# On Linear-Size Pseudorandom Generators and Hardcore Functions

Joshua Baron[1], Yuval Ishai[2], and Rafail Ostrovsky[3]

[1] HRL Laboratories, Malibu, CA, USA 90265
jwbaron@hrl.com
[2] Technion, Haifa, Israel 32000
yuvali@cs.technion.ac.il
[3] UCLA, Los Angeles, CA, USA 90095
rafail@cs.ucla.edu

**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 $\beta > 0$, and the min-entropy of $f(x)$ on a random input $x$ is at least $\gamma n$ for a constant $\gamma > 0$ such that $\beta/3 + \gamma > 1$.

Alternatively, building on the work of Haitner, Harnik and Reingold (SICOMP 2011), one can replace the second requirement by:

**2′.** $f$ is $2^{\beta n}$-hard to invert for some constant $\beta > 0$ and it is *regular* in the sense that the preimage size of every output of $f$ is fixed (but possibly unknown).

Previous constructions of PRGs from one-way functions can do without the entropy or regularity requirements, but even the best such constructions achieve slightly sub-exponential security (Vadhan and Zheng, STOC 2012).

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-sized 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 can be obtained via linear-size computable affine hash functions (Ishai, Kushilevitz, Ostrovsky and Sahai, STOC 2008).

**Keywords:** Pseudorandom generators, hardcore functions, circuit complexity, exponential hardness, pairwise independence, bilinear hash families.

D.-Z. Du and G. Zhang (Eds.): COCOON 2013, LNCS 7936, pp. 169–181, 2013.

## 1 Introduction

A *pseudorandom generator* (PRG) [7,30] 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.

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) [21] 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 [22,17,18,19,20,16,29].

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.
- $G$ 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 [25].

A natural conjecture is that an asymptotically optimal PRG can be constructed from any OWF $f : \{0,1\}^n \to \{0,1\}^n$ which can be computed by linear-size circuits and is exponentially hard to invert. However, this conjecture does not seem to follow from the current state of the art. A recent result of Vadhan and Zheng [29] (improving on [18,20]) comes close to proving the conjecture. Combined with linear-size computable pairwise independent hash functions [25], the result from [29] 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 variants of a one-wayness assumption due to Goldreich [12]. 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 [6] (see also [25,3]). 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 $\beta > 0$. Suppose that either $f$ is regular* or *the min-entropy of $f(x)$ is larger than $\gamma n$ for some constant $\gamma$ such that $\gamma > 1 - \beta/3$ (and for sufficiently large $n$). 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 $f$.*

Using a standard tree-based PRG extension, the above theorem yields an asymptotically optimal PRG with an arbitrary polynomial stretch; see the full version of this paper for further details.

The above entropy requirement seems quite mild and in some cases of interest it can be proved unconditionally. In particular, there are natural variants of Goldreich's OWF candidate [12] that can be shown to have fractional entropy

that tends to 1 with the locality degree (see [9] and the full version of this paper), whereas the expected hardness of inverting does not seem to decrease (and may even grow) with the locality.

**Hardcore Functions.** Our construction of asymptotically optimal PRGs is obtained via a technical result about hardcore functions that may be of independent interest. Recall that a hardcore predicate $b$ is a function that outputs a single bit $b(x)$ which is hard to predict even given $f(x)$. A hardcore *function* for a one-way function $f$ is a function $h$ (which can output more than one bit) whose output $h(x)$ is hard to distinguish from random even when $f(x)$ is known. More precisely, we allow $h$ to be picked at random from a function family $H$ and provide a description of $h$ as an additional input to the distinguisher. Hardcore functions are a fundamental cryptographic object, with applications to pseudoentropy and pseudorandomness. Goldreich and Levin [15] introduced the first hardcore predicates and functions for general OWFs, showing that a random linear function is hardcore and so is the linear function defined by a random Toeplitz matrix.

We consider families of linear functions $H = \{h_i : \{0,1\}^n \to \{0,1\}^m\}$ over the binary field. We refer to such a family as a *bilinear uniform output hash family* if it satisfies two properties. First, for any $x \neq 0$, the random variable $h_i(x)$ (induced by a uniformly random choice of the index $i$) is uniformly distributed over $\{0,1\}^m$. Second, $H$ forms a subgroup of the (additive) group of linear functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ . Using a result of Holenstein, Maurer, and Sjödin [23], we show that any such family of functions is hardcore for any sufficiently hard OWF.

**Theorem 2 (Bilinear Uniform-Output Hash Families are Hardcore).** *Let $H = \{h : \{0,1\}^n \to \{0,1\}^{\alpha n}\}$ be a bilinear uniform output hash family and let $f : \{0,1\}^n \to \{0,1\}^n$ be a $2^{\beta n}$-hard one-way function. Then $H$ is a family of exponentially strong hardcore functions for $f$ if $\beta > 3\alpha$.*

A construction of linear-size computable pairwise independent hash functions was given by Ishai, Kushilevitz, Ostrovsky and Sahai [25]. Observing that the construction can be instantiated so that each function in the family is affine, and constructing linear uniform-output hash families from such families, we can use the above theorem to obtain linear-size computable hardcore functions with a long output. Using such a hardcore function, the construction of an asymptotically optimal PRG proceeds in a simple way. In the high entropy case, we first extract the randomness from the output of $f$ by applying a (linear-size) pairwise independent hash function (appealing to the Leftover Hash Lemma [21]). Then, we extract sufficient pseudorandomness from the input of $f$ by applying the (linear-size) hardcore function to the input $x$. If $f$ has sufficiently high min-entropy and is hard enough to invert, these techniques combine so that the output has length $cn$ for $c > 1$. From this PRG, we can use standard PRG extension techniques to obtain an asymptotically optimal PRG with an arbitrary polynomial stretch.

In the case where the OWF $f$ is regular, we combine the hardcore function result with a PRG construction of Haitner, Harnik and Reingold [17,19] (the

HILL construction [21] yields a similar result for regular $f$ with known preimage size).

### 1.2 Related Work

**Pseudorandom Generators.** Following the pioneering works of Blum and Micali [7] and Yao [30], who constructed a PRG from a one-way *permutation*, Goldreich, Krawczyk and Luby [14] constructed a PRG from any *regular* OWF with unknown preimage size (a OWF is regular if every output of $f$ has the same preimage size). Håstad, Impagliazzo, Levin and Luby [21] gave the first construction of a PRG from any OWF. The first effort towards simplifying and improving the HILL construction was made by Holenstein [22], who also explicitly considered the case of exponentially strong OWFs. Haitner, Harnik and Reingold [17,18,19] improved the construction of [14] by relying only on pairwise independent hash functions ([14] had required $n$-wise independent hash functions) and by reducing the seed length. More recently, Haitner, Reingold and Vadhan [20] further improved the seed length of PRGs from general OWFs. The most efficient general constructions to date are given in the aforementioned work of Vadhan and Zheng [29], who also noted that combining their construction with the pairwise independent hash functions of [25] gives a linear-stretch linear-size PRG from *any* exponentially hard OWF. (This construction does not depend on the hash functions being affine.) As discussed above, this construction still falls short of our main goal because of its polylogarithmic overhead to the seed length, but otherwise it is stronger in several important aspects. In particular, it does not require $f$ to satisfy any entropy or regularity requirement.

Constructions of PRGs in $\mathrm{NC}^0$ (i.e., with constant output locality) were first given by Applebaum, Ishai, and Kushilevitz [5] under standard assumptions. Note that any $\mathrm{NC}^0$ function can be realized by linear-size circuits (in the output length). However, the PRGs in $\mathrm{NC}^0$ from [5] have sublinear stretch. Linear-stretch PRGs in $\mathrm{NC}^0$ were constructed in [6] under an *indistinguishability* assumption due to Alekhnovich [1]. Under an exponentially strong version of the assumption from [1], this construction yields an asymptotically optimal PRG.

A family of linear-stretch PRGs in $\mathrm{NC}^0$ whose security is based on a natural *one-wayness* assumption was given by Applebaum [3], who under similar assumptions also obtained a PRG with polynomial stretch in $\mathrm{NC}^0$. However, the security level of the PRGs constructed in [3] does not meet the third requirement of an asymptotically optimal PRG, even under exponential one-wayness assumptions. Furthermore, the underlying OWFs in these constructions are restricted to special distributions over $\mathrm{NC}^0$ functions, whereas our construction does not require the underlying OWF to be in $\mathrm{NC}^0$ (nor does it yield a PRG in $\mathrm{NC}^0$).

Finally, Applebaum, Bogdanov, and Rosen [4] (following earlier works of Cryan and Miltersen [11] and Mossel, Shpilka, and Trevisan [26]) present a broad class of randomized constructions of small-bias PRGs in $\mathrm{NC}^0$, namely PRGs in $\mathrm{NC}^0$ which provably fool all *linear* distinguishers. Such small-bias PRGs may serve as plausible candidates for asymptotically optimal PRGs, though their security does not seem to follow from any natural one-wayness assumption.

**Goldreich's One-Way Function.** Goldreich [12] put forward the following graph-based one-way function candidate: Consider a $d$-ary (nonlinear) predicate $P$ and a bipartite graph $G = (V, E)$ with left nodes $u_1, \ldots, u_n$, right nodes $v_1, \ldots, v_n$, and right degree $d$. Define $f : \{0,1\}^n \to \{0,1\}^n$ by labeling the left (input) nodes of $G$ with the bits of $x$. We define the $j$th output bit of $f$ on $x$, $f(x)_j$, as $P(x_{i_1}, \ldots, x_{i_d})$, where $u_{i_1}, \ldots, u_{i_d}$ are the input nodes that are in the neighborhood of $v_j$, the $j$th output node of $G$. We note that $f$ can be computed by linear-size circuits as long as $d$ is a constant. Goldreich conjectured that most functions $f$ as above are one-way.

Recent works on this class of functions [28,2,9,10,8] may be viewed as supporting the possibility that they are exponentially hard; however, Bogdanov and Qiao [8] have shown that for variants where the output stretch is a large constant (at least exponential in the input degree), there exist instantiations that are invertible in polynomial time. Applebaum's construction of a linear-stretch PRG in $\mathrm{NC}^0$ [3] uses a variant of Goldreich's one-way function with a large constant stretch. He demonstrates that the one-wayness of such local functions implies that the output has sufficiently good pseudoentropy to allow the construction of a PRG. By contrast, the one-way functions required for the constructions in this paper are from $n$ bits to $n$ bits and, as discussed above, the security reduction from [3] is not tight enough to yield an asymptotically optimal PRG.

In the full version of this paper, we show that a random $d$-local one-way function from $n$ bits to $n$ bits, instantiated with a random and independent $d$-ary predicate for *each* output bit of the function, has high min-entropy except with exponentially small probability over the choice of graph and predicates. This is useful towards instantiating the types of OWFs on which our main result relies. Previous works (e.g., [9,10]) have examined instances with more concrete choices of the predicate $P$ and proved them also to have high min-entropy except with exponentially small probability over the choice of the function.

**Hardcore Functions.** Goldreich and Levin [15] demonstrated that the set of all inner product functions constitutes a family of hardcore predicates for any one-way function. More generally, they proved that the set of all linear functions with input in $\{0,1\}^n$ and the set of Toeplitz matrices with input $\{0,1\}^n$ are families of hardcore functions for any one-way function (for appropriately sized outputs). The central idea of their proof is that if a random XOR of a candidate hardcore function output is hard to distinguish, then the function is indeed hardcore; they constructed such an argument for the set of all matrices and Toeplitz matrices, respectively, by direct calculation.

Näslund [27] showed that the family of all affine functions over $GF[2^n]$ and the family of all linear functions over the integers modulo a prime are families of hardcore functions for any one-way function.

Holenstein, Maurer and Sjödin [23] generalized the results of [15] to give a complete classification of all so-called bilinear hardcore function families over arbitrary fields; that is, the hardcore functions are additively homomorphic both in their function inputs and in the strings that represent each function (this

is the case when the set of hardcore functions forms an additive group). Our construction of linear-size computable hardcore functions will rely on this result.

### 1.3 Definitions and Preliminaries

We denote by $U_n$ the random variable uniformly distributed over $\{0,1\}^n$. We provide some definitions and preliminaries used in this paper; see the full version for other definitions, such as bilinear functions, full rank bilinear functions, one-way functions, hardcore functions, pseudorandom generators and pairwise independent hash families. In particular, we say that a function is a *$\beta$-exponential one-way function* if it is a $(2^{\beta n}, 2^{-\beta n})$ one-way function. We also say that a pairwise independent hash family where each function in the family is affine is an *affine pairwise independent (API) hash family.*

**Definition 3.** *Let $H_{n,m} = \{h_i : \{0,1\}^n \to \{0,1\}^m\}$ be a multiset of functions (that is, we allow distinct indices to represent the same function). We say that $H_{n,m}$ is a* family of uniform-output hash functions *if for every non-zero $x \in \{0,1\}^n$, the random variables $H_{n,m}(x)$ induced by a uniform choice of $h$ from $H_{n,m}$ is uniformly distributed over $\{0,1\}^m$. If every $h_i \in H_{n,m}$ is a linear function over the binary field (i.e., a function of the form $A_i x$), we call $H_{n,m}$ a* linear uniform-output (LUO) hash family.

*Further, a LUO hash family of size $2^k$ that can be expressed as a bilinear function $h : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^m$ (where the second argument represents the index $i$) is denoted a* bilinear uniform-output (BLUO) hash family.

We will typically consider infinite collections of families $H_{n,m}$ parameterized by the input and output length. In such a case we require the existence of a representation length $\ell_{n,m} = poly(n,m)$ such that $H_{n,m}$ contains $2^{\ell_{n,m}}$ (not necessarily distinct) functions $h_i$ indexed by all binary strings of length $\ell_{n,m}$ (which equals $k$ in the above definitions). For convenience, we will abuse notation and refer to $h_i \in H_{n,m}$ as both a function and the string representing it. We assume that there is a polynomial-time evaluation algorithm that, given $h_i$ and $x$, outputs $h_i(x)$. In fact, we will rely on families for which this algorithm can be implemented by linear-size circuits.

**Claim 4.** *Let $H'_{n,m}$ be an API hash family. Then the multiset $H_{n,m} = \{h_i : h_i(x) = h'_i(x) - h'_i(0),\ h'_i \in H'\}$ is an LUO hash family.*

The proof of the claim is immediate from the fact that for any $x \neq 0$, $H'_{n,m}(x)$ and $H'_{n,m}(0)$ are distributed uniformly and independently at random, and that each function in $H_{n,m}$ is linear.

## 2 Linear-Size Hardcore Functions

We now give our main result for the existence of linear-size hardcore functions.

**Theorem 5.** *Let $H_{n,l(n)}$ be a BLUO hash family, let $f : \{0,1\}^n \to \{0,1\}^n$ be a $(t(n), 1/t(n))$ one-way function, and let $\theta > 1$ be an arbitrary constant. Then $H_{n,l(n)}$ is a $(t'(n), 1/t'(n))$ family of hardcore functions for $f$ if $3\theta(l(n) + \log t'(n)) < \log t(n)$.*

**Corollary 6.** *Let $H_{n,l(n)}$ be a BLUO hash family and let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way (resp. $\beta$-exponential one-way) function. Then $H_{n,l(n)}$ is a family of hardcore functions (resp. is a $(2^{\Omega(n)}, 2^{-\Omega(n)})$ family of hardcore functions) for $f$ for any $l(n) \in O(\log n)$ (resp. $l(n) < \frac{\beta n}{3\theta}$ for any constant $\theta > 1$).*

We initiate the proof of Theorem 5 by proving a technical lemma.

**Lemma 7.** *Let $\mathcal{H}$ be a BLUO hash family specified by the bilinear function $h$. Then $h$ is full rank.*

**Proof of Lemma 7.** Let $h : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^m$ be the bilinear function that specifies $\mathcal{H}$. Then, by definition of LUO hash families, for any $0 \neq x \in \{0,1\}^n$, the distribution $\{h(x,r)\}_{r \leftarrow U_k}$ is distributed uniformly over $\{0,1\}^m$. Let $l : \{0,1\}^m \to \{0,1\}$ be an arbitrary non-zero linear function. Then for any $0 \neq x \in \{0,1\}^n$, $\{l \circ h(x,r)\}_{r \leftarrow U_k}$ is also distributed uniformly over $\{0,1\}$ and, in particular, the linear map $r \mapsto h(x,r)$ is surjective onto $\{0,1\}$ for any non-zero $x$.

Let $M_l$ be the $n \times k$ matrix denoting $l \circ h : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}$. We would like to prove that $\text{rank}(M_l) = n$. This follows from the fact that for every non-zero $x \in \{0,1\}^n$, there exists some $r_x$ such that $x^T \cdot M \cdot r_x = 1$, which implies that every non-trivial linear combination of the rows of $M_l$ is non-zero, and the lemma follows. □

We now proceed to prove Theorem 5.

**Proof of Theorem 5.** We will proceed by contradiction, and assume that there exists a probabilistic algorithm $D$ running in time $t'(n)$ such that $|\Pr[x \leftarrow U_n, h \leftarrow H_{n,l(n)} : D(f(x), h, h(x)) = 1] - \Pr[x \leftarrow U_n, h \leftarrow H_{n,l(n)}, y \leftarrow U_{l(n)} : D(f(x), h, y) = 1]| > \epsilon'(n) = 1/t'(n)$ for infinitely many $n$.

More specifically, let $\Pr[x \leftarrow U_n, h \leftarrow H_{n,l(n)} : D(f(x), h, h(x)) = 1] = \delta$ and $\Pr[x \leftarrow U_n, h \leftarrow H_{n,l(n)}, y \leftarrow U_{l(n)} : D(f(x), h, y) = 1] = (1 + \epsilon)\delta$. Without loss of generality, let $\epsilon > 0$ (otherwise, let $D'$ be the algorithm that outputs the opposite bit that $D$ does and use $D'$ for the remainder of this proof); then $\epsilon\delta \geq \epsilon'(n)$.

Let $\alpha(n)$ be such that for some $\theta > 1$, $3\theta(l(n) + \log t'(n)) + \log \alpha(n) < \log t(n)$. Since by Lemma 7, $\mathcal{H}$ can be specified by a full rank bilinear function, a slightly modified version of the hardcore result of [23] (see the full version for details) implies that there exists an algorithm $A_\alpha$ and some $c > 0$ that inverts $f$ in time $\alpha(n) \cdot \frac{2^{2l(n)}}{\delta\epsilon^2} \cdot n^c \cdot t'(n) \leq \alpha(n) \cdot \frac{2^{2l(n)+1}}{\epsilon'(n)^2} \cdot n^c \cdot t'(n) = \alpha(n) \cdot 2^{2l(n)+1} \cdot n^c \cdot t'^3(n)$, which, by assumption, is less than $t(n)$. Further, $A_\alpha$ inverts $f$ with probability $\geq \frac{\delta\epsilon^2}{4 \cdot 2^{2l(n)}} - \frac{1}{\alpha(n)} \geq \frac{\epsilon'(n)^2}{4 \cdot 2^{2l(n)}} - \frac{1}{\alpha(n)}$, which, by assumption, is larger than $\epsilon(n) = 1/t(n)$, contradicting the one-wayness of $f$. □

Ishai et al [25] construct a family of pairwise independent hash functions from $\{0,1\}^n$ to $\{0,1\}^n$ which can be computed by circuits of size $O(n)$. This construction uses an arbitrary pairwise independent hash function (applied on a constant-size input domain) as a building block. Using a family of *affine* functions as a building block (e.g., $Ax + b$ where $A$ is a random binary matrix and $b$ a random binary vector) yields a linear-size computable family of *affine* pairwise independent hash functions. We use this family to construct a linear-size computable BLUO hash family[1].

**Proposition 8 (Implicit in [25]).** *For any $0 < c \leq 1$, there exists a family of affine pairwise independent hash functions from $\{0,1\}^n$ to $\{0,1\}^{cn}$ which can be computed by linear-size circuits.*

Combining Proposition 8 with Claim 4, we obtain the following lemma.

**Lemma 9.** *For any $0 < c \leq 1$, there exists a BLUO hash family from $\{0,1\}^n$ to $\{0,1\}^{cn}$ which can be computed by linear-size circuits.*

Applying Theorem 5 with these hash functions yields the following result.

**Corollary 10.** *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a $\beta$-exponential one-way function. For any $l(n)$ and $\theta > 1$ such that $3l(n) < \beta n\theta$, there exists a BLUO hash family $H_{n,l(n)}$ such that $H_{n,l(n)}$ is a $(2^{\Omega(n)}, 2^{-\Omega(n)})$ family of hardcore functions of $f$ which can be computed by linear-size circuits.*

## 3 PRGs Computable by Linear-Size Circuits

We discuss how hardcore functions that can be computed by linear-size circuits can be used to construct linear-stretch PRGs that can be computed by linear-size circuits. When $f$ is an exponentially hard one-way function, various assumptions about the min-entropy of the output of $f$ can be used to construct such PRGs. We first construct a PRG in the case that the output of $f$ has high enough min-entropy. We then examine previously made restrictions on $f$ that have been used to construct linear-stretch PRGs.

### 3.1 PRGs for One-Way Functions with Lower-Bounded Min-Entropy

We demonstrate that there exist linear-stretch pseudorandom number generators that can be computed by linear-size circuits provided that there exists a suitable class of exponentially hard one-way functions. We discuss the plausibility of these assumptions in the full version of this paper.

[1] When we say that a family of hash functions can be computed by linear-size circuits we mean that there is a universal constant $c$ such that for every sufficiently large $m$ and $n$, there is a circuit $C_{n,m}$ of size $cn$ which computes the restriction of the family to functions from $\{0,1\}^n$ to $\{0,1\}^m$. The input to $C_{n,m}$ includes the (binary representation of) the index $i$ of the hash function and the input for $h_i$.

**Assumption 11.** *There exist a function $f : \{0,1\}^n \to \{0,1\}^n$ and constants $\beta > 0, \theta > 1$, and $\gamma$ such that $\gamma > 1 - \frac{\beta}{3\theta}$ with the following properties:*

*(i) $f$ is a $\beta$-exponential one-way function.*
*(ii) $f$ can be computed by linear-size circuits.*
*(iii) $H_\infty(f(U_n)) > \gamma n$.*

Under this assumption, the following theorem can be proved.

**Theorem 12.** *If Assumption 11 holds, there exists a $(2^{\Omega(n)}, 2^{-\Omega(n)})$ linear-stretch PRG $G$ that can be computed by linear-size circuits with a single oracle call to $f$.*

Using either the construction in [25] or the construction in [13] (see Section 3.3.2 there) with the PRG $G$ of Theorem 12, we obtain the following corollary.

**Corollary 13.** *If Assumption 11 holds, then for any polynomial $l(n) > n$ there exists a $(2^{\Omega(n)}, 2^{-\Omega(n)})$ PRG $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ such that $G$ can be computed by circuits of size $O(l(n))$ with $O(l(n)/n)$ oracle calls to $f$.*

In the following Construction 14, we describe an algorithm that we prove satisfies Theorem 12; see the full version for the full proof of Theorem 12. It can be shown that it is possible to specify a BLUO hash family (and also an API hash family) $h \in H_{m,\alpha m}$ by specifying a string from $\{0,1\}^{\mu m}$ for some constant $\mu$. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a $\beta$-exponential one-way function. Set $c_0 = \gamma$ and $c_1 = 1 - \gamma + \epsilon_2$ for any constant $0 < \epsilon_2 < \gamma - (1 - \frac{\beta}{3\theta})$. Construct an API hash family, $H_{n,c_0 n}$, and a BLUO hash family, $H_{n,c_1 n}$, which are indexed by the sets $\{0,1\}^{k_0 n}$ and $\{0,1\}^{k_1 n}$ for some constants $k_0$ and $k_1$, respectively.

**Construction 14.** *Let $H_{n,c_0 n}$ be an API hash family and $H_{n,c_1 n}$ be a BLUO hash family with $h_0$ and $h_1$ drawn from $H_{n,c_0 n}$ and $H_{n,c_1 n}$, respectively. Let $f : \{0,1\}^n \to \{0,1\}^n$ satisfy Assumption 11. Then set:*

$$G(x, h_0, h_1) = (h_0, h_0(f(x)), h_1, h_1(x)).$$

Note that $|(x, h_0, h_1)| = (1+k_0+k_1)n$ and $|G(x, h_0, h_1)| = k_0 n + c_0 n + k_1 n + c_1 n = (1+\epsilon_2+k_0+k_1)n$, so $G$ has linear stretch. $G$ can also be computed by linear-size circuits because $h_0$, $h_1$, and $f$ can all be computed by linear-size circuits.

We note that it may be the case that one can only generate "good" one-way functions that satisfy Assumption 11 with constant probability; for instance, randomly selected bipartite graphs may only yield "good" OWFs with constant probability. One can still construct a family of PRGs from such a family of one-way functions, but the resulting PRGs will not be optimal because they will only be $(2^{\Omega(\sqrt{n})}, 2^{-\Omega(\sqrt{n})})$ PRGs; see the full version for further details.

**PRGs from Regular One-Way Functions.** We have so far presented a construction of a PRG for exponentially hard one-way functions with certain preimage constraints. Using the hardcore and hash families outlined here that

can be computed by linear sized circuits, we can also modify a result of [19,16] to obtain asymptotically optimal PRGs for regular one-way functions with possibly unknown preimage size (recall that a one-way function $f$ is *regular* if every every output f(x) has the same number of preimages. We refer the reader to the full for details[2].

**Corollary 15.** *If $f : \{0,1\}^n \to \{0,1\}^n$ is a $\beta$-exponential regular one-way function (with possibly unknown preimage size), then there exists a $(2^{\Omega(n)}, 2^{-\Omega(n)})$ pseudorandom generator $G$ with linear stretch that can be computed by linear-size circuits with $O(1)$ oracle calls to $f$.*

**Acknowledgements.** The authors wish to thank Benny Applebaum, Andrej Bogdanov, Iftach Haitner, and Salil Vadhan for helpful discussions. This work was done in part while the first and second authors were at UCLA. The work of the first and third authors is supported in part by NSF grants CCF-0916574, IIS-1065276, CCF-1016540, CNS-1118126, CNS-1136174, and by US-Israel BSF grant 2008411. It was also supported by the OKAWA Foundation Research Award, IBM Faculty Research Award, Xerox Faculty Research Award, B. John Garrick Foundation Award, Teradata Research Award and Lockheed-Martin Corporation Research Award. The material contained herein is also based upon work supported by the Defense Advanced Research Projects Agency through the U.S. Office of Naval Research under Contract N00014-11-1-0392. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. The work of the second author is supported by the European Research Council as part of the ERC project CaC (grant 259426), ISF grant 1361/10, and BSF grant 2008411.

## References

1. Alekhnovich, M.: More on average case vs approximation complexity. In: Proc. FOCS 2003, pp. 298–307 (2003)
2. Alekhnovich, M., Hirsch, E.A., Itsykson, D.: Exponential lower bounds for the running time of DPLL algorithms on satisfiable formulas. J. Autom. Reasoning. 35(1-3), 51–72 (2005)
3. Applebaum, B.: Pseudorandom Generators with Long Stretch and Low Locality from Random Local One-Way Functions. In: Proc. STOC 2012, pp. 805–816 (2012)
4. Applebaum, B., Bogdanov, A., Rosen, A.: A Dichotomy for Local Small-Bias Generators. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 600–617. Springer, Heidelberg (2012)
5. Applebaum, B., Ishai, Y., Kushilevitz, E.: Cryptography in $NC^0$. SIAM J. on Computing 36(4), 845–888 (2006)
6. Applebaum, B., Ishai, Y., Kushilevitz, E.: On Pseudorandom Generators with Linear Stretch in $NC^0$. J. Comp. Compl. 17(1), 38–69 (2008)
7. Blum, M., Micali, S.: How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. SIAM J. on Computing 13(4), 850–864 (1985)

[2] We note that we can similarly modify a result of HILL for OWFs with *known* preimage size to yield asymptotically optimal PRGs as well; see the full version for details.

8. Bogdanov, A., Qiao, Y.: On the Security of Goldreich's One-Way Function. In: Dinur, I., Jansen, K., Naor, J., Rolim, J. (eds.) APPROX and RANDOM 2009. LNCS, vol. 5687, pp. 392–405. Springer, Heidelberg (2009)
9. Cook, J., Etesami, O., Miller, R., Trevisan, L.: Goldreich's One-Way Function Candidate and Myopic Backtracking Algorithms. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 521–538. Springer, Heidelberg (2009)
10. Cook, J., Etesami, O., Miller, R., Trevisan, L.: On the One-Way Function Candidate Proposed by Goldreich. ECCC, Report No. 175 (2012)
11. Cryan, M., Miltersen, P.B.: On Pseudorandom Generators in $NC^0$. In: Sgall, J., Pultr, A., Kolman, P. (eds.) MFCS 2001. LNCS, vol. 2136, pp. 272–284. Springer, Heidelberg (2001)
12. Goldreich, O.: Candidate One-Way Functions Based on Expander Graphs. ECCC, Report No. 90 (2000)
13. Goldreich, O.: Foundations of Cryptography. Cambridge U. Press, Cambridge (2001)
14. Goldreich, O., Krawczyk, H., Luby, M.: On the Existence of Pseudorandom Generators. SIAM J. on Computing 22(6), 1163–1175 (1993)
15. Goldreich, O., Levin, L.A.: Hard-core Predicates for any One-Way Function. In: Proc. STOC 1989, pp. 25–32 (1989)
16. Haitner, I.: New Implications and Improved Efficiency of Constructions Based on One-way Functions. Ph.D. Thesis (March 2008)
17. Haitner, I., Harnik, D., Reingold, O.: Efficient Pseudorandom Generators from Exponentially Hard One-Way Functions. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 228–239. Springer, Heidelberg (2006)
18. Haitner, I., Harnik, D., Reingold, O.: On the Power of the Randomized Iterate. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 22–40. Springer, Heidelberg (2006)
19. Haitner, I., Harnik, D., Reingold, O.: On the Power of the Randomized Iterate. SIAM J. on Computing 40(6), 1486–1528 (2011)
20. Haitner, I., Reingold, O., Vadhan, S.: Efficiency Improvements in Constructing Pseudorandom Generators from One-way Functions. In: Proc. STOC 2010, pp. 437–446 (2010)
21. Hastad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A Psedorandom Generator From Any One-Way Function. SIAM J. on Computing 28(4), 1364–1396 (1999)
22. Holenstein, T.: Pseudorandom Generators from One-Way Functions: A Simple Construction for Any Hardness. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 443–461. Springer, Heidelberg (2006)
23. Holenstein, T., Maurer, U., Sjödin, J.: Complete Classification of Bilinear Hard-Core Functions. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 73–91. Springer, Heidelberg (2004)
24. Impagliazzo, R., Levin, L.A., Luby, M.: Pseudo-Random Generation From One-Way Functions (Extended Abstract). In: Proc. STOC 1989, pp. 12–24 (1989)
25. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Cryptography with Constant Computational Overhead. In: Proc. STOC 2008, pp. 433–442 (2008)
26. Mossel, E., Shpilka, A., Trevisan, L.: On epsilon-biased generators in $NC^0$. Random Struct. Algorithms 2(1), 56–81 (2006)
27. Näslund, M.: Universal Hash Functions & Hard Core Bits. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 356–366. Springer, Heidelberg (1995)

28. Panjwani, S.K.: An experimental evaluation of goldreich's one-way function. Technical report, IIT, Bombay (2001)
29. Vadhan, S., Zheng, C.J.: Characterizing Pseudoentropy and Simplifying Pseudorandom Generator Constructions. In: Proc. STOC 2012, pp. 817–836 (2012)
30. Yao, A.C.: Theory and application of trapdoor functions. In: Proc. FOCS 1982, pp. 80–91 (1982)