ETH Zurich, Department of Computer Science
SS 2021

Prof. Ueli Maurer
Dr. Martin Hirt
Konstantin Gegier
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 6

6.1 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 $\{1, \ldots, n\}$. 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.

6.2 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:

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.

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) What is the difference between the process from **b)** and the one described in the BCC protocol?