Modern Cryptography Jan 15, 2019

Homework 13

Lecturer: Daniel Slamanig, TA: Karen Klein *Due: 23.59 CET, Jan 23, 2019*

To get credit for this homework it must be submitted no later than Wednesday, January 23rd via email to `michael.walter@ist.ac.at`, please use "MC18 Homework 13" as subject.
Please put your solutions into a single pdf file[1] and name this file Yourlastname_HW13.pdf.

1. Hash-and-Sign

   - **(3 Points)** Provide a formal proof of security of the hash-and-sign paradigm, i.e. prove the following theorem:

     Theorem 1 *If Σ is an* EUF-CMA *secure signature scheme for messages of length k and Γ is collision resistant, then Σ' is an* EUF-CMA *secure signature scheme (for arbitrary-length messages).*

2. RSA signatures

   - **[12.3 in book, 2nd edition] (2 Points)** In the lecture we have seen an attack on the textbook RSA signature scheme in which an attacker forges a signature on an arbitrary message using two signing queries. Show how an attacker can forge a signature on an arbitrary message using a single signing query.

3. DSA Signatures

   - **[12.7 in book, 2nd edition] (2 Points)** Consider a variant of DSA in which the message space is $\mathbb{Z}_q$ and H is omitted. (So the second component of the signature is now $s := k^{-1} \cdot (m + xr) \bmod q$.) Show that this variant is not secure.

4. One-time signatures

   - **(1 Point)** Write down the experiment for existential unfogeability under a one-time non-adaptive chosen message attack (EUF-1-naCMA security).
   - **(2 Points)** For the one-time signatures under the discrete logarithm problem from the lecture (slide 24) show the following theorem:

     Theorem 2 *If the discrete-logarithm problem is hard relative to $\mathcal{G}$, then the signature scheme is* EUF-1-naCMA *secure.*

[1] If you don't know how to do it, you can use e.g. `https://www.pdfmerge.com/`