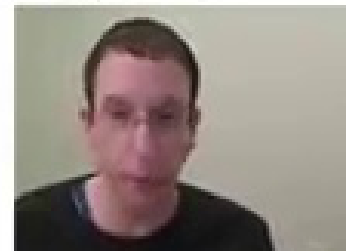




Stream ciphers

Stream ciphers are
semantically secure

Goal: secure PRG \Rightarrow semantically secure stream cipher



Stream ciphers are semantically secure

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

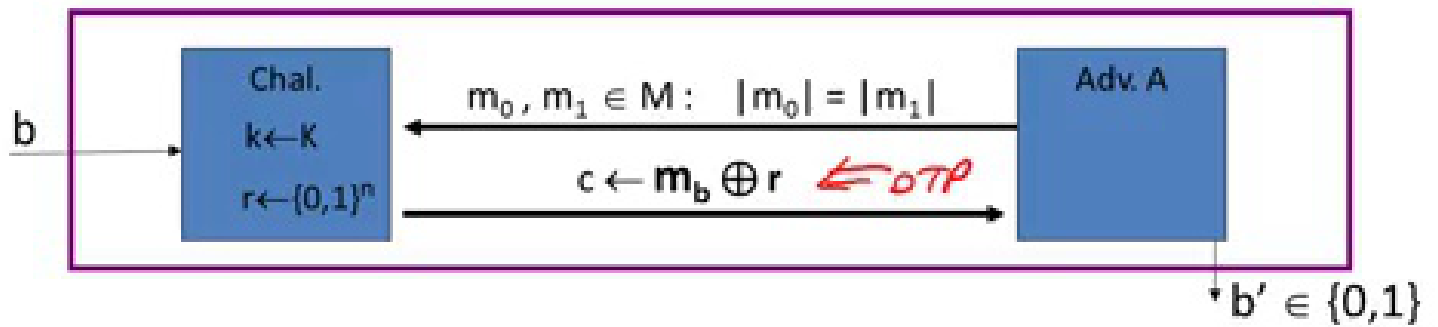
\forall sem. sec. adversary A, \exists a PRG adversary B s.t.

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

neg.

neg.

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



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

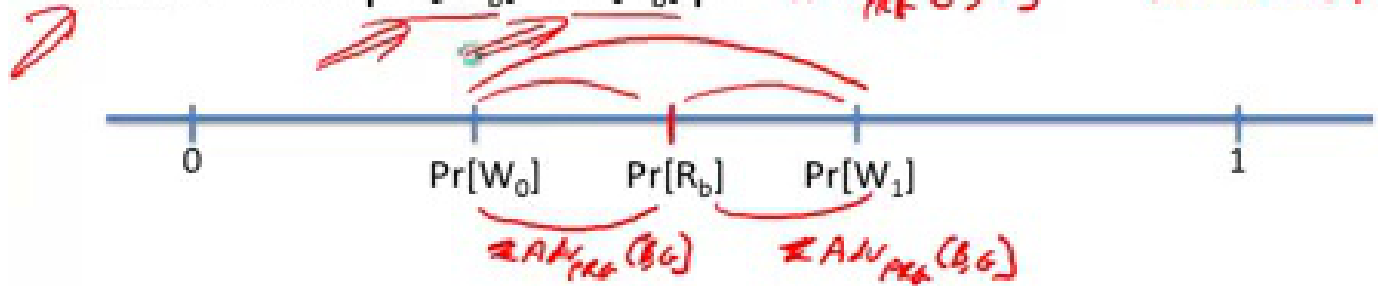
$$\text{Adv}_{\text{SS}}[A,E] = \left| \Pr[W_0] - \Pr[W_1] \right|$$

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

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

Claim 1: $|\Pr[R_0] - \Pr[R_1]| = \text{Adv}_{SS}(A, \text{OTF}) = 0$

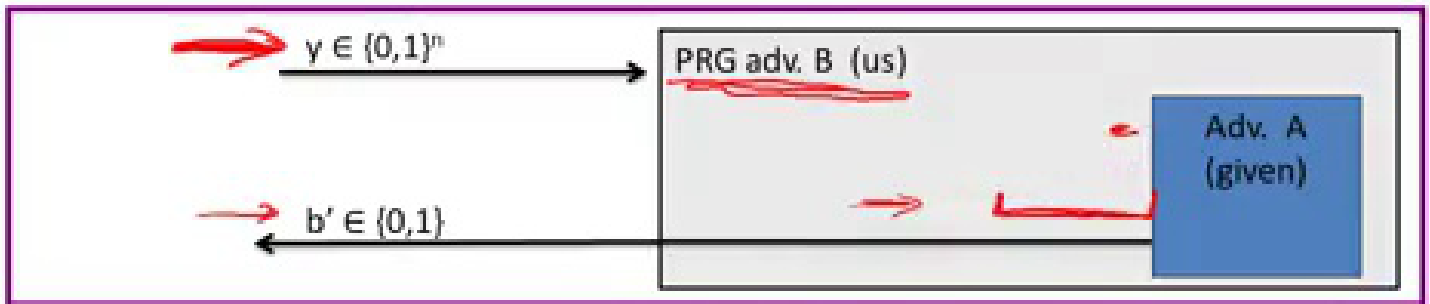
Claim 2: $\exists B: |\Pr[W_b] - \Pr[R_b]| = \text{Adv}_{PRG}(B, G)$ for $b=0,1$



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

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

Algorithm B:

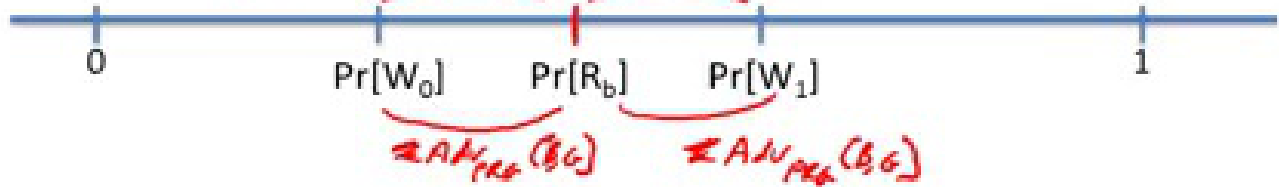


$$\left| \Pr_{k \leftarrow \{0,1\}^n} [B(r)=1] - \Pr_{k \leftarrow \mathcal{R}} [B(k)=1] \right| = \left| \Pr[R_0] - \Pr[W_0] \right|$$

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

Claim 1: $|\Pr[R_0] - \Pr[R_1]| = \text{Adv}_{SS}(A, \text{OTF}) = 0$

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



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

End of Segment