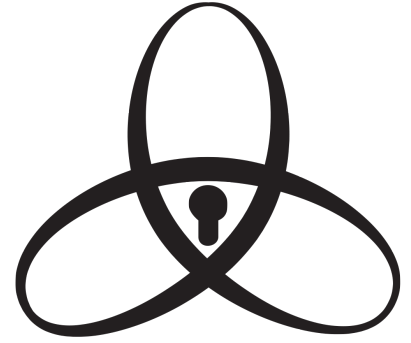


Complexity of the Quantum Algebraic Attack on AES: The condition number of the Macaulay Matrix

Dr. Peter Nonnenmann, Quant-X Security & Coding
Xenia Bogomolec, Quant-X Security & Coding

peter.nonnenmann@quant-x-sec.com
xb@quant-x-sec.com



1 Abstract

We investigate the condition number of the Macaulay matrix in the Quantum Algebraic Attack [1] on the symmetric cryptographic algorithm AES (Advanced Encryption Standard [2]). AES is the standardized version of RIJNDAEL and globally used for hybrid encryption in protocols such as TLS, OpenPGP, SSH, IPsec, etc. as well as for purely symmetric applications such as hard disk encryption.

We show that the complexity of a Quantum Algebraic Attack on AES equals infinity, independent from the key size. Therefore the application of Boolean equation solving [1] on AES is not practical.

2 Introduction

It is known for decades that currently used asymmetric cryptography relying on the hardness of integer factorization and discrete logarithm systems will no longer be valid with the advent of potent enough quantum computers. Quantum cryptanalyses on symmetric cryptography have been published far more recent, amongst them

- 1) Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems
Chen-Gao quantum algorithm [1].
- 2) A fast quantum mechanical algorithm for database search
Grover's search algorithm [3].

Grover's search algorithm can be used to extract the key from a small number of AES plaintext-ciphertext pairs (e. g. 5 for AES-256 [4]). It is an alternative algorithm for an exhaustive key search (brute force attack). There are published papers with quantum resource estimates for AES [4], EAES [5, 14], SHA-3 [6] and SHA-2 [6].

The **Chen-Gao quantum algorithm** raised expectations to a harder impact on the security of AES-256. It involves a quantum algebraic attack on cryptosystems, which can be reduced to Boolean equation solving. This attack reduces the security level of AES-256 from 256 to 78.53, with a factor κ^2 , the condition number of the Boolean equation system used in the algorithm. The condition number κ depends on the cryptosystem which is solved by the Chen-Gao quantum algorithm. We investigated the condition number of AES-256.

3 Chen-Gao Quantum Algorithm: A Quantum Algebraic Attack

The authors of [1] present an algorithm which leads to new considerations of the security of systems which can be reduced to solving Boolean equations. A solution a for the equation $\mathcal{F} \cdot a = 0$ with a set of polynomials $\mathcal{F} \subset \mathbb{C}[X]$ is called *Boolean* if each coordinate of a is either 0 or 1. For the detailed description of the Chen-Gao quantum algorithm, we refer to the original paper [1].

The resulting quantum algebraic attack algorithm includes quantum-monomial solving of polynomial systems over \mathbb{C} by applying a Macaulay linear system. Like this they constructed a Boolean equation solving algorithm, with the following properties:

- 1) It decides if there exists a Boolean solution.
- 2) It returns a Boolean solution with a given probability if there are such solutions to the system.
- 3) It returns \emptyset if no Boolean solution exists.

The matrix M_{MCA} , which represents the Macaulay linear system of the attacked crypto system, defines the desired condition number κ . In order to derive M_{QAA} and then compute κ of AES, we take a look at the structure of QAA.

3.1 Mathematical structure of AES

All RIJNDAEL functions are linear. Only the basic encryption function *SubBytes* (see section Basic RIJNDAEL encryption functions) is often referred as the non-linear part of AES, but in fact it is linear as well. Well chosen linear layers with very strong diffusion properties protect against conventional attacks using statistical properties of a cryptosystem. In the case of the quantum algebraic attack, this effect is limited.

The 4 basic functions of the RIJNDAEL encryption are:

- 1) *AddRoundKey* - addition in $(\mathbb{F}_2)^{128}$:
Bitwise addition of the state and the correspondent round key.
- 2) *SubBytes* - non-linear substitution:
Each byte is replaced by another according to the specified substitution table (*S-Box*). A more resource friendly option is to treat a state byte as an element $\alpha \in \mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$, where the multiplicative inverse of α needs to be found.
- 3) *ShiftRows* - transposition for diffusion:
The second, third and fourth row of the state are shifted to the left, by 1, 2 and 3 steps.
- 4) *MixColumns* - mixing for diffusion:
Multiplication of each column of the state with the following matrix M_{AES} :

$$M_{AES} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

3.2 Analysis

By P. Nonnenmann with the friendly support of S. Rump

In the analysis of the Chen-Gao quantum algorithm on AES, we make the same definitions as Chen-Gao, and use the same numeration of definitions, remarks, Theorems etc. Let \mathbb{C} be the field of complex numbers and $\mathbb{C}[X]$ the polynomial ring in the indeterminates $X = x_1, \dots, x_n$, $n \in \mathbb{N}$ over \mathbb{C} .

For a polynomial $f \in \mathbb{C}[X]$, we denote

$\deg(f)$ = the total degree of f , i. e. the maximal sum of powers of the variables per single monomial,
 $s(f)$ = the sparseness of f , i. e. the number of terms in f ,
 $\Lambda m(f)$ = the set of monomials of f .

For $S \subseteq \mathbb{C}[X]$, we denote $V_{\mathbb{C}}(S) \subseteq \mathbb{C}^n$ the variety of the polynomials in S .

Let $F = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{C}[X]$, $r \in \mathbb{N}$, $d_i = \deg(f_i)$, $t_i = s(f_i)$, $i \in \{1, \dots, r\}$.

Definition 3.2.1

Without loss of generality, we may assume $f_i(0) = -1$ for $i \in \{1, \dots, \rho\}$ and $f_j(0) = 0$ for $j \in \{\rho + 1, \dots, r\}$, where $1 \leq \rho \leq r$.

The f_i are the polynomials with a constant term, and f_j are the polynomials without a constant term. We order the polynomials f_i in the ideal F such that it is convenient for the definition 3.1. Furthermore we are allowed to multiply each polynomial f_i , with constant term c , with the factor $\frac{1}{c}$ without changing the ideal F or its variety

$V_{\mathbb{C}}(F)$.

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

Let d be the minimal integer such that $d \geq (D - \min_{i=1}^r d_i)$ and $d + 1 = 2^\delta$ for some $\delta \in \mathbb{N}$.

Let $\bar{D} \in \mathbb{N}$ be the minimal integer such that $\bar{D} \geq D_{\max}$ and $\bar{D} + 1 = 2^\Delta$ for some $\Delta \in \mathbb{N}$.

Remark 3.2.2

In this paper, the subscripts for a matrix or a vector always start from 0, because the complexity analysis of the 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 [7] of F , and the Macaulay linear equation system of F is solved by the HHL quantum algorithm, see [9].

Macaulay linear equation system: $M_{F,D} \cdot m_D = b_D$, where $M_{F,D}$ is the modified Macaulay matrix of the polynomial system F . By the construction of Chen-Gao, $M_{F,D}$ is a matrix over \mathbb{C} of the following dimension $\dim(M_{F,D})$:

$$\dim(M_{F,D}) = (r(d+1)^n) \times ((\bar{D}+1)^n - 1) = (r \cdot 2^{n\delta})(2^{n\Delta} - 1),$$

with the given parameters above.

Remark 3.2.3

The columns of $m_{\bar{D},j}$ 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 below. The only important fact for us is the existence of 0-columns in the Macaulay matrix.

Remark 3.2.4

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 below for a small, but typical example of a Macaulay matrix [8].

$$\begin{cases} f_1 : x_1x_2 - 2x_2 = 0, \\ f_2 : x_2 - 3 = 0, \end{cases}$$

we have that $\max(d_1, d_2) = 2$ and we want to construct $M(3)$. The first 2 rows then correspond with the coefficient vectors of f_1, f_2 . Since $\max(d_1, d_2) = 2$ and $d_2 = 1$, the next 2 rows correspond to the coefficient vectors of x_1f_2 and x_2f_2 of degree 2. Notice that these first 4 rows make up $M(2)$ when the columns are limited to all monomials of degree 0 up to 2. The next rows that are added are the coefficient vectors of x_1f_1, x_2f_1 and $x_1^2f_2, x_1x_2f_2, x_2^2f_2$ which are all polynomials of degree 3. This way of constructing the Macaulay matrix $M(3)$ then results in

$$M(3) = \begin{matrix} & \begin{matrix} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{matrix} \\ \begin{matrix} f_1 \\ f_2 \\ x_1f_2 \\ x_2f_2 \\ x_1f_1 \\ x_2f_1 \\ x_1^2f_2 \\ x_1x_2f_2 \\ x_2^2f_2 \end{matrix} & \begin{pmatrix} 0 & 0 & -2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \end{pmatrix} \end{matrix}.$$

Figure 1: Example for a simple Macaulay Matrix.

Definition 3.2.5

Let A be a complex matrix, $A \in \mathbb{C}^{M,N}$, and its complex conjugate transpose $A^\top \in \mathbb{C}^{N,M}$. The singular values of A , $s_1 \geq s_2 \geq \dots \geq s_p \geq 0$, $p = \min(M, N)$, are defined to be the positive square roots of the eigenvalues of AA^\top and $A^\top A$. The condition number $\kappa(A) := \frac{s_{\max}}{s_{\min}}$ is the quotient of the maximal and minimal singular values.

Definition 3.2.6

Given $f : \mathbb{C}^N \Rightarrow \mathbb{C}^N$, we denote by $Eig(f, \lambda)$ the eigenspace of f associated with the eigenvalue λ .

The dimension-formula for linear maps $f : \mathbb{C}^N \Rightarrow \mathbb{C}^N$ says that $\dim \ker(f) + \text{rank}(f) = N$. So $Eig(f, 0) = \ker(f)$ (the kernel of f). Now, let $M = M_{F,D}$ (F, D are arbitrary) be one of the modified Macaulay matrices constructed by Chen-Gao as above. Then we consider the linear map $f : \mathbb{C}^N \Rightarrow \mathbb{C}^N$, induced by the matrix $M^\top M$, and our result is:

Theorem 3.2.7

$\kappa(M) = \infty$.

Proof of Theorem 3.2.7

First note that M has at least one 0-row and one 0-column by remarks 3.3 and 3.4 (Actually, for this proof, the existence of a 0-row OR a 0-column is sufficient.) Then $M^\top M = f$ has at least one 0-row, too, by matrix multiplication. Then $\text{rank}(f) \leq N - 1$, and by the dimension-formula for linear maps, it follows that $\dim \ker(f) + \text{rank}(f) \leq \dim \ker(f) + N - 1$, so $N \leq \dim \ker(f) + N - 1$.

Assume that $\dim \ker(f) = 0$, then it also holds that $N \leq N - 1$, which is a contradiction. Therefore we have $\dim \ker(f) \geq 1$ and $\dim Eig(f, 0) \geq 1$, which in turn means, that f has the eigenvalue $\lambda = 0$. So M has the singular value $s = 0 = s_{\min}$, the minimal singular value, and $\kappa(M) = \frac{s_{\max}}{s_{\min}} = \infty$.

Theorem 3.2.8

The condition number of the whole polynomial system F is infinite.

Proof of Theorem 3.2.8

In the paper [1], algorithm 4.2 has the following properties: The runtime complexity of the algorithm is $\mathcal{O}(n^{2.5}(n + T_F)\kappa^2 \log(\frac{1}{\epsilon}))$, where κ is the maximal condition number for all matrices $M_{F^2,D}$ in Step 4, called the CONDITION NUMBER $\kappa(F) = \kappa$ for the polynomial system F . By their Lemma 4.5, there are at most n iterations in the loop, where the matrices $M_{F^2,D}$ are used. Since all their condition numbers are infinite, the condition number of the polynomial system is infinite as well, and so is the runtime complexity of the Chen-Gao-Algorithm (Theorem 4.3).

4 Conclusion

The conclusion of [1] is, that systems which can be solved by Boolean equation solving, are only secure under quantum algebraic attack, if the condition number κ is large. The runtime complexity of the resulting quantum algebraic attack depends on two factors: a constant c and a condition number κ . The complexity of $2^{78.53} c \kappa^2$ for AES-256 is not much higher than the complexity of $2^{73.30} c \kappa^2$ for AES-128 due to the same block size of 128 bit. Therefore we can assume that the complexity won't be much higher for 512-bit key sizes.

The condition number $\kappa = \infty$ for AES does not even depend on the key size. It implies 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, considered that the complexity of EAES is larger than the one of AES [15].

Besides AES and KECCAK, stream ciphers such as TRIVIUM and the multivariate public key cryptosystem MPKC are affected by the attack.

5 Context

5.1 Realization of Quantum Computing

With the advent of 49 qubit processors quantum supremacy, the ability of quantum computing devices to solve problems that classical computers practically cannot solve, lies within reach. IBM's 14th quantum computer is its most powerful so far, a model with 53 of the qubits that form the fundamental data-processing element at the heart of the system [10]. Google participates in the race with their 72-qubit quantum processor Bristlecone [11].

The German Federal Office for Information Security (BSI) published a paper about the state of developments in quantum computing [12]. They outline that the realization of potent quantum computers faces great challenges such as the scaling of needed qubits by error correcting codes and enormous hardware costs.

On the other hand, successful discoveries through research for *topological quantum computation* [13] might create a verbatim "quantum leap" in quantum computation evolution, because they won't depend on error correcting mechanisms. Furthermore, adiabatic quantum computers, which work with *quantum annealing mechanisms*, are already very successfully used for optimization problems.

5.2 Hybrid Cryptosystems

With the availability of potent enough quantum computers, all private keys of asymmetric cryptosystems will be computable within reasonable time from the corresponding public keys. With the knowledge of those private keys, all encrypted data, which was collected and assigned to the relevant key exchanges, will no longer remain secret.

Hybrid encryption systems combine the advantages of both cryptography classes, symmetric and asymmetric crypto systems. Asymmetric protocols allow securely sharing a key via digital connections, and symmetric protocols are about $10^5 \times$ faster than asymmetric ones. The secret session key SK , whose validity is limited in time, is shared via asymmetric cryptography, and the message itself is symmetrically encrypted with the securely shared session key SK . Hybrid cryptosystems are used in all major crypto protocols: TLS, SSH and PGP. They

No asymmetric encryption within hybrid encryption systems can outbalance weaknesses of the symmetric part. ISO currently makes it possible to standardize new symmetric cryptography algorithms and to amend existing ones. Therefore, we strive to establish EAES as an ISO-Standard. Its predecessor AES has been standardized by both organizations.

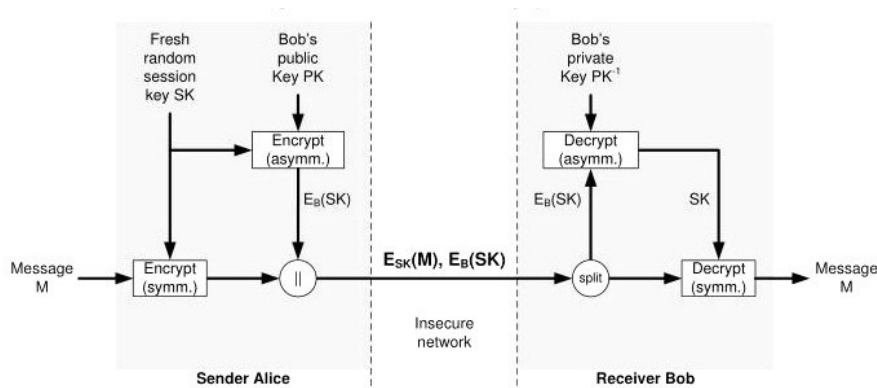


Figure 2: Hybrid encryption.

References

- [1] Y. -A. Chen, X. -S. Gao, Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems, <https://arxiv.org/abs/1712.06239>, 2018.
- [2] Federal Information Processing Standards Publication 197, NIST, Announcing the ADVANCED ENCRYPTION STANDARD (AES), <https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf>, 2000.

- [3] L. K. Grover, A fast quantum mechanical algorithm for database search, *Gary L. Miller, editor, Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (STOC 1996)*, pages 212–219 ACM, 1996.
- [4] M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt, Applying Grover’s algorithm to AES: quantum resource estimates, <https://arxiv.org/abs/1712.06239>, 2018.
- [5] S. Kovac and J. Underhill, Towards post-quantum symmetric cryptography, <https://eprint.iacr.org/2019/553>.
- [6] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, J. Schanck, Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3s, <https://eprint.iacr.org/2016/992.pdf> QCrypt, 2016.
- [7] F.S.M. Macaulay, Some formulas in elimination, *Proc. Of the London Mathematical Society*, 35(1), 3-38, 1902.
- [8] K. Batselier, P. Dreesen, B. De Moor, On the null spaces of the Macaulay matrix, <https://www.eee.hku.hk/~kim-b/pdfs/MacaulayMatrix.pdf>.
- [9] A.W. Harrow, A. Hassidim, S. Lloyd, Quantum algorithm for linear systems equations, *Physical Review Letters*, 103(15): 150502, 2009.
- [10] S. Shankland, MSN News, <https://www.msn.com/en-us/news/technology/ibms-new-53-qubit-quantum-computer-is-its-biggest-yet/ar-AAHtPaW>, September 2019.
- [11] J. Kelly, Google AI Blog, <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>, March 2018.
- [12] BSI, Federal Office for Information Security Germany, Entwicklungsstand Quantencomputer https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie.pdf, May 2018
- [13] S. Ran, C. Eckberg, Q.-P. Ding, Y. Furukawa, T. Metz, S.R. Saha, I-L. Liu, M. Zic, H. Kim, J. Paglione and N.P. Butch, NIST events on paper of above authors, <https://www.nist.gov/news-events/news/2019/08/newfound-superconductor-material-could-be-silicon-quantum-computers>.
- [14] J. Underhill, The CEX Cryptographic library in C++, <https://github.com/Steppenwolfe65/CEX>.
- [15] X. Bogomolec, J. G. Underhill, S. A. Kovac, Towards Post-Quantum secure symmetric Cryptography: A mathematical Perspective, *Cryptology ePrint Archive: Report 2019/1208.*, 2019.