Prof. Dr. Johannes Blömer
Nils Löken, Fabian Eidens

July 8th, 2016
submission due: July 19th, 2016: 11 a.m.

Cryptographic Protocols

SS 2016

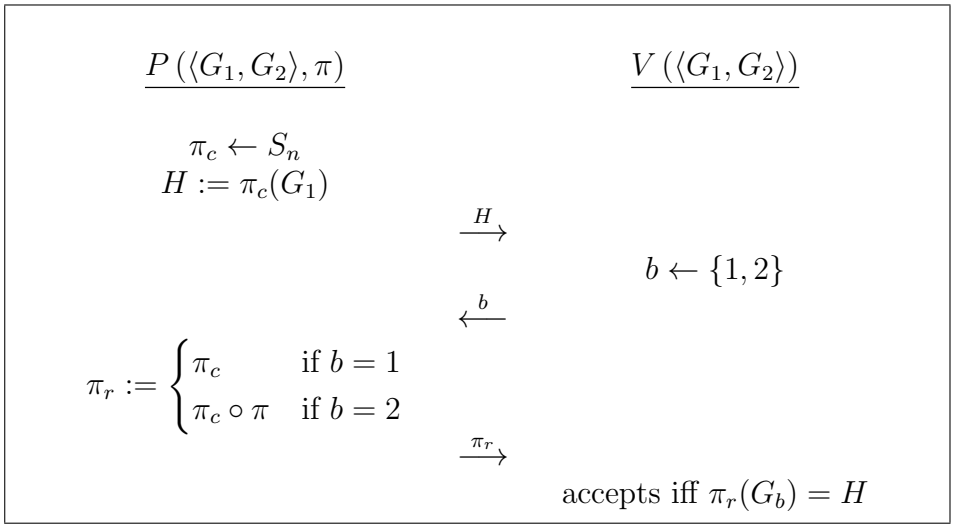
Handout 6

Exercises marked (*) or (**) will be checked by tutors.
We encourage submissions of solutions by small groups of up to four students.

Exercise 1 (4 points)**:**
(**) An undirected graph $G = (V, E)$ consists of the set of n vertices $V = \{1, \ldots, n\}$ and a set E of unordered pairs $\{i, j\} \subseteq V$ called edges. Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are called isomorphic if there exists a bijective mapping $\pi : V_1 \to V_2$ such that $\{i, j\} \in E_1$ if and only if $\{\pi(i), \pi(j)\} \in E_2$. In this case we write $G_1 = \pi(G_2)$ or $G_1 \simeq G_2$. Else they are non-isomorphic. Furthermore, denote S_n the group of permutations on V.
Consider the following protocol for the language

$$GI := \{\langle G_1, G_2\rangle | G_1 \simeq G_2\}$$

and prove, that it is perfect zero-knowledge.
Protocol: To prove the knowledge of π with $\pi(G_2) = G_1$ to V, the prover P runs the following protocol:

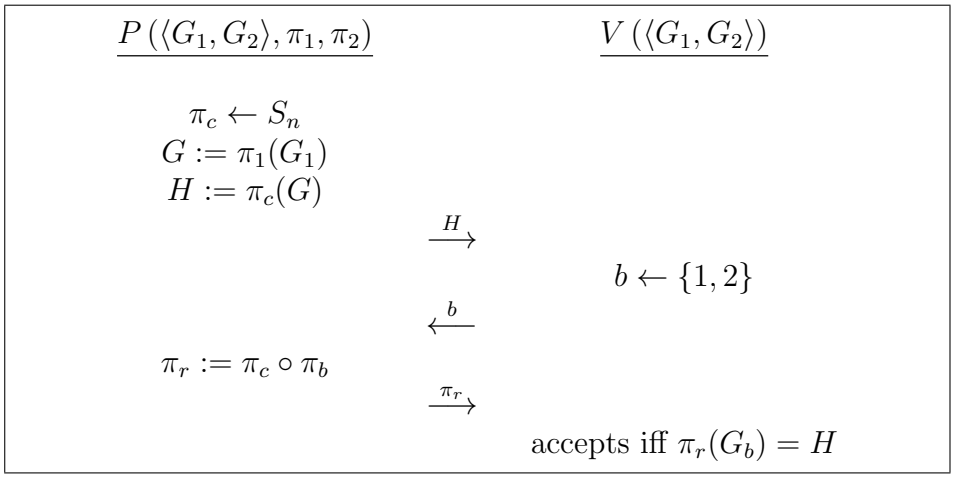


Hint: You may assume that all automorphism groups of all relevant graphs only contain the identity, i. e. for graph G and permutation π $\pi(G) = G$ implies $\pi = 1_{S_n}$.

Exercise 2:
Let $GI := \{\langle G_1, G_2\rangle | G_1 \simeq G_2\}$. Define the set of witnesses for $\langle G_1, G_2\rangle$ as

$$W(\langle G_1, G_2\rangle) = \{(\pi_1, \pi_2) \in S_n \times S_n | \pi_1(G_1) = \pi_2(G_2)\}.$$

Consider the following protocol:
Protocol: To prove the knowledge of witness (π_1, π_2) for $\langle G_1, G_2\rangle$ to V, the prover P runs the following protocol:



Prove, that this protocol is witness indistinguishable, that is for every witness $(\pi_1, \pi_2) \in W(\langle G_1, G_2\rangle)$ and all possible transcripts (H, b, π_r) of this protocol on input $\langle G_1, G_2\rangle$ there is an unique $\pi_c \in S_n$ chosen by P such that on input $\langle G_1, G_2\rangle$ the transcript is (H, b, π_r) and V accepts.

Hint: You may assume that all automorphism groups of all relevant graphs only contain the identity, i. e. for graph G and permutation π $\pi(G) = G$ implies $\pi = 1_{S_n}$.

Exercise 3:
Provide an EQ-composition of Σ-protocols in the discrete logarithm setting, i. e. let g, g' be two generators of groups of prime order q; present a protocol that proves knowledge of witness x_A corresponding to values $X_{A,1} := g^{x_A}$ and $X_{A,2} := g'^{x_A}$ simultaneously. Prove that your protocol is complete, special sound and special honest verifier zero knowledge.