EECS 575: Advanced Cryptography
Fall 2022
Lecture 9

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Functions (PRFs)
- PRFs from length-doubling PRGs (“GGM” construction)
- Analyzing GGM

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Functions (PRFs)
- PRFs from length-doubling PRGs (“GGM” construction)
- Analyzing GGM

Announcements

- Exam 1 is online, due next Monday at 11pm EST
- HW1 grades are out

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Functions (PRFs)
- PRFs from length-doubling PRGs (“GGM” construction)
- Analyzing GGM

Pseudorandom generators

For $G : \{0,1\}^* \to \{0,1\}^*$ is PRG

if $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$

- expands its input: $|G(s)| > |s|$

  $\ell(n) \geq n+1$

- Efficient
- $\{G(U_n)\}_n \approx_c \{U_{\ell(n)}\}_n$

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Functions (PRFs)
- PRFs from length-doubling PRGs (“GGM” construction)
- Analyzing GGM

Pseudorandom Functions (PRFs)

- Oracle indistinguishability

$\Theta = \{O_n\}$ $\Theta' = \{O'_n\}$

dists over $F: \{0,1\}^n \to \{0,1\}^m$

$$Adv^{A}_{\Theta,\Theta'} = \left| \Pr_{f \leftarrow O_n}[A^f = 1] - \Pr_{f \leftarrow O'_n}[A^f = 1] \right| = negl(n)$$

$U_f = U(\{0,1\}^n \to \{0,1\}^n)$ $\Theta \approx_c U_f$

Pseudorandom Functions (PRFs)

family $F = \{F_s : \{0,1\}^n \to \{0,1\}^n\}_s$

F is PRF family

- efficient to sample s
- efficient to evaluate
- $F \approx_c U(\{0,1\}^n \to \{0,1\}^n)$

Pseudorandom Functions (PRFs)

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Functions (PRFs)
- PRFs from length-doubling PRGs (“GGM” construction)
- Analyzing GGM

GGM PRF

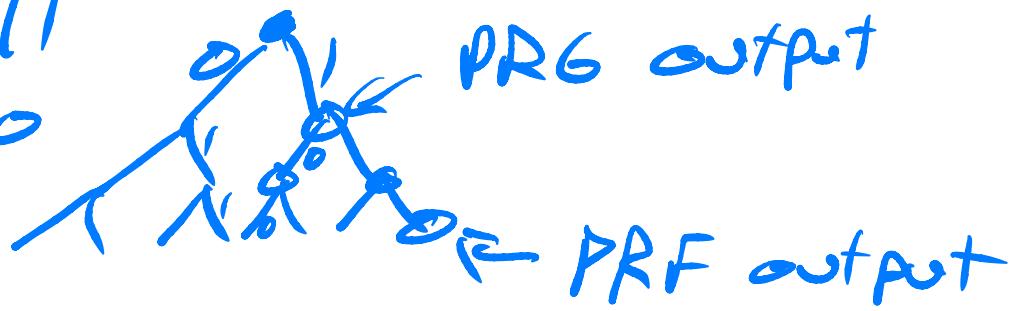
Thm: If $\exists$ length-doubling PRG, then $\exists$ PRF

G s.t. $\ell(n) = 2n$

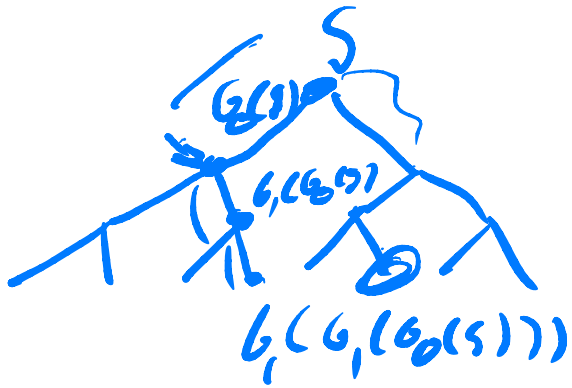
$G_0(s) = G(s)[:n]$

$G_1(s) = G(s)[n:]$

PRF inputs → 011, 100



$f_s(011)$



$f_s(x_1 \cdots x_n) = G_{x_n}(G_{x_{n-1}}(\cdots G_{x_1}(s))\cdots)$

Note: easy to sample, efficient to eval

$$F: \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$$

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Functions (PRFs)
- PRFs from length-doubling PRGs ("GGM" construction)
- Analyzing GGM

Analyzing the GGM construction

$$F_s(x_1 \cdots x_n) = G_{x_n}(\cdots G_{x_1}(s) \cdots)$$

Prove F_{GGM} is a PRF family

$\forall$ n.u. ppt A

$$Adv^{A}_{GGM, U_{n,n}} = \left| \Pr_{f_s \leftarrow F_{GGM}}[A^{f_s} = 1] - \Pr_{f \leftarrow U_{n,n}}[A^{f} = 1] \right| = negl(n)$$

$G^{GGM}(A)$:

$s \leftarrow \{0,1\}^n$

$b \leftarrow A^{F_s(\cdots)}$

Ret b

$F_s(x_1 \cdots x_n)$:

Ret $G_{x_n}(\cdots G_{x_1}(s) \cdots)$

$G^{U_n}(A)$

$R \leftarrow U_{n,n}$

$b \leftarrow A^{f}$

Ret b

$f(x)$:

Ret $R(x)$

Analyzing the GGM construction

Hybrid lemma: 2^n hybrids, replace each leaf

blows up - 2^n hybrids can't work!

Second attempt: n hybrids, one for each level

$H_0 := f_{GGM} = G^{GGM}$

$H_1 :=$ f_{GGM}, except 1st level is random strings instead of $G(\cdot)$

Analyzing the GGM construction

H_i := f_{GGM}, except level i is random strings

$f_{GGM}^i(x_1 \cdots x_n) = G_{x_n}(\cdots G_{x_{n-i}}(s_{x_1 \cdots x_i}) \cdots)$

By hybrid, $H_i \approx_c H_{i+1}$, then $f_{GGM} \approx_c U_{n,n}$

Slight problem: still need 2^i random strings

Analyzing the GGM construction

$G^i(A)$:

$(s_0^1, s_1^1), \ldots, (s_0^q, s_1^q) \leftarrow \{0,1\}^n \times \{0,1\}^n$

$b \leftarrow A^F$

Ret b

Note H_n is random function

$F(x_1 \ldots x_n)$:

$j \leftarrow 1$; $T \leftarrow []$

$P \leftarrow x_1 \ldots x_i$

If $T[P] = \perp$

$T[P] \leftarrow (s_0^j, s_1^j)$

$j += 1$

$s_0^P, s_1^P \leftarrow T[P]$

Ret $G_{x_n}(\ldots G_{x_{i+1}}(s_{x_i}^P)\ldots)$

replace i^{th} level with random strings

"greedy"

Analyzing the GGM construction

To finish: $H_i \approx_c H_{i+1}$. Show via composition

S_i s.t. if its input is PRG, S_i's output is H_i
" " is random, " " " is H_{i+1}

S_i efficient, composition lemma implies

$H_i \approx_c H_{i+1}$

Analyzing the GGM construction

$H_0 \approx_c H_1$, construct $\$_0$

$\$_0^A(s_0, s_1)$:

$b \leftarrow \{0,1\}^\ell$

Ret b

Claim: If $\$_0$'s input is $G(s)$, output is H_0

If $\$_0$'s input is random, output H_1

$F(x_1, \ldots, x_n)$:

Ret $G_{x_n}(\ldots G_{x_2}(G_{x_1}(s))\ldots)$

$\$_0$'s inputs $G(s) \approx_c U_{2n}$

$\Rightarrow H_0 \approx_c H_1$

Finish Wednesday