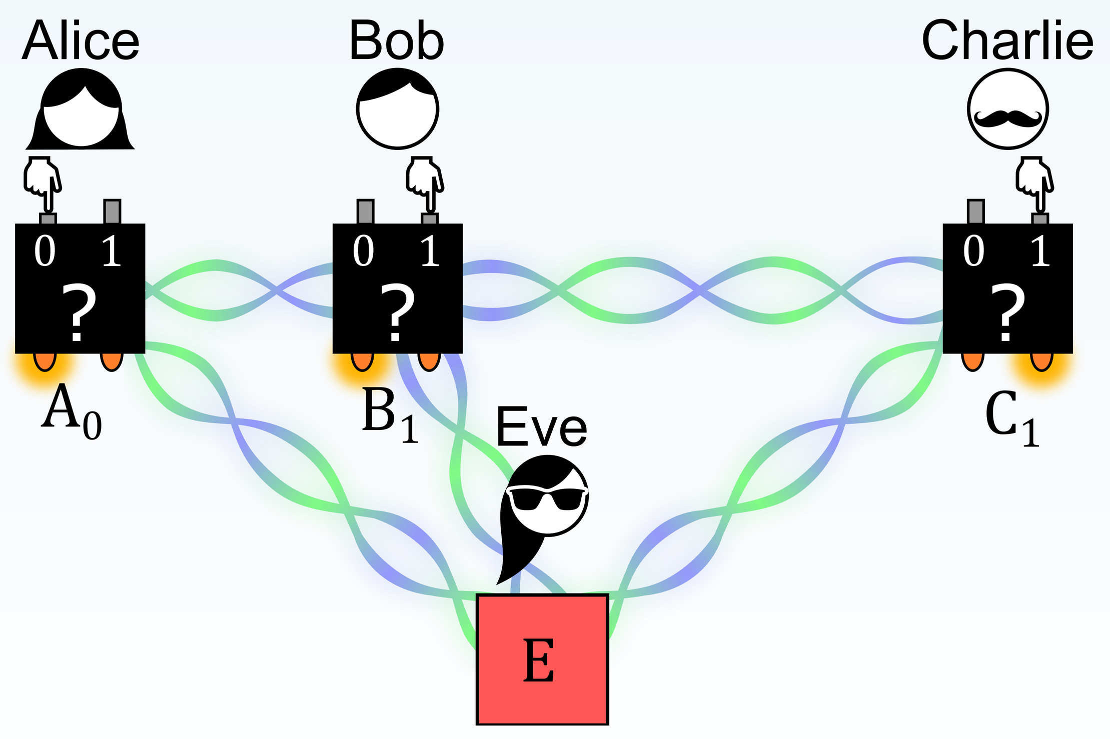
Entropy bounds for multipartite device-independent cryptography

Federico Grasselli, G. Murta, H. Kampermann, and D. Bruß

Heinrich-Heine-Universität Düsseldorf

PRX Quantum 2, 010308 (2021) & work-in-progress

The device-independent (DI) scenario



Each party holds a device with 2 inputs: $\{0,1\}$ and 2 outputs: A_i, B_i, C_i ($i=0,1$).

Bell inequalities

Alice, Bob, and Charlie certify **secret randomness** in their outcomes through the violation of a (multipartite) Bell inequality:

MABK [1]:

$\beta_M = \langle A_0B_0C_1\rangle + \langle A_0B_1C_0\rangle + \langle A_1B_0C_0\rangle - \langle A_1B_1C_1\rangle \leq 2$

Holz [2]:

$\beta_H = \langle A_1B_+C_+\rangle - \langle A_0B_-\rangle - \langle A_0C_-\rangle - \langle B_-C_-\rangle \leq 1$

Parity-CHSH [3]: $\beta_{pC} = \langle A_0B_+\rangle + \langle A_1B_-C\rangle \leq 1$

Asymmetric-CHSH [4]:

$\beta_{\alpha C} = \alpha \langle A_0B_+\rangle + \langle A_1B_-\rangle \leq \max\{1,|\alpha|\}$

where $B_\pm = (B_0 \pm B_1)/2$ and similarly $C_\pm$.

Goal

Given a violation β_M or β_H, find **analytical lower bounds** on the von Neumann entropies

$$H(A_0|E), \quad H(A_0B_0|E)$$

which quantify Eve's uncertainty about the outcomes A_0 or A_0, B_0.

Applications

Entropy bounds $\rightarrow$ fraction of **secret bits** produced by DI conference key agreement (DICKA) and DI randomness expansion (DIRE) protocols.

Two analytical derivations

MABK inequality [5]

Direct **analytical minimization** of $H(A_0|E)$ and $H(A_0B_0|E)$ over all the possible states ρ and measurements yielding a given MABK violation:

- Without loss of generality: ρ is N-qubit state almost diagonal in GHZ basis & Pauli measurements (valid for any N-party full-correlator Bell ineq.).
- We derive bound on maximal violation of MABK inequality given arbitrary N-qubit state ρ.

The one-outcome entropy bound reads:

$$H(A_0|E) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{\beta_M^2}{8} - 1}\right) \quad (1)$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy.

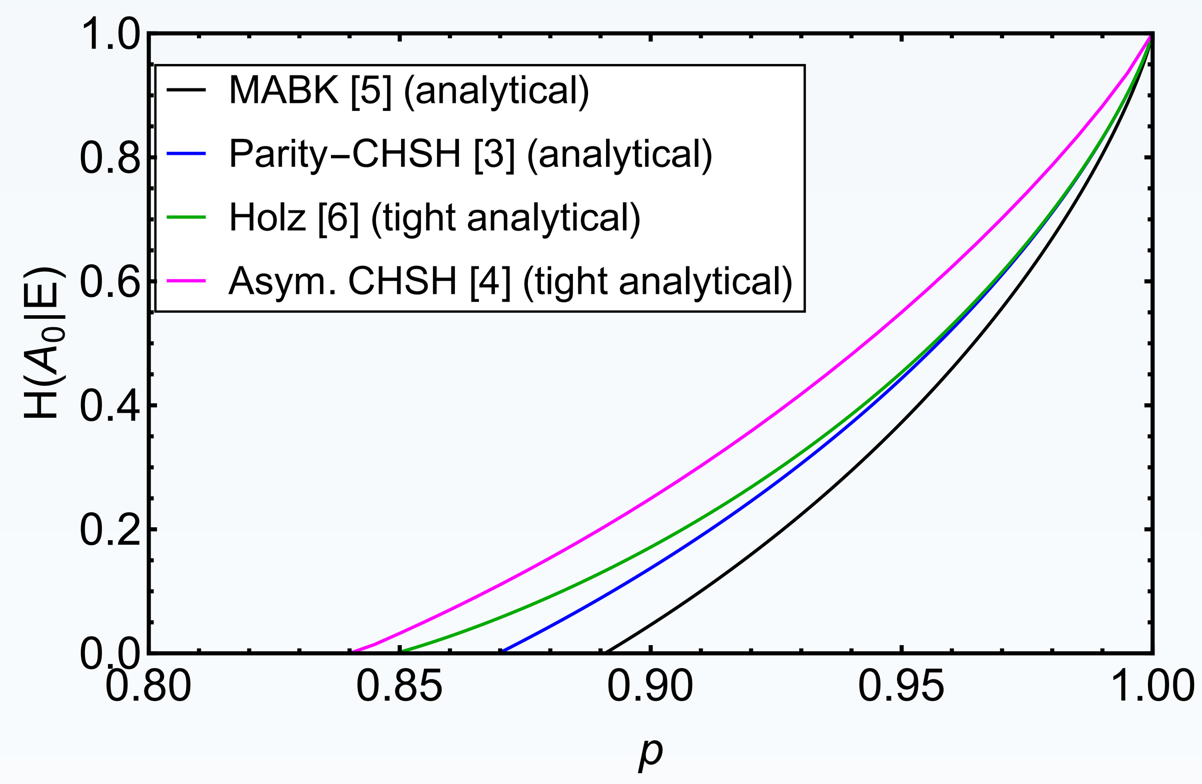
Holz's inequality [6]

1. W.l.o.g.: ρ is three-qubit state & Pauli measurements.
2. Careful choice of local reference frames: $A_0 = Z$; $B_+, C_+ \propto X$ $\Rightarrow$ ρ is almost diagonal in GHZ basis w.l.o.g.
3. Use the **entropic uncertainty relation** and data-proc. ineq.: $H(Z|E) \geq 1 - H(X|BC) \geq 1 - H(X|X_BX_C)$
4. Show that $H(X|X_BX_C) \leq h\left(\frac{1+|\langle XXX\rangle|}{2}\right)$
5. Prove that
$$|\langle XXX\rangle| \geq \frac{\beta_H}{2} - \frac{1}{2} + \frac{1}{2}\sqrt{\beta_H^2 + 2\beta_H - 3}$$
6. Combine 3., 4. and 5. to obtain the **tight** bound
$$H(A_0|E) \geq 1 - h\left[\frac{1}{4}\left(\beta_H + 1 + \sqrt{\beta_H^2 + 2\beta_H - 3}\right)\right] \quad (2)$$

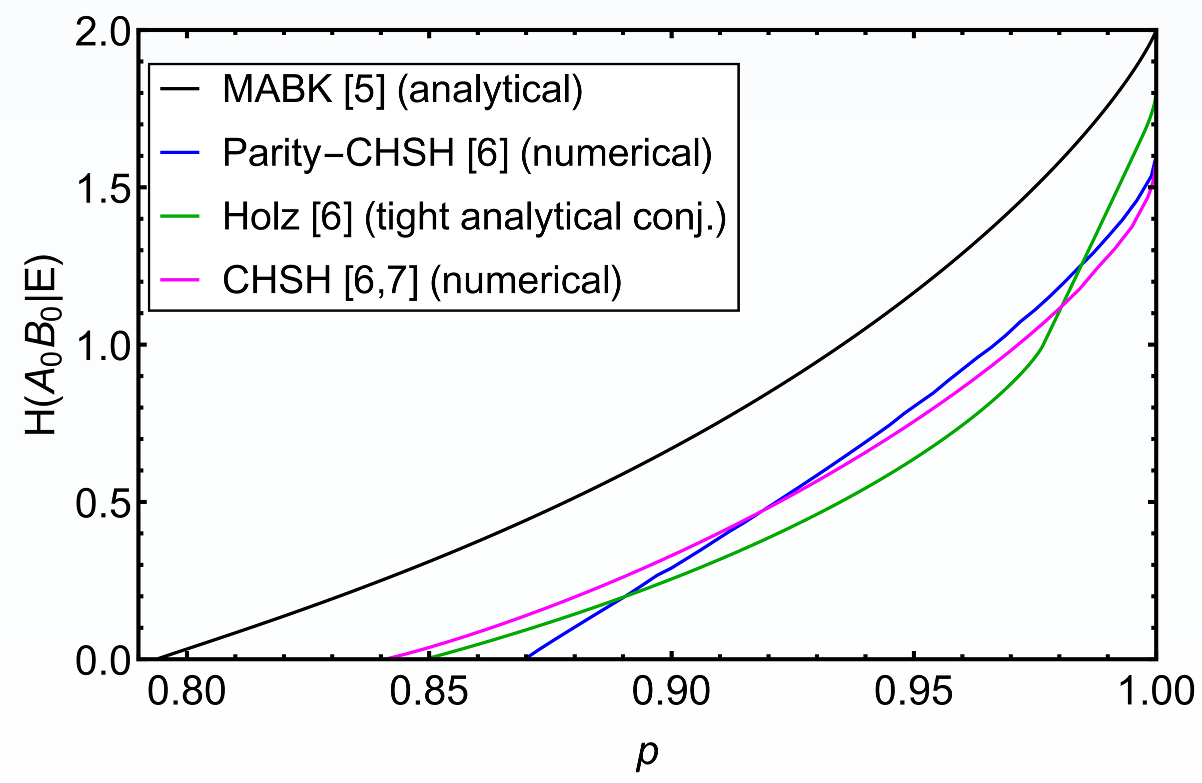
Comparing bounds on $H(A_0|E)$, $H(A_0B_0|E)$

We assume that Alice, Bob and Charlie (Alice and Bob) share the same state: a GHZ state $(1/\sqrt{2})(|000\rangle + |111\rangle)$ (a Bell state $(1/\sqrt{2})(|00\rangle + |11\rangle)$) where each qubit is **depolarized** with probability $1-p$:

$$\beta_M, \beta_H, \beta_{pC} \sim p^3 \quad \beta_{\alpha C} \sim p^2 \quad (3)$$



The Holz bound (2) wins among three-party bounds, loses against the asym. CHSH bound (expected due to lower violation for given p).



The MABK bound certifies the higest fraction of secret bits in A_0, B_0.

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] T. Holz, H. Kampermann, and D. Bruß. Phys. Rev. Res. 2, 023251 (2020).
[3] J. Ribeiro, G. Murta, and S. Wehner. Phys. Rev. A 100, 026302 (2019).
[4] E. Woodhead, A. Acín, and S. Pironio. Quantum 5, 443 (2021).
[5] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß. PRX Quantum 2, 010308 (2021).
[6] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß. In preparation.
[7] R. Bhavsar, S. Ragy, and R. Colbeck. arXiv:2103.07504.

Discussion

DICKA

- The key-generation outcome must be highly correlated among **all** parties: Holz & Parity-CHSH ineq. ✓ MABK ineq. ✗ [2,5]
- Using asym. CHSH needs two independent Bell tests (Bob and Charlie) $\Rightarrow$ "GHZ states + Holz" can yield higher conference key rates

DIRE

- Testing the MABK ineq. requires more input randomness compared to CHSH or Parity-CHSH (bec. one additional party).
- Which inequality actually yields more **net randomness** in the finite-key scenario? MABK? CHSH?