Cryptography and Security

Lecture 5

Pseudorandom Number Generation and Introduction to Stream Cipher

Lecture slides are adopted from slides of Dan Boneh

Review

- Cipher over (K,M,C): a pair of "efficient" algs (***E***, ***D***) s.t. $\forall\ m \in M, k \in K$: ***D***(k, ***E***(k, m)) = m

- A good cipher: **OTP** $M=C=K=\{0,1\}^n$

  $E(k, m) = k \oplus m$, $D(k, c) = k \oplus c$

- **Lemma: OTP** has perfect secrecy (i.e. no CT only attacks)

- **Bad news:** perfect-secrecy $\Rightarrow$ key-len $\geq$ msg-len

Stream Ciphers: making OTP practical

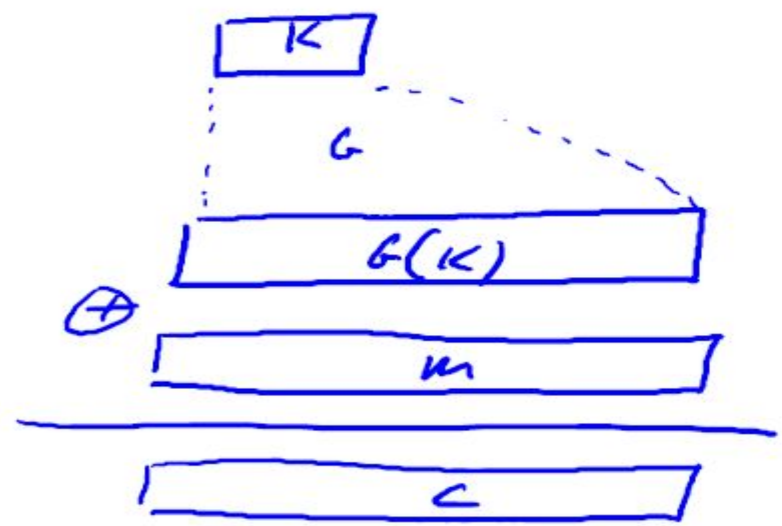
- idea: replace "random" key by "pseudorandom" key.

PRG is a function $G: \underbrace{\{0,1\}^s}_{\text{seed space}} \longrightarrow \{0,1\}^n$ $n \gg s$

(eff. computable by a <u>deterministic</u> algorithm)

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

$D(k,c) = c \oplus G(k)$



Stream Ciphers: making OTP practical

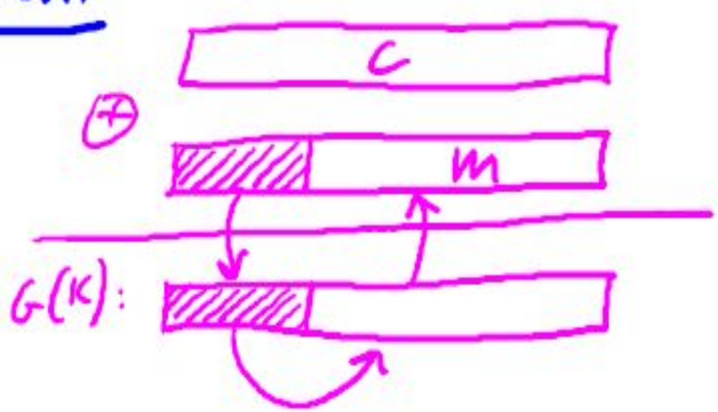
- Stream ciphers cannot have perfect secrecy.
- Need a new definition of perfect secrecy based on specific secrecy.

PRG must be unpredictable

- Suppose PRG is predictable:

  $\exists i: G(K)|_{1,\ldots,i} \rightarrow G(K)|_{i+1,\ldots,n}$

Then:



- Even $G(K)|_{1,\ldots,i} \rightarrow G(K)|_{i+1}$

PRG must be unpredictable

- G: K $\longrightarrow$ $\{0,1\}^n$ is **predictable** if:

$\exists$ "eff" alg. A and $\exists\, 0 \le i \le n-1$ s.t.

$$\Pr_{k \xleftarrow{R} \mathcal{K}}\left[A(G(k))\Big|_{1,\dots,i} = G(k)\Big|_{i+1} \right] > \frac{1}{2} + \varepsilon$$

For non-negligible ε (e.g. $\varepsilon = 1/2^{30}$)

- Def: PRG is **unpredictable** if it is not predictable

$\Rightarrow$ $\forall$ i: no "eff" adv. can predict bit (i+1) for "non-neg" ε

PRG Security Definition

- Let $G: K \longrightarrow \{0,1\}^n$ be a PRG
- Goal: We need to show that

$$[\, k \xleftarrow{R} \mathcal{K},\ \text{output } G(k) \,]$$

is "indistinguishable" from

$$[\, r \xleftarrow{R} \{0,1\}^n,\ \text{output } r \,]$$

Statistical Tests

- **Statistical test** on $\{0,1\}^n$:

  An algorithm A that outputs A(x)=0 when x is not random or outputs A(x)=1 when x is random.

Examples:

(1) $A(x)=1$ iff $\left| \#0(x) - \#1(x) \right| \leq 10 \cdot \sqrt{n}$

(2) $A(x)=1$ iff $\left| \#00(x) - \frac{n}{4} \right| \leq 10 \cdot \sqrt{n}$

(3) $A(x)=1$ iff max-run-of-0$(x) < 10 \cdot \log_2(n)$

Advantage of Statistical Test

- Let $G:K \longrightarrow \{0,1\}^n$ be a PRG and A a stat. test on $\{0,1\}^n$. The advantage of A with respect to G is

$$Adv_{PRG}[A,G] = \left| \Pr_{k \xleftarrow{R} \mathcal{K}} [A(G(k))=1] - \Pr_{r \xleftarrow{R} \{0,1\}^n} [A(r)=1] \right| \in [0,1]$$

- If Adv is close to 1 $\rightarrow$ A can distinguish G(k) from r.
- If Adv is close to 0 $\longrightarrow$ A cannot distinguish G(k) from r.
- Example: A(x)=0 then $Adv_{PRG}[A,G]=0$

Advantage of Statistical Test

- **Example:**

Suppose $G{:}K \longrightarrow \{0,1\}^n$ satisfies **msb(G(k)) = 1** for 2/3 of keys in K

- Define stat. test A(x) as:

if [msb(x)=1] then output "1" else output "0"

- $\mathrm{Adv}_{\mathrm{PRG}}$ [A,G] = | Pr[A(G(k))=1] - Pr[A(r)=1] | = 2/3 - ½ = 1/6.

Secure PRG

- G:K $\longrightarrow\{0,1\}^n$ is a **secure PRG** if

$\forall$ "eff" stat. tests A :

$Adv_{PRG}[A, G]$ is "negligible"

Secure PRG

- Easy fact: **a secure PRG is unpredictable**
- We show: PRG predictable ⇒ PRG is insecure
- Suppose A is an efficient algorithm s.t.

$$\Pr_{k \xleftarrow{R} \mathcal{K}}\left[A(G(k)|_{1,\dots,i}) = G(k)|_{i+1} \right] > \frac{1}{2} + \varepsilon$$

- Define statistical test B as:

$$B(X) = \boxed{\begin{array}{l} \text{if } A(X|_{1,\dots,i}) = X_{i+1} \text{ output } 1 \\ \text{else output } 0 \end{array}}$$

$r \xleftarrow{R} \{0,1\}^n$: $\Pr[B(r)=1] = \frac{1}{2}$

$k \xleftarrow{R} \mathcal{K}$: $\Pr[B(G(k))=1] > \frac{1}{2} + \varepsilon$

$$\Longrightarrow \mathrm{Adv}_{PRG}[B,G] = \left| \Pr[B(r)=1] - \Pr[B(G(k))=1] \right| > \varepsilon$$

Secure PRG

- **Thm (Yao'82): an unpredictable PRG is secure**

- Let $G: K \longrightarrow \{0,1\}^n$ be PRG

- "Thm": if $\forall\ i \in$,0, … , n-1} PRG G is unpredictable at pos. i then G is a secure PRG.

Computational Indistinguishability of Two Distributions

- Let P_1 and P_2 be two distributions over $\{0,1\}^n$
- Def: We say that P_1 and P_2 are **computationally indistinguishable** (denoted $P_1 \approx_p P_2$)

if $\forall$ "eff" stat. tests A

- $\left| \Pr_{x \leftarrow P_1}[A(x)=1] - \Pr_{x \leftarrow P_2}[A(x)=1] \right| <$ negligible

a PRG is secure if $\{ k \longleftarrow K : G(k) \} \approx_p \text{uniform}(\{0,1\}^n)$

Semantic Security

- Goal: secure PRG $\Rightarrow$ "secure" stream cipher
- Attacker's abilities: **obtains one ciphertext**
- Shannon's idea:

  CT should reveal no "info" about PT

Shannon's Perfect Secrecy

Let (E,D) be a cipher over (K,M,C)

- (E,D) has perfect secrecy if $\forall$ m_0, m_1 $\in$ M ($|m_0|$ = |m1|)

  $\{ E(k,m_0) \} = \{ E(k,m_1) \}$ where $k \leftarrow K$

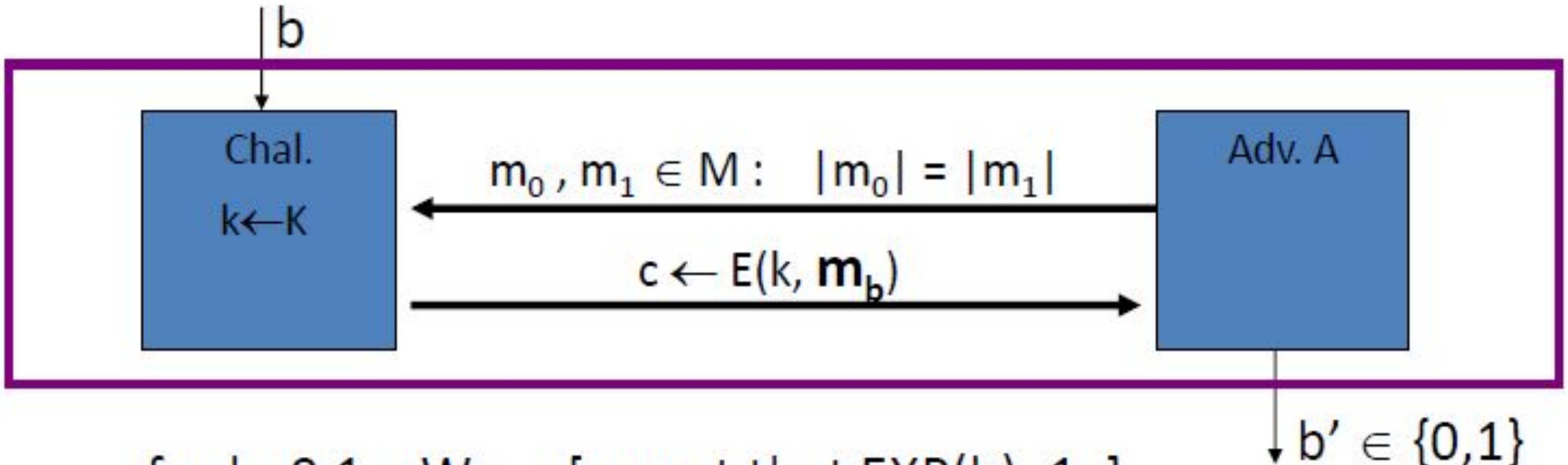
- (E,D) has perfect secrecy if $\forall$ m_0, m_1 $\in$ M ($|m_0| = |m_1|$)

  $\{ E(k,m_0) \}$ **≈p** $\{ E(k,m_1) \}$ where $k \leftarrow K$

- … but also need adversary to exhibit m_0, m_1 $\in$ M explicitly

Semantic Security (one-time key)

For b=0,1 define experiments EXP(0) and EXP(1) as:



for b=0,1: W_b := [event that EXP(b)=1]

$$Adv_{SS}[A,E] := \Big| \Pr[W_0] - \Pr[W_1] \Big| \quad \in [0,1]$$

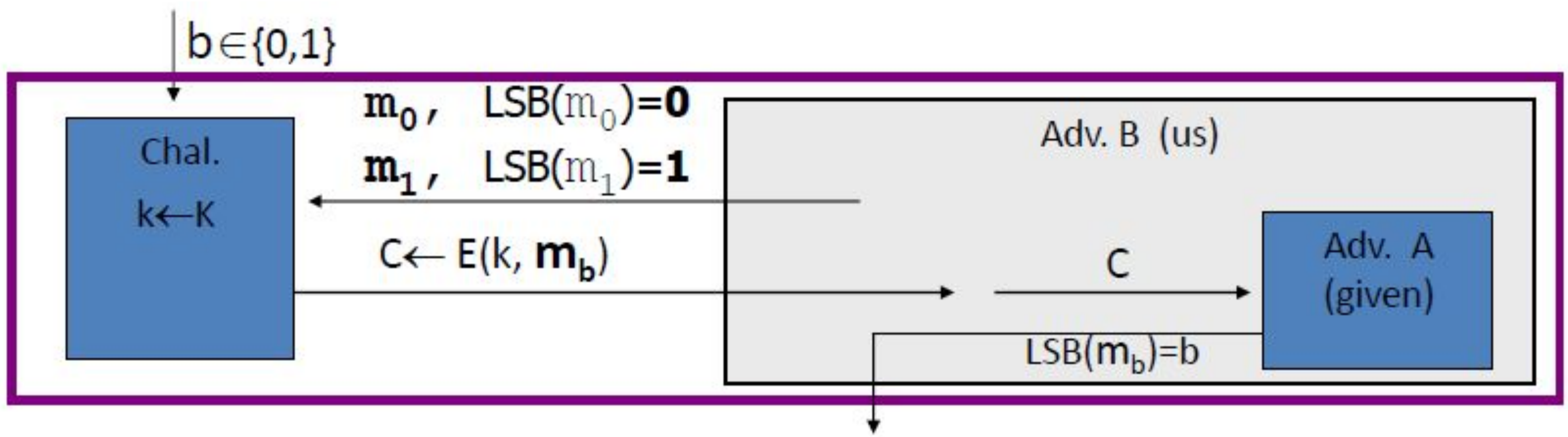
Semantic Security (one-time key)

- E is **semantically secure** if for all efficient A $Adv_{SS}[A,E]$ is negligible.
- $\Rightarrow$ for all explicit m_0 , $m_1 \in M$:

  $\{ E(k,m_0) \}$ **≈p** $\{ E(k,m_1) \}$

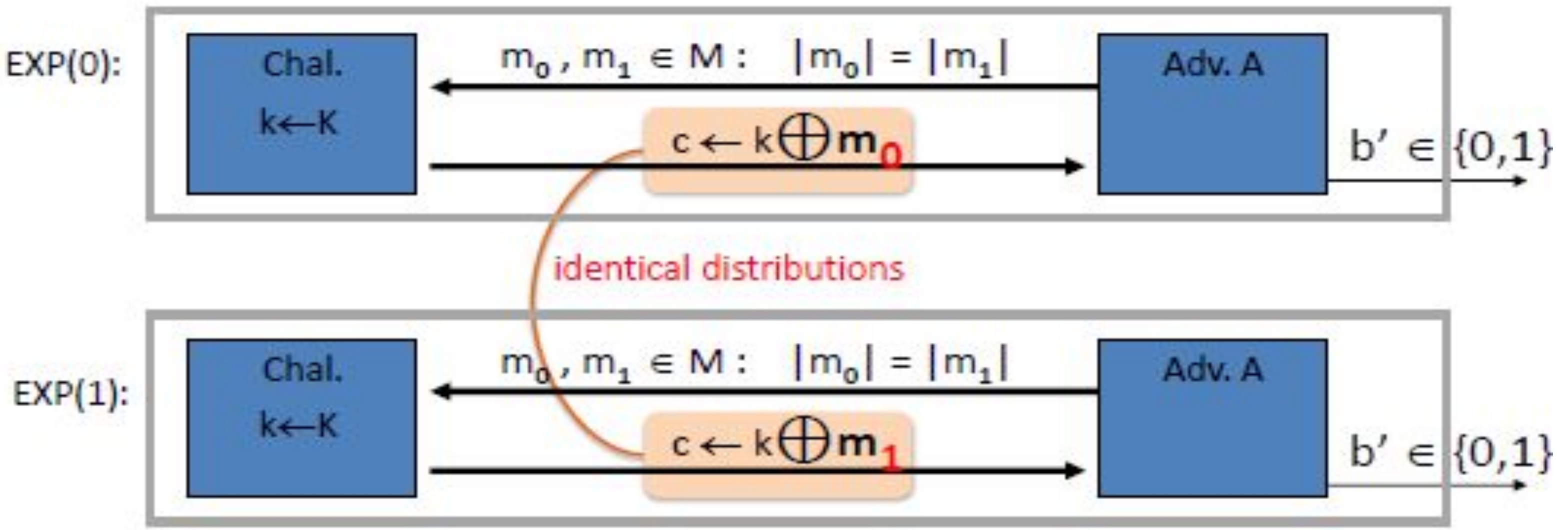
Example

- Suppose efficient A can always deduce LSB of PT from CT.
- ⇒ E = (E,D) is not semantically secure.



$$\mathrm{Adv}_{SS}[B, E] = \left| \Pr[\,\mathbf{EXP(0)}=1\,] - \Pr[\,\mathbf{EXP(1)}=1\,] \right| \quad \mathbf{=0-1=1}$$

OTP is semantically secure



For **all** A: $\mathrm{Adv}_{SS}[A,OTP] = \left| \Pr[A(k \oplus m_0)=1] - \Pr[A(k \oplus m_1)=1] \right|$ **=0**

Stream ciphers are semantically secure

- **Goal:**

  secure PRG ⇒ semantically secure stream cipher

- **Thm:**

  $G:K \longrightarrow \{0,1\}^n$ is a secure PRG ⇒ stream cipher E derived from G is sem. sec.

Prove by Contrapositive:

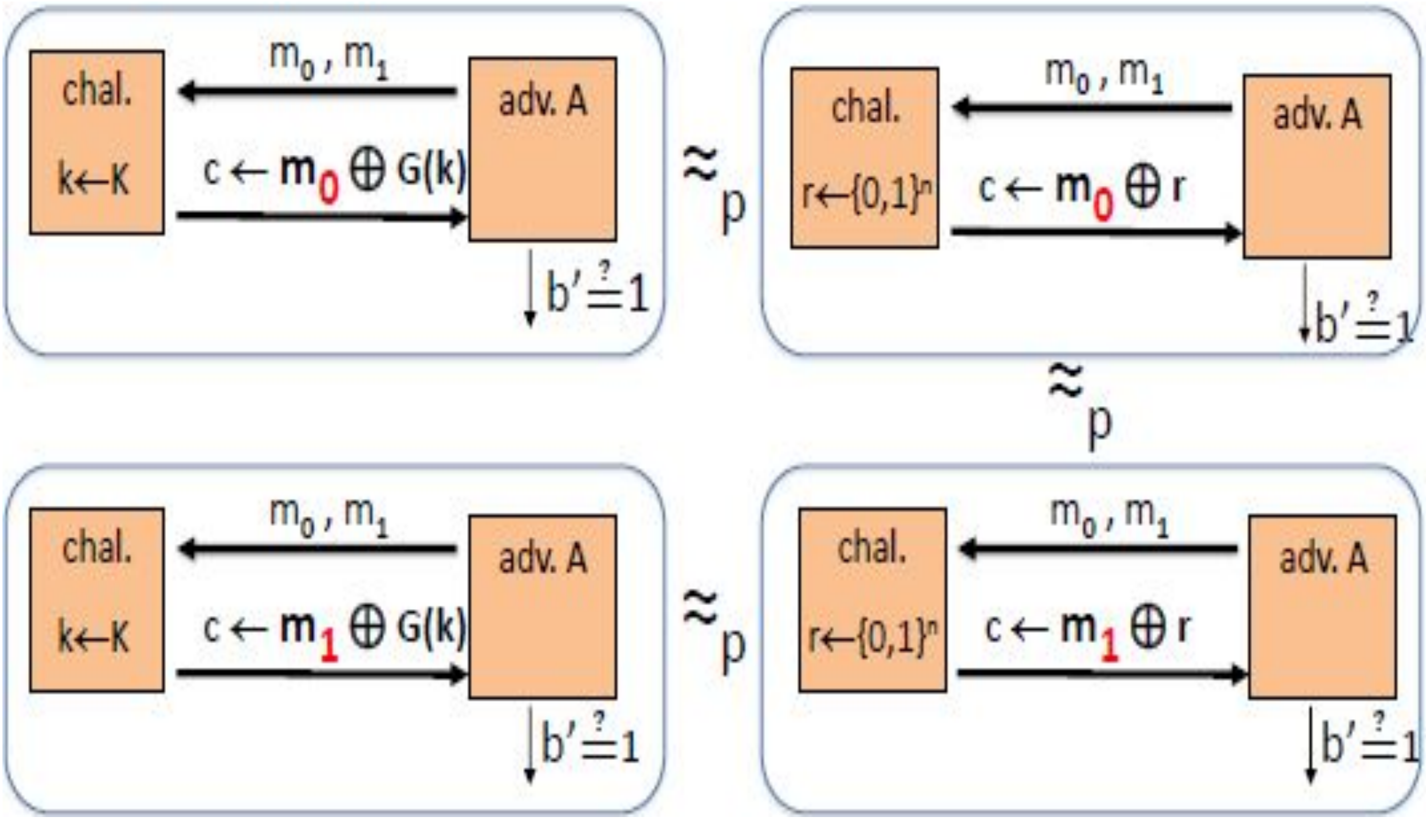
Stream cipher is insecure → PRG used in not secure

∀ sem. sec. adversary A , ∃ a PRG adversary B s.t.

$$\mathbf{Adv_{SS}[A,E] \leq 2 \cdot Adv_{PRG}[B,G]}$$

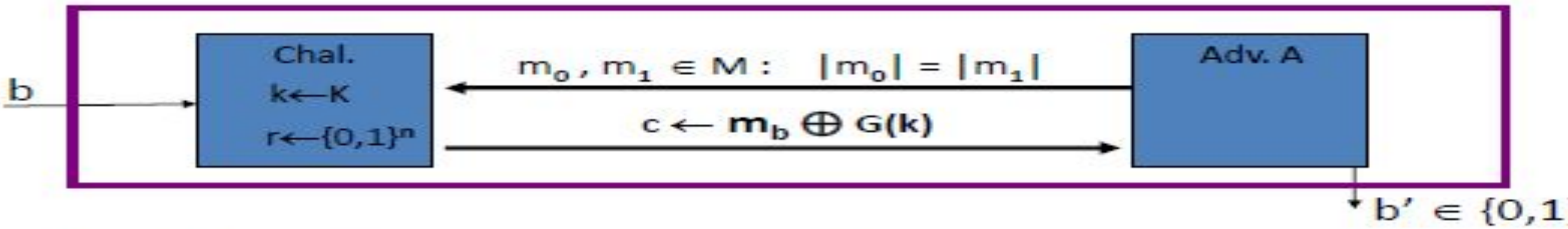
Intuition of Proof

Let A be a semantic security adversary.



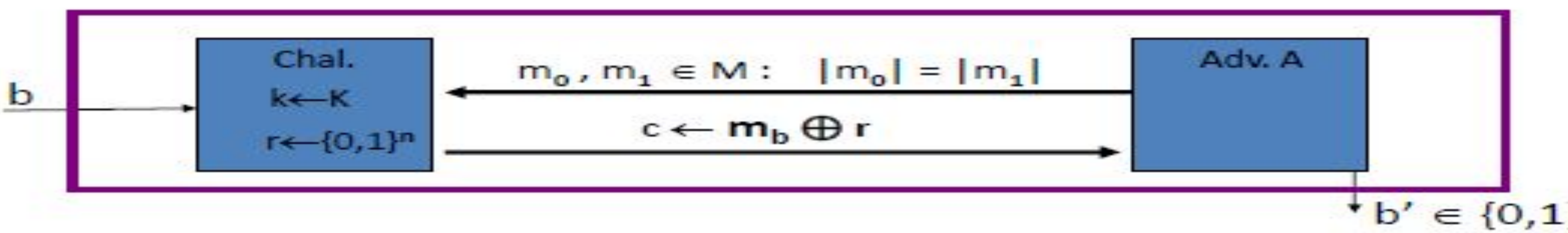
Stream ciphers are semantically secure

Proof: Let A be a sem. sec. adversary.



For b=0,1: W_b := [event that b'=1].

$$\text{Adv}_{SS}[A,E] = \left|\ \Pr[W_0] - \Pr[W_1]\ \right|$$



For b=0,1: W_b := [event that b'=1].

$$\text{Adv}_{SS}[A,E] = \left|\ \Pr[W_0] - \Pr[W_1]\ \right|$$

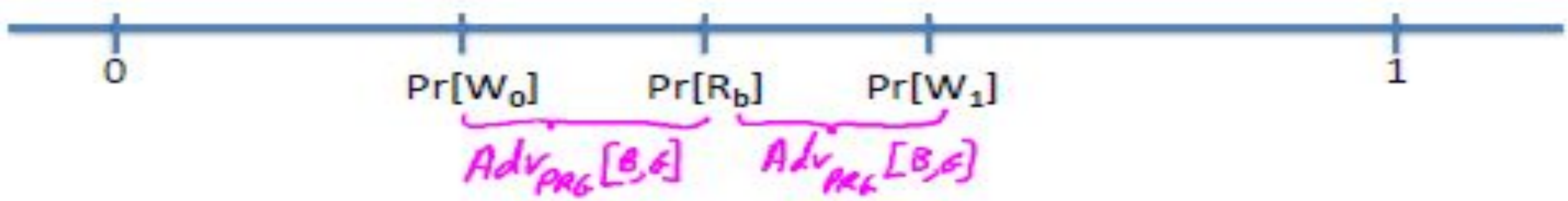
For b=0,1: R_b := [event that b'=1]

Stream ciphers are semantically secure

Proof: Let A be a sem. sec. adversary.

Claim 1: $\left|\Pr[R_0] - \Pr[R_1]\right| = \mathrm{Adv}_{SS}[A, OTP] = 0$

Claim 2: $\exists B$: $\left|\Pr[W_b] - \Pr[R_b]\right| = \mathrm{Adv}_{PRG}[B, G]$ for $b = 0, 1$

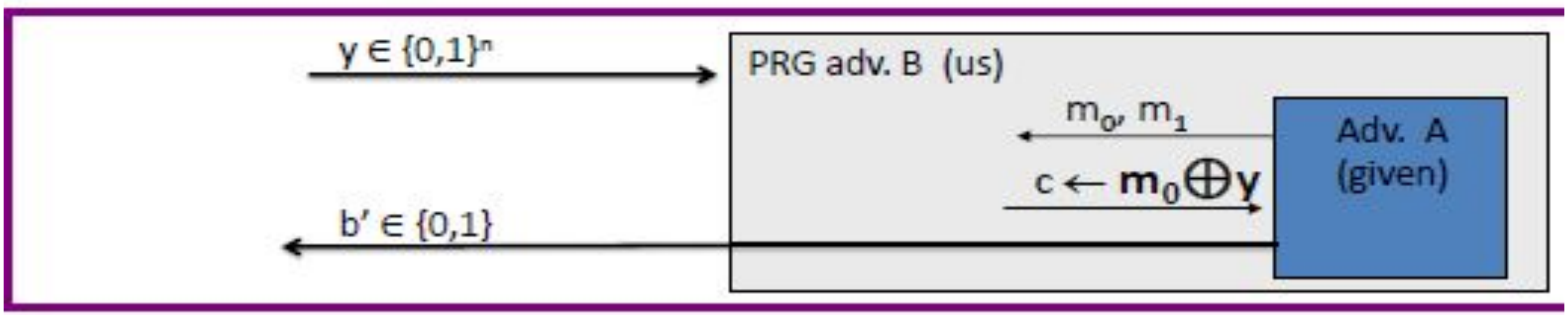


$$\Rightarrow \mathrm{Adv}_{SS}[A,E] = \left|\Pr[W_0] - \Pr[W_1]\right| \le 2 \cdot \mathrm{Adv}_{PRG}[B,G]$$

Stream ciphers are semantically secure

Proof of claim 2: $\exists B$: $\left|\Pr[W_0] - \Pr[R_0]\right| = \mathrm{Adv}_{PRG}[B,G]$

Algorithm B:



$$\mathrm{Adv}_{PRG}[B,G] = \left| \Pr_{r \xleftarrow{R} \{0,1\}^n}[B(r)=1] - \Pr_{k \xleftarrow{R} \mathcal{K}}[B(G(k))=1] \right| = \left| \Pr[R_0] - \Pr[W_0] \right|$$