Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Solutions for Exercise Sheet 8

will be discussed on January 12, 2021

Exercise 8.2

Prove that the encrypt-then-authenticate-scheme is unforgeable if provided with any encryption scheme (even if not CPA-secure) and any secure MAC.

SOLUTION: Let $\mathcal{E} = (\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$ be a private-key encryption sheme and $\mathcal{E}' = (\mathrm{gen}', \mathrm{mac}, \mathrm{val})$ a secure message authentication scheme. The authenticated encryption scheme $\underline{\mathcal{E}} = (\underline{\mathrm{gen}}, \underline{\mathrm{enc}}, \underline{\mathrm{dec}})$ is defined as follows:

$$\begin{aligned} P_{K\times K'}(\langle k, k'\rangle) &= P_K(k) \cdot P_{K'}(k') \\ \underline{\mathrm{enc}}_{\langle k,k'\rangle}(m) &= \langle c, c'\rangle \text{ with } c = \mathrm{enc}_k(m), c' = mac_{k'}(c) \\ \underline{\mathrm{dec}}_{\langle k,k'\rangle}(\langle c, c'\rangle) &= \begin{cases} \mathrm{dec}_k(c) & \text{if } \mathrm{val}_{k'}(c, c') = 1 \\ \bot & \text{else} \end{cases} \end{aligned}$$

Let $\mathcal{A}$ be a PPT adversary with access to an encryption oracle. Assume $\mathcal{A}$ asks the oracle for encryption of the messages $Q = \{m_1, \ldots, m_l\}$ and receives $\langle c_1, c_1'\rangle, \ldots, \langle c_l, c_l'\rangle$. Let $\langle c, c'\rangle$ be the ciphertext outputted by $\mathcal{A}$.
We want to show that

$$\mathrm{P}[\mathrm{Forge}^{\mathrm{ENC}}_{\underline{\mathcal{E}},\mathcal{A}}] \simeq 0$$

Set $m = \underline{\mathrm{dec}}_{\langle k,k'\rangle}(\langle c, c'\rangle)$.
Consider the case $c \notin \{c_1, \ldots, c_l\}$:

$$\begin{aligned} \mathrm{P}[\mathrm{Forge}^{\mathrm{ENC}}_{\underline{\mathcal{E}},\mathcal{A}}] &= \mathrm{P}[m \neq \bot \wedge m \notin Q] \\ &\leq \mathrm{P}[m \neq \bot] \\ &= \mathrm{P}[\mathrm{val}_{k'}(c, c') = 1 \wedge \mathrm{dec}_k(c) \neq \bot] \\ &\leq \underbrace{\mathrm{P}[\mathrm{val}_{k'}(c, c') = 1] \simeq 0}_{\text{because } \mathcal{E}' \text{ is a secure MAC}} \end{aligned}$$

and the case $c = c_i$ for one $1 \leq i \leq l$:

$$\begin{aligned} \mathrm{P}[\mathrm{Forge}^{\mathrm{ENC}}_{\mathcal{E},\mathcal{A}}] &= \mathrm{P}[m \neq \perp \wedge m \notin Q] \\ &\leq \mathrm{P}[m \notin Q] \\ &= \mathrm{P}[m_i \notin Q] = 0, \end{aligned}$$

where the last line comes from

$$\begin{aligned} m &= \underline{\mathrm{dec}}_{\langle k,k' \rangle}(\langle c_i, c'_i \rangle) \\ &= \mathrm{dec}_k(c_i) && \text{(perfect correctness of } \mathcal{E}') \\ &= m_i && \text{(perfect correctness of } \mathcal{E}). \end{aligned}$$

Together we have

$$\mathrm{P}[\mathrm{Forge}^{\mathrm{ENC}}_{\mathcal{E},\mathcal{A}}] \simeq 0$$

and thus the scheme $\underline{\mathcal{E}}$ is unforgeable. ■