# Lecture 6: Pseudorandomness

# Outline Construction: PRG from OWF

- OWF

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG
- OWP $\implies$ Hardcore Predicate for OWP $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG
- OWP $\implies$ Hardcore Predicate for OWP $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG
- OWP $\implies$ Hardcore Predicate for OWP $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG
- OWP $\implies$ Hardcore Predicate for OWP $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG
- Today's Goals:

# Outline Construction: PRG from OWF

- OWF $\implies$ Hardcore Predicate for OWF $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG
- OWP $\implies$ Hardcore Predicate for OWP $\implies$ One-bit extension PRG $\implies$ Poly-stretch PRG
- Today's Goals: "OWF $\implies$ Hardcore Predicate"

# Outline Construction: PRG from OWF

- OWF $\Longrightarrow$ Hardcore Predicate for OWF $\Longrightarrow$ One-bit extension PRG $\Longrightarrow$ Poly-stretch PRG
- OWP $\Longrightarrow$ Hardcore Predicate for OWP $\Longrightarrow$ One-bit extension PRG $\Longrightarrow$ Poly-stretch PRG
- Today's Goals: "OWF $\Longrightarrow$ Hardcore Predicate" and "One-bit extension PRG $\Longrightarrow$ Poly-stretch PRG"

First Construction

- Let $G(s)$ be a one-bit extension PRG

First Construction

- Let $G(s)$ be a one-bit extension PRG
- Then: $P(s) := \overbrace{G(G(\cdots G}^{m\text{-times}}(s)\cdots))$ is an arbitrary stretch PRG

First Construction

- Let $G(s)$ be a one-bit extension PRG
- Then: $P(s) := \overbrace{G(G(\cdots G}^{m\text{-times}}(s)\cdots))$ is an arbitrary stretch PRG
- Proof?

Second Construction

- Let $G(s)$ be a one-bit extension PRG

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s) \| b(s)$, where $|G(\cdot)| = |H(\cdot)|$

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s) \| b(s)$, where $|G(\cdot)| = |H(\cdot)|$
- $b_1 = b(s)$

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s) \| b(s)$, where $|G(\cdot)| = |H(\cdot)|$
- $b_1 = b(s)$
- $b_2 = b(H(s))$

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s) \| b(s)$, where $|G(\cdot)| = |H(\cdot)|$
- $b_1 = b(s)$
- $b_2 = b(H(s))$
- $b_3 = b(H(H(s)))$

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s) \| b(s)$, where $|G(\cdot)| = |H(\cdot)|$
- $b_1 = b(s)$
- $b_2 = b(H(s))$
- $b_3 = b(H(H(s)))$
- $b_i = b(\overbrace{H(\cdots H}^{(i-1)\text{-times}}(s)))$

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s) \| b(s)$, where $|G(\cdot)| = |H(\cdot)|$
- $b_1 = b(s)$
- $b_2 = b(H(s))$
- $b_3 = b(H(H(s)))$
- $b_i = b(\overbrace{H(\cdots H}^{(i-1)\text{-times}}(s)))$
- Then: $P(s) := b_1 \ldots b_m$ is the PRG

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s) \| b(s)$, where $|G(\cdot)| = |H(\cdot)|$
- $b_1 = b(s)$
- $b_2 = b(H(s))$
- $b_3 = b(H(H(s)))$
- $b_i = b(\overbrace{H(\cdots H}^{(i-1)\text{-times}}(s)))$
- Then: $P(s) := b_1 \ldots b_m$ is the PRG
- Proof?

Second Construction

- Let $G(s)$ be a one-bit extension PRG
- Let $G(s) = H(s)\|b(s)$, where $|G(\cdot)| = |H(\cdot)|$
- $b_1 = b(s)$
- $b_2 = b(H(s))$
- $b_3 = b(H(H(s)))$
- $b_i = b(\overbrace{H(\cdots H}^{(i-1)\text{-times}}(s)))$
- Then: $P(s) := b_1 \ldots b_m$ is the PRG
- Proof?
- Think: Which one is preferable?

**Theorem (Hardcore Predicate)**

*If $f\colon \{0,1\}^n \to \{0,1\}^n$ is a OWF (OWP) then*

**Theorem (Hardcore Predicate)**

*If $f\colon \{0,1\}^n \to \{0,1\}^n$ is a OWF (OWP) then*

- *The function $g\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined by $g(x,r) := (\ f(x), r\ )$ is also a OWF (OWP).*

**Theorem (Hardcore Predicate)**

*If $f : \{0,1\}^n \to \{0,1\}^n$ is a OWF (OWP) then*

- *The function $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined by $g(x,r) := (\ f(x), r\ )$ is also a OWF (OWP).*
- *And $h(x,r) := \langle x, r\rangle$ is a hardcore predicate for $g(x,r)$.*

# Warmup Proof (1)

- Given $g(x, r) = (f(x), r)$, the adversary $\mathcal{A}$, always correctly outputs $h(x, r)$

# Warmup Proof (1)

- Given $g(x,r) = (f(x), r)$, the adversary $\mathcal{A}$, always correctly outputs $h(x,r)$
- Use $\mathcal{A}(f(x), e_i)$ to obtain $x_i$, for all $1 \leqslant i \leqslant n$ and

$$e_i = (\overbrace{0,\ldots,0}^{(i-1)\text{-times}}, 1, \ldots, 0)$$

# Warmup Proof (2)

- Given $g(x, r) = (f(x), r)$, the adversary $\mathcal{A}$ computes $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of $(x, r)$)

# Warmup Proof (2)

- Given $g(x, r) = (f(x), r)$, the adversary $\mathcal{A}$ computes $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of $(x, r)$)
- Let,

$$S := \left\{ x \colon \Pr[r \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(f(x), r) = h(x, r)] \geqslant \frac{3}{4} + \frac{\varepsilon(n)}{2} \right\}$$

# Warmup Proof (2)

- Given $g(x, r) = (f(x), r)$, the adversary $\mathcal{A}$ computes $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of $(x, r)$)
- Let,

$$S := \left\{ x \colon \Pr[r \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(f(x), r) = h(x, r)] \geqslant \frac{3}{4} + \frac{\varepsilon(n)}{2} \right\}$$

- Then, $|S| / 2^n \geqslant \varepsilon(n)/2$ (Markov Inequality)

# Warmup Proof (2)

- Given $g(x,r) = (f(x), r)$, the adversary $\mathcal{A}$ computes $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of $(x,r)$)
- Let,

$$S := \left\{ x \colon \Pr[r \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(f(x), r) = h(x,r)] \geqslant \frac{3}{4} + \frac{\varepsilon(n)}{2} \right\}$$

- Then, $|S|/2^n \geqslant \varepsilon(n)/2$ (Markov Inequality)
- Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$

# Warmup Proof (2)

- Given $g(x, r) = (f(x), r)$, the adversary $\mathcal{A}$ computes $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of $(x, r)$)
- Let,

$$S := \left\{ x \colon \Pr[r \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(f(x), r) = h(x, r)] \geqslant \frac{3}{4} + \frac{\varepsilon(n)}{2} \right\}$$

- Then, $|S|/2^n \geqslant \varepsilon(n)/2$ (Markov Inequality)
- Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$
- Compute $c := a \oplus b$

# Warmup Proof (2)

- Given $g(x,r) = (f(x), r)$, the adversary $\mathcal{A}$ computes $h(x,r)$ with probability $3/4 + \varepsilon(n)$ (over choices of $(x,r)$)
- Let,

$$S := \left\{ x\colon \Pr[r \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(f(x), r) = h(x,r)] \geqslant \frac{3}{4} + \frac{\varepsilon(n)}{2} \right\}$$

- Then, $|S|/2^n \geqslant \varepsilon(n)/2$ (Markov Inequality)
- Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$
- Compute $c := a \oplus b$
- The bit $c$ is correct (i.e. $c = x_i$) with probability $\frac{1}{2} + \varepsilon$ (Union Bound)

# Warmup Proof (2)

- Given $g(x, r) = (f(x), r)$, the adversary $\mathcal{A}$ computes $h(x, r)$ with probability $3/4 + \varepsilon(n)$ (over choices of $(x, r)$)
- Let,

$$S := \left\{ x \colon \Pr[r \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(f(x), r) = h(x, r)] \geqslant \frac{3}{4} + \frac{\varepsilon(n)}{2} \right\}$$

- Then, $|S| / 2^n \geqslant \varepsilon(n)/2$ (Markov Inequality)
- Let $a := \mathcal{A}(f(x), e_i + r)$ and $b := \mathcal{A}(f(x), r)$, for $r \xleftarrow{\$} \{0,1\}^n$
- Compute $c := a \oplus b$
- The bit $c$ is correct (i.e. $c = x_i$) with probability $\frac{1}{2} + \varepsilon$ (Union Bound)
- Repeat and take majority to correctly obtain $x_i$ with $(1 - \mathrm{negl}(n))$ probability

# Full Proof

Homework!

# Concluding Remarks

- OWF $\implies$ PRG: [Impagliazzo-Levin-Luby-89] and [Hastad-90]

# Concluding Remarks

- OWF $\implies$ PRG: [Impagliazzo-Levin-Luby-89] and [Hastad-90]
- More Efficient Constructions: [Vadhan-Zheng-12]

# Concluding Remarks

- OWF $\implies$ PRG: [Impagliazzo-Levin-Luby-89] and [Hastad-90]
- More Efficient Constructions: [Vadhan-Zheng-12]
- Computational analogues of Entropy

# Concluding Remarks

- OWF $\implies$ PRG: [Impagliazzo-Levin-Luby-89] and [Hastad-90]
- More Efficient Constructions: [Vadhan-Zheng-12]
- Computational analogues of Entropy
- Non-cryptographic PRGs and Derandomization: [Nisan-Wigderson-88]

# Concluding Remarks

- OWF $\implies$ PRG: [Impagliazzo-Levin-Luby-89] and [Hastad-90]
- More Efficient Constructions: [Vadhan-Zheng-12]
- Computational analogues of Entropy
- Non-cryptographic PRGs and Derandomization: [Nisan-Wigderson-88]
- Non-boolean PRGs: [Dubrov-Ishai-06] and [Artemenko-Shaltiel-14]