Lecture 9: Pseudorandom Function

Recall: GGM Construction

- Let $G(s) = (G_0(s), G_1(s))$ be a length doubling PRG

Recall: GGM Construction

- Let $G(s) = (G_0(s), G_1(s))$ be a length doubling PRG
- $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_1}(s)\cdots\right)\right)$

Security Proof: Query Complexity = 1

Security Proof: Query Complexity = 1

- H_0 has $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_1}(s)\cdots\right)\right)$

Security Proof: Query Complexity = 1

- H_0 has $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_1}(s)\cdots\right)\right)$
- H_n has $f_s(x) := U_n$

Security Proof: Query Complexity = 1

- H_0 has $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_1}(s)\cdots\right)\right)$
- H_n has $f_s(x) := U_n$
- H_1 has $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_2}(U_n)\cdots\right)\right)$

Security Proof: Query Complexity = 1

- H_0 has $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_1}(s)\cdots\right)\right)$
- H_n has $f_s(x) := U_n$
- H_1 has $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_2}(U_n)\cdots\right)\right)$
- H_i has $f_s(x) := G_{x_n}\left(G_{x_{n-1}}\left(\cdots G_{x_{i+1}}(U_n)\cdots\right)\right)$

Security Proof: General Query Complexity

- Query Complexity $= q(n)$

Security Proof: General Query Complexity

- Query Complexity $= q(n)$
- Query Complexity $\leqslant q(n)$

Security Proof: General Query Complexity

- Query Complexity $= q(n)$
- Query Complexity $\leqslant q(n)$
- Think: Expected Query Complexity $= q(n)$

Punctured PRF [Sahai-Waters-14]

- Punctured PRF: A PRF which can be evaluated at all $x \neq x^*$

Punctured PRF [Sahai-Waters-14]

- Punctured PRF: A PRF which can be evaluated at all $x \neq x^*$
- $k(x^*)$ is a key which helps evaluated the PRF at all points x other than x^*

Punctured PRF [Sahai-Waters-14]

- Punctured PRF: A PRF which can be evaluated at all $x \neq x^*$
- $k(x^*)$ is a key which helps evaluated the PRF at all points x other than x^*
- Think: Construction

Example Problem

- Design a box which answers queries with random answers

Example Problem

- Design a box which answers queries with random answers
- Think: Multi-message Encryption

Example Problem

- Design a box which answers queries with random answers
- Think: Multi-message Encryption
- Think: Difference from PRG based construction (Which one would you prefer?)