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

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

[1]Shanghai Jiao Tong University, China

[2]East China Normal University, China

[3]Jinan University, China

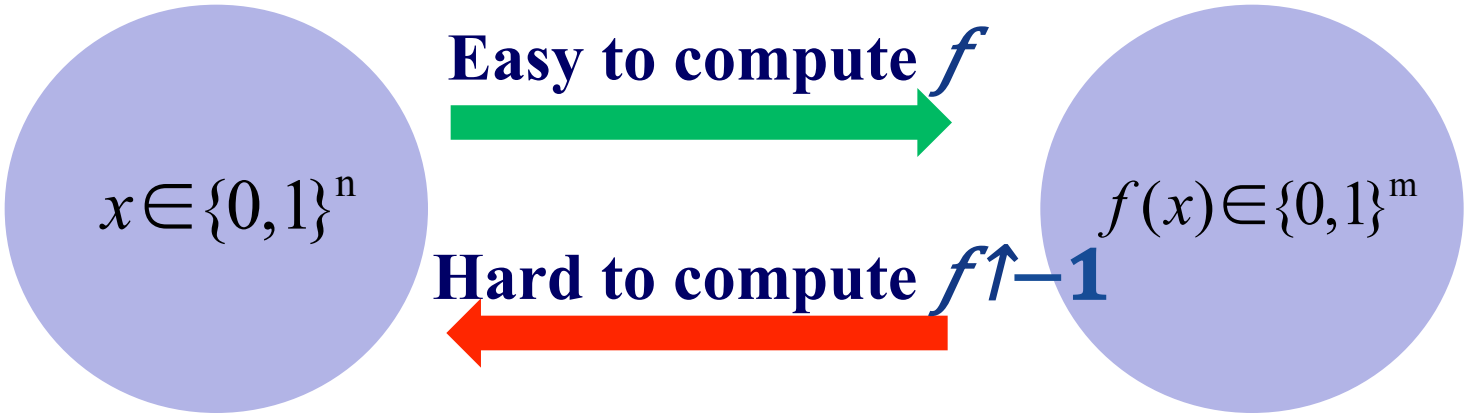
October 1, 2015

电子信息与电气工程学院
School of Electronic ,Information and Electrical Engineering

密码与计算机安全实验室
Lab of Cryptology and Computer Security

One-way Functions

$f:\{0,1\}^n \to \{0,1\}^m$ **is a one-way function if**



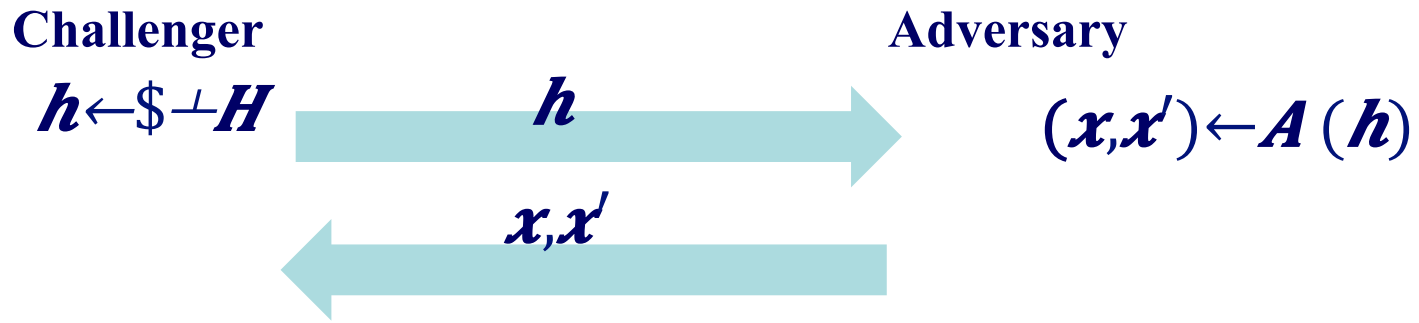
$\forall PPT\ A$: $\Pr[x \leftarrow U_n]$

$[f(A(f(x)))=f(x)]=\text{negl}(n)$

Simplifying assumption: m=n.

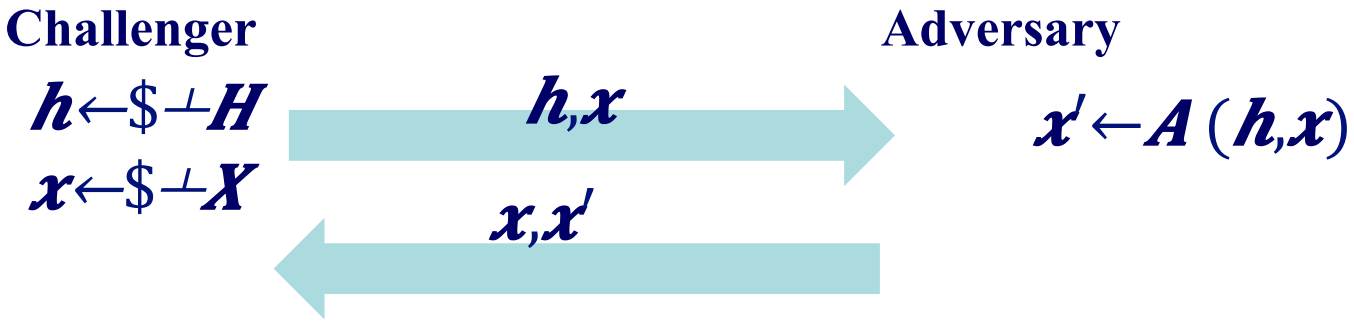
(Target) Collision Resistance

- **Collision Resistance (CR)**



$\mathbf{CR}\downarrow A,H$ outputs 1 iff $x \neq x' \wedge h(x)=h(x')$

- **Target Collision Resistance (TCR)**



$\mathbf{TCR}\downarrow A,H$ outputs 1 iff $x \neq x' \wedge h(x)=h(x')$

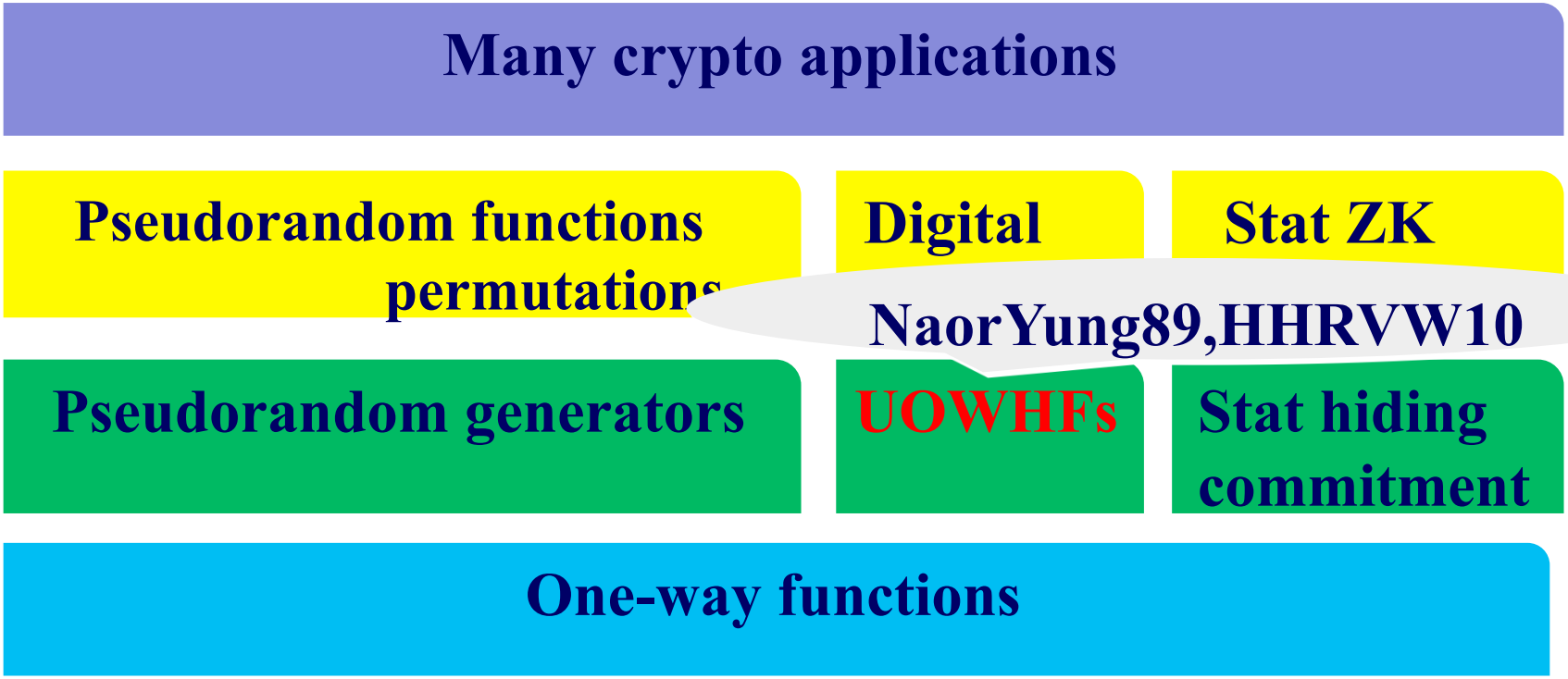
CRHFs vs. UOWHFs

- ***H*** **is a family of Collision Resistant Hash Functions (CRHFs) if** $\forall \text{PPT } A: \Pr[\mathbf{CR}\downarrow_{A,H}(1\uparrow^n)=1]=negl(n)$
- ***H*** **is a family of Universal One-Way Hash Functions (UOWHFs) if** $\forall \text{PPT } A: \Pr[\mathbf{TCR}\downarrow_{A,H}(1\uparrow^n)=1]=negl(n)$
- **Note: *H* is a family of functions (not a single one)**
- **UOWHFs are believed strictly weaker than CRH**
  - **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**

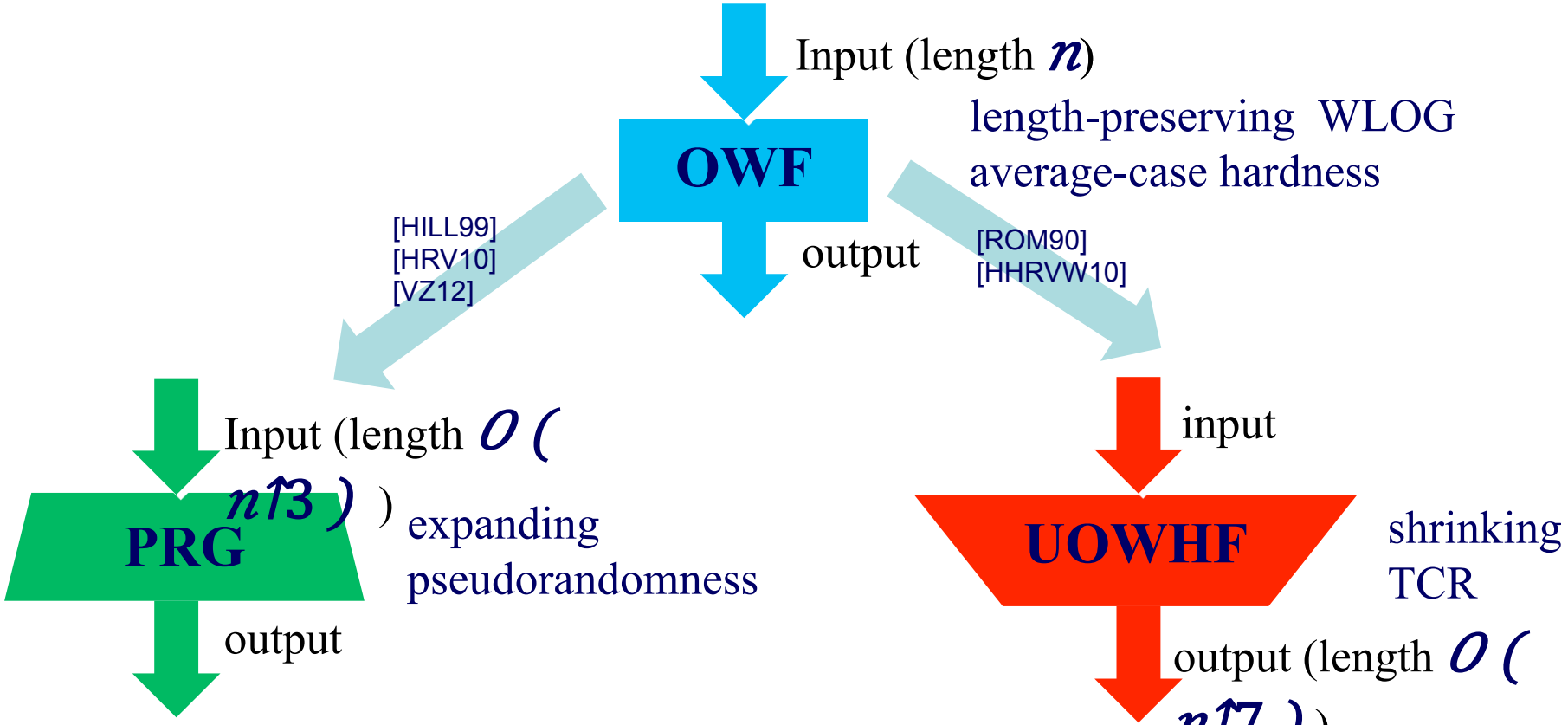
LoCCS

One-way Functions (OWFs)

A building block of many crypto applications



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

underlying primitive	black-box construction of UOWHFs			
	Work	Output length	Key length	# of calls
one-way permutation	[NY89]	$\Theta(n)$	$\Theta(n)$	1
1-to-1 one-way function	[NY89]	$\Theta(n)$	$O(n\cdot\omega(\log n))$	1
	[DY90]	$\Theta(n)$	$\Theta(n)$	1
known-regular one-way function	[Rom90]	$\Theta(n)$	$O(n\cdot\omega(\log^{\uparrow 2} n))$	$O(\omega(\log n))$ adaptive
	[BM12]	$O(n\cdot\omega(\log n))$	$O(n\cdot\omega(\log n))$	$O(\omega(\log n))$
	Our work	$O(n\cdot\omega(1))$	$O(n\cdot\omega(1))$	$O(n\cdot\omega(1))$
+ known hardness	Our work	$\Theta(n)$	$\Theta(n)$	1
unknown-regular one-way function	[AGV12]	$\Theta(n)$	$O(n\cdot\log n)$	$O(n)$
weakly-regular	Our	$\Theta(n)$	$O(n\cdot\log n)$	$n^{\uparrow O(1)}$

(arguably) more close to arbitrary one-way functions

Universal Hashing

- **Universal hash functions: H:{** $h:\{0,1\}^n \to \{0,1\}^m$ **}** ($n \geq m$

is universal if $\forall x_1 \neq x_2 : \Pr_{h \leftarrow H}[h(x_1) = h(x_2)] \leq 2^{-}$

- **E.g., H:{** $h_a:\{0,1\}^n \to \{0,1\}^m$, $h_a(x) = trunc(a \cdot x)$, a, h 2^n **)}**

trunc: $\{0,1\}^n \to \{0,1\}^m$ **outputs only the first m bits**

- **Well-known hashing properties (informal):**
  - **(leftover hash lemma, unconditional indistinguishability**

  For any $X \in \{0,1\}^n$ **with** $H_\infty(X) \geq m + d$**, we have** $h(X)$ **is** $2^{-\Omega}$ **close to uniform (conditioned on a random** $h \leftarrow H$**).**
  - **(injective hash lemma, unconditional TCR):**

  Definition: Max-entropy of X**, denoted by** $H_0(X) := \log|\mathrm{Supp}(X)|$

OWPs → UOWHFs [NY89]

- **Assumption:** (t,ε)**-one-way permutation** $f:\{0,1\}\uparrow n \to \{0,1\}\uparrow n$
- **Tool: universal** H**:** $\{\ h:\{0,1\}\uparrow n \to \{0,1\}\uparrow n\ \}$

  truncating function $trunc$

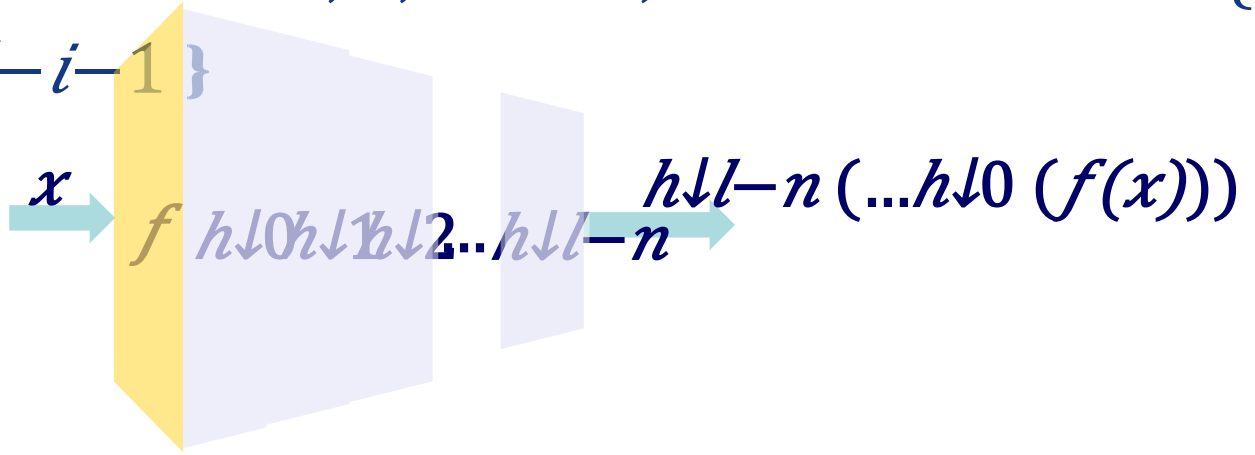
- **Statement:** G**:** $\{\ trunc \circ h \circ f \mid h \in H\}$**is a family of**

  $(t-n\uparrow O(1)\ ,\ 2\uparrow s\cdot\varepsilon)$**-universal one-way hash functions.**

Reduction didn't generalize to 1-to-1 one-way functions

1-to-1 OWFs → UOWHFs [NY89,DY90]

- **Assumption:** (t,ε)-**1-to-1 OWF** $f:\{0,1\}^n \to \{0,1\}^l$ $(l>n)$
- **Tool:universal** $H_0, \ldots, H_{l-n}$, *where* H_i **:{** $h_i:\{0,1\}^{l-i} \to \{0,1\}^{l-i-1}$ **}**



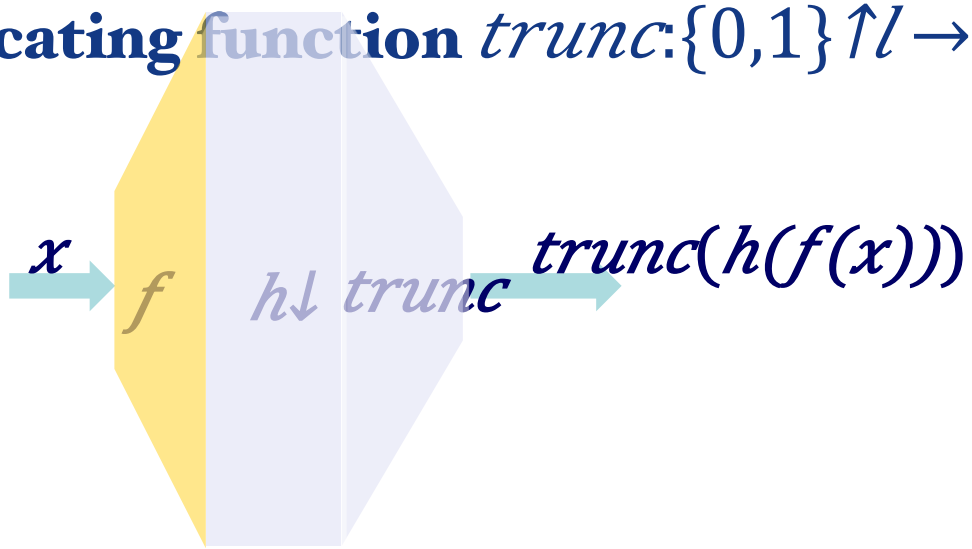
- **Statement:** G**:{**$h_{l-n} \circ \cdots \circ h_1 \circ h_0 \circ f \mid h_0 \in H_0, \cdots, h_{l-n} \in H_{l-n}$**}**

is a family of $(t-n^2 O(1), O(\varepsilon))$-**UOWHFs.**

Construction #1: 1-to-1 OWFs → UOWHFs

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

  truncating function $trunc:\{0,1\}^l \to \{0,1\}^{n-s}$



- **Statement:** $G:\{trunc \circ h \circ f \mid h \in H\}$ **is a family of**

  $(t-n^{O(1)}, 2^{s+1}\ \varepsilon)$-**UOWHFs.**

Construction #1: proof sketch

The fraction of $\{f(x)\}$ in $\{0,1\}^l$

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

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

Need to show this

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

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

- **Proof sketch.**

$Inv^A(y^*)$ **works as follows:**

1. **Sample** $y^* \leftarrow \{0,1\}^l$, $x \leftarrow \{0,1\}^n$, $h \leftarrow \{h: h(f(x)) \oplus h($ $y^*)=0\ldots0 \|_{n-s} x \leftarrow \{0,1\}^{l-n+s}\}$

Construction #1: proof sketch (cont'd)

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

1. **Sample** $y^{\dagger *} \leftarrow \{0,1\}^{\dagger l}$, $x \leftarrow \{0,1\}^{\dagger n}$, $^{\dagger} h \leftarrow \{ h: h(f(x)) \oplus h(y^{\dagger *}) = \tilde{0} \cdots 0 \perp n-s \tilde{v} \leftarrow \{0,1\}^{\downarrow \dagger l-n+s \downarrow} \perp l-n+s$

(assume WLOG $f(x) \neq y^{\dagger *}$ **)**

Claim: above sampling is equivalent to $(x,h,v) \leftarrow \{0,1\}^{\dagger n} \times H \times \{0,1\}^{\downarrow \dagger l-n+s}$

then determine $y^{\dagger *}$ **from** (x,h,v)

2. **Invoke** $x' \leftarrow A(x,h)$ **and returns** x'.

$\Pr[Inv^{\dagger}A(y^{\dagger *}) = 1] \geq 2^{\dagger} s \varepsilon$ (by TCR) $\cdot \Pr[A \text{ outputs } x' : f(x') = y^{\dagger *}] = 2^{\dagger -(l-n+s)}$

$\geq \Pr[A \text{ outputs } x' : x^{\dagger \prime} \neq x \wedge h(f(x)) \oplus h(f(x')) = \tilde{0} \cdots 0 \perp n-s \tilde{v}$

□

Construction #2: known-regular OWFs (with known hardness) → UOWHFs

- **Assumption:** (t,ε)-**(**$2\uparrow r$ **-to-1) OWF** $f:\{0,1\}\uparrow n \to \{0,1\}\uparrow n$

  with known r **and** ε

- **Tool:universal** $H=\{h:\{0,1\}\uparrow n \to \{0,1\}\uparrow n-r-s' \}$

  $H\downarrow 1 =\{h\downarrow 1 :\{0,1\}\uparrow n \to \{0,1\}\uparrow r+s\Upsilon -s \}$

  (value of $s\Upsilon$ **to determined later)**

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

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

  2$\uparrow s\ \varepsilon$

UOWHFs.

Set $s'=(s+\log(1/\varepsilon))/2$

Construction #2: known-regular OWFs (with known hardness) → UOWHFs

- **Theorem:** $G=\{g:\{0,1\}^n \to \{0,1\}^{n-s} \mid g(x)=(h(f(x)), h_1(x))\}$

is a family of $(t-n^{O(1)}, 2^{s-s'}+2^{s'}+1, \varepsilon)$-**UOWHFs.**

- **Proof sketch.**

$\forall$ **PPT** A: $\Pr[x \leftarrow \{0,1\}^n, h \leftarrow H, h_1 \leftarrow H_1, x' \leftarrow A(x,h,h_1): x' \neq x \wedge g(x')=g(x)]$

$\leq$ $\leq 2^{-(s'-s)}$ **by hashing lemma:** $\log|f^{-1}(y)|=r, h_1(x) \in \{0,1\}^{r-(s'-s)}$

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

$\leq$

h_1

$\leq 2^{s'}+1 \cdot \varepsilon$ **by TCR (via a reduction to OWF, similar to construction #1):**

Construction #3: known-regular OWFs → UOWHFs

- **Assumption:** (t,ε)-**(**$2\uparrow r$**-to-1) OWF** f **with known** r**, unknown** ε
- $G=\{g:\{0,1\}\uparrow n\to\{0,1\}\uparrow n-s \mid g(x)=(h(f(x)),h\downarrow 1(x))\}$

with $h:\{0,1\}\uparrow n\to\{0,1\}\uparrow n-r-s\uparrow\prime$, $h\downarrow 1:\{0,1\}\uparrow n\to\{0,1\}\uparrow r+s-s$ **are**

$(t-n\uparrow O(1),2\uparrow s-s\uparrow\prime+2\uparrow s\uparrow\prime+1\ \varepsilon)$-**UOWHFs.**

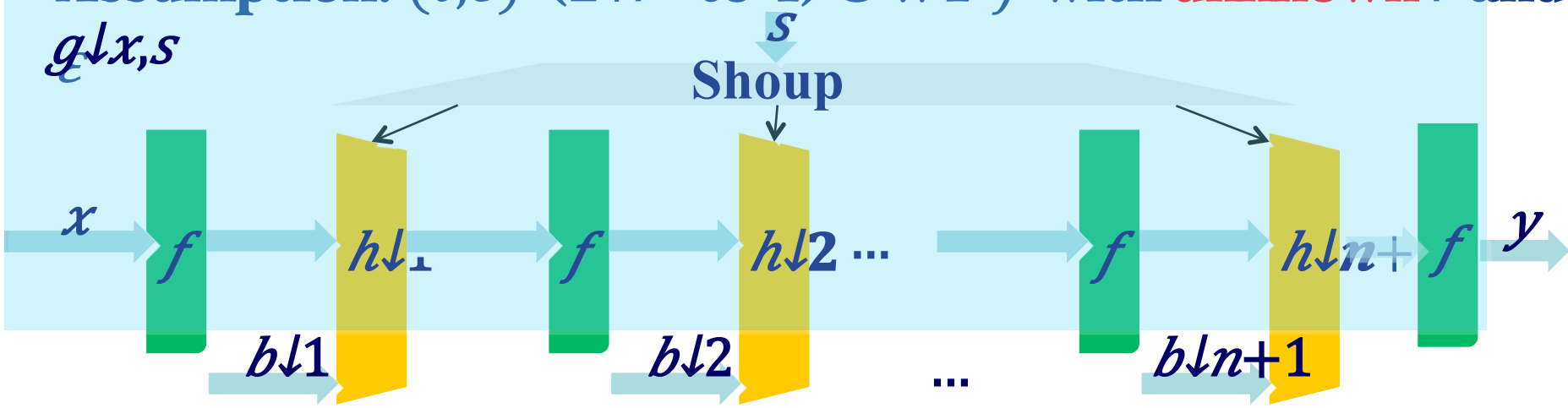
NOT work any more! (need ε **to decide** $s\uparrow\prime$ **)**

- **Remedy: Run** $q=\omega(1)$ **copies of** f**. Then** $G'=\{g:\{0,1\}\uparrow qn\to\{0,1\}\uparrow q(n-\log n) \mid g(x)=(h(f(x)),h\downarrow 1(x))\}$

where $h(f(x))=(h(f(x\downarrow 1)),\ldots,h(f(x\downarrow q)))\in\{0,1\}\uparrow q(n-r-2\log n)$

Construction by [AGV12]: unknown-regular OWFs → UOWHFs

- **Assumption:** (t,ε)-$(2\uparrow r$-**to-**$1)$ **OWF** f **with unknown** r **and** $g\downarrow x,s$



- $\{g\downarrow x,s:\{0,1\}\uparrow n+1\rightarrow\{0,1\}\uparrow n\}$ **is a family of UOWHFs keyed by** $(x,s)\in\{0,1\}\uparrow O(\mathrm{n}\cdot\log n)$ **with input** $b\downarrow 1\ldots b\downarrow n+1$ **,output** $y\in\{0,1\}\uparrow n$ **.**
- **Parameters: Output length** $O(n)$**, key length** $O(n\log n)$**.**

WEAKLY REGULAR OWFs [YGLW15]

- $f:\{0,1\}^{\uparrow}n \to Y_{\downarrow}1 \cup Y_{\downarrow}2 \cup \cdots \cup Y_{\downarrow}n$ ($Y_{\downarrow}j \stackrel{\text{def}}{=} \{y: 2^{\uparrow}j-1 \le |f^{\uparrow}-1(y)| < 2^{\uparrow}j\}$)

[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):** $\exists c \ge 0, \exists \max$:

$\Pr[f(U_{\downarrow}n) \in Y_{\downarrow}\max] \ge n^{\uparrow}-c$ & $\Pr[f(U_{\downarrow}n) \in (Y_{\downarrow}\max+1 \cup Y_{\downarrow}\max+2 \cup \cdots \cup Y_{\downarrow}n)] = 0$

Construction #4: weakly-regular OWFs → UOWHFs

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

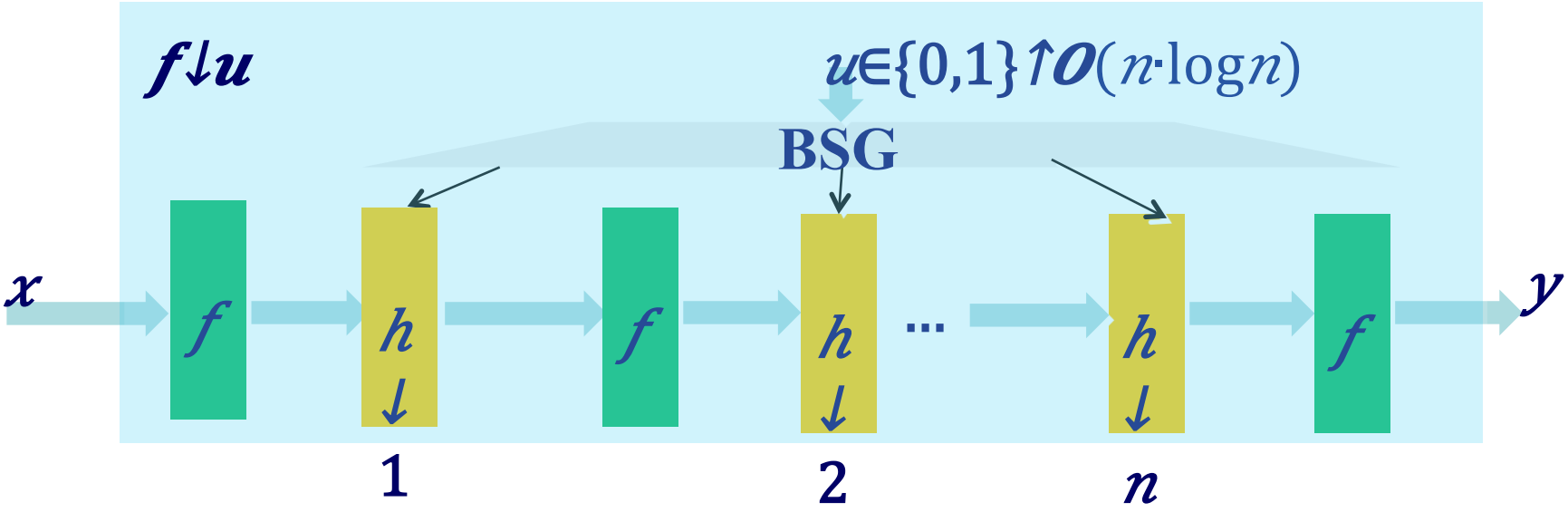
Construction:

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

Parameters:

- **key length** $O(n \cdot \log n)$
- **output length** $O(n)$
- $n^{O(1)}$ **OWF calls**

Constructing almost-regular one-way functions from weakly one-way functions



One-wayness: $\forall \text{PPT } A: \Pr[u \leftarrow \{0,1\}^{O(n \cdot \log n)}, y \leftarrow f_u(U_n)][A(u,y) \in f_u^{-1}(y)] = negl(n)$

Proof adapted from [YGLW15]

Almost-regularity:

$\forall B > 0: \Pr[u \leftarrow U, x \leftarrow \{0,1\}^n [2^{max}/B < |f_u^{-1}(f_u(x))| < 2^{max} \cdot B]] = 1 - O(1)/B - negl(n)$

Open problem

How to construct UOWHFs with key and output $o(n)$ 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!