The complexity of the Chen-Gao-Algorithm on AES 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 $\mathbb{C}$ be the field of complex numbers and $\mathbb{C}[X]$ the polynomial ring in the indeterminates $X = \{x_1, \dots, x_n\}$.

For a polynomial $f \in \mathbb{C}[X]$, denote $\deg(f)\, , \#f, and\ \mathfrak{m}(f)$ to be the total degree of f, the sparseness (the number of terms) of f, and the set of monomials of f, respectively.

For $S \subseteq \mathbb{C}[X]$, we use $\mathbb{V}_{\mathbb{C}}(S) \subseteq \mathbb{C}^n$ to denote the common zeros of the polynomials in S (the variety corresponding to S).

Let $\mathcal{F} = \{f_1, \dots, f_r\} \subseteq \mathbb{C}[X]\, , and\ d_i = \deg(f_i)\ , t_i = \#f_i,\ \ for\ i = 1, \dots, r.$

Definition 3.1 . [Parameters]

Without loss of generality, we may assume $f_i(0) = -1\, , for\ i = 1, . . , rho$ and $f_i(0) = 0\, , for\ i = rho + 1, \dots, r$.

Let $D \in N\, , such\ that\ \ D \geq\ max_{i=1}^{r}\, d_i$.

Let

$\bar{d}$ *be the minimal integer such that* $\bar{d} \geq D - min_i d_i$ *and* $\bar{d} + 1 = 2^{\delta}$, *for some* $\delta \in N$

Let

$\overline{D}$ *be the minimal integer such that* $\overline{D} \geq D$ *and* $\overline{D} + 1 = 2^{\Delta}$, *for some* $\Delta \in N$.

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] :

$$A_{\mathcal{F},D}\, m_D \;=\; b_{\mathcal{F},D} \tag{6}$$

$A_{\mathcal{F},D}$ is called the **modified Macaulay matrix** of the polynomial system F .

By the construction of Chen-Gao, $A_{\mathcal{F},D}$ is a matrix over C with number of rows resp. columns

$$\left[\, r(\bar{d}+1)^n \,\right] \times \left[\, (\overline{D}+1)^n - 1 \,\right] = \left[\, r2^{n\delta} \,\right] \times \left[\, 2^{n\Delta} - 1 \,\right] =: M \times N \,,$$

with the parameters as given above .

Note that since $\bar{d} < \overline{D}$, *we have* $M < N$.

Remark 3.3

$The\ columns\ corresponding\ to\ monomial\ \ m_{\bar{D},j}\ \ with\ \deg(m_{\bar{D},j}) > D$

$are\ all\ 0\ columns\ , where\ \ m_{\bar{D},j}\ \ is\ defined\ on\ page\ 9$.

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

Remark 3.4

$The\ zero\ rows\ are\ added\ so\ that\ the\ modified\ Macaulay\ matrix\ can\ be\ efficiently$

$queried. Refer\ to\ Lemma\ 3.10\ for\ details.$

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]

$Let\ A\ be\ a\ complex\ matrix,\ \ A \in \mathbb{C}^{M,N}. Its\ complex\ conjugate\ transpose\ is\ written\ A^T.$

The singular values of A $\quad , s_1 \geq s_2 \geq, \dots, \geq s_p \geq 0\ , \quad p = \min(M, N),$

are defined to be the positive square roots of the eigenvalues λ_i of $AA^T\ \ if\ \ M \leq N,$

written $\qquad s_i := \sqrt{\lambda_i(\,A\,A^T)}\ \ ,$

and those of $\qquad A^T A\ \ if\ \ \ M > N\ .$

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

$$k(A) := \frac{s_{max}}{s_{min}}\ ,$$

$$that\ is, the\ quotient\ of\ the\ maximal\ and\ minimal\ singular\ values.$$

We need the following standard result from Linear Algebra:

The Dimension-Formula for Linear Maps :

$Let\ \ f: \mathbb{C}^M \longrightarrow \mathbb{C}^M\ \ be\ a\ linear\ map.\ Then$

$$\dim\ker(f)\ +\ rank(f)\ =\ M\ .$$

Definition : $Given\ \ f: \mathbb{C}^M\ \longrightarrow\ \mathbb{C}^M\ \ , we\ denote\ \ by\ \ Eig(f, \lambda)$

$the\ eigenspace\ of\ f\ associated\ with\ the\ eigenvalue\ \ \lambda.$

$Note\ that \qquad Eig(f, 0) = \ker(f)\ \ ,\ the\ kernel\ of\ f.$

$Now, let\ A = A_{\mathcal{F},D} \in \mathbb{C}^{M,N}\ (\mathcal{F}, D\ are\ arbitrary)\ be\ one\ of\ the\ modified$

$Macaulay\ matrices\ constructed\ by\ Chen - Gao\ as\ above.$

$We\ then\ consider\ the\ linear\ map\ f: \mathbb{C}^M \longrightarrow \mathbb{C}^M\ ,\ induced\ by\ the\ matrix$

$A\,A^T = f\ .$

Our result is :

Theorem :

$$k(A) = \infty$$

Proof :

Concerning the Chen-Gao algorithm in general,

$First\ note\ that\ A\ has\ at\ least\ one\ 0\ row\ and\ one\ 0\ column\ by\ remarks\ 3.3\ and\ 3.4$

$Then\ AA^T = f\ \ has\ at\ least\ one\ 0\ row, too\ , by\ matrix\ multiplication.$

$Then\ rank(f) \leq M - 1\ ,\ and\ by\ the\ Dimension - Formula\ for\ Linear\ Maps$

$\dim\ker(f) + rank(f) \leq \dim\ker(f) + M - 1\quad , so$

$M \qquad\qquad\qquad \leq \dim\ker(f) + M - 1$

$Assume\ \dim\ker(f) = 0\ ,\ then\ \ M \leq M - 1\ ,\ \ a\ contradiction.$

$So \qquad \dim\ker(f) \geq 1\ \ ,\ \ so\ \dim Eig(f, 0) \geq 1\ ,$

$which\ in\ turn\ means, that\ f\ \ has\ the\ eigenvalue\ \ \lambda = 0\ ,$

$so\ \ A\ \ has\ the\ singular\ value\ \ s = 0 = s_{min}\ , the\ minimal\ singular\ value, so$

$$k(A) = \frac{s_{max}}{s_{min}} = \infty \qquad \blacksquare$$

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 : [...]

$The\ runtime\ complexity\ of\ the\ algorithm\ is\ \ \tilde{O}\left[n^{2.5}(n + T_{\mathcal{F}})\kappa^2 \log\left(\frac{1}{\epsilon}\right)\right],$

$where\ \kappa\ \ is\ the\ maximal\ condition\ number\ for\ all\ matrices\ A_{\mathcal{F}_2,D}\ in\ Step\ 4$,

$called\ the\ CONDITION\ NUMBER\ \ k(\mathcal{F}) = \kappa\ \ for\ the\ polynomial\ system\ \mathcal{F}.$

Since, by their Lemma 4.5, there are at most n iterations in the loop, where the matrices $A_{\mathcal{F}_2,D}$ 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).

Quantum algebraic attack on AES

We shall show that in this case, A_F,D is of dimension ($\geq\ 10^{500}\ \times\ \geq 10^{500}$) , and that the number of entries not equal 0 is only $\leq\ 10^6$, thus proving that there exist at least one 0 row and at least one 0 column in the Macaulay matrix in this case.

Calculation of parameters for the AES S-Box

We use table 2 in [1], page 26, to calculate , see Definition [Parameters] above :

The S-Box is a **Boolean multivariate quadratic equation system** (BMQ), so that

$D = 2\ ,\ \ \bar{d} \coloneqq min\{\ d \geq 0\ and\ \ d + 1 = 2^{\delta}\ for\ some\ \ \ \delta \in N\ \}$,

that is $\delta = 1\ ,\ d + 1 = 2, so\ \ \bar{d} = 1$.

Also $\overline{D} \coloneqq \min\{\ D \geq 2\ and\ \ D + 1 = 2^{\Delta}\ \ for\ some\ \Delta \in N\ \}$,

that is $\Delta = 2\ ,\ D + 1 = 2^2\ \ ,\ \overline{D} = 3$.

$r = \#Eqs \geq 4400\ \ and\ \ n = \#Vars \geq 1792$

So $M \geq 4400\ (\ 2^{1792}\ ) >\ 10^{500}$ (overflow)

$N \geq 4^{1792} - 1 > 10^{500}$

The number of entries (not equal 0 = ‚1‘) is identical with the **T-Sparseness**

in Table 2 on page 26 : this is at most $696\ 384 \ < 10^6 \ for \ AES - 256$.

Now, even we have 500 000 ‚1‘ in different rows, and 500 000 ‚1‘ in different columns, certainly there exists at least one 0 row and one 0 column in the Macaulay matrix attacking AES . ■

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.