# On Derandomizing Yao's Weak-to-Strong OWF Construction

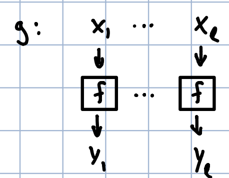
Chris Brzuska[1], Geoffroy Couteau[2], Pihla Karanko[1], and Felix Rohrbach[3]

[1] Aalto University, Finland, {chris.brzuska,pihla.karanko}@aalto.fi
[2] IRIF, CNRS, France, geoffroy.couteau@ens.fr
[3] TU Darmstadt, Germany, felix.rohrbach@cryptoplexity.de

**Thm (Yao):** if $f$ is a $p$-weak OWF
then $g(x_1 \| \ldots \| x_\ell) := f(x_1) \| \ldots \| f(x_\ell)$ is strong OWF
if $\ell \geq |x_i| \cdot p(|x_i|)$

# On Derandomizing Yao's Weak-to-Strong OWF Construction

**Yao:**




**Def:**
$f$ is a $p$-weak OWF if
$\forall$ PPT $\mathcal{A}$

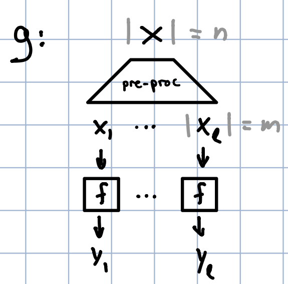
$$\Pr_{x \leftarrow \{0,1\}^n}\left[\mathcal{A}(f(x)) \in f^{-1}(f(x))\right] \leq 1 - \frac{1}{p(n)}$$

poly

**Def:**
$g$ is (strong) OWF if
$\forall$ PPT $\mathcal{A}$

$$\Pr\left[\mathcal{A}(g(x)) \in g^{-1}(g(x))\right] = \text{negl}(n)$$

Is it possible to have $\underbrace{\text{shorter input}}_{\text{i.e. use less randomness}}$?




in particular, $n = cm$ would be nice

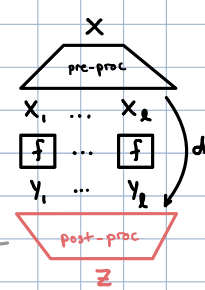
**Answer:** no :(

$\nexists$ pre-proc with $n \leq c \cdot p(m)$ i.e.
you cannot $\underbrace{\text{prove}}_{\text{blackbox, relativizing}}$ that $g_{\text{pre-proc}}$ is a strong OWF

**Open still:**

- Non-adaptive, compressing post-proc?

e.g. XOR




same neg. result holds for any almost-inj. post-proc.

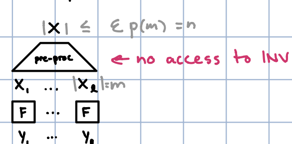
**proof (sketch):**

oracles:

PSPACE
$F$ = random permutation
INV = inverts $\underbrace{\text{random subset}}_{|\text{EASY}| = \left(1 - \frac{1}{p(m)}\right)2^m}$ of $F(\{0,1\}^m)$

Now $F$ is (almost) $p$-weak OWF.

All $g$:




can be inverted with non-negl. prob.

obs 1: if $\ell \leq p(m)$ then

$$\Pr_{F,x}\left[\text{all } y_i \in \text{EASY}\right] \geq \left(1 - \tfrac{1}{p}\right)^p \geq \tfrac{1}{4}$$

$\to e^{-1}$

$\Rightarrow$ WLOG: assume $\ell > p(m)$

obs 2: w.h.p. $\left(1 - \frac{1}{p}\right)$ fraction of $y_i$'s are easy

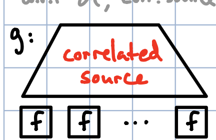
obs 3 (main): the remaining hard $x_i$'s have little entropy left

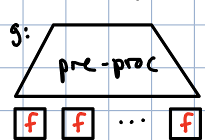
more precisely

$$\mathop{\mathbb{E}}_{\pi}\left[\mathop{H}_{x}\left(x_{\pi(1)}, \ldots, x_{\pi(\frac{1}{p}\cdot\ell)} \,\middle|\, x_{\pi(\frac{1}{p}\ell+1)}, \ldots, x_{\pi(\ell)}\right)\right] \leq \frac{n}{p(m)} = \frac{\varepsilon \cdot p(m)}{p(m)} = \varepsilon$$

$\rotatebox{90}{$\leq$}$
$H_\infty \Rightarrow$ easy to guess $x_{\pi(1)}, \ldots, x_{\pi(\frac{1}{p}\cdot\ell)}$

| Wichs 13 | Our paper |
|---|---|
| rules out BB-proofs w.r.t $\mathcal{A}$, corr. source | rules out BB-proofs w.r.t $\mathcal{A}$, $f$ |
| g: correlated source; f f ... f | g: pre-proc; f f ... f |
| $\exists$ corr. source $\forall f$ | $\exists f$ $\forall$ pre-proc |

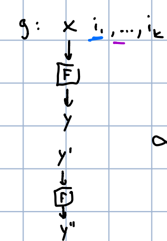


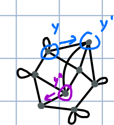




- Adaptive $g$?

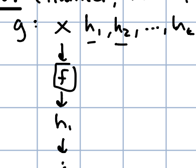
**Thm** (Goldreich, Impagliazzo, Levin, Venkatesan, Zuckerman)

if $f$ is regular, then $\exists$ short-input $g$




**Thm** (Haitner, Harnik, Reingold)



proof:

$$\underbrace{\overbrace{X_{\pi(1)}, \dots, X_{\pi(\frac{1}{p}\cdot \ell)}}^{=: B_1^\pi}}_{\text{block of size } \frac{\ell}{p}}, \overbrace{X_{\pi(\frac{\ell}{p}+1)}, \dots,}^{B_2^\pi} X_{\pi(\ell)}$$

$p$ blocks: $B_1^\pi, \dots, B_p^\pi$

$$\sum_{j=1}^{p} \mathbb{E}_\pi \left[ H(B_j^\pi \mid B_{j+1}^\pi, \dots, B_p^\pi) \right]$$

$$= \mathbb{E}_\pi \Big[ \underbrace{\sum_{j=1}^{p} H(B_j^\pi \mid B_{j+1}^\pi, \dots, B_p^\pi)}_{\overset{\text{chain rule}}{=} H(B_1^\pi, \dots, B_p^\pi) \leq H(X) = n} \Big]$$

$$\Downarrow$$

$$n \geq \sum_{j=1}^{p} \mathbb{E}_\pi \left[ H(B_j^\pi \mid B_{j+1}^\pi, \dots, B_p^\pi) \right]$$

$$\geq \sum \underbrace{\mathbb{E}_\pi \left[ H(B_j^\pi \mid B_1^\pi, \dots, B_{j-1}^\pi, B_{j+1}^\pi, \dots, B_p^\pi) \right]}_{\mathbb{E}_{\pi'} \left[ H(B_1^{\pi'} \mid B_2^{\pi'}, \dots, B_p^{\pi'}) \right]}$$

$$= p \cdot \mathbb{E}_{\pi'} \left[ H(B_1^{\pi'} \mid B_2^{\pi'}, \dots, B_p^{\pi'}) \right] \qquad \square$$