(Almost) Optimal Constructions of UOWHFs from 1-to-1, Regular One-way Functions and Beyond

Yu Yu[1,2,3], Dawu Gu[1], Xiangxue Li[4], and Jian Weng[5]

[1] Department of Computer Science and Engineering, Shanghai Jiao Tong University
Email: {yyuu,dwgu}@sjtu.edu.cn
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China
[3] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)
[4] Department of Computer Science and Technology, East China Normal University
Email: xxli@cs.ecnu.edu.cn
[5] College of Information Science and Technology, Jinan University
Email: cryptjweng@gmail.com

Abstract. We revisit the problem of black-box constructions of universal one-way hash functions (UOWHFs) from several typical classes of one-way functions (OWFs), and give respective constructions that either improve or generalize the best previously known.

- For any 1-to-1 one-way function, we give an optimal construction of UOWHFs with key and output length $\Theta(n)$ by making a single call to the underlying OWF. This improves the constructions of Naor and Yung (STOC 1989) and De Santis and Yung (Eurocrypt 1990) that need key length $O(n \cdot \omega(\log n))$.
- For any known-(almost-)regular one-way function with known hardness, we give an optimal construction of UOWHFs with key and output length $\Theta(n)$ and a single call to the one-way function.
- For any known-(almost-)regular one-way function, we give a construction of UOWHFs with key and output length $O(n{\cdot}\omega(1))$ and by making $\omega(1)$ non-adaptive calls to the one-way function. This improves the construction of Barhum and Maurer (Latincrypt 2012) that requires key and output length $O(n{\cdot}\omega(\log n))$ and $\omega(\log n)$ calls.
- For any weakly-regular one-way function introduced by Yu et al. at TCC 2015 (i.e., the set of inputs with maximal number of siblings is of an n^{-c}-fraction for some constant c), we give a construction of UOWHFs with key length $O(n{\cdot}\log n)$ and output length $\Theta(n)$. This generalizes the construction of Ames et al. (Asiacrypt 2012) which requires an unknown-regular one-way function (i.e., $c = 0$).

Along the way, we use several techniques that might be of independent interest. We show that almost 1-to-1 (except for a negligible fraction) one-way functions and known (almost-)regular one-way functions are equivalent in the known-hardness (or non-uniform) setting, by giving an optimal construction of the former from the latter. In addition, we show how to transform any one-way function that is far from regular (but only weakly regular on a noticeable fraction of domain) into an almost-regular one-way function.

1 Introduction

Informally, a family of compressing hash functions, denoted by $\mathcal{G}$, is called *universal one-way*, if given a random function $g \in \mathcal{G}$ and a random (or equivalently, any pre-fixed) input x, it is infeasible for any efficient algorithm to find any $x' \neq x$ satisfying $g(x) = g(x')$. The seminal result that one-way functions (OWFs) imply universal one-way hash functions (UOWHFs) [17] constitutes one of the central pieces of modern cryptography. Applications of UOWHFs include basing digital signatures [9] on minimal assumptions (one-way functions), Cramer-Shoup encryption scheme [4], statistically hiding commitment scheme [12,13], etc.

UOWHFs from any OWFs. The principle possibility result that UOWHFs can be based on any OWF was established by Rompel [17] (with some corrections given in [18,15]). However, Rompel's construction was quite complicated and extremely unpractical. In particular, for any one-way function on n-bit inputs it requires key length $\tilde{O}(n^{12})$ and output length $\tilde{O}(n^8)$. Haitner et al. [11] improved the construction via the notion of inaccessible entropy [13], and reduced key and output length to $\tilde{O}(n^7)$. Therefore, even the best known generic UOWHF constructions (based on arbitrary OWFs) are mainly of theoretical interest and are too inefficient to be of any practical use.

UOWHFs from special OWFs. Another line of research focuses on more efficient (and nearly practical) constructions of UOWHFs from special structured OWFs. Naor and Yung gave an elegant "hash-then-truncate" construction of UOWHFs with key and output length $\Theta(n)$ which does a single call to any one-way permutation. However, for a slightly weaker primitive, namely, 1-to-1 one-way functions, the authors of [16] only gave a rather complicated construction. De Santis and Yung [19] gave an improved construction from any 1-to-1 OWF $f : \{0,1\}^n \to \{0,1\}^l$ as below:

$$\mathcal{G}_{\text{1-1}} \stackrel{\text{def}}{=} \{(h^n_{n-1} \circ \ldots \circ h^{l-1}_{l-2} \circ h^l_{l-1} \circ f) : \{0,1\}^n \to \{0,1\}^{n-1}, h^i_{i-1} \in \mathcal{H}^i_{i-1}, n \leq i \leq l\},$$

where "$\circ$" denotes function composition, each $\mathcal{H}^i_{i-1}$ denotes a family of pairwise-independent hash functions that compress i-bit strings into $(i-1)$ bits. Although $\mathcal{G}_{\text{1-1}}$ enjoys linear output length and a single function call, it requires[6] key length $O(\omega(\log n) \cdot n)$. In addition, the work of [19] also introduced a construction from any known-regular[7] one-way function with key and output length $O(\omega(\log^2 n) \cdot n)$

[6] A straightforward calculation suggests that $\mathcal{G}_{\text{1-1}}$ needs key length $O(l \cdot (l-n))$, and we know (see Fact 1) that every 1-to-1 one-way function implies another one-way function $f' : \{0,1\}^{n' \in \Theta(n)} \to \{0,1\}^{n' + \omega(\log n)}$ that is 1-to-1 except on a negligible fraction of inputs, which implies that the key length of [16,19] can be pushed to $O(\omega(\log n) \cdot n)$.

[7] A function f is regular if every image has the same number (say α) of preimages, and it is known- (resp., unknown-) regular if α is efficiently computable (resp., inefficient to approximate). More generally (as introduced in [21]), f is weakly unknown-regular if the fraction of x's with maximal $|f^{-1}(f(x))|$ (which is not necessarily efficiently computable) is noticeable. We stress that here "weakly" is used to describe "regularity" (rather than "one-way-ness" as in "weakly one-way functions").

and $O(\omega(1) \cdot \log n)$ adaptive calls, which was recently improved by Barhum and Maurer [3] to key and output length $O(\omega(\log n) \cdot n)$ and $O(\omega(1) \cdot \log n)$ non-adaptive calls. Based on unknown-regular one-way functions, Ames et al. [1] presented a more general construction with output length $\Theta(n)$, key length $O(\log n \cdot n)$ and $\tilde{O}(n)$ adaptive calls. We refer to Table 1 for a summary of previous constructions and a comparison to our work.

Table 1. A summary of existing constructions [16,19,3,1] and our work, where KR-OWF and UR-OWF are the shorthands for known-regular and unknown-regular one-way functions respectively, ε-hard KR-OWF additionally assumes that the hardness parameter ε of KR-OWF is known, and n^{-c}-WUR-OWF is the shorthand for weakly unknown-regular one-way functions (see Footnote 7 and formally Definition 9).

	Assumption	Output Length	Key Length	# of Calls	Type of Call
[16]	OWP	$\Theta(n)$	$\Theta(n)$	1	non-adaptive
[19,16]	1-to-1 OWF	$\Theta(n)$	$O(\omega(\log n) \cdot n)$	1	non-adaptive
[19]	KR-OWF	$O(\omega(\log^2 n) \cdot n)$	$O(\omega(\log^2 n) \cdot n)$	$O(\omega(\log n))$	adaptive
[3]	KR-OWF	$O(\omega(\log n) \cdot n)$	$O(\omega(\log n) \cdot n)$	$O(\omega(\log n))$	non-adaptive
[1]	UR-OWF	$\Theta(n)$	$O(\log n \cdot n)$	$\tilde{O}(n)$	adaptive
ours	1-to-1 OWF	$\Theta(n)$	$\Theta(n)$	1	non-adaptive
ours	ε-hard KR-OWF	$\Theta(n)$	$\Theta(n)$	1	non-adaptive
ours	KR-OWF	$O(\omega(1) \cdot n)$	$O(\omega(1) \cdot n)$	$O(\omega(1))$	non-adaptive
ours	n^{-c}-WUR-OWF	$\Theta(n)$	$O(\log n \cdot n)$	$\tilde{O}(n^{2c+1})$	adaptive

Summary of our constructions. In this paper, we give the following constructions from the respective aforementioned one-way functions. The first two constructions enjoy optimal parameters simultaneously and they are (almost) security-preserving[8], the third achieves parameters that are almost optimal up to an arbitrarily small super-constant factor $\omega(1)$ (e.g., $\log \log \log n$ or even less), and thus they all improve upon the respective known constructions. The fourth construction generalizes to beyond regular one-way functions (as introduced in [21]) with optimal output length $\Theta(n)$ and key length $O(n \cdot \log n)$.

1. For any 1-to-1 one-way function, we construct an optimal family of UOWHFs with key and output length $\Theta(n)$ and a single OWF call.
2. For any known-regular one-way function with known hardness, we give another optimal construction of UOWHFs with key and output length $\Theta(n)$ and a single call.
3. For any known-regular one-way function, we give a construction of UOWHFs with key and output length $O(\omega(1) \cdot n)$ and $\omega(1)$ non-adaptive calls.

[8] The security of the first UOWHF is essentially the same as the respective OWF, and the security of the second one is roughly a square root of its underlying OWF.

4. For any one-way function f that is weakly unknown-regular on a noticeable fraction (i.e., n^{-c} for constant c) of domain [21], we give a construction of UOWHFs with key length $O(n{\cdot}\log n)$ and output length $\Theta(n)$.

On the (a)symmetry to PRGs. Our results further exhibit the inherent "black-box duality" [5,13,11] between UOWHFs and PRGs. Firstly, we abstract out a lemma about universal hashing (see Lemma 1) that is implicit in previous works [17,15,13] and plays a dual role in UOWHF constructions to the leftover hash lemma in PRG constructions. Secondly, constructions #2 and #3 above match the best known results about constructions of PRGs from known-regular OWFs (see [22]), namely, seed length $O(\omega(1){\cdot}n)$ or even $\Theta(n)$ if the hardness of the underlying OWF is known. Thirdly, construction #4 is symmetric to the recent PRG construction [21] based on the same class of one-way functions with succinct key/seed length $O(n \cdot \log n)$. Finally (and perhaps more interestingly), construction #1 is asymmetric to the case of PRGs, where we do not know how to construct a linear seed length PRG from an arbitrary 1-to-1 one-way function[9].

On the efficiency, feasibility and limits. Constructions #1, #2 and #3 are practically relevant as most one-way function candidates turn out to be known-almost-regular or even 1-to-1. Goldreich, Levin and Nisan [8] showed how to base almost 1-to-1 (except for a negligible fraction) one-way functions on intractable problems such as RSA and DLP, and thus construction #1 enables to build optimal UOWHFs from those problems. A byproduct of construction #2 is the equivalence of almost 1-to-1 one-way functions and known-(almost-)regular one-way functions in certain (known-hardness or non-uniform) settings, where we give an optimal construction of the former from the latter. Moreover, unknown regular one-way functions further reduce the knowledge required about the underlying one-way functions, and the problem of basing cryptographic primitives (PRGs, UOWHFs, etc.) on weaker assumptions is of theoretic interests. It improves our understanding about the feasibility and limits of black-box reductions. In particular, Holenstein and Sinha [14], Barhum and Holenstein [2] showed that $\Omega(n/\log n)$ black-box calls to an arbitrary (including unknown-regular) one-way function is necessary to construct PRGs and UOWHFs, and the lower bound is matched by explicit constructions of PRGs [10] and UOWHFs [1] respectively. The recent work of [21] carried on this line of research even further by considering a more general class of one-way functions (which they call weakly unknown-regular one-way functions), namely, the underlying one-way function can have an arbitrary structure as long as the set of x with maximal number of siblings (i.e., x and x' are siblings of each other if $f(x) = f(x')$) is of noticeable fraction. The authors of [21] gave a construction of PRG with seed

[9] Given a 1-to-1 one-way function f, one might think of getting a PRG by hashing $f(U_n)$ into $n-s$ bits concatenated with $s+1$ hard-core bits of f, where $s \in \omega(\log n)$ is the necessary entropy loss due to the leftover hash lemma. This is in general not possible without knowing the exact hardness of the underlying f. See more discussions and the relaxed solutions to this problem by Goldreich [6, Section 3.5.1.3].

length $O(n \cdot \log n)$ from weakly unknown-regular OWFs. However, their analysis is quite ad-hoc (see Remark 2), and doesn't seem to generalize to UOWHFs. As an intermediate step of construction #4, we prove that "iterating such a one-way function (weakly regular on only a noticeable fraction) polynomially many times yields a one-way function that is almost-regular on an overwhelming fraction" and thus unify the approach to the two dual objects (i.e., PRGs and UOWHFs).

THE ROADMAP. We outline below the steps to build UOWHFs from the respective one-way function $f : \{0,1\}^n \to \{0,1\}^l$ introduced above. We note that the following assumptions (about output length) can be made without loss of generality: $l \in O(n)$ for 1-to-1 one-way functions and length-preserving-ness (i.e., $l = n$) for arbitrary one-way functions. More specifically, any 1-to-1 one-way function $f : \{0,1\}^n \to \{0,1\}^l$ implies a one-way function $f' : \{0,1\}^{n' \in \Theta(n)} \to \{0,1\}^{l' \in \Theta(n)}$ that is 1-to-1 except for a negligible fraction. Any one-way function f with $\alpha \leq |f^{-1}(y)| \leq \alpha \cdot \beta$ implies another length-preserving one-way function $f' : \{0,1\}^{n' \in \Theta(n)} \to \{0,1\}^{n'}$ with $\alpha' \leq |f'^{-1}(y)| \leq \alpha' \cdot \beta$ except for a negligible fraction, where the size of range β is preserved, and α' is efficiently computable if α is. We refer to [20] for a full proof.

BASED ON 1-TO-1 OWFS. We adapt Naor-Yung's elegant "hash-then-truncate" approach (for one-way permutation) to any 1-to-1 one-way function:

$$\mathcal{G}_1 \stackrel{\text{def}}{=} \{\ (\mathsf{trunc}\ \circ\ h\ \circ\ f) : \{0,1\}^n \to \{0,1\}^{n-s}\ ,\ h \in \mathcal{H}\ \}\ ,$$

where $\mathcal{H}$ is a family of universal hash permutations on l bits, and $\mathsf{trunc} : \{0,1\}^l \to \{0,1\}^{n-s}$ is a truncating function that outputs the first $n-s$ bits of input. We show that if f is a (t,ε)- 1-to-1 OWF then the resulting $\mathcal{G}_1$ is a $(t - n^{O(1)}$, $2^{s+1} \cdot \varepsilon)$-UOWHF family with key and output length $\Theta(n)$ and shrinkage s (see Definition 3 and Definition 7 for formal definitions). The construction enjoys optimal parameters and somewhat counter-intuitively the security bound drops only by factor 2^s (which is optimal by [5]) rather than by 2^{l-n+s} (i.e., exponential in the number of bits truncated which would render the construction useless). We refer to the proof of Theorem 1 and Remark 1 for more technical details and further discussions.

BASED ON KNOWN-(ALMOST-)REGULAR ε-HARD OWFS. Given an almost-regular f (see Definition 6) which is known to be (t,ε)-one-way for some efficiently computable ε, we define the following function family

$$\mathcal{G}_2 \stackrel{\text{def}}{=} \{\ g : \{0,1\}^n \to \{0,1\}^{n-s}, g(x) = (\ \mathsf{trunc}(h(f(x))), h_1(x)\ ), h \in \mathcal{H}, h_1 \in \mathcal{H}_1\ \}$$

where $\mathcal{H}$ is a family of universal hash permutations, and let $\mathcal{H}_1$ and trunc be a family of universal hash functions and the truncating function (both with appropriate output sizes) respectively. We show that $\mathcal{G}_2$ is a UOWHF family with key and output length $\Theta(n)$ and shrinkage s. The rationale is that for any[10] $x \neq x'$ colliding on $g \in \mathcal{G}_2$ it either satisfies "$f(x) = f(x') \wedge h_1(x) = h_1(x')$" or

[10] More precisely, x is sampled at random and x' can be any distinct value (i.e., $x' \neq x$) efficiently computable from x and g.

"$f(x) \neq f(x') \wedge \mathsf{trunc}(h(f(x))) = \mathsf{trunc}(h(f(x')))$". The former is unconditionally bounded by universal hashing, and the latter is computationally bounded (and reducible to the one-way-ness of f). Interestingly, by abstracting out function $f'(x, h_1) \stackrel{\text{def}}{=} (f(x), h_1(x), h_1)$ from the above construction, we further show that f' is a one-way function that is 1-to-1 except for a negligible fraction. We refer to Theorem 2, Lemma 2 and Theorem 3 for the details.

Based on known-(almost-)regular OWFs. Next, we consider any known-(almost)-regular OWF f whose hardness parameter is ε unknown (i.e., ε is negligible but may not be efficiently computable). In this case, we run q independent copies of f, and we get a construction by making q non-adaptive calls with shrinkage $q \log n$, key and output length $O(q \cdot n)$, where $q \in \omega(1)$ can be any efficiently computable super-constant. The parallel repetition technique was also used in similar contexts (e.g., the construction of PRG from any known regular OWF [22]). We refer to Theorem 4 for the detailed construction and proof.

Based on a more general class of OWFs. We show iterating the class of one-way functions introduced in [21] sufficiently many times yields a one-way function f' that is almost-regular, and thus plugging this f' into the construction of Ames et al.[1] yields a construction of UOWHFs with output length $\Theta(n)$ and key length $O(n \cdot \log n)$.

2 Preliminaries

Notations and definitions. We use $[n]$ to denote set $\{1, \ldots, n\}$. We use capital letters (e.g., X, Y) for random variables, standard letters (e.g., x, y) for values, and calligraphic letters (e.g. $\mathcal{X}$, $\mathcal{Y}$) for sets. The support of a random variable X, denoted by $\mathsf{Supp}(X)$, refers to the set of values on which X takes with non-zero probability, i.e., $\{x : \Pr[X = x] > 0\}$. For a binary string $x = x_1 \ldots x_n$, denote by $x_{[t]}$ the first t bits of x, i.e., $x_1 \ldots x_t$. $x \| y$ refers the concatenation of x and y. We denote by $\mathsf{trunc} : \{0,1\}^n \to \{0,1\}^t$ a truncating function that outputs the first t bits of input, i.e., $\mathsf{trunc}(x) = x_{[t]}$. $|\mathcal{S}|$ denotes the cardinality of set $\mathcal{S}$. For function $f : \{0,1\}^n \to \{0,1\}^{l(n)}$, we use shorthand $f(\{0,1\}^n) \stackrel{\text{def}}{=} \{f(x) : x \in \{0,1\}^n\}$, and denote by $f^{-1}(y)$ the set of y's preimages under f, i.e., $f^{-1}(y) \stackrel{\text{def}}{=} \{x : f(x) = y\}$. We say f is length-preserving if $l(n) = n$. We use $s \leftarrow S$ to denote sampling an element s according to distribution S, and let $s \xleftarrow{\$} \mathcal{S}$ denote sampling s uniformly from set $\mathcal{S}$, and $y := f(x)$ denote value assignment. We use U_n and $U_{\mathcal{X}}$ to denote uniform distributions over $\{0,1\}^n$ and $\mathcal{X}$ respectively, and let $f(U_n)$ be the distribution induced by applying function f to U_n. For probabilistic algorithm A, we use $\mathsf{A}(x; r)$ to denote the output of A on input x and internal coin r. The min-entropy and max-entropy (see, e.g., [13]) of a random variable X, denoted by $\mathbf{H}_\infty(X)$ and $\mathbf{H}_0(X)$ respectively, are defined as:

$$\mathbf{H}_\infty(X) \stackrel{\text{def}}{=} \log \min_{x \in \mathsf{Supp}(X)} \frac{1}{\Pr[X = x]} \; ; \quad \mathbf{H}_0(X) \stackrel{\text{def}}{=} \log |\mathsf{Supp}(X)| \; .$$

We use '$+/-$' and '$\cdot$' for addition/subtraction and multiplication between field elements respectively. The zero element of any finite field is denoted by $\mathbf{0}$.

Collision probability. We use $\mathsf{CP}(X)$ to denote the collision probability of X, i.e., $\mathsf{CP}(X) \stackrel{\text{def}}{=} \sum_x \Pr[X = x]^2$, and denote by $\mathsf{CP}(X|Z)$ the average collision probability of X conditioned on another (possibly correlated) random variable Z by

$$\mathsf{CP}(X|Z) \stackrel{\text{def}}{=} \mathbb{E}_{z \leftarrow Z} \left[\ \textstyle\sum_x \Pr[X = x| \ Z = z]^2 \ \right] \quad .$$

Simplifying Notations. Parameters (e.g., ε, r) are said to be known if they are polynomial-time computable from the security parameter n. By notation $f : \{0,1\}^n \to \{0,1\}^l$ we refer to the ensemble of functions $\{f : \{0,1\}^n \to \{0,1\}^{l(n)}\}_{n\in\mathbb{N}}$. As slight abuse of notion, poly might be referring to the set of all polynomials or a certain polynomial, and h might be either a function or its description which will be clear from context. For example, in $h(y) \stackrel{\text{def}}{=} h \cdot y$ the first h denotes a function, the second h refers to a string (a finite field element) that describes the function (i.e., multiplying y by h).

Definition 1 (ρ-almost universal hashing). *A family of functions $\mathcal{H} = \{h : \{0,1\}^l \to \{0,1\}^t\}$ is ρ-almost universal if for any distinct $x_1, x_2 \in \{0,1\}^l$, it holds that*

$$\Pr_{h \xleftarrow{\$} \mathcal{H}} [h(x_1) = h(x_2)] \leq \rho \ .$$

In the special case $\rho = 2^{-t}$, we say that $\mathcal{H}$ is universal.

Definition 2 (pairwise independent hashing). *A family of functions $\mathcal{H} = \{h : \{0,1\}^l \to \{0,1\}^t\}$ is pairwise independent if any distinct $x_1, x_2 \in \{0,1\}^l$ and any $v_1, v_2 \in \{0,1\}^t$ it holds that $\Pr_{h \xleftarrow{\$} \mathcal{H}}[\ h(x_1) = v_1 \wedge h(x_2) = v_2 \ ] = 2^{-2t}$.*

Definition 3 (one-way functions). *A sequence of functions $\{f : \{0,1\}^n \to \{0,1\}^{l(n)}\}_{n\in\mathbb{N}}$ is $(t(n),\varepsilon(n))$-one-way if f is polynomial-time computable and for any probabilistic algorithm A of running time $t(n)$*

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathsf{A}(1^n, f(x)) \in f^{-1}(f(x))] \ \leq \ \varepsilon(n).$$

Hereafter we use simplified notation $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ for the above one-way function, where $t(\cdot)$ and $1/\varepsilon(\cdot)$ are super-polynomial.

Definition 4 (a family of one-way functions). *A sequence of function family $\mathcal{F} = \{\mathcal{F}_n\}_{n\in\mathbb{N}}$, where $\mathcal{F}_n = \{f_u : \{0,1\}^n \to \{0,1\}^{l(n)}, u \in \{0,1\}^{q(n)}\}$, is $(t(n),\varepsilon(n))$-one-way if for any $n \in \mathbb{N}$, $u \in \{0,1\}^{q(n)}$ and $x \in \{0,1\}^n$, the value $f_u(x)$ can be computed in polynomial time, and for any probabilistic algorithm A of running time $t(n)$, we have that*

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n;\ u \xleftarrow{\$} \{0,1\}^{q(n)}}[\ \mathsf{A}(1^n, u, f_u(x)) \in f_u^{-1}(f_u(x)) \ ] \ \leq \ \varepsilon(n) \quad .$$

We use shorthands $\mathcal{F} = \{f_u : \{0,1\}^n \to \{0,1\}^{l(n)}, u \in \{0,1\}^{q(n)}\}$ for $\{\mathcal{F}_n\}_{n\in\mathbb{N}}$.

Definition 5 (almost 1-to-1 functions). *A function $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ is $\varepsilon(n)$-almost 1-to-1 if there exists a negligible function $\varepsilon(n)$, such that for every $n \in \mathbb{N}$ we have*

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\ \exists x' :\ x' \neq x \wedge f(x) = f(x')\ ] \leq \varepsilon(n).$$

In particular, f is 1-to-1 if $\varepsilon(n) \equiv 0$.

Definition 6 (almost regular functions). *For integer functions $\alpha = \alpha(n)$ and $\beta = \beta(n)$, a function $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ is α-regular if for every $n \in \mathbb{N}$ and $x \in \{0,1\}^n$ we have*

$$|f^{-1}(f(x))| = \alpha.$$

f is (α, $\alpha{\cdot}\beta$)-almost regular if for every $n \in \mathbb{N}$ and $x \in \{0,1\}^n$ we have

$$\alpha \ \leq\ |f^{-1}(f(x))| \ \leq\ \alpha \cdot \beta.$$

In particular, f is known-(almost)-regular if α is polynomial-time computable, or otherwise it is called unknown-(almost)-regular. Standard "almost-regularity" for a (t,ε)-one-way function f refers to that f is (α, $\alpha{\cdot}\beta$)-almost-regular for $\beta = \mathsf{poly}(n)$ or at most $\beta = (1/\varepsilon)^{\Theta(1)}$ for certain small constant $0 < \Theta(1) < 1$.

Definition 7 (UOWHFs [16]). *A sequence of function family $\mathcal{G} = \{\mathcal{G}_n\}_{n\in\mathbb{N}}$, where $\mathcal{G}_n = \{g_u : \{0,1\}^{\ell(n)} \to \{0,1\}^{\ell(n)-s(n)}, u \in \{0,1\}^{q(n)}, \ell \in \mathsf{poly}\}$, is a family of $(t(n)$,$\varepsilon(n))$-universal one-way hash functions if for every $n \in \mathbb{N}$, $u \in \{0,1\}^{q(n)}$ and $x \in \{0,1\}^{\ell(n)}$, the value $g_u(x)$ can be computed in polynomial time, and for every probabilistic algorithm A of running time $t(n)$, it holds that*

$$\Pr_{x \xleftarrow{\$} \{0,1\}^{\ell(n)};\ u \xleftarrow{\$} \{0,1\}^{q(n)};\ x' \leftarrow \mathsf{A}(1^n,x,u)} [\ x \neq x' \wedge g_u(x) = g_u(x')\ ] \ \leq\ \varepsilon(n) \quad .$$

*The difference between input and output lengths (i.e., $s(n)$) is called **shrinkage**. For succinctness, hereafter we will use shorthand $\mathcal{G} = \{g_u : \{0,1\}^\ell \to \{0,1\}^{\ell-s}$, $u \in \{0,1\}^q\}$ for $\{\mathcal{G}_n\}_{n\in\mathbb{N}}$ defined above.*

3 UOWHFs from 1-to-1 One-way Functions

3.1 A Technical Lemma and Its Applications

We state below a folklore lemma about universal hashing which is symmetric to the leftover hash lemma.

Lemma 1 (The injective hash lemma [20]). *For any integers a, d, k and l satisfying $a{\leq}l$, let Y be any random variable over $\{0,1\}^l$ with $\mathbf{H}_0(Y){\leq}a$, and let $\mathcal{H} \stackrel{def}{=} \{h\ :\ \{0,1\}^l \to \{0,1\}^{a+d}\}$ be a family of $(k{\cdot}2^{-(a+d)})$-almost universal hash functions. Then, we have that*

$$\Pr_{y \leftarrow Y,\ h \xleftarrow{\$} \mathcal{H}} [\ \exists \tilde{y} \in \mathsf{Supp}(Y) :\ \tilde{y} \neq y \wedge h(\tilde{y}) = h(y)\ ] \leq k{\cdot}2^{-d} \ \ .$$

Recall that $k = 1$ corresponds to the special case that $\mathcal{H}$ is universal.

We also mention the fact that the input and output lengths of a 1-to-1 one-way function $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ can be assumed to be linearly related (i.e., $l(n) = O(n)$). For almost regular one-way functions, we can even assume that they are length-preserving (i.e., $l(n) = n$). We refer to [20] for the proof of Fact 1.

Fact 1 *For any $r_1 = r_1(n) \leq r_2 = r_2(n)$ and any efficiently computable $\kappa = \kappa(n) \in O(n)$, we have*

1. *Any 1-to-1 (t,ε)-one-way function $f : \{0,1\}^n \to \{0,1\}^l$ implies a $(t - n^{O(1)}, \varepsilon + \mathsf{poly}(n) \cdot 2^{-\kappa})$-one-way function $f' : \{0,1\}^{n' \in \Theta(n)} \to \{0,1\}^{(n'+\kappa) \in \Theta(n)}$ which is 1-to-1 except on a $(\mathsf{poly}(n) \cdot 2^{-\kappa})$-fraction of inputs, i.e.,*

$$\Pr_{x \xleftarrow{\$} \{0,1\}^{n'}} [\ \exists x' \in \{0,1\}^{n'} : x' \neq x \ \wedge \ f'(x) = f'(x')\ ] \ \leq \ \mathsf{poly}(n) \cdot 2^{-\kappa}$$

2. *Any $(2^{r_1}, 2^{r_2})$-almost regular (t,ε)-one-way function $f : \{0,1\}^n \to \{0,1\}^l$ implies a length-preserving $(t - n^{O(1)}, \varepsilon + \mathsf{poly}(n) \cdot 2^{-(r_1+\kappa)})$-one-way function $\bar{f} : \{0,1\}^{n' \in \Theta(n)} \to \{0,1\}^{n'}$ which is $(2^{\kappa+r_1}, 2^{\kappa+r_2})$-almost regular except on a $(\mathsf{poly}(n) \cdot 2^{-(r_1+\kappa)})$-fraction of inputs, i.e.,*

$$\Pr_{x \xleftarrow{\$} \{0,1\}^{n'}} [\ 2^{\kappa+r_1} \ \leq \ |\bar{f}^{-1}(\bar{f}(x))| \ \leq \ 2^{\kappa+r_2}\ ] \ \geq \ 1 - \mathsf{poly}(n) \cdot 2^{-(r_1+\kappa)} \quad .$$

Therefore, we will assume in the remainder of the paper that the underlying 1-to-1 one-way function has linear output length (i.e., $l(n) = O(n)$) and that the almost-regular and weakly unknown-regular one-way functions are length-preserving (i.e., $l(n) = n$).

3.2 UOWHFs from 1-to-1 OWFs

For a 1-to-1 OWF $f : \{0,1\}^n \to \{0,1\}^l$, we define a cryptographic game between a challenger C and an inverter Inv. That is, C samples a random $y^* \xleftarrow{\$} \{0,1\}^l$ and sends it to Inv, and Inv wins the game iff he comes up with any x' satisfying $f(x') = y^*$. Note that even unbounded Inv wins this game with advantage no more than $2^{-(l-n)}$ (which is probability that $y^* \in f(\{0,1\}^n)$), and Fact 2 states that the chance to win is even smaller for computationally bounded Inv.

Fact 2 *For any 1-to-1 (t,ε)-one-way function $f : \{0,1\}^n \to \{0,1\}^l$ and any probabilistic algorithm Inv of running time t, it holds that*

$$\Pr_{y^* \xleftarrow{\$} \{0,1\}^l} [\ f(\mathsf{Inv}(y^*)) = y^*\ ] \ \leq \ 2^{-(l-n)} \cdot \varepsilon \quad .$$

Proof.

$$\Pr_{y^* \xleftarrow{\$} \{0,1\}^l} [\ f(\mathsf{Inv}(y^*)) = y^*\ ] \leq \Pr_{y^* \xleftarrow{\$} \{0,1\}^l} [y^* \in f(\{0,1\}^n)] \cdot \Pr_{y^* \xleftarrow{\$} f(\{0,1\}^n)} [\ f(\mathsf{Inv}(y^*)) = y^*\ ] \leq \ 2^{-(l-n)} \cdot \varepsilon \quad .$$

Remark 1 (on the proof sketch of Theorem 1). We use a trick to prove Theorem 1. We show that any A that ε'-breaks the TCR of the constructed UOWHF implies an $\mathsf{Inv}^{\mathsf{A}}$ (of almost the same efficiency as A) that wins the above game (i.e., inverting f on a random $y^* \in \{0,1\}^l$) with advantage roughly $2^{n-l-s} \cdot \varepsilon'$. This may seem useless since $l-n$ can be $\Omega(n)$ or even $\mathsf{poly}(n)$. However, by Fact 2 this term (i.e., $2^{n-l-s} \cdot \varepsilon'$) is actually upper bounded by $2^{-(l-n)} \cdot \varepsilon$. The conclusion $\varepsilon' \leq 2^s \varepsilon$ immediately follows by cancelling the factor $(l-n)$. In other words, the security bound does not depend on the number of bits truncated (i.e., $l-n+s$), but only on shrinkage s, and it is tight due to [5].

Theorem 1 (UOWHFs from 1-to-1 OWFs). *Let $f : \{0,1\}^n \to \{0,1\}^{l \in O(n)}$ be any 1-to-1 (t, ε)-one-way function, let $\mathcal{H}$ be a family of permutations*[11] *over $\{0,1\}^l$ as follows:*

$$\mathcal{H} = \{h : \{0,1\}^l \to \{0,1\}^l \ , \ h(y) \stackrel{def}{=} h \cdot y, \quad where \ \ y \in GF(2^l), \ \mathbf{0} \neq h \in GF(2^l) \ \} \ ,$$

let $\mathsf{trunc} : \{0,1\}^l \to \{0,1\}^{n-s}$ be a truncating function, where $s = s(n)$ is efficiently computable. Then, we have that

$$\mathcal{G}_1 \stackrel{def}{=} \{ \ (\mathsf{trunc} \circ h \circ f \ ) : \{0,1\}^n \to \{0,1\}^{n-s} \ , \ h \in \mathcal{H} \ \}$$

is a family of $(t - n^{O(1)}, \ 2^{s+1} \cdot \varepsilon)$-UOWHFs with key and output length $\Theta(n)$, and shrinkage s.

Proof. Suppose for contradiction that there exists a $\mathcal{G}_1$-collision finder A of running time t' that on input (x, h), breaks the target collision resistance with some non-negligible probability ε', i.e.,

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n, h \xleftarrow{\$} \mathcal{H}}[\ x' \leftarrow \mathsf{A}(x,h) : \ x \neq x' \wedge h(f(x))_{[n-s]} = h(f(x'))_{[n-s]} \ ] \ = \ \varepsilon' \ > \ 2^{s+1} \cdot \varepsilon$$

We define algorithm $\mathsf{Inv}^{\mathsf{A}}$ (that inverts f on input $y^* \xleftarrow{\$} \{0,1\}^l$ by invoking A) as in Algorithm 1. Define event $\mathcal{E}_{\mathsf{neq}} \stackrel{\text{def}}{=} (f(x) \neq y^*)$. We argue that $\mathsf{Inv}^{\mathsf{A}}$ inverts f with the following probability (see the rationale below)

$$\begin{aligned}
& \Pr_{y^* \xleftarrow{\$} \{0,1\}^l, \ x \xleftarrow{\$} \{0,1\}^n, \ v \xleftarrow{\$} \mathcal{V}} [\ f(\mathsf{Inv}^{\mathsf{A}}(y^*)) = y^* \ ] \\
\geq & \Pr_{x \xleftarrow{\$} \{0,1\}^n, y^* \xleftarrow{\$} \{0,1\}^l} [\ \mathcal{E}_{\mathsf{neq}} \ ] \cdot \Pr_{x \xleftarrow{\$} \{0,1\}^n, \ y^* \xleftarrow{\$} \{0,1\}^l \setminus \{f(x)\}, \ v \xleftarrow{\$} \mathcal{V}} [\ f(\mathsf{Inv}^{\mathsf{A}}(y^*)) = y^* \mid \mathcal{E}_{\mathsf{neq}} \ ] \\
\geq & (1 - 2^{-l}) \cdot \Pr_{x \xleftarrow{\$} \{0,1\}^n, h \xleftarrow{\$} \mathcal{H}, x' \leftarrow \mathsf{A}(x,h), v \xleftarrow{\$} \mathcal{V}} [x \neq x' \ \wedge \ h(f(x))_{[n-s]} = h(f(x'))_{[n-s]} \ \wedge \ y^* = f(x') \ ] \\
\geq & (1 - 2^{-l}) \cdot \varepsilon' \cdot \Pr_{v \xleftarrow{\$} \mathcal{V}} [y^* = f(x') \mid \mathcal{E}_{\mathsf{neq}} \ \wedge \ x \neq x' \wedge h(f(x))_{[n-s]} = h(f(x'))_{[n-s]}] \\
= & \frac{(1 - 2^{-l}) \cdot \varepsilon'}{|\mathcal{V}|} \ = \ \frac{(1 - 2^{-l}) \cdot \varepsilon'}{2^{l-n+s} - 1} \ > \ \frac{\varepsilon'/2}{2^{l-n+s}} \ > \ \varepsilon \cdot 2^{-(l-n)} \ ,
\end{aligned}$$

[11] In fact, $\mathcal{H}$ constitutes a family of universal hash permutations. However, our proofs only use the concrete construction of $\mathcal{H}$ and benefit from its algebraic property over finite fields, rather than assuming a universal $\mathcal{H}$ plus a constructible property [13] (given any x and y there exists a PPT sampler to output $h \xleftarrow{\$} \{h \in \mathcal{H} : h(x) = y\}$).

Algorithm 1 $\mathsf{Inv}^{\mathsf{A}}$ that inverts f on input y^* using random coins (x, v).

Input: $y^* \xleftarrow{\$} \{0,1\}^l$

Sample $x \xleftarrow{\$} \{0,1\}^n$
if $f(x) = y^*$ **then**
  Output x and **terminate**.
end if
sample $h := (f(x) - y^*)^{-1} \cdot v$, where $v \xleftarrow{\$} \mathcal{V} = \{v \in \{0,1\}^l \setminus \{\mathbf{0}\} : v_{[n-s]} = \overbrace{0\ldots0}^{n-s}\}$
{The above implies $h \xleftarrow{\$} \{h \in \mathcal{H} : \; h(f(x))_{[n-s]} = h(y^*)_{[n-s]}\}$ by the $GF(2^l)$ arithmetics. }
$x' \leftarrow \mathsf{A}(x, h)$
if $f(x'){=}y^*$ **then**
  Output x'
else
  Output $\perp$
end if
Terminate

where the first inequality is straightforward (note that conditioned on $\mathcal{E}_{\mathsf{neq}}$ the sampling of x and y^* are uniform over $\{0,1\}^n$ and $\{0,1\}^l \setminus \{f(x)\}$ respectively), the second inequality follows from Claim 1, namely, conditioned on $\mathcal{E}_{\mathsf{neq}}$ it is equivalent to consider $(x,\, h,\, v) \xleftarrow{\$} \{0,1\}^n \times \mathcal{H} \times \mathcal{V}$ and then $y^* := f(x) - v \cdot h^{-1}$, and the third inequality is due to that A takes only x and h as input (i.e., independent of v). That is, conditioned on that A produces a valid $x' \neq x$ satisfying $h(f(x'))_{[n-s]} = h(f(x))_{[n-s]}$, we have by Claim 1 that string y^* is uniformly distributed over set $\mathcal{Y}^* \stackrel{\text{def}}{=} \{f(x) - v{\cdot}h^{-1}, v \in \mathcal{V}\}$. Note that the already fixed $f(x')$ is also an element of $\mathcal{Y}^*$ and thus y^* hits $f(x')$ with probability $1/|\mathcal{Y}^*|{=}1/|\mathcal{V}|$. We complete the proof by reaching a contradiction to Fact 2.

Claim 1 (equivalent sampling) *Let the values h, v, x, y^* be sampled as in Algorithm 1, and conditioned on event $\mathcal{E}_{\mathsf{neq}} \stackrel{def}{=} (f(x){\neq}y^*)$, it is equivalent to sample $(x,\, h,\, v) \xleftarrow{\$} \{0,1\}^n \times \mathcal{H} \times \mathcal{V}$ uniformly and independently and then determine $y^* := f(x) - v \cdot h^{-1}$.*

Proof of Claim 1. We know that (x, v) is uniformly sampled from $\{0,1\}^n \times \mathcal{V}$ by definition, and thus it suffices to show that "fix any (x, v), and conditioned on $y^* \neq f(x)$ (i.e., Y^* is uniform distributed over $\{0,1\}^l \setminus \{f(x)\}$), it holds that h is uniform over $\mathcal{H}$". This follows from that $v \neq \mathbf{0}$ ($\mathcal{V}$ excludes $\mathbf{0}$ by definition) and hence $h = (f(x) - Y^*)^{-1} \cdot v$ is uniform over $\{0,1\}^l \setminus \{\mathbf{0}\}$, namely, $h \xleftarrow{\$} \mathcal{H}$. Finally, for any given $(x,\, h,\, v)$, one efficiently determines the value $y^* = f(x) - v \cdot h^{-1}$ due to the arithmetics over the finite field. $\square$

4 UOWHFs from Known Regular OWFs

We proceed to the more general case that f is a known almost-regular function. Recall that by Fact 1 we can assume WLOG that the underlying almost regular one-way function is length-preserving. We first show a construction where the hardness parameter ε is known, and then remove the dependency on ε.

4.1 Compressing the Output is Necessary but Not Sufficient

We attempt to generalize the Naor-Yung approach for one-way permutations (and 1-to-1 one-way functions) to almost regular one-way functions by compressing (using $\mathsf{trunc} \circ h$) the output $Y = f(X)$ into $\mathbf{H}_\infty(Y) - s'$ bits for $s' \in O(\log(1/\varepsilon))$. However, this only gives a weak form of guarantee, as stated in Lemma 2 below, that given a random x it is infeasible for efficient algorithms to find any $f(x') \neq f(x)$ such that $\mathsf{trunc}(h(f(x'))) = \mathsf{trunc}(h(f(x)))$. Otherwise said, it does not rule out the possibility that one may easily find $x' \neq x$ satisfying $f(x') = f(x)$. Hence, compressing the output is only a useful intermediate step to obtain UOWHFs. Lemma 2 below further generalizes Theorem 1 to known-(almost-)regular functions, whose proof is similar to that of Theorem 1 (see [20]).

Lemma 2. *For any constant c, any efficiently computable $r = r(n)$ and $s' = s'(n)$, let $f : \{0,1\}^n \to \{0,1\}^n$ be any $(2^r, 2^r n^c)$-almost regular (length-preserving) (t, ε)-one-way function, let $\mathcal{H}$ be a family of permutations over $\{0,1\}^n$ as below*

$$\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^n \ , \ h(y) \stackrel{def}{=} h{\cdot}y, \ \ \textit{where} \ \ y \in GF(2^n), \ \mathbf{0} \neq h \in GF(2^n) \ \} \ ,$$

let $\mathsf{trunc} : \{0,1\}^n \to \{0,1\}^{n-r-c\cdot\log n - s'}$ *be a truncating function. Then, for any* $\tilde{\mathsf{A}}$ *of running time* $t - n^{O(1)}$ *(for some universal constant $O(1)$) we have that*

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n, \ h \xleftarrow{\$} \mathcal{H}, \ x' \leftarrow \tilde{\mathsf{A}}(x,h)} [\ f(x) \neq f(x') \ \wedge \ \mathsf{trunc}(h(f(x))) = \mathsf{trunc}(h(f(x'))) \ ] \ \leq \ n^c \cdot 2^{s'+1} \cdot \varepsilon \ .$$

4.2 Known (Almost-)Regular OWFs with Known Hardness

We first give an optimal construction assuming that the inversion probability upper bound ε is known. Note that in addition to hashing the output $f(x)$ (as we did in Lemma 2), we also hash the input x to ensure that no distinct x' collides with x with respect to the resulting function.

Theorem 2 (UOWHFs from known-almost-regular ε-hard OWFs). *Let $f : \{0,1\}^n \to \{0,1\}^n$ be any $(2^r, 2^r n^c)$-almost regular (length-preserving) (t,ε)-one-way function as assumed in Lemma 2. Let shrinkage $s = s(n)$ be any efficiently computable function, and let $\mathcal{H}$ and* trunc *be as defined in Lemma 2 with $s' = (s + \log(1/\varepsilon) - c\log n)/2$, and let $\mathcal{H}_1 = \{h_1 : \{0,1\}^n \to \{0,1\}^{r + c\log n + s' - s}\}$ be a family of universal hash functions. Then, we have that*

$$\mathcal{G}_2 \stackrel{def}{=} \{ \ g : \{0,1\}^n \to \{0,1\}^{n-s} \ , \ g(x) \stackrel{def}{=} (g_1(x), h_1(x)), \ g_1 \in \mathcal{H} \ , h_1 \in \mathcal{H}_1 \ \}$$

where $g_1 \stackrel{\text{def}}{=} (\mathsf{trunc} \circ h \circ f)$*, is a* $(t - n^{O(1)}, O(\sqrt{2^s \cdot n^c \cdot \varepsilon}))$*-universal one-way hash function family with key and output length* $\Theta(n)$*.*

Proof. Define shorthands $\mathcal{E}_1 \stackrel{\text{def}}{=} \big(x \neq x' \wedge f(x) = f(x') \wedge h_1(x) = h_1(x')\big)$ and $\mathcal{E}_2 \stackrel{\text{def}}{=} \big(f(x) \neq f(x') \wedge g_1(x) = g_1(x')\big)$. For any $\mathcal{G}_2$-collision finder A, we have

$$\begin{aligned}
&\Pr_{x \stackrel{\$}{\leftarrow} \{0,1\}^n,\ (h,h_1) \stackrel{\$}{\leftarrow} (\mathcal{H},\mathcal{H}_1),\ x' \leftarrow \mathsf{A}(x,h,h_1)}[\ x \neq x' \ \wedge\ g(x) = g(x')\ ] \\
&\leq \Pr_{x \stackrel{\$}{\leftarrow} \{0,1\}^n,\ (h,h_1) \stackrel{\$}{\leftarrow} (\mathcal{H},\mathcal{H}_1),\ x' \leftarrow \mathsf{A}(x,h,h_1)}[\ \mathcal{E}_1 \ \vee\ \mathcal{E}_2\ ] \\
&\leq \Pr_{x \stackrel{\$}{\leftarrow} \{0,1\}^n,\ h_1 \stackrel{\$}{\leftarrow} \mathcal{H}_1}[\ \exists\ x' \neq x \ \wedge\ f(x) = f(x') \ \wedge\ h_1(x) = h_1(x')\ ] \\
&\quad + \Pr_{x \stackrel{\$}{\leftarrow} \{0,1\}^n,\ (h,h_1) \stackrel{\$}{\leftarrow} (\mathcal{H},\mathcal{H}_1),\ x' \leftarrow \mathsf{A}(x,h,h_1)}[\ f(x) \neq f(x') \ \wedge\ g_1(x) = g_1(x')\ ] \\
&\leq\ 2^{-(s'-s)} \ +\ n^c \cdot 2^{s'+1} \cdot \varepsilon \ =\ \sqrt{2^s \cdot n^c \cdot \varepsilon} \ +\ 2\sqrt{2^s \cdot n^c \cdot \varepsilon} \ =\ 3\sqrt{2^s \cdot n^c \cdot \varepsilon}\ ,
\end{aligned}$$

where the first inequality refers to that any collision on $g \in \mathcal{G}_2$ (for $x' \neq x$) must satisfy either $\mathcal{E}_1$ or $\mathcal{E}_2$ and the second inequality follows by a union bound. We already know by Lemma 2 that the second term is bounded by $n^c \cdot 2^{s'+1}\varepsilon$, and it thus remains to show that the first term is bounded by $2^{-(s'-s)}$. Conditioned on any $y = f(X)$ random variable X is a flat distribution on a set of size at most $2^r \cdot n^c$, so we apply Lemma 1 (setting $a = r + c \cdot \log n$, $d \geq s' - s$ and $k = 1$) to get

$$\begin{aligned}
&\Pr_{x \stackrel{\$}{\leftarrow} \{0,1\}^n,\ h_1 \stackrel{\$}{\leftarrow} \mathcal{H}_1}[\ \exists\ x' \neq x \ \wedge\ f(x) = f(x') \ \wedge\ h_1(x) = h_1(x')\ ] \\
&=\ \mathbb{E}_{y \leftarrow f(U_n)}\Big[\Pr_{x \stackrel{\$}{\leftarrow} f^{-1}(y),\ h_1 \stackrel{\$}{\leftarrow} \mathcal{H}_1}[\ \exists\ x' \neq x \ \wedge\ f(x) = f(x') \ \wedge\ h_1(x) = h_1(x')\ ]\ \Big] \\
&\leq\ \mathbb{E}_{y \leftarrow f(U_n)}[\ 2^{-(s'-s)}\ ] \ = 2^{-(s'-s)}\ ,
\end{aligned}$$

which completes the proof.

4.3 An Alternative Approach to Section 4.2

A neater (and perhaps more intuitive) approach is to construct an almost 1-to-1 one-way function f' (with input and output lengths $\Theta(n)$) based on f (stated as Theorem 3) and then plug f' into Theorem 1 (using f' in place of f) [12] . This statement is interesting in its own right as it implies that almost 1-to-1 one-way functions and known-(almost-)regular one-way functions (with known hardness) are equivalent. Taking a closer look at Theorem 3 we find that this almost 1-to-1 f' is also present (as an intermediate function) in construction $\mathcal{G}_2$ of Theorem 2 (except with slightly different length parameters). Lemma 3 and Lemma 4 state the almost injectiveness and one-way-ness of f' respectively, for which we determine a judicious value for d (assuming knowledge about ε) in Theorem 3 to achieve injectiveness and one-way-ness simultaneously.

[12] Strictly speaking, we need to show that the construction works even if the underlying OWF is only 1-to-1 on an overwhelming fraction of inputs. The proof is given in [20].

Theorem 3 (almost 1-to-1 OWF from almost-regular ε-hard OWF). *Let $f : \{0,1\}^n \to \{0,1\}^n$ be any $(2^r, 2^r n^c)$-almost regular (length-preserving) (t,ε)-one-way function as assumed in Lemma 2. For efficiently computable $d = d(n) \in \mathbb{N}$, define*

$$f' : \{0,1\}^n \times \mathcal{H}_1 \to \{0,1\}^n \times \{0,1\}^{r+c\cdot\log n+d} \times \mathcal{H}_1$$

$$f'(x, h_1) \stackrel{def}{=} (f(x), h_1(x), h_1)$$

where $\mathcal{H}_1$ is a family of universal hash functions from n bits to $r + c{\cdot}\log n + d$ bits. Then, for $d = \frac{\log(1/\varepsilon)-c\cdot\log n-3}{3}$ we have that f' is $2\sqrt[3]{\varepsilon \cdot n^c}$-almost 1-to-1 and $(t - O(n),\ 2\sqrt[3]{\varepsilon \cdot n^c})$-one-way with input and output lengths $\Theta(n)$.

Proof. The almost 1-to-1-ness and one-way-ness of f' follow from Lemma 3 and Lemma 4 respectively by setting parameter $d = \frac{\log(1/\varepsilon)-c\cdot\log n-3}{3}$.

Lemma 3 (f' is almost 1-to-1 [20]). *f' defined in Theorem 3 is 2^{-d}-almost 1-to-1.*

Lemma 4 (f' is one-way [20]). *f' defined in Theorem 3 is a $(t - O(n), \sqrt{2^{d+3} \cdot n^c \cdot \varepsilon})$-one-way function.*

4.4 UOWHFs from any Known (Almost-)Regular OWFs

Removing the dependency on ε. Unfortunately, Theorem 2 doesn't immediately apply to an arbitrary regular function as in general we assume no knowledge about ε (other than that ε is negligible). To see the difficulty, check the proof of Theorem 2 where the security of the resulting UOWHF is bounded by the sum of two terms, i.e., $2^{-(s'-s)} + n^c{\cdot}2^{s'+1} \cdot \varepsilon$. Without knowing ε, one may end up setting some super-polynomial $2^{s'}$ (to make the first term negligible) which kills the second term $n^c{\cdot}2^{s'+1} \cdot \varepsilon$. Same problems arise in similar situations (e.g., construction of PRGs from regular OWFs [22]). A remedy for this is parallel repetition: run $q \in \omega(1)$ copies of f on $\boldsymbol{x} = (x_1, \ldots, x_q)$, apply hash-then-truncate (setting $s' = 2\log n$) to every copy $f(x_i)$, which shrinks the entropies by $2q\log n$ bits and yields a bound $O(\varepsilon{\cdot}n^{c+2})$. Next, apply a single hashing to $\boldsymbol{x}$ that expands $q{\cdot}\log n$ bits (to yield another negligible term n^{-q}). This gives a family of UOWHFs with shrinkage $2q\log n - q\log n = q\log n$, and key and output length $O(q \cdot n)$ for any (efficiently computable) $q \in \omega(1)$. The proof is similar in spirit to that of Theorem 2 (see [20]).

Definition 8 (parallel repetition). *For any function $g : \mathcal{X} \to \mathcal{Y}$, we define its q-fold parallel repetition $g^q : \mathcal{X}^q \to \mathcal{Y}^q$ as*

$$g^q(x_1, ..., x_q) = (\ g(x_1)\ , ...,\ g(x_q)\ ) \quad .$$

For simplicity, we use shorthand $\boldsymbol{x} \stackrel{def}{=} (x_1, \ldots, x_q)$ and thus $g^q(\boldsymbol{x}) = g^q(x_1, \ldots, x_q)$.

Theorem 4 (UOWHFs from any known almost-regular OWFs). *Let $f : \{0,1\}^n \to \{0,1\}^n$ be any $(2^r, 2^r n^c)$-almost regular (length-preserving) (t,ε)-one-way function as assumed in Lemma 2. Then, for any efficiently computable $q = q(n) = \omega(1)$, let $\mathcal{H}$ and trunc be as defined in Lemma 2 with $s' = 2\log n$, and let $\mathcal{H}_1 = \{h_1 : \{0,1\}^{q\cdot n} \to \{0,1\}^{q(r+(c+1)\log n)}\}$ be a family of universal hash functions, we have that*

$$\mathcal{G}_3 \stackrel{def}{=} \{\ g : \{0,1\}^{qn} \to \{0,1\}^{qn-q\log n}\ ,\ g(\boldsymbol{x}) \stackrel{def}{=} (g_1(\boldsymbol{x}), h_1(\boldsymbol{x})),\ h \in \mathcal{H}\ , h_1 \in \mathcal{H}_1\ \}$$

where $g_1 \stackrel{def}{=} (\mathsf{trunc} \circ h \circ f)^q$, is a $(t - n^{O(1)}, n^{-q} + 2q\cdot n^{c+2}\cdot\varepsilon)$-universal one-way hash function family with key and output length $O(q\cdot n)$, and shrinkage $q\cdot\log n$.

5 Going Beyond Almost-Regular OWFs

Although (almost) optimal, our foregoing constructions need at least almost-regularity, i.e., the one-way function f satisfies $\alpha \le |f^{-1}(f(x))| \le \alpha\cdot\beta$ for all (or at least an overwhelming portion of) x, where α is efficiently computable and $\beta = \mathsf{poly}(n)$ (or at most $\beta = O(\log(1/\varepsilon))$ for an $(\varepsilon^{-1},\varepsilon)$-hard f). Complementary to our work, Ames et al. [1] gave an elegant construction from unknown-(almost-)regular one-way functions, namely, without knowledge about α, for which they pay a cost of much increased number of one-way function calls (i.e., $O(n/\log n)$) and key length $O(n\log n)$. In this section, we further weaken the assumption so that f can have an arbitrary structure (i.e., β is not bounded) as long as the fraction of x's with (nearly) maximal number of siblings is noticeable.

5.1 A More General Class of OWFs

The following class of one-way functions was introduced in [21] as a relaxation to unknown-(almost-)regular one-way functions.

Definition 9 (weakly unknown-regular OWFs [21]). *Let $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a one-way function, and for every $n \in \mathbb{N}$, divide domain $\{0,1\}^n$ into sets $\mathcal{X}_1, \ldots, \mathcal{X}_n$ (i.e., $\mathcal{X}_1 \cup \ldots \cup \mathcal{X}_n = \{0,1\}^n$) such that $\mathcal{X}_j \stackrel{def}{=} \{x : 2^{j-1} \le |f^{-1}(f(x))| < 2^j\}$, and define $\max = \max(n)$ to be the maximal subscript of the non-empty sets, i.e., $|\mathcal{X}_{\max}| > 0$ and $|\mathcal{X}_{\max+1} \cup \ldots \cup \mathcal{X}_n| = 0$. We say that f is* ***weakly unknown-regular*** *if there exists a constant c such that for all sufficiently large n :*

$$\Pr[U_n \in \mathcal{X}_{\max}] \ge n^{-c}\ . \qquad (1)$$

Note that $\max(\cdot)$ can be arbitrary (not necessarily efficient) functions and thus unknown-regular one-way functions fall into a special case[13] *for $c = 0$.*

[13] In fact, our construction #4 only assumes a relaxed condition than (1), i.e., $\Pr[U_n \in \mathcal{X}_{\max - O(\log n)} \cup \ldots \cup \mathcal{X}_{\max}] \ge n^{-c}$, so that unknown-almost-regular one-way functions become a special case for $c = 0$.

5.2 UOWHFs from Beyond Almost-Regular OWFs

We state below the main results of this section, namely, the fourth construction which is based on weakly unknown-regular one-way functions (see Definition 9).

Theorem 5. *Assume that f is a weakly unknown-regular one-way function on an n^{-c}-fraction of domain for constant c. Then, there exists an explicit construction of UOWHF family with output length $\Theta(n)$, key length $O(n \cdot \log n)$ by making $n^{2c+1} \cdot \omega(1)$ black-box calls to f.*

The main idea is to transform any weakly unknown-regular one-way function f into a family of functions $\mathcal{F} = \{f_u : u \in \{0,1\}^{O(n \log n)}\}$ such that $\mathcal{F}$ is almost regular and that it preserves the one-way-ness of f. $\mathcal{F}$ is constructed based on (the derandomized version of) the randomized iterate with a succinct description u. Finally, we sample a random $f_u \xleftarrow{\$} \mathcal{F}$ and plug it into the construction by Ames et al. to get the UOWHFs as desired. We refer to [20] for more details about the explicit construction.

Definition 10 (the randomized iterate [10,7]). *Let $n \in \mathbb{N}$, function $f : \{0,1\}^n \to \{0,1\}^n$, and let $\mathcal{H}$ be a family of pairwise-independent length-preserving hash functions over $\{0,1\}^n$. For $k \in \mathbb{N}$, $x_1 \in \{0,1\}^n$ and vector $\boldsymbol{h}^k = (h_1, \ldots, h_k) \in \mathcal{H}^k$, recursively define the i^{th} randomized iterate by:*

$$x_1 \xrightarrow{f} y_1 \xrightarrow{h_1} x_2 \xrightarrow{f} y_2 \xrightarrow{h_2} \quad \cdots \quad x_k \xrightarrow{f} y_k \xrightarrow{h_k}$$

$$y_i = f(x_i), \; x_{i+1} = h_i(y_i) \; .$$

We denote the i^{th} iterate by function f^i, i.e., $y_i = f^i(x_1, \boldsymbol{h}^k)$, where $\boldsymbol{h}^k$ is possibly redundant as for $i \le k+1$ y_i only depends on $\boldsymbol{h}^{i-1}$.
*The **randomized version** refers to the case where $x_1 \xleftarrow{\$} \{0,1\}^n$ and $\boldsymbol{h}^k \xleftarrow{\$} \mathcal{H}^k$.*
*The **derandomized version** refers to that $x_1 \xleftarrow{\$} \{0,1\}^n$, $u \xleftarrow{\$} \{0,1\}^{q \in O(n \cdot \log n)}$, $\boldsymbol{h}^k := BSG(u)$, where $BSG : \{0,1\}^q \to \{0,1\}^{k \cdot \log|\mathcal{H}|}$ is a bounded-space generator that 2^{-2n}-fools every $(2n+1, k, \log|\mathcal{H}|)$-LBP (layered branching program), and $\log|\mathcal{H}|$ is the description length of $\mathcal{H}$ (e.g., $2n$ bits for concreteness).*

Remark 2 (on what is proven in [21]). The authors of [21] introduced weakly unknown-regular one-way functions from which they constructed a pseudorandom generator with seed length $O(n \cdot \log n)$ based on the randomized iterate. They showed that "every $k = n^{2c} \cdot \log n \cdot \omega(1)$ iterations are hard-to-invert", i.e., for any j it is hard to predict x_j given $y_{j+k} = f^{j+k}(x_1, BSG(u))$ and u. A PRG thus follows by outputting $\log n$ hardcore bits for every k iterations. In this paper, we first adapt their findings to show that $f_u(\cdot) = f^k(\cdot, BSG(u))$ constitutes a family of one-way functions, i.e., given $y_k = f_u(x_1)$ and u it is infeasible to find any x'_1 such that $y_k = f^k(x'_1, BSG(u))$. This is stated as Lemma 6. However, it is still insufficient to construct UOWHFs with the one-way-ness of f_u. We further show in Lemma 7 that a random $f_u \xleftarrow{\$} \mathcal{F}$ is almost regular (in a slightly weaker sense than Definition 6 but already suffices for our needs).

Following [21], we define the following event and recall some inequalities.

Definition 11. *For any $n, j \leq k \in \mathbb{N}$, define events*

$$\mathcal{E}'_j \stackrel{\text{def}}{=} \left((X_1, U_q) \in \{\ (x_1, u) : y_j = f^j(x_1, BSG(u)) \in \mathcal{Y}_{\max}\ \} \right)$$

where $\mathcal{Y}_{\max} \stackrel{\text{def}}{=} \{y : 2^{\max -1} \leq |f^{-1}(y)| < 2^{\max}\}$, and (X_1, U_q) are uniform over $\{0,1\}^n \times \{0,1\}^q$. Note that by definition $\mathcal{Y}_{\max} = f(\mathcal{X}_{\max})$ (see Definition 9) and thus $\Pr[f(U_n) \in \mathcal{Y}_{\max}] \geq n^{-c}$.

Lemma 5 (Some inequalities from [20]).

$$\mathsf{CP}(\ Y'_k \mid U_q) \ \leq\ k \cdot 2^{\max - n + 1} + 2^{-2n}, \tag{2}$$

$$\Pr[\mathcal{E}'_1 \vee \mathcal{E}'_2 \vee \ldots \vee \mathcal{E}'_k] \ \geq\ 1 - 2^{-k/n^{2c}} - 2^{-2n}\ , \tag{3}$$

where $Y'_k \stackrel{\text{def}}{=} f^k(X_1, BSG(U_q))$.

Lemma 6 ($\mathcal{F}$ is one-way [20]). *Assume that f is a (t,ε)-OWF that is weakly unknown-regular on an n^{-c} fraction of domain, define a family of functions*

$$\mathcal{F} \stackrel{\text{def}}{=} \{\ f_u : \{0,1\}^n \to \{0,1\}^n, f_u(x) = f^k(x, BSG(u)), u \in \{0,1\}^{O(n \cdot \log n)}\ \} \tag{4}$$

where $\mathcal{H}$, f^k and $BSG : \{0,1\}^{q \in O(n \cdot \log n)} \to \{0,1\}^{k \cdot \log|\mathcal{H}|}$ are as defined in Definition 10. Then, for any A of running time $t - n^{O(1)}$ it holds that

$$\Pr_{u \xleftarrow{\$} \{0,1\}^q,\ x \xleftarrow{\$} \{0,1\}^n} [\ \mathsf{A}(u, f_u(x)) \in f_u^{-1}(\ f_u(x)\ )\ ] \ \leq\ \sqrt{2^8 \cdot k^4 \cdot n^{3c} \cdot \varepsilon} + 2^{-k/n^{2c}} + 2^{-2n}\ . \tag{5}$$

Lemma 7 ($\mathcal{F}$ is almost-regular). *Let $\mathcal{F} = \{f_u\}$ be as defined in Lemma 6. Then, for any $a \geq 0$ it holds that*

$$\Pr_{u \xleftarrow{\$} \{0,1\}^q,\ x \xleftarrow{\$} \{0,1\}^n} [\ 2^{\max - a - 1}\ \leq\ |f_u^{-1}\ (\ f_u(x)\ )|\ \leq\ 2^{\max + a + 1}\ ] \ \geq\ 1 - \frac{k}{2^{a-2}} - \frac{1}{2^{k/n^{2c}}}, \tag{6}$$

where $u \in \{0,1\}^{q \in O(n \cdot \log n)}$ and $f_u(x) = f^k(x, BSG(u))$.

Proof. We define $\mathcal{S}_{low} \stackrel{\text{def}}{=} \left((X_1, U_q) \in \{(x,u) : 0 < |f_u^{-1}(f_u(x))| < 2^{\max - a - 1}\} \right)$ and $\mathcal{S}_{up} \stackrel{\text{def}}{=} \left((X_1, U_q) \in \{(x,u) : |f_u^{-1}(f_u(x))| > 2^{\max + a + 1}\} \right)$, where X_1 is uniform over $\{0,1\}^n$. The left-hand of (6) is lower bounded by $1 - \Pr[\mathcal{S}_{low}] - \Pr[\mathcal{S}_{up}]$ and thus it suffices to upper bound both $\Pr[\mathcal{S}_{low}]$ and $\Pr[\mathcal{S}_{up}]$. We have

$$\begin{aligned}
\Pr[\mathcal{S}_{low}] \ &=\ \Pr[\mathcal{S}_{low} \wedge (\mathcal{E}'_1 \vee \mathcal{E}'_2 \vee \ldots \vee \mathcal{E}'_k)] \ +\ \Pr[\mathcal{S}_{low} \wedge \neg(\mathcal{E}'_1 \vee \mathcal{E}'_2 \vee \ldots \vee \mathcal{E}'_k)] \\
&\leq\ \Pr[\bigvee_{j=1}^{k} (\mathcal{S}_{low} \wedge \mathcal{E}'_j)] \ +\ \Pr[\neg(\mathcal{E}'_1 \vee \mathcal{E}'_2 \vee \ldots \vee \mathcal{E}'_k)] \\
&\leq\ \sum_{j=1}^{k} \Pr[\mathcal{S}_{low} \wedge \mathcal{E}'_j] \ +\ (2^{-k/n^{2c}} \ +\ 2^{-2n}) \\
&\leq k \cdot 2^{-a} \ +\ 2^{-k/n^{2c}} \ +\ 2^{-2n}
\end{aligned}$$

where the first inequality is trivial, the second is by the union bound and (3), and the third is due to that for every $j \in [k]$ with shorthand $f_{u,j}(x) \stackrel{\text{def}}{=} f^j(x, BSG(u))$ it holds that

$$\begin{aligned}
\Pr[\mathcal{S}_{low} \wedge \mathcal{E}'_j] \;&=\; \sum_{u} \Pr[U_q = u] \cdot \sum_{x:\; f_{u,j}(x) \in \mathcal{Y}_{\max} \,\wedge\, 0<|f_u^{-1}(f_u(x))|<2^{\max -a-1}} \Pr[X_1 = x | U_q = u] \\
&\le \sum_{u} \Pr[U_q = u] \cdot \sum_{x:\; f_{u,j}(x) \in \mathcal{Y}_{\max} \,\wedge\, 0<|f_{u,j}^{-1}(f_{u,j}(x))|<2^{\max -a-1}} \Pr[X_1 = x \mid U_q = u] \\
&\le \sum_{u} \Pr[U_q = u] \cdot |\mathcal{Y}_{\max}| \cdot 2^{\max -a-1} \cdot 2^{-n} \\
&\le 2^{n+1-\max} \cdot 2^{-n+\max -a-1} \;=\; 2^{-a}
\end{aligned}$$

where the first inequality is due to Fact 3 (setting $f_1{=}f_{u,j}$, $f_2 = f \circ h_{k-1} \circ \ldots \circ f \circ h_j$ and thus $\bar{f} = f_u$), the second follows from the fact that there are $|\mathcal{Y}_{\max}|$ possible values for $f_{u,j}(x) \in \mathcal{Y}_{\max}$ and every $f_{u,j}(x)$ has less than $2^{\max -a-1}$ preimages (by definition of $\mathcal{S}_{low}$), and the third is due to $|\mathcal{Y}_{\max}| {\le} 2^{n+1-\max}$. Next we proceed to bounding the second term, i.e., $\Pr[\mathcal{S}_{up}] \;\le\; k{\cdot}2^{-a+1}$.

$$\begin{aligned}
k{\cdot}2^{\max - n+1} + 2^{-2n} \;\ge\; \mathsf{CP}(\, Y'_k \mid U_q) \;&=\mathbb{E}_{u \leftarrow U_q}\left[\sum_{y} \Pr[\, f_u(X_1) = y \mid U_q = u]^2 \right] \\
&>\; 2^{\max + a - n+1} \cdot \mathbb{E}_{u \leftarrow U_q}\left[\sum_{y:\; |f_u^{-1}(y)| > 2^{\max +a+1}} \Pr[\, f_u(X_1) = y \mid U_q = u] \right] \\
&=\; 2^{\max + a - n+1} \cdot \Pr[\mathcal{S}_{up}] \;\; ,
\end{aligned}$$

where the first inequality is by (2), and the second is due to that for any (y, u) satisfying $|f_u^{-1}(y)| > 2^{\max +a+1}$ and it holds that

$$\Pr[\, f_u(X_1) = y \,|\, U_q = u] \;=\; \Pr[\, X_1 \in f_u^{-1}(y)\,] \;> 2^{-n} {\cdot} 2^{\max + a+1} = 2^{\max + a - n+1} \;\; .$$

It follows that $\Pr[\mathcal{S}_{up}] \le (k{\cdot}2^{\max - n+1} + 2^{-2n}) / 2^{\max + a - n+1} {\le} k{\cdot}2^{-a+1}$ and hence completes the proof.

Fact 3 *Let $f_1 : \mathcal{X} \to \mathcal{Y}$ and $f_2 : \mathcal{Y} \to \mathcal{Z}$ be any functions, and let $\bar{f} \stackrel{\text{def}}{=} f_2 \circ f_1$. Then for any $t \in \mathbb{N}^+$ it holds that*

$$\{x : 0 < |\bar{f}^{-1}(\bar{f}(x))| < t\} \;\subseteq\; \{x : 0 < |f_1^{-1}(f_1(x))| < t\} \;\; .$$

Proof. Any x satisfying $0 < |\bar{f}^{-1}(\bar{f}(x))| < t$ implies $0 < |f_1^{-1}(f_1(x))| < t$.

Given that $\mathcal{F}$ is a family of unknown-(almost-)regular one-way functions with description length $O(n \cdot \log n)$, we just plug a random $f_u \in \mathcal{F}$ into the Ames et al.'s construction [1] to yield a family of UOWHFs with output length $\Theta(n)$ and key length $O(n \cdot \log n)$. We refer to a more complete version of this work [20], where we put together all the necessary technical details.

Acknowledgement

This research work was supported by the National Basic Research Program of China (Grant 2013CB338004). Yu Yu was supported by the National Natural Science Foundation of China Grant (Nos. 61472249, 61103221). Dawu Gu was supported by the National Natural Science Foundation of China Grant (Nos. 61472250, 61402286), the Doctoral Fund of Ministry of Education of China (No. 20120073110094) and the Innovation Program by Shanghai Municipal Science and Technology Commission (No. 14511100300). Xiangxue Li was supported by the National Natural Science Foundation of China (Nos. 61472472, 61272536) and Science and Technology Commission of Shanghai Municipality (Grant 13JC1403500). Jian Weng was supported by NSFC under Grant Nos. 61133014, 61472165 and 61272413, the Program for New Century Excellent Talents in University under Grant No. NCET-12-0680, and the Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20100073110060.

References

1. Ames, S., Gennaro, R., Venkitasubramaniam, M.: The generalized randomized iterate and its application to new efficient constructions of UOWHFs from regular one-way functions. In: ASIACRYPT. pp. 154–171 (2012)
2. Barhum, K., Holenstein, T.: A cookbook for black-box separations and a recipe for uowhfs. In: Proceedings of the 5th Theory of Cryptography Conference (TCC 2013). pp. 662–679 (2013)
3. Barhum, K., Maurer, U.: UOWHFs from OWFs: Trading regularity for efficiency. In: LATINCRYPT. pp. 234–253 (2012)
4. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing 33(1), 167–226 (2003)
5. Gennaro, R., Gertner, Y., Katz, J., Trevisan, L.: Bounds on the efficiency of generic cryptographic constructions. SIAM Journal on Computing 35(1), 217–246 (2005)
6. Goldreich, O.: Foundations of Cryptography: Basic Tools. Cambridge University Press (2001)
7. Goldreich, O., Krawczyk, H., Luby, M.: On the existence of pseudorandom generators. SIAM Journal on Computing 22(6), 1163–1175 (1993)
8. Goldreich, O., Levin, L.A., Nisan, N.: On constructing 1-1 one-way functions. In: Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation, pp. 13–25 (2011)
9. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing 17(2), 281–308 (April 1988)
10. Haitner, I., Harnik, D., Reingold, O.: On the power of the randomized iterate. In: Proceedings of the 26th International Cryptology Conference (CRYPTO 2006). pp. 22–40 (2006)
11. Haitner, I., Holenstein, T., Reingold, O., Vadhan, S.P., Wee, H.: Universal one-way hash functions via inaccessible entropy. In: EUROCRYPT. pp. 616–637 (2010)

12. Haitner, I., Nguyen, M.H., Ong, S.J., Reingold, O., Vadhan, S.P.: Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. SIAM Journal on Computing 39(3), 1153–1218 (2009)
13. Haitner, I., Reingold, O., Vadhan, S.P., Wee, H.: Inaccessible entropy. In: Proceedings of the 41st ACM Symposium on the Theory of Computing. pp. 611–620 (2009)
14. Holenstein, T., Sinha, M.: Constructing a pseudorandom generator requires an almost linear Number of calls. In: Proceedings of the 53rd IEEE Symposium on Foundation of Computer Science. pp. 698–707 (2012)
15. Katz, J., Koo, C.Y.: On constructing universal one-way hash functions from arbitrary one-way functions. IACR Cryptology ePrint Archive (2005), http://eprint.iacr.org/2005/328
16. Naor, M., Yung, M.: Universal one-way hash functions and their cryptographic applications. In: Johnson, D.S. (ed.) Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing. pp. 33–43. Seattle, Washington (15–17 May 1989)
17. Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In: Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing. pp. 387–394. Baltimore, Maryland (14–16 May 1990)
18. Rompel, J.: Techniques for computing with low-independence randomness. Ph.D. thesis, Massachusetts Institute of Technology (1990), http://dspace.mit.edu/handle/1721.1/7582
19. Santis, A.D., Yung, M.: On the design of provably secure cryptographic hash functions. In: EUROCRYPT. pp. 412–431 (1990)
20. Yu, Y., Gu, D., Li, X., Weng, J.: (Almost) Optimal Constructions of UOWHFs from 1-to-1, Regular One-way Functions and Beyond. Cryptology ePrint Archive, Report 2014/393 (2014), http://eprint.iacr.org/2014/393/
21. Yu, Y., Gu, D., Li, X., Weng, J.: The randomized iterate revisited - almost linear seed length PRGs from a broader class of one-way functions. In: 12th Theory of Cryptography Conference (TCC 2015). pp. 7–35 (2015)
22. Yu, Y., Li, X., Weng, J.: Pseudorandom generators from regular one-way functions: New constructions with improved parameters. In: ASIACRYPT. pp. 261–279 (2013)