ETH Zurich, Department of Computer Science
SS 2019

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

Cryptographic Protocols
Exercise 4

4.1 "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?

4.2 Zero-Knowledge Proofs of Knowledge of a Preimage of a Group Homomorphism

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 $(x, y) \in \mathbb{Z}_m^* \times \mathbb{Z}_m^*$, 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. Peggy wants to prove to Vic that for two values $z_1, z_2 \in H$ 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 $z_2 = h_1^{x_2} h_2^{x_4} h_3^{x_1}$.

c) Let H be a cyclic group of prime order q. Consider the following protocol, presented in [CS97], to prove knowledge of discrete logs x_1, x_2 such that $z_1 = h_1^{x_1}$, $z_2 = h_2^{x_2}$ and $a_1 x_1 + a_2 x_2 = b$ for some known values $a_1, a_2, b \in \mathbb{Z}_q$ with $a_1, a_2 \neq 0$ and generators $h_1, h_2 \in H$:

Peggy		**Vic**
$(v_1, v_2) \in_R \{(u_1, u_2) \in \mathbb{Z}_q^2 :$ $a_1 u_1 + a_2 u_2 = 0\}$ $(t_1, t_2) = (h_1^{v_1}, h_2^{v_2})$	$\xrightarrow{(t_1, t_2)}$	
	$\xleftarrow{c}$	choose $c \in_R C \subseteq \mathbb{Z}_q$
$(r_1, r_2) = (v_1, v_2) + c(x_1, x_2)$	$\xrightarrow{(r_1, r_2)}$	check $h_1^{r_1} \stackrel{?}{=} t_1 \cdot z_1^c$ $h_2^{r_2} \stackrel{?}{=} t_2 \cdot z_2^c$ $a_1 r_1 + a_2 r_2 \stackrel{?}{=} cb$

Prove that the protocol is a zero-knowledge proof of knowledge. Can the problem be solved using the zero-knowledge proof of knowledge of a preimage of a group homomorphism?

References

[CS97] Jan Camenisch and Markus Stadler. Proof systems for general statements about discrete logarithms. *Technical report/Dept. of Computer Science, ETH Zürich*, 260, 1997.