Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

7. Exercise sheet
Hand in solutions until Monday, 8 December 2014, 13:59

Let's have a look at some mid- and low-level symmetric primitives. Pick and solve one of the following exercises.

Exercise 7.1 (GCM: Galois Counter Mode). (10 points)

Find documentation and security proof for GCM.

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

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

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

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

Exercise 7.2 (*BLK*-CCM: *BLK*-CTR & CBC-MAC). (10 points)

Find documentation and security proof for CCM.

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

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

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

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

Exercise 7.3 (SNOW3G). (10 points)

Find the documentation on SNOW3G.

4 (i) Describe how it works. [A picture is probably helpful.] Argue for correctness.

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

4 (iii) What is known about its security? Which attacks are known? Describe one. [It's ok, if it's only an attack on a downgraded version. But mention the differences and what it means for the full version.]

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