Wednesday, September 1, 2021 3:51 PM

# Using PRG for Encryption

Recall (and fix) PRG definition
$\lambda$ negl($\lambda$) or $\{0,1\}^\lambda$

- A collection of functions

$$\{G_\lambda\}_\lambda : \{D_\lambda\}_\lambda \longrightarrow \{C_\lambda\}$$

true random sample

$$\forall \mathcal{A}. \left| \Pr\left[\begin{array}{c} s \xleftarrow{\$} D_\lambda \\ x \leftarrow G_\lambda(s) \\ b \leftarrow \mathcal{A}(1^\lambda, x) \\ \hline b=0 \end{array}\right] - \Pr\left[\begin{array}{c} x \xleftarrow{\$} C_\lambda \\ b \leftarrow \mathcal{A}(1^\lambda, x) \\ \hline b=0 \end{array}\right] \right| \le \text{negl}(\lambda)$$

This event is about output of Attacker $\mathcal{A}$, not output of PRG

~~Ass~~ A successful distinguisher outputs "0" to guess left, "1" to guess right...
or the other way around

## Symmetric Encryption based on PRG.

Let $\{G_\lambda\} : \{0,1\}^\lambda \longrightarrow \{0,1\}^{2\lambda}$
be length-doubling PRG

codomain: "set of values $G_\lambda$ could output"

Range($G$) is
$\{y \mid \exists x, G(x)=y\}$
$|\text{Range}(G)| \le (\{0,1\}^\lambda)$

$K = \{0,1\}^\lambda$
$M = \{0,1\}^{2\lambda}$

Then:

$\text{Gen}(1^\lambda)$: $k \xleftarrow{\$} \{0,1\}^\lambda$

$\text{Enc}(k, m)$: return $c = m \oplus G(k)$

$\text{Dec}(k, c)$: return $m' = c \oplus G(k)$

Is one time secret.

Claim: $\forall m_1, m_2, \mathcal{A}, \left| \Pr\left[\begin{array}{c} k \leftarrow \text{Gen}() \\ c \leftarrow \text{Enc}(k, m_1) \\ b \leftarrow \mathcal{A}(1^\lambda, c) \\ \hline b=0 \end{array}\right] - \Pr\left[\begin{array}{c} k \leftarrow \text{Gen}() \\ c \leftarrow \text{Enc}(k, m_2) \\ b \leftarrow \mathcal{A}(1^\lambda, c) \\ \hline b=0 \end{array}\right] \right|$

$H_L \overset{?}{\approx} H_R$

$H_L$ $H_R$

by chaining lemma

(by substituting indistinguishable subroutines)

$H_L \overset{\mathrm{I}}{\approx} H_1 \overset{\mathrm{II}}{\approx} H_2 \overset{\mathrm{II}}{\approx} H_3 \overset{\mathrm{I}}{\approx} H_R$

replace PRG w/ real random sample

exactly same distributions

replace ciphertext w/ real random ciphert.

$$H_L = \begin{array}{l} k \leftarrow Gen() \\ c \leftarrow Enc(k, m_1) \end{array} = \begin{array}{l} k \xleftarrow{\$} \{0,1\}^\lambda \\ c = G(k) \oplus m_1 \end{array}$$

$$H_1 = \begin{array}{l} k \xleftarrow{\$} \{0,1\}^\lambda \\ r \xleftarrow{\$} \{0,1\}^{2\lambda} \\ c = r \oplus m_1 \end{array}$$

$H_L \approx H_1$ by substituting rando. for PRG.

here $\underline{c \sim Uniform(\{0,1\}^{2\lambda})}$

$$H_2 = \begin{array}{l} k \xleftarrow{\$} \{0,1\}^\lambda \\ c \xleftarrow{\$} \{0,1\}^{2\lambda} \end{array}$$

also $c \sim$ Uniform

$H_3$ same as $H_1$ but $m_2$ also uniform

$H_R$ = same as $H_L$ but $m_2$

To think about: Q. 5.8

Claim: PRG exists $\Rightarrow$ P != NP

Proof: $\underline{P = NP}$ $\Rightarrow$ No PRG.

$\Leftarrow$ INRANGE$(G, y)$:

$P = NP$ $\Longrightarrow$ return true iff $\exists x \text{ s.t. } G(x) = y$

INRANGE has an efficient solution.

Let $\mathcal{A}(1^\lambda, x)$:

$b \leftarrow$ INRANGE$(G, x)$

return $b$

$\Pr[b = 1]$ in left experiment? $\Pr[b=1]$ right side?

$1.0$

$\leq |\{0,1\}^\lambda| / |\{0,1\}^{2\lambda}| = \frac{1}{2^\lambda}$

# of elements in range of $G$

# of elements in $C_\lambda$