Introduction to Cryptology

Lecture 9

Announcements

- HW4 up, due on Tuesday, 3/3
- If you did not receive a grade for HW2 (but handed it in) please see TA
- Substitute on 3/5 (Dr. Feng-Hao Liu)
- Upcoming: Midterm in class on 3/12
  - Review problems and review session
  - Details coming soon

Agenda

- Last time:
  - Construction of SKE from PRG (3.3)
  - Security Analysis of Scheme (3.3)

- This time:
  - CPA security (3.4)
  - Construction of CPA-secure SKE from PRF (3.5)
  - Modes of Operation (3.6)

PRG Example
Similar to Homework Problems

Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$.

Is $G'(s) = G(s||s)$ a pseudorandom generator?

Answer: No.

Intuition: Although s is uniformly distributed, $(s||s)$ is not. Guarantees for PRG hold only when the seed is selected uniformly at random.

PRG Example
Similar to Homework Problems

Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$.
Is $G'(s) = G(s||s)$ a pseudorandom generator?

Answer: No.
To get full credit, must give a counterexample.

1. Define G in terms of *another* PRG G^*
2. Show that G is a secure PRG
3. Show that G' is insecure by presenting a distinguisher.

PRG Example
Similar to Homework Problems

1. Define G in terms of *another* PRG G^*

$$G(s) = G(s_1||s_2) = G^*(s_1 \oplus s_2)$$

(assume G^*has expansion factor $\ell(n) > 4n$.

2. Show that G is a secure PRG
   – Intuition: If $s = s_1||s_2$ is uniformly distributed, then so is $s_1 \oplus s_2$
3. Show that G' is insecure by presenting a distinguisher.
   – Distinguisher $D(\mathrm{w})$ outputs 1 if $w = G^*(0^{n/2})$
   – Otherwise, output 0.

PRG Example
Similar to Homework Problems

$$|\Pr[D(G'(s)) = 1] - \Pr[D(r) = 1]| =$$
$$|\Pr[D(G(s||s)) = 1] - \Pr[D(r) = 1]| =$$
$$|\Pr[D(G^*(s \oplus s)) = 1] - \Pr[D(r) = 1]| =$$
$$\left|\Pr[D\left(G^*(0^{n/2})\right) = 1\right] - \Pr[D(r) = 1]\right| =$$
$$\left|1 - \Pr[r = G^*(0^{n/2})]\right| =$$
$$\left|1 - \frac{1}{2^{\ell(n)}}\right|$$

This is non-negligible and so D is indeed a distinguisher.

New Material

CPA-Security

The CPA Indistinguishability Experiment $PrivK^{cpa}{}_{A,\Pi}(n)$:

1. A key k is generated by running $Gen(1^n)$.
2. The adversary A is given input 1^n and oracle access to $Enc_k(\cdot)$, and outputs a pair of messages m_0, m_1 of the same length.
3. A random bit $b \leftarrow \{0,1\}$ is chosen, and then a challenge ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to A.
4. The adversary A continues to have oracle access to $Enc_k(\cdot)$, and outputs a bit b'.
5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

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.

CPA-security for multiple encryptions

Theorem: Any private-key encryption scheme that has indistinguishable encryptions under a chosen-plaintext attack also has indistinguishable multiple encryptions under a chosen-plaintext attack.

CPA-secure Encryption Must Be Probabilisitic

Theorem: If $\Pi = (Gen, Enc, Dec)$ is an encryption scheme in which Enc is a deterministic function of the key and the message, then Π cannot be CPA-secure.

Why not?

Constructing CPA-Secure Encryption Scheme

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

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.