Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 7

will be discussed on December 15, 2020

Exercise 7.1

Consider an extension of definition §7.4 where the adversary is provided with both a mac- and a val-oracle. (Access to val-oracle is not restricted).

(a) Assume $\mathcal{E}$ is a (deterministic) MAC using canonical verification that satisfies definiton §7.4 (Secure MAC). Prove that $\mathcal{E}$ also satisfies the extended definition above.
This means access to a val-*oracle does not result in a stronger definition when using canonical verification.*

(b) Assume secure MACs exist. Construct a MAC that is secure (in the sense of §7.4) but not secure in the sense of the extended definition above.

Exercise 7.2

Let f be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. In each case $\mathrm{gen}(1^n)$ outputs a uniform $k \in \{0,1\}^n$. Let $[i]$ denote an $n/2$-bit encoding of the integer i.

(a) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^n$, compute $c := f_k(m_1) \oplus \ldots \oplus f_k(m_l)$.

(b) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^{n/2}$, compute $c := f_k([1] \mid\mid m_1) \oplus \ldots \oplus f_k([l] \mid\mid m_l)$.

(c) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^{n/2}$, choose uniform $r \leftarrow \{0,1\}^n$, compute

$$c := f_k(r) \oplus f_k([1] \mid\mid m_1) \oplus \ldots \oplus f_k([l] \mid\mid m_l)$$

and let the tag be $\langle r, c \rangle$.

Here *fixed-length* means that mac_k is only defined for messages of length $l(n)$ for a function l.