Advanced cryptography: Pairing-based cryptography winter term 2012/13

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

7. Exercise sheet
Hand in solutions until Monday, 17 December 2012, 23:59:59

Exercise 7.1 (Some easy calculations). (2 points)

Prove correctness of the Boneh-Franklin identity based cryptosystem. 2

Exercise 7.2 (Unsketching und generalizing). (15 points)

In the lecture we have encountered the Boneh-Franklin identity based cryptosystem. However, the definition of the system as well as the associated security reduction were only done in the symmetric setup. Generalize it such that it also works in the asymmetric setting. To do so, elaborate on the details of the proof. 15

Exercise 7.3 (Parallelity). (7 points)

Compare the relationship of Boneh-Franklin encryption and the Sakai, Ohgishi & Kasahara key-distribution system to ElGamal encryption and the Diffie-Hellman key-exchange. Which similarities do you observe? 7