Multivariate Cryptography – Exercise

(Exercise by Albrecht Petzoldt)

Postquantum Crypto Minischool
Taipei, Taiwan, July 12–15, 2022

Oil and Vinegar

Let $\mathbb{F} = \mathrm{GF}(7)$ and $o = v = 3$ (balanced Oil and Vinegar). Let the affine transformation $\mathcal{T} : \mathbb{F}^6 \mapsto \mathbb{F}^6$ be given as:

$$\mathcal{T}(x_1, \ldots, x_6) = \begin{pmatrix} 6 & 5 & 5 & 5 & 5 & 4 \\ 6 & 6 & 4 & 5 & 0 & 6 \\ 2 & 5 & 2 & 1 & 5 & 0 \\ 1 & 1 & 6 & 2 & 2 & 3 \\ 3 & 6 & 2 & 2 & 3 & 0 \\ 0 & 5 & 4 & 6 & 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \\ 4 \\ 1 \\ 3 \\ 2 \end{pmatrix}$$

The central map $\mathcal{F} : \mathbb{F}^6 \mapsto \mathbb{F}^3$ of our scheme is given by:

$$\begin{aligned} f^{(1)} &= 4x_1^2 + 4x_1x_3 + 5x_1x_4 + 6x_1x_5 + x_1x_6 + 6x_1 + 4x_2^2 + x_2x_3 + 6x_2x_4 + 6x_2x_5 + 5x_2x_6 \\ &\quad + 5x_2 + 5x_3^2 + 3x_3x_4 + 5x_3x_5 + 2x_3x_6 + 5x_3 + 6x_4 + 3x_5, \\ f^{(2)} &= 3x_1x_3 + 4x_1x_4 + 3x_1x_5 + 4x_1x_6 + 3x_1 + 6x_2^2 + x_2x_3 + 4x_2x_4 + 4x_2x_5 + 5x_2x_6 \\ &\quad + 6x_2 + 6x_3^2 + 4x_3x_4 + 2x_3x_5 + x_3x_6 + 3x_3 + x_4 + x_6 + 1, \\ f^{(3)} &= 6x_1^2 + 6x_1x_3 + 4x_1x_5 + 2x_1x_6 + 2x_2^2 + 5x_2x_3 + 6x_2x_4 + 5x_2x_5 + 5x_2x_6 + 6x_2 + 3x_3^2 \\ &\quad + 5x_3x_4 + 6x_3x_5 + x_3x_6 + 3x_3 + 4x_4 + 6x_5 + 5. \end{aligned}$$

Tasks:

1. Compute the corresponding public key.
2. Compute a signature $\mathbf{z} \in \mathbb{F}^6$ for the message $\mathbf{w} = (3, 6, 4)$ (use $(v_1, v_2, v_3) = (1, 0, 6)$ for the values of the Vinegar variables).
3. Is $\mathbf{z} = (6, 5, 2, 1, 1, 1)$ a valid signature for the message $\mathbf{w} = (3, 2, 5)$?