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:

\begin{align*}
\text{Peggy} & \quad \text{Vic} \\
\text{knows } x, y \in \mathbb{Z}_q \text{ s.t } g^x h^y = z & \quad \text{knows } z \\
\text{choose } k, l \in R \mathbb{Z}_q & \quad t \\
\text{compute } t := g^k h^l & \quad c \\
\text{let } c \in R \mathcal{C} \subseteq \mathbb{Z}_q, |\mathcal{C}| > 1 \\
\text{in } \mathbb{Z}_q & \quad (r, s) \\
r := k + cx & \quad \text{check if } g^r h^s \stackrel{?}{=} t z^c \\
s := l + cy & \quad \text{such that } g^{x'} h^{y'} = z \\
& \quad \text{Let } (t, c, (r, s)) \\
& \quad \text{and } (t, c', (r', s')) \text{ be two accepting transcripts with } c \neq c'. \\
& \quad \text{That is, } g^r h^s = tz^c \text{ and } g^{r'} h^{s'} = tz^{c'}. \text{ By dividing the first equation by the second one we get:} \\
g^{r-r'} h^{s-s'} = z^{c-c'}, \\
\text{which implies that } x' = \frac{z-r'}{c-c'} \text{ and } y' = \frac{z-s'}{c-c'} \text{ are values with } g^{x'} h^{y'} = z. \text{ Note that since } q \text{ is prime, } c - c' \neq 0 \text{ has an inverse modulo } q. \\
\text{Zero-Knowledge: Similarly to all previous examples, the protocol is } c\text{-simulatable: Choose random } r, s \in \mathbb{Z}_q \text{ and set } t := g^r h^s z^{-c}, \text{ which is easily checked to result in the correct distribution. If } \mathcal{C} \text{ is chosen to be polynomially large the protocol is zero-knowledge.}
\end{align*}
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

knows $(b,\sigma)$: $T = \sigma g_b \sigma^{-1}$, $b \in \{0,1\}$

$(T_{1-b}, c_{1-b}, \rho_{1-b}) \leftarrow S(T, G_{1-b})$

choose random permutation $\pi$

$T_b := \pi T \pi^{-1}$

Vic

knows $T, G_0, G_1$

\[ c \]

choose $c \in_R \{0,1\}$

\[ c_b \equiv 2c - c_{1-b} \]

compute $\rho_b := \pi \sigma^{-c_0}$

\[ c_0, c_1, \rho_0, \rho_1 \]

check $c_0 + c_1 \equiv_2 c$

for $i \in \{0,1\}$, check whether $T_i = \rho_i T \rho_i^{-1}$

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 $C$ be an additive group.

Peggy

knows $(b, w)$

$(t_{1-b}, c_{1-b}, r_{1-b}) \leftarrow S(x_{1-b})$

choose $t_b$ according to $P$

Vic

knows $(x_0, x_1)$

\[ t_0, t_1 \]

choose $c \in_R C$

\[ c \]

check $c_0 + c_1 \equiv c$

for $i = 0, 1$, check whether $(t_i, c_i, r_i)$ is valid according to $V$

\[ c_b := c - c_{1-b} \]

compute $r_b$ according to $P$

\[ c_0, c_1, r_0, r_1 \]

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 $((t_0, t_1), c_0 + c_1, (c_0, c_1, r_0, r_1))$. 
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**

knows $x \in \mathbb{Z}_m^*$  
choose $k \in R \mathbb{Z}_m^*$  
compute $t := k^e$  
r := $k \cdot x^e$

**Vic**

knows $z = x^c$

$t$  
$c$  
r

let $c \in R \mathcal{C} \subseteq [0, e - 1]$, $|\mathcal{C}| > 1$

check if $r^e \equiv t \cdot z^c$

**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 $e$-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.