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 14

14.1 Multiplication Triples of Different Degree

Consider the case, where $n = 10$ parties want to compute a value $y = (x_1 \cdot x_2) + (x_3 \cdot x_4)$ towards all parties (where $x_1, \ldots, x_4$ are the inputs of 4 distinct users). The adversary corrupts $t = 3$ parties. Since the computation consists of two multiplications and one addition, in the preparation phase two multiplication triples are generated for the two multiplications.

The adversary has the following strategy:

1. During the generation of the first multiplication triple, all corrupted parties behave honestly. Thus, a triple $([a_1]_3, [b_1]_3, [c_1]_3)$ of degree $t = 3$ is generated.

2. During the generation of the second multiplication triple, the adversary enforces two block repetitions (by sending incorrect values from one corrupted party to an honest party during the first two executions). Thus, two corrupted parties and two honest parties are eliminated, we obtain $t' = 1$ and $n' = 6$, and a triple $([a_2]_1, [b_2]_1, [c_2]_1)$ of degree $t' = 1$ is generated.

3. During the computation stage, the remaining corrupted party sends correct messages.

Let $z_1 = x_1 \cdot x_2$ and $z_2 = x_3 \cdot x_4$. In the computation stage, the first triple is used to compute a sharing $[z_1]_3$ of z_1. Since the first triple was of degree 3, the sharing will also have degree 3. Note that, since $[z_1]_3$ is a linear combination of the sharings $[a_1]_3, [b_1]_3, [c_1]_3$, the adversary knows three points on the polynomial f_{z_1} corresponding to $[z_1]_3$. Next, the second triple is used to compute a degree-1-sharing $[z_2]_1$ of z_2. Finally, a sharing of y is computed (locally), which yields a degree-3-sharing $[y]_3 = [z_1]_3 + [z_2]_1$, which then is reconstructed towards all $n' = 6$ parties. Thus, every party learns the corresponding polynomial $f_y(\alpha) = y + y_1\alpha + y_2\alpha^2 + y_3\alpha^3$. Since $[y]_3$ is the sum of a degree-3-sharing $[z_1]_3$ and a degree-1-sharing $[z_2]_1$, the coefficients y_2 and y_3 of f_y must be the same as in f_{z_1}. Thus, the adversary knows two coefficients and three points on f_{z_1}, which he can use to compute the remaining coefficients and consequently the value z_1.

14.2 Properties of Hyper-Invertible Matrices 2

Let $f : \mathbb{F}^c \to \mathbb{F}^r$ be a hyper-invertible linear function. Due to linearity, it can be described by a matrix M. To show that M is hyper-invertible, consider sets $R \subseteq \{1, \ldots, n\}$ and $C \subseteq \{1, \ldots, n\}$ with $|R| = |C| > 0$ and the submatrix M_R^C of M. Since $|R| = |C|$, it suffices to show that M_R^C is surjective. To that end, consider an arbitrary $\vec{y}_R$. We are to show that there exists an $\vec{x}_C$ such that $\vec{y}_R = M_R^C \vec{x}_C$. This is equivalent to the existence of an $\vec{x}$ such that $\vec{y}_R = M_R \vec{x}$ with $\vec{x}_{\overline{C}} = \vec{0}$. Consider the values $x_i = 0$ for $i \in \overline{C}$ and the values y_i for $i \in R$. By the hyper-invertibility of f, $\vec{x}_C$ can be computed (linearly) from these values. Thus, M_C^R is invertible.