The complexity of the Chen-Gao-Algorithm is infinity

Dr. Peter Nonnenmann

DHBW Mannheim and Quant-X Security & Coding

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

condition number .

For analyzing the Chen-Gao-Quantum-Algorithm, we make the same definitions as Chen-Gao,

and use the same numeration of definitions, remarks, Theorems etc., for easy reference, see [1].

Let be the field of complex numbers and the polynomial ring in the

indeterminates .

For a polynomial , denote

to be the total degree of f, the sparseness (the number of terms) of f, and the set of

monomials of f, respectively.

For , we use

to denote the common zeros of the polynomials in S ( the variety corresponding to S ).

Let

**Definition** 3.1 . [ Parameters ]

Without loss of generality, we may assume

and

Let

Let

Let

.

**Remark** 3.2

In this paper, the subscripts for a matrix or a vector always start from 0, because

the complexity analysis oft he algorithm in this paper depends on the representation of

the subscripts .

For a quantum attack on cryptosystems such as AES and eAES, it is necessary to solve

a polynomial equation system F as above, which in the case of AES is given in terms of

the AES-S-Box, see pages 32-34 in [1] . This polynomial equation system is solved by solving

an equivalent linear equation system, the so-called **Macaulay linear system** (6) of F,

and the Macaulay linear system of F is solved by the HHL quantum algorithm, see [2] :

is called the **modified Macaulay matrix** of the polynomial system F .

By the construction of Chen-Gao, is a matrix over C of dimension

with the parameters as given above .

**Remark** 3.3

The only important fact for us , is the existence of 0 columns in the Macaulay matrix.

**Remark** 3.4

Again, the only important fact for us , is the existence of 0 rows in the Macaulay matrix.

See also **Example** 3.5 for a small, but typical example of the Macaulay matrix.

**Definition** : [ condition number ]

.

**The singular values** of A ,

are defined to be the positive square roots of the eigenvalues of

**The condition number** k(A) , is defined to be

,

We need the following standard result from Linear Algebra:

**The Dimension-Formula for Linear Maps** :

**Definition** :

Our result is :

**Theorem** :

**Proof** :

But also the condition number of the whole polynomial system F is infinite :

**Theorem** 4.3 in [1]. Algorithm 4.2 has the following properties : […]

,

Since, by their Lemma 4.5, there are at most n iterations in the loop, where the

matrices are used, and since all their condition numbers are infinite,

the condition number of the polynomial system is infinite, and so is the runtime

complexity of the Chen-Gao-Algorithm ( Theorem 4.3 ).

**Discussion**

The condition number being infinity implies by the complexity analysis of this quantum

algebraic attack on AES by the authors , that the complexity of the whole quantum

algebraic attack on AES equals infinity, too.

This in turn means, that the Chen-Gao-Algorithm constitutes no practically realizable

quantum attack neither on AES nor eAES, the complexity of eAES being larger than

that of AES, see the recent paper by X. Bogomolec, J. Underhill and S. Kovac [3].

**CAUTION**:

This is a **mathematical** Theorem and a corresponding mathematical proof, and

therefore, by no means can we make a statement or prediction about the potential

**physical** outcome of an actual attack on eAES with a quantum computer in the future.

**References**

[1] Yu-Ao Chen, Xiao-Shan Gao,

Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack

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

[2 ] A.W. Harrow, A.Hassidim, S.Lloyd, Quantum algorithm for linear systems equations,

Physical Review Letters, 103(15): 150502, 2009.

[3] X. Bogomolec, J. Underhill, S. Kovac, Towards Post-Quantum secure symmetric Cryptography:

A mathematical Perspective, Cryptology ePrint Archive: Report 2019/1208.

[4] N. Yanofsky, M. Mannucci, Quantum computing for computer scientists,

Cambridge University Press 2008.

[5] F. Lorenz, Lineare Algebra I,II , BI 1984.

[4] C. Kassel, Quantum groups , GTM Springer 1994

[5] M. Grassl, B.Langenberg, M.Roetteler, R.Steinwandt, Applying Grover’s algorithm to AES:

Quantum resource estimates, International Workshop on Post-Quantum Cryptography,

Post-Quantum Cryptography, 29-43, Springer 2016.

[6] F.S. Macaulay, Some formulas in elimination, Proc. Of the London Mathematical

Society, 35(1), 3-38, 1902.

[7] D. Cox, J. Little, D. O’Shea, Using Algebraic Geometry, Springer 1998.

[8] G.M. Gramlich, Lineare Algebra, Pro Business 2013.

[9] S. Gukov, A.Kapustin,

Topological Quantum Field Theory, Nonlocal Operators, and Gapped Phases

of Gauge Theories, 2013, arXiv:1307, 4793v2 [hep-th]

[10] J.K.Pachos, Introduction to Topological Quantum Computing,

Cambridge U Press 2012.

[11] D.Aharonov,A.Ta-Shama, Adiabatic quantum state generation and statistical zero

Knowledge, Proc. STOC’03, 20-29, ACM Press, New York, 2003.

[12] D.W.Berrs, A.M.Childs,R.Kothari, Hamiltonian simulation with nearly optimal dependence

on all parameters, Proc. 56th FOCS, 792-809, 2015.

[13] A.Caminata, E.Gorla, Solving multivariate polynomial systems and an invariant from

Commutative Algebra, arXiv 1706.06319, 2017.

[14] Y.A.Chen,X.S.Gao,C.M.Yuan, Quantum Algorithms for Optimization and Polynomial

Systems Solving over Finite Fields, arXiv 1802.03856, 2018.

[15] A.M.Childs, Quantum algorithms : equation solving by simulation,

Nature Physics, 5(12), 861-861, 2009.

[16] J.Daemen,V.Rijmen, AES Proposal: Rijndael , NIST, 1999.

[17] L.K.Grover, A fast quantum mechanical algorithm for database search,

Proc. STOC’96, 212-219, ACM Press, 1996.

[18] D.Lazard, Gröbner bases, Gaussian elimination and resolution of systems of

Algebraic equations, Proc. Eurocal 83, LNCS, vol. 162, 146-156, Springer, 1983.

[19] S.Murphy,M.Robshaw, Essential algebraic structure within AES, CRYPTO ´02,

1-16, 2002.

[20] P.W.Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete

Logarithms on a Quantum Computer, SIAM J. Comp., 26(5), 1484-1509, 1997.