Multivariate Cryptography - Exercise 2 - Solution
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)?
Solution:

$+$	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
0	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
1	1	0	$b+1$	b	b^2+1	b^2	b^2+b+1	b^2+b
b	b	$b+1$	0	1	b^2+b	b^2+b+1	b^2	b^2+1
$b+1$	$b+1$	b	1	0	b^2+b+1	b^2+b	b^2+1	b^2
b^2	b^2	b^2+1	b^2+b	b^2+b+1	0	1	b	$b+1$
b^2+1	b^2+1	b^2	b^2+b+1	b^2+b	1	0	$b+1$	b
b^2+b	b^2+b	b^2+b+1	b^2	b^2+1	b	$b+1$	0	1
b^2+b+1	b^2+b+1	b^2+b	b^2+1	b^2	$b+1$	b	1	0

Note that for each element $a \in \mathbb{E}$ we have $-a = a$.

$\cdot$	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
0	0	0	0	0	0	0	0	0
1	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
b	0	b	b^2	b^2+b	$b+1$	1	b^2+b+1	b^2+1
$b+1$	0	$b+1$	b^2+b	b^2+1	b^2+b+1	b^2	1	b
b^2	0	b^2	$b+1$	b^2+b+1	b^2+b	b	b^2+1	1
b^2+1	0	b^2+1	1	b^2	b	b^2+b+1	$b+1$	b^2+b
b^2+b	0	b^2+b	b^2+b+1	1	b^2+1	$b+1$	b	b^2
b^2+b+1	0	b^2+b+1	b^2+1	b	1	b^2+b	b^2	$b+1$

We find $(b^2)^{-1} = b^2 + b + 1$

i	r_i	q_i	s_i	t_i
-1	b^3+b+1	-	1	0
0	b^2	-	0	1
1	$b+1$	b	1	b
2	1	$b+1$	$b+1$	b^2+b+1

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

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

Solution: First we have to invert the first affine map $\mathcal{S}$. We obtain

$$\mathbf{x} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \left(\mathbf{w} - \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right) = (1,0,1)^T.$$

Lifting $\mathbf{x}$ to the extension field yields $\mathbf{X} = b^2 + 1$.

We substitute $x_4 = 1$ into the central map $\mathcal{F}$ and obtain

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

Computing $\gcd(\mathcal{F}_V(X) - \mathbf{X}, X^8 - X)$ yields $bX + b$.

$$\begin{aligned}
P_1 &= X^8 + X \\
P_2 &= \mathcal{F}_V(X) - \mathbf{X} = (b+1) \cdot X^5 + (b^2+b+1) \cdot X^4 + b^2 \cdot X^4 + (b^2+1) \cdot X + b^2 + 1 \\
P_3 &= P_1 - ((b^2+b) \cdot X^3 + (b^2+1) \cdot X^2 + X + b + 1) \cdot P_2 = (b^2+1) \cdot X^4 + (b+1) \cdot X^3 + b \cdot X^2 + b^2 \\
P_4 &= P_2 - ((b^2+b) \cdot X + b^2 + b + 1) \cdot P_3 = X^3 + (b^2+1) \cdot X^2 + b^2 \\
P_5 &= P_3 - ((b^2+1) \cdot X + b^2) \cdot P_4 = b \cdot X + b \\
P_6 &= P_4 - ((b^2+1) \cdot X^2 + b \cdot x + b) \cdot P_5 = 0
\end{aligned}$$

Thus, $\mathbf{Y} = 1$ is a solution to the equation

$$\mathcal{F}_V(\mathbf{Y}) = \mathbf{X}.$$

Moving $\mathbf{Y}$ to the vector space and appending $x_4 = 1$ yields

$$\mathbf{y} = (1, 0, 0, 1).$$

Therefore, a signature for the message $\mathbf{w}$ is given by

$$\mathbf{z} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \left(\mathbf{y} - \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right) = (0, 0, 0, 1)^T.$$