COS 496: Cryptography Due: Oct 9

Problem Set 2

Professor Amit Sahai

Please list everyone you collaborated with when solving the problems on this problem set. If you make use of outside material, make a note of that as well. Make sure you write up your solutions on your own.

Problem 1. In class, we saw the following definition of security for a public-key encryption scheme (G, E, D), which we call *indistinguishability-security*:

For all PPT M, A, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, when we consider the following experiment:

$$\begin{aligned} (PK, SK) &\leftarrow G(1^k) \\ (m_0, m_1, \sigma) &\leftarrow M(PK) \\ b &\leftarrow \{0,1\} \\ c &\leftarrow E(m_b, PK) \\ b' &\leftarrow A(c, PK, \sigma) \end{aligned}$$

we have that $\Pr[b' = b] \leq \frac{1}{2} + \alpha(k)$.

Using a hybrid argument, prove that indistinguishability-security above implies the following definition, which we will call *many-encryption indistinguishability*:

For all PPT M, A, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, when we consider the following experiment:

$$\begin{aligned} (PK, SK) &\leftarrow G(1^k) \\ (m_0, m_1, \sigma) &\leftarrow M(PK) \\ b &\leftarrow \{0,1\} \\ c_1 &\leftarrow E(m_b, PK), c_2 \leftarrow E(m_b, PK), \ldots, c_k \leftarrow E(m_b, PK) \\ b' &\leftarrow A(c_1, c_2, \ldots, c_k, PK, \sigma) \end{aligned}$$

we have that $\Pr[b' = b] \leq \frac{1}{2} + \alpha(k)$.

Can we actually prove this implication without using a hybrid argument explicitly?

Problem 2. For each of the variants of the definition of security below, show that it is either equivalent to the standard definition of security, it is impossible to meet, or that it is too weak to give security because it can be met trivially.

- For all PPT M, A, and all constants q, it is the case that for all sufficiently large k, when we consider the following experiment:

$$\begin{aligned} (PK, SK) &\leftarrow G(1^k) \\ (m_0, m_1, \sigma) &\leftarrow M(PK) \\ b &\leftarrow \{0,1\} \\ c &\leftarrow E(m_b, PK) \\ b' &\leftarrow A(c, PK, \sigma) \end{aligned}$$

we have that $\Pr[b' = b] \leq \frac{1}{2} + 2^{-k^q}$.

- There exists a PPT M, such that for all PPT A, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, when we consider the following experiment:

$$\begin{array}{rcl} (PK, SK) & \leftarrow & G(1^k) \\ (m_0, m_1, \sigma) & \leftarrow & M(PK) \\ b & \leftarrow & \{0,1\} \\ c & \leftarrow & E(m_b, PK) \\ b' & \leftarrow & A(c, PK, \sigma) \end{array}$$

we have that $\Pr[b' = b] \leq \frac{1}{2} + \alpha(k)$.

- For all PPT M, A, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, when we consider the following experiment:

$$\begin{array}{rcl} (PK, SK) & \leftarrow & G(1^k) \\ (c_0, c_1, \sigma) & \leftarrow & M(PK) \\ b & \leftarrow & \{0,1\} \\ b' & \leftarrow & A(c_b, PK, \sigma) \end{array}$$

we have that $\Pr[b' = b] \leq \frac{1}{2} + \alpha(k)$.

- For all PPT A, M, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, if we consider the following two experiments:

$$\begin{array}{l} Expt_{RealLife}: \\ \begin{array}{rcl} (PK, SK) & \leftarrow & G(1^k) \\ (m_0, m_1, \sigma) & \leftarrow & M(PK) \\ b & \leftarrow & \{0,1\} \\ c & \leftarrow & E(m_b, PK) \\ b' & \leftarrow & A(c, PK, \sigma) \end{array} \end{array}$$

and

$$\begin{array}{l} Expt_{WeirdWorld}: \\ \begin{array}{rcl} (PK, SK) & \leftarrow & G(1^k) \\ (m_0, m_1, \sigma) & \leftarrow & M(PK) \\ b & \leftarrow & \{0,1\} \\ t & \leftarrow & \{0,1\} \\ c & \leftarrow & E(m_t, PK) \\ b' & \leftarrow & A(c, PK, \sigma) \end{array} \end{array}$$

then we have that $\left| \Pr_{Expt_{RealLife}}[b = b'] - \Pr_{Expt_{WeirdWorld}}[b = b'] \right| \leq \alpha(k)$.

Problem 3.

- Assume f is a length-preserving one-way function, mapping k bits to k bits. For each of the following functions g_f, show that either g_f must always be a one-way function, or that there exists some other one-way function f' such that $g_{f'}$ is not one-way.

  1. $g_f(x) = (f(x), 0)$
  2. $g_f(x) = f(\bar{x})$, where $\bar{x}$ denotes the bit-wise complement of x.
  3. $g_f(x) = (f(x), f(\bar{x}))$
  4. $g_f(x) = (f(x), \overline{f(x)}))$

- Suppose that f were a length-doubling one-way function. Using f, construct a length-preserving one-way function.

Problem 4. Note, this one is a tad hard. We know that one-way functions can reveal some of their input. How bad can this get? Suppose f is a length-preserving one-way function. Show how to construct a one-way function g with the property that given $g(x)$ for a randomly chosen $x \in \{0,1\}^k$, one can guess *any* single bit of x correctly with probability at least 2/3.