AARHUS UNIVERSITY, COMPUTER SCIENCE

Protocol Theory - Handin 6

JPeter Burgaard

March 8, 2017

1 EXERCISE 1

Let p, q be chosen as in Schnorr's protocol, and let $g, \bar{g}, h, \bar{h} \in \mathbb{Z}_p^*$ be of order q. Assume P gets as input w where $h = g^w \mod p$, $\bar{h} = \bar{g}^w \mod p$. Consider the following protocol:

1. P chooses r at random in Z_q and sends $a = g^r \mod p$, $\bar{a} = \bar{g}^r \mod p$ to V.
2. V chooses a challenge e at random in $\mathbb{Z}_{2^t}$ and sends it to P. Here, t is fixed such that $2^t < q$.
3. P sends $z = r + ew \mod q$ to V, who checks that $g^z = ah^e \mod p$ and $\bar{g}^z = \bar{a}\bar{h}^e \mod p$, that p, q are prime that $g, \bar{g}, h, \bar{h}$ have order q and accepts iff this is the case.

Prove that this is a Σ- protocol for equality of discrete logs, more precisely show that this is a Σ-protocol for the relation

$$\{(x, w) | x = (p, q, g, \bar{g}, h, \bar{h}) \quad and \quad h = g^w, \bar{h} = \bar{g}^w\}$$

- here it is understood that it should, also be satisfied that p, q are prime, that $w \in \mathbb{Z}_q$, and that $g, h, \bar{g}, \bar{h} \in \mathbb{Z}_p^*$ have order q.

COMPLETENESS

We see that the protocol have the 3-move form, and it trivially holds, if P, V follows the protocol, since $g^{r+ew} = g^z = ah^e = g^r(g^w)^e = g^{r+ew}$, and symmetricly for the $\bar{g}, \bar{h}$ and $\bar{a}$ version.

SPECIAL SOUNDNESS

$(\bar{a}, a, e, z), (\bar{a}, a, e', z')$ which gives us 4 equations

$$g^z = ah^e, g^{z'} = ah^{e'}, \bar{g}^z = \bar{a}\bar{h}^e, \bar{g}^{z'} = \bar{a}\bar{h}^{e'}$$

$$g^{z-z'} = \frac{g^z}{g^{z'}} = \frac{ah^e}{ah^{e'}} = h^(e-e')$$
$$\bar{g}^{z-z'} = \frac{\bar{g}^z}{\bar{g}^{z'}} = \frac{\bar{a}\bar{h}^e}{\bar{a}\bar{h}^{e'}} = \bar{h}^(e-e')$$

choose $w = (z-z')(e-e')^{-1}$ then it solves both equations

SPECIAL HONEST-VERIFIER ZERO-KNOWLEDGE

To simulate we choose at random $z \in \mathbb{Z}_p^*$ and $e \in \mathbb{Z}_q$ and compute both $a = g^z h^{-e}$ and $\bar{a} = \bar{g}^z \bar{h}^{-e}$, then the conversation $((a, \bar{a}), e, z)$ has the same distribution as a real conversation between a honest prover and a honest verifier.