Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

2. Exercise sheet
Hand in solutions until Monday, 3 November 2014, 13:59

Exercise 2.1 (UBK-KPA-security of AES-CBC2). (6 points)

Consider AES with CBC mode on two blocks: $\boxed{6}$

$$\text{AES-CBC2}\colon \begin{array}{rcl} \{0,1\}^{128} \times (\{0,1\}^{128} \times \{0,1\}^{128}) & \longrightarrow & \{0,1\}^{128} \times \{0,1\}^{128}, \\ (k, (p^L, p^R)) & \longmapsto & (c^L, c^R) \end{array}$$

with $c^L = \text{AES}_k(p^L)$, $c^R = \text{AES}_k(c^L \oplus p^R)$. Prove the following

Theorem. *If there is a (q, ε)-attacker against* AES-CBC2 *who tries to find the key and gets a plaintext/ciphertext pair oracle (UBK-KPA security), then there is a $(2q, \varepsilon)$-attacker against* AES *who tries to find the key and gets a plaintext/ ciphertext pair oracle (UBK-KPA security).*

In other words: if AES is UBK-KPA-secure then so is AES-CBC2.

Exercise 2.2 (IND-CPA-security of AES-CBC2). (12+4 points)

In this exercise, we change the security notion.

The *means* or attack scenario is CPA now, that is the attacker gets an oracle which on input $\text{ENCRYPT}(p_i)$ returns the corresponding ciphertext $c_i = \text{AES}_k(p_i)$ under the unknown key k.

The *task* however is different, it's indistinguishability: the attacker gets access to a challenge oracle and when he asks $\text{CHALLENGE}(p_0, p_1)$ this oracle randomly chooses a bit $s \in \{0,1\}$ and returns the encryption $c^* = \text{ENC}_k(p_s)$ of p_s. The attacker may use this oracle only once.

The attacker *succeeds* if

- the attacker gives the correct answer, ie. his output t is equal to s, and
- the attacker did not cheat, ie. neither p_0 nor p_1 have ever been returned as part of a plaintext/ciphertext pair.

A (q, ε)-attacker uses at most q oracle queries and has advantage at least ε, where the advantage is the success probability minus the guessing probability (here $\frac{1}{2}$).

$\boxed{8}$ (i) Prove or disprove

Theorem. *If there is a* (q, ε)*-attacker against* $\mathrm{AES\text{-}CBC2}$ *in the IND-CPA setting, then there is a* $(2q, \frac{\varepsilon}{2})$*-attacker against* AES *in the IND-CPA setting.*

$\boxed{4}$ (ii) What happens if we consider IND-KPA security?

$\boxed{+4}$ (iii) Formulate and prove a correct version considering IND-KPA security for $\mathrm{AES\text{-}CBC2}$.