Lecture 8.2: Pseudorandom Function Construction

[Goldreich-Goldwasser-Micali-84] Construction

- Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG

[Goldreich-Goldwasser-Micali-84] Construction

- Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG
- WLOG $G(s) = (G_0(s), G_1(s))$, where $G_0, G_1 : \{0,1\}^n \to \{0,1\}^n$

[Goldreich-Goldwasser-Micali-84] Construction

- Let $G\colon \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG
- WLOG $G(s) = (G_0(s), G_1(s))$, where $G_0, G_1\colon \{0,1\}^n \to \{0,1\}^n$
- $f_s(x) := G_{x_n}(G_{x_{n-1}}(\cdots G_{x_1}(s)\cdots))$

[Goldreich-Goldwasser-Micali-84] Construction

- Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG
- WLOG $G(s) = (G_0(s), G_1(s))$, where $G_0, G_1 : \{0,1\}^n \to \{0,1\}^n$
- $f_s(x) := G_{x_n}(G_{x_{n-1}}(\cdots G_{x_1}(s)\cdots))$
- Proof: Next Lecture

[Naor-Reingold-97] Construction

- Let ℓ and p be prime numbers such that $\ell | (p-1)$

[Naor-Reingold-97] Construction

- Let ℓ and p be prime numbers such that $\ell | (p-1)$
- Let $g \in \mathbb{F}_p^*$ be a generator of order ℓ

[Naor-Reingold-97] Construction

- Let ℓ and p be prime numbers such that $\ell | (p-1)$
- Let $g \in \mathbb{F}_p^*$ be a generator of order ℓ
- $f_s(x) := g^{s_1^{x_1} \cdots s_n^{x_n}}$, for $(s_1, \ldots, s_n) \in \mathbb{F}_\ell^n$

[Naor-Reingold-97] Construction

- Let ℓ and p be prime numbers such that $\ell | (p-1)$
- Let $g \in \mathbb{F}_p^*$ be a generator of order ℓ
- $f_s(x) := g^{s_1^{x_1} \cdots s_n^{x_n}}$, for $(s_1, \ldots, s_n) \in \mathbb{F}_\ell^n$
- Proof: Read on your own

Food for Thought

- Constrained PRFs [Boneh-Waters-13]

Food for Thought

- Constrained PRFs [Boneh-Waters-13]
- PRFs with "Punctured Keys" [Sahai-Waters-14]

Food for Thought

- Constrained PRFs [Boneh-Waters-13]
- PRFs with "Punctured Keys" [Sahai-Waters-14]
- Should evaluation of $f_s(x)$ help predict $f_{s'}(x')$?

Food for Thought

- Constrained PRFs [Boneh-Waters-13]
- PRFs with "Punctured Keys" [Sahai-Waters-14]
- Should evaluation of $f_s(x)$ help predict $f_{s'}(x')$?
- Can PRFs be computed by shallow circuits? [Linial-Mansour-Nisan-94]