Complexity Theory (fall 2016) Dominique Unruh

Solution of Exercise Sheet 11

Problem 1: One-way functions

Which of the following are one-way functions? For each function that is a one-way function, explain why (no formal proof required). For each function that is not a one-way function, describe a polynomial-time attack (i.e., describe how, given y, one can find a preimage x in polynomial-time with non-negligible probability).

Hint: Out of the five functions, one is a OWF, the other four are not.

Note: You may assume that the RSA assumption holds. And that E_{AES} is a PRF.

Note: Remember that to break a one-way function, it is sufficient to find some preimage, not necessarily the "true" one that was fed into the one-way function.

(a) $f_1(x) := 0$ for all $x \in \{0,1\}^\eta$.

Solution. Not a one-way function.

Given an image $y = 0$, we can set $x := 0^\eta$. Then $y = 0 = f(x)$ and we have inverted f. (Remember that it is not necessary to find out, which value x was really used when computing $y \leftarrow f(x)$.) **.noitulo2**

(b) $f(x) := x_1 \dots x_{\eta/2}$ for $x \in \{0,1\}^\eta$.

Solution. Not a one-way function.

Given an image $y = x_1 \dots x_{\eta/2}$, we can set $x := x_1 \dots x_{\eta/2} 0 \dots 0 \in \{0,1\}^\eta$. Then $y = f(x)$ and we have inverted f. (Remember that it is not necessary to find out, which value x was really used when computing $y \leftarrow f(x)$.) **.noitulo2**

(c) $f(k\|m) := E_{AES}(k,m)$.

Here $E_{AES} : \{0,1\}^{\ell_k} \times \{0,1\}^{\ell_m} \to \{0,1\}^{\ell_m}$ is the AES block cipher. That is, it is a deterministic algorithm, and there is another (polynomial-time) function D_{AES} that decrypts it, i.e., $D_{AES}(k, E_{AES}(k,m)) = m$ for all k, m. Also you can assume that E_{AES} is a secure encryption scheme in the sense defined in the lecture.

Solution. Not a one-way function.

Given y, the adversary picks a random key k and computes $x \leftarrow D_{AES}(k, y)$. Then $f(k, x) = y$. **.noitulo2**

(d) $f(x) := g(x)\|g(x)$ where g is a one-way function.

Note: Here (and in (e)), the question is whether f would be a one-way function for *every* one-way function g.

Solution. A one-way function in general.

Assume that there is an adversary A that, given $y\|y$, finds x with $y\|y = f(x)$ with non-negligible probability. Then we can construct an adversary B that, given y, finds x with $y = g(x)$. Namely, $B(y)$ invokes $A(y\|y)$. But the existence of such a B contradicts the one-wayness of g. **.noitulo2**

(e) $f(x) := g(g(x))$ where g is a one-way function.

Hint: The first thought here might be wrong. Remember that a one-way function g might not be surjective. E.g., the first half of $g(x)$ might always consist of zeroes.

Solution. Not a one-way function.

Assume a one-way function $g' : \{0,1\}^\eta \to \{0,1\}^\eta$. We construct the one-way function $g : \{0,1\}^{2\eta} \to \{0,1\}^{2\eta}$ as follows: $g(x_1x_2) := 0^\eta\|g'(x_1)$.

Then $f(x_1x_2) = g(g(x_1x_2)) = g(0^\eta\|g'(x_1)) = 0^\eta\|g'(0^\eta)$. Thus f is a constant function and thus not a one-way function. (And adversary that outputs an arbitrary preimage always successfully inverts g.) **.noitulo2**

Problem 2: OWFs and P = NP

Show that, if **P** = **NP**, then no one-ways functions exist.

Hint: Assume a one-way function f. First show that if **P** = **NP**, then there exists a polynomial-time algorithm that given η, x_0, and y with $|x_0| \leq \eta$ finds out whether there is an $x \in \{0,1\}^\eta$ such that x_0 is a prefix of x and $f(x) = y$. Then use this algorithm to find a preimage of y under f in polynomial-time.

Solution. Assume a one-way function f. (In particular, f is polynomial-time computable.)

Let $L := \{(1^\eta, x_0, y) : \exists x.\, |x| = \eta, f(x) = y, x_0 \leq x\}$. Here $x_0 \leq x$ means that x_0 is a prefix of x.

$L \in$ **NP** because x with $|x| = \eta, f(x) = y, x_0 \leq x$ is a witness for $(1^\eta, x_0, y)$. (And we use the fact that f is efficiently computable to ensure that a witness can be checked in

deterministic polynomial-time.) Since we assume $\mathbf{P} = \mathbf{NP}$, we have $L \in \mathbf{P}$. Thus there is a polynomial-time algorithm A such that $A(1^\eta, x_0, y)$ returns 1 iff $(1^\eta, x_0, y) \in L$.

The following algorithm B then finds x_0 with $y = f(x_0)$ and $|x_0| = \eta$ if such x_0 exists (ε denotes the empty string):

Input: $1^\eta, y$
$x_0 := \varepsilon$ // Invariant (if preimage of f of length η exists):
  $\exists x.\, |x| = \eta, f(x) = y, x_0 \leq x$
for $i = 1, \ldots, \eta$ **do**
  if $A(1^\eta, x_0\|0, y) = 1$ **then**
    // $\exists x.\, |x| = \eta, f(x) = y, x_0\|0 \leq x$
    $x_0 := x_0\|0$
    // Invariant holds again
  else
    // $\nexists x.\, |x| = \eta, f(x) = y, x_0\|0 \leq x$
    // With invariant and $|x_0| < \eta$, this implies
      $\exists x.\, |x| = \eta, f(x) = y, x_0\|1 \leq x$
    $x_0 := x_0\|1$
    // Invariant holds again
// Now $|x_0| = \eta$. Then invariant implies $f(x_0) = y$.
return x_0

This algorithm B is clearly polynomial-time since A is. The comments explain why it will always return x_0 with $y = f(x_0)$ if such x_0 exists.

Thus

$$\Pr[f(x_0) = f(x) : x \xleftarrow{\$} \{0,1\}^\eta,\ y := f(x),\ x_0 \leftarrow A(1^\eta, y),\ ] = 1.$$

Since 1 is not a negligible function, this implies that f is not a one-way function.

This shows that one-way functions do not exist (under the assumption $\mathbf{P} = \mathbf{NP}$).

Solution.

Problem 3: One-time pad

The one-time pad is an encryption scheme with message space $M = \{0,1\}^\eta$, key space $K = \{0,1\}^\eta$, and ciphertext space $C = \{0,1\}^\eta$. (That is, messages, keys, and ciphertexts have the same length.) Encryption is done by $E(k, m) := k \oplus m$, and decryption by $D(k, c) = k \oplus c$.

Show that (E, D) satisfy the secrecy definition (IND-OT-CPA) from the lecture.

Solution. Recall the definition of secrecy:

Definition 1 *E has secrecy iff for any probabilistic polynomial-time A, there exists a negligible function μ such that for all η and all $m_1, m_2 \in M$, we have*

$$\Pr[A(1^\eta, E(k, m_b)) = b : k \xleftarrow{\$} K, b \xleftarrow{\$} \{0,1\}] \leq \tfrac{1}{2} + \mu(\eta). \quad (1)$$

For our particular encryption scheme, (1) becomes:

$$p := \Pr[A(1^\eta, k \oplus m_b) = b : k \xleftarrow{\$} \{0,1\}^\eta, b \xleftarrow{\$} \{0,1\}] \leq \tfrac{1}{2} + \mu(\eta).$$

where $m_0, m_1 \in \{0,1\}^\eta$.

Since k is uniformly random in $\{0,1\}^\eta$, $k \oplus m_b$ has the same distribution as a uniformly random $c \in \{0,1\}^\eta$. Thus we can replace $k \oplus m_b$ by c in the above probability and get:

$$p := \Pr[A(1^\eta, c) = b : c \xleftarrow{\$} \{0,1\}^\eta, b \xleftarrow{\$} \{0,1\}]$$

(Here we use the fact that k is used nowhere else. Because given k, we do not have that $k \oplus m_b$ and c have the same distribution.)

Since $A(1^\eta, c)$ does not depend on b, and b is a uniform bit, we have that $\Pr[A(1^\eta, c) = b] = \frac{1}{2}$. I.e., $p = \frac{1}{2}$. Thus for any negligible μ (e.g., $\mu := 0$), we have $p \leq \frac{1}{2} + \mu(eta)$. This shows (1), thus E has secrecy. **Solution.**