The art of cryptography, summer 2016

MICHAEL NÜSKEN

10. Exercise sheet
Hand in solutions until Monday, 27 June 2016, 11:59

Exercise 10.1 (Project, part 2). (5+5 points)

Consider your chosen protocol for this exercise.

(i) Discuss the security of the chosen protocol under the following security aspects: $\boxed{5+5}$

(a) Session key agreement.

(b) Perfect forward security.

(c) Denial of Service.

(d) Endpoint identifier hiding.

(e) Live partner reassurance.

We will summarize your results in the course and tutorial soon.

(ii) Make sure that relevant literature is available in class next Tuesday!

Exercise 10.2 (Never real-or-random). (5 points)

In the authenticated key exchange (AKE) model a key exchange is considered and the attacker's challenge is to tell whether a given key is real or random. $\boxed{5}$

Assume that a key exchange produces a key k which is indistinguishable from random. But then during the data exchange this key is used in an authenticated encryption scheme. (Formulate the game!) Show that the key in that combination is always distinguishable from random.

Hint: Just formalize what I told you in class.

Exercise 10.3 (Single to multi-user). (0+10 points)

ℓ-EUF-CMA Game.

Input: $\kappa, \mathcal{L}$.
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 $(\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Sign}}, \mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Corrupt}}, \mathrm{pk}_{.})$ 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 $\mathrm{SIG.Vfy}(\mathrm{pk}_{P'}, m', s')$.
```

Oracle. $\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Sign}}$.

Input: P, m.
Output: s.

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

Oracle. $\mathcal{O}^{\ell\text{-EUF-CMA}}_{\text{Corrupt}}$.

Input: P.
Output: sk_P.

```
1. Return $\mathrm{sk}_P$.
```

$\boxed{+10}$ Prove:

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. You have to specify a reduction to the EUF-CMA game and prove that it works.