Thoughts on Unbalanced Oil and Vinegar

Jacob Alperin-Sheriff

NIST jacob.alperin-sheriff@nist.gov

1 Introduction

In the simplified version of UOV where the polynomials are all homogenous, we have that each "secret" polynomial can be represented by

$$\mathbf{F}^{(i)} = \begin{bmatrix} \mathbf{0} & \mathbf{A}^{(i)} \\ \mathbf{B}^{(i)} & \mathbf{C}^{(i)} \end{bmatrix} \in \mathbb{F}^{(n+v)\times(n+v)},$$

where $\mathbf{A}^{(i)} \in \mathbb{F}^{n\times v}, \mathbf{B}^{(i)} \in \mathbb{F}^{v\times n}, \mathbf{C}^{(i)} \in \mathbb{F}^{v\times v}$, and we have

$$\mathbf{G}^{(i)} = \mathbf{S}^t\mathbf{F}^{(i)}\mathbf{S},$$

where

$$\mathbf{S} = \begin{bmatrix} \mathbf{S}_{1,1} & \mathbf{S}_{1,2} \\ \mathbf{S}_{2,1} & \mathbf{S}_{2,2} \end{bmatrix} \in \mathbb{F}^{(n+v)\times(n+v)}$$

is invertible.

Let $\mathbf{X} \in \mathbb{F}^{v\times n}$ be such that $\mathbf{S}_{2,2}\mathbf{X} = \mathbf{S}_{2,1}$ (this should certainly exist whenever $\mathbf{S}_{2,2}$ is invertible, which is at least relatively likely).

Then for all $\mathbf{G}^i$, we have that

$$[\mathbf{I} \mid \mathbf{X}^t]\mathbf{G}^i \begin{bmatrix} \mathbf{I} \\ \mathbf{X} \end{bmatrix} = 0$$

References