ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 4

4.1 Discrete Logarithms and Interactive Proofs

Consider a cyclic group H of prime order q, two generators h and g, and two arbitrary group elements elements $z_1, z_2 \in H$.

a) Construct an interactive protocol that allows a prover P to prove to a verifier V that

$$\log_h z_1 = \log_g z_2, \tag{1}$$

where $\log_h(\cdot)$ is the discrete logarithm in H to the base h.
HINT: Base your protocol on Schnorr's protocol. Note that (1) is equivalent to the existence of an x such that $z_1 = h^x$ and $z_2 = g^x$.

b) Analyze your protocol w.r.t. the completeness, soundness and zero-knowledge (for the honest verifier) properties. Is your protocol a proof of a statement? Is it a proof of knowledge? Justify your answers.

c) Compare your protocol from **a)** to Schnorr's protocol and find a unified view on both protocols.

4.2 The Zero-Knowledge Property

a) Prove that both the Fiat-Shamir and the graph-isomorphism protocols are perfectly zero-knowledge.

b) Why does your argument from **a)** not work for the Schnorr protocol? Modify the protocol such that it becomes zero-knowledge and argue (informally) why your modification preserves the proof-of-knowledge property.

c) The definition of the perfect zero-knowledge property requires that the simulator S be polynomially bounded. Why is this restriction important?

4.3 Proofs of Knowledge

In the lecture we will see that a convenient way for proving that an interactive proof is a proof of knowledge is the notion of 2-extractability. In the setting of three-move protocols[1], the idea of 2-extractability is that if the prover P can answer two different challenges that make V accept given the same first message, he can also extract the witness from the transcript.

a) Prove that the graph-isomorphism protocol is 2-extractable.

b) Prove that the Fiat-Shamir protocol is 2-extractable.

c) Prove that the Schnorr's protocol is 2-extractable.

[1] P sends a message, V sends a challenge and P sends a response.