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 pseudoentropy 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. Firstly, the added layer of "computational capabilities" makes the definitions much less analytically tractable; for example the most widely used variant relates pseudoentropy 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 pseudoentropy 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 joint 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 [Skő16], 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) [Skő17a].

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 pseudorandom 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 [Skő15a], 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


