Stream ciphers

PRG Security Defs

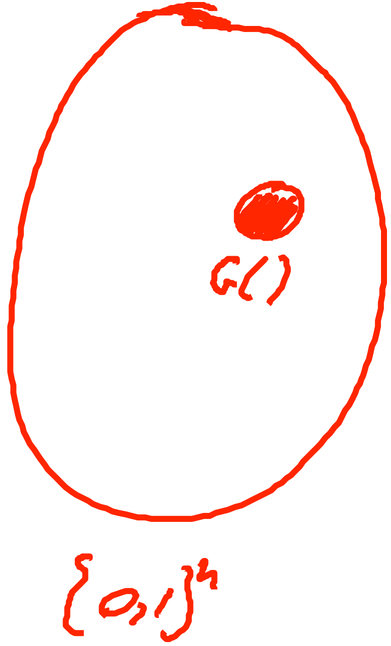
Let $G: K \longrightarrow \{0,1\}^n$ be a PRG

Goal: define what it means that

$[\, k \xleftarrow{R} \mathcal{K},\ \text{output } G(k) \,]$

is "indistinguishable" from

$[\, r \xleftarrow{R} \{0,1\}^n,\ \text{output } r \,]$



Statistical Tests

<u>Statistical test</u> on $\{0,1\}^n$:

an alg. A s.t. A(x) outputs "0" or "1"

not random   random

Examples:

(1) $A(x)=1$ iff $\left| \#0(x) - \#1(x) \right| \le 10 \cdot \sqrt{n}$

(2) $A(x)=1$ iff $\left| \#00(x) - \frac{n}{4} \right| \le 10 \cdot \sqrt{n}$

Statistical Tests

More examples:

(3) $A(x)=1$ iff max-run-of-0$(x) < 10 \cdot \log_2(n)$

$\vdots$

Advantage

Let $G: K \longrightarrow \{0,1\}^n$ be a PRG and A a stat. test on $\{0,1\}^n$

Define:

$$Adv_{PRG}[A,G] := \left| \Pr_{k \xleftarrow{R} \mathcal{K}} \left[A(G(k)) = 1 \right] - \Pr_{r \xleftarrow{R} \{0,1\}^n} \left[A(r) = 1 \right] \right| \in [0,1]$$

Adv close to 1 $\Longrightarrow$ A can dist. G from random

Adv close to 0 $\Longrightarrow$ A cannot

A silly example: $A(x) = 0 \;\Rightarrow\; Adv_{PRG}[A,G] =$

Suppose $G:K \longrightarrow \{0,1\}^n$ satisfies **msb(G(k)) = 1** for 2/3 of keys in K

Define stat. test $A(x)$ as:

if [msb(x)=1] output "1" else output "0"

Then

$$\text{Adv}_{\text{PRG}}[A,G] = \left| \overbrace{\Pr[A(G(k))=1]}^{2/3} - \overbrace{\Pr[A(r)=1]}^{1/2} \right| =$$

Secure PRGs: crypto definition

Def: We say that $G: K \longrightarrow \{0,1\}^n$ is a **secure PRG** if

$\forall$ "eff" stat. tests A :

$Adv_{PRG}[A, G]$ is "negligible"

Are there provably secure PRGs?

but we have heuristic candidates.

Easy fact: a secure PRG is unpredictable

We show: PRG predictable $\Rightarrow$ PRG is insecure

Suppose A is an efficient algorithm s.t.

$$\Pr_{k \xleftarrow{R} \mathcal{K}}\left[A\left(G(k)\big|_{1,\dots,i}\right) = G(k)\big|_{i+1} \right] > \frac{1}{2} + \varepsilon$$

for non-negligible ε (e.g. ε = 1/1000)

Easy fact: a secure PRG is unpredictable

Define statistical test B as:

$$B(x) = \boxed{\begin{array}{l} \text{if } \; A(x|_{1,\dots,i}) = x_{i+1} \; \text{ output } 1 \\ \text{else output } 0 \end{array}}$$

$r \xleftarrow{R} \{0,1\}^n : \quad \Pr[B(r)=1] = \frac{1}{2}$

$r \xleftarrow{R} \mathcal{K} : \quad \Pr[B(G(k))=1] > \frac{1}{2} + \varepsilon$

$\Longrightarrow \; Adv_{PRG}[B,G] = \left| \Pr[B(r)=1] - \Pr[B(G(k))=1] \right| > \varepsilon$

Thm (Yao'82): an unpredictable PRG is secure

Let $G: K \longrightarrow \{0,1\}^n$ be PRG

"Thm": if $\forall\ i \in \{0, \dots, n\text{-}1\}$ PRG G is unpredictable at pos. i
then G is a secure PRG.

If next-bit predictors cannot distinguish G from random
then no statistical test can !!

Let $G: K \longrightarrow \{0,1\}^n$ be a PRG such that

from the last n/2 bits of G(k)

it is easy to compute the first n/2 bits.

Is G predictable for some $i \in \{0, \ldots, n-1\}$?

- ○ Yes
- ○ No

More Generally

Let P_1 and P_2 be two distributions over $\{0,1\}^n$

Def: We say that P_1 and P_2 are

computationally indistinguishable (denoted $P_1 \approx_p P_2$)

if $\forall$ "eff" stat. tests A

$$\left| \Pr_{x \leftarrow P_1}[A(x)=1] - \Pr_{x \leftarrow P_2}[A(x)=1] \right| < \text{negligible}$$

Example: a PRG is secure if $\{ k \xleftarrow{R} K : G(k) \} \approx_p \text{uniform}(\{0,1\}^n)$

End of Segment