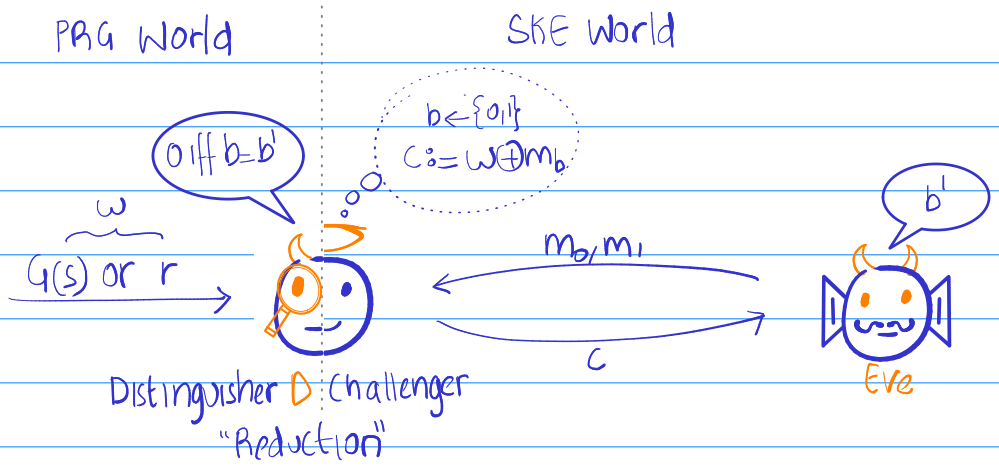
CS409m: Introduction to Cryptography (Aut' 25)

Lecture 05

Instructor: Chethan Kamath

1) **Theorem 1** Assuming G is a PRG, construction 2 is computationally secret against eavesdroppers

Proof. Assume for contradiction that there exists an eavesdropper Eve that breaks secrecy of construction 2. Recall the reduction from Slide 15. The analysis follows.



Since Eve is assumed to break secrecy of construction 2 with non-negligible probability, there exists a polynomial p, such that for infinely many* ns,

$$\Pr\left[\text{Eve}(G(s)\oplus m_b)=b\right]-1/2 \geq 1/p(n) \quad \text{---(1)}$$

$\{0,1\}^{\ell(n)} \ni m_0, m_1 \leftarrow \text{Eve}(1^n)$

$s\leftarrow\{0,1\}^n,\ b\leftarrow\{0,1\}$

On the other hand, by security of OTP, $\forall n\in\mathbb{N}$

$$\Pr\left[\text{Eve}(r\oplus m_b)=b\right]=1/2 \quad \text{---(2)}$$

$m_0, m_1 \leftarrow \text{Eve}(1^n)$

$r\leftarrow\{0,1\}^{\ell(n)},\ b\leftarrow\{0,1\}$

*This is obtained by negating the definition of negligible

"reduction"

Now note that our distinguisher D outputs 0 if and only if Eve correctly guesses b (i.e. $b'=b$) in the reduction.

Therefore for the infinitely-many ns guaranteed above, we get that

$$\left| \Pr_{s\leftarrow\{0,1\}^n}[D(G(s))=0] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D(r)=0] \right|$$

$$= \left| \Pr_{\substack{m_0,m_1\leftarrow Eve(1^n) \\ s\leftarrow\{0,1\}^n,\ b\leftarrow\{0,1\}}}[Eve(G(s)\oplus m_b)=b] - \Pr_{\substack{m_0,m_1\leftarrow Eve(1^n) \\ r\leftarrow\{0,1\}^{\ell(n)},\ b\leftarrow\{0,1\}}}[Eve(r\oplus m_b)=b] \right|$$

$$\geq \left| \underbrace{\tfrac{1}{2}+1/p(n)}_{(1)} - \underbrace{1/2}_{(2)} \right| \geq 1/p(n). \lightning$$

This contradicts the pseudorandomness of G. Thus such an Eve cannot exist ∎