ETH Zurich, Department of Computer Science
SS 2021

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

Cryptographic Protocols
Exercise 12

12.1 Hyper-Invertible Matrices

Recall the definition of hyper-invertible matrices from the lecture:

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 $R \subseteq \{1, \dots, r\}$ and $C \subseteq \{1, \dots, c\}$ with $|R| = |C| > 0$, M_R^C denotes the matrix consisting of rows $i \in R$ and colums $j \in C$ of M.

a) Determine whether the following matrices are hyper-invertible:

$$A = \begin{bmatrix} 5 & 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 5 & 5 \end{bmatrix} \text{ over GF}(7) \quad B = \begin{bmatrix} 4 & 1 & 4 \\ 6 & 4 & 1 \\ 3 & 1 & 1 \end{bmatrix} \text{ over GF}(7)$$

$$C = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 4 & 7 \\ 4 & 2 & 6 \\ 2 & 2 & 4 \end{bmatrix} \text{ over GF}(11) \qquad D = \begin{bmatrix} 5 & 1 & 10 & 6 & 1 \\ 1 & 6 & 0 & 1 & 5 \\ 5 & 9 & 1 & 4 & 4 \\ 4 & 7 & 5 & 5 & 2 \end{bmatrix} \text{ over GF}(11)$$

Next, we want to show that permuting hyper-invertible matrices and multiplying columns (or rows) by constants preserves hyper-invertibility. Let $M \in \mathbb{F}^{r \times c}$ be a hyper-invertible matrix over some field $\mathbb{F}$.

b) Let M' be the matrix obtained from M by exchanging the ith and jth column of M. Show that M' is hyper-invertible.

c) Let $\bar{M}$ be the matrix obtained from M by multiplying each entry of the ith column of M by some value $a \in \mathbb{F} \setminus \{0\}$.
Show that $\bar{M}$ is hyper-invertible.

12.2 Properties of Hyper-Invertible Matrices

In this task we prove one direction of the lemma from the lecture: for a matrix M, which induces a linear function f, we have that M is hyper-invertible if and only if f is hyper-invertible.

Recall the definition of hyper-invertible mappings:

Definition 2. Consider a function $f : \mathbb{F}^c \to \mathbb{F}^r$, 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 $f' : \mathbb{F}^c \to \mathbb{F}^r$ that maps the values $\{x_i\}_{i\in A}, \{y_i\}_{i\in B}$ to the values $\{x_i\}_{i\in \overline{A}}, \{y_i\}_{i\in \overline{B}}$.

Prove that any hyper-invertible matrix defines a hyper-invertible linear function.

HINT: Note that for A, B as in Definition 2 we have $\vec{y}_B = M_B\vec{x} = M_B^A\vec{x}_A + M_B^{\overline{A}}\vec{x}_{\overline{A}}$.

12.3 Beaver's Multiplication Triples

In the lecture we saw a multiplication protocol based on precomputing random double sharings. An alternative multiplication protocol can be obtained by precomputing *multiplication triples*, which are sharings of values (a, b, c), all shared by polynomials of degree t, where a and b are uniform random values and $c = ab$.

Let (a, b, c) be a multiplication triple. Given a share of $[x]$ and a share of $[y]$, how can a party compute a share of $[xy]$ efficiently?