AARHUS UNIVERSITY - COMPUTER SCIENCE

Protocol Theory - Handin 4

Peter Burgaard -201209175

March 1, 2017

EXERCISE 4

Consider the unconditionally hiding commitment scheme based on discrete logarithms, where the public key is $pk = (p, g, y)$ for a prim p, a generate g of $\mathbb{Z}_p^*$ and $y \in \mathbb{Z}_p^*$. And a commitment to b using randomness r has form $commit_{pk}(r, b) = y^b g^r \mod p$. The randomness r is chosen uniformly from $\mathbf{Z}_{p-1} = 0, 1, 2, \cdots, p-2$. Suppose a prover P has committed to bits b_1, b_2 using commitments c_1, c_2 where $b_1 \neq b_2$. Now P wants to convince the verifier V that the bits are different. We claim he can do this by sending to V a number $s \in \mathbb{Z}_{p-1}$ such that $c_1 c_2 = yg^s \mod p$

- Show how an honest P can compute the requiced s, and argue that the distribution of s is the same when $(b_1, b_2) = (0, 1)$ as when $(b_1, b_2) = (1, 0)$. This means that V learns nothing excepts that $b_1 \neq b_2$

  No matter the combination of (b_1, b_2) it is seen that

  $$(y^1 g^r) \cdot (y^0 g^{r'}) = yg^{r+r'} = (y^0 g^r) \cdot (y^1 g^{r'})$$

  It is thus posible for P to compute $s = r + r' \mod p - 1$

- Argue that if P has in fact committed in c_1, c_2 to $(0, 0)$ or $(1, 1)$, he cannot efficiently find s as above unless he can compute the discrete logarithm of y.

  We can calculate s as follows

  $$yg^s = (y^{b_1} g^r) \cdot (y^{b_2} g^{r'}) = y^{b_1+b_2} g^{r+r'}$$

from this we can isolate

$$g^s = y^{(b_1+b_2)-1} g^{r+r'} \implies g^{s-(r-r')} = y^{(b_1+b_2)-1}$$

which means by taking the log, we get

$$\log_g(y^{(b_1+b_2)-1}) + r + r' = s$$

- Argue in a similar way that P can convince V that he has committed to two bits that are *equal* by revealing s such that $c_1 c_2^{-1} = g^s \mod p$

  We see, that we will always have g^s with $s = r - r' \mod p-1$ since

$$\begin{aligned}
(y^{b_1} g^r) \cdot (y^{b_2} g^{r'})^{-1} &= (y^{b_1} g^r) \cdot (y^{-b_2} g^{-r'}) \\
&= y^{b_1 - b_2} g^{r-r'} \\
&= g^{r-r'} \\
&= g^s
\end{aligned}$$