Theoretical Computer Science 554 (2014) 50–63

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

On linear-size pseudorandom generators and hardcore functions

Joshua Baron [a,*], Yuval Ishai [b], Rafail Ostrovsky [c]

[a] RAND Corporation, Santa Monica, CA 90401, USA
[b] Department of Computer Science, Technion, Haifa, Israel
[c] Departments of Mathematics and Computer Science, UCLA, Los Angeles, CA 90095, USA

ARTICLE INFO

Article history:
Received 21 September 2013
Received in revised form 5 May 2014
Accepted 4 June 2014
Available online 10 June 2014

Keywords:
Cryptography
Circuit complexity
Pseudorandom generators
One-way functions

ABSTRACT

We consider the question of constructing pseudorandom generators that simultaneously have linear circuit complexity (in the output length), exponential security (in the seed length), and a large stretch (linear or polynomial in the seed length). We refer to such a pseudorandom generator as an *asymptotically optimal PRG*. We present a simple construction of an asymptotically optimal PRG from any one-way function $f : \{0,1\}^n \to \{0,1\}^n$ which satisfies the following requirements:

1. f can be computed by linear-size circuits;
2. f is $2^{\beta n}$-hard to invert, for some constant $\beta > 0$;
3. f either has *high entropy*, in the sense that the min-entropy of $f(x)$ on a random input x is at least γn where $\beta/3 + \gamma > 1$, or alternatively it is *regular* in the sense that the preimage size of every output of f is fixed.

Known constructions of PRGs from one-way functions can do without the entropy or regularity requirements, but they achieve slightly sub-exponential security (Vadhan and Zheng (2012) [27]).

Our construction relies on a technical result about hardcore functions that may be of independent interest. We obtain a family of hardcore functions $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^{\alpha n}\}$ that can be computed by linear-size circuits for any $2^{\beta n}$-hard one-way function $f : \{0,1\}^n \to \{0,1\}^n$ where $\beta > 3\alpha$. Our construction of asymptotically optimal PRGs uses such hardcore functions, which are obtained via linear-size computable affine hash functions (Ishai et al. (2008) [24]).

1. Introduction

A *pseudorandom generator* (PRG) [6,28] is a deterministic algorithm which stretches a short random seed into a longer output which looks random to any computationally bounded observer. PRGs have numerous applications in cryptography. In particular, they serve as useful building blocks for basic cryptographic tasks such as (symmetric) encryption, commitment, and message authentication.

* Corresponding author.
E-mail addresses: jbaron@rand.org (J. Baron), yuvali@cs.technion.ac.il (Y. Ishai), rafail@cs.ucla.edu (R. Ostrovsky).

http://dx.doi.org/10.1016/j.tcs.2014.06.013
0304-3975/

A seemingly weaker primitive, which satisfies a much milder form of hardness requirement, is a *one-way function* (OWF). A OWF is an efficiently computable function which is hard to invert on a random input. We say that f is $t(n)$*-hard to invert* (or $t(n)$-hard for short) if every algorithm running in time $t(n)$ can find a preimage of $f(x)$ for a random $x \in \{0,1\}^n$ with at most $1/t(n)$ probability, for all sufficiently large n. We say that f is *exponentially hard* if it is $2^{\beta n}$-hard for some constant $\beta > 0$.

Every PRG which significantly stretches its seed is also a OWF. However, because of its crude form of security, a OWF is easier to construct heuristically than a PRG. There are many natural candidates for a OWF (even an exponentially strong OWF) which do not immediately give rise to a similar PRG. This motivated a line of work on constructing PRGs from different types of OWFs, which culminated in the seminal result of Håstad, Impagliazzo, Levin and Luby (HILL) [20] that a PRG can be constructed from an *arbitrary* OWF. More recently, there has been another fruitful line of work on simplifying and improving the efficiency of the HILL construction [21,16–19,15,27].

The main focus in the above works has been on optimizing efficiency under *minimal assumptions*. The present work is motivated by the following dual question: under which assumptions can we obtain *optimal efficiency*? Ideally, we would like to obtain a PRG $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ satisfying the following requirements:

- G has *large stretch*; that is, $l(n) > cn$ or even $l(n) > n^c$ for some constant $c > 1$. A large stretch is crucial for most cryptographic applications of PRGs.
- G has *linear circuit complexity*; that is, the output of G can be computed by a uniform family of (bounded fan-in) boolean circuits of size $O(l(n))$. This implies linear-time computation also in other, more liberal, models such as unbounded fan-in circuits or different flavors of RAM with polynomial-time computable advice.
- G has *exponential security*; that is, there exists a constant $\delta > 0$ such that any algorithm running in time $2^{\delta n}$ can distinguish between the output of G and a truly random string of length $l(n)$ with at most a $2^{-\delta n}$ advantage. In typical PRG applications, exponential security is useful for minimizing the asymptotic length of the secret keys or the amount of true randomness.

We refer to a PRG as above as an *asymptotically optimal PRG*. Using this terminology, the main question we pose in this work is the following:

Which types of one-way functions imply an asymptotically optimal PRG?

The above question is motivated by the broad goal of obtaining efficient cryptographic constructions whose security can be proved under conservative assumptions. Indeed, the efficiency of encryption schemes and other cryptographic applications of PRGs is often dominated by the efficiency of the underlying PRG [24].

An asymptotically optimal PRG clearly implies a OWF that can be computed by linear-size circuits and is exponentially hard to invert. A natural conjecture is that the converse also holds, namely that an asymptotically optimal PRG can be constructed from any OWF $f : \{0,1\}^n \to \{0,1\}^n$ that can be computed by linear-size circuits and is exponentially hard to invert. This conjecture does not seem to follow from the current state of the art. A recent result of Vadhan and Zheng [27] (improving on [17,19]) comes close to proving the conjecture. Combined with linear-size computable pairwise independent hash functions [24], the result from [27] implies a PRG construction which satisfies the first two requirements but falls short of the third. More concretely, the construction adds a polylog(n) multiplicative overhead to the seed length.

A recent PRG construction of Applebaum [3] satisfies the first two requirements and has the additional feature of a constant output locality (namely, each output bit depends on a constant number of input bits). This construction relies on the assumption that a concrete OWF candidate due to Goldreich [11] is indeed one-way. Roughly speaking, this assumption asserts that a randomly chosen function from the class of functions having constant output locality is one-way with high probability.

A construction of an asymptotically optimal PRG based on an exponential version of an indistinguishability assumption due to Alekhnovich [1] follows from the work of Applebaum, Ishai, and Kushilevitz [5] (see also [24,3]). The question of constructing asymptotically optimal PRGs under more general assumptions remained open.

1.1. Our contribution

We prove the above conjecture for one-way functions f that are either "regular" (in the sense that every output $f(x)$ has the same number of preimages) or alternatively have a "random enough output" on a random input x. More concretely, we prove the following result:

Theorem 1 *(Asymptotically optimal PRGs). Suppose that $f : \{0,1\}^n \to \{0,1\}^n$ is $2^{\beta n}$-hard to invert for some constant $\beta > 0$. Suppose that either f is regular or the min-entropy of $f(x)$ is larger than γn for some constant γ such that $\gamma > 1 - \beta/3$. Then there exists an exponentially strong PRG $G : \{0,1\}^n \to \{0,1\}^{2n}$ that can be computed by linear-size circuits using $O(1)$ oracle calls to f.*