Prof. Dr. Johannes Blömer
Nils Löken

June 2nd, 2017

Cryptography - Provable Security

SS 2017

Handout 8

Exercise 1:
Let $MAC = (\text{Gen}, \text{Mac}, \text{Vrfy})$ be a MAC and for $k \in \{0,1\}^n$ the tag generation algorithm Mac_k always outputs tags of length $t(n)$. Prove that if $t(n) = \mathcal{O}(\log(n))$ then MAC cannot be a secure MAC.

Exercise 2:
Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Show that the following MACs are insecure. For all the schemes the key $k \leftarrow \{0,1\}^n$ is chosen uniformly at random.

a) To authenticate a message $m_1 \,||\, m_2$ with $|m_1| = |m_2| = n - 1$, compute the tag

$$t := F_k(0 \,||\, m_1) \,||\, F_k(1 \,||\, m_2).$$

b) To authenticate a message $m_1 \,||\, m_2$ with $|m_1| = |m_2| = n$, compute the tag

$$t := F_k(m_1) \,||\, F_k(F_k(m_2)).$$

c) To authenticate a message $m_1 \,||\, m_2 \,||\, \cdots \,||\, m_\ell$ with $|m_i| = n$, compute the tag

$$t := F_k(m_1) \,||\, F_k(m_2) \,||\, \ldots \,||\, F_k(m_\ell).$$

d) To authenticate a message $m = m_1 \,||\, m_2 \,||\, \ldots \,||\, m_\ell$ with $|m_i| = n - \log(n)$, choose $r \leftarrow \{0,1\}^n$ uniformly at random and compute the tag

$$t := \langle r, F_k(r) \oplus F_k(<1> \,||m_1) \oplus \cdots \oplus F_k(<\ell> \,||m_\ell)\rangle,$$

where $<i>$ is the $\log(n)$ bit encoding of integer i.

Note that the following MAC is secure: To authenticate $m = m_1, || \ldots || \, m_\ell$ with $|m_i| = n$ set $k_\ell := F_k(<\ell>)$, $t_0 := 0^n$, for $i = 1, \ldots, \ell$ compute $t_i := F_{k_\ell}(t_{i-1} \oplus m_i)$ and output tag $t := t_\ell$. Compare the secure construction to the insecure constructions as well as to Constructions 8.4 and 8.6 from the lecture.

Exercise 3:
Let $MAC = (\text{Gen}', \text{Mac}', \text{Vrfy}')$ be a secure fixed-length MAC for messages of length n. Assume for simplicity that Gen' chooses a random n-bit key uniformly at random. Break the message $m = m_1 \,||\, \ldots \,||\, m_\ell$ into ℓ blocks in an appropriate way. Consider the following MAC schemes:

- $\text{Mac}_k(m) = \langle \text{Mac}'_k(m_1), \ldots, \text{Mac}'_k(m_\ell)\rangle$

- $\mathrm{Mac}_k(m) = \langle \mathrm{Mac}'_k(<1>, m_1), \ldots, \mathrm{Mac}'_k(<\ell>, m_\ell)\rangle$, where $< i >$ denotes the binary representation of i of length $n/2$.
- $r \leftarrow \{0,1\}^{n/3}$, $\mathrm{Mac}_k(m) = \langle r, \mathrm{Mac}'_k(<r>, <1>, m_1), \ldots, \mathrm{Mac}'_k(<r>, <\ell>, m_\ell)\rangle$, where $<i>$ denotes the binary representation of i of length $n/3$.

Compare the schemes to Construction 8.6 from the lecture. What kind of attacks are possible against the introduced schemes and what kind of attacks are prevented?