Modern Cryptography Jan 15, 2020

Homework 13

Lecturer: Daniel Slamanig, TA: Guillermo Perez, Karen Klein Due: 23.59 CET, Jan 22, 2020

To get credit for this homework it must be submitted no later than Wednesday, January 15th via TUWEL. If you have not registered for the tutorial (192.063 Tutorial on Introduction to Modern Cryptography 2019W) on TUWEL, please do so. If you are unable to register for the course on TUWEL for some reason, submit your homework via email to via email to `guillermo.pascualperez@ist.ac.at`, please use "MC19 Homework 13" as subject.

1. Derandomizing signatures

   - **(3 Points)** Let $\Sigma = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Verify})$ be an $\mathsf{EUF\text{-}CMA}$ secure signature scheme, where the signing algorithm Sign is probabilistic. In particular, algorithm Sign uses randomness r chosen from a space $\mathcal{R}$. We let $\mathsf{Sign}(sk, m; r)$ denote the execution of algorithm Sign with randomness r. Let F be a secure pseudo-random function (PRF) with key space $\mathcal{K}$ and output space being $\mathcal{R}$. Prove that the signature scheme $\Sigma' = (\mathsf{KGen}', \mathsf{Sign}', \mathsf{Verify})$ is also $\mathsf{EUF\text{-}CMA}$ secure, where

   KGen': Run $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$, $k \leftarrow_{\$} \mathcal{K}$, set $sk' := (sk, k)$ and return (sk', pk).

   Sign': Compute $r \leftarrow F(k, m)$, $\sigma \leftarrow \mathsf{Sign}(sk, m; r)$ and output σ.

2. Attack on derandomized signatures

   - **(1.5 Points)** Consider the Schnorr signature scheme (see slide 21 of Lecture 13) using the derandomization strategy in Task 1. Present a detailed attack that recovers the secret signing key if we assume that you can introduce a single bit fault into the signing process (as discussed on slide 23 of Lecture 13).

3. One-time signatures

   - Let us consider the signature scheme Σ in Fig. 1 with message space $\mathcal{M} = \{0,1\}^*$ and hash function $H : \{0,1\}^* \to \mathbb{Z}_q$ (which we assume to be sampled randomly from the hash function family $\{H_k\}_{k \in \mathcal{K}}$).
     - **(0.5 Points)** Show that the scheme is correct
     - **(3.5 Points)** Prove the following theorem:

       Theorem 1 *If the discrete-logarithm problem is hard relative to $\mathcal{G}$ and* H *is modeled as a random oracle, then the signature scheme is* $\mathsf{EUF\text{-}1\text{-}CMA}$ *secure.*
     - **(1.5 Point)** Show that Σ is not two-time secure: given signatures on two distinct messages m_0 and m_1 in $\mathbb{Z}_q$, the adversary can forge the signature on every message $m \in \mathbb{Z}_q$ of its choice.

```
$\mathsf{KGen}(1^\lambda)$:
- $\mathcal{G} = (\mathbb{G}, q, g) \leftarrow \mathsf{GGen}(1^\lambda)$;
- $H \leftarrow\!\!\$\, \{H_k\}_{k \in \mathcal{K}}$;
- $\alpha, \beta \leftarrow\!\!\$\, \mathbb{Z}_q$;
- $u := g^\alpha; v := g^\beta$;
- $(sk, pk) := ((\alpha, \beta), (u, v, \mathcal{G}, H))$
- return $(sk, pk)$.
```

```
$\mathsf{Sign}(sk, m)$:
- $\sigma := H(m)\alpha + \beta \mod q$;
- return $\sigma$.
```

```
$\mathsf{Verify}(pk, m, \sigma)$:
- if $g^\sigma = v \cdot u^{H(m)}$ return $1$
  else return $0$.
```

Figure 1: Signature scheme Σ.