6.875/18.425J Cryptography and Cryptanalysis March 2, 2005

Handout 5: Problem Set #3

This problem set is due on: Friday, March 11, 2005.

Problem 1 - Yao Security

We consider a definition of security for a public-key cryptosystem proposed by Yao. The idea is that Alice has a polynomial number (n^k) of strings that she wants to send to Bob using as few bits as possible. These strings are selected from a probability distribution known to both Alice and Bob and Alice wants to send enough bits to Bob so that he can (with high probability) reconstruct all of the messages. Note that Alice and Bob are *not* trying to keep any of these messages secret; Alice is just trying to deliver them to Bob as efficiently as possible.

Now suppose that Bob gets encryptions of the messages "for free," in addition to the bits that Alice sends him (however, Bob doesn't know the secret key to decrypt those ciphertexts). We say that a cryptosystem is Yao-Secure if the average number of bits which Alice must send to Bob is the same regardless of whether or not Bob possesses a copy of the ciphertexts. (That is, sharing the ciphertexts does not help Alice compress the messages.)

In the definitions below, we let $M = \{M_n\}$ be a sequence of probability distributions over $\{0,1\}^*$ where M_n only assigns positive probability to n-bit strings. We denote by $\{A_n\}$ a family of probabilistic polynomial-size encoding circuits, and by $\{B_n\}$ a family of probabilistic polynomial-size decoding circuits.

- **The cost of communicating M:**

  We say that *the cost of communicating M is less than or equal to $f(n)$* (in symbols, $C(M) \le f(n)$) if there exist $\{A_n\}$ and $\{B_n\}$ such that the following two properties are satisfied: (for some constant k, for all c, and for all sufficiently large $n\ldots$)

  1. "B_n understands A_n"

  $$\Pr[m_1 \leftarrow M_n; \ldots m_{n^k} \leftarrow M_n; \beta \leftarrow A_n(\vec{\mathbf{m}}); \vec{\mathbf{y}} \leftarrow B_n(\beta) : \vec{\mathbf{m}} = \vec{\mathbf{y}}] > 1 - n^{-c}$$

  2. "A_n transmits at most $f(n)$ bits per message"

  $$E\left[m_1 \leftarrow M_n; \ldots m_{n^k} \leftarrow M_n; \beta \leftarrow A_n(\vec{\mathbf{m}}) : \frac{|\beta|}{n^k}\right] \le f(n)$$

- **The cost of communicating M, given encryptions**:

  Let (G, E, D) be a cryptosystem. We say that *the cost of communicating M, given encryptions using E, is less than or equal to $f(n)$* (in symbols, $C(M|E(M)) \leq f(n)$) if there exist $\{A_n\}$ and $\{B_n\}$ such that the following two properties are satisfied: (for some constant k, for all c, and for all sufficiently large $n \dots$)

  1. "B_n understands A_n"

  $$\Pr[(PK, SK) \leftarrow G(1^n); m_1 \leftarrow M_n; \dots m_{n^k} \leftarrow M_n; c_1 \leftarrow E_{PK}(m_1), \dots, \\ c_{n^k} \leftarrow E_{PK}(m_{n^k}); \beta \leftarrow A_n(\vec{\mathbf{m}}, PK, \vec{\mathbf{c}}); \vec{\mathbf{y}} \leftarrow B_n(\beta, PK, \vec{\mathbf{c}}) : \vec{\mathbf{m}} = \vec{\mathbf{y}}] > 1 - n^{-c}$$

  2. "A_n transmits at most $f(n)$ bits per message"

  $$E\Big[(PK, SK) \leftarrow G(1^n); m_1 \leftarrow M_n; \dots m_{n^k} \leftarrow M_n; \\ c_1 \leftarrow E_{PK}(m_1), \dots, c_{n^k} \leftarrow E_{PK}(m_{n^k}); \beta \leftarrow A_n(\vec{\mathbf{m}}, PK, \vec{\mathbf{c}}) : \frac{|\beta|}{n^k}\Big] \leq f(n)$$

- **Yao-Security**

  We say that a cryptosystem is Yao-secure if for all M, for all c and for all sufficiently large n,

  $$C(M|E(M)) \leq f(n) \Rightarrow C(M) \leq f(n) + \frac{1}{n^c}$$

Part A: Prove that Yao-security implies GM-security. (Use a definition of GM-security in which adversaries are polynomial-size families of circuits.)

Part B: Prove that GM-security implies Yao-security.

Problem 2 - Neighbour Indistinguishability

For this problem, we will always have $M_k = \{0, 1\}^k$. Consider the following potential definition of security:

Neighbour Indistinguishability (NI): This notion aims at capturing the intuition that the encryption of each message (considered as an integer in $\{0, 1, \dots, 2^k - 1\}$) should look like the encryption of the next message:

$$\forall PPT\ A\ \forall c > 0\ \exists k_0\ \forall k > k_0\ \forall m \in \{0,1\}^k \\ \Pr\left[(pk, sk) \leftarrow G(1^k);\ c \leftarrow E_{pk}(m) :\ A(1^k, pk, c) = 1\right] - \\ \Pr\left[(pk, sk) \leftarrow G(1^k);\ c \leftarrow E_{pk}(m + 1 \bmod 2^k) :\ A(1^k, pk, c) = 1\right] < k^{-c}$$

For the problem, prove or carefully disprove each of the following statements.

Part A: Prove or Disprove: Any system which is GM-secure is NI.

Part B: Prove or Disprove: Any system which is NI is GM-secure.

Problem 3 - Non-Uniform Message Spaces

When we discussed one-bit cryptosystems in class, we considered only the message space where a bit is drawn uniformly from $\{0,1\}$. This problem will consider other message spaces for one-bit cryptosystems. Let D_q be the probability distribution over $\{0,1\}$ that assigns probability q to 0 and probability $1-q$ to 1. For $\frac{1}{2} \leq q < 1$, We will say that a public-key cryptosystem (G, E, D) is q-secure if

$$\forall PPT\ A\ \forall c > 0, \exists k_0 \text{ s.t. } \forall k > k_0$$
$$Pr[(PK, SK) \leftarrow G(1^k); b \leftarrow D_q; x \leftarrow E_{PK}(b); g \leftarrow A(1^k, PK, x) : b = g] < q + \frac{1}{k^c}$$

Observe that this is the same definition we discussed in class when $q = 1/2$.

Part A: Prove or Disprove: If a cryptosystem, (G, E, D), is 1/2-secure than it is q-secure for any $1/2 \leq q < 1$.

Part B: Prove or Disprove: If a cryptosystem, (G, E, D), is q-secure for any $1/2 \leq q < 1$ then it is 1/2-secure.

Problem 4 - Active Adversaries

The definition of GM-Security embodies security against a passive adversary who listens to a conversation between Alice and Bob and after hearing the ciphertext, attempts to understand what is being said. In particular, the adversary is not a participant in the system and is not allowed any interaction with Alice and Bob.

Define security against an active adversary. Explain why your definition is good. (In particular, a system satisfying your definition should not be vulnerable to the type of active attack we discussed in class.) Prove that your definition implies GM-Security.