

Homework  
Modern Cryptography  
BISS  
March 2009  
Stefan Dziembowski

**Exercise 1** Suppose that the one-way functions exist. Show that there exists a one-way function  $f$  such that

- for every  $x$  we have  $|f(x)| = |x|$ , and
- a function  $g$  defined as  $g(x) := f(x) \oplus x$  is not a one-way function.

**Exercise 2** Let  $F$  be a pseudorandom function. Show that the following MAC for messages of length  $2n$  is not secure. The shared key has length  $n$ . A tag on a message  $(m_1, m_2)$  (with  $|m_1| = |m_2| = n$ ) is equal to

$$(F_k(m_1), F_k(F_k(m_2))).$$

**Exercise 3** Let  $H$  be a collision-resistant hash function. Define  $\hat{H}$  as

$$\hat{H}^s(x) := H^s(H^s(x)).$$

Is  $\hat{H}$  necessarily collision resistant? If your answer is yes then give a proof. Otherwise give an example of  $H$  such that  $\hat{H}$  is not collision resistant.

**Exercise 4** Let  $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$  be a function such that for every  $S$  we have  $|G(S)| = t \cdot |S|$  (for some constant  $t$ ). Consider the following game between the adversary  $\mathcal{A}$  and an oracle  $\Omega$ .

1. The oracle  $\Omega$  takes as input parameters  $m$ , selects a random string  $S \in \{0, 1\}^m$  and sets  $x = (x_1, \dots, x_{mt}) := G(S)$ . The oracle sends  $1^m$  to the adversary  $\mathcal{A}$ .
2. The adversary chooses  $i \in \{1, \dots, m\}$  and sends it to the oracle.
3. The oracle sends  $(x_1, \dots, x_{t(i-1)})$  to the adversary.
4. The oracle selects a random bit  $b \in \{0, 1\}$  and:
  - (a) if  $b = 0$  the oracle sends  $(x_{t(i-1)+1}, \dots, x_{ti})$  to the adversary,
  - (b) if  $b = 1$  the oracle sends a random string of  $t$  bits to the adversary.
5. The adversary outputs  $b' \in \{0, 1\}$ . We say that he won the game if  $b = b'$ .

Suppose that every polynomial time adversary guesses  $b$  with probability at most  $0.5 + \mu(m)$  (where  $\mu$  negligible). Show that this implies that  $G$  is a cryptographic pseudorandom generator.