ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

# Cryptographic Protocols
# Exercise 7

### 7.1 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 $t$,[1] 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 $r$.

**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)** Why would it be interesting for the BCC protocol if one could perform *all* binary operations on these blobs?

**d)** 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 $x_0 \neq x_1$?

### 7.2 Permuted Truth Tables

In their protocol, which we discussed in the lecture, Brassard, Chaum, and Crépeau use "permuted" truth tables of binary logical operations.

| x | y | x ∧ y |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

truth table

| x | y | x ∧ y |
|---|---|---|
| 1 | 0 | 0 |
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 1 | 1 |

"permuted" truth table

In this exercise we consider an alternative way of processing gates in a circuit:

**a)** 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. Let $c_1$, $c_2$, and $c_3$ be blobs for the bits $b_1$, $b_2$, and $b_3$, respectively. Construct a zero-knowledge protocol which allows Peggy to convince Vic that $b_3 = b_1 \wedge b_2$. Show that your protocol is complete, sound, and zero-knowledge.

Hint: Use an approach based on "permuted" truth tables.

[1] For technical reasons, one would need to require that $t$ has Jacobi symbol 1.

**b)** Show how Peggy can use the above construction to prove for an arbitrary circuit that she knows an input that evaluates to a given output.

**c)** Discuss the difference between the process from **b)** and the one described in the BCC protocol.

## 7.3 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.