Lecture 5: Pseudorandomness

Recall

- Computational Indistinguishability

Recall

- Computational Indistinguishability
  - All n.u. PPT D can distinguish $\{X_n\}$ from $\{Y_n\}$ only with negligible probability

Recall

- Computational Indistinguishability
  - All n.u. PPT D can distinguish $\{X_n\}$ from $\{Y_n\}$ only with negligible probability
- "Data Processing Inequality" (in crypto setting)

Recall

- Computational Indistinguishability
  - All n.u. PPT D can distinguish $\{X_n\}$ from $\{Y_n\}$ only with negligible probability
- "Data Processing Inequality" (in crypto setting)
  - Efficient processing cannot help distinguish computationally indistinguishable distributions

Recall

- Computational Indistinguishability
  - All n.u. PPT D can distinguish $\{X_n\}$ from $\{Y_n\}$ only with negligible probability
- "Data Processing Inequality" (in crypto setting)
  - Efficient processing cannot help distinguish computationally indistinguishable distributions
- Hybrid Lemma

Recall

- Computational Indistinguishability
  - All n.u. PPT D can distinguish $\{X_n\}$ from $\{Y_n\}$ only with negligible probability
- "Data Processing Inequality" (in crypto setting)
  - Efficient processing cannot help distinguish computationally indistinguishable distributions
- Hybrid Lemma
  - If the first and last hybrid is computationally distinguishable then at least a pair of consecutive hybrids are computationally distinguishable

Pseudorandom Generators

Definition (Pseudorandom Generator)

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

Definition (Pseudorandom Generator)

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

1. Impossible unconditionally (needs computational indistinguishability)

Pseudorandom Generators

Definition (Pseudorandom Generator)

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

1. Impossible unconditionally (needs computational indistinguishability)
2. Think: *Non-boolean* PRGs?

Pseudorandom Generators

Definition (Pseudorandom Generator)

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

1. Impossible unconditionally (needs computational indistinguishability)
2. Think: *Non-boolean* PRGs?
3. Think: How do we test indistinguishability against *all computational tests*?

Next-bit Unpredictability

Next-bit Unpredictability

Definition (Next-bit Unpredictability)

An ensemble of distributions $\{X_n\}$ over $\{0,1\}^{\ell(n)}$ is next-bit unpredictable if, for all $0 \leqslant i < \ell(n)$ and n.u. PPT A there exists negligible $\nu(\cdot)$ such that:

$$\Pr[t_1 \dots t_{\ell(n)} \sim X_n \colon A(t_1 \dots t_i) = t_{i+1}] \leqslant \frac{1}{2} + \nu(n)$$

Next-bit Unpredictability

Definition (Next-bit Unpredictability)

An ensemble of distributions $\{X_n\}$ over $\{0,1\}^{\ell(n)}$ is next-bit unpredictable if, for all $0 \leqslant i < \ell(n)$ and n.u. PPT A there exists negligible $\nu(\cdot)$ such that:

$$\Pr[t_1 \ldots t_{\ell(n)} \sim X_n \colon A(t_1 \ldots t_i) = t_{i+1}] \leqslant \frac{1}{2} + \nu(n)$$

- If $\{X_n\}$ is next-bit unpredictable then $\{X_n\}$ is pseudorandom

$$H_n^{(i)} := \left\{x \sim X_n, u \sim U_{\ell(n)} : x_1 \ldots x_i u_{i+1} \ldots u_{\ell(n)}\right\}$$

Next-bit unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \sim X_n, u \sim U_{\ell(n)} : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- Suppose this distribution is next-bit unpredictable

$$H_n^{(i)} := \left\{ x \sim X_n, u \sim U_{\ell(n)} : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)} \right\}$$

- Suppose this distribution is next-bit unpredictable
- If possible let this distribution not be pseudorandom

Next-bit unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \sim X_n, u \sim U_{\ell(n)} : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- Suppose this distribution is next-bit unpredictable
- If possible let this distribution not be pseudorandom
- $H_n^{(0)}$ is the uniform distribution

Next-bit unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{ x \sim X_n, u \sim U_{\ell(n)} : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)} \right\}$$

- Suppose this distribution is next-bit unpredictable
- If possible let this distribution not be pseudorandom
- $H_n^{(0)}$ is the uniform distribution
- $H_n^{(\ell(n))}$ is the distribution X_n

Next-bit unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{ x \sim X_n, u \sim U_{\ell(n)} \colon x_1 \dots x_i u_{i+1} \dots u_{\ell(n)} \right\}$$

- Suppose this distribution is next-bit unpredictable
- If possible let this distribution not be pseudorandom
- $H_n^{(0)}$ is the uniform distribution
- $H_n^{(\ell(n))}$ is the distribution X_n
- If $H_n^{(0)}$ and $H_n^{(\ell(n))}$ are distinguishable then there exists $0 \leqslant i < \ell(n)$ such that $H_n^{(i)}$ and $H_n^{(i+1)}$ are distinguishable

Next-bit unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{ x \sim X_n, u \sim U_{\ell(n)} \colon x_1 \dots x_i u_{i+1} \dots u_{\ell(n)} \right\}$$

- Suppose this distribution is next-bit unpredictable
- If possible let this distribution not be pseudorandom
- $H_n^{(0)}$ is the uniform distribution
- $H_n^{(\ell(n))}$ is the distribution X_n
- If $H_n^{(0)}$ and $H_n^{(\ell(n))}$ are distinguishable then there exists $0 \leqslant i < \ell(n)$ such that $H_n^{(i)}$ and $H_n^{(i+1)}$ are distinguishable
- Now next bit unpredictability is violated

Next-bit unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{ x \sim X_n, u \sim U_{\ell(n)} \colon x_1 \dots x_i u_{i+1} \dots u_{\ell(n)} \right\}$$

- Suppose this distribution is next-bit unpredictable
- If possible let this distribution not be pseudorandom
- $H_n^{(0)}$ is the uniform distribution
- $H_n^{(\ell(n))}$ is the distribution X_n
- If $H_n^{(0)}$ and $H_n^{(\ell(n))}$ are distinguishable then there exists $0 \leqslant i < \ell(n)$ such that $H_n^{(i)}$ and $H_n^{(i+1)}$ are distinguishable
- Now next bit unpredictability is violated
- Think: Where did we use "n.u."-ity in the adversary construction?

Hardcore Predicate

- Hardcore Predicate suffices to construct PRG

Hardcore Predicate

- Hardcore Predicate suffices to construct PRG
- $h(x)$ is hard to predict even if $f(x)$ is provided to the adversary

Hardcore Predicate

- Hardcore Predicate suffices to construct PRG
- $h(x)$ is hard to predict even if $f(x)$ is provided to the adversary

Hardcore Predicate

- Hardcore Predicate suffices to construct PRG
- $h(x)$ is hard to predict even if $f(x)$ is provided to the adversary

Definition (Hardcore Predicate)

The predicate $h\colon \{0,1\}^* \to \{0,1\}$ is hardcore for $f(\cdot)$ if for all n.u. PPT A there exists a negligible function $\nu(\cdot)$ such that:

$$\Pr\left[x \xleftarrow{\$} \{0,1\}^n \colon A(1^n, f(x)) = h(x)\right] \leqslant \frac{1}{2} + \nu(n)$$

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

- Construction: $G(s) = f(s) \parallel h(s)$

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

- Construction: $G(s) = f(s) \parallel h(s)$
- Proof?