Multivariate Cryptography - Exercise 2
PQ Crypto Summer School 2017

1 HFEv

Let $\mathbb{F} = GF(2)$ and $(n, D, a, v) = (3, 5, 0, 1)$. Let the extension field $\mathbb{E} \cong \mathbb{F}_{2^3}$ be given as $\mathbb{E} = \mathbb{F}[x]/\langle X^3 + X + 1\rangle$.
We use the isomorphism

$$\phi : \mathbb{F}^3 \to \mathbb{E},\ \phi(x_1, x_2, x_3) = x_1 + x_2 b + x_3 b^2$$

to lift an element of the vector space $\mathbb{F}^3$ to the extension field $\mathbb{E}$.

Let the two affine transformations $\mathcal{S} : \mathbb{F}^3 \to \mathbb{F}^3$ and $\mathbb{F}^4 \to \mathbb{F}^4$ be given by

$$\mathcal{S}(x_1, x_2, x_3) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

$$\mathcal{T}(x_1, \ldots, x_4) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_4 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Let the central map $\mathcal{F} : \mathbb{E} \times \mathbb{F} \to \mathbb{E}$ of our scheme be given by

$$\mathcal{F}(X) = (b+1)\cdot X^5 + (x_4\cdot b^2 + b + x_4)\cdot X^4 + b^2\cdot X^3 + (x_4+1)\cdot X^2 + (x_4\cdot b^2 + (x_4+1)\cdot b + 1)\cdot X + x_4^2 + 1.$$

1. Compute addition and multiplication tables for the field $\mathbb{E}$. What is the multiplicative inverse of b^2 (extended euclidean algorithm)?

2. Compute a signature $\mathbf{z} \in \mathbb{F}^4$ for the message $\mathbf{w} = (1, 0, 1)^T \in \mathbb{F}^3$.
   Use $x_4 = 1$ for the value of the Vinegar variable x_4.
   Hint: A solution to the equation $\mathcal{F}_V(\mathbf{Y}) = \mathbf{X}$ can be found by computing

$$\gcd(\mathcal{F}_V - \mathbf{X}, X^8 - X) = \gcd\left((\mathcal{F}_V - \mathbf{X}, \prod_{a \in \mathbb{E}} (X - a)\right).$$