ETH Zurich, Department of Computer Science
SS 2021

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

Cryptographic Protocols
Solution to Exercise 12

12.1 Hyper-Invertible Matrices

a) Matrices A and B are hyper-invertible, since all square sub-matrices are invertible. Matrix C is not hyper-invertible, as can be seen by e.g. determining

$$det\left(\begin{bmatrix}1 & 2 & 3\\ 3 & 4 & 7\\ 4 & 2 & 6\end{bmatrix}\right) = 0.$$

Matrix D is not hyper-invertible, since e.g. the sub-matrix $\begin{bmatrix}0\end{bmatrix}$ is not invertible.

b) Let $C \subseteq \{1,\dots,c\}$, $R \subseteq \{1,\dots,r\}$ with $|C| = |R| > 0$. We have 4 cases:
Case $i, j \notin C$: We have $M_R'^C = M_R^C$, thus $M_R'^C$ is invertible.
Case $i, j \in C$: Let i (j) be the k-th smallest (l-th smallest) number in C. Then we have $M_R'^C = M_R^C P$, where P is the permutation matrix for the transposition (kl).
Case $i \in C, j \notin C$: Let i be the k-th smallest number in C, j be the l-th smallest number in $C' = (C \setminus \{i\}) \cup \{j\}$. Then we have $M_R'^C = M_R^{C'} P$, where P is the permutation matrix for the cycle $(l\; l{+}1 \dots k)$, if $l \leq k$ and for the cycle $(k\; k{+}1 \dots l)$ otherwise.
The case $j \in C, i \notin C$ is analogous to the previous.

c) Let $C \subseteq \{1,\dots,c\}$, $R \subseteq \{1,\dots,r\}$ with $|C| = |R| > 0$. We have two cases:
Case $i \notin C$: We have $M_R'^C = M_R^C$, thus $M_R'^C$ is invertible.
Case $i \in C$: Let i be the k-th smallest number in C. Then we have $M_R'^C = M_R^C D$, where $D = (d_{lm})_{1\leq l,m\leq |C|}$ is the diagonal matrix with $d_{lm} = \begin{cases} 0, & \text{if } l \neq m \\ a, & \text{if } l = m = k \\ 1, & \text{otherwise} \end{cases}$.

12.2 Properties of Hyper-Invertible Matrices

Consider a hyper-invertible matrix M. Denote by $f : \mathbb{F}^c \to \mathbb{F}^r$ the linear function defined by M and let $\vec{y} = (y_1,\dots,y_r) = f(x_1,\dots,x_c)$ for arbitrary values $\vec{x} = (x_1,\dots,x_c) \in \mathbb{F}^c$. Consider two sets $A \subseteq \{1,\dots,c\}, B \subseteq \{1,\dots,r\}$ with $|A| + |B| = c$. Then, we have $\vec{y} = M\vec{x}$ and $\vec{y}_B = M_B\vec{x} = M_B^A\vec{x}_A + M_B^{\overline{A}}\vec{x}_{\overline{A}}$. Since M is hyper-invertible, $M_B^{\overline{A}}$ is invertible, and $\vec{x}_{\overline{A}} = (M_B^{\overline{A}})^{-1}(\vec{y}_B - M_B^A\vec{x}_A)$. The remaining values $\vec{y}_{\overline{B}}$ can be computed from $\vec{x}$.

12.3 Beaver's Multiplication Triples

Assume that we are given sharings of x and y and want to compute a sharing of xy. Let a, b, c be a multiplication triple. The party computes a sharing of $x - a$ and $y - b$ and reconstruct $\alpha = x - a$ and $\beta = y - b$. Observe that since a, b are uniformly random, α and β are also random values. Moreover, observe that $xy = ab + \alpha b + a\beta + \alpha\beta$, and hence each player P_i can compute locally a degree-t-sharing of xy as follows: $[xy]_i = [c]_i + \alpha[b]_i + \beta[a]_i + \alpha\beta$. Observe that only two reconstructions (and some local computation) are needed to execute this protocol.