

# Cryptographic Protocols

## Exercise 5

### 5.1 Perfectly Binding/Hiding Commitments

- a) Prove that it is not possible that a commitment scheme is both perfectly hiding and perfectly binding.

For a string-commitment scheme of type H, let  $C_H(x, r)$  denote the function that for a string  $x \in \{0, 1\}^*$  computes the corresponding blob  $b$ , where  $b \in \{0, 1\}^*$ . Similarly, for a commitment scheme of type B, let  $C_B(x, r)$  denote the function that for an  $x \in \{0, 1\}^*$  computes the corresponding blob  $b \in \{0, 1\}^*$ . We combine these two schemes to design the following three schemes:

1. The blob  $b'$  corresponding to  $x$  is computed as  $b' = (C_H(x, r_1), C_B(x, r_2))$ .
2. The blob  $b'$  corresponding to  $x$  is computed as  $b' = C_H(C_B(x, r_1), r_2)$ .
3. The blob  $b'$  corresponding to  $x$  is computed as  $b' = C_B(C_H(x, r_1), r_2)$ .

b) Show that the three schemes are commitment schemes.

c) Which of these schemes are of type H/type B?

### 5.2 Graph Coloring

Consider an undirected graph  $G = (V, E)$ , where  $V$  denotes the set of vertices, and  $E$  the set of edges. A  $k$ -coloring of a graph is a labeling of the vertices with  $k$  different colors such that no two adjacent vertices have the same color. It is known that the 3-coloring problem, that is, deciding whether a given graph has a 3-coloring is NP-complete.

Construct a zero-knowledge protocol for graph 3-coloring. Is it a proof of knowledge or a proof of statement?

### 5.3 Homomorphic Commitments

Consider the following bit-commitment scheme based on the quadratic residuosity assumption: For an RSA modulus  $m = pq$  and a quadratic non-residue  $t$ ,<sup>1</sup> Peggy commits to  $x \in \{0, 1\}$  by choosing  $r \in_R \mathbb{Z}_m^*$  and computing the blob  $b = r^2 t^x$ . To open the commitment, Peggy sends  $r$  and  $x$  to Vic, who checks that  $b \stackrel{?}{=} r^2 t^x$ .

- a) Show that this commitment scheme is homomorphic, i.e., show that from two blobs  $b_0$  and  $b_1$  for two bits  $x_0$  and  $x_1$ , a blob  $b$  for the bit  $x_0 \oplus x_1$  can be computed. Also show how Peggy can compute the randomness  $r$  (given  $r_0$  and  $r_1$ ), such that she can open  $b$  using  $r$ .

---

<sup>1</sup>For technical reasons, one would need to require that  $t$  has Jacobi symbol 1.

- b) Show that from a blob  $b$  for bit  $x$ , one can compute a blob  $b'$  corresponding to a commitment to  $1 - x$ . Again, show how Peggy can compute the randomness  $r'$  of blob  $b'$ .
- c) Assume two blobs  $b_0$  and  $b_1$  for  $x_0$  and  $x_1$  are given. How could Peggy prove to Vic in zero-knowledge that  $x_0 = x_1$ ? What about  $x_0 \neq x_1$ ?

#### 5.4 Sudoku

An instance of the general Sudoku problem consists of an  $n \times n$  grid with subgrids of size  $k \times k$  for  $n = k^2$ . Some cells are already preprinted with values in the range  $\{1, \dots, n\}$ . The goal is to fill the remaining cells with numbers from the same range such that each number appears exactly once in each row, column, and subgrid. For  $n = 9$  and  $k = 3$ , one recovers the classical Sudoku that is typically found in newspapers.

In the lecture we saw a proof that a given Sudoku has a solution. However, this protocol is not 2-extractable (why?), and it is not clear whether it is a proof of knowledge.

The goal of this task is to design a zero-knowledge protocol that allows Peggy to prove that she *knows* a solution of a given Sudoku. For that, assume that a commitment scheme of type B is given along with a protocol that allows to prove in zero-knowledge that two blobs are commitments to equal values.