Solutions to Problem Set 1

1. Let $G : \{0,1\}^k \to \{0,1\}^m$ be a (t,ϵ)-secure pseudoradom generator with $m \geq k+1$ and $\epsilon \leq \frac{1}{2}$.

   Prove that

   $$\frac{t}{\epsilon} \leq 2^k \cdot O(m)$$

Solution

First, we need to unpack the meaning of the statement that we have to prove.

We need to show that there is an upper bound $U = O(m2^k)$ such that, for every t, ϵ, if G is (t,ϵ) secure then $t/\epsilon \leq U$. This is equivalent to showing that, for every ϵ, if $t > \epsilon U$ then G is not (t,ϵ) secure. In turn, this is equivalent to showing that, for every ϵ, G is not $(1+\epsilon U, \epsilon)$ secure. That is, for every ϵ, we need to find an algorithm of complexity at most $1 + \epsilon U = O(\epsilon m 2^k)$ that has distinguishing probability at least ϵ for the generator.

Now the solution is very simple. Let the algorithm A keep a look-up table containing $2\epsilon 2^k$ distinct possible outputs of the generator. (If the generator has fewer than so many distinct possible outputs, then the look-up table just contains all possible outputs.) On input $y \in \{0,1\}^m$, the algorithm outputs 1 if y is in the table, and 0 otherwise.

So we have

$$\mathop{\mathbb{P}}_{x \in \{0,1\}^k}[A(G(x)) = 1] \geq \frac{2\epsilon 2^k}{2^k} \geq 2\epsilon$$

because every possible output of G occurs with probability at least $1/2^k$.

And we have

$$\mathop{\mathbb{P}}_{y \in \{0,1\}^m}[A(y) = 1] \leq \frac{2\epsilon 2^k}{2^m} \leq \epsilon$$

because $m \geq k+1$.

Thus

$$|\mathop{\mathbb{P}}_{x\in\{0,1\}^k}[A(G(x))=1]-\mathop{\mathbb{P}}_{y\in\{0,1\}^m}[A(y)=1]|\geq\epsilon$$

the algorithm has distinguishing probability ϵ and complexity $O(m\cdot 2^k)$ (dominated by the size of the look-up table) as required.

2. Let $F:\{0,1\}^k\times\{0,1\}^m\to\{0,1\}^m$ be a (t,ϵ)-secure pseudorandom function with $k=m$, $\epsilon\leq 1/2$, and $t>3m$

   Prove that

$$\frac{t}{\epsilon}\leq 2^k\cdot O(m)$$

Solution

If F is a (t,ϵ)-secure pseudorandom function, then the mapping

$$G(K)=F_K(0,\cdots,0),F_K(0,\cdots,1)$$

is a $(t-2m,\epsilon)$ pseudorandom generator mapping m bits into $2m$ bits.

(An algorithm A of complexity t' that has distinguishing probability ϵ for G can easily be converted into an algorithm of complexity $t+2m$ that has distinguishing probability ϵ for F: just query F at the points $(0,\cdots,0)$ and $(0,\cdots,1)$ and then pass the result to A.)

From the previous solution we know

$$\frac{t-2m}{\epsilon}\leq O(m2^k)$$

and from our assumption $t\leq 3\cdot(t-2m)$, so

$$\frac{t}{\epsilon}\leq O(m2^k)$$

3. Problem 3.7 in Katz-Lindell: assuming the existence of a CPA-secure cryptosystem (Enc,Dec), show that there is a cryptosystem (Enc',Dec') that satisfies plain security for multiple encryptions but that is not CPA secure.

   [Hint: insert a kind of "backdoor" in (Enc',Dec') which can be exploited in a CPA attack but that is exponentially unlikely to be exploitable in the plain multiple encryption model.]

Solution

Let $Enc : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^c$ and assume $c = \ell m$ is a multiple of m. (Otherwise pad the output of Enc with zeroes to ensure this condition; this does not affect CPA-security.)

The encryption Enc' takes in input a plaintext of length c. If it happens to be a valid encryption of the all-zero string $\mathbf{0}$ using Enc, then Enc' allows itself to be broken, and outputs the secret key as part of the encryption of the plaintext. In all other cases, Enc' parses its input as ℓ blocks of length m, and then encodes each block using Enc.

In a CPA attack, we can find out the encryption of $\mathbf{0}$, and force the first case to happen, thus finding out the key and breaking the system. In the plain security model with no encryption oracle, however, we are almost always in the second case (otherwise it would be easy to recognize the encryption of $\mathbf{0}$), and the security for multiple encryptions of Enc' follows from the security of Enc.

In more detail, we have $Enc' : \{0,1\}^k \times \{0,1\}^c \to \{0,1\}^{1+\ell \cdot c}$ and $Dec' : \{0,1\}^k \times \{0,1\}^{1+\ell \cdot m} \to \{0,1\}^c$ defined as follows:

- $Enc'(K, M)$:
  - If $Dec(K, M) = 0 \cdots 0$, then output $(0, K, M)$ followed by as many zeroes as needed to get an output of length $1 + \ell \cdot c$;
  - Else, parse M as $(M_1, \ldots, M_\ell)$, where each block has length m, and output $(1, Enc(K, M_1), \ldots, Enc(K, M_\ell)$.
- $Dec'(K, (b, C))$
  - If the first bit b of the ciphertext is 0, then parse C as $(K, M, 0 \cdots 0)$ and output M
  - Else parse C as $C_1, \ldots, C_\ell$ and output $Dec(K, C_1), \ldots, Dec(K, C_\ell)$.

It is easy to see that (Enc', Dec') suffers a total break under a CPA attack, meaning that with an encryption oracle for $Enc'(K, \cdot)$ it is easy to reconstruct the key K. We first ask the encryption oracle for an encryption of 0^c (by which we mean the string made of a sequence of c zeroes). Then we either get back the key (because by an amazing coincidence, $Dec(K, 0^c)$ happened to be equal to 0^m), or we get back $(1, C_1, \ldots, C_\ell)$, where each C_i is an encryption of 0^m using $Enc(K, \cdot)$. Now we give C_1 to the encryption oracle, and we get back the key.

It remains to show that (Enc', Dec') is secure for multiple encryptions.

Fix two sequences of messages $M_1, \ldots, M_t$ and $M'_1, \ldots, M'_t$, fix an efficient algorithm A, and consider the probabilities

$$\mathop{\mathbb{P}}_{K}[A(Enc'(K, M_1), \ldots, Enc'(K, M_t) = 1] \tag{1}$$

$$\mathop{\mathbb{P}}_{K}[A(Enc'(K, M'_1), \ldots, Enc'(K, M'_t) = 1] \tag{2}$$

We need to show that (1) $\approx$ (2). Let Enc'' be the encryption algorithm that always behaves like the "else" branch of the computation of Enc'. That is, $Enc''(M)$ parses its input as blocks of length m and then uses $Enc()$ on each block. Since Enc is CPA secure, and so also secure for multiple encryptions, we have

$$\mathop{\mathbb{P}}_{K}[A(Enc''(K, M_1), \ldots, Enc''(K, M_t) = 1] \approx \mathop{\mathbb{P}}_{K}[A(Enc''(K, M'_1), \ldots, Enc''(K, M'_t) = 1] \tag{3}$$

finally, we argue that for every M, $\mathbb{P}_K[Enc'(K, M) \neq Enc''(K, M)]$ is very small. (And now we are done, because this means that (1) is approximately the left-hand side of (3), and that (2) is approximately the right-hand side of (3), so that (1) is approximately equal to (2).

Suppose there is a message such that $\mathbb{P}_K[Enc'(K, M) \neq Enc''(K, M)] \geq \epsilon$. This means that $\mathbb{P}_K[Enc(K, 0^m) = M] \geq \epsilon$. On the other hand, there must exist a plaintext $P \in \{0,1\}^m$ such that $\mathbb{P}_K[Enc(K, P) = M] \leq 2^{-m}$ and so we would have that

$$|\mathop{\mathbb{P}}_{K}[Enc(K, P) = M] - \mathop{\mathbb{P}}_{K}[Enc(K, 0^m) = M]| \geq \epsilon - 2^{-m}$$

which would violate the message indistinguishability of Enc.

4. Suppose that F is a pseudorandom permutation $F : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^m$. Consider the following encryption scheme:

   - $Enc(K, M)$: pick a random string r, output $(F_K(r), r \oplus M)$
   - $Dec(K, C_0, C_1) := I_K(C_0) \oplus C_1$

   Is it CPA secure?

Solution

It is CPA-secure.

Let $\overline{Enc}$ be the variant of Enc in which a truly random permutation R is used instead of F_K.

Let A be an algorithm of complexity t mounting a CPA, and M, M' be two messages.

A gets in input a cyphertext (C, C') and then, adaptively, generate plaintexts $M_1, \ldots, M_t$ and passes them to the encryption oracle, receiving ciphertexts $(C_1, C_1'), \ldots, (C_t, C_t')$. Let REP be the event that C, C_1, C_t are all different. When given $\overline{Enc}$ as an encryption oracle, then for every (C, C') the probability that the event REP happens in the computation of $A^{\overline{Enc}}(C, C')$ is at most $t^2 \cdot 2^{-m}$.

We can show that

$$\mathbb{P}[A^{\overline{Enc}}(\overline{Enc}(M)) = 1 | \neg REP] = \mathbb{P}[A^{\overline{Enc}}(\overline{Enc}(M')) = 1 | \neg REP]$$

and so

$$|\,\mathbb{P}[A^{\overline{Enc}}(\overline{Enc}(M)) = 1] - \mathbb{P}[A^{\overline{Enc}}(\overline{Enc}(M')) = 1]| \leq \mathbb{P}[REP] \leq \frac{t^2}{2^m}$$

Finally, if F is a $(O(tm), \epsilon)$ secure pseudorandom permutation, we must have

$$|\,\mathbb{P}[A^{Enc}(Enc(M)) = 1] - \mathbb{P}[A^{\overline{Enc}}(\overline{Enc}(M)) = 1]| \leq \epsilon$$

and

$$|\,\mathbb{P}[A^{Enc}(Enc(M')) = 1] - \mathbb{P}[A^{\overline{Enc}}(\overline{Enc}(M')) = 1]| \leq \epsilon$$

so

$$|\,\mathbb{P}[A^{Enc}(Enc(M)) = 1] - \mathbb{P}[A^{Enc}(Enc(M')) = 1]| \leq 2\epsilon + \frac{t^2}{2^m}$$