Total Break of the Fully Homomorphic Multivariate Encryption Scheme of [1]: Decryption can not be of low degree

Jacob Alperin-Sheriff[1], Jintai Ding[2], Albrecht Petzoldt[1], Daniel Smith-Tone[1,3]

[1] National Institute for Standards and Technology, Gaithersburg, Maryland, USA
[2] University of Cincinnati, Ohio, USA
[3] University of Louisville, Kentucky, USA
{jacob.alperin-sheriff,albrecht.petzoldt,daniel.smith}@nist.gov,jintai.ding@gmail.com

Yesterday, Faugere et al. published a very interesting paper on building a fully homomorphic encryption scheme based on multivariate cryptography [1]. The scheme is based on a symmetric scheme, whose encryption function is given by the formula

$$\mathrm{Enc} : \mathbb{F}^n \to \mathbb{F}^{2n},\ \mathrm{Enc}_{sk}(\mathbf{m}) = M \begin{bmatrix} \mathbf{m} + f(r) \\ r \end{bmatrix},$$

where M is an $2n \times 2n$ matrix over $\mathbb{F}$, $r \in \mathbb{F}^n$ is a random value and f is a nonlinear multivariate polynomial. The decryption is given by

$$\mathrm{Dec}_{sk}(\mathbf{c}) = ((M^{-1}\mathbf{c}_1) + f((M^{-1}\mathbf{c}_2))).$$

While this design is actually perfectly sensible, it is infeasible to find parameter sets which make the scheme both secure and efficient. In the paper [1], the authors chose the degree of the polynomial f to be only 4 and the number of variables to be 64 or 128. Therefore, the decryption function is a polynomial of degree 4, resulting in a total number of monomials of $\binom{128+4}{4} \cdot 64 \leq 2^{30}$ $(n = 64)$ and $\binom{256+4}{4} \cdot 128 \leq 2^{35}$ $(n = 128)$. It is therefore easy to compute a list of plaintext/ciphertext pairs and to recover the polynomial f by polynomial interpolation [2]. For any value of n, the secret key can be therefore recovered in polynomial time. In general, the encryption scheme can be seen as a one round DES like scheme.

Acknowledgements: Jintai Ding wants to thank NIST for support.

References

1. M. Tamayo-Rios, J.C Faugere, L. Perret, P.H. How, R. Zhang: Fully Homomorphic Encryption Using Multivariate Polynomials. IACR Eprint 2017/458.
2. J. Lagrange, 1795.