ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Solution to Exercise 5

5.1 Okamoto's ID Scheme

One possible protocol for the task, which is along the lines of Schnorr's protocol, is the following one:

Peggy		**Vic**
knows $x, y \in \mathbb{Z}_q$ s.t $g^x h^y = z$		knows z
choose $k, l \in_R \mathbb{Z}_q$ compute $t := g^k h^l$	$\xrightarrow{\quad t \quad}$	
	$\xleftarrow{\quad c \quad}$	let $c \in_R \mathcal{C} \subseteq \mathbb{Z}_q$, $\lvert\mathcal{C}\rvert > 1$
$r := k + cx$ in $\mathbb{Z}_q$ $s := l + cy$ in $\mathbb{Z}_q$	$\xrightarrow{\quad (r,s) \quad}$	check if $g^r h^s \stackrel{?}{=} tz^c$

Completeness: It is easily verified that if Peggy is honest and knows (x, y), then Vic always accepts.

Proof of Knowledge: From the prover's replies to two different challenges for the same first message t, one can compute values x' and y' such that $g^{x'} h^{y'} = z$: Let $(t, c, (r, s))$ and $(t, c', (r', s'))$ be two accepting transcripts with $c \neq c'$. That is, $g^r h^s = tz^c$ and $g^{r'} h^{s'} = tz^{c'}$. By dividing the first equation by the second one we get:

$$g^{r-r'} h^{s-s'} = z^{c-c'},$$

which implies that $x' = \frac{r-r'}{c-c'}$ and $y' = \frac{s-s'}{c-c'}$ are values with $g^{x'} h^{y'} = z$. Note that since q is prime, $c - c' \neq 0$ has an inverse modulo q.

Zero-Knowledge: Similarly to all previous examples, the protocol is c-simulatable: Choose random $r, s \in \mathbb{Z}_q$ and set $t := g^r h^s z^{-c}$, which is easily checked to result in the correct distribution. If $\mathcal{C}$ is chosen to be polynomially large the protocol is zero-knowledge.

5.2 "OR"-Proof

a) Intuitively, the idea is that Vic sends Peggy a challenge c, and she has to give answers to two challenges that add up to c. This way, Peggy can use the simulator for GI to prepare for the isomorphism that she does not know. Let S be the simulator for the GI protocol.

Peggy		**Vic**
knows (b,σ): $\mathcal{T} = \sigma \mathcal{G}_b \sigma^{-1}$, $b \in \{0,1\}$		knows $\mathcal{T}, \mathcal{G}_0, \mathcal{G}_1$
$(\mathcal{T}_{1-b}, c_{1-b}, \rho_{1-b}) \leftarrow S(\mathcal{T}, \mathcal{G}_{1-b})$ choose random permutation π $\mathcal{T}_b := \pi \mathcal{T} \pi^{-1}$	$\xrightarrow{\mathcal{T}_0, \mathcal{T}_1}$	
	$\xleftarrow{c}$	choose $c \in_R \{0,1\}$
$c_b \equiv_2 c - c_{1-b}$ compute $\rho_b := \pi \sigma^{-c_b}$	$\xrightarrow{c_0, c_1, \rho_0, \rho_1}$	check $c_0 + c_1 \overset{?}{\equiv}_2 c$ for $i \in \{0,1\}$, check whether $\mathcal{T}_i = \rho_i \mathcal{T} \rho_i^{-1}$

The proof that this protocol is complete, a proof of knowledge and zero-knowledge is given in the next subtask for the general case.

b) The desired predicate is $Q'((x_0, x_1), (b, w)) := Q(x_b, w)$, where $b \in \{0,1\}$ indicates for which instance w is a witness.
In the following, let S be the HVZK simulator for (P, V) and let $\mathcal{C}$ be an additive group.

Peggy		**Vic**
knows (b, w)		knows (x_0, x_1)
$(t_{1-b}, c_{1-b}, r_{1-b}) \leftarrow S(x_{1-b})$ choose t_b according to P	$\xrightarrow{t_0, t_1}$	
	$\xleftarrow{c}$	choose $c \in_R \mathcal{C}$
$c_b := c - c_{1-b}$ compute r_b according to P	$\xrightarrow{c_0, c_1, r_0, r_1}$	check $c_0 + c_1 \overset{?}{=} c$ for $i = 0,1$, check whether (t_i, c_i, r_i) is valid according to V

Completeness: The protocol is easily seen to be complete.
Proof of Knowledge: The protocol is 2-extractable: Fix a first message (t_0, t_1) and let (c_0, c_1, r_0, r_1) and (c_0', c_1', r_0', r_1') be accepting answers for two challenges $c \neq c'$. Since $c \neq c'$, $c_i \neq c_i'$ for at least one $i \in \{0,1\}$. Since (t_i, c_i, r_i) and (t_i, c_i', r_i') are two accepting transcripts for the same first message, the 2-extractability of (P, V) allows to compute w such that $Q(x_i, w) = 1$. The witness for Q' is thus (i, w).
Honest-Verifier Zero-Knowledge: The simulator for the protocol is as following: Run the simulator honest-verifier simulator S on both instances x_0 and x_1: $(t_0, c_0, r_0) \leftarrow S(x_0)$ and $(t_1, c_1, r_1) \leftarrow S(x_1)$. The simulated transcript is $\big((t_0, t_1), c_0 + c_1, (c_0, c_1, r_0, r_1)\big)$.

Observe that since the challenges c_0 and c_1 are uniformly distributed, so is the challenge $c = c_0 + c_1$. Also, if we additionally have that $\mathcal{C}$ is polynomially bounded, we have that the protocol is zero-knowledge.

5.3 Guillou-Quisquater Protocol

A possible protocol for the task, generalizing Fiat-Shamir's protocol is the following one:

Peggy		**Vic**
knows $x \in \mathbb{Z}_m^*$		knows $z = x^e$
choose $k \in_R \mathbb{Z}_m^*$ compute $t := k^e$	$\xrightarrow{\quad t \quad}$	
	$\xleftarrow{\quad c \quad}$	let $c \in_R \mathcal{C} \subseteq [0, e-1]$, $\lvert\mathcal{C}\rvert > 1$
$r := k \cdot x^c$	$\xrightarrow{\quad r \quad}$	check if $r^e \stackrel{?}{=} t \cdot z^c$

Completeness: The protocol is easily seen to be complete.

Proof of Knowledge: The protocol is 2-extractable: Fix a first message t and let (c_0, r_0) and (c_1, r_1) be accepting answers for two challenges $c_0 \neq c_1$. That is, $r_0^e = t \cdot z^{c_0}$ and $r_1^e = t \cdot z^{c_1}$. We have:

$$\left(\frac{r_0}{r_1}\right)^e = z^{c_0 - c_1}.$$

Hence, we have two different powers of x: $\frac{r_0}{r_1} = x^{c_0 - c_1}$, and $z = x^e$. Moreover, since $c_0, c_1 \in [0, e-1]$ and e is prime, e is coprime with $c_0 - c_1$, so we can use Euclid's extended algorithm to find coefficients a, b such that $ae + b(c_0 - c_1) = 1$. This means:

$$x = x^{ae + b(c_0 - c_1)} = (x^e)^a \cdot (x^{c_0 - c_1})^b = z^a \cdot \left(\frac{r_0}{r_1}\right)^b.$$

Zero-Knowledge: The protocol is c-simulatable: Given $c \in \mathcal{C}$, choose random $r \in_R \mathbb{Z}_m^*$, and set $r := r^e \cdot z^{-c}$, which is easily checked to result in the correct distribution. If $\mathcal{C}$ is chosen polynomially bounded, the protocol is zero-knowledge.