AARHUS UNIVERSITY - COMPUTER SCIENCE

Protocol Theory - Handin 2

Peter Burgaard -201209175

February 8, 2017

EXERCISE 6

Let p be a prime, an g an elemen in the multiplicative group $\mathbb{Z}_p^*$ of order q. Such an element always exist if q divide $p-1$.

Note that the function $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*, x \mapsto g^x \mod p$ is a group homomorphism, namely $f(x+y \mod p-1) = f(x)f(y) \mod p$. It is generally believed that f is one-way for large enough primes p, q.

Use this assumption to construct an unconditionally hiding and computationally binding bit commitment scheme - use the RSA construction as inspiration, and write down the commitment function explicitly. Argue that if one can efficiently break the binding property, one can also efficiently solve the discrete log problem $\mod p$, i.e., invert f. Note that it is part of the construction that one can check that public key is correctly formed, in particular y must be in $Im(f)$. For this you may use (without proof) the fact that in $\mathbb{Z}_p^*$, an element is in the subgroup genereted by g if and only if it has order q.

We generate a public $pk = f(x) = g^x \mod q = y$ for $x \in_R \mathbb{Z}_{p-1}$ and $g \in_R \mathbb{Z}_p^*$. When commiting we use the function $commit_{pk}(b,r) = y^b \cdot f(r) \mod q = (g^x)^b \cdot g^r \mod q = g^{x \cdot b + r} \mod q$. Lets set $c = x \cdot b + r$, such that $commit_{pk}(b,r) = g^c \mod q$. If the prover were to change his mind, he would have to find a number k such that $g^x \cdot f(k) \mod q = g^{x \cdot k} \mod q = g^c \mod q$. Finding such a k is the same as solving the Diffie-Hellman problem, which by Lemma 1 in [DLBS - Damgård] is no harder than the discrete log problem. This implies, for a prover the binding property only holds if he can't solve the discret log problem.

As a matter of checking whether a pk is valid, since we map to a group of order q where each element is a generator of the whole group, so the verifier may send q such that we can calculate $pk^q \mod q = pk$ and $f(r)^q \mod q = f(r)$ for some $r \in_R \mathbb{Z}_{p-1}$, just to verify that the pk isn't a special element with the wanted characteristic. This should insure that $pk \in Im(f)$.