Multivariate Cryptography - Exercise 1 - Solution
PQ Crypto Summer School 2017

1 UOV

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

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

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

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

1. Compute the corresponding public key

   Solution: The public key $\mathcal{P} = \mathcal{F} \circ \mathcal{T} : \mathbb{F}^6 \to \mathbb{F}^3$ is given by

$$\begin{aligned} p^{(1)} &= 4x_1x_2 + x_1x_3 + 2x_1x_4 + 3x_1x_5 + x_1 + 2x_2^2 + x_2x_3 + 5x_2x_4 + 6x_2x_5 + x_2x_6 + 5x_2 \\ &+ x_3^2 + 2x_3x_4 + 4x_3x_5 + 3x_3x_6 + 3x_3 + 3x_4^2 + 3x_4x_5 + 2x_4x_6 + 6x_4 + 4x_5^2 + 5x_5 + 4x_6 + 6, \\ p^{(2)} &= 6x_1^2 + 4x_1x_2 + 5x_1x_3 + 2x_1x_4 + 5x_1x_5 + 5x_2^2 + 3x_2x_3 + 4x_2x_4 + 5x_2x_5 + 5x_2x_6 \\ &+ 5x_2 + 2x_3^2 + 2x_3x_4 + 2x_3x_5 + 4x_3 + 5x_4^2 + 6x_4x_6 + 2x_4 + 6x_5^2 + 2x_5x_6 + 3x_5 + 6x_6^2 + 5, \\ p^{(3)} &= 4x_1^2 + 3x_1x_2 + 2x_1x_3 + 3x_1x_5 + x_1x_6 + 5x_1 + 5x_2^2 + x_2x_3 + 3x_2x_4 \\ &+ 6x_2x_5 + 3x_2x_6 + 5x_2 + 2x_3^2 + 4x_3x_5 + 4x_3x_6 + 2x_3 + 2x_4^2 + 6x_4x_6 + 6x_4 \\ &+ 2x_5^2 + 5x_5x_6 + x_5 + 4x_6^2 + 2x_6 + 5. \end{aligned}$$

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).

   Solution: We substitute the values of the Vinegar variables into the central polynomials $f^{(1)}, f^{(2)}, f^{(3)}$ and obtain

$$\begin{aligned} \tilde{f}^{(1)} &= x_4 + 4x_5 + 6x_6 + 6, \\ \tilde{f}^{(2)} &= x_4 + x_5 + 4x_6 + 4, \\ \tilde{f}^{(3)} &= 6x_4 + 4x_5 + x_6 + 5. \end{aligned}$$

   We set $\tilde{f}^{(1)} = w_1 = 3, \tilde{f}^{(2)} = w_2 = 6$ and $\tilde{f}^{(3)} = w_3 = 4$. Solving this system by Gaussian Elimination yields $(x_4, x_5, x_6) = (6, 3, 0)$. Therefore, we get the pre-image $\mathbf{y} = (1, 0, 6, 6, 3, 0)^T$.
   In the second step, we have to invert the affine transformation $\mathcal{T}$. First, we compute T^{-1}, obtaining

$$T^{-1} = \begin{pmatrix} 2 & 4 & 6 & 2 & 0 & 5 \\ 1 & 3 & 3 & 1 & 6 & 2 \\ 4 & 6 & 6 & 4 & 5 & 4 \\ 2 & 0 & 3 & 4 & 2 & 3 \\ 6 & 0 & 3 & 0 & 0 & 5 \\ 2 & 2 & 2 & 5 & 3 & 3 \end{pmatrix}.$$

   and compute the signature $\mathbf{z} \in \mathbb{F}^6$ of the message $\mathbf{w}$ by

$$\mathbf{z} = T^{-1}(\mathbf{y} - (1, 2, 4, 1, 3, 2)^T) = (4, 1, 5, 6, 3, 5)^T.$$

3. Is $\mathbf{z} = (6, 5, 2, 1, 1, 1)$ a valid signature for the message $\mathbf{w} = (3, 2, 5)$?

   Solution: We get $\mathcal{P}(\mathbf{z}) = (3, 5, 5)$. Therefore, the signature $\mathbf{z}$ is invalid for the message $\mathbf{w}$.

2 Rainbow

Let $\mathbb{F}$=GF(7) and $(v_1, o_1, o_2) = (2, 2, 2)$. Let the central map $\mathcal{F} : \mathbb{F}^4 \to \mathbb{F}^6$ of the 2-layer Rainbow scheme be given by

$$\begin{aligned} f^{(3)} &= x_1^2 + 5x_1x_2 + 5x_1x_3 + 5x_1x_4 + 2x_1 + 4x_2^2 + 6x_2x_4 + 6x_2 + 5x_3 + 2x_4 + 1, \\ f^{(4)} &= 3x_1^2 + 2x_1x_2 + 4x_1x_3 + 3x_1x_4 + 3x_1 + 5x_2^2 + x_2x_3 + 3x_2x_4 + 5x_2 + 5x_3, \\ f^{(5)} &= 5x_1^2 + 2x_1x_2 + 4x_1x_3 + 6x_1x_6 + 2x_1 + 5x_2^2 + 4x_2x_3 + 2x_2x_4 + 3x_2x_5 + 2x_2 \\ &+ 2x_3^2 + x_3x_5 + 2x_3x_6 + 2x_4^2 + 5x_4x_5 + 5x_4x_6 + 3x_4 + 3x_5 + 2x_6 + 2, \\ f^{(6)} &= x_1^2 + 4x_1x_2 + 2x_1x_3 + 4x_1x_4 + 4x_1x_5 + 6x_1 + 4x_2^2 + 5x_2x_4 + x_2x_6 + 6x_2 \\ &+ 6x_3^2 + 3x_3x_5 + 5x_3x_6 + 3x_3 + 4x_4^2 + 5x_4x_5 + x_4 + 3x_5 + 2x_6 + 1. \end{aligned}$$

1. Compute a pre-image $\mathbf{y} \in \mathbb{F}^6$ of $\mathbf{x} = (3, 5, 0, 4)$ under the central map $\mathcal{F}$ (use $(v_1, v_2) = (4, 3)$ as the values of the Vinegar variables).

Solution: Substituting the Vinegar Variables into $f^{(3)}$ and $f^{(4)}$ yields

$$\begin{aligned} \tilde{f}^{(3)} &= 4x_3 + 5x_4 + 6, \\ \tilde{f}^{(4)} &= 3x_3 + 4. \end{aligned}$$

Setting $\tilde{f}^{(3)} = x_1 = 3$ and $\tilde{f}^{(4)} = x_2 = 5$ yields $(y_3, y_4) = (5, 1)$.
Substituting the values of $x_1, \ldots, x_4$ into $f^{(5)}$ and $f^{(6)}$ yields

$$\begin{aligned} \tilde{\tilde{f}}^{(5)} &= x_5 + 6x_6 + 2, \\ \tilde{\tilde{f}}^{(6)} &= 4x_5 + 2x_6 + 6. \end{aligned}$$

Setting $\tilde{\tilde{f}}^{(5)} = x_3 = 0$ and $\tilde{\tilde{f}}^{(6)} = x_4 = 4$ yields $(y_5, y_6) = (6, 1)$.
Therefore, the required pre-image is given by $\mathbf{y} = (4, 3, 5, 1, 6, 1) \in \mathbb{F}^6$.