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

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

5. Exercise sheet
Hand in solutions until Monday, 26 November 2012, 23:59:59

Exercise 5.1 (Some reductions). (10 points)

Consider the setup from the lecture: We have two groups G_1 and G_3 with $\#G_1 = \#G_3 = \ell$ prime and a pairing $e\colon G_1 \times G_1 \to G_3$.

(i) Show that DBDH $\leq$ DDH$_{G_3}$. 5

(ii) Show that DL$_{G_3} \equiv$ (DL$_{G_1}$ and GTI). 5

Exercise 5.2 (Man-in-the-middle). (7 points)

Consider the Joux's three party key-exchange protocol. Show that the protocol is vulnerable to man-in-the-middle attacks, i.e. describe how a malicious fourth party can modify the protocol to be afterwards able to intercept all communication. 7

Exercise 5.3 (Notions). (5 points)

Explain why we call Smart's key agreement protocol "authenticated". 5

Exercise 5.4 (A simple proof). (4 points)

Show that the forward-security of Smart's authenticated key agreement protocol can be reduced to the BDH problem and vice versa. 4