Improving device-independent randomness expansion rates using two sided randomness

Rutvij Bhavsar [1] Sammy Ragy [1] Roger Colbeck [1]

[1]Department of Mathematics, University of York

Abstract

A device-independent randomness expansion protocol aims to take an initial random string and generate a longer one, where the security of the protocol does not rely on knowing the inner workings of the devices used to run it. In order to do so, the protocol tests that the devices violate a Bell inequality and one then needs to bound the amount of extractable randomness in terms of the observed violation. The entropy accumulation theorem lower bounds the extractable randomness of a protocol with many rounds in terms of the single-round von Neumann entropy of any strategy achieving the observed score. Tight bounds on the von Neumann entropy are known for the one-sided randomness (i.e., where the randomness from only one party is used) when using the Clauser-Horne-Shimony-Holt (CHSH) game. Here we investigate the possible improvement that could be gained using the two-sided randomness. To do so we try to numerically compute the minimum von Neumann entropies for a given CHSH score in the two sided case. Because the numerical technique is not guaranteed to converge, strictly the generated numerical curves are upper bounds, but we conjecture that they are tight and provide analytic formulae in two cases. We also consider a modified protocol in which the input randomness is recycled. This modified protocol shows the possibility of rate gains of several orders of magnitude based on recent experimental parameters, making device-independent randomness expansion significantly more practical. It also enables the locality loophole to be closed while expanding randomness in a way that typical spot-checking protocols do not.

Key Results

- We conjecture numerical bounds on various conditional von Neumann entropies that are relevant for CHSH-based device-independent protocols and discuss when each can be applied.
- Assuming our numerical bounds to be tight we have shown that use of two-sided randomness has the potential to make a big difference.
- Taking the experimental conditions from [4], using the two sided randomness and randomness recycling gives a rate increase of several orders of magnitude.
- The biased inputs protocol removes the spot checking to allow expansion while closing the locality loophole.

Bell tests for Randomness Expansion

A typical DIRNE protocol consists of the following 3 steps as shown in Figure 1.

1. **Generation step** (repeated n times): Alice and Bob do repeated Bell tests using some random input strings $\{X_i\}, \{Y_i\}$ to generate random output strings $\{A_i\}, \{B_i\}$.
2. **Estimation Step**: Using the input-output strings $\{A_i\}, \{B_i\}, \{X_i\}, \{Y_i\}$, Alice and Bob estimate Bell violation.
3. **Extraction Step**: The input/output strings are processed to get a final string $\{R_i\}$ with uniform probability distribution to Alice, Bob and any adversary.

Repeatedly performing CHSH tests does not expand randomness because the input randomness rate is 2 bits,and the output randomness rate is below 2 bits. However, using appropriate protocols enables expansion. In our work, we consider not only the usual spot-checking protocol, but also two modified protocols.

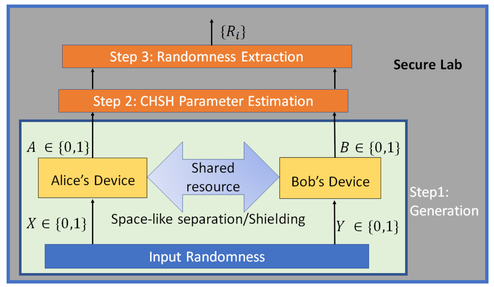

Figure 1. Sketch of a typical DI protocol for randomness expansion.

Protocols for randomness expansion

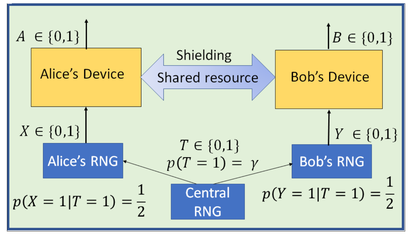

Figure 2. Schematic diagram for spot checking protocol

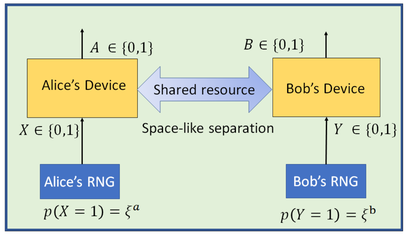

Figure 3. Schematic diagram for Biased inputs protocol

	Spot checking	Recycled randomness	Biased inputs
Generation Step	Central RNG generates $T \in \{0,1\}$ such that $\mathbb{P}(T=1)=\gamma \approx 0$	Inputs X and Y are chosen with a uniform probability distribution i.e. $\mathbb{P}(X=0)=\mathbb{P}(Y=0)=\frac{1}{2}$.	Inputs X and Y are chosen with biased probability distribution such that $\mathbb{P}(X=0)=\zeta_A \approx 1$ and $\mathbb{P}(Y=0)=\zeta_B \approx 1$.
	If $T=0$ is received: Fixed Inputs $X=0$ and $Y=0$ are chosen.		
	If $T=1$ is received (Test round): then inputs X and Y are chosen with a uniform probability distribution.		
Estimation step	The CHSH score is estimated using the input output statistics of test rounds.	CHSH score is estimated using inputs and outputs of all rounds.	CHSH score is estimated using inputs and outputs of all rounds.
Extraction step	Randomness is extracted from outputs of all rounds	Randomness is extracted from all inputs and outputs	Randomness is extracted from outputs of all rounds

Conjectured asymptotic rates

In our work, we compute the conditional von Neumann entropy bounds (asymptotic rates) $F_{A|.E}$ and $F_{AB|.E}$, (here . is used to denote either $(X=0,Y=0)$ or (X,Y) or is empty) the former being the asymptotic randomness rate of Alice's outputs and the later being the randomness rate of both Alice and Bob's outputs. The one sided rates $F_{A|.E}$ are primarily useful for QKD, where as the two sided-rates are more useful for randomness expansion. Because the numerical technique is not guaranteed to converge, strictly the generated numerical curves are upper bounds, but we conjecture that they are tight.

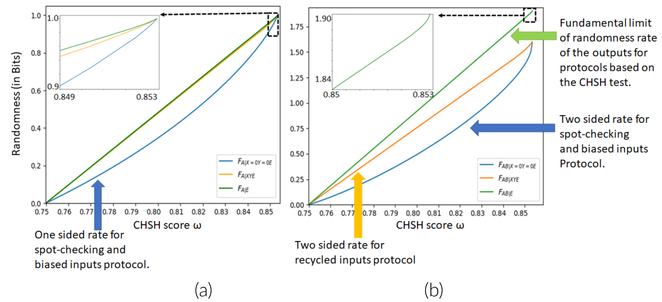

Figure 4. Conjectured (a) one sided and (b) two sided asymptotic rates

Results

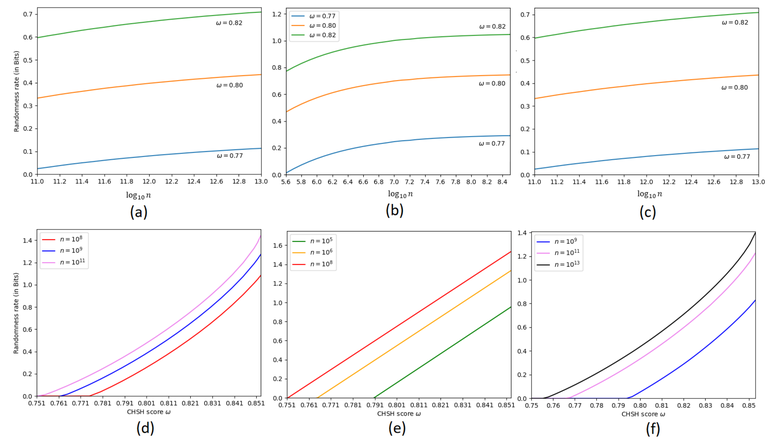

Figure 5. Graphs of the net rate of certifiable randomness according to the Entropy Accumulation Theorem for (a) the spot checking protocol, (b) the recycled inputs ,and (c) the Biased inputs Protocol, and showing the variation with the number of rounds for three different scores, ω. Graphs (d) the spot checking protocol, (e) the recycled inputs ,and (f) the Biased inputs Protocol, show the variation of net rate of certifiable random seed with the CHSH score ω.The error parameters used were $\epsilon_S = 3.09 \times 10^{-12}$ and $\epsilon_C = 10^{-6}$. For each point on the curve (a),(d) an optimization over γ was performed to maximize the randomness; similarly, the values of $\zeta^A = \zeta^B$ were optimized over to generate the curves in (b),(d).

Selected References

[1] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[2] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, 2009.

[3] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, 2020.

[4] Wen-Zhao Liu, Ming-Han Li, Sammy Ragy, Si-Ran Zhao, Bing Bai, Yang Liu, Peter J. Brown, Jun Zhang, Roger Colbeck, Jingyun Fan, Qiang Zhang, and Jian-Wei Pan. Device-independent randomness expansion against quantum side information. *Nature Physics*, 17:448–451, 2021.