Pseudorandom Generator

Chanathip Namprempre

Computer Science
Reed College

Agenda: Pseudorandom Generator

1. What is a PRG?
2. PRG-based stream cipher
3. Unpredictability
4. PRG security notion and statistical tests
5. Examples of PRGs
   - 5.1 Toy
   - 5.2 RC4
   - 5.3 CSS
   - 5.4 eStream: Salsa20
6. PRG security vs. unpredictability

Pseudorandom Generator

Let $n > s$.

$$G : \{0,1\}^s \longrightarrow \{0,1\}^n$$

Use PRG to estimate OTP

$$C \leftarrow G(K) \oplus M$$

Unpredictability is important

Sendmail: fixed format e.g. email messages begin with "From:"

1. Snoop ciphertext C
2. $X \leftarrow C \oplus$ "From:"
3. X is the first part of the output of $G(K)$

Bottom line: If G is predictable, then a small prefix reveals entire message.

PRG security notion and statistical tests

Definition (PRG)

Let s, n be positive integers.

Subroutines

Subroutine `Initialize`
$b \xleftarrow{\$} \{0,1\}$
If $b = 1$
then $x \xleftarrow{\$} \{0,1\}^s$; $y \leftarrow G(x)$
else $y \xleftarrow{\$} \{0,1\}^n$
Return y

Subroutine `Finalize`(d)
Return (d = b)

Experiment

Experiment $\mathbf{Exp}^{\mathrm{prg}}_G(A)$

$y \xleftarrow{\$}$ `Initialize`
$d \xleftarrow{\$} A(y)$
Return `Finalize`

We define the **prg advantage** of an adversary A attacking G as

$$\mathbf{Adv}^{\mathrm{prg}}_G(A) = 2 \cdot \Pr\left[\, \mathbf{Exp}^{\mathrm{prg}}_G(A) \Rightarrow \mathrm{true} \,\right] - 1 \ .$$

Examples

1. Consider generator G such that, for all K,

$$\mathrm{XOR}(G(K)) = 1$$

2. RC4
3. CSS
4. eStream: Salsa20

PRG security vs. Unpredictability

They are equivalent!

Theorem

Let G be a PRG. Then, it is secure if and only if it is unpredictable.

[$\Longrightarrow$] Easy.

[$\Longleftarrow$] Yao.