

## Problem Set 2 &amp; 3

Due: Thur 10/29/09, by the beginning of class (preferably electronically)

Reading: Chapter 3

- Let  $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$  be a pseudorandom generator with expansion  $\ell(n) = n + c$  for some constant  $c$  (that is, the length of the output is always the length of the input plus  $c$ ). For each of the following constructions, indicate what the expansion is, and determine whether or not the new construction must also be a PRG (assuming  $G$  is). Prove your answer. As an example, solutions are provided for the first two constructions (and you are only requested to solve the last three).

- $G_1(s) = 0G(s)$ .

**Solution:**

The expansion of  $G_1$  is  $\ell_1(n) = n + c + 1$ , because for  $|s| = n$ ,  $|0G(s)| = 1 + |G(s)| = 1 + n + c$ .

$G_1$  is not a PRG. The intuition is that the output of  $G_1$  on a random input string always starts with a 0, and thus does not look random. To prove this, we construct the following distinguisher  $D$ .

$D(z)$ : If  $z$  starts with a 0, output 0. Else, output 1.

This  $D$  is obviously polynomial time (it just outputs the first bit of its input).

$$\Pr_{z \leftarrow \{0,1\}^{n+c+1}} [D(z) = 1] = \Pr_{z \leftarrow \{0,1\}^{n+c+1}} [z \text{ starts with a 1}] = \frac{1}{2}$$

On the other hand,

$$\Pr_{s \leftarrow \{0,1\}^n} [D(G_1(s)) = 1] = \Pr_{s \leftarrow \{0,1\}^n} [0G(s) \text{ starts with a 1}] = 0$$

Thus, the difference between the probabilities is  $\frac{1}{2}$ , which is obviously non-negligible.

- $G_2(s) = G(s)$  with bits in reverse order.

**Solution:**

The expansion of  $G_2$  is  $\ell_2(n) = n + c$ , because for  $|s| = n$ ,  $|G_2(s)| = |G(s)| = n + c$ .  $G_2$  is a PRG (assuming  $G$  is). The intuition is that the output of  $G$  on a random input string looks random (as we're assuming  $G$  is a PRG), and a random string in reverse order is also random, thus the output of  $G_2$  on a random input string also looks random. To prove this, assume towards contradiction there was a polynomial time  $D_2$  that distinguishes the output of  $G_2$  from truly random. That is, if we denote

$$p_1 = \Pr_{z \leftarrow \{0,1\}^{n+c}} [D_2(z) = 1]$$

and

$$p_2 = \Pr_{s \leftarrow \{0,1\}^n} [D_2(G_2(s)) = 1],$$

we have that  $|p_1 - p_2|$  is non-negligible.

We construct the following distinguisher  $D$  for  $G$ :

$D(z)$ : Let  $rev(z) = z$  with bits in reverse order. Run  $D_2(rev(z))$  and output same.

Now we have

$$\begin{aligned} \Pr_{z \leftarrow \{0,1\}^{n+c}} [D(z) = 1] &= \Pr_{z \leftarrow \{0,1\}^{n+c}} [D_2(rev(z)) = 1] = \\ &= \Pr_{rev(z) \leftarrow \{0,1\}^{n+c}} [D_2(rev(z)) = 1] = p_1 \end{aligned}$$

(because choosing  $z$  uniformly at random induces the same probability distribution over  $rev(z)$  as choosing  $rev(z)$  uniformly at random). On the other hand,

$$\begin{aligned} \Pr_{s \leftarrow \{0,1\}^n} [D(G(s)) = 1] &= \Pr_{s \leftarrow \{0,1\}^n} [D_2(rev(G(s))) = 1] = \\ &= \Pr_{s \leftarrow \{0,1\}^n} [D_2(G_2(s)) = 1] = p_2. \end{aligned}$$

Thus, the difference (distinguishing probability for  $D$ ) is  $|p_1 - p_2|$  (exactly the same as for  $D_2$ ), which was assumed to be non-negligible. This means  $G$  is not a PRG, contradiction.

- $G_3(s, t) = G(s)t$  where  $|s| = |t|$   
(That is, parse the input as two equal-length parts, apply  $G$  to the first, and then concatenate the second part).
- $G_4(s, t) = G(s, t)t$  where  $|s| = |t|$   
(That is, parse the input as two equal-length parts, apply  $G$  to the input, and then concatenate the second part).
- $G_5(s) = G(G(s))$

2. Let  $F$  be a PRF and  $G$  a PRG which expands by one bit (i.e.,  $\ell(n) = n + 1$ ). Below we describe a few private-key encryption schemes – the key generation algorithm always chooses a random key  $k \in \{0, 1\}^n$ , and the decryption algorithm is omitted. For each of these encryption schemes, state whether the scheme is secure (satisfying our indistinguishability definition) against a ciphertext only attack (eavesdropper), and whether it is secure against a CPA (chosen plaintext attack). Provide a brief informal justification (a formal proof is not necessary).

As a reminder/example, the first two schemes are examples we saw in class, and we provide their solutions.

- (a) To encrypt a message  $m$  of length  $n$ , output the ciphertext  $G(k) \oplus m$ .

**Solution:** We proved in class that this is secure against an eavesdropper (the intuition being that  $G(k)$  looks random for a random key  $k$ , and thus this is a computational version of the one-time-pad, where the ciphertext looks random and independent from the message). We also saw in class it does not achieve CPA-security (actually, not even eavesdropper security for more than one message). Moreover, we proved that no deterministic encryption scheme can be CPA-secure

- (b) To encrypt a message  $m$  of length  $n$ , choose a random  $r \in \{0, 1\}^n$ , and output the ciphertext  $(r, F_k(r) \oplus m)$ .

**Solution:** We saw in class that this achieves CPA security (the intuition being that if  $F$  was a truly random function this would be secure, as the same  $r$  has only negligible probability to be chosen during the CPA phase, and once the same  $r$  is not repeated,  $F_k(r)$  is like a fresh independent random pad, leaking no information). Since it achieves CPA security, it also achieves (the weaker) security against an eavesdropper.

- (c) To encrypt a message  $m$  of length  $n + 2$ , parse each of  $m$  and  $k$  as two equal-length parts (you may assume  $n$  is even): write  $m := m_1 \circ m_2$  ( $|m_1| = |m_2|$ ) and  $k := k_1 \circ k_2$  ( $|k_1| = |k_2|$ ). Output the ciphertext  $(G(k_1) \oplus m_1, G(k_2) \oplus m_2)$ .
- (d) To encrypt a message  $m$  of length  $2n + 2$ , parse  $m$  as two equal-length parts  $m := m_1 \circ m_2$  ( $|m_1| = |m_2|$ ). Output the ciphertext  $(G(k) \oplus m_1, G(k + 1) \oplus m_2)$ .
- (e) To encrypt a message  $m$  of length  $n + 1$  choose a random  $r \in \{0, 1\}^n$  and output the ciphertext  $(r, G(r) \oplus m)$ .
- (f) To encrypt a message  $m$  of length  $n$  choose a random  $r \in \{0, 1\}^n$  and output the ciphertext  $(F_k(r), r \oplus m)$ .
- (g) To encrypt a message  $m$  of length  $2n$ , parse  $m$  as two equal-length parts  $m := m_1 \circ m_2$  ( $|m_1| = |m_2|$ ), and choose a random  $r \in \{0, 1\}^n$ . Output the ciphertext  $(r, F_k(r) \oplus m_1, F_k(r + 1) \oplus m_2)$ .
3. Let  $(Gen, Enc, Dec)$  be a CPA-secure encryption scheme that encrypts messages of length  $2n$ . Let  $f$  be a polynomially computable function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ . Define the augmented encryption scheme  $(fGen, fEnc, fDec)$  that encrypts messages of length  $n$  by first appending  $f(m)$  to  $m$ , and then running  $Enc$ . That is:
- $fGen$  is the same as  $Gen$ .
  - $fEnc_k(m) := Enc_k(m, f(m))$ .
  - $fDec_k(c) : \text{compute } Dec_k(c) = (m_1, m_2)$ , and output  $m_1$ .

Prove that if  $(Gen, Enc, Dec)$  is CPA-secure, then so is  $(fGen, fEnc, fDec)$ . You may assume  $f$  is a deterministic function.

**Extra Credit:** Prove the same for  $f$  that is a randomized function (defined as the output of a polynomial time randomized algorithm).