CSE 575: Advanced Cryptography
Fall 2024
Lecture 7

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- PRGs with arbitrary stretch
- Building PRGs (overview)
- Pseudorandom functions
- Building PRFs from PRGs (GGM)
- Analyzing GGM

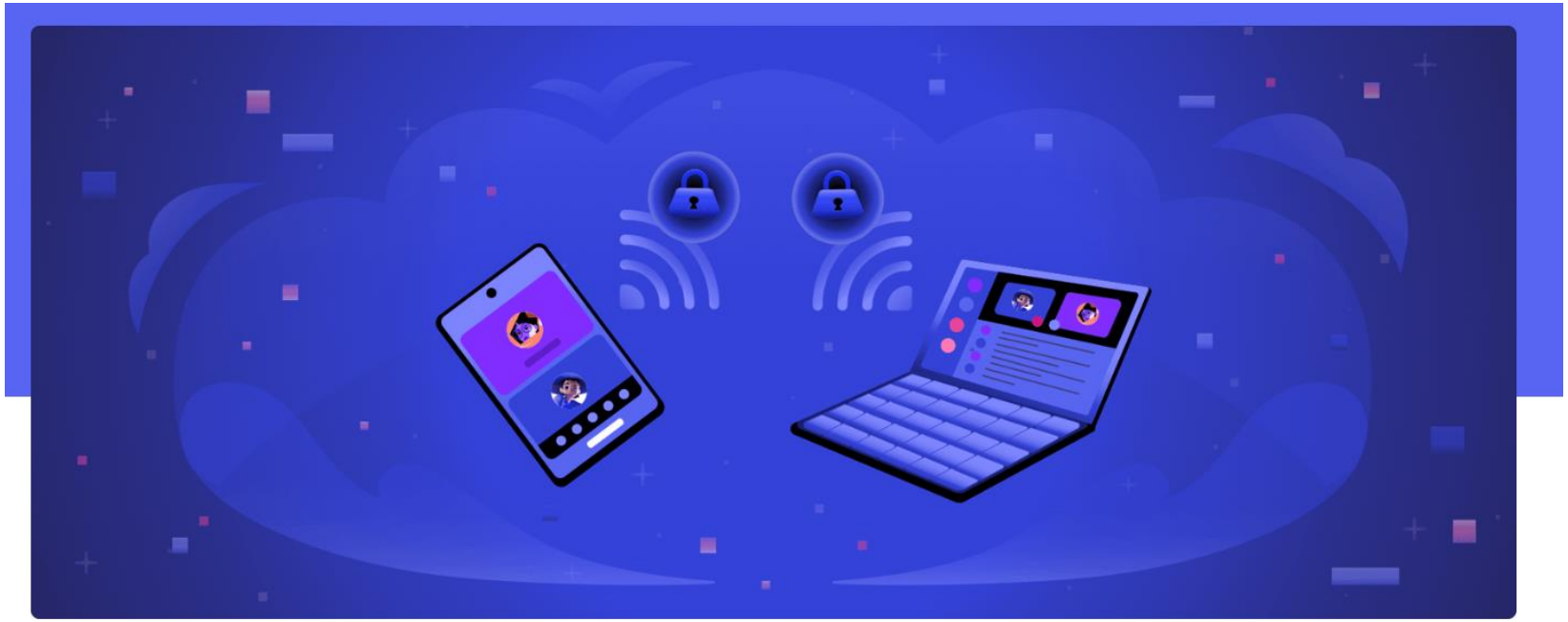
Agenda for this lecture

- Announcements
- PRGs with arbitrary stretch
- Building PRGs (overview)
- Pseudorandom functions
- Building PRFs from PRGs (GGM)
- Analyzing GGM

Announcements

- HW2 online, due 9/26

News

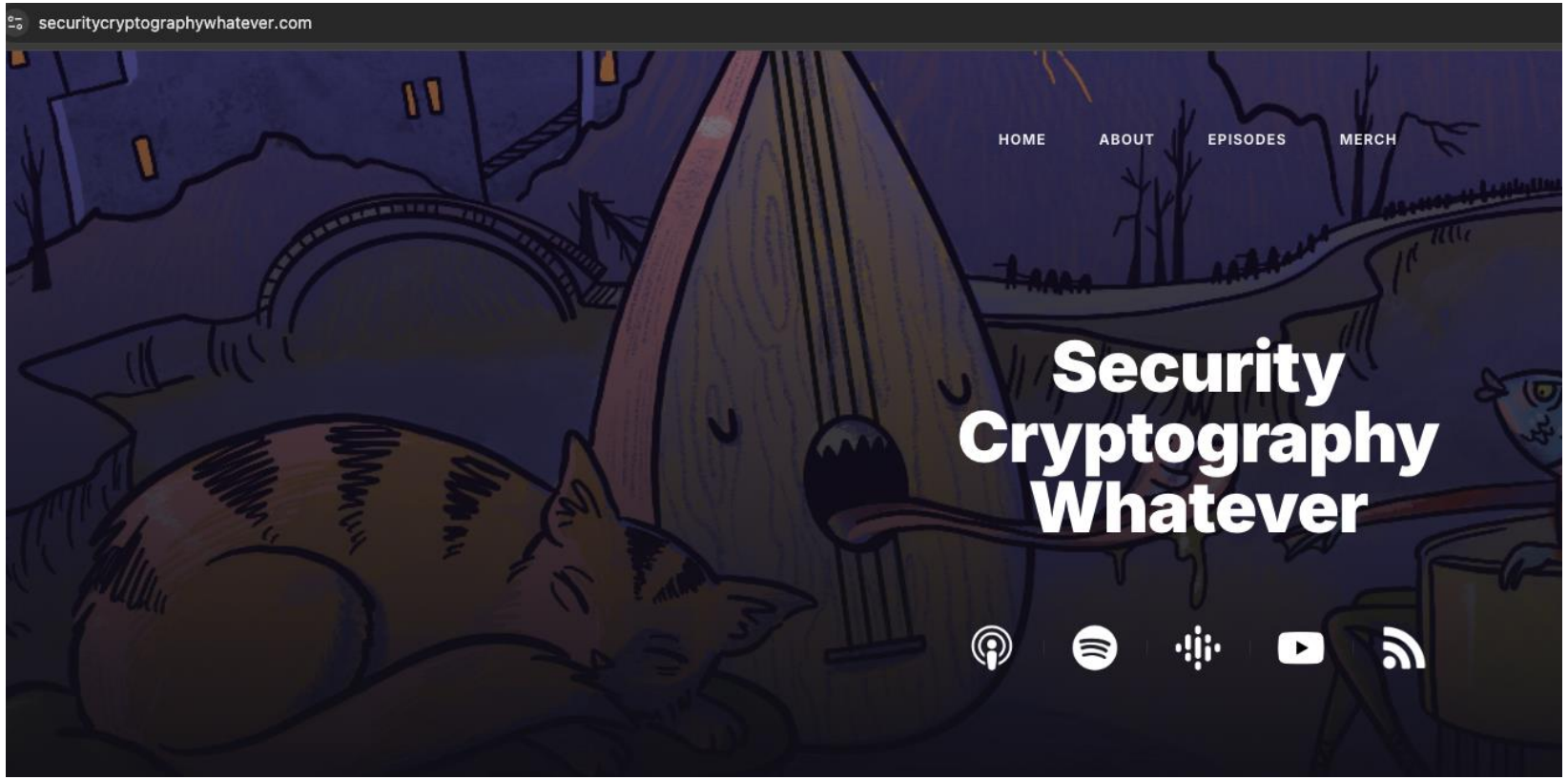


ENGINEERING & DEVELOPERS

MEET DAVE: DISCORD'S NEW END-TO-END ENCRYPTION FOR AUDIO & VIDEO

Safety is intertwined with our product and policies. While audio and video will be end-to-end encrypted, messages on Discord will continue to follow our content moderation approach and are not end-to-end encrypted. The E2EE A/V protocol was designed from the outset to be compatible with additional safety features that support the E2EE experience.

A cool podcast



Michigan PhD alum David Adrian is a co-host!

Agenda for this lecture

- Announcements
- PRGs with arbitrary stretch
- Building PRGs (overview)
- Pseudorandom functions
- Building PRFs from PRGs (GGM)
- Analyzing GGM

PRGs with arbitrary stretch

$G_t(s)$:

If $t = 0$
  Ret ε

Else
  $x \| b = G(s)$
  Ret $b \| G_{t-1}(x)$

$H_0 = G_t(U_n)$
$H_1 = U_1 \| G_{t-1}(U_n)$
$H_2 = U_2 \| G_{t-2}(U_n)$
$\vdots$
$H_i = U_i \| G_{t-i}(U_n)$
$\vdots$
$H_t = U_t$

Strategy:

Show $H_{i-1} \approx_c H_i$ using composition lemma

then $H_0 \approx_c H_t$ via hybrid lemma

PRGs with arbitrary stretch

$(y \in \{0,1\}^{n+1})$:

$x \| b = y$

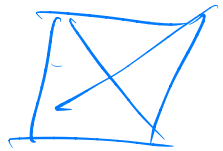
Ret $U_{i-1} \| b \| G_{t-i}(x)$

$ input is $G(s)$:

Get H_{i-1} !

$ input is U_{n+1}:

Get H_i !



Agenda for this lecture

- Announcements
- PRGs with arbitrary stretch
- Building PRGs (overview)
- Pseudorandom functions
- Building PRFs from PRGs (GGM)
- Analyzing GGM

How do we build PRGs?

- From OWFs, but non trivial...
- Hardcore predicates from OWPs
  - Blum-Micali: from DLog
  - HCP for any OWF - Goldreich-Levin
  - From any OWF: HILL

HCP

PRGs => PRFs !

Agenda for this lecture

- Announcements
- PRGs with arbitrary stretch
- Building PRGs (overview)
- Pseudorandom functions
- Building PRFs from PRGs (GGM)
- Analyzing GGM

Oracle indistinguishability

Let $\mathcal{O} = \{O_n\}$ $\mathcal{O}' = \{O_n'\}$

be ensembles over functions

$$\{0,1\}^{\ell_1(n)} \longrightarrow \{0,1\}^{\ell_2(n)} \qquad \ell_1, \ell_2 = poly(n)$$

Say $\mathcal{O} \approx_c \mathcal{O}'$ if $\forall$ nuPPT D,

$$Adv_{\mathcal{O},\mathcal{O}'} = \left| \Pr_{f \leftarrow O_n}[D^f = 1] - \Pr_{f \leftarrow O_n'}[D^f = 1] \right| = negl(n)$$

Say $\mathcal{O}$ pseudorandom if

$$\mathcal{O} \approx \{U(\{0,1\}^{\ell_1(n)} \longrightarrow \{0,1\}^{\ell_2(n)})\}$$

Unif. dist. over functions $\ell_1(n) \to \ell_2(n)$ bits

Pseudorandom functions (PRF)

F is PRF if

- Easy to sample
- Easy to evaluate
- (oracle) Pseudorandom

Agenda for this lecture

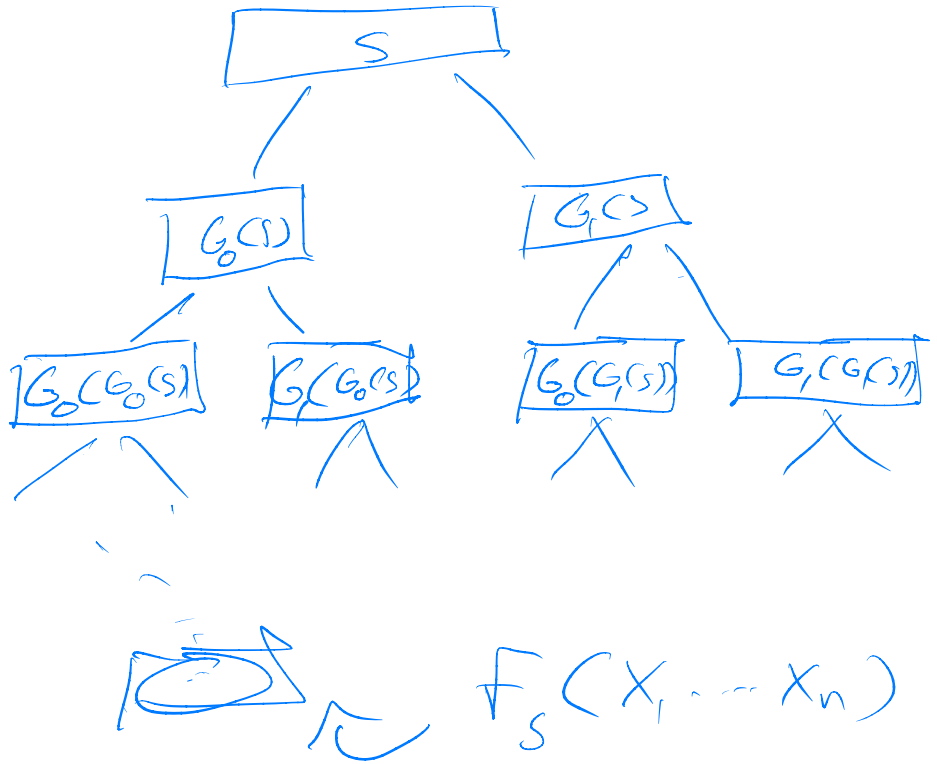
- Announcements
- PRGs with arbitrary stretch
- Building PRGs (overview)
- Pseudorandom functions
- Building PRFs from PRGs (GGM)
- Analyzing GGM

Building PRFs: the GGM construction

$F: \{0,1\}^n \to \{0,1\}^n \quad G(s) = G_0(s) \,||\, G_1(s) \quad G: \{0,1\}^n \to \{0,1\}^{2n}$

$F_s(x_1 \cdots x_n)$:

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



Agenda for this lecture

- Announcements
- PRGs with arbitrary stretch
- Building PRGs (overview)
- Pseudorandom functions
- Building PRFs from PRGs (GGM)
- Analyzing GGM

Analyzing GGM

$f_s(x_1, \ldots x_n)$:

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

H_0 : F_s

H_1 : $G_{x_n}(\cdots(S_{x_1})\cdots)$

Takes S_0, S_1 to replace level 1

H_i : $G_{x_n}\cdots G_{x_{i+1}}(S_{x_1\cdots x_i})$

Takes $S_0, S_1, \ldots, S_{2^i}$

H_n : on. f. funct $\{0,1\}^n \to \{0,1\}$

Warmup: $H_0 \approx_c H_1$

$\$(S_0, S_1)$:

Simulate as $G_{x_n}(\cdots G_{x_2}(S_{x_1})\cdots)$

By comp. lemma

$H_0 \approx_c H_1$