6. Problem Set

Secure Channels

(Winter Term 2014/2015)

Bauhaus-Universität Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Jakob Wenzel (jakob.wenzel@uni-weimar.de)
URL: http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/

Date: 13.01.2015 (1:30 pm) **Room:** SR013, B11

Submit your solutions until **12th of January 2015, 12:00 am** via E-Mail or feed my postbox in Room 112.

Task 1 (3+3 Credits) Robustness – IACBC
Given a nonce N and a secret key K, the authenticated encryption mode IACBC encrypts a plaintext $M = m_1, \ldots, m_\ell$ to a ciphertext $C = c_1, \ldots, c_\ell$ as follows:

Initialization: Generate $\ell + 1$ values $s_0, \ldots, s_\ell$ (key stream) depending on N and K, but not on the plaintext M.

Encryption: $x_0 \leftarrow N$; For $i \in \{1, \ldots, \ell\} : x_i \leftarrow E_K(m_i \oplus x_{i-1}), C_i \leftarrow x_i \oplus s_i$.

Authentication: $T \leftarrow E_K(x_\ell \oplus \sum_{1 \le i \le \ell} m_i) \oplus s_0$.

a) Describe an efficient IND-CPA adversary against IACBC in the nonce-misuse setting.

b) Describe an efficient INT-CTXT adversary against IACBC in the nonce-misuse setting.

Task 2 (3 Credits) Generic SIV
Provide a proof for Theorem 37 (Slide 184, RoR-CPA plus UF-CMA is insufficient).

Task 3 (3 Credits) HCBC1
Provide a proof for Theorem 42 (Slide 194).

Task 4 (2+2+4+2+2 Credits) CHM
Consider the authenticated encryption scheme CHM (CENC with Hash-based MAC). See the following links for details:

- http://www.math.unicaen.fr/~nitaj/AFrica08Slides/slides-iwata.pdf
- https://eprint.iacr.org/2006/188.pdf

The decryption – as for almost all AE schemes – works as follows:

1. Decrypt the ciphertext.
2. Verify the integrity.
3. Return either the plaintext (if valid) or $\perp$ (if invalid).

Assume that one wants to use a smart card with only a small amount of memory to decrypt ciphertexts. Nevertheless, it should still be possible to process messages/ciphertexts of arbitrary length.

(a) Illustrate the AE scheme CHM (encryption, decryption, authentication).

(b) How can the decryption/verification work for CHM in this case?

(c) How can an adversary exploit the algorithm explained in b) to undermine the AE security definition?

(d) Explain a technique to avoid such attacks.

(e) To what extent are the results from (b)-(d) relevant for the AE scheme SIV?