W1 2-7 Stream Ciphers are Semantically Secure

1、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.

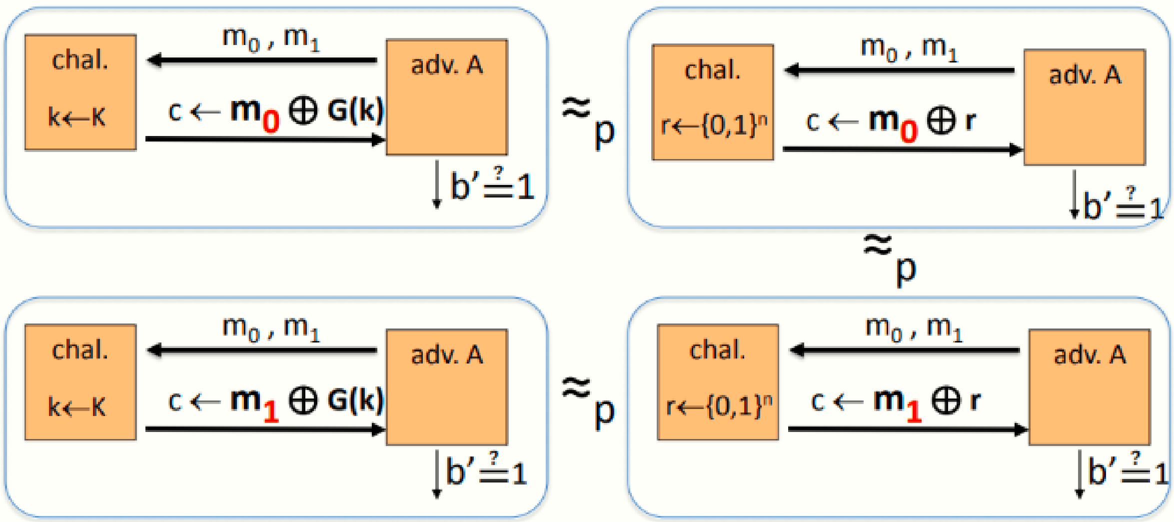
$\forall$ sem. sec. adversary A , $\exists$a PRG adversary B s.t.

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

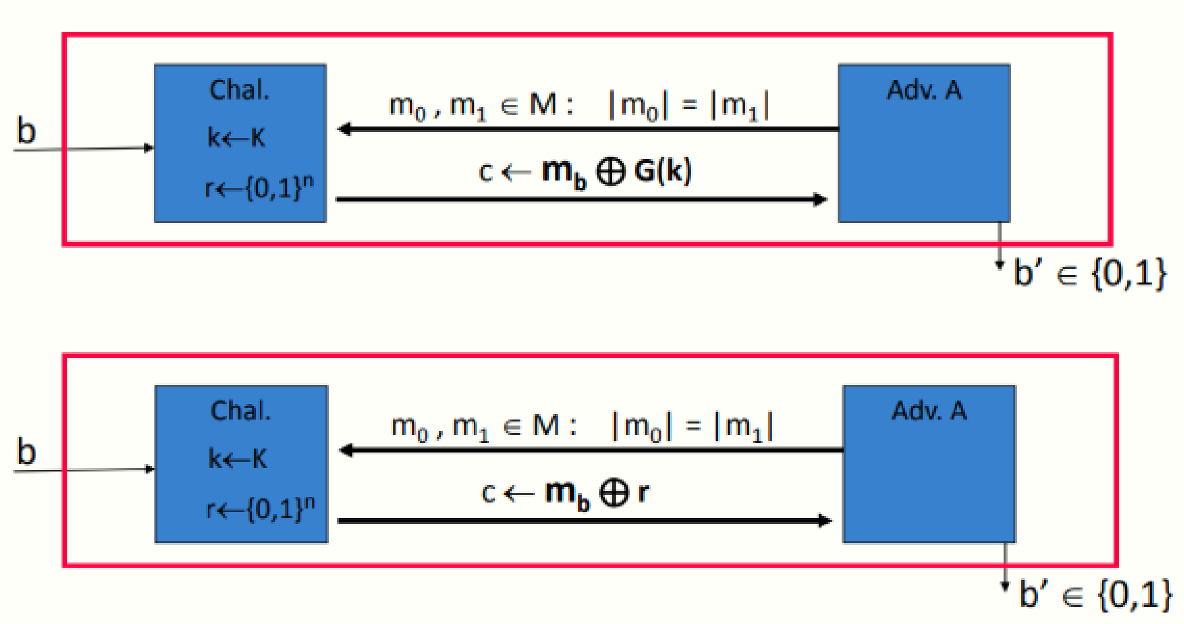
定理：用安全的PRG产生的流密钥进行流加密是语义安全的（语义安全SS，不是香农的完美安全Perfect Security）

2、Proof: intuition

比较直观的证明如下：

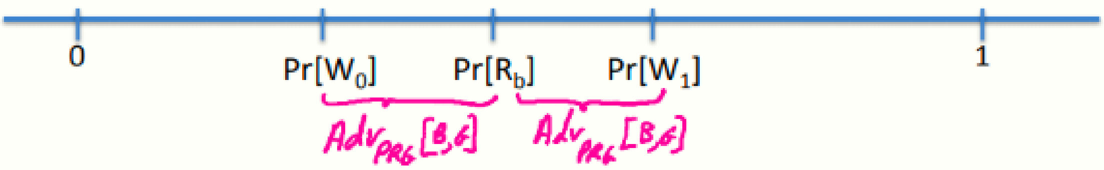


对于真随机串r和PRG生成的串G(k)，如果PRG是安全的，则攻击者无法区分挑战者到底使用的是真随机还是PRG



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 $b=0,1$



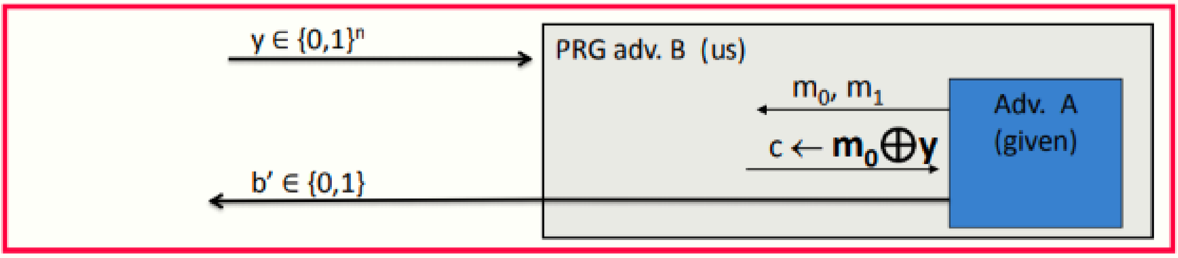
$$\Rightarrow \ Adv_{SS}[A,E] = \left|\Pr[W_0] - \Pr[W_1]\right| \le 2 \cdot Adv_{PRG}[B,G]$$

符号说明：

- W_b：在伪随机密码本下的事件（原始的语义安全游戏的事件）
- R_b：在一次性密码本下的事件（更换为OTP后的游戏的事件）
- A：语义安全的攻击者

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

Algorithm B:



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