LECTURE 2024/10/11

Last time, PRG definition

$\text{GAME}^{PRG}_{G,A}(\lambda, b)$

$A \xleftarrow{z} \mathcal{C}_{PRG}$

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

$b=0;\ z \in G(s);\ s \leftarrow U_\lambda$

$b=1;\ z \leftarrow U_{\lambda+\ell}$

$\text{GAME}^{PRG}_{G,A}(\lambda,0) \approx_c \text{GAME}^{PRG}_{G,A}(\lambda,1)$

$\forall$ PPT A

$|\Pr[\text{GAME}(\lambda,0)=1] - \Pr[\text{GAME}(\lambda,1)=1]| < negl(\lambda)$

We want to show:

- OWF $\Rightarrow$ PRG
- PRG $\Rightarrow$ SKE (beating Shannon)

① PRG $\Rightarrow$ SKE

assuming

$G : \{0,1\}^\lambda \longmapsto \{0,1\}^{\lambda+\ell}$

simple $\Pi = (\text{ENC}, \text{DEC})$ for $\mathcal{K} = \{0,1\}^\lambda$ (key's space), $\mathcal{M} = \{0,1\}^{\lambda+\ell}$ (message's space)

$\text{ENC}(k,m) = G(k) \oplus m$

$\text{DEC}(k,c) = c \oplus G(k) \oplus m$

Secure SKE against PPT A?

$\text{GAME}^{SKE}_{\Pi,A}(\lambda,b)$

$A \xrightarrow{m_0, m_1 \in \mathcal{M}} \mathcal{C}_{SKE}$

$k \leftarrow U_\lambda$

$\xleftarrow{c}$

$\xrightarrow{b'}$

$c = \text{Enc}(k, m_b)$

2 world: $b=0 \rightarrow$ encrypt m_0

$b=1 \rightarrow$ encrypt m_1

DEF. Π is <u>ONE TIME SECURE</u> if $\text{GAME}^{SKE}_{\Pi,A}(\lambda,0) \approx_c \text{GAME}^{SKE}_{\Pi,A}(\lambda,1)$

Why is it good?

For secure SKE it should be HARD to:

- get the key from c, but $\underbrace{\text{ENC}(k,m)=m}_{\text{stupid encryption}}$ satisfies this!
- get m from c
- get first bit of m from c $\longrightarrow$ Adversary choose the messages
- get ANY info of m!

THM if G is a PRG, then: above Π is ONE TIME SECURE

PROOF We start with original game: GAME $H(\lambda, b)$ — another universe $H'(\lambda, b)$

$A \xrightarrow{m_0, m_1} \mathcal{C}$

$k \leftarrow U_\lambda$ | $z \leftarrow U_{\lambda+\ell}$

$\xleftarrow{c}$ $c = G(k) \oplus m_b$ | $c \leftarrow z \oplus m_b$

$\xrightarrow{b'}$

1. observation: the adv. cannot distinguish m_0 and m_1

Need to show : $H(\lambda, 0) \approx_c H(\lambda, 1)$

LEMMA: $H'(\lambda, 0) = H'(\lambda, 1)$

Follows by PERFECT SECRECY

LEMMA: $\forall\, b \in \{0, 1\}$, $H(\lambda, b) \approx_c H'(\lambda, b)$

PROOF. by reduction. Fix $b = 0$ and assume not

$\exists$ PPT A s.t.

$$|\Pr[H(\lambda, b) = 1] - \Pr[H'(\lambda, b)]| \geq 1/\text{negl}(\lambda)$$

$\exists$ PPT $\mathcal{B}$ "breaking" G

$A \xleftarrow{\text{"STARTING"}} \mathcal{B} \xleftarrow{z} \mathcal{C}_{PRG}$

$$z = \begin{cases} G(k);\ k \leftarrow U_\lambda ; & b = 0 \\ z \leftarrow U_{\lambda+\ell} & b = 1 \end{cases}$$

$\xrightarrow{m_0, m_1}$

$\xleftarrow{c = z \oplus m_0}$

$\xrightarrow{b'}$ $\xrightarrow{b'}$

$\Pr[\mathcal{B} \text{ output } b' = 1 : z = G(s);\ s \leftarrow U_\lambda]$

$= \Pr[\text{GAME}^{PRG}(\lambda, 0) = 1]$

$= \Pr[A \text{ output } b' = 1 : c = G(s) \oplus m_0]$

$= \Pr[H(\lambda, 0) = 1]$

$\Pr[H'(\lambda, 0) = 1] = \Pr[\text{GAME}^{PRG}(\lambda, 1) = 1]$

$$\Rightarrow |\Pr[\text{GAME}^{PRG}_{G,\mathcal{B}}(\lambda, 0) = 1] - \Pr[\text{GAME}^{PRG}_{G,\mathcal{B}}(\lambda, 1) = 1]| \geq \frac{1}{\text{negl}(\lambda)}$$

so A can't exists ■

$$\Rightarrow H(\lambda, 0) \approx_c H'(\lambda, 0) \equiv H'(\lambda, 1) \approx_c H(\lambda, 1) \quad ■$$

(by triangle inequality)