CIS 5560

Cryptography
Lecture 5

Course website:

pratyushmishra.com/classes/cis-5560-s24/

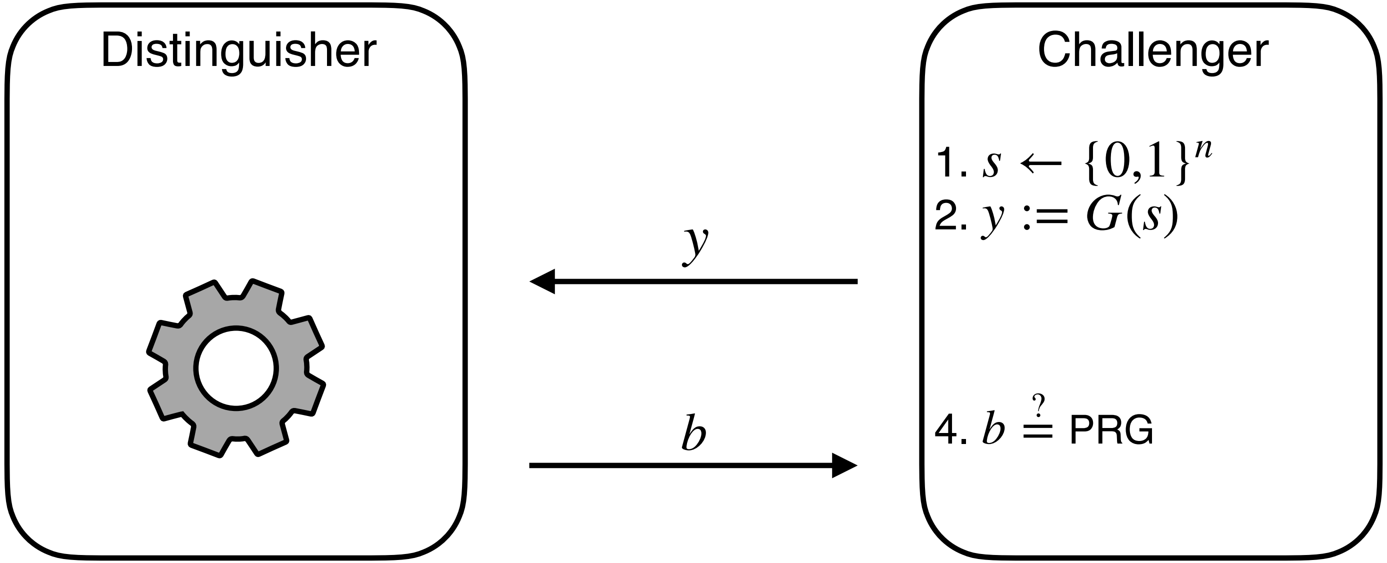
Slides adapted from Dan Boneh and Vinod Vaikuntanathan

Announcements

- **HW 2 is out;** due Monday, Feb 5 at 5PM on Gradescope
  - Covers PRGs, OWFs, and semantic security
  - Get started today and make use of office hours!
- New Office Hours:
  - Alireza: Tuesday 5-6PM Levine 3rd floor bump space
  - Jack: Wednesday 2-3:30PM Living 6th floor bump space

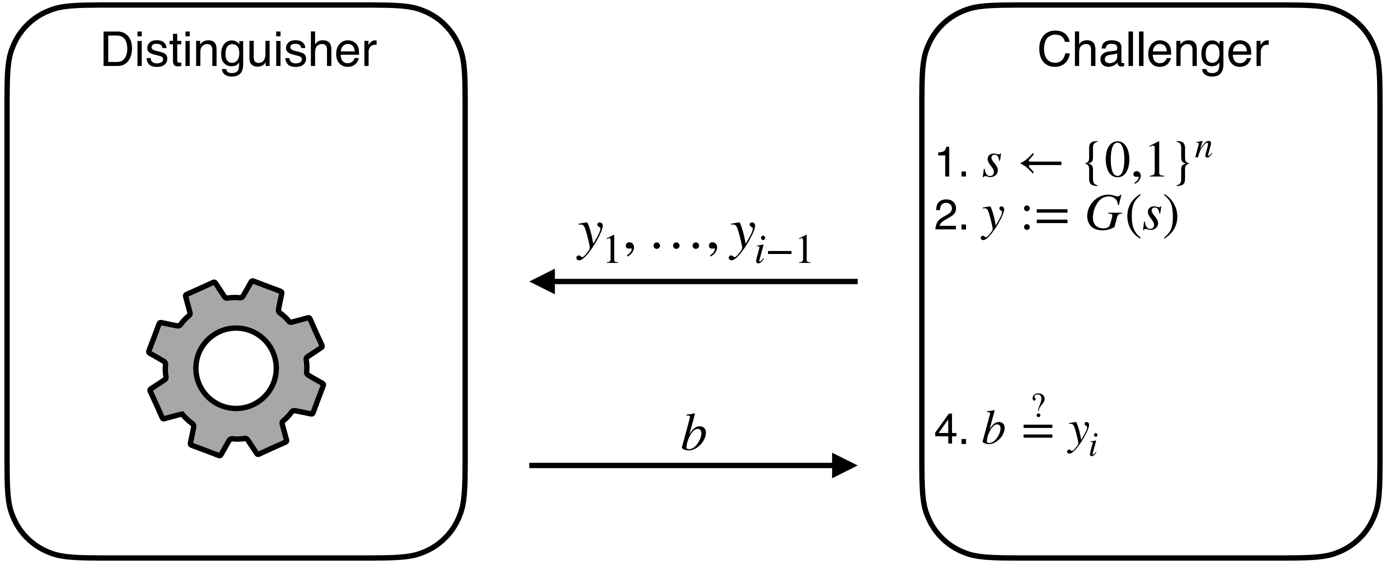
Recap of last lecture

PRG Indistinguishability



$$\left| \Pr[D(G(U_n)) = 1] - \Pr[D(U_m) = 1] \right| = \varepsilon(n)$$

PRG Next-Bit Unpredictability



$$\Pr\left[A(y_1, \ldots, y_{i-1}) = y_i \;\middle|\; \begin{array}{r} s \leftarrow \{0,1\}^n \\ y \leftarrow G(s) \end{array}\right] = 1/2 + \varepsilon(n)$$

Def 1 and Def 2 are Equivalent

Theorem:
A PRG G is indistinguishable if and only if it is next-bit unpredictable.

One-way Functions: The Definition

A function (family) $\{F_n\}_{n\in\mathbb{N}}$ where $F(\cdot) : \{0,1\}^n \to \{0,1\}^{m(n)}$ is **one-way** if for every p.p.t. adversary A, the following holds:

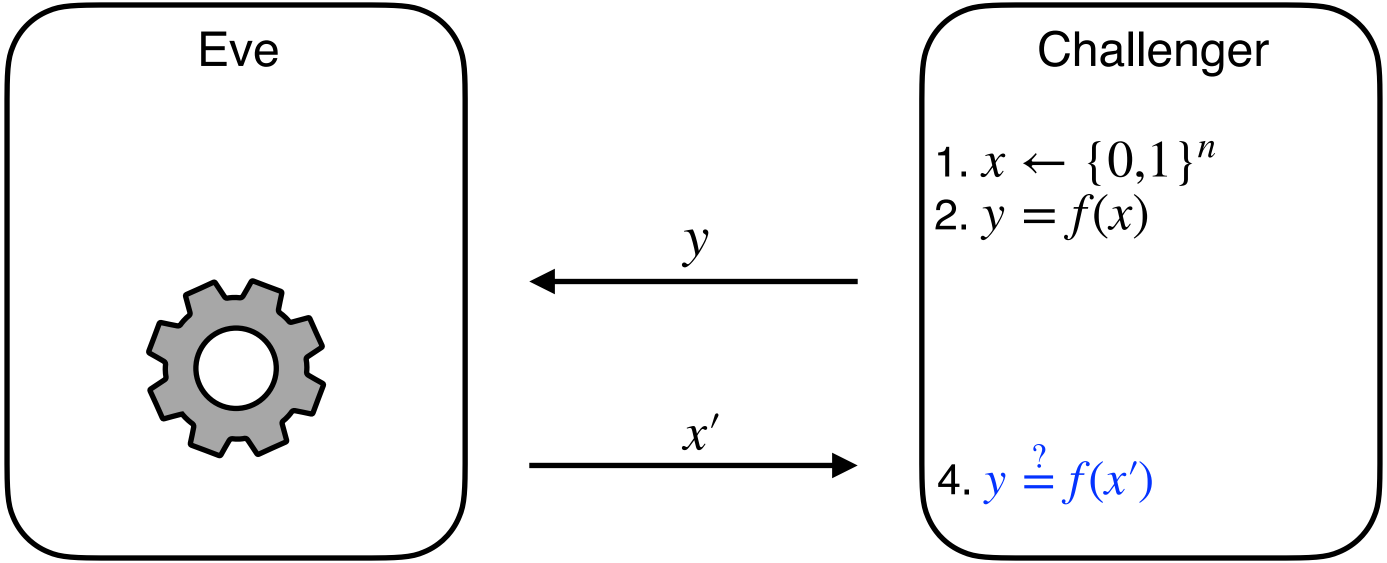
$$\Pr\left[F_n(x') = y \;\middle|\; \begin{array}{r} x \leftarrow \{0,1\}^n \\ y := F_n(x) \\ x' \leftarrow A(1^n, y) \end{array} \right] = \text{negl}(n)$$

- Can always find *an* inverse with unbounded time
- … but should be hard with probabilistic polynomial time

One-way Permutations:

One-to-one one-way functions with $m(n) = n$.

OWF Security Attempt #2



Today’s Lecture

- PRG Indistinguishability → PRG Unpredictability
- One way functions and permutations
- OWPs → PRGs

How to get PRG from OWF?

OWF → PRG, Attempt #1

PRG(k)

1. Output $F_n(k)$

(Assume $m(n) > n$)

Does this work?

OWF → PRG, Attempt #1

Consider $F_n(x)$ constructed from another OWF F'_n:

1. Compute $y := F'_n(x)$
2. Output $y' := (y_0,\ 1, y_1,\ 1, \ldots, y_n,\ 1)$

PRG(k)

1. Output $F_n(k)$

Is F one-way?

Yes!

Is PRG unpredictable?

No!

Our problem:

OWFs don’t tell us anything about how their outputs are distributed.

They are only hard to invert!

OW**P** → PRG, Attempt #1

Let $F : \{0,1\}^n \rightarrow \{0,1\}^n$ **be a one-way permutation**

Consider the following PRG candidate

PRG(k)

1. Output $F(k)$

Does this work?

No, it's not expanding!

But how are outputs distributed?

Claim: Output of F is uniformly distributed

Claim: Output of OWP is uniformly distributed

Proof: Assume for contradiction that this is not the case.

This means that there exists some y such that

$$\Pr[F(x) = y \,|\, x \leftarrow \{0,1\}^n] > 1/2^n$$

This means that $\dfrac{\left|\{x \,|\, F(x) = y\}\right|}{2^n} > \dfrac{1}{2^n}$,

which in turn means that F is not a permutation!

Our problem:

OWFs don’t tell us anything about how their outputs are distributed.

Solution: use OWP

Problem: no expansion

OW**P** → PRG, Attempt #2

Let $F : \{0,1\}^n \rightarrow \{0,1\}^n$ be a one-way permutation

Imagine there existed $B : \{0,1\}^n \rightarrow \{0,1\}$ such that the following was a PRG

PRG(k)

1. Output $F(k) \mid\mid B(k)$

What properties do we need of B?

1. One-way: can't find k from $B(k)$
2. Pseudorandom: $B(k)$ looks like a random bit
3. Unpredictable: $B(k)$ is unpredictable given $F(k)$

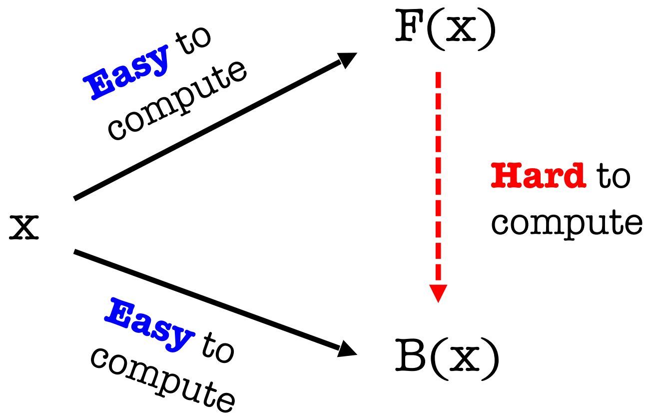
Hardcore Bits

HARDCORE PREDICATE

For any $F: \{0,1\}^n \rightarrow \{0,1\}^m$, $B: \{0,1\}^n \rightarrow \{0,1\}$ is a **hardcore predicate** if for every efficient A, there is a negligible function μ s.t.

$$\Pr\left[b = B(x) \,\middle|\, \begin{array}{c} x \leftarrow \{0,1\}^n \\ b \leftarrow A(F(x)) \end{array} \right] = 1/2 + \mu(n)$$

Hardcore Predicate (in pictures)



Existence of hardcore predicates

Goldreich-Levin Theorem

Let $F : \{0,1\}^n \rightarrow \{0,1\}^n$ be a one-way function.
Define $H(x \,||\, r) := F(x) \,||\, r$.

Then $B(x \,||\, r) := \langle x, r \rangle$ is a hardcore predicate for H

Existence of hardcore predicates

Hardcore predicate for RSA

Define $F_{N,e}(x) := x^e \mod N$ to be the **RSA** OWF.

Then $\mathsf{lsb}(x)$ is a hardcore predicate for F

OWP → PRG

OWP $\Rightarrow$ PRG

Theorem

Let F be a one-way permutation, and let B be a hardcore predicate for F.
Then, $G(x) := F(x) \mid\mid B(x)$ is a PRG.

Proof (next slide): Use next-bit unpredictability.

OWP $\Rightarrow$ PRG

Theorem: G is a PRG assuming F is a one-way permutation.

Proof: Assume for contradiction that G is not a PRG.
Therefore, there is a next-bit predictor P, and index i, and a polynomial p such that

$$\Pr\left[P(y_1,\ldots,y_{i-1}) = y_i \,\middle|\, \begin{array}{c} x \leftarrow \{0,1\}^n \\ y \leftarrow G(x) \end{array}\right] = 1/2 + 1/p(n)$$

Observation: The index i has to be $n+1$. Do you see why?

Hint: $G(x) := F(x) || B(x)$ and we *know* $F(x)$ is uniformly distributed

OWP $\Rightarrow$ PRG

Theorem: G is a PRG assuming F is a one-way permutation.

Proof: Assume for contradiction that G is not a PRG.
Therefore, there is a next-bit predictor P, and polynomial p such that

$$\Pr\left[P(y_1,\ldots,y_n) = y_{n+1} \,\middle|\, \begin{array}{r} x \leftarrow \{0,1\}^n \\ y \leftarrow G(x) \end{array}\right] = 1/2 + 1/p(n)$$

OWP $\Rightarrow$ PRG

Theorem: G is a PRG assuming F is a one-way permutation.

Proof: Assume for contradiction that G is not a PRG.
Therefore, there is a next-bit predictor P, and polynomial p such that

$$\Pr\left[P(F(x)) = B(x) \,\middle|\, \begin{array}{r} x \leftarrow \{0,1\}^n \\ y \leftarrow G(x) \end{array}\right] = 1/2 + 1/p(n)$$

So, P can figure out $B(x)$ and break hardcore property!
QED.

- **So far: PRG with 1-bit expansion**
- Resulting secret-key encryption:
  - Key can be 1 bit shorter than message
  - Not much better than OTP!

Can we do better?

PRG length extension.

Theorem: If there is a PRG that stretches by one bit, there is one that stretches by poly many bits

- **New Proof Technique: Hybrid Arguments.** 

Before we go there, a puzzle…

<u>Lemma</u>: Let $p_0, p_1, p_2, \ldots, p_m$ be real numbers s.t.

$$\boldsymbol{p_m - p_0 \geq \varepsilon} \,.$$

Then, there is an index i such that $\boldsymbol{p_i - p_{i-1} \geq \varepsilon/\mathbf{m}}$.

<u>Proof</u>:

$$p_m - p_0 = \left(p_m - p_{m-1}\right) + \left(p_{m-1} - p_{m-2}\right) + \ldots + (p_1 - p_0)$$
$$\geq \varepsilon$$

At least one of the m terms has to be at least ε/m (averaging).

$\blacksquare$

Length extension: One bit to Many bits

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

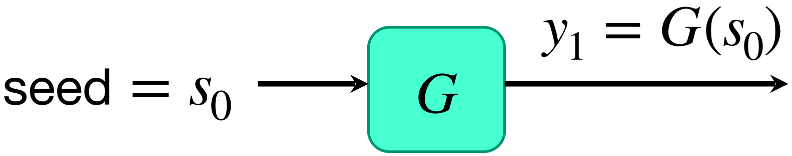
Goal: use G to generate **many** pseudorandom bits.

Length extension: One bit to Many bits

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

Goal: use G to generate **many** pseudorandom bits.

Construction of $G'(s_0)$



Length extension: One bit to Many bits

Let $G : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a PRG

Goal: use G to generate **many** pseudorandom bits.

<u>Construction of $G'(s_0)$</u>

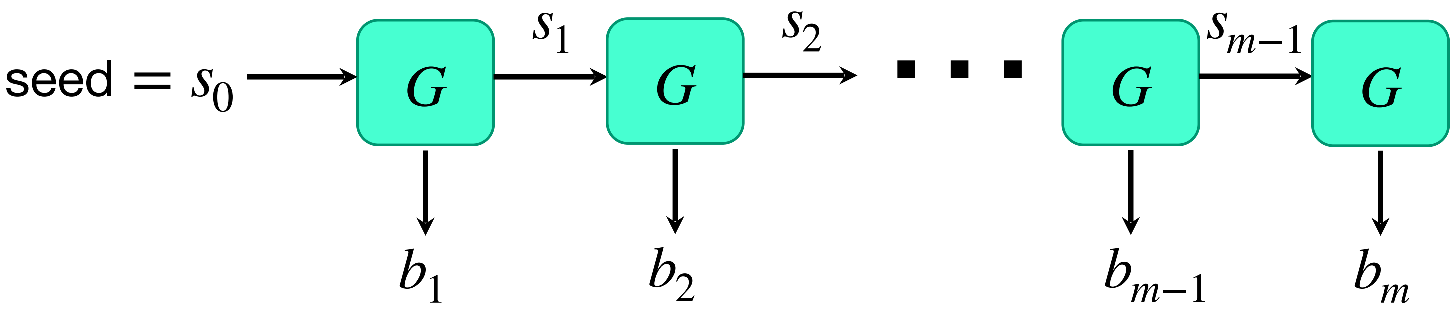
$$\text{seed} = s_0 \longrightarrow \boxed{G} \xrightarrow{y_1 = b_1 || s_1}$$

Length extension: One bit to Many bits

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

Goal: use G to generate **many** pseudorandom bits.

<u>Construction of $G'(s_0)$</u>

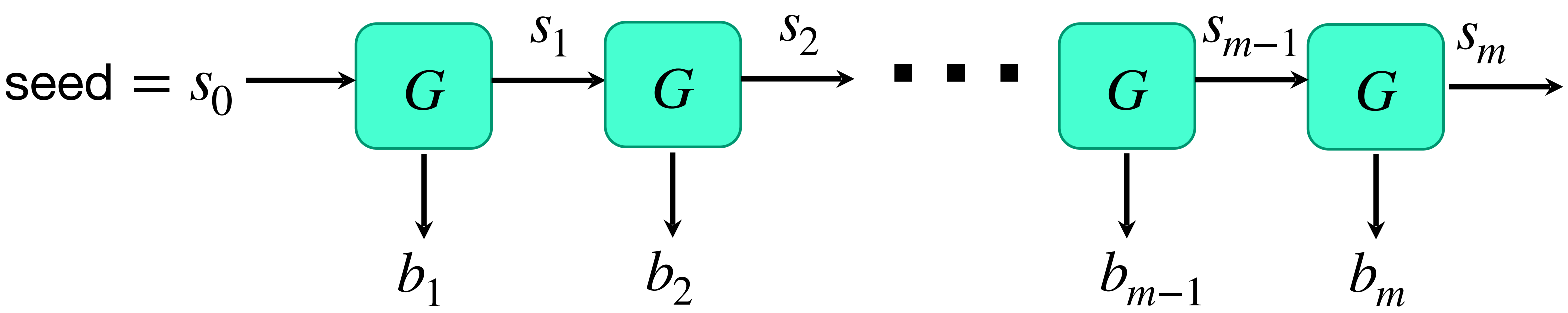


Length extension: One bit to Many bits

Proof of Security (exercise):

Use next-bit (or previous-bit?) unpredictability!

<u>Construction of $G'(s_0)$</u>



Next class

- PRFs: How to get PRGs with “exponentially-large” output