THE DEVICE-INDEPENDENT (DI) SCENARIO

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

MABK [1]:

\[ \beta_M = \langle A_0 B_1 C_1 \rangle + \langle A_0 B_1 C_0 \rangle + \langle A_1 B_0 C_0 \rangle - \langle A_1 B_1 C_1 \rangle \leq 2 \]

Holz [2]:

\[ \beta_H = \langle A_1 B_1 C_+ \rangle - \langle A_0 B_1 C_- \rangle - \langle A_0 C_+ \rangle - \langle B_0 C_- \rangle \leq 1 \]

Parity-CHSH [3]:

\[ \beta_{BC} = \langle A_0 B_+ \rangle + \langle A_1 B_- \rangle \leq 1 \]

Asymmetric-CHSH [4]:

\[ \beta_{AC} = \langle A_0 B_+ \rangle + \langle A_1 B_- \rangle \leq \max(1, |a|) \]

where \( \beta_{\pm} = \langle B_0 \pm B_1 \rangle / 2 \) and similarly \( C_{\pm} \).

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 \( \rho \) and measurements yielding a given MABK violation:

• Without loss of generality: \( \rho \) 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 \( \rho \).

The one-outcome entropy bound reads:

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

(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.: \( \rho \) is three-qubit state & Pauli measurements.

2. Careful choice of local reference frames: \( A_0 = Z; B_+; C_+ \propto X \) \( \Rightarrow \rho \) is almost diagonal in GHZ basis w.l.o.g.

3. Use the entropic uncertainty relation and data-proc. ineq.:

\[ H(Z|E) \geq 1 - H(X|BC) \geq 1 - H(X|X_X C) \]

4. Show that

\[ H(X|X_X C) \leq h \left( 1 + \frac{1}{2} |\langle X|X_X \rangle| \right) \]

5. Prove that

\[ |\langle X|X_X \rangle| \geq \frac{\beta_H}{2} = \frac{1}{2} + \frac{1}{2} \sqrt{\frac{\beta_M}{4} + 2\beta_H - 3} \]

6. Combine 3., 4. and 5. to obtain the tight bound

\[ H(A_0|E) \geq 1 - h \left( \frac{1}{4} \left( \beta_H + 1 + \sqrt{\frac{\beta_M}{4} + 2\beta_H - 3} \right) \right) \]

(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 \( 1 - p \):

\[ \beta_M, \beta_H, \beta_{BC} \sim p^3 \quad \beta_{AC} \sim p^2 \]

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 highest fraction of secret bits in \( A_0, B_0 \).

DISCUSSION

DICKA

• The key-generation outcome must be highly correlated among all parties: Holz & Parity-CHSH ineq. √ MABK ineq. √ [2,5]

• Using asymmetric CHSH needs two independent Bell tests (Bob and Charlie) ⇒ “GHZ states + Holz” can yield higher conference key rates

DIRE

• Testing the MABK ineq. requires more input randomness compared to CHSH or Parity-CHSH (b.c. one additional party).

• Which inequality actually yields more net randomness in the finite-key scenario? MABK? CHSH?

REFERENCES