ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 6

6.1 One-Way Homomorphism Zero-Knowledge Proofs of Knowledge

Construct zero-knowledge proofs of knowledge for the following settings:

a) Let m be an RSA modulus and $e_1, e_2 \in \mathbb{Z}_m$ such that $e_1 + e_2$ is prime. Let $z \in \mathbb{Z}_m^*$. Peggy wants to prove to Vic that she knows a pair $x, y \in \mathbb{Z}_m^*$, such that $z = x^{e_1} y^{e_2}$.

b) Let H be a cyclic group of prime order q and let h_1, h_2, and h_3 be three generators. Let $z_1, z_2 \in H$. Peggy wants to prove to Vic that she knows values $x_1, x_2, x_3, x_4 \in \mathbb{Z}_q$ such that $z_1 = h_1^{x_3} h_2^{x_1}$ and $z_2 = h_1^{x_2} h_2^{x_4} h_3^{x_1}$.

6.2 Perfectly Binding/Hiding Commitments

a) Prove that it is not possible that a commitment scheme is both perfectly hiding and perfectly binding.

For a string-commitment scheme of type H, let $C_H(x, r)$ denote the function that for a string $x \in \{0,1\}^*$ computes the corresponding blob b, where $b \in \{0,1\}^*$. Similarly, for a commitment scheme of type B, let $C_B(x, r)$ denote the function that for an $x \in \{0,1\}^*$ computes the corresponding blob $b \in \{0,1\}^*$. We combine these two schemes to design the following three schemes:

1. The blob b' corresponding to x is computed as $b' = (C_H(x, r_1), C_B(x, r_2))$.
2. The blob b' corresponding to x is computed as $b' = C_H(C_B(x, r_1), r_2)$.
3. The blob b' corresponding to x is computed as $b' = C_B(C_H(x, r_1), r_2)$.

b) Show that these three scheme are commitments schemes.

c) Which of these schemes are of type H/type B?

6.3 Graph Coloring

Consider an undirected graph $G = (V, E)$, where V denotes the set of vertices, and E the set of edges. A k-coloring of a graph is a labeling of the vertices with k different colors such that no two adjacent vertices have the same color. It is known that the 3-coloring problem, that is, deciding whether a given graph has a 3-coloring is NP-complete.

Construct a zero-knowledge protocol for graph 3-coloring. Is it a proof of knowledge or a proof of statement?