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

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

9. Exercise sheet
Hand in solutions until Monday, 21 January 2013, 23:59:59

Exercise 9.1 (Correctness of Water's encryption scheme). (3 points)

Prove correctness of Water's encryption scheme as presented in the lecture. 3

Exercise 9.2 (Security of Water's encryption scheme and BDH). (0+3 points)

Prove that if BDH is is easy, we can break Water's encryption scheme. +3

Exercise 9.3 (Creating). (10 points)

Try to understand how Waters has constructed his encryption scheme by working backwards: Try to explain the proof from the back, i.e. try to explain why it looks like it is. 10

Exercise 9.4 (Rest of the course). (0+10 points)

Have a look at the literature! Try to find interesting articles about pairing-based schemes that you would like to discuss in the lecture. +10