Pseudoentropy

PhD Dissertation Talk

University of Warsaw

May 23, 2023

- ✔ Overviews the goals, resources, and deliverables of my PhD project.
- ✔ Demonstrates/sketches interesting techniques used in the dissertation.
- ✔ Defends my position on the dissertation form, in view of reviews received 🛡.
- ❌ Avoids complex definitions and proofs for brevity's sake (see the papers) ⏱.
- ❌ Does not assess my own academic KPIs (see the documentation) 😳.

Outline

Outline

Credits

I am particularly grateful:

- ❤️ for love, to my wife Aneta
- 💰 for funding and know-how, to my advisor Stefan Dziembowski
- 💡 for merit support, to my co-advisor Krzysztof Pietrzak
- 👏 for motivation and recognition, to dozens of people with whom I shared ideas: research collaborators, reviewers, audience of my talks 😊

Funding

My PhD research received support from numerous funding sources:

FNP Foundation for Polish Science — Ideas for Poland

FNP Foundation for Polish Science — WELCOME

erc European Research Council — TOCNeT

National Science Centre Poland — PRELUDIUM

$+$ several travel grants from various research institutions

Outline

About Pseudoentropy

- Introduced in [ILL89, HILL99] as a **computational variant of information-theoretic entropy**.
- Recognized as a **useful tool and convenient language** in research around cryptography, computational complexity and information theory. Examples:
  - Pseudorandom generators from one-way functions [HILL99]
  - Computational Dense Model Theorem [RTTV08, Zha11], improving upon the key ingredient in the results of Green-Tao-Ziegler [GT08, TZ08].
- Promising but messy: suffers from **contextual definitions** and **insufficiently developed foundations**.

Goals

My PhD project set these goals:

- **improve understanding of foundational properties** of pseudoentropy notions
- **demonstrate further technical applications**
- optionally, identify **new inspirational application areas**

Contribution

Works presented under the scope of this PhD project:

- ✔ **obtained characterizations and manipulation rules** for pseudoentropy notions, using **convex analysis as a toolbox**, as well as **impossibility results**
- ✔ **simplified some of existing technical proofs**, for instance of Dense Model Theorem and of Computational Simulators
- ✔ **developed machine-learning inspired framework** for proving computational indistinguishability

My self-assesment:

- 🥅 these works contributed to the goals 🧹, ⚙️ and 💎 respectively.
- 🏃 goals were set broadly, leaving still room for improvement

Outline

Outline

Background

- Pseudoentropy at least k when the distribution behaves *nearly as well* as with information-theoretic (min)entropy k in *cryptographic games*.
- Program-input games used in definitions
  (a) Distinguish: discriminate between two distributions based on a sample. Pseudoentropy example: for a pseudorandom generator G from d-bit seeds to k-bit outputs, $|\mathbb{E}\mathrm{D}(G(U_d)) - \mathbb{E}\mathrm{D}(U_k)| \leqslant \epsilon$ for small ϵ and comp. bounded D.
  (b) Predict: guess a sampled outcome. Pseudoentropy example: a one way function f satisfies $\mathbf{P}\{f(\mathrm{D}(f(x))) = f(x)\} \leqslant 2^{-k}$ for computationally bounded D and large k.
  (c) Compress: decoding / encoding games, see [Yao82, BSW03].
  (d) ... and even more exotic examples, see [HRVW09].

Outline

1. Acknowledgments 🙏
2. Introduction 🏁
3. Detailed Overview 🔎
   - Preliminaries
   - Geometric Characterizations of Pseudoentropy 🧹⚙️
   - Unpredictability Pseudoentropy 🧹
   - Best Generic Attacks on Pseudoentropy ⚙️
   - Lower Bounds for Pseudoentropy Chain Rules and Transformations ⚙️
   - Simulating Auxiliary Information 💎
4. References 📚
5. Discussion 💬

Outline

- 📖 Indistinguishability quantifies how close are two distributions under a given class of computationally bounded tests.
- ❓ What is the geometrical meaning of indistinguishability?
- ✋ Computational indistinguishability can be **characterized by inseparability by a class of feasible hyperplanes**. The separation margin can be determined analytically too!

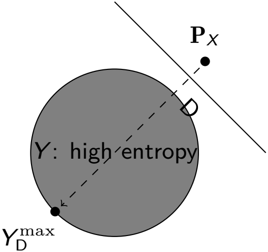
Contribution

The characterizations [Sko15a] has found the following applications:

- Unifying unpredictability-based and indistinguishability-based pseudoentropy notions [SGP15]
- Short proof of the Dense Model Theorem [Sko15c]
- New proofs of Hardcore Lemmas [Sko15c]
- Further applications to key derivation [Sko17b]
- Simplifies other technical arguments [VZ12]

Technique (Sketch)

- In program-input indistinguishability games, it makes sense to **characterize the optimal input player** Y against a given program player D.
- View D as a *separating hyperplane*, *maximize margin* with high-entropy Y.



Symbol/Operator	Crypto	Geometry
X	candidate distribution	
Y	input player	feasible point
D	distinguisher/program player	separating hyperplane
$\mathbf{E}\mathrm{D}(Y)$	expectation	$\mathrm{D}\cdot\mathbf{P}_Y$ (dot-product)
$\epsilon = \mathbf{E}\mathrm{D}(Y) - \mathbf{E}\mathrm{D}(X)$	advantage	separation margin

Figure 1: Geometrical meaning of cryptographic indistinguishability.

- **Closed-form solutions found** in interesting cases by **convex optimization**. For pseudoentropy of at least k bits against attackers $\mathcal{D}$ with advantage ϵ:

$$\forall \mathrm{D}\in\mathcal{D}: \quad \mathbf{E}\mathrm{D}(X) \leqslant 2^{-k}|\mathrm{D}| + \epsilon$$

instead of the standard depth-2 formula $\forall \mathrm{D}\exists Y : \mathbf{H}_\infty(Y) \geqslant k \& \ \mathbf{E}\mathrm{D}(X) \leqslant \mathbf{E}\mathrm{D}(Y) + \epsilon$.

- Characterization depend on feasible distinguishers and the baseline entropy.

Outline

Outline

- Applications of pseudoentropy use different notions, most commonly unpredictability-based and indistinguishability-based.
- Are unpredictability and indistinguishability entropies different? Note: usually, distinguishing is easier than predicting[1].
- Surprisingly, **equivalent in high-entropy regimes**!

[1]Think of discriminating between dogs and cats versus predicting the breed.

Contribution

The following result was obtained [SGP15]:

- **equivalence of unpredictability and indistinguishability** pseudoentropy definitions in **high-entropy regimes**, namely $n - O(\log n)$ for n-bit strings,
- **geometric characterizations as a workhorse** of the proof.

Technique (Sketch)

The proof strategy is to *constructively convert a distinguisher into a predictor*:

(a) Indistinguishability fails: $\mathbf{E}\mathsf{D}(X) \geqslant \mathbf{E}\mathsf{D}(Y) + \epsilon$ for all Y of min-entropy k.

(b) $\mathbf{E}\mathsf{D}(X) \geqslant |\mathsf{D}|/2^k + \epsilon$ for boolean D, by geometrical characterizations (!)

(c) Sample A from the image of D, then $\mathbf{P}\{A = X\} > 2^{-k} + \frac{\epsilon}{\#\mathsf{D}}$.

(d) Approximate image sampling by *rejection sampling* ℓ times, then

$$\mathbf{P}\{A = X\} > \left(2^{-k} + \frac{\epsilon}{\#\mathsf{D}}\right) \cdot \left(1 - \frac{\#\mathsf{D}}{2^n}\right)^{\ell}.$$

(e) $\mathbf{P}\{A = X\} > 2^{-k}$ when $\ell \approx 2^{n-k}/\epsilon$ independently of $\#\mathsf{D}$!

⚠ More sophisticated rejection-sampling handles X with auxiliary input Z.

Outline

Outline

- Applications of pseudoentropy assume strength parameters that propagate through reduction proofs. Not clear what regimes are non-trivial to start with.
- Can we characterize when quality parameters are non-trivial?
- Yes, by time-advantage tradeoffs - similarly to pseudorandomness!

Contribution

The following result was obtained [Sko17b]:

- generic attacks with time t succeed against psuedoentropy amount k with advantage $\epsilon = O\left(\sqrt{t/2^k}\right)$.
- generalization of the famous time-advantage tradeoffs against pseudorandomness [DTT10].

Technique (Sketch)

The proof leverages **random walk techniques**, see also [Ber97].

(a) Let D : $\{0,1\}^n \rightarrow \{-1,1\}$ be fully random (Rademacher), then $|\mathbf{E}\mathrm{D}(X) - \mathbf{E}\mathrm{D}(Y)| \approx \|\mathbf{P}_X - \mathbf{P}_Y\|_2$ w.h.p. (random walks theory [Haa81]).

(b) By slicing the domain $\{0,1\}^n$ into t random parts and flipping the signs accordingly, we can have $|\mathbf{E}\mathrm{D}'(X) - \mathbf{E}\mathrm{D}'(Y)| \approx t \cdot \frac{\|\mathbf{P}_X - \mathbf{P}_Y\|_2}{\sqrt{t}}$ w.h.p., with $O(t)$ extra memory.

(c) Under mild assumptions on Y (far from having k bits of min-entropy) the attack achieves advantage $\epsilon \approx \sqrt{t/2^k}$. Compare with $\epsilon \approx \sqrt{t/2^n}$ for pseudorandomness!

(d) "Random" can be weakened to $O(1)$-**wise independent**, and the construction complexity is indeed $O(t)$, alternatively complexity t yields $\epsilon = O(\sqrt{t/2^k})$!

Outline

Outline

- Applications of pseudoentropy **heavily rely on manipulation rules**, particularly chain rules and transformations [BSW03, FOR12]. However, their use **weakens security guarantees**, due to tradeoffs in quality parameters **caused by reduction proofs**.
- Can we improve known manipulation rules?
- No, not by black-box reductions!

Contribution

The following results were obtained in [PS16]:

- **Impossibility of better proofs** by black-box reductions!
- A **probabilistic construction of an oracle**, of independent interest, inspired by the earlier work on limitations of dense model theorems [Zha11].
- Inspired techniques used in research on black-box limitations of auxiliary input simulators [CCL18].

Techniques (Sketch)

(a) Proofs, in case of indistinguishability-based pseudoentropy, rely on *building distinguishers from distinguishers in other setups*. In particular, we have $D' = \mathbb{I}\{\sum_i w_i D_i > t_0\}$ in the proof of the Dense Model Theorem [Zha11] or transformations [BSW03, Sko15b].

(b) Loosely speaking, black-box reductions *aggregate distinguishers by high-level operations*. To prove the need of many operations (queries) we manipulate distinguishers at low-level by *choosing values probabilistically and sophistically*!

(c) Examples (from the proof, see also [CCL18]):
   (1) $D_i \sim \mathrm{Bern}(1/2+\epsilon)$ on a small set and $D_i \sim \mathrm{Bern}(1/2)$ elsewhere.
   (2) $D_i \sim \mathrm{Bern}(1/2+\epsilon)$ and $D_i \sim \mathrm{Bern}(1/2-\epsilon)$ on complementary random subsets.

⚠ High-level aggregations are essential. For example, without them Dense Model Theorems can fail [IM20].

Outline

Outline

- In security proofs, it helps to model leakages as explicit functions of secrets [JP14].
- What leakages can be modelled as functions of secrets?
- Short leakages can be efficiently simulated!

Contribution

The following important results were obtained [Sko16a]:

- Construction of a simulator for m bits of leakage which makes only $2^{O(m)}\epsilon^{-2}$ calls to achieve ϵ-indistinguishability. Significantly improved upon prior works [VZ13, JP14]
- The reasoning, inspired by ML techniques, **builds on the gradient descent algorithm** and was recognized with the *best student paper award at TCC'16*.
- Inspired follow-up works that solved the simulator problem [CCL18], and generalized the learning framework [Sko16b, Sko17a], and studied quantum pseudoentropy (c.f. Chen's dissertation [Che19]).

Technique (Sketch)

(a) The algorithm below demonstrates the procedure

Algorithm 1: Auxiliary Input Simulator

Data:

- Oracle access to distinguishers/test functions $\mathcal{D}$

Result: Simulator h of $Z \in \{0,1\}^m$ given $X \in \{0,1\}^n$

$\mathbf{P}\{h(x) = z\} \leftarrow 2^{-m}$ `// initialize the solution as uniform`

while $\max_{D\in\mathcal{D}} \mathbf{E}D(X,Z) - \mathbf{E}D(X,h(X)) > \epsilon$ `// as long as can distinguish...`

do

  $\mathbf{P}\{h'(x) = z\} \leftarrow \mathbf{P}\{h(x) = z\} - \gamma D(x,z)$ `// improve candidate`

  $\mathbf{P}\{h'(x) = z\} \leftarrow \mathbf{P}\{h'(x) = z\} + \mathsf{Correct}(x,z)$ `// guarantee constraints`

  $h \leftarrow h'$

end

return h

(b) Outputs an efficient simulator p.d.f., with appropriate γ and Correct operation.

(c) Finishes after $2^{O(m)}\epsilon^{-2}$ steps, proved by "energy" arguments.

(d) Resembles boosting: we learn how to (strongly) simulate from (weak) distinguishers

(e) Resembles convex optimization: with D as subgradient, γ as a stepsize, Correct as a projection operation!

Outline

References I

Bonnie Berger.
The Fourth Moment Method.
SIAM Journal on Computing, 26(4):1188–1207, August 1997.

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*, pages 200–215, 2003.

Yi-Hsiu Chen, Kai-Min Chung, and Jyun-Jie Liao.
On the Complexity of Simulating Auxiliary Input.
In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, volume 10822, pages 371–390. Springer International Publishing, Cham, 2018.

Yi-Hsiu Chen.
Computational Notions of Entropy: Classical, Quantum, and Applications.
PhD thesis, Harvard University, 2019.

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*, pages 649–665, 2010.

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*, pages 582–599, 2012.

References II

Ben Green and Terence Tao.
The primes contain arbitrarily long arithmetic progressions.
Annals of mathematics, pages 481–547, 2008.

Uffe Haagerup.
The best constants in the khintchine inequality.
Studia Mathematica, 70(3):231–283, 1981.

Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby.
A pseudorandom generator from any one-way function.
SIAM J. Comput., 28(4):1364–1396, 1999.

Iftach Haitner, Omer Reingold, Salil Vadhan, and Hoeteck Wee.
Inaccessible entropy.
In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 611–620, 2009.

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, pages 12–24, New York, NY, USA, 1989. ACM.

Russell Impagliazzo and Sam McGuire.
Comparing computational entropies below majority (or: When is the dense model theorem false?).
arXiv preprint arXiv:2011.06166, 2020.

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*, pages 566–590, 2014.

References III

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 14*, pages 183–203. Springer, 2016.

Omer Reingold, Luca Trevisan, Madhur Tulsiani, and Salil P. Vadhan.
Dense subsets of pseudorandom sets.
In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 76–85, 2008.

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*, pages 1046–1057, 2015.

Maciej Skorski.
Metric pseudoentropy: Characterizations, transformations and applications.
In *Information Theoretic Security - 8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings*, pages 105–122, 2015.

Maciej Skorski.
A new approximate min-max theorem with applications in cryptography.
In *Algorithms and Computation: 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings 26*, pages 653–663. Springer, 2015.

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*, pages 123–140, 2015.

References IV

Maciej Skorski.
Simulating auxiliary inputs, revisited.
In *Theory of Cryptography: 14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part I 14*, pages 159–179. Springer, 2016.

Maciej Skorski.
A subgradient algorithm for computational distances and applications to cryptography.
Cryptology ePrint Archive, 2016.

Maciej Skorski.
Approximating min-max strategies by statistical learning.
2017.

Maciej Skorski.
Lower bounds on key derivation for square-friendly applications.
In *34th Symposium on Theoretical Aspects of Computer Science (STACS 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

Terence Tao and Tamar Ziegler.
The primes contain arbitrarily long polynomial progressions.
2008.

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*, pages 817–836, 2012.

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*, pages 93–110, 2013.

References V

Andrew C Yao.
Theory and application of trapdoor functions.
In *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)*, pages 80–91. IEEE, 1982.

Jiapeng Zhang.
On the query complexity for showing dense model.
Electronic Colloquium on Computational Complexity (ECCC), 18:38, 2011.

Outline

Addressing Reviewers Feedback

R: Editorial changes and reference requests.

M: Addressed, thanks for the feedback!

R: A book-style dissertation would be better than a mixture of conference works.

M: I discussed this form with senior researchers, but found *ineffective*:

- 🥕 Gain citations! 🤔 *Time-consuming, better to keep writing papers.*
- 🥕 Get your PhD distinguished. 🤔 *Prestigious conferences not enough?*
- 💦 Take your time to present it better! 🤔 *Why to work harder? We count conference works when granting junior/senior professorships!*

R: Parts of lengthy works might not have been fully reviewed at conferences.

M: Same can happen for junior professorships, but we had extra reviewers 😌.