Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

7. Exercise sheet
Hand in solutions until Sunday, 13 June 2010, 23.59 h

Exercise 7.1 (Pros and Cons of CTR). (10+4 points)

(i) Prove that you read +2

- HELGER LIPMAA, PHILLIP ROGAWAY, AND DAVID WAGNER. *Comments to NIST concerning AES modes of operation: CTR-mode encryption*. 2000

(ii) Prove that you read +2

- R. TIRTEA AND G. DECONINCK. *Specifications overview for counter mode of operation. security aspects in case of faults.* In Electrotechnical Conference, 2004. MELECON 2004. Proceedings of the 12th IEEE Mediterranean, pages 769–773 Vol.2, 2004.

(iii) Do you agree with the claim of the first paper, that "most of the perceived disadvantages of CTR mode are not valid criticisms, but rather caused by the lack of knowledge." 4

(iv) List and explain two Pros and two Cons of CTR found in the two texts – or elsewhere. 6

Exercise 7.2 (Protocols for Civitas). (13 points)

(i) Find 3

- MICHAEL R. CLARKSON, STEPHEN CHONG, ANDREW C. MYERS. *Civitas: Toward a Secure Voting System.* In Proc. IEEE Symposium on Security and Privacy, pages 354-368, May 2008.

and rewrite the Algorithms for ElGamal encryption (enc), ElGamal reencryption (reenc), ElGamal decryption (dec) and EqDlogs in additive notation.

(ii) Assume that an attacker can retrieve the plaintext from a ciphertext using only public knowledge and no oracle. Prove that the attacker can also solve CDH. 4

6 (iii) The protocol EqDlogs is a zero-knowledge proof. Generally, these have three properties:

- If the prover's claim is true, the verification returns true – always.
- If the prover's claim is false, the verification fails – with high probability.
- The verifier does not learn anything about the private information.

Now, an attacker would like to do the following:

(a) Receive a ciphertext c of a plaintext m.

(b) Return a ciphertext c' of a different plaintext $m' \neq m$.

(c) Convince a verifier that c' and c are encryptions of the same plaintext using the protocol EqDlog.

Argue that this is impossible (with high probability).