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

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

8. Exercise sheet
Hand in solutions until Monday, 07 January 2013, 23:59:59

Exercise 8.1 (Completing the proof). (15 points)

Fill the gaps of the security proof of the Boneh & Boyen cryptosystem presented in the lecture by reading the full version of the article to be found at 15

`http://eprint.iacr.org/2004/173`.

Exercise 8.2 (Pairings for mobile communication). (0+30 points)

In the last few month we have seen many different pairing based systems with amazing properties. Assume you want to construct a secure mobile voice communication app for smartphones. Analyze which properties we need in such a setting and try to figure out whether pairing based systems (with their special properties) are suitable for that task. Elaborate thoroughly on the details. +30