ETH Zurich, Department of Computer Science
SS 2018

Prof. Ueli Maurer
Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 2

2.1 Definition of Interactive Proofs

An *interactive proof* of membership for some language L is a protocol between two interactive probabilistic algorithms P and V that satisfies the following properties:

(i) Completeness: If $x \in L$, then P makes V accept with probability at least $p = 3/4$.

(ii) Soundness: If $x \notin L$, then any probabilistic algorithm P' makes V accept with probability at most $q = 1/2$.

The class of all languages L for which there exists an interactive proof (P, V) with a polynomially bounded verifier V is denoted by **IP**. Note that the prover P is assumed to be unbounded, i.e., there are no restrictions on its computing power.

a) Name a language that is not in **IP**.

b) Show that a deterministic prover is as powerful as a probabilistic one, i.e., prove that for every interactive proof (P, V), there exists a deterministic $\widehat{P}$ such that $(\widehat{P}, V)$ is an interactive proof that accepts the same language. Hint: $\widehat{P}$ may use P and V (but only with fixed random coins).

c) Show that a language L for which there exists an interactive proof (P, V) with a deterministic verifier V is in **NP**.

d) Show that a language L for which there exists an interactive proof with $q = 0$ is in **NP**.

e) Argue that the definition of **IP** is independent of the actual choice of p and q. More precisely, given an interactive proof (P, V) with parameters $1 > p > q > 0$, construct an interactive proof (P', V') with parameters p', q' for $1 > p' > q' > 0$.

Hint: Use Hoeffding's inequality. Let $\varepsilon > 0$ and let $X_1, \ldots, X_n$ be i.i.d. Bernoulli random variables where $\overline{X} = \frac{1}{n} \sum X_i$ and $E[\overline{X}] = \mu$. Then it holds that:

$$P[\overline{X} \leq \mu - \varepsilon] \leq e^{-2n\varepsilon^2}$$
$$P[\overline{X} \geq \mu + \varepsilon] \leq e^{-2n\varepsilon^2}$$

2.2 Discrete Logarithms and Interactive Proofs

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

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

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

where $\log(\cdot)$ is the discrete logarithm in G.

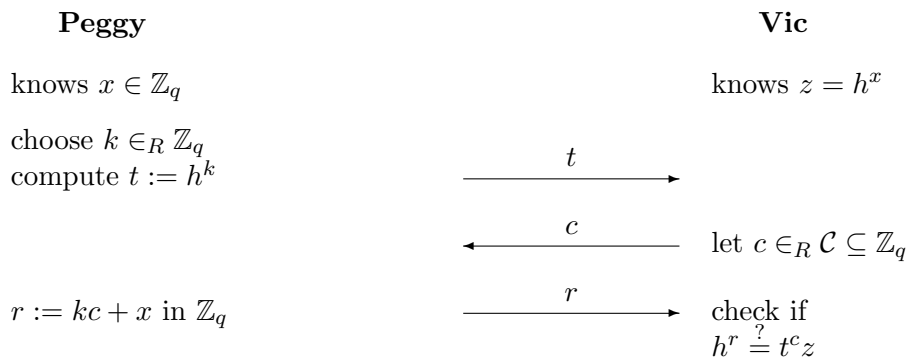
Hint: Base your protocol on Schnorr's. Note that (1) is equivalent to the existence of an x such that $z_1 = g^x$ and $z_2 = h^x$.

b) Analyze your protocol as a proof of statement. Is it honest-verifier zero-knowledge?. Is your protocol also a proof of knowledge?

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

2.3 A Modification of the Schnorr Protocol

Consider the following variation of Schnorr's protocol:



Is it complete and sound? What about zero-knowledge?

2.4 IP and PSPACE

Prove that **IP** $\subseteq$ **PSPACE**.