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

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

10. Exercise sheet
Hand in solutions until Monday, 28 January 2013, 23:59:59

Exercise 10.1 (Correctness of Gentry's scheme). (3 points)

Prove correctness of Gentry's ID-based encryption scheme. 3

Exercise 10.2 (A signature scheme underlying Gentry's scheme). (10 points)

Specify the signature scheme underlying Gentry's id-based encryption scheme, by using Naor's observation that an IBE scheme that is secure against adaptive ID-attacks implies that you directly obtain a signature scheme that is secure against EF-CMA. 10

Exercise 10.3 (Two secret keys in Gentry's scheme). (4 points)

Assume in Gentry's ID-based encryption scheme you have two different private keys for a given ID. Can you derive any secret from it? 4

Exercise 10.4. (0+400 points)

Prove or disprove equivalence of BDH or DBDH with q-ABDHE or its decisional variant, respectively. +400