Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2019/02/06

Cryptography – Questionnaire 4

Name: ______________________________

Matr.: ______________________________

"One-liners"– 1+2+4 = 7P

Exercise 4.1 **1P**

Let F be a PRP. How do you obtain a PRF from F?
Answer:

Exercise 4.2 **2P**

Let F be a PRP. Sketch graphically the computation of F-NMAC.

Exercise 4.3 **2P+2P**

Let F be a PRF with block length $l(n) = n$. Consider the following two MAC schemes where in both cases $\mathsf{Gen}(1^n)$ outputs $k \overset{u}{\in} \{0,1\}^n$ and $\mathsf{Vrf}_k(t, m)$ outputs 1 iff $\mathsf{Mac}_k(m) = t$. The message space is $(\{0,1\}^n)^+$. We can write every message m as $m = m^{(1)}||\cdots||m^{(|m|/n)}$ with $m^{(i)} \in \{0,1\}^n$ for $1 \leq i \leq |m|/n$. Show for each of the following two choices of Mac_k how Eve can use her oracle access to Mac_k to forge a tag for the message 0^n0^n in the MAC-experiment:

(a) $\mathsf{Mac}_k(m) := F_k(m^{(1)}) \oplus \cdots \oplus F_k(m^{(|m|/n)})$
Answer:

(b) $\mathsf{Mac}_k(m) := F^*_k(m)$
Answer:

Recall that $F^*_k(m)$ for $m = m^{(1)}||\cdots||m^{(d)}$ is the "cascading-construction" defined by the algorithm:

- Set $k^{(0)} := k$
- For $i = 1$ to d: set $k^{(i)} := F_{k^{(i-1)}}(m^{(i)})$.
- Output $F^*_k(m) := k^{(d)}$

Questions–1P each = 3P

	true	false
Let F be a PRP of block length n. Define an ES $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with $\mathsf{Gen}(1^n)$ choosing a key k uniformly at random from $\{0,1\}^n$ and $\mathsf{Enc}_k(x_1 \dots x_{2n}) = F_k(x_1 \dots x_n) \| F_k(x_{n+1} \dots x_{2n})$. $\mathcal{E}$ is CPA-secure.	☐	☐
Let F be a PRP. Then there is a PPT adversary which can distinguish F from a random-permutation-oracle with non-zero advantage.	☐	☐
Let F be a PRF. F-rCTR Mode, i.e. $\mathsf{Mac}_k(m) := \text{ctr} \| m^{(1)} \oplus F_k(\lfloor \text{ctr} + 1 \rceil) \| \dots \| m^{(t)} \oplus F_k(\lfloor \text{ctr} + t \rceil).)$ yields a secure MAC.	☐	☐