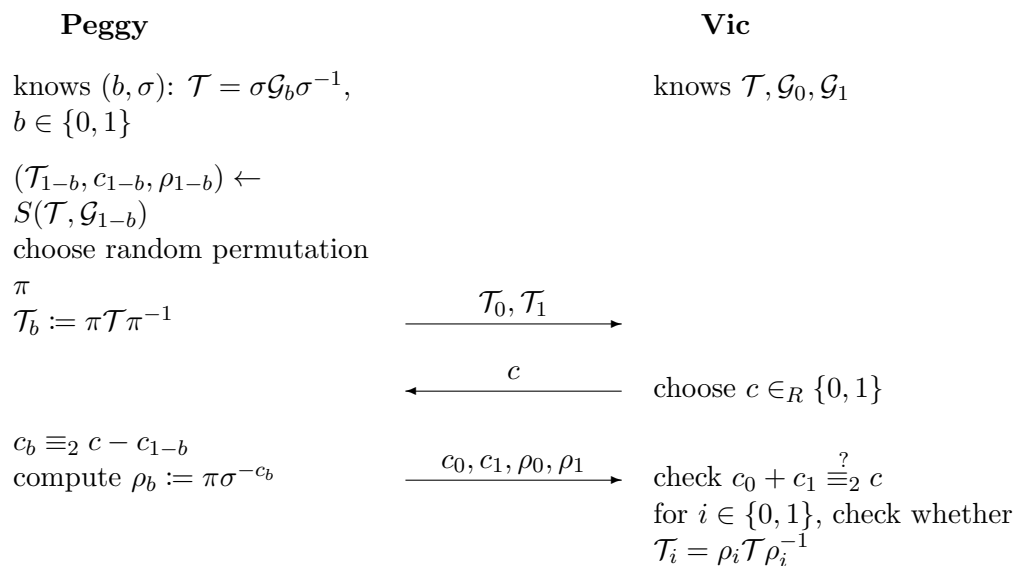


## Cryptographic Protocols

### Solution to Exercise 4

#### 4.1 “OR”-Proof

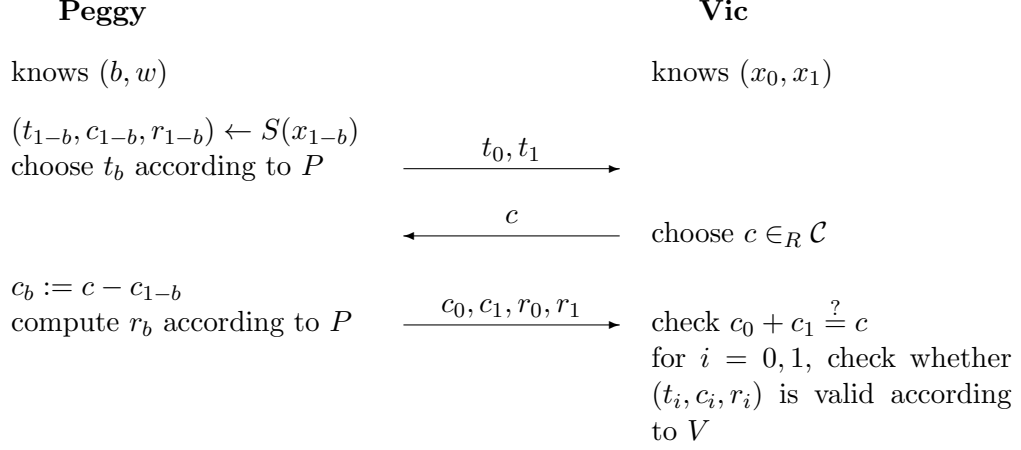
- a) Intuitively, the idea is that Vic sends Peggy a challenge  $c$ , and she has to give answers to two challenges that add up to  $c$ . This way, Peggy can use the simulator for GI to prepare for the isomorphism that she does not know. Let  $S$  be the simulator for the GI protocol.



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.

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

The protocols are instantiations of the proof of knowledge of a pre-image of a one-way group homomorphism. That is, for each scenario, one needs to provide a suitable homomorphism  $\phi$  between two groups,  $u$  and  $\ell$  (for each  $z$ ), as well as a challenge space  $\mathcal{C}$  such that the preconditions of the theorem are satisfied.

a) Let  $\phi : \mathbb{Z}_m^* \times \mathbb{Z}_m^* \rightarrow \mathbb{Z}_m^*$ ,  $(x, y) \mapsto x^{e_1} y^{e_2}$ . Then,  $\phi$  is a homomorphism since

$$\begin{aligned} \phi((x, y) \cdot (x', y')) &= \phi((xx', yy')) = (xx')^{e_1} (yy')^{e_2} = x^{e_1} y^{e_2} x'^{e_1} y'^{e_2} \\ &= \phi(x, y) \cdot \phi(x', y'). \end{aligned}$$

Let  $\mathcal{C} \subseteq \{0, \dots, e_1 + e_2 - 1\}$  be polynomially bounded. For  $z \in \mathbb{Z}_m^*$ , let  $u := (z, z)$  and  $\ell := e_1 + e_2$ . Then,

1.  $\ell$  is prime, and thus  $\gcd(c_1 - c_2, \ell) = 1$  for all  $c_1, c_2 \in \mathcal{C}$ , and
2.  $\phi(u) = \phi(z, z) = z^{e_1} z^{e_2} = z^{e_1 + e_2} = z^\ell$ .

b) Let  $\phi : \mathbb{Z}_q^4 \rightarrow H^2$ ,  $(x_1, x_2, x_3, x_4) \mapsto (z_1, z_2) = (h_1^{x_3} h_2^{x_1}, h_1^{x_2} h_2^{x_4} h_3^{x_1})$ . Clearly,  $\phi$  is a

homomorphism since

$$\begin{aligned}
& \phi((x_1, x_2, x_3, x_4) + (x'_1, x'_2, x'_3, x'_4)) \\
&= (h_1^{x_3+x'_3} h_2^{x_1+x'_1}, h_1^{x_2+x'_2} h_2^{x_4+x'_4} h_3^{x_1+x'_1}) \\
&= (h_1^{x_3} h_2^{x_1} \cdot h_1^{x'_3} h_2^{x'_1}, h_1^{x_2} h_2^{x_4} h_3^{x_1} \cdot h_1^{x'_2} h_2^{x'_4} h_3^{x'_1}) \\
&= (h_1^{x_3} h_2^{x_1}, h_1^{x_2} h_2^{x_4} h_3^{x_1}) \cdot (h_1^{x'_3} h_2^{x'_1}, h_1^{x'_2} h_2^{x'_4} h_3^{x'_1}) \\
&= \phi((x_1, x_2, x_3, x_4)) \cdot \phi((x'_1, x'_2, x'_3, x'_4)).
\end{aligned}$$

Let  $\mathcal{C} \subseteq \mathbb{Z}_q$ . For  $z \in H^2$ , let  $u := (0, 0, 0, 0)$  and  $\ell := q$ . Then,

1.  $\ell$  is prime, and thus  $\gcd(c_1 - c_2, \ell) = 1$  for all  $c_1, c_2 \in \mathcal{C}$ , and
2.  $\phi(u) = \phi(0, 0, 0, 0) = (1, 1) = z^q = z^\ell$ .

c) **COMPLETENESS:** The protocol is easily seen to be complete.

**PROOF OF KNOWLEDGE:** The protocol is 2-extractable: Fix a first message  $(t_1, t_2)$  and let  $(r_1, r_2)$  and  $(r'_1, r'_2)$  be accepting answers for two challenges  $c \neq c'$ . Since both answers are accepting, this means that  $h_1^{r_1} = t_1 \cdot z_1^c$ ,  $h_2^{r_2} = t_2 \cdot z_2^c$ ,  $h_1^{r'_1} = t_1 \cdot z_1^{c'}$ ,  $h_2^{r'_2} = t_2 \cdot z_2^{c'}$ ,  $a_1 r_1 + a_2 r_2 = cb$  and  $a_1 r'_1 + a_2 r'_2 = c'b$ . From here, one can obtain that  $h_1^{r_1 - r'_1} = z_1^{c - c'} = h_1^{x_1(c - c')}$  and  $h_2^{r_2 - r'_2} = z_2^{c - c'} = h_2^{x_2(c - c')}$ . Hence,  $x_1 = \frac{r_1 - r'_1}{c - c'}$  and  $x_2 = \frac{r_2 - r'_2}{c - c'}$ . Also,  $a_1 x_1 + a_2 x_2 = a_1 \frac{r_1 - r'_1}{c - c'} + a_2 \frac{r_2 - r'_2}{c - c'} = \frac{1}{c - c'}(a_1 r_1 + a_2 r_2 - a_1 r'_1 - a_2 r'_2) = \frac{1}{c - c'}(cb - c'b) = b$ .

**ZERO-KNOWLEDGE:** We restrict the challenge space to be polynomially bounded. Then, as seen in the lecture, it is enough to show that the protocol is  $c$ -simulatable. Given a challenge  $c \in \mathcal{C}$ , we can sample a random pair  $(r_1, r_2)$  from  $S := \{(s_1, s_2) \in \mathbb{Z}_q^2 : a_1 s_1 + a_2 s_2 = cb\}$ . Then, we assign  $t_1 = h_1^{r_1} z_1^{-c}$  and  $t_2 = h_2^{r_2} z_2^{-c}$ . Observe that the distribution is as in the protocol execution. In the protocol execution  $(r_1, r_2) = (v_1, v_2) + c(x_1, x_2)$ , where  $(v_1, v_2)$  is a random pair that satisfies  $a_1 v_1 + a_2 v_2 = 0$ , and  $(x_1, x_2)$  is a pair that satisfies  $a_1 x_1 + a_2 x_2 = b$ . Then, the pair  $(r_1, r_2)$  is a random pair that satisfies  $a_1 r_1 + a_2 r_2 = cb$ .

The problem can actually be solved as using the zero-knowledge proof of knowledge for a preimage of a homomorphism.

Let  $h$  be a generator from  $H$ , and let us define  $h_3 := h^{a_1}$ ,  $h_4 := h^{a_2}$ . Moreover, we define the homomorphism  $\phi : \mathbb{Z}_q^2 \rightarrow H^3, (x_1, x_2) \mapsto (h_1^{x_1}, h_2^{x_2}, h_3^{x_1} h_4^{x_2})$ . The goal is to prove knowledge of a preimage of the triple  $(z_1, z_2, h^b)$ . It is easy to see that with  $u := (0, 0)$  and  $\ell := q$ , we have the conditions:  $\gcd(c_1 - c_2, \ell) = 1$  for all  $c_1, c_2 \in \mathcal{C}$ , and  $\phi(u) = \phi(0, 0) = (1, 1, 1) = z^q = z^\ell$ .