# Esecurity: secure internet & e-cash, summer 2015

MICHAEL NÜSKEN

## 7. Exercise sheet
## Hand in solutions until Monday, 8 June 2015, 11:59

**Exercise 7.1** (Translate literature definition to challenger). (10 points)

In Krawczyk, Paterson & Wee (2013) we find the

**Definition** (OW-PCA forKEM). *For a stateful adversary $\mathcal{A}$ and a key encapsulation mechanism* kem *with algorithms* $(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$*, we define the advantage function*

$$\mathrm{Adv}^{OWPCA}_{\mathrm{kem}}(\mathcal{A}) := \mathrm{prob}\left[ K' = K^* \;\middle|\; \begin{array}{l} (\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{KeyGen}(1^\lambda) \\ (\psi^*, K^*) \leftarrow \mathrm{Enc}(\mathrm{pk}) \\ K' \leftarrow \mathcal{A}^{\mathrm{PCA}(\mathrm{sk},\cdot,\cdot)}(\mathrm{pk}, \psi^*) \end{array} \right]$$

*where* $\mathrm{PCA}(\mathrm{SK}, \cdot, \cdot)$ *is the oracle that takes as input* $(K, \psi)$ *with* $K \neq \perp$ *and outputs* $1$ *if* $\mathrm{Dec}(\mathrm{SK}, \psi) = K$ *and* $0$ *otherwise. An encryption scheme is said to be one-way against plaintext checking attacks (OW-PCA) if for all PPT adversaries A, the advantage* $\mathrm{Adv}^{OWPCA}_{\mathrm{kem}}(\mathcal{A})$ *is a negligible function in* $\lambda$*.*

*Hint*: A key encapsulation mechanism is similar to a public key encryption, but there is no message. The encapsulation routine Enc generates a session key and produces an encrypted version, that's the encapsulated key. The decapsulation routine Dec retrieves the key. Other than picking a random session key and encrypting it in a public key scheme, this 'picking' is part of the Encapsulation.

Write a challenger and redefine the advantage, just like we did in the course with other definitions. 10

**Exercise 7.2** (Never real-or-random). (6 points)

In the authenticated key exchange (AKE) model a key exchange is considered and the attacker's challenge is to tell whether a given key is real or random. 6

Assume that a key exchange produces a key $k$ which is indistinguishable from random. But then this key is used in an authenticated encryption scheme. (Formulate the game!) Show that the key in that combination is always distinguishable from random.

*Hint*: Just formalize what I told you in class.

**Exercise 7.3** (GCM: Galois Counter Mode). (0+10 points)

Find documentation and security proof for GCM.

+4 (i) Describe how the mode works. Which components are used? How are they put together? Argue for correctness.

+2 (ii) For use in which protocols (IPsec, TLS, SSH, GSM/UMTS/LTE, ...) is it standardized?

+4 (iii) In which model is it proved secure? Desribe which oracles are given to an attacker. How does the model relate to sLHAE?

[I do not need to say that you should do all this in your own words, do I?]

## References

HUGO KRAWCZYK, KENNETH G. PATERSON & HOETECK WEE (2013). On the Security of the TLS Protocol: A Systematic Analysis. *Cryptology ePrint Archive* **2013/339**, 49 pages. URL `http://eprint.iacr.org/2013/339`. Last visited 2 march 2015.