Stream ciphers

Stream ciphers are semantically secure

Goal: secure PRG ⇒ semantically secure stream cipher

Stream ciphers are semantically secure

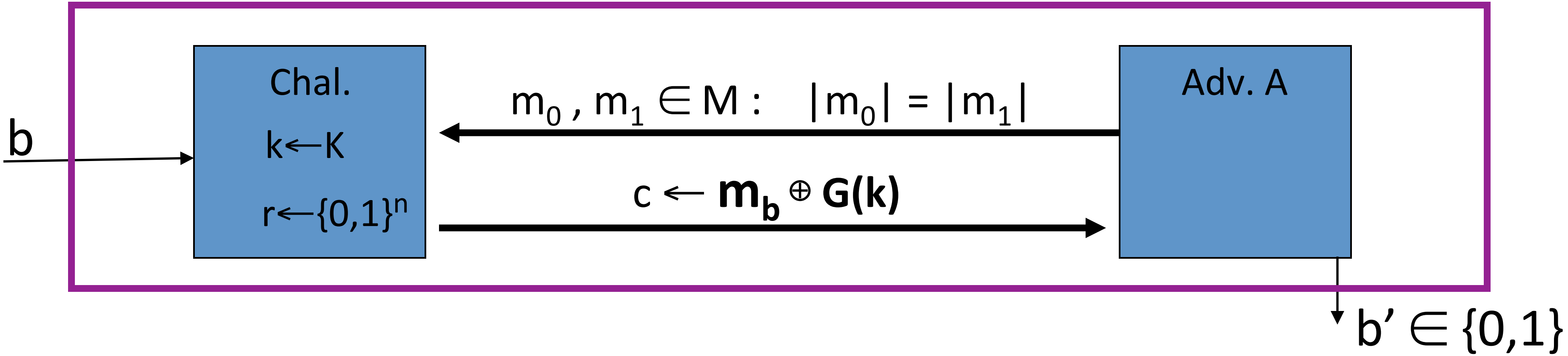
Thm: $G: K \longrightarrow \{0,1\}^n$ is a secure PRG $\Rightarrow$

stream cipher E derived from G is sem. sec.

$\forall$ sem. sec. adversary A , $\exists$ a PRG adversary B s.t.

$$\mathrm{Adv}_{SS}[A,E] \leq 2 \cdot \mathrm{Adv}_{PRG}[B,G]$$

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

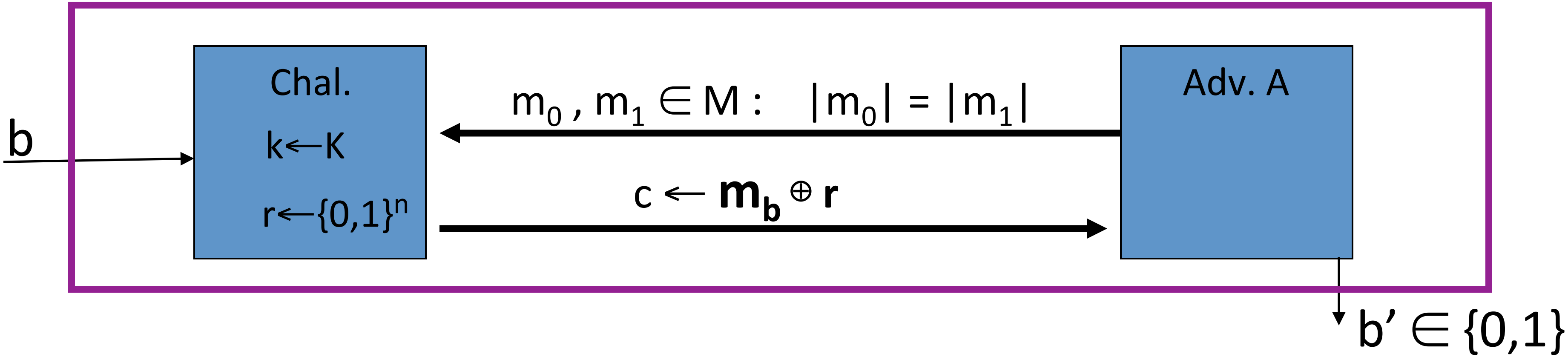


b
Chal.
$k \leftarrow K$
$r \leftarrow \{0,1\}^n$
$m_0, m_1 \in M : \quad |m_0| = |m_1|$
$c \leftarrow \mathbf{m_b} \oplus \mathbf{G(k)}$
Adv. A
$b' \in \{0,1\}$

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

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

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


b
Chal.
$k \leftarrow K$
$r \leftarrow \{0,1\}^n$
$m_0 , m_1 \in M : \quad |m_0| = |m_1|$
$c \leftarrow \mathbf{m_b} \oplus \mathbf{r}$
Adv. A
$b' \in \{0,1\}$

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

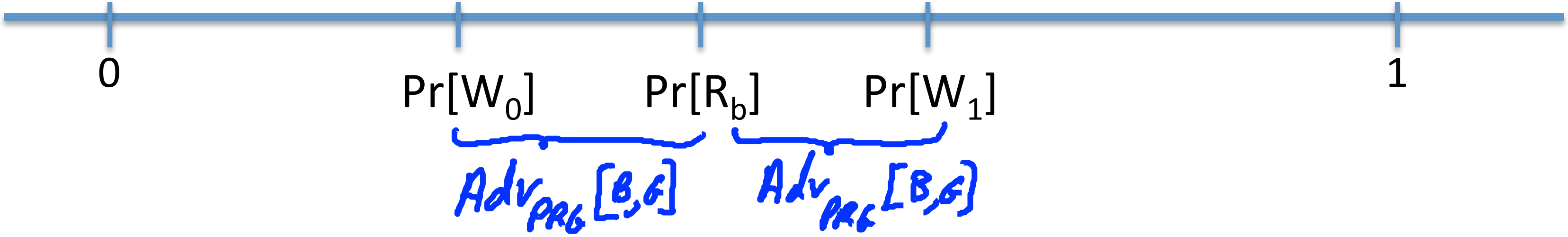
$$\text{Adv}_{SS}[A,E] = \Big|\ \Pr[\ W_0\ ] - \Pr[\ W_1\ ]\ \Big|$$

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

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

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

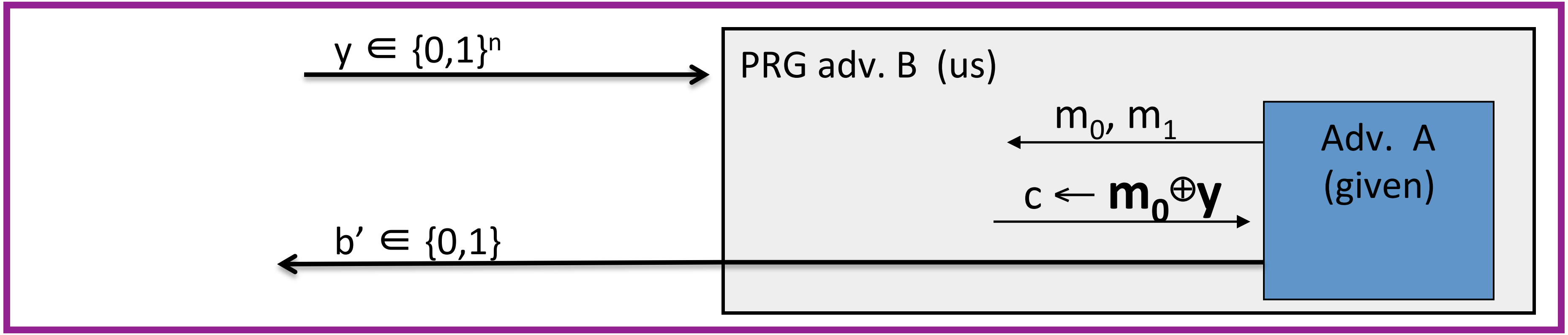
Claim 2: $\exists$ B: $\left|\Pr[W_b] - \Pr[R_b]\right| = \mathrm{Adv}_{PRG}[B, G]$ for $b = 0, 1$



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

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

Algorithm B:



$y \in \{0,1\}^n$

PRG adv. B (us)

m_0, m_1

$c \leftarrow \mathbf{m_0 \oplus y}$

Adv. A (given)

$b' \in \{0,1\}$

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

Dan Boneh

End of Segment