ETH Zurich, Department of Computer Science
SS 2018

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

Cryptographic Protocols
Exercise 13

13.1 Properties of Hyper-Invertible Matrices

In this task we prove 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.

More precisely, recall the definitions:

Definition. An $m \times n$-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 $R \subseteq \{1, \ldots, m\}$ and $C \subseteq \{1, \ldots, n\}$ with $|R| = |C| > 0$, M_R^C denotes the matrix consisting of rows $i \in R$ and colums $j \in C$ of M.

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

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

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

c) Do hyper-invertible matrices over GF(2) exist?

13.2 Sharings of Zero

a) Describe a passively secure protocol that allows n players to jointly generate $\Omega(n)$ random sharings of 0 and prove its security.

b) Modify your protocol such that it becomes actively-secure with abort, and prove its security.

13.3 Passive Packed Secret-Sharing

In this task we show a modification of the Shamir secret-sharing scheme that allows one sharing to contain multiple secrets (this is known as "packed" secret sharing).

In particular, a vector of l secrets $(s_1, \ldots, s_l)$ is correctly shared with degree d if there exists a polynomial $p(x)$ of degree at most d, such that $p(\beta_j) = s_j$, for $j = 1, \ldots, l$, and each player P_i holds $p(\alpha_i)$, where α_i and β_j are distinct field elements.

a) For given t and l, find the smallest sharing degree d, such that the above scheme is private. More precisely, let $\mathbf{s} = (s_1, \ldots, s_l)$ be a vector of shared secrets. Prove that, for your choice of d, any subset of t shares has a distribution independent of $\mathbf{s}$.

b) Modify the passive multiplication protocol using hyper-invertible matrices to deal with packed secret sharing. You can assume that appropriate random double-sharings are given. What is the assumption on t?