**The case of non-zero singular values**

**Peter Nonnenmann**

**Quant-X-Security & Coding and DHBW Mannheim**

**Xenia Bogomolec**

**Quant-X-Security & Coding**

**Keywords :** Polynomial equation system , Quantum algebraic attack on AES ,

condition number .

We calculated the condition number of the Quantum algebraic attack on AES , to be

Infinity, in the case that one considers ALL singular values of the Macaulay Matrix corresponding

to the quadratic polynomial equation system corresponding to the globally used symmetric

block cipher AES .

In this paper, we investigate the same Macaulay Matrix , but work out in detail the assumption

of Chen-Gao in their QAA [1], that all singular values be greater than zero .

It is a standard fact from Linear Algebra, that one has

The kernel of A is associated with the Null singular values, whereas the other summand in the

direct sum decomposition corresponds to the non-zero singular values, implying that

we can restrict the linear mapping induced by A to this subspace R(A), which is also the

orthogonal complement of the kernel.

To determine a basis of R(A), we first can ommit all the zero-row-vectors, which are added

by Chen-Gao, so that the modified Macaulay matrix can be efficiently queried, see

Remark 3.4.

The remaining non-zero rows may still not be a basis of the complement, to determine one,

a Gaussian eliminitation on the row-vectors is necessary, which is a non-trivial step in terms

of computational complexity, that we will investigate in a forthcoming paper.

The calculation of the number of remaining rows of A is based on definition (4), page 9.

…..

The monomials with , are all Zero by definition,

so the non-zero rows of A are those with

So we have

**Lemma :**

The maximum number r of polynomials or number of equations is

r = 29 520 for AES-256 , see Table 2 on page 26 .

So after omission of all zero-row-vectors, the remaining matrix has 29 520 rows .

**Further work in progress**

The QAA of Chen-Gao reduces the quadratic polynomial equation system ( QPES ) of AES,

to the Macaulay Linear System, based on the classic reference by Macaulay of 1902, [3].

There is a vast generalization of this work , based on the sophisticated tools of

Homological Algebra, Jet Bundles and Spectral Sequences, see Gelfand et al., [2],

which we shall try to exploit to reduce the QPES of AES to an as yet to be properly defined

„Homological Linear System“ .

**References**

[1] Y. Chen, X. Gao,

Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack

On Cryptosystems, arXiv : 1712.06239v3 [quant-ph] 2018 .

[2] I.M. Gelfand, M.M. Kapranov, A.V. Zelevinsky,

Discriminants, Resultants and Multidimensional Determinants,

Birkhäuser , 1994 .

[3] F.S. Macaulay ,

Some formulas in elimination, Proc. of the London Mathematical Society,

35(1), 3-38, 1902 .