Cryptography

5. Extension of the PRG

$$G : \Sigma^\lambda \to \Sigma^\lambda \qquad\qquad H_n : \Sigma^\lambda \to \Sigma^{(n+1)\lambda}$$

$\underline{H_n(s)}$
$s_o \ := \ s$
$\underline{\text{for}}\ i = 1 \text{ to } n\ \underline{\text{do}}$
$\quad t_i \| s_i \ := \ G(s_{i-1})$
return $t_1 \| t_2 \| ... \| t_n \| s_n$

Theroem:

If G is a (2x) PRG, then H_n is a ((n+1)x) PRG.

$L^G_{PRG-real}$
$\underline{\text{QUERY}()}$
$s \leftarrow \Sigma^\lambda$
return G(s)

$\approx$

$L^G_{PRG-rand}$
$\underline{\text{QUERY}()}$
$r \leftarrow \Sigma^{2\lambda}$
return r

$L^{H_n}_{PRG-real}$
$\underline{\text{QUERY}()}$
$s_0 \leftarrow \{0,1\}^\lambda$
$\underline{\text{for}}\ i = 1 \text{ to } n\ \underline{\text{do}}$
$t_i \| s_i \ := \ G(s_{i-1})$
return $t_1 \| t_2 \| ... \| t_n \| s_n$

$\approx$

Define hybrid-k L

L^H_{hyb-k}
$\underline{\text{QUERY}()}$
$s_0 \leftarrow \{0,1\}^\lambda$
$\underline{\text{for}}\ i = 1 \text{ to } k\ \underline{\text{do}}$
$t_i \| s_i \ := \ \{0,1\}^{2\lambda}$
$t_{k+1} \| s_{k+1} \leftarrow G(s_k)$
$\underline{\text{for}}\ i = k+2 \text{ to } n\ \underline{\text{do}}$
$t_i \| s_i \ := \ G(s_{i-1})$
return $t_1 \| t_2 \| ... \| t_n \| s_n$

$L^H_{hyb-0} \ \equiv \ L^H_{PRG-real}$ (actual H_n)

$\vdots$

$\left.\begin{matrix} L^H_{hyb-k} \\ L^H_{hyb-k+1} \end{matrix}\right\} \approx \qquad \downarrow n - times$

$\vdots$

$L^H_{hyb-n} \ \equiv \ L^H_{PRG-rand}$ ((n+1)λ-bit random output)

L^H_{hyb-k}
$\underline{\textsc{Query}()}$
$s_0 \leftarrow \{0,1\}^\lambda$
$\underline{\text{for}}$ $i = 1$ to k $\underline{\text{do}}$
$t_i \| s_i \ := \ \{0,1\}^{2\lambda}$
$t_{k+1} \| s_{k+1} \leftarrow G(s_k)$
$\underline{\text{for}}$ $i = k+2$ to n $\underline{\text{do}}$
$t_i \| s_i \ := \ G(s_{i-1})$
return $t_1 \| t_2 \| ... \| t_n \| s_n$

$\approx$

$L^H_{hyb-k+1}$
$\underline{\textsc{Query}()}$
$s_0 \leftarrow \{0,1\}^\lambda$
$\underline{\text{for}}$ $i = 1$ to k $\underline{\text{do}}$
$t_i \| s_i \ := \ \{0,1\}^{2\lambda}$
$t_{k+1} \| s_{k+1} \leftarrow \{0,1\}^{2\lambda}$
$\underline{\text{for}}$ $i = k+1$ to n $\underline{\text{do}}$
$t_i \| s_i \ := \ G(s_{i-1})$
return $t_1 \| t_2 \| ... \| t_n \| s_n$

This substitution can be made because $L^G_{PRG-real} \approx L^G_{PRG-rand}$

Therefore the theorem is proved.

6. Pseudorandom Functions

* Stream cipher from PRG ($\leftarrow$ one-time use)
  $G_k() \rightarrow$ □□□.... (pseudorandom keys
  - sequential access only
* "Blockciphers" from a PRF (=pseudorandom function)
  - random-access characteristic

Definition:

A pseudorandom function (PRF)

$$F : \{0,1\}^\lambda \times \{0,1\}^{in} \rightarrow \{0,1\}^{out}$$

is a deterministic function, s.t.

$$L^F_{PRF-real} \approx L^F_{PRF-rand}$$

$L^F_{PRF-real}$
$k \leftarrow \{0,1\}^\lambda$
$\underline{\textsc{Lookup}}(x \in \{0,1\}^{in})$
return F(k,x)

$\approx$

$L^F_{PRF-rand}$
$T \ := \ $ *empty associated array*
$\underline{\textsc{Lookup}(\text{x})}$
if $T[x]$ undefined:
$T[x] \leftarrow \{0,1\}^{out}$
return $T[x]$

For particular key k, F(k,-) is a deterministic function from in-bit strings to out-bit strings.
There are 2^λ such functions.
But in total there are $(2^{out})^{2^{in}} = 2^{out \cdot 2^{in}}$ functions in-bits to out-bits.

Failed attempts to build a PRG

1. $F^*(k,x) := G(k) \oplus x$
   where $k \in \{0,1\}^\lambda$, $G : \{0,1\}^k \to \{0,1\}^{2k}$
   $F^*(k,x) = G(k) \oplus x$
   $F^*(k,y) = G(k) \oplus y$
   $F^*(k,x) \oplus F^*(k,y) = x \oplus y$
   $P[A \diamond L_{real}^{F^*} \to 1] = 1$
   $P[A \diamond L_{rand}^{F^*} \to 1] = 2^{-out}$
   This F^* is distinguishable from random.