Computational Notions of Quantum Min-Entropy

Yi-Hsiu Chen,[1] Kai-Min Chung,[2] Ching-Yi Lai,[3] Salil P. Vadhan,[4] and Xiaodi Wu[5]
[14]John A. Paulson School of Engineering and Applied Sciences, Harvard University, USA
[23]Institute of Information Science, Academia Sinica, Taipei, Taiwan
[5]Computer and Information Science Department, University of Oregon, USA

***Abstract*—In this paper, we initiate the study of computational notions of min-entropy in the quantum setting. We extend the classical Leakage Chain Rule for pseudoentropy to the case where the leakage information is quantum. Then we demonstrate an application to quantum leakage-resilient stream ciphers in the bounded-quantum-storage model, assuming the existence of a quantum-secure pseudorandom generator.**

I. Introduction

Computational notions of entropy measure how much (min-)entropy a source X has from the eyes of a computationally bounded party who may hold certain "leakage information" B that is correlated with X. They have several applications in cryptography, such as leakage-resilient cryptography [1], memory delegation [2], deterministic encryption [3], zero-knowledge [4], pseudorandom generators [5] and other cryptographic primitives [6], and also have close connections to important results in complexity theory, such as Impagliazzo's hard-core lemma [7], and in additive number theory, such as the Dense Model Theorem [8], [9], [10].

In this work, we initiate the study of computational entropy in the *quantum* setting, where X and/or B may be quantum states and the computationally bounded observer is modeled as a small quantum circuit. Specifically, we investigate to what extent the classical notions of computational entropy generalize to the quantum setting, and whether quantum analogues of classical theorems still hold. We find that some classical phenomena have (nontrivial) extensions to the quantum setting, but for others, the quantum setting behaves quite differently and we can even prove that the natural analogues of classical theorems are false. As an application of some of our results, we construct a quantum leakage-resilient stream-cipher in the bounded-quantum-storage model, assuming the existence of a quantum-secure pseudorandom generator. To the best of our knowledge, this is the first result on quantum leakage in the computational setting.

We expect that computational notions of quantum entropy will find other natural applications in quantum cryptography. Moreover, by blending quantum information theory and quantum complexity theory, our study may provide new insights and perspectives in both of these areas.

In the following sections, we highlight our primary results without proofs. For more details, including some negative results, please refer to [11].

II. Pseudorandomness of Quantum States

We start by investigating the pseudorandomness of quantum states. Brandao *et al.* [12] and Gross *et al.* [13] showed that there exist *pure* states that are pseudorandom, and indeed this holds for a pure state chosen uniformly at random from the unit sphere with high probability. Brandao *et al.* [14], [15] also showed the existence of (fixed) polynomial-size quantum circuits that generate pseudorandom pure states. We provide a simpler sampling method to show the existence of pseudorandom pure states.

Theorem 1. *For all $s \in \mathbb{N}$ and $\varepsilon > 0$, there exists $m = O(\log(s/\varepsilon))$ such that, if we uniformly sample $(\alpha_1, \ldots \alpha_{2^m})$ from $\{-2^{-m/2}, -2^{-m/2}\}^{2^m}$ and let $\rho = \sum_{i=1}^{2^m} \alpha_i |i\rangle$, then with all but $2^{-\Omega(2^m)}$ probability, ρ is a pure state that is ε-pseudorandom against quantum circuit of size s.*

In [12], the pseudorandomness of random pure states was viewed as a negative result, showing that random

[1]Supported by NSF grant CCF-1420938 and work done in part while visiting the Institute of Information Science, Academia Sinica, Taiwan.

[2]Partially supported by 2016 Academia Sinica Career Development Award under Grant no. 23-17 and the Ministry of Science and Technology, Taiwan under Grant no. MOST 103-2221-E-001-022-MY3. This work was done in part while KMC was visiting the Simons Institute for the Theory of Computing, supported in part by the Simons Foundation and by the DIMACS/Simons Collaboration in Cryptography through NSF grant CNS-1523467. This work was supported in part by the IARPA QCS program; by HRL subcontract No. 1144-400707-DS; and by NSF Grant No. CCF-1421078.

[4]Work done in part while visiting the Shing-Tung Yau Center and the Department of Applied Mathematics at National Chiao-Tung University, Taiwan. Supported by NSF grant CCF-1420938 and a Simons Investigator Award.

pure states are not useful for efficient quantum computation, since they can be replaced by uniform classical bits. However, from the perspective of pseudorandomness and computational entropy, it is a *positive* result, asserting the existence of a pseudorandom state that has *zero* entropy.

III. Computational Quantum Min-Entropy

We next investigate *computational* notions of min-entropy in the quantum setting.

a) (Conditional) pseudoentropy: There are several ways to define computational min-entropy with different applications and interesting connections to other fields. Here, we focus on pseudoentropy definitions in the HILL style [5], which are the most widely used notions in the classical setting. For definitions and connections to other computational notions, please refer to the full version [11].

Let $\rho_{XB} \in \mathcal{X} \otimes \mathcal{B}$ be a bipartite cq-state with $n + \ell$ qubits. We say that X conditioned on B has *conditional quantum rHILL pseudo(min-)entropy* at least k (informally written as $H^{\mathsf{rHILL}}(X|B)_\rho \geq k$) if there exists a quantum state σ_{XB} such that (i) $H_{\min}(X|B)_\sigma \geq k$ and (ii) ρ_{XB} and σ_{XB} are computationally indistinguishable by all $\mathrm{poly}(\kappa)$-size quantum distinguishers, where again κ is the security parameter[1].

b) Information-theoretic Quantum Leakage Chain Rule: The Information-theoretic Quantum Leakage Chain Rule is necessary toward the Leakage Chain Rules for computational quantum min-entropies. Most classical entropy notions, such as min- and Shannon entropies satisfy a Leakage Chain Rule stating that $H(X|B) \geq H(X) - |B|$, i.e., conditioned on a leakage B, the entropy of X can only be decreased by the length of B. It is often useful to generalize these to the case there there is prior *side* information Z: $H(X|Z,B) \geq H(X|Z) - |B|$. The following theorems are the special cases of the results by Winkler *et al.* .

Theorem 2 ([17, Lemma 13])**.** *Let $\rho = \rho_{XZB}$ be a state on the space $\mathcal{X} \otimes \mathcal{Z} \otimes \mathcal{B}$. Suppose $\mathcal{B}$ is an ℓ-qubit system, assume $\dim(\mathcal{B}) \leq \dim(\mathcal{X} \otimes \mathcal{Z})$. Then*

$$H_{\min}(X|ZB)_\rho \geq H_{\min}(X|Z)_\rho - 2\ell. \tag{III.1}$$

Moreover, when $\rho = \rho_{XZB}$ is a separable state on the space $(\mathcal{X} \otimes \mathcal{Z}) \otimes \mathcal{B}$, namely, $\rho_{XZB} = \sum_k p_k \rho^k_{XZ} \otimes \rho^k_B$, then

$$H_{\min}(X|ZB)_\rho \geq H_{\min}(X|Z)_\rho - \ell. \tag{III.2}$$

[1] "rHILL" stands for "relaxed HILL" and refers to the fact that we do not require their partial trace agreed, i.e., $\mathrm{Tr}_{\mathcal{X}}(\sigma_{XB}) = \mathrm{Tr}_{\mathcal{X}}(\rho_{XB})$. Under standard cryptographic assumptions, the analogous statement for (standard) HILL pseudoentropy is false [16].

Remark 3. *There are several chain rules for various quantum entropy notions in the literature [18], [19], [20], [21], [22], but they consider the relation between $H_{\min}(X|ZB)$ and $H_{\min}(XB|Z)$, which is commonly studied in quantum information theory. Motivated by cryptographic applications, the difference between $H_{\min}(X|ZB)$ and $H_{\min}(X|Z)$ captures how much entropy can $(X|Z)$ loss given an additional leakage B. We discovered an interesting application of the quantum Leakage Chain Rule – it provides a much simpler lower bound proof of* superdense coding *[23]. We refer to [11] for more detail.*

c) Leakage Chain Rule for quantum HILL pseudoentropy: The classical Leakage Chain Rule for rHILL pseudoentropy, first proved by [1], [10] and improved by [24], [25], states that for a joint distribution (X, Z, B) where B consists of $\ell = O(\log \kappa)$ bits,

$$H^{\mathsf{rHILL}}(X|Z) \geq k \Rightarrow H^{\mathsf{rHILL}}(X|Z,B) \geq k - \ell.$$

The leakage chain rule is an important property for pseudoentropy and has a number of applications in cryptography, such as leakage-resilient cryptography [1], memory delegation [2], and deterministic encryption [26].

In this work, we prove that this Leakage Chain Rule can be generalized to handle quantum leakage B when both the source X and the prior leakage Z remain classical.

Theorem 4 (Quantum Pseudoentropy Leakage Chain Rule; informal)**.** *Let ρ_{XZB} be a ccq-state, where X and Z are classical and B consists of ℓ qubits, for $\ell = O(\log \kappa)$, where κ is the security parameter. Then*

$$H^{\mathsf{rHILL}}(X|Z)_\rho \geq k \Rightarrow H^{\mathsf{rHILL}}(X|Z,B)_\rho \geq k - \ell.$$

Note that since X, Z are classical, ρ_{ZXB} is separable on the space $(\mathcal{X} \otimes \mathcal{Z}) \otimes \mathcal{B}$; this is why the entropy has a lost of at most ℓ bits of entropy, rather than 2ℓ (c.f., Theorem 2).

Theorem 4 is proved by a quantum generalization of the *Leakage Simulation Lemma* [27], [28], [4] to its quantum analogue (which implies Theorem 4 immediately). In fact, there are two classical proofs of the Leakage Simulation Lemma: one based on the Min-Max Theorem and one based on Boosting. We show how to generalize both techniques to the quantum setting in the full version, which may be of independent interest. Our proofs also rely on efficient algorithms for quantum tasks such as *POVM tomography* and *quantum circuit synthesis* to construct efficient reductions. This leads to a variant of POVM tomography problem that merits further study.

An interesting open question is to prove the leakage chain rule when the source X and/or the prior leakage

Z are quantum. In particular, handling a prior quantum leakage seems important for applications to leakage-resilient cryptography with quantum leakage, which is discussed in the next section.

IV. Application to Quantum Leakage-Resilient Stream-Ciphers

In this section, we demonstrate an application of computational quantum entropy to leakage-resilient cryptography, where we seek to construct cryptographic protocols that maintain secure even if the side information about the honest parties' secrets leak to an adversary. Specifically, we construct a leakage-resilient stream-cipher that is secure against *quantum leakage*. To the best of our knowledge, this is the first result on quantum leakage in the computational setting.

Classical leakage-resilient stream-ciphers were investigated in the seminal work of Dziembowski and Pietrzak [1], where they considered the security of a stream-cipher SC in the *only computation leaks* model [29] with continual leakage. Specifically, let S_i denote the secret state of SC. At each round i when the stream cipher evaluates $(S_{i+1}, X_{i+1}) = \mathsf{SC}(S_i)$, an adversary can adaptively chooses any leakage function f_i and learns the output of f_i applied to the part of S_i involved in the computation of $\mathsf{SC}(S_i)$. Under the assumption that the leakage functions are efficient and of bounded output length $\ell = O(\log \kappa)$[2], they proved that the output of the i-th round remains pseudorandom given the output and leakage of the first $i-1$ rounds. While the length of each leakage is bounded, in total the adversary can collect long leakage accumulated over many rounds.

Now we consider the case when the leakage is quantum (where the stream-cipher remains classical). Namely, the output of the leakage functions become a bounded-length quantum state. We show that the construction of Dziembowski and Pietrzak [1] remains secure against quantum leakage in the bounded-quantum-storage model [30], [31], [32], [33], where the adversary has limited quantum memory (but no restriction on its classical memory). This model was previously investigated in the literature as a way to bypass impossibility results [30], [32], [33] or to prove security [31].

Theorem 5 (Quantum Leakage-Resilient Stream-Cipher; informal)**.** *Assuming the existence of quantum-secure pseudorandom generators, there exists quantum leakage-resilient stream-cipher secure against bounded quantum storage adversaries with $O(\log \kappa)$ quantum memory and $\mathrm{poly}(\kappa)$ circuit size, where κ is the security parameter.*

We note that both bounds on the leakage and quantum storage are logarithmic in the security of the underlying primitives. If the PRG has exponential security, then the leakage and adversary's quantum storage can be linear in the size of the secret state.

The reason that we need the assumption of bounded quantum storage is that, over many rounds, the adversary accumulates auxiliary quantum information and we do not know how to extend our Pseudoentropy Leakage Chain Rule (Theorem 4) to the case that there is quantum prior knowledge. When the prior knowledge is classical, the Leakage Chain Rule holds. Then we can use alternating extraction to circumvent this obstacle as in [1].

[2]Note that both assumptions are necessary. Without the efficiency assumption, the leakage function can invert the secret state and leak on the initial secret S_0 bit by bit. Without the length bound, the adversary can learn the entire new secret state.

Acknowledgments

KMC is grateful to Krzysztof Pietrzak for an inspiring discussion that led to this research. CYL acknowledges useful discussions with Todd A. Brun and Nengkun Yu.

References

[1] S. Dziembowski and K. Pietrzak, "Leakage-resilient cryptography," in *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pp. 293–302, 2008.

[2] K. Chung, Y. T. Kalai, F. Liu, and R. Raz, "Memory delegation," in *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pp. 151–168, 2011.

[3] B. Fuller, A. O'Neill, and L. Reyzin, *A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy*, pp. 582–599. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[4] K. Chung, E. Lui, and R. Pass, "From weak to strong zero-knowledge and applications," in *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, pp. 66–92, 2015.

[5] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM J. Comput.*, vol. 28, no. 4, pp. 1364–1396, 1999.

[6] I. Haitner, O. Reingold, S. P. Vadhan, and H. Wee, "Inaccessible entropy," in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pp. 611–620, 2009.

[7] R. Impagliazzo, "Hard-core distributions for somewhat hard problems," in *36th Annual Symposium on Foundations of Computer Science, Milwaukee, Wisconsin, 23-25 October 1995*, pp. 538–545, 1995.

[8] B. Green and T. Tao, "The primes contain arbitrarily long arithmetic progressions," *Annals of Mathematics*, pp. 481–547, 2008.

[9] T. Tao and T. Ziegler, "The primes contain arbitrarily long polynomial progressions," *Acta Mathematica*, vol. 201, no. 2, pp. 213–305, 2008.

[10] O. Reingold, L. Trevisan, M. Tulsiani, and S. P. Vadhan, "Dense subsets of pseudorandom sets," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 15, no. 045, 2008.

[11] Y.-H. Chen, K.-M. Chung, C.-Y. Lai, S. P. Vadhan, and X. Wu, "Computational notions of quantum min-entropy," *arXiv preprint arXiv:1704.07309 [cs.CR]*, 2017.

[12] M. J. Bremner, C. Mora, and A. Winter, "Are random pure states useful for quantum computation?," *Physical review letters*, vol. 102, no. 19, p. 190502, 2009.

[13] D. Gross, S. T. Flammia, and J. Eisert, "Most quantum states are too entangled to be useful as computational resources," *Physical review letters*, vol. 102, no. 19, p. 190501, 2009.

[14] F. G. Brandao, A. W. Harrow, and M. Horodecki, "Local random quantum circuits are approximate polynomial-designs," *arXiv preprint arXiv:1208.0692*, 2012.

[15] F. G. Brandão, A. W. Harrow, and M. Horodecki, "Efficient quantum pseudorandomness," *Physical review letters*, vol. 116, no. 17, p. 170502, 2016.

[16] S. Krenn, K. Pietrzak, and A. Wadia, "A counterexample to the chain rule for conditional HILL entropy - and what deniable encryption has to do with it," in *TCC*, pp. 23–39, 2013.

[17] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner, "Impossibility of growing quantum bit commitments," *Physical review letters*, vol. 107, no. 9, p. 090502, 2011.

[18] R. Renner, "Security of quantum key distribution," in *Ausgezeichnete Informatikdissertationen 2005*, pp. 125–134, 2005.

[19] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, "Chain rules for smooth min- and max-entropies," *ArXiv e-prints*, May 2012.

[20] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum renyi entropies: a new definition and some properties," *CoRR*, vol. abs/1306.3142, 2013.

[21] F. Dupuis, "Chain rules for quantum rényi entropies," *Journal of Mathematical Physics*, vol. 56, no. 2, p. 022203, 2015.

[22] M. Tomamichel, "Quantum information processing with finite resources - mathematical foundations," *CoRR*, vol. abs/1504.00233, 2015.

[23] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, Nov 1992.

[24] B. Fuller and L. Reyzin, "Computational entropy and information leakage," *IACR Cryptology ePrint Archive*, vol. 2012, p. 466, 2012.

[25] M. Skorski, "Modulus computational entropy," in *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013, Proceedings*, pp. 179–199, 2013.

[26] B. Fuller, A. O'Neill, and L. Reyzin, "A unified approach to deterministic encryption: New constructions and a connection to computational entropy," *Journal of Cryptology*, vol. 28, no. 3, pp. 671–717, 2015.

[27] L. Trevisan, M. Tulsiani, and S. P. Vadhan, "Regularity, boosting, and efficiently simulating every high-entropy distribution," in *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pp. 126–136, 2009.

[28] D. Jetchev and K. Pietrzak, "How to fake auxiliary input," in *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pp. 566–590, 2014.

[29] S. Micali and L. Reyzin, "Physically observable cryptography (extended abstract)," in *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, pp. 278–296, 2004.

[30] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, "Cryptography in the bounded quantum-storage model," in *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23-25 October 2005, Pittsburgh, PA, USA, Proceedings*, pp. 449–458, 2005.

[31] R. T. König and B. M. Terhal, "The bounded-storage model in the presence of a quantum adversary," *IEEE Trans. Information Theory*, vol. 54, no. 2, pp. 749–762, 2008.

[32] S. Wehner and J. Wullschleger, "Composable security in the bounded-quantum-storage model," in *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations*, pp. 604–615, 2008.

[33] D. Unruh, "Concurrent composition in the bounded quantum storage model," in *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pp. 467–486, 2011.