Pseudoentropy

Summary of PhD Dissertation

Maciej Skorski

September 28, 2018

1 Introduction

The notion of *pseudoentropy* [ILL89; HILL99] was introduced as a tool for extending classical information-theoretic entropy (which doesn't address computational limitations) to the computational world, where all uncertainty needs to be quantified with respect to capabilities (computational resources) and prior knowledge (e.g. leakages). A simple example is pseudorandom generator, whose outputs look unbiased to computationally restricted observers, but are statistically biased under no computational constraints.

Pseudoentropy has been recognized as a useful technical tool and convenient unifying language in various problems lying at the intersection of cryptography, computational complexity and information-theory. Some of them are breakthrough, world-famous results. For example, quantifying randomness by psuedoentropy is an important ingredient of the construction of pseudorandom generators from one-way functions [HILL99]. Another example is a computationally efficient variant of the Green-Tao-Ziegler Dense Model Theorem [RTTV08; Zha11] that can be easily proved in the language of pseudoentropy.

The dissertation presents the author's contribution to unify and further develop pseudoentropy notions. The key technical ingredient and novelty is the *convex optimization approach*, which is demonstrated to be quite powerful in unifying and strengthening results.

2 Summary of Results

The thesis includes 5 papers that are a representative selection of the research done by the author on the pseudoentropy project.

2.1 Equivalence of Most Important Pseudoentropy Variants in High-Entropy Regimes

While information-theoretic entropies are defined by simple algebraic formulas, the case of pseudoentropy is much more complicated. Firsly, the added layer of "computational capabilities" makes the definitions much less analytically tractable; for example the most widely used variant relates peudoentropy to information-theoretic entropy by means of game theory [BSW03]. Secondly, we have several definition depending on applications as no single approach can fit all purposes.

It is thus important to clarify relations and differences between different approaches used. The dissertation presents a result that - somewhat surprisingly - shows the equivalence of two important but much different pseuodoentropy definitions, in certain parameter regimes; this in turn has interesting implications for key derivation. This is joint work with Krzysztof Pietrzak and Alexander Golovnev [SGP15].

2.2 Lower Bounds for Pseudoentropy Chain Rules and Transformations

There are two important tools to manipulate pseudoentropy notions: (a) chain rules [DP08; RTTV08] which quantify the randomness decrease when addition information is revealed, and (b) transformations which allow for switching between stronger and relaxed variants of definitions [BSW03].

Unfortunately, chain rules and transformations suffer from heavy losses in quality parameters; this is further reflected in (quite) weak bounds in leakage resilient cryptography (e.g. [DP08; Pie09]). One might hope for improving pseudoentropy bounds, and then claim better quality for some cryptographic constructions.

The dissertation presents a result which gives a negative answer: existing bounds for chain rules and transformations are basically optimal. This is a join work with Krzysztof Pietrzak [PS16].

2.3 Simulating Auxiliary Information

Most of leakage-resilient cryptography results guarantee security as long as leakages are "simple" functions of the secret state. The dissertation presents a construction of a generic *leakage simulator* [Skó16], which is efficient as long as leakage is sufficiently short. This nicely unifies and simplifies some proofs, e.g. constructions of leakage-resilient stream ciphers [JP14]. The presented result improves upon previous constructions [JP14; VZ13]. The techniques found recently further applications to combinatoric constructions (variants of Semeredy's Regularity Lemma) [Skó17a].

2.4 Best Generic Attacks Against Pseudoentropy

As pseudoentropy takes adversarial resources into account, one expects the amount of pseudoentropy to decrease when the adversary utilizes more time/space. The thesis present a result, being a joint work with Krzyszof Pietrzak, which gives the optimal tradeoff between pseudoentropy amount and adversarial resources [PS17]. This result can be thought of as the *amount-quality tradeoff* for pseudoentropy, and nicely extends the well-known time-advantage tradeoff for peudorandom generators found by De et. all [DTT10].

2.5 Geometrical Characterizations of Pseudoentropy

As already advertised, the results summarized in the thesis leverage convex optimization techniques. An overview of this approach is presented in the paper [Sko15a], included as a chapter of the thesis. It discusses how cryptographic "indistinguishability", which is used to define pseudorandomness and pseudoentropy, can be studied by convex optimization methods. Some interesting applications are discussed, for example a short proof of Dense Model Theorem with optimal bounds.

References

[Bar+11] Boaz Barak et al. "Leftover Hash Lemma, Revisited". In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. 2011, pp. 1–20. DOI: 10.1007/978-3-642-22792-9_1. URL: http://dx.doi.org/10.1007/978-3-642-22792-9_1.

[BSW03] Boaz Barak, Ronen Shaltiel, and Avi Wigderson. "Computational Analogues of Entropy". In: *Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques, 6th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2003 and 7th International Workshop on Randomization and Approximation Techniques in Computer Science, RANDOM 2003, Princeton, NJ, USA, August 24-26, 2003, Proceedings*. 2003, pp. 200–215. DOI: 10.1007/978-3-540-45198-3_18. URL: http://dx.doi.org/10.1007/978-3-540-45198-3_18.

[CKLR11] Kai-Min Chung et al. "Memory Delegation". In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. 2011, pp. 151–168. DOI: 10.1007/978-3-642-22792-9_9. URL: http://dx.doi.org/10.1007/978-3-642-22792-9_9.

[DP08] Stefan Dziembowski and Krzysztof Pietrzak. "Leakage-Resilient Cryptography". In: *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*. 2008, pp. 293–302. DOI: 10.1109/FOCS.2008.56. URL: http://dx.doi.org/10.1109/FOCS.2008.56.

[DPW14] Yevgeniy Dodis, Krzysztof Pietrzak, and Daniel Wichs. "Key Derivation without Entropy Waste". In: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*. 2014, pp. 93–110. DOI: 10.1007/978-3-642-55220-5_6. URL: http://dx.doi.org/10.1007/978-3-642-55220-5_6.

[DTT10] Anindya De, Luca Trevisan, and Madhur Tulsiani. "Time Space Tradeoffs for Attacks against One-Way Functions and PRGs". In: *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*. 2010, pp. 649–665. DOI: 10.1007/978-3-642-14623-7_35. URL: http://dx.doi.org/10.1007/978-3-642-14623-7_35.

[DY13] Yevgeniy Dodis and Yu Yu. "Overcoming Weak Expectations". In: *TCC*. 2013, pp. 1–22. DOI: 10.1007/978-3-642-36594-2_1. URL: http://dx.doi.org/10.1007/978-3-642-36594-2_1.

[FOR12] Benjamin Fuller, Adam O'Neill, and Leonid Reyzin. "A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy". In: *Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Proceedings*. 2012, pp. 582–599. DOI: 10.1007/978-3-642-28914-9_33. URL: http://dx.doi.org/10.1007/978-3-642-28914-9_33.

[FR11] Benjamin Fuller and Leonid Reyzin. *Computational entropy and information leakage. 2011*. Available fro m http://www. cs. bu. edu/fac/reyzin. 2011.

[GW11] Craig Gentry and Daniel Wichs. "Separating succinct non-interactive arguments from all falsifiable assumptions". In: *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*. 2011, pp. 99–108. DOI: 10.1145/1993636.1993651. URL: http://doi.acm.org/10.1145/1993636.1993651.

[HILL99] Johan Håstad et al. "A Pseudorandom Generator from any One-way Function". In: *SIAM J. Comput.* 28.4 (1999), pp. 1364–1396. DOI: 10.1137/S0097539793244708. URL: http://dx.doi.org/10.1137/S0097539793244708.

[HLR07] Chun-Yuan Hsiao, Chi-Jen Lu, and Leonid Reyzin. "Conditional Computational Entropy, or Toward Separating Pseudoentropy from Compressibility". In: *Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings*. 2007, pp. 169–186. DOI: 10.1007/978-3-540-72540-4_10. URL: http://dx.doi.org/10.1007/978-3-540-72540-4_10.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby. "Pseudo-random Generation from One-way Functions". In: *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*. STOC '89. Seattle, Washington, USA: ACM, 1989, pp. 12–24. ISBN: 0-

89791-307-8. DOI: 10.1145/73007.73009. URL: http://doi.acm.org/10.1145/73007.73009.

[JP14] Dimitar Jetchev and Krzysztof 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*. 2014, pp. 566–590. DOI: 10.1007/978-3-642-54242-8_24. URL: http://dx.doi.org/10.1007/978-3-642-54242-8_24.

[KPW13] Stephan Krenn, Krzysztof Pietrzak, and Akshay Wadia. "A Counterexample to the Chain Rule for Conditional HILL Entropy - And What Deniable Encryption Has to Do with It". In: *TCC*. 2013, pp. 23–39. DOI: 10.1007/978-3-642-36594-2_2. URL: http://dx.doi.org/10.1007/978-3-642-36594-2_2.

[Pie09] Krzysztof Pietrzak. "A Leakage-Resilient Mode of Operation". In: *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*. 2009, pp. 462–482. DOI: 10.1007/978-3-642-01001-9_27. URL: http://dx.doi.org/10.1007/978-3-642-01001-9_27.

[PS16] Krzysztof Pietrzak and Maciej Skórski. "Pseudoentropy: Lower-Bounds for Chain Rules and Transformations". In: *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part I*. 2016, pp. 183–203. DOI: 10.1007/978-3-662-53641-4_8. URL: https://doi.org/10.1007/978-3-662-53641-4_8.

[PS17] Krzysztof Pietrzak and Maciej Skorski. "Non-Uniform Attacks Against Pseudoentropy". In: *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland*. 2017, 39:1–39:13. DOI: 10.4230/LIPIcs.ICALP.2017.39. URL: https://doi.org/10.4230/LIPIcs.ICALP.2017.39.

[Rén61] Alfréd Rényi. "On Measures of Entropy and Information". In: *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*. Berkeley, Calif.: University of California Press,

1961, pp. 547–561. URL: http://projecteuclid.org/euclid.bsmsp/1200512181.

[Rey11] Leonid Reyzin. "Some Notions of Entropy for Cryptography - (Invited Talk)". In: *Information Theoretic Security - 5th International Conference, ICITS 2011, Amsterdam, The Netherlands, May 21-24, 2011. Proceedings*. 2011, pp. 138–142. DOI: 10.1007/978-3-642-20728-0_13. URL: http://dx.doi.org/10.1007/978-3-642-20728-0_13.

[RTTV08] Omer Reingold et al. "Dense Subsets of Pseudorandom Sets". In: *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*. 2008, pp. 76–85. DOI: 10.1109/FOCS.2008.38. URL: http://dx.doi.org/10.1109/FOCS.2008.38.

[SGP15] Maciej Skorski, Alexander Golovnev, and Krzysztof Pietrzak. "Condensed Unpredictability". In: *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I*. 2015, pp. 1046–1057. DOI: 10.1007/978-3-662-47672-7_85. URL: http://dx.doi.org/10.1007/978-3-662-47672-7_85.

[Sha01] C. E. Shannon. "A Mathematical Theory of Communication". In: *SIGMOBILE Mob. Comput. Commun. Rev.* 5.1 (Jan. 2001), pp. 3–55. ISSN: 1559-1662. DOI: 10.1145/584091.584093. URL: http://doi.acm.org/10.1145/584091.584093.

[Sko15a] Maciej Skorski. "Metric Pseudoentropy: Characterizations, Transformations and Applications". In: *Information Theoretic Security - 8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings*. 2015, pp. 105–122. DOI: 10.1007/978-3-319-17470-9_7. URL: http://dx.doi.org/10.1007/978-3-319-17470-9_7.

[Sko15b] Maciej Skorski. "Nonuniform Indistinguishability and Unpredictability Hardcore Lemmas: New Proofs and Applications to Pseudoentropy". In: *Information Theoretic Security - 8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings*. 2015, pp. 123–140. DOI: 10.1007/978-3-319-17470-9_8. URL: http://dx.doi.org/10.1007/978-3-319-17470-9_8.

[Sko15c] Maciej Skorski. "On Provable Security of wPRF-Based Leakage-Resilient Stream Ciphers". In: *Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings*. 2015, pp. 391–411. DOI: 10.1007/978-3-319-26059-4_22. URL: http://dx.doi.org/10.1007/978-3-319-26059-4_22.

[Skó16] Maciej Skórski. "Simulating Auxiliary Inputs, Revisited". In: *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part I*. 2016, pp. 159–179. DOI: 10.1007/978-3-662-53641-4_7. URL: https://doi.org/10.1007/978-3-662-53641-4_7.

[Sko17] Maciej Skorski. "Lower Bounds on Key Derivation for Square-Friendly Applications". In: *34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany*. 2017, 57:1–57:12. DOI: 10.4230/LIPIcs.STACS.2017.57. URL: https://doi.org/10.4230/LIPIcs.STACS.2017.57.

[Skó17a] Maciej Skórski. "A Cryptographic View of Regularity Lemmas: Simpler Unified Proofs and Refined Bounds". In: *Theory and Applications of Models of Computation - 14th Annual Conference, TAMC 2017, Bern, Switzerland, April 20-22, 2017, Proceedings*. 2017, pp. 586–599. DOI: 10.1007/978-3-319-55911-7_42. URL: https://doi.org/10.1007/978-3-319-55911-7_42.

[Skó17b] Maciej Skórski. "On the Complexity of Breaking Pseudoentropy". In: *Theory and Applications of Models of Computation - 14th Annual Conference, TAMC 2017, Bern, Switzerland, April 20-22, 2017, Proceedings*. 2017, pp. 600–613. DOI: 10.1007/978-3-319-55911-7_43. URL: https://doi.org/10.1007/978-3-319-55911-7_43.

[VZ12] Salil P. Vadhan and Colin Jia Zheng. "Characterizing pseudoentropy and simplifying pseudorandom generator constructions". In: *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*. 2012, pp. 817–836. DOI: 10.1145/2213977.2214051. URL: http://doi.acm.org/10.1145/2213977.2214051.

[VZ13] Salil P. Vadhan and Colin Jia Zheng. "A Uniform Min-Max Theorem with Applications in Cryptography". In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*. 2013, pp. 93–110. DOI: 10.1007/978-3-642-40041-4_6. URL: http://dx.doi.org/10.1007/978-3-642-40041-4_6.

[Zha11] Jiapeng Zhang. "On the query complexity for Showing Dense Model". In: *Electronic Colloquium on Computational Complexity (ECCC)* 18 (2011), p. 38. URL: http://eccc.hpi-web.de/report/2011/038.