Optimal Constructions of Universal One-way Hash Functions from Special One-way Functions

Yu Yu¹, Dawu Gu¹, Xiangxue Li², Jian Weng³
¹Shanghai Jiao Tong University, China
²East China Normal University, China
³Jinan University, China

October 1, 2015
One-way Functions

\[ f: \{0,1\}^n \rightarrow \{0,1\}^m \text{ is a one-way function if} \]

Simplifying assumption: \( m = n \).
(Target) Collision Resistance

Collision Resistance (CR)

Challenger
\[ h \leftarrow \$ \perp H \]
Adversary
\[ (x, x') \leftarrow A (h) \]

\[ h, x \]
\[ x, x' \]

\[ \text{CR} \downarrow A, H \] outputs 1 iff \( x \neq x' \land h(x) = h(x') \)

Target Collision Resistance (TCR)

Challenger
\[ h \leftarrow \$ \perp H \]
\[ x \leftarrow \$ \perp X \]
Adversary
\[ x' \leftarrow A (h, x) \]

\[ h, x \]
\[ x, x' \]

\[ \text{TCR} \downarrow A, H \] outputs 1 iff \( x \neq x' \land h(x) = h(x') \)
CRHFs vs. UOWHFs

- **H** is a family of Collision Resistant Hash Functions (CRHFs) if \( \forall \text{PPT } A: \Pr[\text{CR} \downarrow A, H (1 \uparrow n) = 1] = \text{negl}(n) \)

- **H** is a family of **Universal One-Way Hash Functions** (UOWHFs) if \( \forall \text{PPT } A: \Pr[\text{TCR} \downarrow A, H (1 \uparrow n) = 1] = \text{negl}(n) \)

- **Note**: **H** is a family of functions (not a single one)

- **UOWHFs** are believed strictly weaker than CRHFs
  - CRHFs are UOWHFs
  - OWFs imply UOWHFs but not CRHFs

- **Yet, UOWHFs suffice for many applications**
  - Basing digital signatures on one-way functions alone!
  - Cramer-Shoup PKE Schemes
  - Statistical hiding
One-way Functions (OWFs)

A building block of many crypto applications

Many crypto applications

- Pseudorandom functions
- Pseudorandom generators
- Digital
- Stat ZK
- Permutations
- UOWHFs
- NaorYung89, HHRVW10
- Stat hiding commitment

One-way functions
Duality between PRGs and UOWHFs

OWFs → UOWHFs was established even earlier than OWFs → PRGs.

But now efficiency improvement of UOWHFs lag much behind PRGs!
An overview of literature and our work: UOWHFs from special one-way functions.

<table>
<thead>
<tr>
<th>underlying primitive</th>
<th>black-box construction of UOWHFs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Work</td>
</tr>
<tr>
<td>one-way permutation</td>
<td>[NY89]</td>
</tr>
<tr>
<td>1-to-1 one-way function</td>
<td>[NY89]</td>
</tr>
<tr>
<td>known-regular one-way function</td>
<td>[BM12]</td>
</tr>
<tr>
<td>unknown-regular one-way function</td>
<td>Our work</td>
</tr>
<tr>
<td>+ known hardness</td>
<td>Our work</td>
</tr>
<tr>
<td>weakly-regular one-way function</td>
<td>[AGV12]</td>
</tr>
</tbody>
</table>

(arginably) more close to arbitrary one-way functions
Universal Hashing

- **Universal hash functions:** \( H: \{0,1\}^n \rightarrow \{0,1\}^m \) \((n \geq m)\) is **universal** if \( \forall x \downarrow 1 \neq x \downarrow 2 : \Pr \downarrow h \leftarrow H \left[ h(x \downarrow 1) = h(x \downarrow 1) \right] \leq 2^{-m} \)

- **E.g.,** \( H: \{ h \downarrow a \} : \{0,1\}^n \rightarrow \{0,1\}^m \), \( h \downarrow a (x) = \text{trunc}(a \cdot x), a, h \in \text{GF}(2^n) \)

\( \text{trunc}: \{0,1\}^n \rightarrow \{0,1\}^m \) outputs only the first \( m \) bits

- **Well-known hashing properties (informal):**
  - **(leftover hash lemma, unconditional indistinguishability):**
    For any \( X \in \{0,1\}^n \) with \( H \downarrow \infty (X) \geq m + d \), we have \( h(X) \) is \( 2^{\Omega(d)} \)-close to uniform (conditioned on a random \( h \leftarrow H \)).

  - **(injective hash lemma, unconditional TCR):**
    Definition: Max-entropy of \( X \), denoted by \( H \downarrow 0 (X) = \log |\text{Supp}(X)| \)
    For any \( X \in \{0,1\}^n \) with \( H \downarrow 0 (X) \leq m - d \), we have
**OWPs \(\rightarrow\) UOWHFs [NY89]**

- **Assumption:** \((t, \varepsilon)\)-one-way permutation \(f: \{0,1\}^n \rightarrow \{0,1\}^n\)

- **Tool:** universal \(H:\{ h: \{0,1\}^n \rightarrow \{0,1\}^n \} \)

  \[
  \text{truncating \ } \circ \ f \rightarrow h(\circ) \rightarrow \text{truncating}
  \]

- **Statement:** \(G:\{ \text{trunc} \circ h \circ f \ | \ h \in H \}\) is a family of

  \((t-n^\Theta(1), 2^s \cdot \varepsilon)\)-universal one-way hash functions.

Reduction didn’t generalize to 1-to-1 one-way functions.
1-to-1 OWFs $\rightarrow$ UOWHFs \[NY89,DY90\]

- **Assumption:** $(t, \varepsilon)$-1-to-1 OWF $f: \{0,1\}^n \rightarrow \{0,1\}^l$ ($l > n$)

- **Tool:** universal $H\downarrow0, \ldots, H\downarrow l - n$, where $H\downarrow i : \{ h\downarrow i : \{0,1\}^l \rightarrow \{0,1\} \}$

- **Statement:** $G:\{ h\downarrow l - n \circ \cdots \circ h\downarrow 1 \circ h\downarrow 0 \circ f \mid h\downarrow 0 \in H\downarrow 0, \ldots, h\downarrow l - n \in H\downarrow l - n \}$

is a family of $(t - n \uparrow O(1), O(\varepsilon))$-UOWHFs.

The use of many hash functions seems to be an artifact of proof.

Can we derandomize this (ideally to key length $O(n)$)?
Construction #1: 1-to-1 OWFs $\rightarrow$ UOWHFs

- **Assumption:** $(t, \varepsilon)$-1-to-1 OWF $f: \{0,1\}^n \rightarrow \{0,1\}^l$ ($l > n$)
- **Tool:** universal $H = \{ h: \{0,1\}^l \rightarrow \{0,1\}^l \}$

**Truncating function** $\text{trunc} : \{0,1\}^l \rightarrow \{0,1\}^n - s$

- **Statement:** $G = \{ \text{trunc} \circ h \circ f \mid h \in H \}$ is a family of $(t - n \uparrow O(1), 2 \uparrow s + 1 \varepsilon)$-UOWHFs.
Construction #1: proof sketch

• Assumption (equivalent to \((t, \varepsilon)\)-OWF \(f: \{0,1\}^n \rightarrow \{0,1\}^l\)):

\[
\forall A \text{ of running time } t: \Pr \downarrow y^* \leftarrow \{0,1\}^l [\text{Inv}^A (y^*)] < 2^{l-(l-n)} \varepsilon
\]

• Lemma: Any \(A\) that \(2^s \varepsilon\)-breaks the TCR of \(\{\text{trunc} \circ h \circ f\}\) implies \(\text{Inv}^A\) (-same efficiency as \(A\)) such that

\[
\Pr \downarrow y^* \leftarrow \{0,1\}^l [\text{Inv}^A (y^*)] \in f^{-1} (y^*)] \geq 2^{l-(l-n)} \varepsilon
\]

• Proof sketch.

\(\text{Inv}^A (y^*)\) works as follows:

1. Sample \(y^* \leftarrow \{0,1\}^l, x \leftarrow \{0,1\}^n, \uparrow h \leftarrow \{ h: h(f(x)) \oplus h(y^*)\}

\(\text{trunc} \circ h \circ f\) = \(\sim 0 \ldots 0 \uparrow l - n - s \sim y \leftarrow \{0,1\}^l/\uparrow l - n + s / \)}
Construction #1: proof sketch (cont’d)

Inv↑A (y↑*) works as follows:

1. Sample y↑* ← {0,1}↑l, x←{0,1}↑n, ↑ h← { h: h(f(x)) ⊕ h(y↑*) = 0⋯0 ⊖ n−s ⊖ v←{0,1}↓↑l−n+s ↓ ⊖ l−n+s

(assume WLOG f(x) ≠ y↑*)

Claim: above sampling is equivalent to (x,h,v)←{0,1}↑n × H×{0,1}↓↑l−n+s

then determine y↑* from (x,h,v)

2. Invoke x'←A(x,h) and returns x'.

\[\Pr[Inv↑A (y↑*)] \geq 2↑s \epsilon \text{(by TCR)}\]

\[\Pr[A \text{ outputs } x, x' : x↑' \neq x \land h(f(x)) \oplus h(f(x↑')) = 0⋯0 \ominus n−s \ominus v] \geq \Pr[A \text{ outputs } x' : x↑' \neq x \land h(f(x)) \oplus h(f(x↑')) = 0⋯0 \ominus n−s \ominus v] \geq 2↑(l−n−s) \epsilon\]
Construction #2: known-regular OWFs (with known hardness) \( \rightarrow \) UOWHFs

- **Assumption:** \((t, \varepsilon)-(2 \uparrow r - \text{to}-1)\) OWF \( f : \{0,1\} \uparrow n \rightarrow \{0,1\} \uparrow n \) with known \( r \) and \( \varepsilon \)

- **Tool:** universal \( H = \{ h : \{0,1\} \uparrow n \rightarrow \{0,1\} \uparrow n - r - s' \} \)
  
  \[ H\downarrow 1 = \{ h\downarrow 1 : \{0,1\} \uparrow n \rightarrow \{0,1\} \uparrow r + s' - r - s \} \]

  (value of \( s' \) to determined later)

- **Theorem:** \( G = \{ g : \{0,1\} \uparrow n \rightarrow \{0,1\} \uparrow n - s \mid g(x) = (h(f(x)), h\downarrow 1 (x)) \} \)

  is a family of \((t - n \uparrow O(1), 2 \uparrow s - s) = 3 \sqrt{2 \uparrow s} + 1 \varepsilon)\)-UOWHFs.

Set \( s' = (s + \log(1/\varepsilon))/2 \)
Construction #2: known-regular OWFs (with known hardness) $\rightarrow$ UOWHFs

• Theorem: $G=\{g:\{0,1\}^n\rightarrow\{0,1\}^{n-s} | g(x)=(h(f(x)), h\downarrow 1(x))\}$

is a family of $(t-n^{O(1)}, 2^s-s^r + 2^s^r + 1\varepsilon)$-UOWHFs.

• Proof sketch.

$\forall$ PPT $A: \Pr \downarrow x\leftarrow\{0,1\}^n, h\leftarrow H, h\downarrow 1 \leftarrow H\downarrow 1 [x'\leftarrow A(x,h,h\downarrow 1): x\neq x\wedge g(x^{r}) = g(x)]$

$\leq 2^{t-(s^r-s)}$ by hashing lemma: $\log|f^{\uparrow -1}\{y\}|=r, h\downarrow 1(x)\in \{0,1\}^{r-(s^r-s)}$

$+ \Pr [f(x')\neq f(x) \wedge h(f(x))=h(f(x'))]$}

$\leq 2^{s^r} + 1\varepsilon$ by TCR (via a reduction to OWF, similar to construction #1):
Construction #3: known-regular OWFs $\rightarrow$ UOWHFs

- Assumption: $(t, \epsilon) - (2 \uparrow r \rightarrow 1)$ OWF $f$ with known $r$, unknown $\epsilon$

- \[ G = \{ g: \{0,1\}^{n} \rightarrow \{0,1\}^{n-s} \mid g(x) = (h(f(x)), h\downarrow 1(x)) \} \]

  with $h: \{0,1\}^{n} \rightarrow \{0,1\}^{n-r-s^{\uparrow}}$, $h\downarrow 1: \{0,1\}^{n} \rightarrow \{0,1\}^{r+s}$

  $- s$ are

  \[ (t-n^{\Omega}(1), 2^{\uparrow s}-s^{\uparrow} + 2^{\uparrow s^{\uparrow}} + 1^{\epsilon}) \text{-UOWHFs.} \]

  NOT work any more! (need $\epsilon$ to decide $s^{\uparrow}$)

- Remedy: Run $q = \omega(1)$ copies of $f$. Then

  \[ G' = \{ g: \{0,1\}^{qn} \rightarrow \{0,1\}^{q(n-\log n)} \mid g(x) = (h(f(x)), h\downarrow 1(x)) \} \]

  where $h(f(x)) = (h(f(x\downarrow 1)), \ldots, h(f(x\downarrow Q))) \in \{0,1\}^{q(n-r-2\log n)}$
Construction by [AGV12]: unknown-regular OWFs $\rightarrow$ UOWHFs

- **Assumption:** $(t, \varepsilon)$-$(2 \uparrow r \rightarrow 1)$ OWF $f$ with unknown $r$ and

  \[
  \{g \downarrow x, s\} : \{0,1\}^{\uparrow n+1} \rightarrow \{0,1\}^{\uparrow n}
  \]

  is a family of UOWHFs keyed by $(x,s) \in \{0,1\}^{\Theta(n \cdot \log n)}$ with input $b \downarrow 1 \ldots b \downarrow n + 1$, output $y \in \{0,1\}^{\uparrow n}$.

- Parameters: Output length $\Theta(n)$, key length $\Theta(n \log n)$. 

- Can we generalize beyond almost-regular OWFs?

---

\[
\begin{array}{c}
\text{x} \\
\downarrow f \\
\downarrow h_{\downarrow 1} \\
\downarrow f \\
\downarrow h_{\downarrow 2} \\
\vdots \\
\downarrow f \\
\downarrow h_{\downarrow n+1} \\
\uparrow y
\end{array}
\]
WEAKLY REGULAR OWFs\cite{YGLW15}

- \( f: \{0,1\}^n \rightarrow Y\\ inducing \ Y\downarrow j = \{ y: 2^{j-1} \leq |f^{-1}(y)| < 2^j \} \)

\[AGV12\] assumes \( f \) is **regular** or at least **almost-regular**

1. **Def (regular):** \( \exists \max: \Pr \downarrow [f(U\downarrow n) \in Y\downarrow \max] = 1 \)

2. **Def (almost-regular):** \( \exists \max, \ \exists d = O(\log n) : \)
   \[ \Pr [f(U\downarrow n) \in (Y\downarrow \max - d \cup Y\downarrow \max - d + 1 \cup \cdots \cup Y\downarrow \max)] = 1 - \text{negl}(n) \]

Construction #4 assumes (much) less: 3. or even 4.

3. **Def (weakly-regular):** \( \exists c \geq 0, \ \exists \max: \)
   \[ \Pr [f(U\downarrow n) \in Y\downarrow \max] \geq n^{1-c} \ \& \ \Pr [f(U\downarrow n) \in (Y\downarrow \max + 1 \cup Y\downarrow \max + 2 \cup \cdots \cup Y\downarrow n)] = 0 \]
Construction #4:
weakly-regular OWFs $\rightarrow$ UOWHFs

Assumption: weakly regular OWF $f:\{0,1\}^n \rightarrow Y_1 \cup Y_2 \cup \cdots \cup Y_n$, i.e. $\exists c \geq 0, \exists \text{max} : \Pr[f(U \downarrow n) \in Y_{\text{max}}] \geq n^{\uparrow - c} \& \Pr[f(U \downarrow n) \in (Y_{\text{max}} + 1 \cup \cdots \cup Y_n)] = 0$

Construction:

- **Step 1**: Construct a family of almost-regular OWFs $F = \{f \downarrow u : \{0,1\}^n \rightarrow \{0,1\}^n \mid u \in \{0,1\}^{O(n \cdot \log n)}\}$ from $f$
- **Step 2**: Plug $f \downarrow u \leftarrow F$ into [AGV12].

Parameters:

- **key length**: $O(n \cdot \log n)$
- **output length**: $O(n)$
- $n^{\uparrow \mathcal{O}(1)}$, OWF calls
Constructing almost-regular one-way functions from weakly one-way functions

One-wayness: \( \forall \text{PPT } A: \Pr \downarrow u \leftarrow \{0,1\} \uparrow O(n \cdot \log n), \ y \leftarrow f \downarrow u (U \downarrow n) [A(u,y) \in f \downarrow u \uparrow \uparrow \uparrow -1(y)] = \text{negl}(n) \)

Proof adapted from [YGLW15]

Almost-regularity:

\( \forall B > 0: \Pr \downarrow u \leftarrow U, \ x \leftarrow \{0,1\} \uparrow n [2 \uparrow \max /B < |f \downarrow u \uparrow \uparrow \uparrow -1(f \downarrow u(x))| < 2 \uparrow \max \cdot B] = 1 - O(1)/B - \text{negl}(n) \)
Open problem

How to construct UOWHFs with key and output $o(n^{17})$ from any one-way function?

• The currently best [HHRVW10]-UOWHF is dual to the PRG (from any OWF) by [HILL99,Holenstein06].

• However, PRGs have been significantly improved recently ([HRV10,VZ12]) via “next-bit pseudoentropy”.

• Can more efficiently UOWHFs be constructed in a symmetric fashion to [HRV10,VZ12]?
Thank you!