Esecurity: secure internet & e-cash, summer 2015

MICHAEL NÜSKEN

11. Exercise sheet
Hand in solutions until Tuesday, 7 July 2015, 09:00

Exercise 11.1 (Details of the Ferguson cash system). (12+16 points)

(i) Consider possible transcripts of Protocol 4, namely syntactically correct sequence $(\widetilde{A}, a'', e, \widetilde{S})$. Prove:

(a) For any possible transcript and any a there is a unique choice for the remaining parameters a', e, $\widetilde{S}$. [4]

(b) Any possible transcript can occur as a transcript if and only if $\widetilde{S}^v = \widetilde{A} a'' g^e$. [4]

(c) A possible transcript can occur as a transcript if and only if Alice' target equation $S = a g^{f(a)}$ holds for any a and the S matching the possible transcript. [4]

(ii) Verify carefully the Ferguson Withdrawal protocol, namely that (***) in Protocol 6 holds. [4+4]

(iii) Can you generalize the system to multi-spendable coins? Say, such that every coin can be spent five times. [+8]