OV example

$$F_3, o = 2, v = 2, n = o + v$$

Central map F

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{pmatrix} 0 & 2 & 2 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + 1$$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 \\ 2 & 1 & 1 & 2 \\ 2 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + 1$$

F:

$$\begin{pmatrix} x_1^2 + x_2x_1 + 2x_3x_1 + 2x_2^2 + 2x_2 + 2x_3 + 2x_2x_4 + 2x_4 + 1 \\ x_2^2 + x_1 + x_4 + 1 \end{pmatrix}$$

Affine map T

$$\begin{pmatrix} 1 & 1 & 2 & 2 \\ 2 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 \\ 2 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \to \begin{pmatrix} x_1 + x_2 + 2x_3 + 2x_4 + 1 \\ 2x_1 + x_4 + 1 \\ x_2 + 2x_3 + 2x_4 + 1 \\ 2x_1 + x_2 + x_3 + x_4 + 2 \end{pmatrix}$$

Public key P = T o F

$$\begin{pmatrix} x_1^2 + x_2x_1 + x_3x_1 + 2x_4x_1 + 2x_1 + x_2 + x_3 + x_3x_4 + 1 \\ x_1^2 + x_4x_1 + x_1 + x_4^2 + 2x_2 + 2x_4 + 2 \end{pmatrix}$$

Signing

Hash(message) = $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$

Choose random fixed values for vinegar: $\begin{pmatrix} x_1 & x_2 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 \end{pmatrix}$
F is reduced to linear multivariates

$$\begin{pmatrix} 2x_3 + x_4 + 2 \\ x_4 + 2 \end{pmatrix}$$

Linear system is solved by Gaussian elimination

$$\begin{pmatrix} 2x_3 + x_4 + 2 \\ x_4 + 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

Solution for oil: $\{x_3 \rightarrow 1, x_4 \rightarrow 0\}$
Solution including fixed vinegar:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}$$

T was defined using the affine mapping

$$\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{b} = \begin{pmatrix} 1 & 1 & 2 & 2 \\ 2 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 \\ 2 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 2 \end{pmatrix}$$

Inverse of T is

$$\mathbf{z} = \mathbf{A}^{-1}(\mathbf{y} - \mathbf{b}) = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 2 & 0 & 0 & 2 \\ 1 & 2 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix} \left[\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 1 \\ 2 \end{pmatrix} \right] = \begin{pmatrix} 2 \\ 0 \\ 1 \\ 2 \end{pmatrix}$$

Verification

Test if

$$\begin{pmatrix} x_1^2 + x_2 x_1 + x_3 x_1 + 2x_1 + x_2 + x_3 + (2x_1)\, x_4 + x_3 x_4 + 1 \\ x_1^2 + x_4 x_1 + x_1 + x_4^2 + 2x_2 + 2x_4 + 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

for

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 & 2 \end{pmatrix}$$