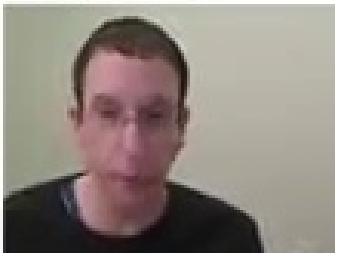
Stream ciphers

Stream ciphers are semantically secure

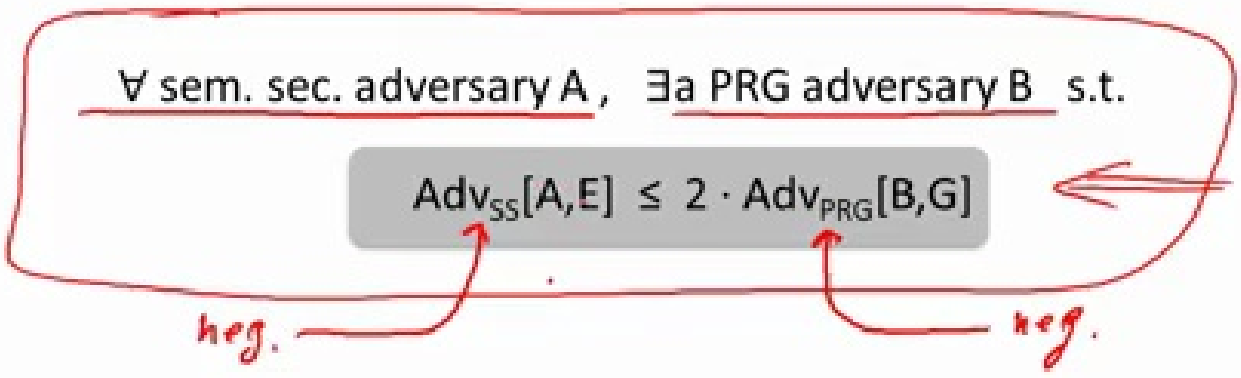


Goal: secure PRG ⇒ semantically secure stream cipher

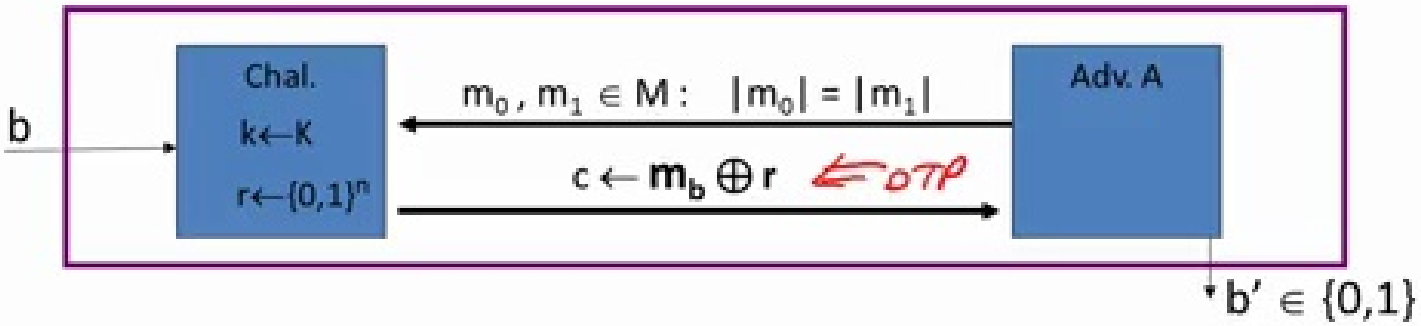
Stream ciphers are semantically secure

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

stream cipher E derived from G is sem. sec.



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



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

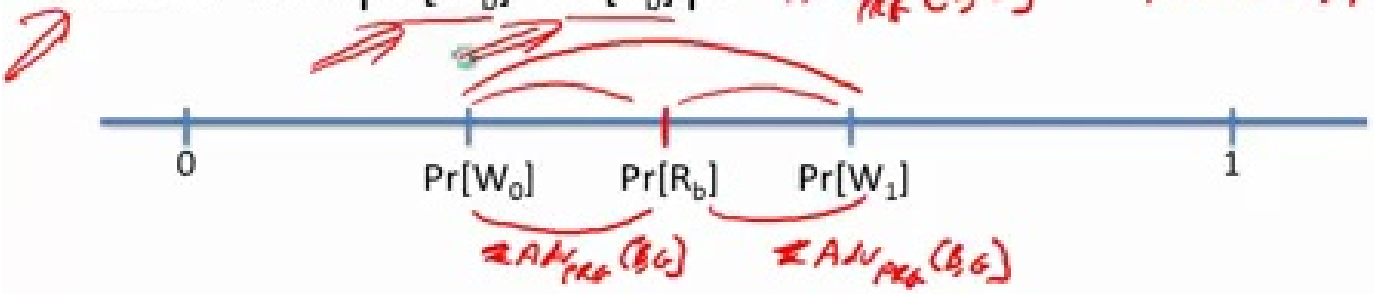
$$Adv_{SS}[A,E] = \left| Pr[W_0] - Pr[W_1] \right|$$

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

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

Claim 1: $\left|\Pr[R_0] - \Pr[R_1]\right| = Adv_{SS}(A, OTP) = 0$

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

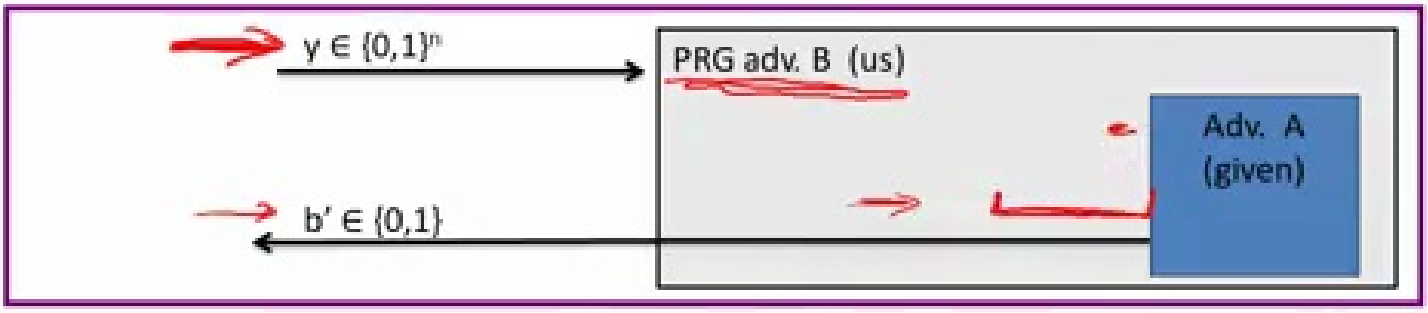


$\Rightarrow$ $Adv_{SS}[A,E] = \left|\Pr[W_0] - \Pr[W_1]\right| \le 2 \cdot Adv_{PRG}[B,G]$

Dan Boneh

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

Algorithm B:

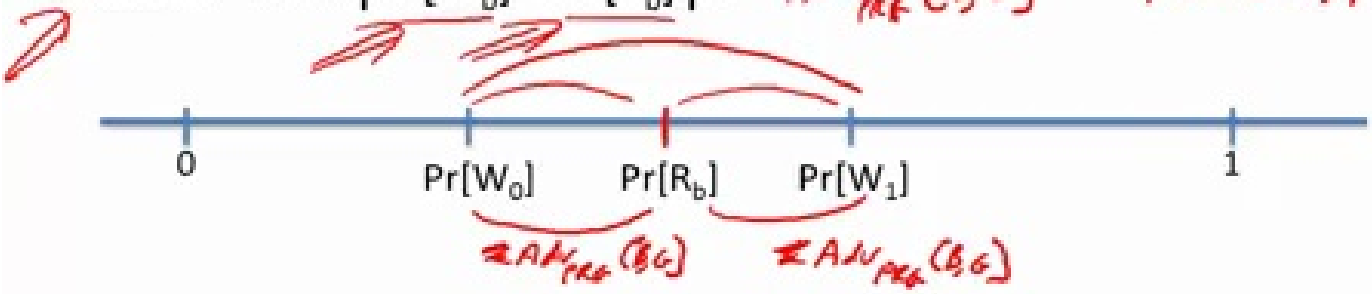


$$\left|\Pr_{k\leftarrow\{0,1\}^n}[B(G(k))=1] - \Pr_{r\leftarrow\{0,1\}^{n'}}[B(r)=1]\right| = \left|\Pr[R_0] - \Pr[W_0]\right|$$

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

Claim 1: $|\Pr[R_0] - \Pr[R_1]| = Adv_{SS}(A, OTP) = 0$

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



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

Dan Boneh

End of Segment