The art of cryptography, summer 2016

MICHAEL NÜSKEN

11. Exercise sheet
Hand in solutions until Monday, 4 July 2016, 11:59

Exercise 11.1 (Single to multi-user). (5+5 points)

ℓ-EUF-CMA Game.

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

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

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

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

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

1. Return sk_P.

Prove: 5+5

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 to compare ℓ-EUF-CMA Game and Reduction to EUF-CMA.

Reduction to EUF-CMA. $\mathcal{R}$.
Input: pk, $\mathcal{O}_{\mathrm{Sign}}$.
Output: (m, s) or $\perp$.

1. For $P \in \mathcal{L}$ do
   $(\mathrm{pk}_P, \mathrm{sk}_P) \xleftarrow{\$} \mathrm{SIG.Keygen}(1^\kappa)$.
2. Pick $P^* \xleftarrow{\$} \mathcal{L}$ and replace $\mathrm{pk}_{P^*} \leftarrow \mathrm{pk}$, $\mathrm{sk}_{P^*} \leftarrow \perp$.
3. Invoke the player $\mathcal{P}$ with input $(\mathcal{O}^{\mathrm{red}}_{\mathrm{Sign}}, \mathcal{O}^{\mathrm{red}}_{\mathrm{Corrupt}}, \mathrm{pk}_\cdot)$ to obtain a party $P' \in \mathcal{L}$ and a message signature pair (m', s').
4. If $P' \neq P^*$ then Return $\perp$.
5. Return (m', s').

Oracle. $\mathcal{O}^{\mathrm{red}}_{\mathrm{Sign}}$.
Input: P, m.
Output: s.

1. If $P = P^*$ then
   $s \leftarrow \mathcal{O}_{\mathrm{Sign}}(m)$.
2. Else
   $s \leftarrow \mathrm{SIG.Sign}(\mathrm{sk}_P, m)$.
3. Return s.

Oracle. $\mathcal{O}^{\mathrm{red}}_{\mathrm{Corrupt}}$.
Input: P.
Output: sk_P or $\perp$.

1. If $P = P^*$ then Return $\perp$.
2. Return sk_P