Randomness from causally independent processes

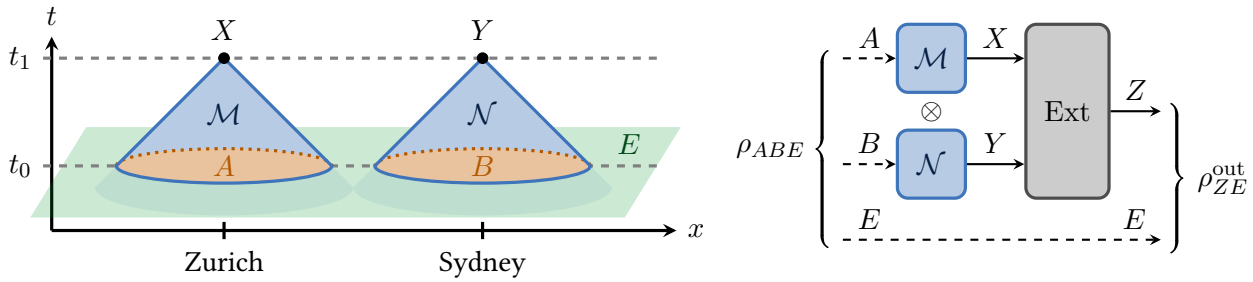
Preprint available at https://arxiv.org/abs/2510.05203

Martin Sandfuchs[1], Carla Ferradini[1], and Renato Renner[1]

[1]Institute for Theoretical Physics, ETH Zurich, Zurich, Switzerland

1 Introduction

Consider two experimentalists who are located in distant places, say Zurich and Sydney. Simultaneously, they both perform experiments designed to generate random numbers, X and Y, respectively. Due to experimental imperfections, neither X or Y will be perfectly random. Because of their geographic locations, X and Y are produced in a spacelike separated fashion, i.e., there is no causal influence from Zurich to Sydney or vice versa during the course of the experiment. Nevertheless, the two experimentalists' data may be correlated due to the influence of events in their common past (e.g., solar radiation). The central question of this paper is whether, in this setup, one can process X and Y into some uniformly random bitstring Z. More precisely, we would like to find a function Ext such that $Z = \mathrm{Ext}(X, Y)$ is uniform and independent from any information which was available before the experiment began. A sketch of the setup is given in Figure 1 below.



(a) Spacetime description. Two processes, $\mathcal{M}$ and $\mathcal{N}$, start at time t_0 and finish producing (imperfect) randomness, X and Y, by time t_1. Due to their spatial distance, $\mathcal{M}$ and $\mathcal{N}$ act independently on A and B, which are spacelike separated regions of the Cauchy surface at time t_0. The region E contains any information available outside of A and B.

(b) Circuit diagram description. The two independent channels $\mathcal{M}$ and $\mathcal{N}$ are applied to an initial state ρ_{ABE} to produce the classical values X and Y. Here E is a purifying system containing any available side information. The goal is for Z to be uniform and independent from E.

Figure 1: **Setup.** The spacetime picture on the left illustrates the range of action of the processes $\mathcal{M}$ and $\mathcal{N}$. Their spacelike separation justifies the tensor product between the corresponding channels in the circuit diagram on the right. The latter also shows the extractor, which is a deterministic function supposed to convert the channel outputs X and Y into a uniform bitstring Z.

The function Ext described above is commonly referred to as a two-source extractor and has been studied extensively in both classical and quantum information theory (see [Cha22] for a review). Prior works required the outputs X and Y to be (conditionally) independent [SV86, CG88, KK10, AFPS16]. Unfortunately, this independence is hard (or even impossible) to justify in practice. On the other hand, as illustrated by

the example above, the independence of quantum processes can be experimentally enforced.[1] This makes our setup attractive for constructing quantum random number generators, where one aims to eliminate unnecessary device assumptions.

2 Results

Naturally, in order to extract any randomness, we must quantify the randomness produced by the measurements $\mathcal{M}$ and $\mathcal{N}$. We say that $\mathcal{M}$ and $\mathcal{N}$ have entropies k_1 and k_2 on the pure state ρ_{ABE} if

$$H_{\min}(X|BE)_{\mathcal{M}[\rho]} \geq k_1 \quad \text{and} \quad H_{\min}(Y|AE)_{\mathcal{N}[\rho]} \geq k_2 \tag{1}$$

hold. We then call the function Ext a (k_1, k_2, ε) *two-process extractor* if [2]

$$\frac{1}{2}\left\|\rho_{ZE}^{\text{out}} - \omega_Z \otimes \rho_E^{\text{out}}\right\|_1 \leq \varepsilon \tag{2}$$

holds for all channels $\mathcal{M}, \mathcal{N}$ and states ρ_{ABE} satisfying the conditions in Equation (1). Here, ω_Z is the maximally mixed state and ρ_{ZE}^{out} is as defined in Figure 1b.

Our first result concerns the feasibility of extracting randomness in the setup given in the introduction. We show that the construction from [DEOR04] can be used to extract randomness in our setting.

Result 1 (Informal)**.** The extractor from [DEOR04] is a (k_1, k_2, ε) two-process extractor with error

$$\varepsilon = \frac{1}{2}\sqrt{2^{2m+n-k_1-k_2}},$$

where n is the number of bits in X and Y and m is the number of output bits.

In practice, it can be difficult (or even impossible) to satisfy the conditions in Equation (1) exactly. Therefore, one often considers the scenario when these conditions are satisfied only approximately, i.e., the channels produce states with high smooth min-entropies. Our next result shows that in this relaxed scenario, one can still extract randomness. This can be seen as the statement that our model is robust.

Result 2 (Informal)**.** Any (k_1, k_2, ε) two-process extractor is also a two-process extractor for channels with smooth min-entropy $k_1' \approx k_1$ and $k_2' \approx k_2$ with slightly modified ε.

The above result is particularly useful since there are powerful tools to bound the smooth min-entropy of the output of a quantum channel, such as the entropy accumulation theorem [DFR20, MFSR22].

Our results apply to randomness generation in the device-independent setting, in particular to *randomness amplification* [CR12, KAF20], where low-quality seed randomness is used to generate high-quality output randomness.[3] A common class of randomness sources considered in this context are *Santha–Vazirani (SV)*

[1] Independence holds even without spacelike separation if the processes take place in separate and sealed laboratories, as is commonly assumed in cryptography.

[2] In fact, we consider a slightly more general model in the paper. More precisely, we allow the processes $\mathcal{M}$ and $\mathcal{N}$ to also produce additional quantum side information, see [SFR25] for details.

[3] A related notion is *randomness expansion* [Col09], which increases the quantity rather than the quality of randomness. Randomness expansion requires high-quality input randomness, which may be obtained by first performing randomness amplification.

sources [SV84]. Since SV sources are a purely classical notion, existing randomness amplification protocols assume that any side information about the initial randomness is classical [KAF20, FWE+23]. Such an assumption is generally unjustified in cryptographic settings. Our results remove this restriction by allowing for quantum side information. To formalize this scenario, we introduce the notion of a *quantum SV source*, which generalizes the classical SV model [SV84]. The setup for randomness amplification with a quantum SV source is sketched in Figure 2 below.

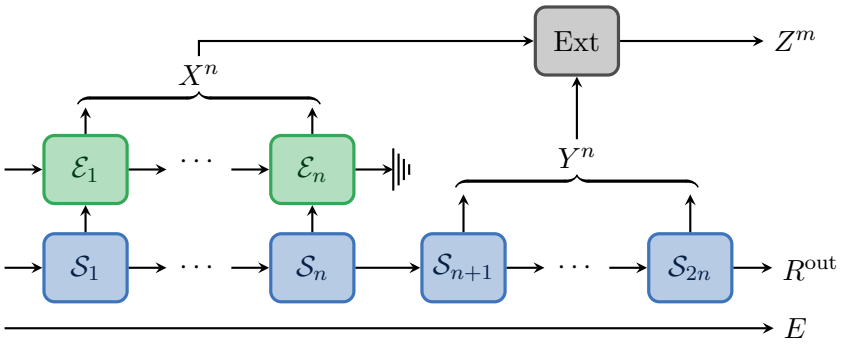


Figure 2: **Diagram of a randomness amplification setup with a quantum source.** We model the quantum SV source as a sequence of channels $\mathcal{S}_1, \ldots, \mathcal{S}_{2n}$, producing classical random variables. The first n pairs of bits are used as the input to a Bell test. The remaining n pairs of bits Y^n are used as the seed to our extractor Ext. The green boxes represent a Bell test producing the measurement results X^n.

Result 3 (Informal)**.** Device-independent randomness amplification using a quantum SV source is possible.

3 Conclusions

Understanding the minimal assumptions under which uniform randomness can be generated is a fundamental problem. Previous work has shown that perfect randomness can be extracted from two (conditionally) independent quantum states. However, justifying such state independence is problematic: correlations are ubiquitous, and no physical principle forbids distant degrees of freedom from being correlated.

In this work, we adopt a different perspective. Rather than assuming independence at the level of quantum states, we impose independence on the processes that generate them. Unlike state independence, process independence can be physically motivated, for instance by non-signalling constraints. Our main result shows that two independent processes suffice for randomness generation, provided that each process produces a sufficient amount of entropy.

We demonstrate the usefulness of our approach in device-independent randomness amplification. In particular, we remove the standard assumption that an adversary's side information about the randomness source is purely classical. To this end, we introduce a quantum generalization of the SV model, in which a sequence of quantum channels produces only weakly biased bits. Besides more accurately reflecting how physical randomness sources are realized, this model accommodates quantum side information.

References

[AFPS16] R. Arnon-Friedman, C. Portmann, V. B. Scholz, "Quantum-Proof Multi-Source Randomness Extractors in the Markov Model", in *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, volume 61, 2:1–2:34, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, doi:10.4230/LIPIcs.TQC.2016.2, 2016.

[CG88] B. Chor, O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *SIAM Journal on Computing*, 17(2):230–261, doi:10.1137/0217015, 1988.

[Cha22] E. Chattopadhyay, "Recent advances in randomness extraction", *Entropy*, 24(7), doi:10.3390/e24070880, 2022.

[Col09] R. Colbeck, *Quantum And Relativistic Protocols For Secure Multi-Party Computation*, Ph.D. thesis, University of Cambridge, 2009.

[CR12] R. Colbeck, R. Renner, "Free randomness can be amplified", *Nature Physics*, 8(6):450–453, doi:10.1038/nphys2300, 2012.

[DEOR04] Y. Dodis, A. Elbaz, R. Oliveira, R. Raz, "Improved randomness extraction from two independent sources", in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, 334–344, Springer Berlin Heidelberg, Berlin, Heidelberg, doi:10.1007/978-3-540-27821-4_30, 2004.

[DFR20] F. Dupuis, O. Fawzi, R. Renner, "Entropy accumulation", *Communications in Mathematical Physics*, 379(3):867–913, doi:10.1007/s00220-020-03839-5, 2020.

[FWE+23] C. Foreman, S. Wright, A. Edgington, M. Berta, F. J. Curchod, "Practical randomness amplification and privatisation with implementations on quantum computers", *Quantum*, 7:969, doi:10.22331/q-2023-03-30-969, 2023.

[KAF20] M. Kessler, R. Arnon-Friedman, "Device-independent randomness amplification and privatization", *IEEE Journal on Selected Areas in Information Theory*, 1(2):568–584, doi:10.1109/jsait.2020.3012498, 2020.

[KK10] R. Kasher, J. Kempe, "Two-source extractors secure against quantum adversaries", in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, 656–669, Springer Berlin Heidelberg, Berlin, Heidelberg, doi:10.1007/978-3-642-15369-3_49, 2010.

[MFSR22] T. Metger, O. Fawzi, D. Sutter, R. Renner, "Generalised entropy accumulation", in *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, 844–850, IEEE, doi:10.1109/focs54457.2022.00085, 2022.

[SFR25] M. Sandfuchs, C. Ferradini, R. Renner, "Randomness from causally independent processes", URL https://arxiv.org/abs/2510.05203, 2025.

[SV84] M. Santha, U. Vazirani, "Generating quasi-random sequences from slightly-random sources", in *25th Annual Symposium on Foundations of Computer Science*, 434–440, doi:10.1109/SFCS.1984.715945, 1984.

[SV86] M. Santha, U. V. Vazirani, "Generating quasi-random sequences from semi-random sources", *Journal of Computer and System Sciences*, 33(1):75–87, doi:10.1016/0022-0000(86)90044-9, 1986.