ETH Zurich, Department of Computer Science
SS 2021

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

Cryptographic Protocols
Exercise 14

14.1 Multiplication Triples of Different Degree

The efficient actively secure MPC protocol seen in the lecture consists of a preparation phase, where multiplication triples are generated using Player Elimination, and a computation phase, where the circuit is evaluated. Consider the following modification to the preparation phase:

Instead of always generating multiplication triples of degree t, after some players are eliminated, multiplication triples of degree t' are generated. Is the modified protocol secure?

HINT: Consider the computation of a value $y = (x_1 \cdot x_2) + (x_3 \cdot x_4)$ where $n = 10$ and $t = 3$.

14.2 Properties of Hyper-Invertible Matrices 2

Recall the definitions of hyper-invertible matrices and hyper-invertible mappings:

Definition 1. A $r \times c$-matrix M over some field $\mathbb{F}$ is called *hyper-invertible* if every square sub-matrix M_R^C of M is invertible, where, for sets $R \subseteq \{1, \ldots, r\}$ and $C \subseteq \{1, \ldots, c\}$ with $|R| = |C| > 0$, M_R^C denotes the matrix consisting of rows $i \in R$ and colums $j \in C$ of M.

Definition 2. Consider a function $f : \mathbb{F}^c \rightarrow \mathbb{F}^r$, as well as some arbitrary inputs $(x_1, \ldots, x_c)$ and the corresponding function values $(y_1, \ldots, y_r) = f(x_1, \ldots, x_c)$. The function f is called *hyper-invertible* if for any sets $A \subseteq \{1, \ldots, c\}, B \subseteq \{1, \ldots, r\}$ with $|A| + |B| = c$, there exists a function $f' : \mathbb{F}^c \rightarrow \mathbb{F}^r$ that maps the values $\{x_i\}_{i \in A}, \{y_i\}_{i \in B}$ to the values $\{x_i\}_{i \in \overline{A}}, \{y_i\}_{i \in \overline{B}}$.

Any linear function $f : \mathbb{F}^c \rightarrow \mathbb{F}^r$ can be expressed as a $r \times c$-matrix M. Show that M is hyper-invertible, if f is a hyper-invertible mapping.