A PSEUDORANDOM GENERATOR FROM ANY ONE-WAY FUNCTION

JOHAN HÅSTAD , RUSSELL IMPAGLIAZZO , LEONID A. LEVIN , AND MICHAEL LUBY

DEFINITION 3.1 (breaking adversary and security). *An* adversary A *is a function ensemble. The* time–success ratio *of A for an instance f of a primitive is defined as $\mathbf{R}_{t_n} = T_n/sp_n(A)$, where t_n is the length of the private input to f, T_n is the worst-case expected running time of A over all instances parameterized by n, and $sp_n(A)$ is the success probability of A for breaking f. In this case, we say A is an* $\mathbf{R}$-breaking *adversary for f. We say f is* $\mathbf{R}$*-secure if there is no* $\mathbf{R}$*-breaking adversary for f.*

3.2. One-way function.

DEFINITION 3.2 (one-way function). *Let* $f : \{0,1\}^{t_n} \to \{0,1\}^{\ell_n}$ *be a* $\mathbf{P}$*-time function ensemble and let* $X \in_{\mathcal{U}} \{0,1\}^{t_n}$. *The* success probability *of adversary* A *for inverting* f *is*

$$sp_n(A) = \Pr[f(A(f(X))) = f(X)].$$

Then f *is an* $\mathbf{R}$*-secure one-way function if there is no* $\mathbf{R}$*-breaking adversary for* f.

DEFINITION 3.3 (computationally indistinguishable). *Let* $\mathcal{D} : \{0,1\}^{\ell_n}$ *and* $\mathcal{E} : \{0,1\}^{\ell_n}$ *be probability ensembles. The* success probability *of adversary* A *for distinguishing* $\mathcal{D}$ *and* $\mathcal{E}$ *is*

$$sp_n(A) = |\Pr[A(X) = 1] - \Pr[A(Y) = 1]|,$$

where X *has distribution* $\mathcal{D}$ *and* Y *has distribution* $\mathcal{E}$. $\mathcal{D}$ *and* $\mathcal{E}$ *are* $\mathbf{R}$*-secure* computationally indistinguishable *if there is no* $\mathbf{R}$*-breaking adversary for distinguishing* $\mathcal{D}$ *and* $\mathcal{E}$.

Definition 3.5 (pseudorandom generator). *Let $g : \{0,1\}^{t_n} \to \{0,1\}^{\ell_n}$ be a* **P***-time function ensemble where $\ell_n > t_n$. Then g is an* **R***-secure pseudorandom generator if the probability ensembles $g(\mathcal{U}_{t_n})$ and $\mathcal{U}_{\ell_n}$ are* **R***-secure computationally indistinguishable.*

PROPOSITION 3.6. *Suppose* $g : \{0,1\}^n \to \{0,1\}^{n+1}$ *is a pseudorandom generator that stretches by one bit. Define* $g^{(1)}(x) = g(x)$*, and inductively, for all* $i \geq 1$*,*

$$g^{(i+1)}(x) = \langle g(g^{(i)}(x)_{\{1,\ldots,n\}}), g^{(i)}(x)_{\{n+1,\ldots,n+i\}} \rangle.$$

Let k_n *be an integer-valued* $\mathbf{P}$*-time polynomial parameter. Then* $g^{(k_n)}$ *is a pseudorandom generator.*

DEFINITION 3.7 (computational entropy). *Let* $f : \{0,1\}^{t_n} \to \{0,1\}^{\ell_n}$ *be a* $\mathbf{P}$*-time function ensemble and let* s_n *be a polynomial parameter. Then* f *has* $\mathbf{R}$*-secure* computational entropy s_n *if there is a* $\mathbf{P}$*-time function ensemble* $f' : \{0,1\}^{m_n} \to \{0,1\}^{\ell_n}$ *such that* $f(\mathcal{U}_{t_n})$ *and* $f'(\mathcal{U}_{m_n})$ *are* $\mathbf{R}$*-secure computationally indistinguishable and* $\mathbf{H}(f'(\mathcal{U}_{m_n})) \geq s_n$.

DEFINITION 3.8 (pseudoentropy generator). *Let $f : \{0,1\}^{t_n} \to \{0,1\}^{\ell_n}$ be a* **P***-time function ensemble and let s_n be a polynomial parameter. Then f is an* **R***-secure* pseudoentropy generator *with pseudoentropy s_n if $f(\mathcal{U}_{t_n})$ has* **R***-secure computational entropy $t_n + s_n$.*

DEFINITION 3.9 (false-entropy generator). *Let $f : \{0,1\}^{t_n} \to \{0,1\}^{\ell_n}$ be a* **P***-time function ensemble and let s_n be a polynomial parameter. Then f is an* **R***-secure* false-entropy generator *with false entropy s_n if $f(\mathcal{U}_{t_n})$ has* **R***-secure computational entropy $\mathbf{H}(f(\mathcal{U}_{t_n})) + s_n$.*

DEFINITION 3.10 (hidden bit). *Let* $f : \{0,1\}^{t_n} \to \{0,1\}^{\ell_n}$ *and* $b : \{0,1\}^{t_n} \to \{0,1\}$ *be* **P***-time function ensembles. Let* $\mathcal{D} : \{0,1\}^{t_n}$ *be a* **P***-samplable probability ensemble, let* $X \in_{\mathcal{D}} \{0,1\}^{t_n}$*, and let* $\beta \in_{\mathcal{U}} \{0,1\}$*. Then* $b(X)$ *is* **R***-secure* hidden *given* $f(X)$ *if* $\langle f(X), b(X)\rangle$ *and* $\langle f(X), \beta\rangle$ *are* **R***-secure computationally indistinguishable.*

PROPOSITION 4.1. *Let $f : \{0,1\}^n \to \{0,1\}^{\ell_n}$ be a one-way function. Then $X \odot R$ is hidden given $\langle f(X), R\rangle$, where $X, R \in_{\mathcal{U}} \{0,1\}^n$.*

PROPOSITION 4.3. *Let* $f : \{0,1\}^n \to \{0,1\}^{\ell_n}$ *be a one-way function. Then* $\langle f(X), R, X \odot R \rangle$ *and* $\langle f(X), R, \beta \rangle$ *are computationally indistinguishable, where* $X, R \in_{\mathcal{U}} \{0,1\}^n$ *and* $\beta \in_{\mathcal{U}} \{0,1\}$.

PROPOSITION 4.4. *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way permutation. Let $x, r \in \{0,1\}^n$ and define $\mathbf{P}$-time function ensemble $g(x,r) = \langle f(x), r, x \odot r \rangle$. Then g is a pseudorandom generator.*

Proof. Let $X, R \in_{\mathcal{U}} \{0,1\}^n$, and $\beta \in_{\mathcal{U}} \{0,1\}$. Because f is a permutation, $\langle f(X), R, \beta \rangle$ is the uniform distribution on $\{0,1\}^{2n+1}$. By Proposition 4.3, $g(X,R)$ and $\langle f(X), R, \beta \rangle$ are computationally indistinguishable. □

Proposition 4.4 works when f is a permutation because

(1) $f(X)$ is uniformly distributed and hence already looks random;
(2) for any $x \in \{0,1\}^n$, $f(x)$ uniquely determines x. So no entropy is lost by the application of f.

For a general one-way function neither (1) nor (2) necessarily holds. Intuitively, the rest of the paper constructs a one-way function with properties (1) and (2) from a general one-way function. This is done by using hash functions to smooth the entropy of $f(X)$ to make it more uniform and to recapture the entropy of X lost by the application of $f(X)$.

Proposition 4.4 produces a pseudorandom generator that only stretches the input by one bit. To construct a pseudorandom generator that stretches by many bits, combine this with the construction described previously in Proposition 3.6.

4.3. One-to-one one-way function to a pseudoentropy generator.

PROPOSITION 4.5. *Let $f : \{0,1\}^n \to \{0,1\}^{\ell_n}$ be a one-to-one one-way function. Let $x, r \in \{0,1\}^n$ and define $\mathbf{P}$-time function ensemble $g(x,r) = \langle f(x), r, x \odot r \rangle$. Then g is a pseudoentropy generator with pseudoentropy 1.*

Proof. Let $X, R \in_{\mathcal{U}} \{0,1\}^n$ and $\beta \in_{\mathcal{U}} \{0,1\}$. Proposition 4.3 shows that $g(X,R)$ and $\langle f(X), R, \beta \rangle$ are computationally indistinguishable, where the reduction is linear-preserving with respect to the alternative definition of computationally indistinguishable. Because f is a one-to-one function and β is a random bit, $\mathbf{H}(f(X), R, \beta) = 2n+1$, and thus $g(X,R)$ has pseudoentropy 1. □

Note that it is not possible to argue that g is a pseudorandom generator. For example, let $f(x) = \langle 0, f'(x) \rangle$, where f' is a one-way permutation. Then f is a one-to-one one-way function and yet $g(X,R) = \langle f(X), R, X \odot R \rangle$ is not a pseudorandom generator, because the first output bit of g is zero independent of its inputs, and thus its output can easily be distinguished from a uniformly chosen random string.

DEFINITION 4.6 (universal hash functions). *Let* $h : \{0,1\}^{\ell_n} \times \{0,1\}^n \to \{0,1\}^{m_n}$ *be a* $\mathbf{P}$*-time function ensemble. Recall from Definition* 2.9 *that for fixed* $y \in \{0,1\}^{\ell_n}$*, we view* y *as describing a function* $h_y(\cdot)$ *that maps* n *bits to* m_n *bits. Then* h *is a (pairwise independent)* universal hash function *if, for all* $x \in \{0,1\}^n$*,* $x' \in \{0,1\}^n \setminus \{x\}$*, and for all* $a, a' \in \{0,1\}^{m_n}$*,*

$$\Pr[(h_Y(x) = a) \text{ and } (h_Y(x') = a')] = 1/2^{2m_n},$$

where $Y \in_{\mathcal{U}} \{0,1\}^{\ell_n}$*.*

DEFINITION 2.4 (Renyi entropy). *Let $\mathcal{D}$ be a distribution on a set S. The* Renyi entropy *of $\mathcal{D}$ is $\mathbf{H_{Ren}}(\mathcal{D}) = -\log(\Pr[X = Y])$, where $X \in_{\mathcal{D}} S$ and $Y \in_{\mathcal{D}} S$ are independent.*

There are distributions that have arbitrarily large entropy but have only a couple of bits of Renyi entropy.

PROPOSITION 2.5. *For any distribution $\mathcal{D}$, $\mathbf{H_{Ren}}(\mathcal{D}) \leq \mathbf{H}(\mathcal{D})$.*

LEMMA 4.8. *Let $\mathcal{D} : \{0,1\}^n$ be a probability ensemble that has Renyi entropy at least m_n. Let e_n be a positive-integer-valued parameter. Let $h : \{0,1\}^{\ell_n} \times \{0,1\}^n \to \{0,1\}^{m_n - 2e_n}$ be a universal hash function. Let $X \in_{\mathcal{D}} \{0,1\}^n$, $Y \in_{\mathcal{U}} \{0,1\}^{\ell_n}$, and $Z \in_{\mathcal{U}} \{0,1\}^{m_n - 2e_n}$. Then*

$$\mathbf{L_1}(\langle h_Y(X), Y\rangle, \langle Z, Y\rangle) \leq 2^{-(e_n+1)}.$$

Theorem 3: Let X be a random variable over the alphabet $\mathcal{X}$ with probability distribution P_X and Rényi entropy $R(X)$, let G be the random variable corresponding to the random choice (with uniform distribution) of a member of a universal class of hash functions $\mathcal{X} \to \{0,1\}^r$, and let $Q = G(X)$. Then

$$H(Q|G) \geq R(Q|G) \geq r - \log_2\left(1 + 2^{r-R(X)}\right) \geq r - \frac{2^{r-R(X)}}{\ln 2}.$$

Generalized Privacy Amplification

Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer, *Senior Member, IEEE*

PROPOSITION 4.9. *Let k_n be an integer-valued polynomial parameter.*

- *Let $\mathcal{D} : \{0,1\}^n$ be a probability ensemble.*
  There is a probability ensemble $\mathcal{E} : \{0,1\}^{nk_n}$ satisfying
  - $\mathbf{H_{Ren}}(\mathcal{E}) \geq k_n \mathbf{H}(\mathcal{D}) - nk_n^{2/3}$,
  - $\mathbf{L_1}(\mathcal{E}, \mathcal{D}^{k_n}) \leq 2^{-k_n^{1/3}}$.

- *Let $\mathcal{D}_1 : \{0,1\}^n$ and $\mathcal{D}_2 : \{0,1\}^n$ be not necessarily independent probability ensembles; let $\mathcal{D} = \langle \mathcal{D}_1, \mathcal{D}_2 \rangle$. There is a probability ensemble $\mathcal{E} : \{0,1\}^{2nk_n}$, with $\mathcal{E} = \langle \mathcal{E}_1, \mathcal{E}_2 \rangle$, satisfying the following:*
  - *For every value $E_1 \in \{0,1\}^{nk_n}$ such that $\Pr_{\mathcal{E}_1}[E_1] > 0$,*
    $\mathbf{H_{Ren}}(\mathcal{E}_2 | \mathcal{E}_1 = E_1) \geq k_n \mathbf{H}(\mathcal{D}_2 | \mathcal{D}_1) - nk_n^{2/3}$.
  - $\mathbf{L_1}(\mathcal{E}, \mathcal{D}^{k_n}) \leq 2^{-k_n^{1/3}}$.

COROLLARY 4.10. *Let k_n be an integer-valued* **P***-time polynomial parameter.*

- *Let $\mathcal{D} : \{0,1\}^n$ be a probability ensemble, let $m_n = k_n \mathbf{H}(\mathcal{D}) - 2nk_n^{2/3}$, and let $h : \{0,1\}^{p_n} \times \{0,1\}^{nk_n} \to \{0,1\}^{m_n}$ be a universal hash function. Let $X' \in_{\mathcal{D}^{k_n}} \{0,1\}^{k_n \times n}$ and let $Y \in_{\mathcal{U}} \{0,1\}^{p_n}$. Then*

$$\mathbf{L_1}(\langle h_Y(X'), Y\rangle, \mathcal{U}_{m_n+p_n}) \leq 2^{1-k_n^{1/3}}.$$

- *Let $\mathcal{D}_1 : \{0,1\}^n$ and $\mathcal{D}_2 : \{0,1\}^n$ be not necessarily independent probability ensembles, and let $\mathcal{D} = \langle \mathcal{D}_1, \mathcal{D}_2\rangle$. Let $m_n = k_n \mathbf{H}(\mathcal{D}_2|\mathcal{D}_1) - 2nk_n^{2/3}$. Let $h : \{0,1\}^{p_n} \times \{0,1\}^{nk_n} \to \{0,1\}^{m_n}$ be a universal hash function. Let $\langle X_1', X_2'\rangle \in_{\mathcal{D}^{k_n}} \{0,1\}^{k_n \times 2n}$ and let $Y \in_{\mathcal{U}} \{0,1\}^{p_n}$. Then*

$$\mathbf{L_1}(\langle h_Y(X_2'), Y, X_1'\rangle, \langle \mathcal{U}_{m_n+p_n}, X_1'\rangle) \leq 2^{1-k_n^{1/3}}.$$

4.6. Pseudoentropy generator to a pseudorandom generator.

PROPOSITION 4.11. *Let $\mathcal{D} : \{0,1\}^n$ and $\mathcal{E} : \{0,1\}^n$ be two probability ensembles and let $f : \{0,1\}^n \to \{0,1\}^{\ell_n}$ be a $\mathbf{P}$-time function ensemble. Let $\mathcal{D}$ and $\mathcal{E}$ be computationally indistinguishable. Then $f(\mathcal{D})$ and $f(\mathcal{E})$ are computationally indistinguishable.*

PROPOSITION 4.12. *Let k_n be an integer-valued $\mathbf{P}$-time polynomial parameter. Let $\mathcal{D} : \{0,1\}^{\ell_n}$ and $\mathcal{E} : \{0,1\}^{\ell_n}$ be $\mathbf{P}$-samplable probability ensembles. Let $\mathcal{D}$ and $\mathcal{E}$ be computationally indistinguishable. Then $\mathcal{D}^{k_n}$ and $\mathcal{E}^{k_n}$ are computationally indistinguishable.*

CONSTRUCTION 4.13. *Let $f : \{0,1\}^n \to \{0,1\}^{m_n}$ be a* **P***-time function ensemble and let s_n be a* **P***-time polynomial parameter. Let $k_n = (\lceil (2m_n + 1)/s_n \rceil)^3$ and $j_n = \lfloor k_n(n + s_n) - 2m_n k_n^{2/3} \rfloor$. Let $h : \{0,1\}^{p_n} \times \{0,1\}^{k_n m_n} \to \{0,1\}^{j_n}$ be a universal hash function. Let $u \in \{0,1\}^{k_n \times n}$, $y \in \{0,1\}^{p_n}$, and define* **P***-time function ensemble $g(u, y) = \langle h_y(f^{k_n}(u)), y \rangle$.*

THEOREM 4.14. *Let f and g be as described in Construction 4.13. Let f be a pseudoentropy generator with pseudoentropy s_n. Then g is a pseudorandom generator.*

Proof. Let $f' : \{0,1\}^{n'_n} \to \{0,1\}^{m_n}$ be the **P**-time function ensemble that witnesses the pseudoentropy generator of f as guaranteed in Definition 3.7 of computational entropy; i.e., $f'(X')$ and $f(X)$ are **R**-secure computationally indistinguishable and $\mathbf{H}(f'(X')) \geq n + s_n$, where $X \in_{\mathcal{U}} \{0,1\}^n$ and $X' \in_{\mathcal{U}} \{0,1\}^{n'_n}$. Let $U \in_{\mathcal{U}} \{0,1\}^{k_n \times n}$, $W \in_{\mathcal{U}} \{0,1\}^{k_n \times n'_n}$, and $Y \in_{\mathcal{U}} \{0,1\}^{p_n}$. By Proposition 4.12, $f^{k_n}(U)$ and $f'^{k_n}(W)$ are computationally indistinguishable. From Proposition 4.11, it follows that $g(U,Y) = \langle h_Y(f^{k_n}(U)), Y\rangle$ and $\langle h_Y(f'^{k_n}(W)), Y\rangle$ are computationally indistinguishable. Because $\mathbf{H}(f'(X')) \geq n + s_n$, by choice of k_n and j_n, using Corollary 4.10, it follows that $\mathbf{L_1}(\langle h_Y(f'^{k_n}(W)), Y\rangle, \mathcal{U}_{j_n+p_n}) \leq 2^{-k_n^{1/3}}$. Thus, it follows that $g(U,Y)$ and $\mathcal{U}_{j_n+p_n}$ are computationally indistinguishable. Note that by choice of k_n, the output length $j_n + p_n$ of g is longer than its input length $nk_n + p_n$. ∎

CONSTRUCTION 4.15. *Let $f : \{0,1\}^n \to \{0,1\}^{\ell_n}$ be a* **P***-time function ensemble. Let s_n be a* **P***-time polynomial parameter and assume for simplicity that $s_n \leq 1$. Let $\mathbf{e}_n$ be an approximation of $\mathbf{H}(f(X))$ to within an additive factor of $s_n/8$, where $X \in_{\mathcal{U}} \{0,1\}^n$. Fix $k_n = \lceil (4n/s_n)^3 \rceil$ and $j_n = \lceil k_n(n - \mathbf{e}_n) - 2nk_n^{2/3} \rceil$. Let $h : \{0,1\}^{p_n} \times \{0,1\}^{nk_n} \to \{0,1\}^{j_n}$ be a universal hash function. For $u \in \{0,1\}^{k_n \times n}$ and $r \in \{0,1\}^{p_n}$, define* **P***-time function ensemble*

$$g(\mathbf{e}_n, u, r) = \langle f^{k_n}(u), h_r(u), r \rangle.$$

LEMMA 4.16. *Let f and g be as described in Construction* 4.15. *Let f be a false-entropy generator with false entropy s_n. Then g is a mildly nonuniform pseudoentropy generator with pseudoentropy* 1.

4.8. Mildly nonuniform to a uniform pseudorandom generator.

PROPOSITION 4.17. *Let* $\mathbf{a}_n$ *be any value in* $\{0, \ldots, k_n\}$*, where* k_n *is an integer-valued* $\mathbf{P}$*-time polynomial parameter. Let* $g : \{0,1\}^{\lceil \log(k_n) \rceil} \times \{0,1\}^n \to \{0,1\}^{\ell_n}$ *be a* $\mathbf{P}$*-time function ensemble, where* $\ell_n > nk_n$*. Let* $x' \in \{0,1\}^{k_n \times n}$ *and define* $\mathbf{P}$*-time function ensemble* $g'(x') = \oplus_{i=1}^{k_n} g(i, x'_i)$*. Let* g *be a mildly nonuniform pseudorandom generator when the first input is set to* $\mathbf{a}_n$*. Then* g' *is a pseudorandom generator.*

4.9. Summary.

- a reduction from a one-way permutation to a pseudorandom generator (from subsection 4.2);

- a reduction from a one-to-one one-way function to a pseudorandom generator(combining subsections 4.3 and 4.6);

- a reduction from a pseudoentropy generator to a pseudorandom generator (from subsection 4.6);

- a reduction from a false-entropy generator to a pseudorandom generator (combining subsections 4.7, 4.6, and 4.8).

6.2. Construction and main theorem.

Let

$$f : \{0,1\}^n \to \{0,1\}^{\ell_n} \tag{6.1}$$

be a one-way function and let

$$h : \{0,1\}^{p_n} \times \{0,1\}^n \to \{0,1\}^{n+\lceil \log(2n) \rceil} \tag{6.2}$$

be a universal hash function. Similar to Construction 5.1, for $x \in \{0,1\}^n$, $i \in \{0,\ldots,n-1\}$, and $r \in \{0,1\}^{p_n}$, define **P**-time function ensemble

$$f'(x,i,r) = \langle f(x), h_r(x)_{\{1,\ldots,i+\lceil \log(2n) \rceil\}}, i, r \rangle \tag{6.3}$$

$$k_n \geq 125n^3. \tag{6.4}$$

DEFINITION 2.7 (degeneracy of f). *Let* $f : \{0,1\}^n \to \{0,1\}^{\ell_n}$ *and let* $X \in_{\mathcal{U}} \{0,1\}^n$. *The* degeneracy *of* f *is* $\mathbf{D}_n(f) = \mathbf{H}(X|f(X)) = \mathbf{H}(X) - \mathbf{H}(f(X))$.

DEFINITION 2.13 ($\tilde{\mathbf{D}}_f$). *Let* $f : \{0,1\}^n \to \{0,1\}^{\ell_n}$ *be a* $\mathbf{P}$*-time function ensemble. For* $z \in \text{range}_f$, *define the* approximate degeneracy of z *as*

$$\tilde{\mathbf{D}}_f(z) = \left\lceil \log(\sharp \text{pre}_f(z)) \right\rceil .$$

Part of the construction is to independently and randomly choose k_n sets of inputs to f' and concatenate the outputs. In particular, let $X' \in_{\mathcal{U}} \{0,1\}^{k_n \times n}$, $I' \in_{\mathcal{U}} \{0,1\}^{k_n \times \lceil \log(n) \rceil}$, $R' \in_{\mathcal{U}} \{0,1\}^{k_n \times p_n}$. Part of the construction is then $f'^{k_n}(X', I', R')$.

Let $I \in_{\mathcal{U}} \{0, \ldots, n-1\}$, let

$$\mathbf{p}_n = \Pr[I \leq \tilde{\mathbf{D}}_f(f(X))], \tag{6.5}$$

$$m_n = k_n \mathbf{p}_n - 2k_n^{2/3} \tag{6.6}$$

$$h' : \{0,1\}^{p'_n} \times \{0,1\}^{k_n} \to \{0,1\}^{m_n} \tag{6.7}$$

be a universal hash function, let $U \in_{\mathcal{U}} \{0,1\}^{p'_n}$, and define **P**-time function ensemble

$$\begin{aligned} &g(\mathbf{p}_n, X', Y', I', R', U) \\ &= \langle h'_U(\langle X'_1 \odot Y'_1, \ldots, X'_{k_n} \odot Y'_{k_n} \rangle), f'^{k_n}(X', I', R'), U, Y' \rangle. \end{aligned} \tag{6.8}$$

THEOREM 6.2. *Let f be a one-way function and g be as described above in* (6.1)–(6.8). *Then g is a mildly nonuniform false-entropy generator with false entropy $10n^2$.*

7. A direct construction. We have shown how to construct a false-entropy generator from an arbitrary one-way function, a pseudoentropy generator from a false-entropy generator, and finally a pseudorandom generator from a pseudoentropy generator. The combinations of these constructions give a pseudorandom generator from an arbitrary one-way function as stated in Theorem 6.3. By literally composing the reductions given in the preceding parts of this paper, we construct a pseudorandom generator with inputs of length n^{34} from a one-way function with inputs of length n. This is obviously not a suitable reduction for practical applications. In this subsection, we use the concepts developed in the rest of this paper, but we provide a more direct and efficient construction. However, this construction still produces a pseudorandom generator with inputs of length n^{10}, which is clearly still not suitable for practical applications. (A sharper analysis can reduce this to n^8, which is the best we could find using the ideas developed in this paper.) The result could only be considered practical if the pseudorandom generator had inputs of length n^2, or perhaps even close to n. (However, in many special cases of one-way functions, the ideas from this paper are practical; see, e.g., [Luby96].)

CONSTRUCTION 7.1.

$$g(\mathcal{X}', Y', R_1, R_2, R_3) = \langle h_{R_1}(\mathcal{X}'), h_{R_2}(b^{k_n}(\mathcal{X}', Y')), h_{R_3}(f'^{k_n}(\mathcal{X}')), Y', R_1, R_2, R_3 \rangle.$$

THEOREM 7.2. *If f is a one-way function and g is as in Construction* 7.1*, then g is a mildly nonuniform pseudorandom generator.*

We still need to use Proposition 4.17 to get rid of the mild nonuniformity. From the arguments above, it is clear that an approximation of both $\mathbf{e}_n$ and $\mathbf{p}_n$ that is within $1/(8n)$ of their true values is sufficient. Since $0 \leq \mathbf{e}_n \leq n$, and $0 \leq \mathbf{p}_n < 1$, there are at most $\mathcal{O}(n^3)$ cases of pairs to consider. This means that we get a total of $\mathcal{O}(n^3)$ generators, each needing an input of length $\mathcal{O}(n^7)$. Thus the total input size to the pseudorandom generator is $\mathcal{O}(n^{10})$, as claimed.

A PSEUDORANDOM GENERATOR FROM ANY ONE-WAY FUNCTION

JOHAN HÅSTAD , RUSSELL IMPAGLIAZZO , LEONID A. LEVIN , AND MICHAEL LUBY