Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

12. Exercise sheet
Hand in solutions until Monday, 2 February 2015, 13:59

Exercise 12.1 (sLHAE). (6+24 points)

Consider the paper Paterson, Ristenpart & Shrimpton (2011). It seems that the often mentioned 'full version' never appeared.

(i) Compare the definitions of CTXT and PTXT in Figure 5 to the definitions of INT-CTXT and INT-PTXT in Bellare & Namprempre (2000). +6

(ii) Interpret the definition for CRD in Figure 5 in your own words. +6

(iii) They claim that length-hiding IND-CPA and CTXT implies LHAE. Can you prove that? +6

(iv) They claim that MEE is length hiding IND-CPA and PTXT. Can you prove this? *Note*: The reference [3] there is Bellare & Namprempre (2000), which we started discussing in the lecture. +6

(v) They claim Theorem 1 stating that PTXT and CRD implies CTXT. Can you write the 'straightforward proof'? 6

References

MIHIR BELLARE & CHANATHIP NAMPREMPRE (2000). Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in Cryptology: Proceedings of ASIACRYPT 2000,* Kyoto, Japan, TATSUAKI OKAMOTO, editor, volume 1976 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Heidelberg. ISBN 3-540-41404-5. ISSN 0302-9743. URL `http://dx.doi.org/10.1007/3-540-44448-3_41`. See also the 2007 update at `http://cseweb.ucsd.edu/~mihir/papers/oem.html`.

KENNETH G. PATERSON, THOMAS RISTENPART & THOMAS SHRIMPTON (2011). Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol. In *Advances in Cryptology: Proceedings of ASIACRYPT 2011,* Seoul, South Korea, DONG HOON LEE & XIAOYUN WANG, editors, volume 7073 of *Lecture Notes in Computer Science*. Springer-Verlag. ISBN 978-3-642-25385-0. ISSN 0302-9743. URL `http://dx.doi.org/10.1007/978-3-642-25385-0_20`. See also `http://www.isg.rhul.ac.uk/~kp/mee-comp.pdf`.