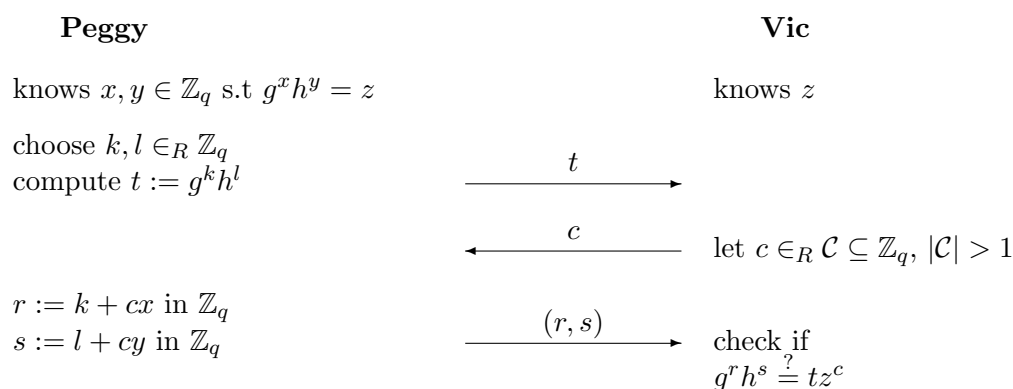


Cryptographic Protocols

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:



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:

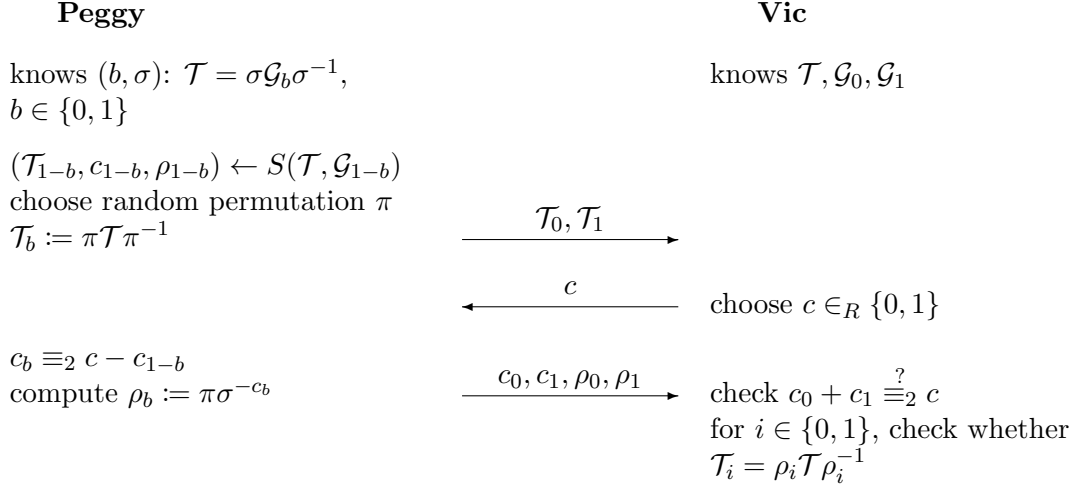
$$g^{r-r'} h^{s-s'} = z^{c-c'},$$

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

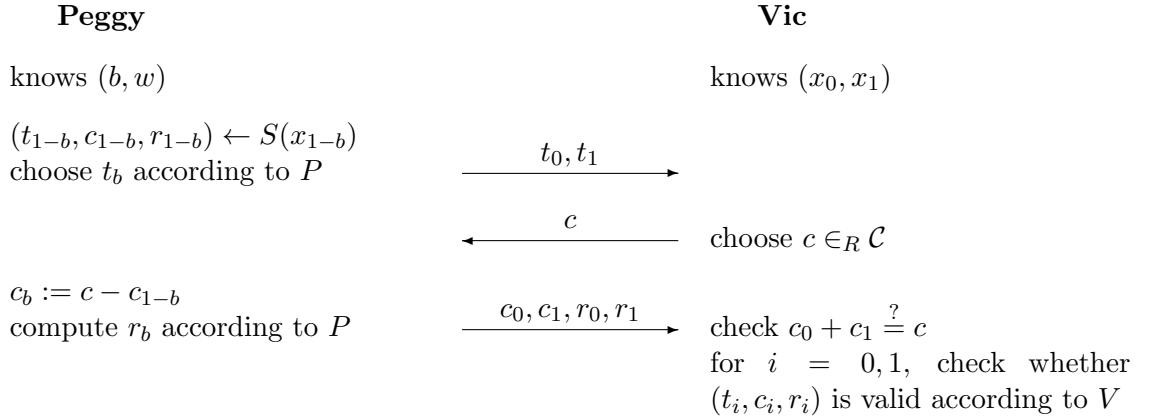
- a) Intuitively, the idea is that Vic sends Peggy a challenge c , and she has to give answers to two challenges that add up to c . This way, Peggy can use the simulator for GI to prepare for the isomorphism that she does not know. Let S be the simulator for the GI protocol.



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.



COMPLETENESS: The protocol is easily seen to be complete.

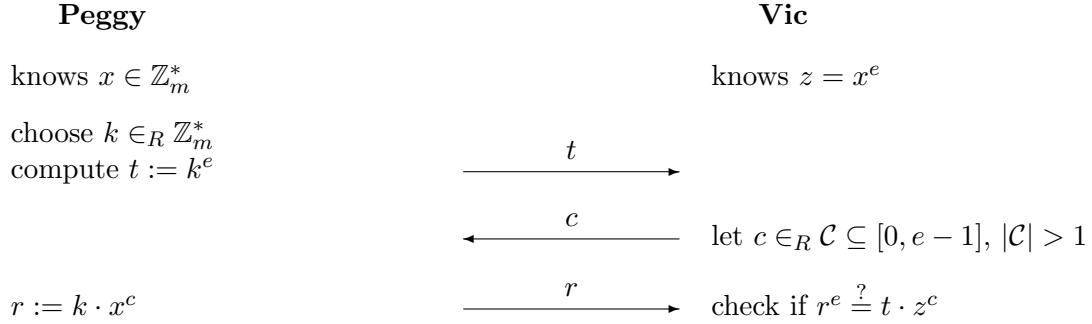
PROOF OF KNOWLEDGE: The protocol is 2-extractable: Fix a first message (t_0, t_1) and let (c_0, c_1, r_0, r_1) and (c'_0, c'_1, r'_0, r'_1) be accepting answers for two challenges $c \neq c'$. Since $c \neq c'$, $c_i \neq c'_i$ for at least one $i \in \{0, 1\}$. Since (t_i, c_i, r_i) and (t_i, c'_i, 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:



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.