

# CS171: Cryptography

Lecture 4

Sanjam Garg

# Defining Computationally Secure Encryption (syntax)

- A *private-key encryption scheme* is a tuple of algorithms (Gen, Enc, Dec):
  - $Gen(1^n)$ : outputs a key  $k$  (assume  $|k| > n$ )
  - $Enc_k(m)$ : takes key  $k$  and message  $m \in \{0,1\}^*$  as input; outputs ciphertext  $c$

$$c \leftarrow Enc_k(m)$$

- $Dec_k(c)$ : takes key  $k$  and ciphertext  $c$  as input; outputs  $m$  or “error”

$$m := Dec_k(c)$$

**Correctness:** For all  $n$ ,  $k$  output by  $Gen(1^n)$ ,  $m \in \{0,1\}^*$  it holds that  $Dec_k(Enc_k(m)) = m$

# Computational Indistinguishability

$\text{PrivK}_{A,\Pi}^{\text{eav}}(n)$

1.  $A$  outputs  $m_0, m_1 \in \mathcal{M}, |m_0| = |m_1|$
2.  $b \leftarrow \{0,1\}, k \leftarrow \text{Gen}(1^n), c \leftarrow \text{Enc}_k(m_b)$
3.  $c$  is given to  $A$
4.  $A$  output  $b'$
5. Output 1 if  $b = b'$  and 0 otherwise

Encryption scheme  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$  with message space  $\mathcal{M}$

is ~~perfectly~~ computationally indistinguishable if

$\forall A^{\text{PPT}}$  it holds that:

$$\Pr[\text{PrivK}_{A,\Pi}^{\text{eav}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n)$$

Does not hide message length! A scheme that only supports messages of fixed length is called a fixed-length encryption scheme.

# Constructing Secure Encryption



Pseudorandom Generators (a building block)

# What does it mean to be random?

- Is this string random?
  - 010101010101010101
  - 010100010110101010
- Uniformity is a property of a *distribution* and not a specific *string*.
- A distribution on  $n$ -bit strings is a function  $D: \{0,1\}^n \rightarrow [0,1]$  such that  $\sum_x D(x) = 1$ 
  - For *uniform* distribution on  $n$ -bit strings, denoted  $U_n$ ,  $\forall x \in \{0,1\}^n$  we set  $D(x) = 2^{-n}$

# What about pseudorandomness?

- Intuitively: should be indistinguishable from uniform.
- As before: pseudorandomness is a property of a *distribution* and not a specific *string*

# Pseudorandom Generators PRG

- Stretches a short uniform ``seed'' into a larger ``uniform looking'' larger output
- Useful when only a few random bits are available.

# Pseudorandom Generators

- $G: \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ , where  $\ell(n) > n$



- $G$  is pseudorandom generator if  $\forall$  PPT  $A$  we have  $\exists \text{negl}(\cdot)$  such that,  
$$\left| \Pr_{x \leftarrow U_{\ell(n)}} [A(x) = 1] - \Pr_{s \leftarrow U_n} [A(G(s)) = 1] \right| \leq \text{negl}(n)$$



# PRG (Predicting Game Style)

$\text{PRG}_{A,G}(1^n)$

1.  $b \leftarrow \{0,1\}$ ,
2. If  $b = 0$  set  $x \leftarrow G(U_n)$  else set  $x \leftarrow U_{\ell(n)}$ .
3. Give  $x$  to  $A$
4.  $A$  output  $b'$
5. Output 1 if  $b = b'$  and 0 otherwise

$G$  is a PRG if

$\forall$  PPT  $A$  it holds that:

$$\Pr[\text{PRG}_{A,G}(1^n) = 1] \leq \frac{1}{2} + \text{negl}(n)$$

Seed must be kept secret. Analogous to the secret key in an encryption scheme.

# Fixed-Length Encryption Scheme

Let  $G$  be a  $PRG$ :  $\{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ .

- $Gen(1^n)$ : Choose uniform  $k \in \{0,1\}^n$  and output it as the key

- $Enc_k(m)$ : On input a message  $m \in \{0,1\}^{\ell(n)}$  output the ciphertext

$$c := G(k) \oplus m$$

- $Dec_k(c)$ : On input a ciphertext  $c \in \{0,1\}^{\ell(n)}$  output the message

$$m := G(k) \oplus c$$

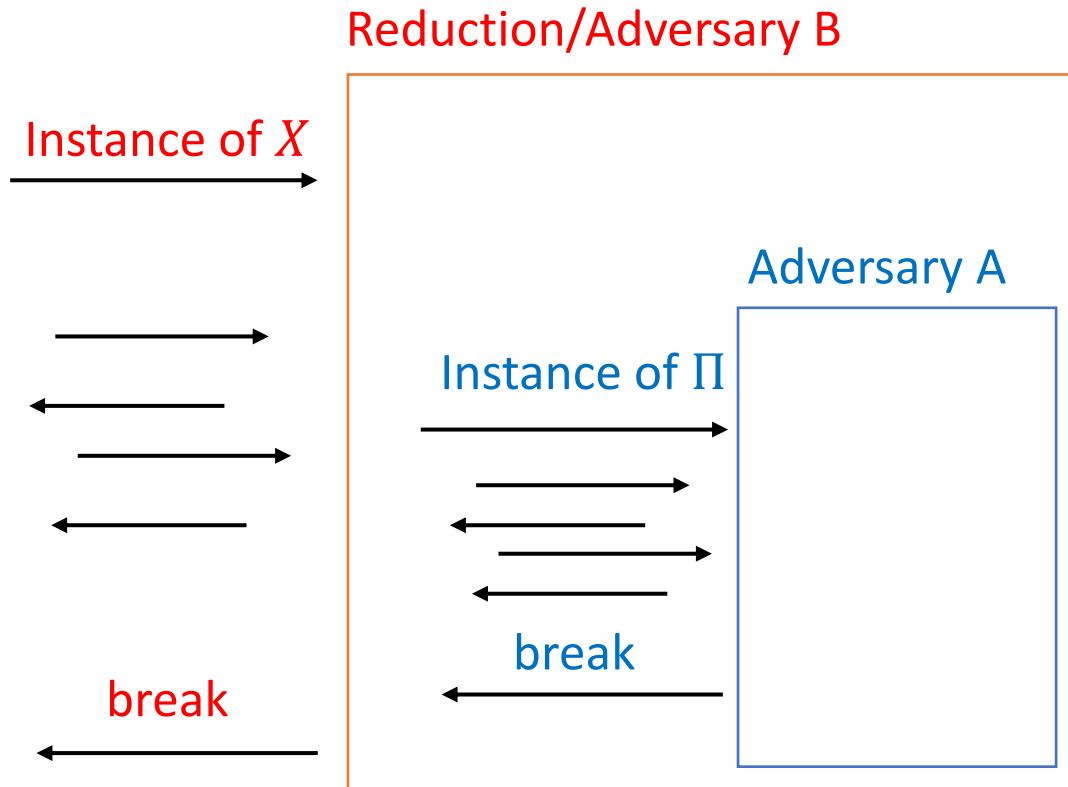
# Proof of Security

Theorem: If  $G$  is a PRG, then this construction is a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.

# Proof by Reduction (If $X$ then $\Pi$ )

- To Prove: If no PPT  $B$  breaks  $X$ , then no PPT  $A$  breaks  $\Pi$
- Assume there exists a PPT  $A$  that “breaks”  $\Pi$ , then we construct PPT  $B$  that “breaks”  $X$
- However, such a  $B$  cannot exist. Thus, our assumption that there exists  $A$  that “breaks”  $\Pi$  must have been false.

# Proof by Reduction (If $X$ then $\Pi$ )



Important:

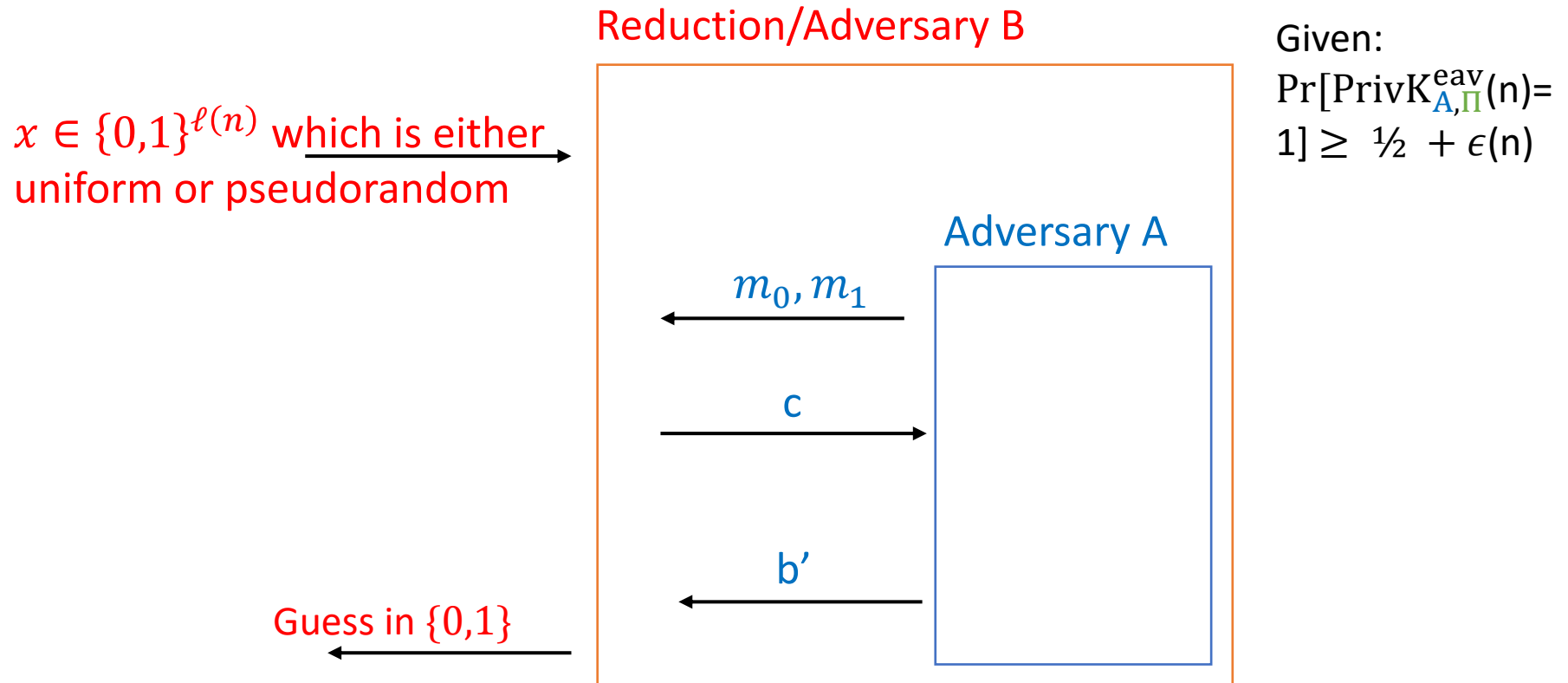
1. View of  $A$ : No change
2.  $B$  is PPT given  $A$  is PPT
3.  $B$  succeeds with degrades wrt.  $A$ 's by  $1/\text{poly}(n)$

# Proof of Security

Theorem: If  $G$  is a PRG, then this construction is a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.

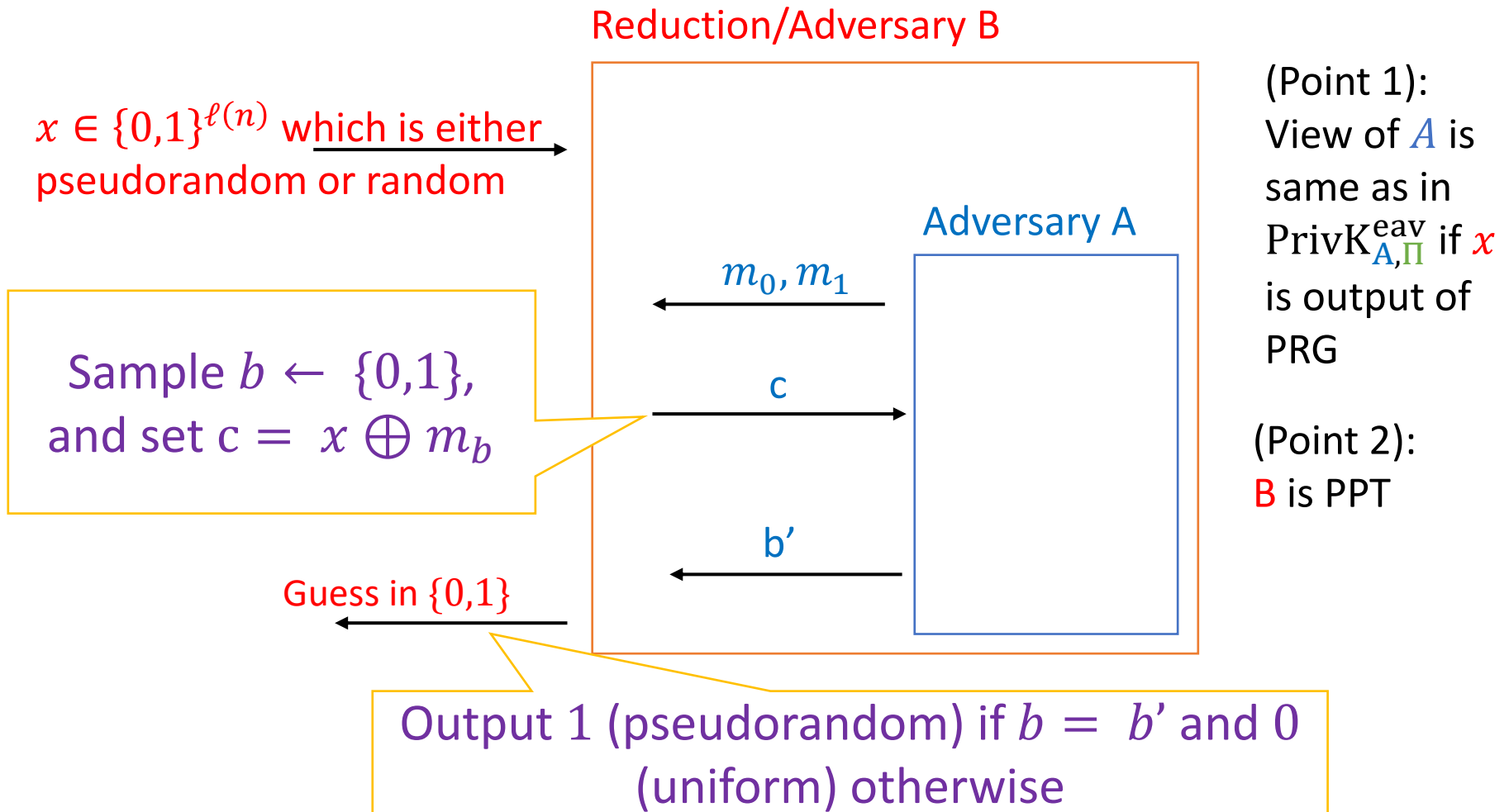
- Proof by reduction: Given a PPT adversary  $A$  ``breaking'' the encryption scheme construct a PPT adversary  $B$  ``breaking'' the PRG

# Proof by Reduction (If *PRG* then Indistinguishable Encryption)



To prove:  $|\Pr[B(G(U_n)) = 1] - \Pr[B(U_{\ell(n)}) = 1]| \geq \delta(n)$

# Proof by Reduction (If *PRG* then Indistinguishable Encryption)





## (Point 3) Success of **B**

1. If **x** is sampled from  $U_{\ell(n)}$ , then  $\Pr[b = b'] = \frac{1}{2}$ .
  - The scheme behaves like a one-time pad.
2. If **x** is sampled from  $G(U_n)$ , then  $\Pr[b = b'] \geq \frac{1}{2} + \epsilon(n)$
3. 
$$\begin{aligned} \Pr[\text{B guesses correct}] &= \\ &\Pr[\text{B guesses correct} \mid \text{x is from } U_{\ell(n)}] + \\ &\Pr[\text{B guesses correct} \mid \text{x is from } G(U_n)] \\ &= \frac{1}{2} \left( \frac{1}{2} \right) + \frac{1}{2} \left( \frac{1}{2} + \epsilon(n) \right) \\ &= \frac{1}{2} + \frac{\epsilon(n)}{2} \end{aligned}$$

# Lessons

- Pseudo OTP is secure
  - Assuming  $G$  is a PRG
  - With respect to our definition
- Gain: Pseudo OTP has a short key
  - $n$  bits instead of  $\ell(n)$  bits
- Does pseudo OTP allow encryption of multiple messages?
  - Let's first define it!

# Practice Question

Step 2: Prove  
 $H$  is not a  
PRG!

- Let  $G: \{0,1\}^n \rightarrow \{0,1\}^{2n}$  be a PRG, then is  
 $H: \{0,1\}^n \rightarrow \{0,1\}^{2n}$  a PRG?

$$H(s) = (s || 0^n) \oplus G(s)$$

For any  $G$ !

- Yes?
- No?

Step 1: Prove  
 $G$  is a PRG!

- No! Let  $F: \{0,1\}^{n/2} \rightarrow \{0,1\}^{3n/2}$  be a PRG then

$$G(s = (s_0, s_1)) = s_0 || F(s_1), \text{ where } s_0, s_1 \in \{0,1\}^{n/2}$$

# Step 1: $G$ is a PRG

- Given:  $F$  is a PRG
- To Prove:  $G(s = (s_0, s_1)) = s_0 || F(s_1)$  is a PRG
- Proof:

1. Assume  $G$  is not a PRG

2.  $\exists A$ , such that  $\left| \Pr_{x \leftarrow U_{2n}} [A(x) = 1] - \Pr_{s \leftarrow U_n} [A(G(s)) = 1] \right| \geq \epsilon(n)$

3.  $\exists A$ , such that  $\left| \Pr_{x \leftarrow U_{2n}} [A(x) = 1] - \Pr_{s_0 \leftarrow U_{\frac{n}{2}}, s_1 \leftarrow U_{\frac{n}{2}}} [A(s_0 || F(s_1)) = 1] \right| \geq \epsilon(n)$

4.  $\exists B$ , such that  $\left| \Pr_{x \leftarrow U_{3n/2}} [B(x) = 1] - \Pr_{s_1 \leftarrow U_{\frac{n}{2}}} [B(F(s_1)) = 1] \right| \geq \epsilon(n)$

5.  $F$  is not a PRG, contradicting the given. Thus,  $G$  must be a PRG.

Step 2:  $H$  is not a PRG

$$\begin{aligned} H(s) &= (s || 0^n) \oplus G(s) \\ &= (s_0 || s_1 || 0^n) \oplus (s_0 || F(s_1)) \\ &= 0^{\overline{2}} || ((s_1 || 0^n) \oplus F(s_1)) \end{aligned}$$

Thank You!

