Pseudo Randomness

Presentation by:
V. Balasubramanian
SSN College of Engineering

Objectives

- Pseudo random Functions

Pseudorandomness

- Important building block for computationally secure encryption

- Important concept in cryptography

What does Random Mean?

- What does "uniform" mean?
- Which of the following is a uniform string?
  - 0101010101010101
  - 0010111011100110
  - 0000000000000000
- If we generate a uniform 16-bit string, each of the above occurs with probability 2^{-16}

Uniform

- "Uniformity" is not a property of a *string*, but a property of a *distribution*

- A distribution on *n*-bit strings is a function D: $\{0,1\}^n \to [0,1]$ such that Σ_x D(x) = 1
  - The *uniform* distribution on *n*-bit strings, denoted U_n, assigns probability 2^{-n} to every $x \in \{0,1\}^n$

Pseudo Random

- Informal: cannot be distinguished from uniform (i.e., random)
- Which of the following is pseudorandom?
  - 0101010101010101
  - 0010111011100110
  - 0000000000000000
- Pseudorandomness is a property of a *distribution*, not a *string*

Contd…

- Fix some distribution D on *n*-bit strings
  - $x \leftarrow D$ means "sample x according to D"
- Historically, D was considered pseudorandom if it "passed a bunch of statistical tests"
  - $\Pr_{x \leftarrow D}[1^{st} \text{ bit of x is } 1] \approx ½$
  - $\Pr_{x \leftarrow D}[\text{parity of x is } 1] \approx ½$
  - $\Pr_{x \leftarrow D}[A_i(x)=1] \approx \Pr_{x \leftarrow U_n}[A_i(x)=1]$ for i = 1, …, 20

Contd...

- This is not sufficient in an adversarial setting!
  - Who knows what statistical test an attacker will use?

- Cryptographic def'n of pseudorandomness:
  - D is pseudorandom if it passes all *efficient* statistical tests

Pseudo Random

- Let D be a distribution on *p*-bit strings
- D is (t, ε)-pseudorandom if for all A running in time at most t,

$$| \Pr_{x \leftarrow D}[A(x)=1] - \Pr_{x \leftarrow U_p}[A(x)=1] | \leq \varepsilon$$

Contd…

- Security parameter *n*, polynomial *p*

- Let D_n be a distribution over *p(n)*-bit strings
- Pseudorandomness is a property of a *sequence* of distributions $\{D_n\} = \{D_1, D_2, \ldots\}$

Contd…

- $\{D_n\}$ is *pseudorandom* if for all probabilistic, polynomial-time distinguishers A, there is a negligible function ε such that

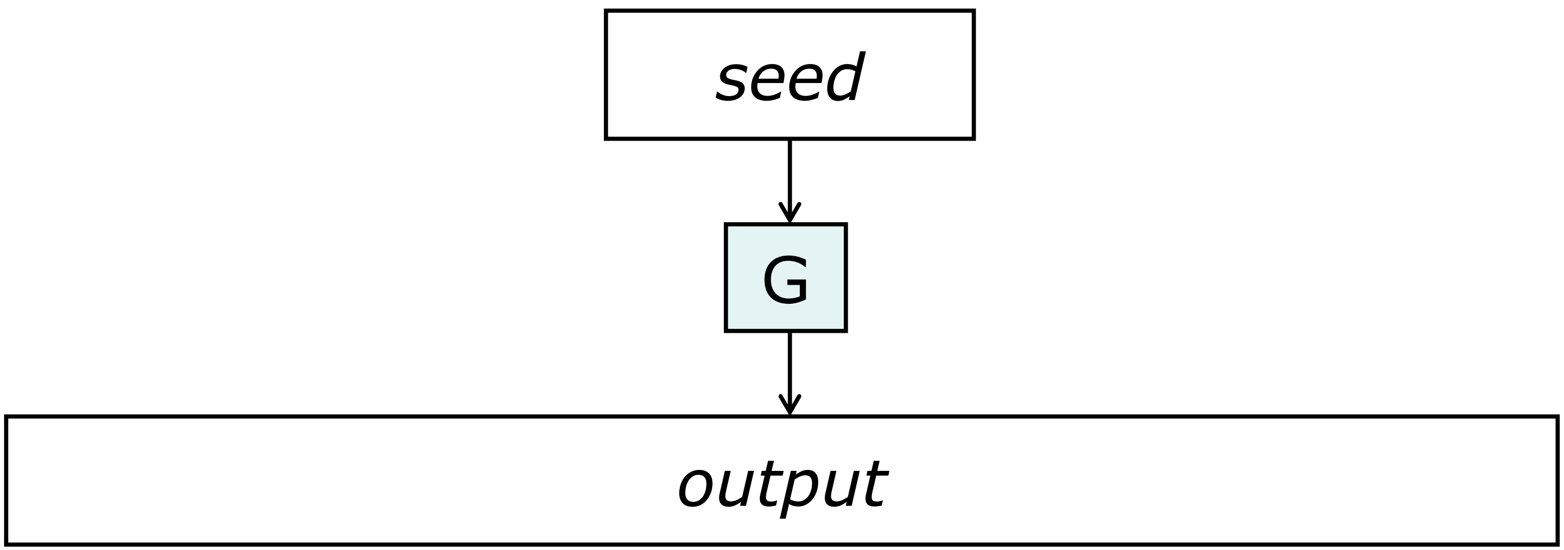
$$\left| \Pr_{x \leftarrow D_n}[A(x)=1] - \Pr_{x \leftarrow U_{p(n)}}[A(x)=1] \right| \leq \varepsilon(n)$$

Pseudo Random Generator

- A PRG is an efficient, deterministic algorithm that expands a *short, uniform seed* into a *longer, pseudorandom* output
  - Useful whenever you have a “small” number of true random bits, and want lots of “random-looking” bits

PRGs

- Let G be a deterministic, poly-time algorithm that is *expanding*, i.e., $|G(x)| = p(|x|) > |x|$



PRGs

- Let G be a deterministic, poly-time algorithm that is *expanding*, i.e., $|G(x)| = p(|x|) > |x|$
- G defines a sequence of distributions!
  - D_n = the distribution on p(n)-bit strings defined by choosing $x \leftarrow U_n$ and outputting G(x)
  - $\Pr_{D_n}[y] = \Pr_{U_n}[G(x) = y] = \Sigma_{x\,:\,G(x)=y} \Pr_{U_n}[x]$
    $= \Sigma_{x\,:\,G(x)=y} 2^{-n}$
    $= |\{x : G(x)=y\}|/2^n$
  - Note that most y occur with probability 0