ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 5

5.1 Okamoto's ID Scheme

Let H be a cyclic group of prime order q and let $g, h \in H$ be two generators.
Construct a zero-knowledge interactive proof of knowledge such that, given some $z \in H$, allows Peggy to convince Vic that she knows some pair (x, y) such that $z = g^x h^y$. Prove that your protocol is complete, a proof of knowledge and zero-knowledge.

5.2 "OR"-Proof

Recall the GNI protocol for graphs $\mathcal{G}_0$ and $\mathcal{G}_1$ from the lecture. This protocol can be made zero-knowledge by requiring the verifier to prove to the prover that the graph $\mathcal{T}$ he sends is isomorphic to $\mathcal{G}_0$ or $\mathcal{G}_1$. In this exercise, we show how to construct such "OR"-proofs.

a) Consider three graphs $\mathcal{T}$, $\mathcal{G}_0$ and $\mathcal{G}_1$. Construct a zero-knowledge protocol that allows a prover P to convince a verifier V that he knows an isomorphism between $\mathcal{T} \cong \mathcal{G}_0$ or $\mathcal{T} \cong \mathcal{G}_1$.

More generally, consider an arbitrary protocol (P, V) satisfying the following conditions:

- The protocol is a three-move protocol drawing challenges uniformly at random from $\mathcal{C}$.
- The protocol is honest-verifier zero-knowledge.
- The protocol is 2-extractable for some predicate $Q(\cdot, \cdot)$.

b) Let x_0, x_1 be two instances of the protocol. Construct an honest-verifier zero-knowledge protocol that allows a prover P to convince a verifier V that he knows values w_0 with $Q(x_0, w_0) = 1$ *or* w_1 with $Q(x_1, w_1) = 1$ (or both). What is the exact predicate $Q'(\cdot, \cdot)$ underlying your protocol?

5.3 Guillou-Quisquater Protocol

Recall the Fiat-Shamir protocol we have seen in the lecture. This protocol allows Peggy to prove to Vic that she knows the square root of an element z modulo an RSA modulus m. We can generalize this protocol to an interactive proof of knowledge that allows Peggy to convince Vic that she knows the e-th root of z for prime e.[1]
Construct a zero-knowledge interactive proof of knowledge that allows Peggy to convince Vic that she knows the e-th root x modulo m of a given number $z \in \mathbb{Z}_m^*$, i.e., that she knows x such that $x^e = z$ in $\mathbb{Z}_m^*$. Prove that your protocol is complete, a proof of knowledge and zero-knowledge.

[1] Formally, we would consider e with $\gcd(e, \phi(m)) = 1$ so that the e-th root exists.