Cryptology ePrint Archive: Report 2011/708

Computational Extractors and Pseudorandomness

Dana Dachman-Soled and Rosario Gennaro and Hugo Krawczyk and Tal Malkin

Abstract: Computational extractors are efficient procedures that map a source of sufficiently high min-entropy to an output that is computationally indistinguishable from uniform. By relaxing the statistical closeness property of traditional randomness extractors one hopes to improve the efficiency and entropy parameters of these extractors, while keeping their utility for cryptographic applications. In this work we investigate computational extractors and consider questions of existence and inherent complexity from the theoretical and practical angles, with particular focus on the relationship to pseudorandomness.

An obvious way to build a computational extractor is via the ``extract-then-prg" method: apply a statistical extractor and use its output to seed a PRG. This approach carries with it the entropy cost inherent to implementing statistical extractors, namely, the source entropy needs to be substantially higher than the PRG's seed length. It also requires a PRG and thus relies on one-way functions.

We study the necessity of one-way functions in the construction of computational extractors and determine matching lower and upper bounds on the ``black-box efficiency" of generic constructions of computational extractors that use a one-way permutation as an oracle. Under this efficiency measure we prove a direct correspondence between the complexity of computational extractors and that of pseudorandom generators, showing the optimality of the extract-then-prg approach for generic constructions of computational extractors and confirming the intuition that to build a computational extractor via a PRG one needs to make up for the entropy gap intrinsic to statistical extractors.

On the other hand, we show that with stronger cryptographic primitives one can have more entropy- and computationally-efficient constructions. In particular, we show a construction of a very practical computational extractor from any weak PRF without resorting to statistical extractors.

Category / Keywords: foundations / randomness extractors, pseudo-randomness

Publication Info: A conference version of this paper is published in TCC'2012.

Date: received 28 Dec 2011

Contact author: hugo at ee technion ac il

Available formats: PDF | BibTeX Citation

Version: 20111231:153727 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]