The art of cryptography, summer 2017

MICHAEL NÜSKEN

9. Exercise sheet
Hand in solutions until Monday, 17 July 2017, 09:00

Exercise 9.1 (Single to multi-user). (10 points)

ℓ-EUF-CMA Game.

Input: κ, $\mathcal{L}$.
Output: ACCEPT or REJECT.

1. For $P \in \mathcal{L}$ do
   $(K_P, k_P) \xleftarrow{\$} \mathrm{SIG.Keygen}(1^\kappa)$.
2. Invoke the player $\mathcal{P}$ with input $(\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Sign}}, \mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Corrupt}}, K_\cdot)$ to obtain a party $P' \in \mathcal{L}$ and a message signature pair (m', s').
3. If $\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Corrupt}}$ was called on input P' then Return REJECT.
4. If $((P', m'), s')$ is the input output pair of a call to the oracle $\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Sign}}$ then Return REJECT.
5. Return $\mathrm{SIG.Vfy}(K_{P'}, m', s')$.

Oracle. $\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Sign}}$.
Input: P, m.
Output: s.

1. $s \leftarrow \mathrm{SIG.Sign}(k_P, m)$.
2. Return s.

Oracle. $\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Corrupt}}$.
Input: P.
Output: k_P.

1. Return k_P.

Prove: $\boxed{10}$

Theorem. *Any (t, ε)-EUF-CMA secure signature scheme is also $(t - t_{\mathcal{R}}, \ell \cdot \varepsilon)$-$\ell$-EUF-CMA secure, where $t_{\mathcal{R}} \in \mathcal{O}(\ell)$ is the overhead runtime of the reduction.*

Hint: Apply Game-Hopping. In some hop, you have to specify a reduction to the EUF-CMA game and prove that it works.