Problem Set 5
Course **Secure Channels**
(Summer Term 2018)

Bauhaus-Universität Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Eik List
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/`

Due Date: 14 June 2018, 11:00 AM, via email to `eik.list(at)uni-weimar.de`.

In all tasks, let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a secure block cipher, and let all keys be secret and sampled independently uniformly at random.

Task 1 – Masks (2 Credits)

Inform yourselves about PMAC1 [3]. PMAC1 derives a masking key $\Theta = 10 \cdot E_K(0^n)$. Assume, you found two inputs to PMAC1, $M = (M_1, M_2, M_3)$ and $M' = (M'_1, M'_2, M'_3)$ with $M_1 \neq M'_1$ and $M_2 \neq M'_2$, whose outputs collide: $\text{PMAC1}[E_K](M) = \text{PMAC1}[E_K](M')$. Show **or** disprove briefly that such a collision can allow you to recover Θ with significant probability.

Task 2 – Universal-hashing-based MACs (4+4 Credits)

Polynomial hashing is used frequently. As you may remember from the 3rd problem set, one has to take care how the input length(s) are treated, and to avoid fix points such as all-zero blocks or empty inputs.

a) Consider CWC from [2], Section 3. Verify **or** falsify the following claim: It is possible to choose associated data A and a nonce $N \in \{0,1\}^{88}$ s. t. $(10^7 \,\|\, N \,\|\, 0^{32}) = \text{CWC-HASH}_K(A, C)$, which can break its integrity.

b) Inform yourselves about the Decrypted Wegman-Carter Davies-Meyer MAC, DWCDM [1] (mind the version of the paper, it might be updated). Verify **or** falsify the following claim: One can construct a forgery on its instantiation nPolyMAC with PolyHash in Section 4.4 with few queries.

Task 3 – Authenticated-Encryption Security (4 Credits)

Show **or** disprove in your own words Theorem 37, part 2: RoR-CPA-security + INT-CTXT-security $\Longrightarrow$ RoR-CCA-security.

This means: given a nonce-based authenticated encryption scheme $\Pi = (\mathcal{E}, \mathcal{D})$ that is RoR-CPA-secure and INT-CTXT-secure. Then, Π is also RoR-CCA-secure. By secure, we mean: for any RoR-CCA adversary $\mathbf{A}$ on Π, there exists a RoR-CPA adversary $\mathbf{A}$ on Π and an INT-CTXT-adversary $\mathbf{A}''$ on Π such that

$$\mathbf{Adv}_{\Pi}^{\text{RoR-CCA}}(\mathbf{A}) \leq \mathbf{Adv}_{\Pi}^{\text{RoR-CPA}}(\mathbf{A}') + \mathbf{Adv}_{\Pi}^{\text{INT-CTXT}}(\mathbf{A}'').$$

Task 4 – AE Security under Release of Unverified Plaintexts (4 Credits)
Consider a secure PRF $F : \mathcal{K} : \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \mathcal{T}$. Let $\mathrm{CTR}[E_{K_2}]$ be IV-based counter-mode. We define $\Pi = (\mathcal{E}, \mathcal{D})$ to denote $\mathrm{SIV}[F_{K_1}, \mathrm{CTR}[E_{K_2}]]$ with F_{K_1} as PRF and $\mathrm{CTR}[E_{K_2}]$ for encryption. We define the encryption and decryption as

```
function $\mathcal{E}_{K_1,K_2}(N, A, M)$
    $T \leftarrow F_{K_1}(N, A, M)$
    $C \leftarrow \mathrm{CTR}[E_{K_2}](T, M)$
    return $(C, T)$
end function
```

```
function $\mathcal{D}_{K_1,K_2}(N, A, C, T)$
    $M \leftarrow \mathrm{CTR}[E_{K_2}](T, C)$
    $b \leftarrow F_{K_1}(N, A, M) \overset{?}{=} T.$
    return $(M, b)$
end function
```

So, Π always outputs M and a bit b that tells if the ciphertext was valid. Sketch a proof **or** disprove that Π is INT-RUP-secure. This means, does there exist an INT-RUP adversary $\mathbf{A}$ on Π that can successfully forge with higher advantage than the birthday bound?

References

[1] Nilanjan Datta and Avijit Dutta and Mridul Nandi and Kan Yasuda: Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC. Cryptology ePrint Archive, Report 2018/500, Version: 20180528:045608. `https://eprint.iacr.org/2018/500` (Full version of the paper to appear at CRYPTO 2018).

[2] Tadayoshi Kohno, John Viega, Doug Whiting: CWC: A High-Performance Conventional Authenticated Encryption Mode. FSE 2004: 408-426. Full version at `https://eprint.iacr.org/2003/106.pdf`.

[3] Phillip Rogaway: Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. ASIACRYPT 2004: 16-31. `http://web.cs.ucdavis.edu/~rogaway/papers/offsets.pdf`.