Fully Quantum Computational Entropies

Noam Avidan
The Center for Quantum Science and Technology, Faculty of Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel

Thomas A. Hahn
The Center for Quantum Science and Technology, Faculty of Physics of Complex Systems, Weizmann Institute of Science, Rehovot, Israel

Joseph M. Renes
Institute for Theoretical Physics, ETH Zurich, Switzerland

Rotem Arnon
The Center for Quantum Science and Technology, Faculty of Physics of Complex Systems, Weizmann Institute of Science, Rehovot, Israel

Abstract

Quantum information theory has provided the formal framework for describing how information is stored, transmitted, and transformed in physical quantum systems [6, 7, 9]. Its entropic formulations underpin our understanding of quantum computation, communication, and cryptography. Yet this theory traditionally treats all quantum operations as freely available, ignoring computational restrictions. In practice, however, any manipulation of quantum information must be performed by devices of bounded complexity and runtime. Capturing such realistic constraints requires extending quantum information theory to include computational efficiency as a fundamental component.

This work takes a first step toward building a computational version of quantum information theory, one that treats efficiency as part of the theory itself. The goal is to understand how the behavior of quantum information changes when the parties involved can only perform computationally efficient operations. This approach bridges the abstract, ideal setting of quantum information theory with the practical limitations of real quantum devices, offering a means to study information processing under realistic resource constraints.

At the center of this work are two new quantities: the quantum computational min-entropy and the quantum computational max-entropy. These entropies extend standard quantum entropies by explicitly limiting the computational power of the observer or adversary. The quantum computational min-entropy captures how unpredictable a quantum system A remains to an observer holding system B, when that observer is restricted to quantum circuits of bounded size. Formally, for a bipartite state ρ_{AB}, we define

$$\overset{c\ s}{\mathrm{H}}_{\min}(A|B)_\rho \coloneqq -\log d_A \max_{\mathcal{E}^s_{B\to A'}} F\left((\mathbb{I}_A \otimes \mathcal{E}^s)(\rho_{AB}), |\Phi_{AA'}\rangle\langle\Phi_{AA'}|\right) ,$$

where the maximization is over quantum channels that can be implemented by circuits of size at most s, and F denotes fidelity with a maximally entangled state. In the classical setting, the min-entropy can be expressed through the maximal probability of correctly guessing a random variable given some side-information. In the fully quantum setting, this idea extends to uncertainty about quantum information [4], quantifying how well one system can be inferred from another using local quantum operations. Our definition generalizes this operational viewpoint by restricting the computational power of the observer to efficient quantum circuits. This definition extends the operational meaning of the information-theoretic quantum min-entropy [4] by incorporating computational constraints, and it provides the fully quantum counterpart of the classical unpredictability entropy [3].

We establish fundamental properties for the computational min-entropy, including monotonicity in the circuit size and smoothing parameters, efficient data-processing inequalities, and fully quantum leakage and purification chain rules, which were left as open questions in earlier definitions of quantum computational entropies [2, 5]. For classical–quantum states, it coincides with the previously defined quantum computational unpredictability entropy [1], showing that the new definition correctly generalizes known results. We also introduce the quantum computational max-entropy through a

17th Innovations in Theoretical Computer Science Conference (ITCS 2026).
Editor: Shubhangi Saraf; Article No. 13; pp. 13:1–13:3

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

duality relation [8] with the min-entropy using a fixed purification. Finally, we prove unconditional separations between the computational and information-theoretic entropies, demonstrating that computational restrictions can fundamentally alter entropic behavior even for simple states.

These results establish the fundamental mathematical framework for studying quantum information within realistic computational constraints. By integrating efficiency directly into entropic quantities, they open the door to a fully developed computational quantum information theory that parallels its information-theoretic counterpart. Such a framework provides the foundation for analyzing cryptographic security against computationally bounded quantum adversaries [1] and the limits of efficient quantum state manipulation. More broadly, it suggests that many core notions in quantum information theory may have refined computational analogues yet to be explored.

2012 ACM Subject Classification Theory of computation → Quantum information theory; Theory of computation → Quantum complexity theory

Keywords and phrases quantum information theory, computational entropy, min-entropy, max-entropy

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.13

Category Extended Abstract

Related Version *Full Version*: https://arxiv.org/abs/2506.14068

Funding *Noam Avidan*: Supported by the Peter and Patricia Gruber Award and by the Air Force Office of Scientific Research under award number FA9550-22-1-0391.
Thomas A. Hahn: Supported by the Peter and Patricia Gruber Award and by the Air Force Office of Scientific Research under award number FA9550-22-1-0391.
Joseph M. Renes: Supported by the CHIST-ERA project "Modern Device Independent Cryptography" and the ETH Zurich Quantum Center.
Rotem Arnon: Supported by the Peter and Patricia Gruber Award, the Air Force Office of Scientific Research under award number FA9550-22-1-0391 and the Koshland Research Fund and is the Daniel E. Koshland Career Development Chair.

References

1 Noam Avidan and Rotem Arnon. Quantum computational unpredictability entropy and quantum leakage resilience, 2025. arXiv:2505.13710.
2 Yi-Hsiu Chen, Kai-Min Chung, Ching-Yi Lai, Salil P. Vadhan, and Xiaodi Wu. Computational notions of quantum min-entropy, 2017. arXiv:1704.07309.
3 Chun-Yuan Hsiao, Chi-Jen Lu, and Leonid Reyzin. Conditional computational entropy, or toward separating pseudoentropy from compressibility. In *Proceedings of the 26th Annual International Conference on Advances in Cryptology*, EUROCRYPT '07, pages 169–186, Berlin, Heidelberg, 2007. Springer-Verlag. doi:10.1007/978-3-540-72540-4_10.
4 Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theor.*, 55(9):4337–4347, 2009. doi:10.1109/TIT.2009.2025545.
5 Anthony Munson, Naga Bhavya Teja Kothakonda, Jonas Haferkamp, Nicole Yunger Halpern, Jens Eisert, and Philippe Faist. Complexity-constrained quantum thermodynamics. *PRX Quantum*, 6:010346, March 2025. doi:10.1103/PRXQuantum.6.010346.
6 Joseph M. Renes. *Quantum Information Theory: Concepts and Methods*. De Gruyter Oldenbourg, Berlin, Boston, 2022. doi:10.1515/9783110570250.
7 Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Springer Publishing Company, Incorporated, 1st edition, 2015. doi:10.1007/978-3-319-21891-5.

8 Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theor.*, 56(9):4674–4681, 2010. doi:10.1109/TIT.2010.2054130.

9 Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, Cambridge, 2013. doi:10.1017/CBO9781139525343.