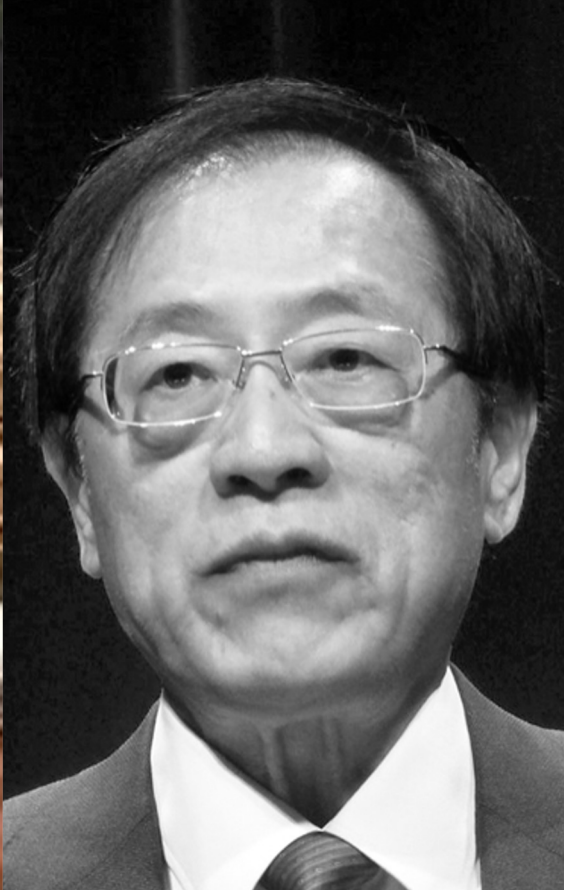


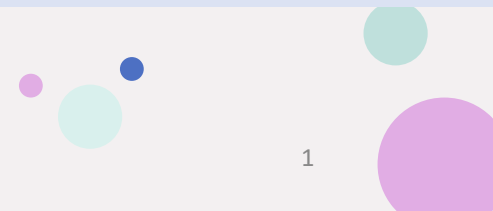


Lecture 6

Hybrid Arguments, More about PRGs

CS409/6011: Introduction to Cryptography

Instructor: Sruthi Sekar



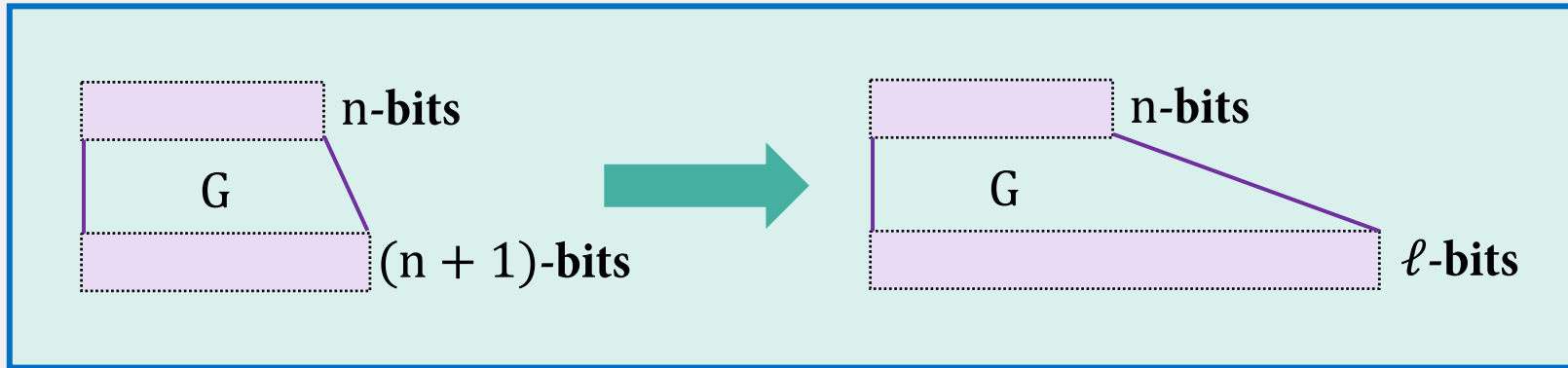
Recap

- We defined two notions for Pseudorandom Generators:
 - Unpredictability
 - Pseudorandomness

RECALL: PRGs **do not exist** if

- you have an unbounded Eve, or
 - if $\mathbf{P} = \mathbf{NP}$
- We saw a new proof technique called **security reduction**:
 - Pseudorandomness $\Rightarrow$ Unpredictability
 - Computational Indistinguishability of Computational one-time pad
- Some ideas for building PRGs

Today

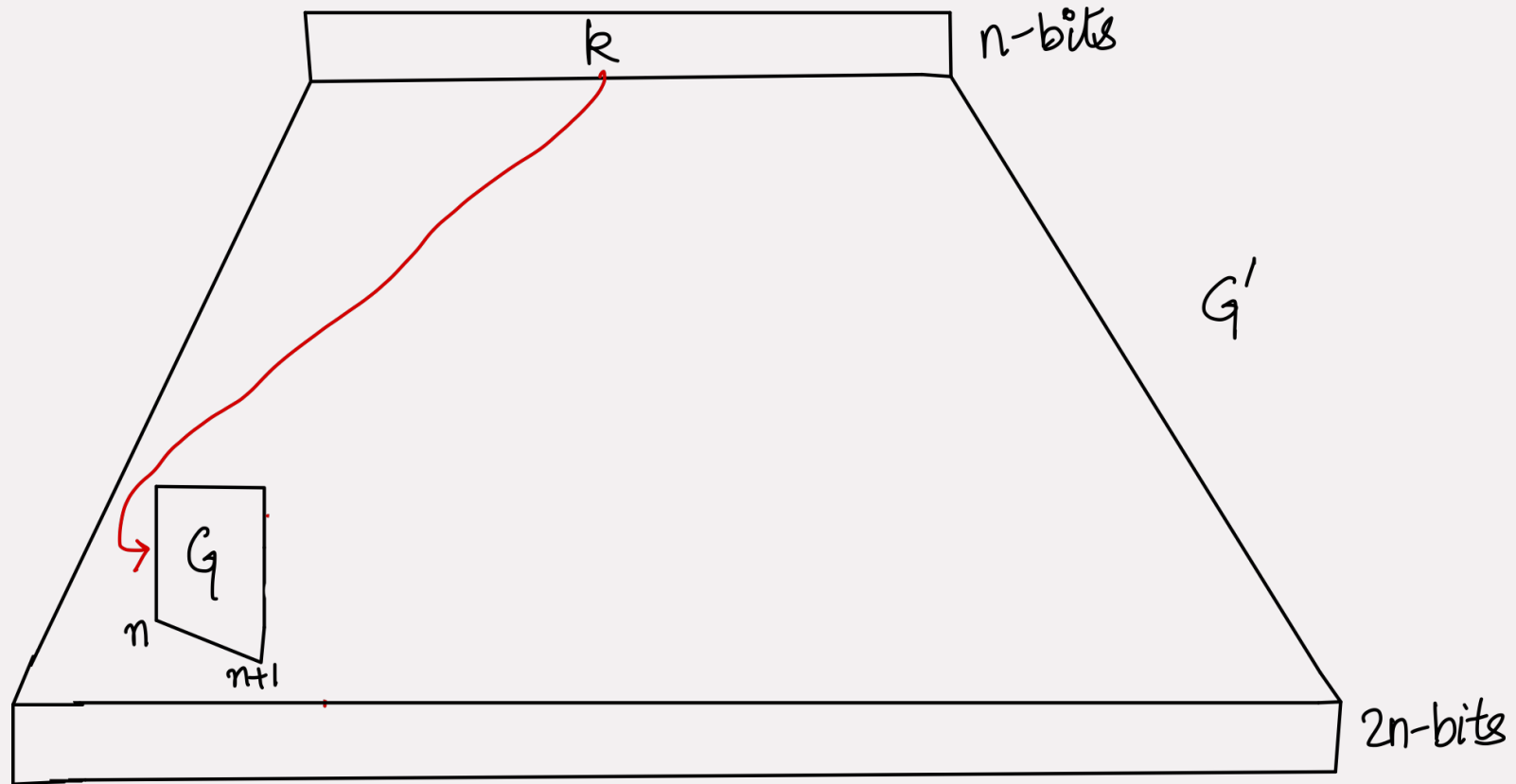


Length-Extension of PRGs

New proof technique called “**hybrid argument**”

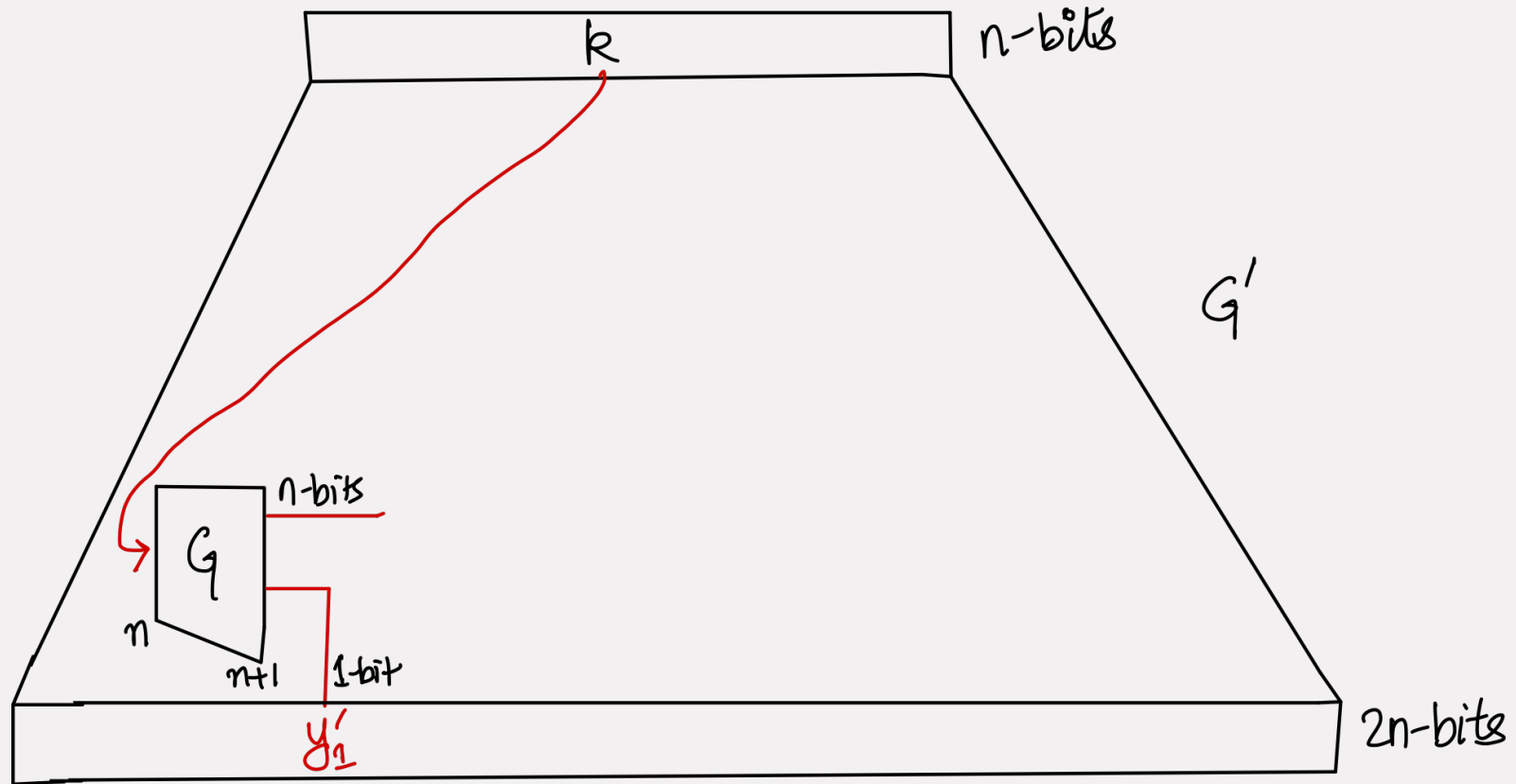
Length Extension of PRGs

GOAL: Given a PRG, G with stretch $n + 1$, can we build a PRG, G' with stretch $2n$



Length Extension of PRGs

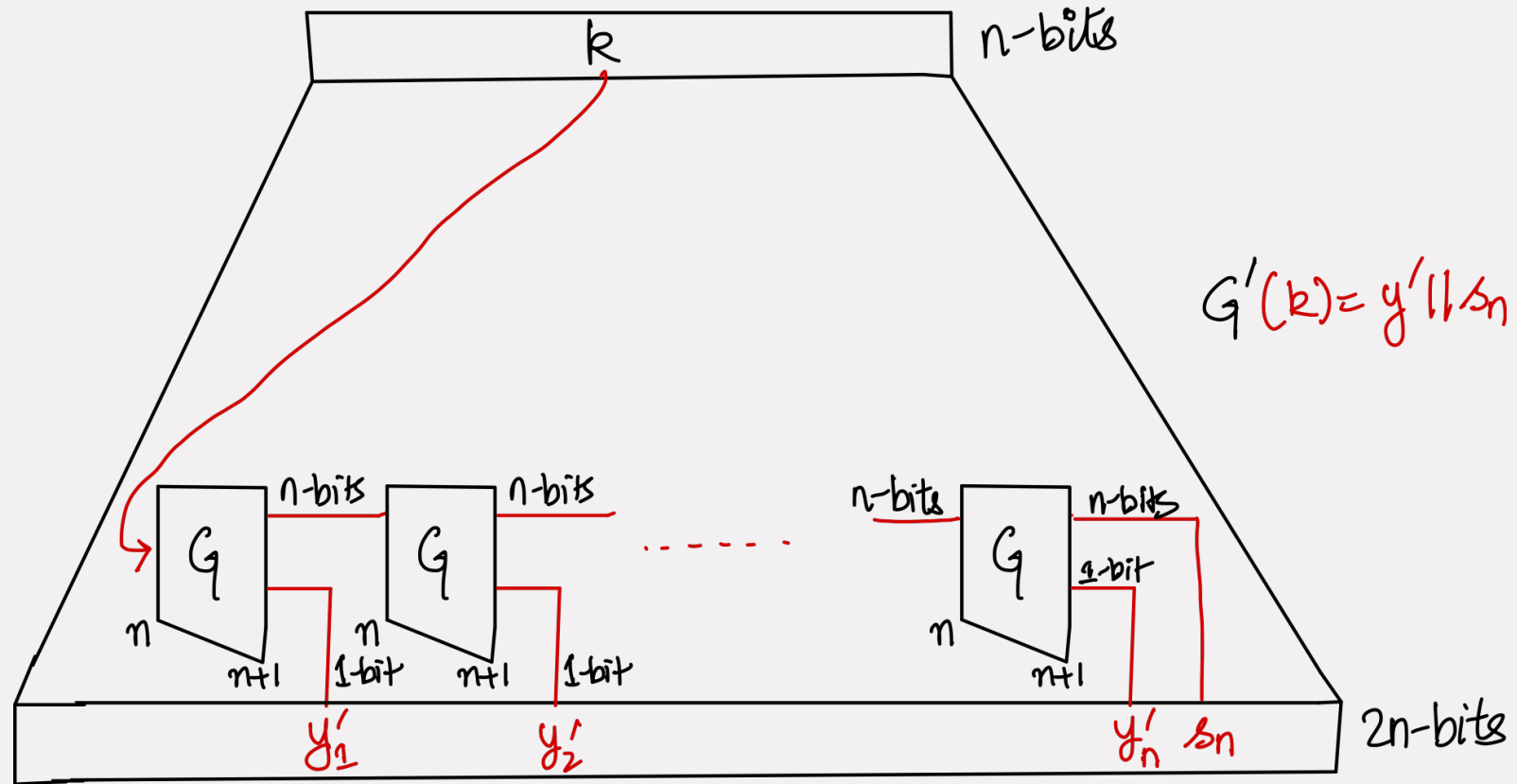
GOAL: Given a PRG, G with stretch $n + 1$, can we build a PRG, G' with stretch $2n$



Construction 1

Length Extension of PRGs

GOAL: Given a PRG, G with stretch $n + 1$, can we build a PRG, G' with stretch $2n$



Construction 1

Length Extension of PRGs

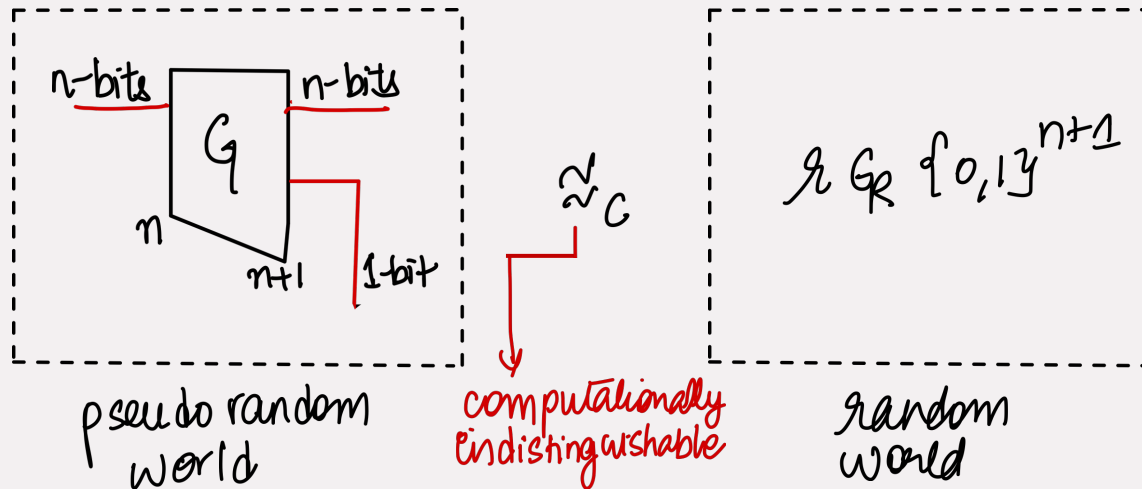
Theorem 1

If G is a pseudorandom generator, then so is G' .



INTUITION

Since G is a PRG



Length Extension of PRGs

Theorem 1

If G is a pseudorandom generator, then so is G' .

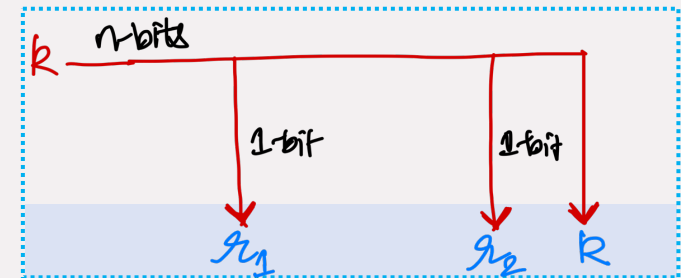
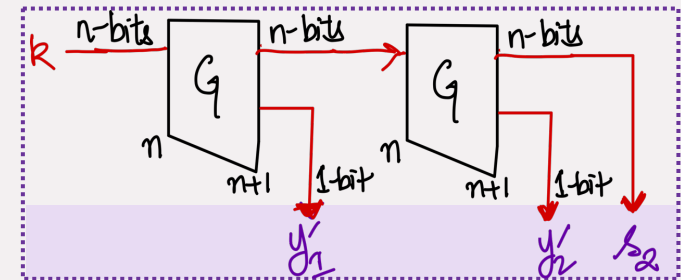


INTUITION Let's understand two iterations first...

Goal is to show that these two worlds are computationally indistinguishable.

H_0 : Pseudorandom World

H_2 : Random World



Length Extension of PRGs

Theorem 1

If G is a pseudorandom generator, then so is G' .



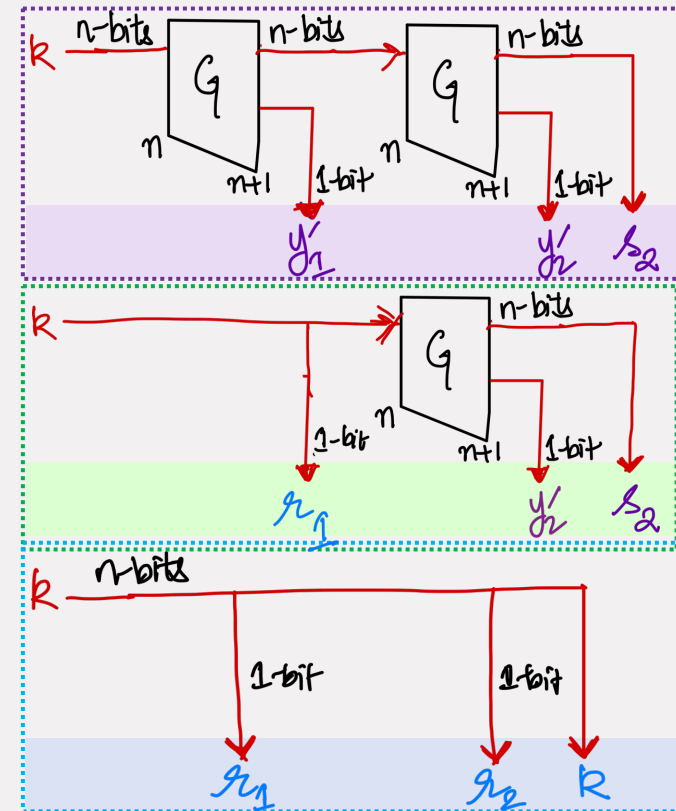
INTUITION Let's understand two iterations first...

Consider a hybrid world
between the two of them as an
intermediate step!

H_0 : Pseudorandom World

H_1 : Hybrid World

H_2 : Random World



Length Extension of PRGs

Theorem 1

If G is a pseudorandom generator, then so is G' .



INTUITION Let's understand two iterations first...

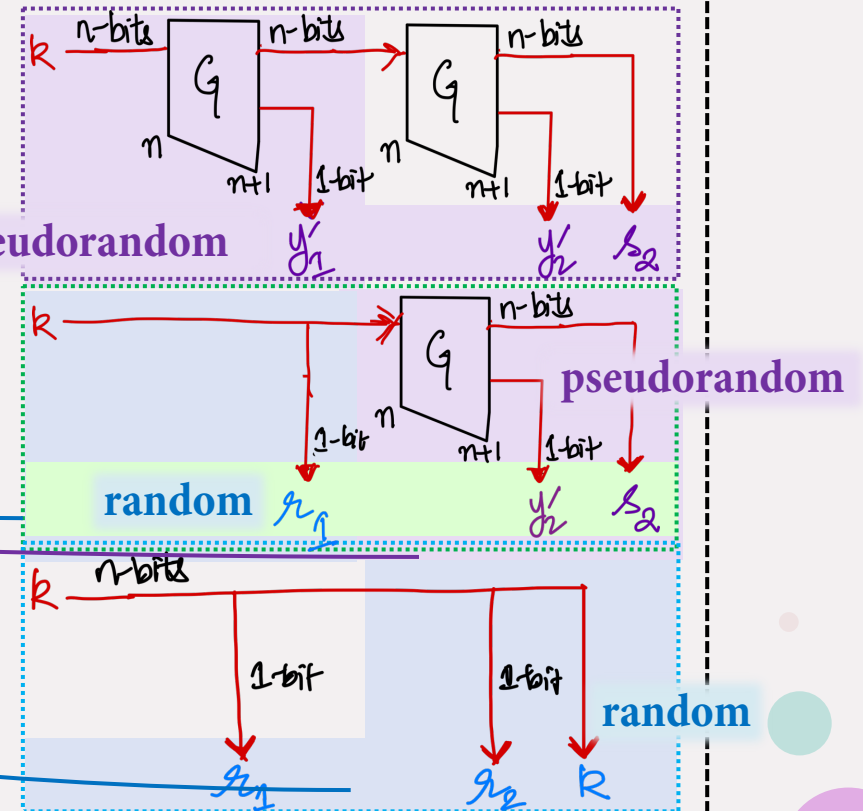
H_0 : Pseudorandom World

pseudorandom

Computationally indistinguishable
since G is a PRG!

H_1 : Hybrid World

H_2 : Random World



Length Extension of PRGs

Theorem 1

If G is a pseudorandom generator, then so is G' .



INTUITION Let's understand two iterations first...

Claim 1: If there exists $\text{Eve}^{G'}$ such that

$$|\Pr[\text{Eve}^{G'}(H_0) = 1] - \Pr[\text{Eve}^{G'}(H_2) = 1]| > \delta$$

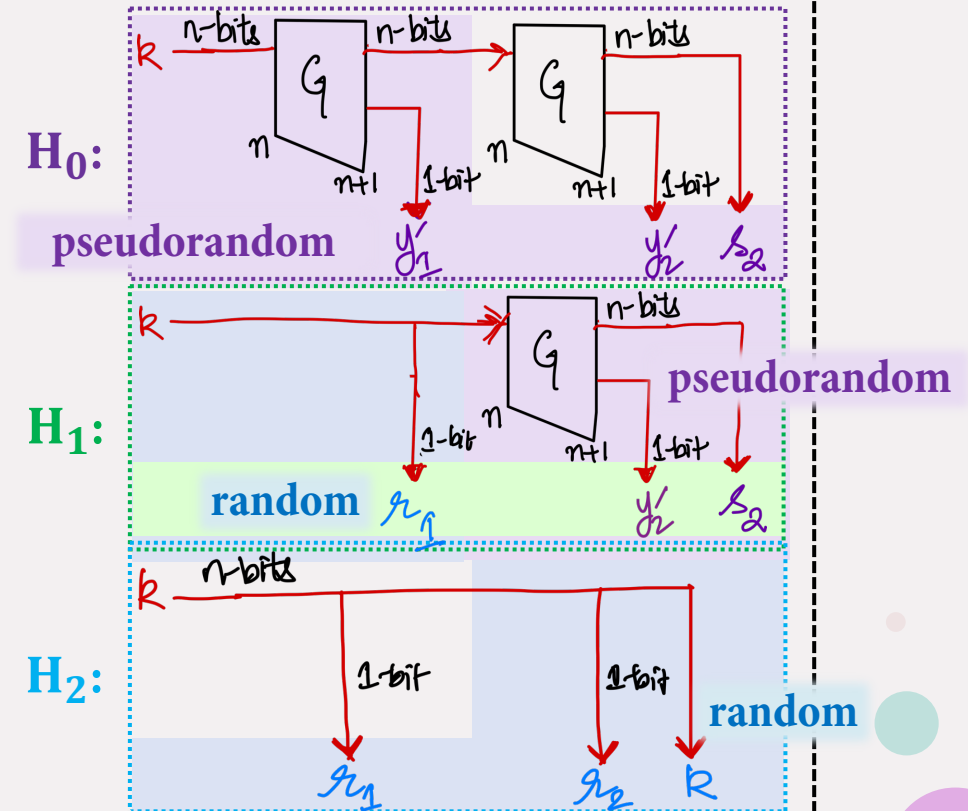
then, $\exists i \in \{0, 1\}$ such that

$$|\Pr[\text{Eve}^{G'}(H_i) = 1] - \Pr[\text{Eve}^{G'}(H_{i+1}) = 1]| > \delta/2$$

Claim 2:

$$|\Pr[\text{Eve}^{G'}(H_i) = 1] - \Pr[\text{Eve}^{G'}(H_{i+1}) = 1]| > \delta/2 \\ \Rightarrow \text{A distinguisher } \text{Eve}^G \text{ for } G$$

Claim 1 & Claim 2 $\Rightarrow$ Theorem 1



Length Extension of PRGs

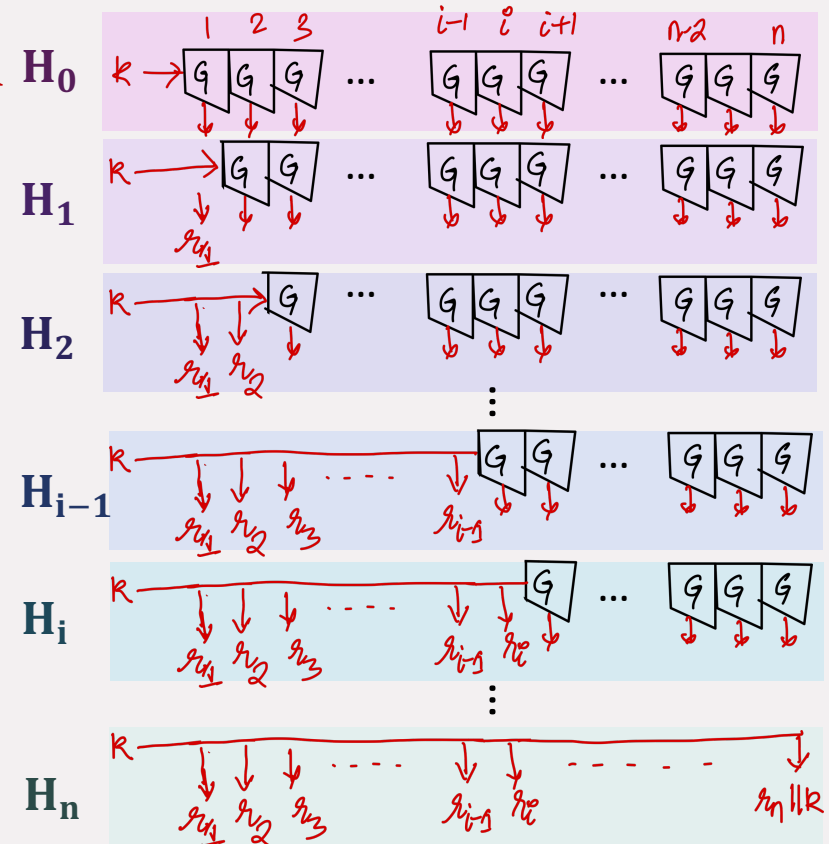
Theorem 1

If G is a pseudorandom generator, then so is G' .



INTUITION (All hybrids)

pseudorandom H_0



random H_n

Length Extension of PRGs

Theorem 1

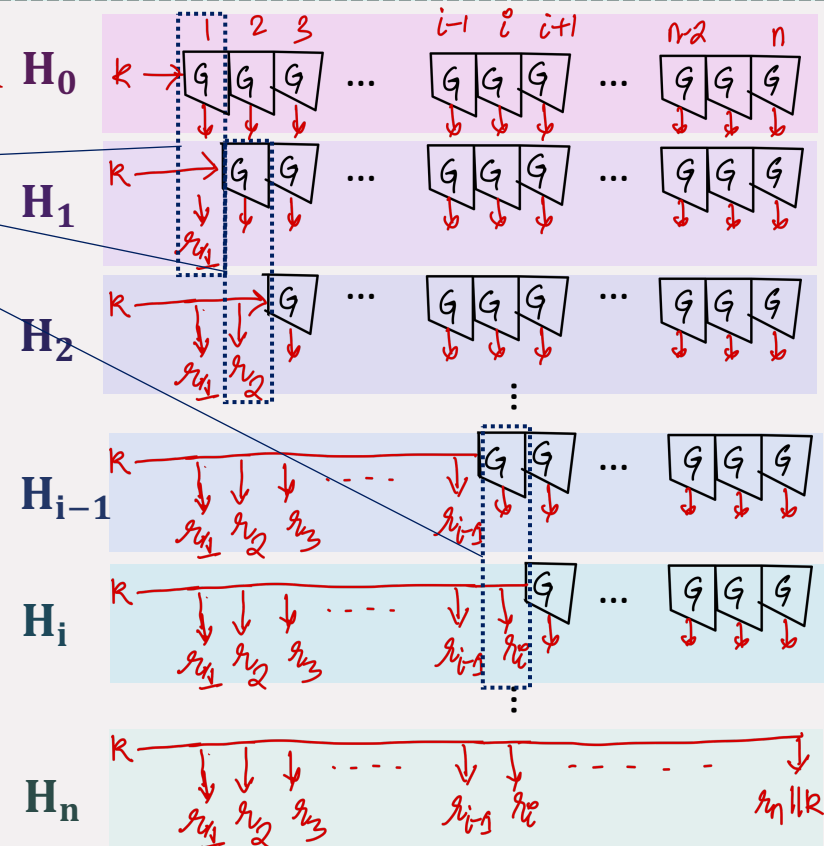
If G is a pseudorandom generator, then so is G' .



INTUITION (All hybrids)

Each pair of hybrids look computationally indistinguishable since G is a PRG

pseudorandom H_0



random H_n

Length Extension of PRGs

Theorem 1

If G is a pseudorandom generator, then so is G' .

Proof: Suppose $\exists \text{Eve}^{G'}$ that breaks pseudorandomness of G'

Claim 1: If there exists $\text{Eve}^{G'}$ such that
 $|\Pr[\text{Eve}^{G'}(H_0) = 1] - \Pr[\text{Eve}^{G'}(H_n) = 1]| > \delta$
then, $\exists i \in \{0, 1, \dots, n-1\}$ such that
 $|\Pr[\text{Eve}^{G'}(H_i) = 1] - \Pr[\text{Eve}^{G'}(H_{i+1}) = 1]| > \delta/n$

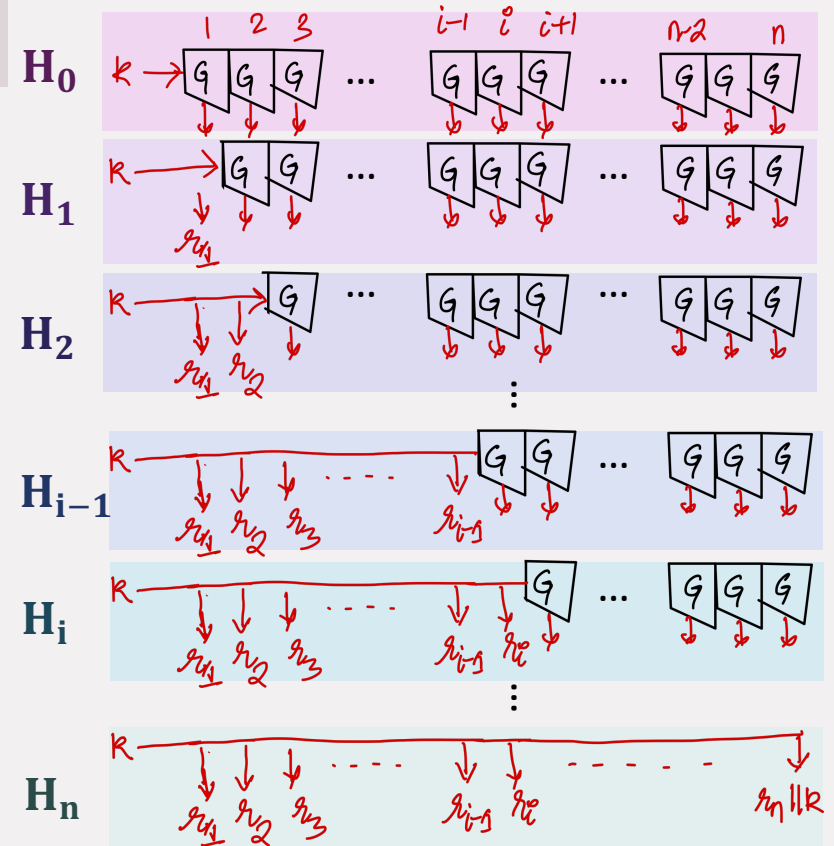


This claim will be implicitly used in our proof!

Eve^G wants to pick this “ i ” and use $\text{Eve}^{G'}$ to win her game!



Eve^G doesn't know which i ,
so she will just pick one at random!



Length Extension of PRGs

Theorem 1

If G is a pseudorandom generator, then so is G' .

Proof: Suppose $\exists \text{Eve}^{G'}$ that breaks pseudorandomness of G'

Claim 1: If there exists $\text{Eve}^{G'}$ such that $|\Pr[\text{Eve}^{G'}(H_0) = 1] - \Pr[\text{Eve}^{G'}(H_n) = 1]| > \delta$
then, $\exists i \in \{0, 1, \dots, n-1\}$ such that $|\Pr[\text{Eve}^{G'}(H_i) = 1] - \Pr[\text{Eve}^{G'}(H_{i+1}) = 1]| > \delta/n$

Eve^G

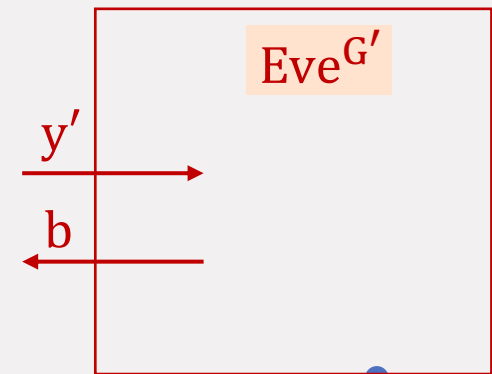
$$\Pr[i^* = i] = \frac{1}{n}$$

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

- Picks $i^* \in_R \{0, \dots, n-1\}$
- Computes challenge for $\text{Eve}^{G'}$ as:

Plug in the challenge at $(i^* + 1)$ th location

Outputs: b



Length Extension of PRGs

Theorem 1

If G is a pseudorandom generator, then so is G' .

Proof: Suppose $\exists \text{Eve}^{G'}$ that breaks pseudorandomness of G'

Combining ideas to complete the proof!

Eve^G

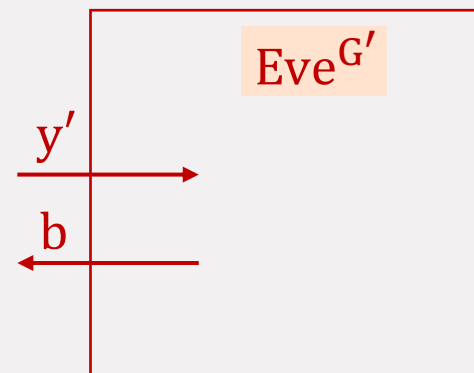
Input: $y \in \{0,1\}^{n+1}$

- Picks $i^* \in_R \{0, \dots, 2n-1\}$
- Computes challenge for $\text{Eve}^{G'}$ as:

Plug in the challenge at (i^*+1) th location



Outputs: b



$$\begin{aligned}
 & |\Pr[\text{Eve}^G(G(k)) = 1] - \Pr[\text{Eve}^G(r) = 1]| \\
 &= |\Pr[\text{Eve}^{G'}(H_{i^*}) = 1] - \Pr[\text{Eve}^{G'}(H_{i^*+1}) = 1]| = \frac{1}{n} \left| \sum_{i=0}^{n-1} \Pr[\text{Eve}^{G'}(H_i) = 1] - \sum_{i=0}^{n-1} \Pr[\text{Eve}^{G'}(H_{i+1}) = 1] \right| \\
 &= \frac{1}{n} |\Pr[\text{Eve}^{G'}(H_0) = 1] - \Pr[\text{Eve}^{G'}(H_n) = 1]| > \frac{\delta}{n}
 \end{aligned}$$

Sanity Check: Trick Question

$n + 1$ Hybrids (where n is the security parameter): $H_0, H_1, \dots, H_n$

Claim: If there exists $\text{Eve}^{G'}$ such that $|\Pr[\text{Eve}^{G'}(H_0) = 1] - \Pr[\text{Eve}^{G'}(H_n) = 1]| > \delta(n)$
then, $\exists i \in \{0, 1, \dots, n-1\}$ such that $|\Pr[\text{Eve}^{G'}(H_i) = 1] - \Pr[\text{Eve}^{G'}(H_{i+1}) = 1]| > \frac{\delta(n)}{n}$

Hence, for any such $\text{Eve}^{G'}$, if we show that **advantage to distinguish H_i and H_{i+1} is negligible for every i**
then it must hold that the **advantage to distinguish H_0 and H_n is also negligible!**

Is this true?

This conclusion is false!

Note: It seems this example doesn't quite work. Will discuss the fix next class!

$\forall i \in \{0, 1, \dots, n\}: H_i := \begin{cases} 1, & \text{if } i \geq n \\ 0 & \text{otherwise} \end{cases}$

$\forall i, H_i \approx_c H_{i+1}, \because \text{for } n \geq i + 2, \text{ both random variables} = 0$
But clearly H_0 is distinguishable from H_n ! Why?

But note that we never proved theorem 1 using this false claim... Think about what this is saying!

Can we keep stretching?

- [Construction 1](#) can be generalized to work for a $p(n)$ -extension, where p is a polynomial. **WHY?**
- Can you get an exponential stretch?
- What is the loss here?

When $\text{Eve}^{G'}$ distinguishes with probability $\delta(n)$ then Eve^G only distinguishes with probability $\frac{\delta(n)}{p(n)}$
 $\Rightarrow$ More you stretch, greater is the security loss!



Is there a better construction that doesn't result in this much loss?

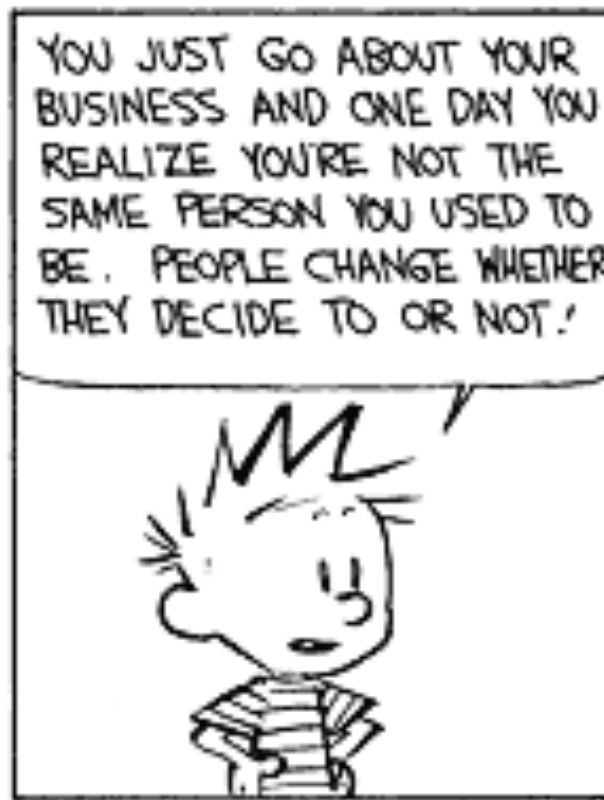
Summary + Next Class

- **SUMMARY**

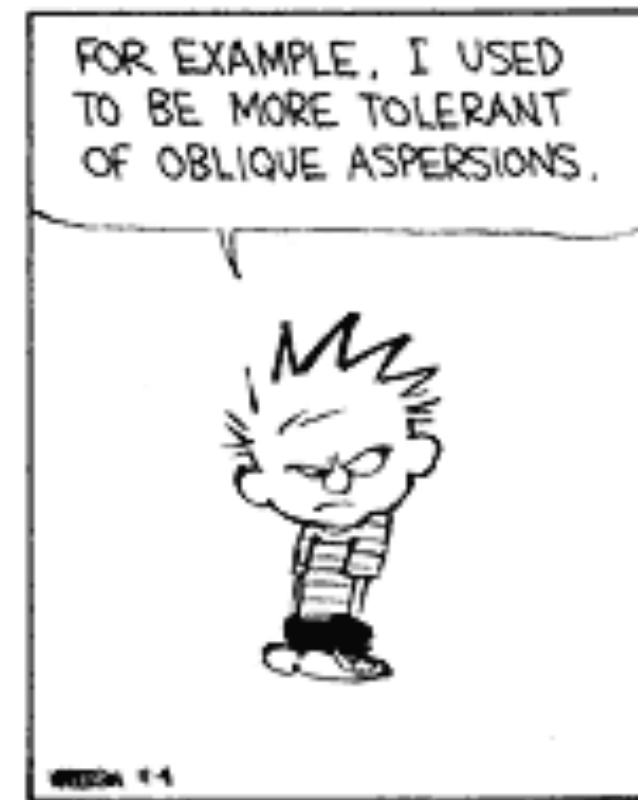
- What have we seen so far?
PRGs (two notions), Extending PRGs, Hybrid Argument
- Computational Indistinguishability of Computational one-time pad
(showed how to overcome the key length drawback of perfect security)

- **NEXT CLASS**

- What about reusing the same key? (overcoming the second drawback of perfect security)
- What about a stronger Eve? (CPA Secure Encryption)
- How do we build stronger schemes? (Pseudorandom Functions, Block ciphers)



© 1995 Universal Press Syndicate



THANK YOU