Cryptography

Lecture 7

Announcements

- HW2 due Monday, 2/26

Agenda

- Last time:
  - Stream Ciphers
  - CPA Security (K/L 3.4)
- This time:
  - Pseudorandom Functions (PRF) (K/L 3.5)
  - CPA-secure encryption from PRF (K/L 3.5)
  - PRP (Block Ciphers) (K/L 3.5)
  - Modes of operation (K/L 3.6)

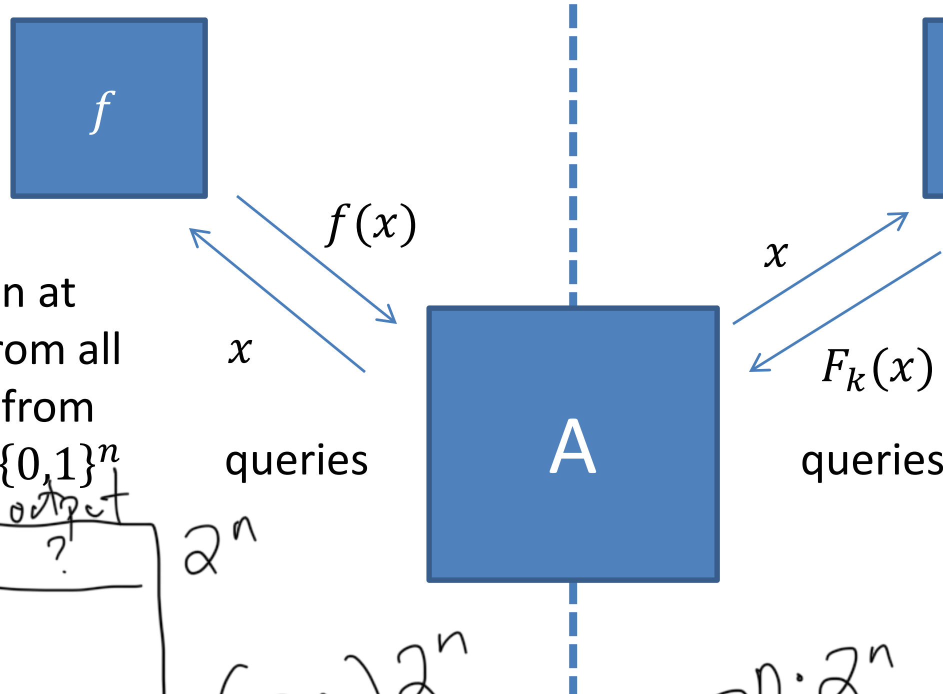
Pseudorandom Function

Definition: A keyed function $F: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ is a two-input function, where the first input is called the key and denoted k.

Pseudorandom Function (PRF)

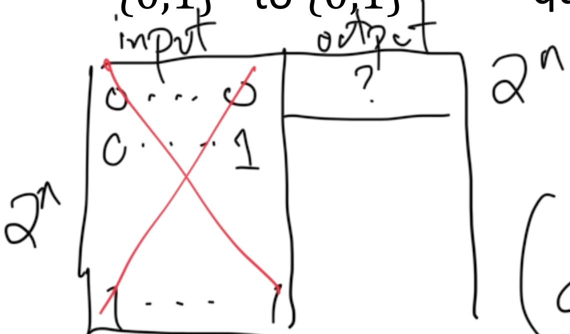
Ideal

Real



f is chosen at random from all functions from $\{0,1\}^n$ to $\{0,1\}^n$

k is chosen at random from $\{0,1\}^n$. F_k is the pseudorandom function indexed by k.



$(2^n)^{2^n} = 2^{n \cdot 2^n}$

$\frac{2^n}{2^{n \cdot 2^n}}$

PRF: Any efficient A cannot tell which world it is in.

$$\left|\Pr[A^f() = 1] - \Pr[A^{F_k}() = 1]\right| \le negligible$$

(x_1, y_1)

(x_2, y_2)

Pseudorandom Function

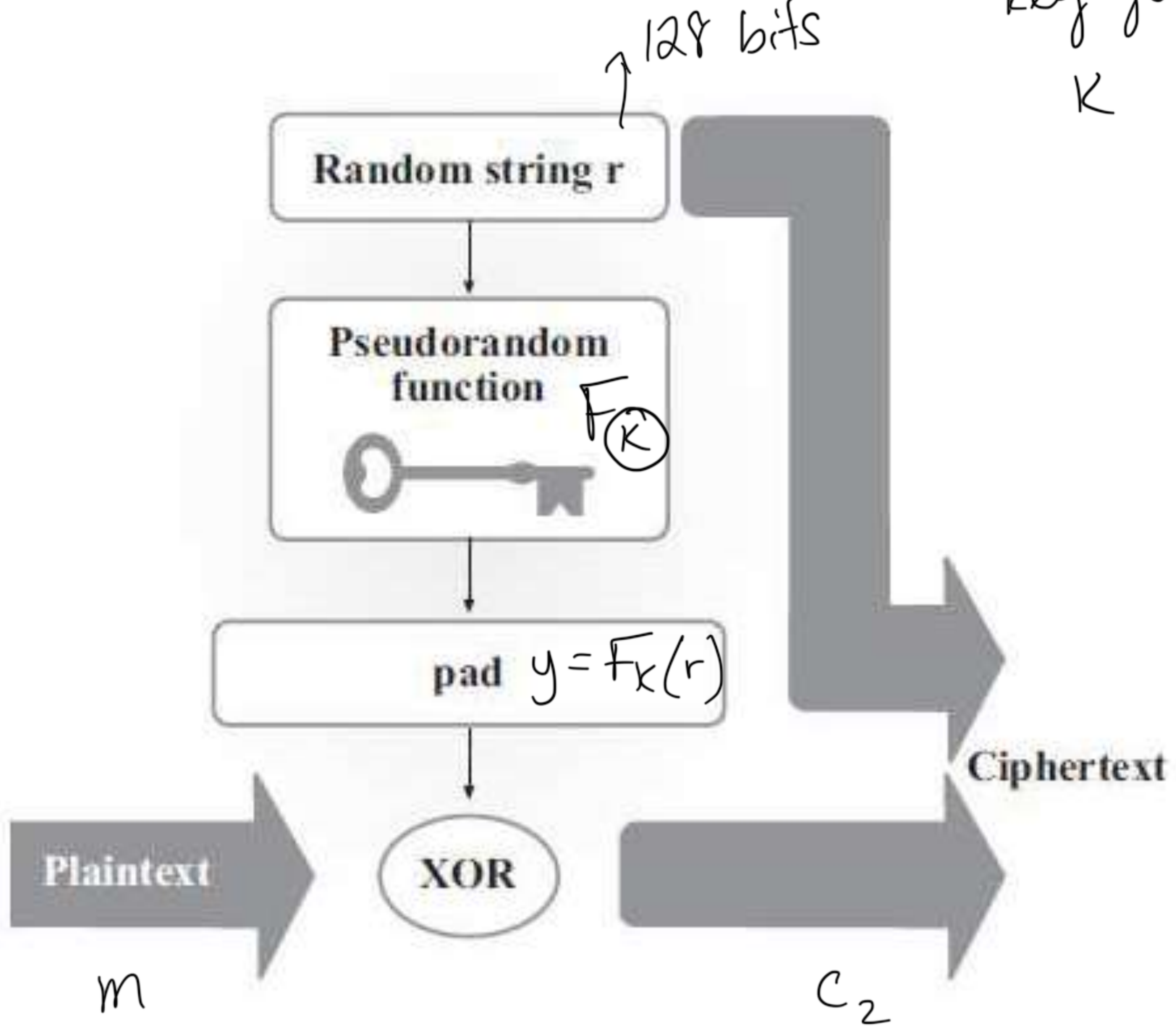
Definition: Let $F: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be an efficient, length-preserving, keyed function. We say that F is a pseudorandom function if for all ppt distinguishers D, there exists a negligible function $negl$ such that:

$$\left|\Pr\left[D^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| \leq negl(n).$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from the set of all functions mapping n-bit strings to n-bit strings.

Construction of CPA-Secure Encryption from PRF

Key gen: random key
K



$c = r \| c_2 \quad (r, c_2)$

Formal Description of Construction

Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:

- Gen: on input 1^n, choose $k \leftarrow \{0,1\}^n$ uniformly at random and output it as the key.
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ uniformly at random and output the ciphertext
$$c := \langle r, F_k(r) \oplus m \rangle.$$
- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the plaintext message
$$m := F_k(r) \oplus s.$$

Security Analysis

Theorem: If $\underbrace{F \text{ is a pseudorandom function}}$, then the Construction above is a $\underbrace{\text{CPA-secure}}$ private-key encryption scheme for messages of length n.

Assume const. not CPA-secure

Prove $\mathbb{F}$ is not a secure PRF

Recall: CPA Security

Consider a private-key encryption scheme $\Pi = (Gen, Enc, Dec)$, any adversary A, and any value n for the security parameter.

Experiment $PrivK^{cpa}_{A,\Pi}(n)$

Adversary $A(1^n)$		Challenger
$A^{Enc_k(\cdot)}$	$\xrightarrow{m'}$	$k \leftarrow Gen(1^n)$
	$\xleftarrow{c'}$	
	$\vdots$	
	$\xrightarrow{m_0, m_1}$	$b \leftarrow \{0,1\}$
	$\xleftarrow{c}$	$c \leftarrow Enc_k(m_b)$
$A^{Enc_k(\cdot)}$	$\xrightarrow{m'}$	
	$\xleftarrow{c'}$	
	$\vdots$	
	$\xrightarrow{b'}$	

$PrivK^{cpa}_{A,\Pi}(n) = 1$ if $b' = b$ and $PrivK^{cpa}_{A,\Pi}(n) = 0$ if $b' \neq b$.

Recall: CPA-Security

Definition: A private-key encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions under a chosen-plaintext attack if for all ppt adversaries A there exists a negligible function $negl$ such that

$$\Pr\left[PrivK^{cpa}{}_{A,\Pi}(n) = 1\right] \leq \frac{1}{2} + negl(n),$$

where the probability is taken over the random coins used by A, as well as the random coins used in the experiment.

non-negl func

$$\exists \text{ ppt } A \text{ s.t. } \Pr\left[PrivK^{cpa}_{A,\Pi}(n) = 1\right] \geq \frac{1}{2} + f(n)$$

Pseudorandom Function

Definition: Let $F: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient, length-preserving, keyed function. We say that F is a pseudorandom function if for all ppt distinguishers D, there exists a negligible function $negl$ such that:

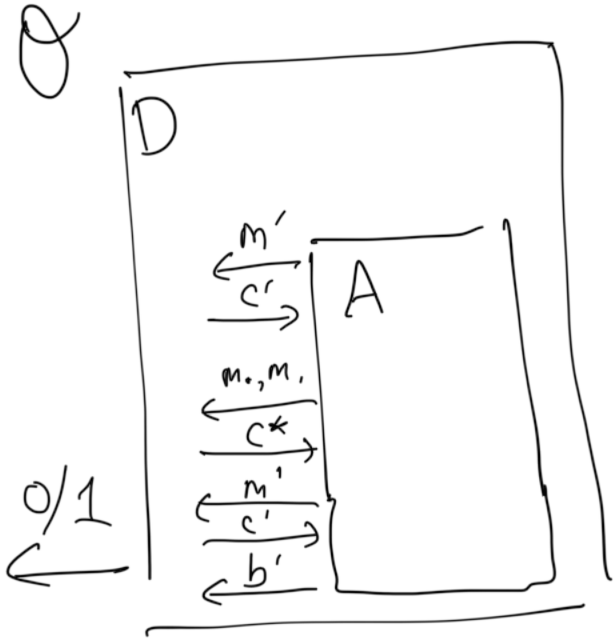
$$\left|\Pr\left[D^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| \leq negl(n).$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from the set of all functions mapping n-bit strings to n-bit strings.

non-negl.

$$\geq f'(n)$$

$$\exists \text{ ppt } D \text{ s.t. } \left|\Pr_{k \leftarrow \{0,1\}^n}\left[D^{F_k(\cdot)}(1^n) = 1\right] - \Pr_{f \xleftarrow{R} \mathcal{F}_n}\left[D^{f(\cdot)}(1^n) = 1\right]\right|$$



1. How to respond to CPA queries

   Choose $r \xleftarrow{R} \{0,1\}^n$

   query r, get back $\mathcal{O}(r)$

   return $c' = (r, \mathcal{O}(r) \oplus m')$

2. How to generate c^*

   Choose bit $b \xleftarrow{R} \{0,1\}$, $r^* \xleftarrow{R} \{0,1\}^n$

   query r^*, get back $\mathcal{O}(r^*)$

   return $c^* = (r^*, \mathcal{O}(r^*) \oplus m_b)$

3. How to determine output given b'

   Output 1 if $b' = b$

   " 0 o/w

Case 1: $\mathcal{O}$ is a PRF

$$\Pr\left[D^{F_k(\cdot)}(1^n) = 1\right] = \Pr\left[\mathrm{PrivK}^{cpa}_{A,\Pi}(n) = 1\right]$$

$$\geq \frac{1}{2} + \rho(n) \quad (\text{non-negl } \rho)$$

Case 2: $\mathcal{O}$ is a random function

$$\Pr\left[D^{f(\cdot)}(1^n) = 1\right] \leq \Pr\left[\text{BAD Event}\right] +$$

$$\Pr\left[D^{f(\cdot)}(1^n) = 1 \mid \neg \text{BAD Event}\right] \quad \frac{1}{2}$$

BAD Event = coll of r^* w/ some r $= \dfrac{q(n)}{2^n}$

Diff. in prob's is at least $p(n) - \underbrace{\boxed{\frac{q(n)}{2^n}}}_{\text{negligible}} = p'(n)$

$p'(n)$ is non-negligible

and D is ppt if A is ppt. $\boxed{\checkmark}$

Security Analysis

Let A be a ppt adversary trying to break the security of the construction. We construct a distinguisher D that uses A as a subroutine to break the security of the PRF.

Distinguisher D:

D gets oracle access to oracle O, which is either F_k, where F is pseudorandom or f which is truly random.

1. Instantiate $A^{Enc_k(\cdot)}(1^n)$.
2. When A queries its oracle, with message m, choose r at random, query $O(r)$ to obtain z and output c $:= \langle r, z \oplus m \rangle$.
3. Eventually, A outputs $m_0, m_1 \in \{0,1\}^n$.
4. Choose a uniform bit $b \in \{0,1\}$. Choose r at random, query $O(r)$ to obtain z and output c $:= \langle r, z \oplus m \rangle$.
5. Give c to A and obtain output b'. Output 1 if $b' = b$, and output 0 otherwise.

Security Analysis

Consider the probability D outputs 1 in the case that O is truly random function f vs. O is a pseudorandom function F_k.

- When O is pseudorandom, D outputs 1 with probability $\Pr\left[PrivK^{cpa}{}_{A,\Pi}(n) = 1\right] = \frac{1}{2} + \rho(n)$, where ρ is non-negligible.
- When O is random, D outputs 1 with probability at most $\frac{1}{2} + \frac{q(n)}{2^n}$, where $q(n)$ is the number of oracle queries made by A. Why?

Security Analysis

D's distinguishing probability is:

$$\left|\frac{1}{2} + \frac{q(n)}{2^n} - \left(\frac{1}{2} + \rho(n)\right)\right| = \rho(n) - \frac{q(n)}{2^n}.$$

Since, $\frac{q(n)}{2^n}$ is negligible and $\rho(n)$ is non-negligible, $\rho(n) - \frac{q(n)}{2^n}$ is non-negligible.

This is a contradiction to the security of the PRF.