Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

6. Exercise sheet
Hand in solutions until Wednesday, 11 December 2013, 23:59

Exercise 6.1 (Security reduction). (8 points)

(i) Reconsider the proof sketch from the course that if the ElGamal signature scheme is EUF-CMA secure it is necessary that the discrete logarithm problem is hard. Which oracles were used? 2

Does the proof show the following? If the ElGamal signature scheme is EUF-KOA secure then the DLP is hard.

(ii) Now consider any signature scheme where a message is first hashed and then the hash value is signed. Assume that the signature scheme is EUF-CMA secure. Does this imply that the hash function is collision resistant? Prove your answer. 6