ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Solution to Exercise 4

4.1 Discrete Logarithms and Interactive Proofs

a) Consider the following interactive protocol:

Peggy		**Vic**
knows x		knows $z_1 = g^x$, $z_2 = h^x$
choose $k \in_R \mathbb{Z}_p$ compute $t_1 = g^k$, $t_2 = h^k$	$\xrightarrow{(t_1, t_2)}$	
	$\xleftarrow{c}$	let $c \in_R \mathcal{C} \subseteq \mathbb{Z}_p$
$r = k + cx$ in $\mathbb{Z}_p$	$\xrightarrow{r}$	check if $(g^r, h^r) \stackrel{?}{=} (t_1 z_1^c, t_2 z_2^c)$

b) The protocol in **a)** can be seen both as a proof of the statement that $\log_g z_1 = \log_h z_2$ as well as proof of knowledge of the exponent x such that $z_1 = g^x$ and $z_2 = h^x$.

To prove that it is a proof of knowledge, we can observe that somebody able to provide two answers r, r' to two different challenges $c \neq c'$ for the same (t_1, t_2) successfully, can compute x as follows: Since Vic accepts,

$$(g^r, h^r) = (t_1 z_1^c, t_2 z_2^c) \quad \text{and} \quad (g^{r'}, h^{r'}) = (t_1 z_1^{c'}, t_2 z_2^{c'}).$$

Therefore,

$$(g^{r-r'}, h^{r-r'}) = (z_1^{c-c'}, z_2^{c-c'}) = (g^{x(c-c')}, h^{x(c-c')}),$$

and x can be computed by

$$x = \frac{r - r'}{c - c'}.$$

Note that the proof-of-knowledge property actually implies soundness, as we shall see once we formalize it properly.

Completeness: It is easily seen that Vic always accepts if Peggy knows x and follows the protocol.

Soundness: Suppose $z_1 = g^{x_1}$ and $z_2 = h^{x_2}$ for $x_1 \neq x_2$. Consider a cheating prover P' and assume her first message is (t_1, t_2). Such a message can be seen as $(t_1, t_2) = (g^{k_1}, h^{k_2})$ where $k_1 = \log_g t_1, k_2 = \log_h t_2$. Consider a challenge $c \in \mathcal{C}$. A reply r causing V to accept must satisfy

$$(g^r, h^r) = (g^{k_1} g^{cx_1}, h^{k_2} h^{cx_2}),$$

which is equivalent to

$$(g^r, g^{\ell \cdot r}) = (g^{k_1} g^{cx_1}, g^{\ell \cdot k_2} g^{\ell \cdot cx_2}),$$

where $\ell \in \mathbb{Z}_p$ is such that $h = g^\ell$. Thus, Vic accepts if and only if

$$r = k_1 + cx_1$$
$$r = k_2 + cx_2,$$

or, equivalently, if $k_1 + cx_1 = k_2 + cx_2$. This is satisfied only by a single $c \in \mathbb{Z}_p$, namely by $c = (k_2 - k_1)/(x_1 - x_2)$ (where the denominator is non-zero since $x_1 \neq x_2$). Thus, Vic accepts only if said c is chosen, i.e., with probability $1/|\mathcal{C}|$.

ZERO-KNOWLEDGE: For the honest verifier V, the zero-knowledge property is proved by showing that for any given challenge c, one can sample transcript triples with the correct conditional distribution. For a given c, simply sample a random r and set $t_1 := g^r z_1^{-c}$ and $t_2 := h^r z_2^{-c}$. The reader can verify that this results in the proper distribution.

c) Consider the mapping $\phi : \mathbb{Z}_p \to G$, $x \mapsto g^x$. For a group element $z \in G$, Schnorr's protocol allows to prove knowledge of a preimage x of z (w.r.t. to ϕ). The protocol in **a)** proceeds exactly like Schnorr's except that it works for the mapping $\phi' : \mathbb{Z}_q \to G \times G$, $x \mapsto (g^x, h^x)$. We will see in the next weeks how this can be generalized to any mapping that is a so-called *one-way homomorphism* between two groups.

4.2 The Zero-Knowledge Property

a) We prove that both protocols are *c-simulatable* and have the (obviously) polynomially-bounded challenge space $\mathcal{C} = \{0, 1\}$. Then, they are honest-verifier zero-knowledge, and, by Theorem 3.1 in Section 3.3.2 of the course notes, they are perfectly zero-knowledge.

Consider a single round between P and the honest V (for either protocol). Let $P_{TCR}(t, c, r)$ be the distribution of the triple (t, c, r) they produce. To prove c-simulatability one has to show that, for both challenges $c \in \{0, 1\}$, one can efficiently sample T and R such that $(T, R, c) \sim P_{TR|C}(\cdot, \cdot, c)$.

- FIAT-SHAMIR:[1] In an actual execution for the instance $z = x^2$, t is a random quadratic residue since it is chosen as $t = k^2$ for a random $k \in \mathbb{Z}_m^*$, and r is computed as $r = kx^c$. Note that r is computed bijectively from a random k and, therefore, choosing r randomly and computing $k = rx^{-c}$ and $t = k^2$ results in the same distribution. To avoid having to know the witness x, one simply chooses r randomly and directly computes $t = rz^{-c}$.
- GRAPH ISOMORPHISM: Let $(\mathcal{G}, \mathcal{H})$ be the instance. Given $c \in \{0, 1\}$, proceed as follows: Choose a random permutation ρ. If $c = 0$, set $\mathcal{T} := \rho\mathcal{G}\rho^{-1}$; if $c = 1$, set $\mathcal{T} := \rho\mathcal{H}\rho^{-1}$. In both cases, the resulting triple $(\mathcal{T}, c, \rho)$ has the desired distribution, i.e., when $c = 0$, then $\mathcal{T} = \rho\mathcal{G}\rho^{-1}$ is a random permutation of $\mathcal{G}$, and when $c = 1$, then $\mathcal{T} = \rho\mathcal{H}\rho^{-1}$ is a random permutation of $\mathcal{H}$ and thus of $\mathcal{G}$ (as in the real protocol).

b) The above argument fails for the Schnorr protocol, as the challenge space has size $|H|$ which is exponential in the size of the representation of z.

If one modifies the Schnorr protocol such that the challenge is chosen from any polynomially-sized set $\mathcal{C} \subseteq \mathbb{Z}_q$ with at least two elements, it becomes zero-knowledge and remains sound if it is repeated sufficiently often (for the original Schnorr protocol, a single round was sufficient).

c) The motivation for introducing a simulator is to state that everything Vic sees in an execution of the protocol he could have simulated himself. Since Vic is polinomially bounded, he can only run simulators that are polynomially bounded as well.

[1] See also Exercise 2.2.

4.3 Proofs of Knowledge

a) In the GI protocol, P proves knowledge of a permutation σ between two graphs $\mathcal{G}_0$ and $\mathcal{G}_1$ such that $\mathcal{G}_1 = \sigma\mathcal{G}_0\sigma^{-1}$. If P can provide two answers ρ_0, ρ_1 to two different challenges $c_0 = 0$ and $c_1 = 1$ for the same $\mathcal{T}$ such that V accepts:

$$\mathcal{T} = \rho_0\mathcal{G}_0\rho_0^{-1} \quad \text{and} \quad \mathcal{T} = \rho_1\mathcal{G}_1\rho_1^{-1}.$$

Therefore ρ_0 and ρ_1 satisfy:

$$\rho_0\mathcal{G}_0\rho_0^{-1} = \rho_1\mathcal{G}_1\rho_1^{-1}.$$

and

$$\rho_1^{-1}\rho_0\mathcal{G}_0\rho_0^{-1}\rho_1 = \mathcal{G}_1.$$

This means that P can compute σ as follows:

$$\sigma = \rho_1^{-1} \cdot \rho_0.$$

b) In the Fiat-Shamir protocol, P proves knowledge of a square root x of a given $z \in \mathbb{Z}_m^*$. If P can provide two answers r_0, r_1 to two different challenges $c_0 = 0$ and $c_1 = 1$ for the same t so that V accepts, this means that r_0 and r_1 satisfy:

$$r_0^2 = t \quad \text{and} \quad r_1^2 = t \cdot z$$

Therefore, P can compute:

$$x = r_0^{-1} \cdot r_1.$$

Because

$$x^2 = (r_0^{-1} \cdot r_1) \cdot (r_0^{-1} \cdot r_1) = t^{-1} \cdot (t \cdot z) = z.$$

c) In the Schnorr's protocol, P proves knowledge of a discrete logarithm x of a given $z \in H$, where $H = \langle h \rangle$ is a cyclic group of prime order. If P can provide two answers r, r' to two different challenges $c \neq c'$ for the same t successfully:

$$g^r = tz^c \quad \text{and} \quad g^{r'} = tz^{c'}.$$

Therefore,

$$g^{r-r'} = z^{c-c'} = g^{x(c-c')},$$

and P can compute x by

$$x = \frac{r - r'}{c - c'}.$$