Game Changer Computeralgebra

In the Context of Quantum Computing

Xenia Bogomolec, Information Security
Dr. Peter Nonnenmann, Quantum Theory
(with scientific employment at DHBW Mannheim)

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

Introduction

It has been widely accepted by industrial and governmental instances 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 sufficiently potent quantum computers. Much less considered are quantum cryptanalyses on symmetric cryptography, amongst them

1) Chen and Gao's Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems, short **Quantum Algebraic Attack (QAA)** [1].
2) A fast quantum mechanical algorithm for database search, short **Grover's Search Algorithm** [2].

Grover's Search Algorithm was devised by *Lov Grover* in 1996. Many complexity analyses of Grover's Search on currently used cryptographic algorithms, such as AES, SHA-2 and SHA-3 have been published ever since [3, 4].

The Quantum Algebraic Attack, short QAA, published 2018, is far less understood but at the same time a strong potential game changer for basic design requirements of cryptographic algorithms. Computeralgebra plays an essential role within the innovative approach of solving the involved Boolean Multivariate Quadratic Equation System (BMQ) with a quantum computer.

Mechanism of QAA

The Quantum Algebraic Attack applies to cryptosystems which can be reduced to a BMQ. A Boolean Quadratic Multivariate Equation System is a system of quadratic multivariate equations in which the values of the variables are the Boolean values *true* and *false*, or 1 and 0 respectively. Globally used cryptographic algorithms such as KECCAK (SHA-3), AES, TRIVIUM and MPQC (Multivariate Public Key Cryptosystem) can be reduced to a BMQ and are therefore affected by the Quantum Algebraic Attack - if it is practical.

The key ingredients of the QAA are:

1) The HHL quantum algorithm [5], a Gaussian elimination solver for linear equation systems.
2) Computing a variety of the BMQ over $\mathbb{C}$.
3) Mapping the system to $\mathcal{F}_2$.

The QAA reduces the polynomial system in step 2) to a linear equation system in step 1) by encoding the polynomial system in step 2) into a specified Macaulay matrix. In the case of AES, the BMQ is in the ring $\mathbb{C}[\underline{x}]$ with 14 variables, and the Macaulay matrix of AES-256 is built from polynomials with 11904 variables (see [1], page 25, section before proposition 6.1.

Feasibility of the QAA

The feasibility of the QAA depends on two factors:

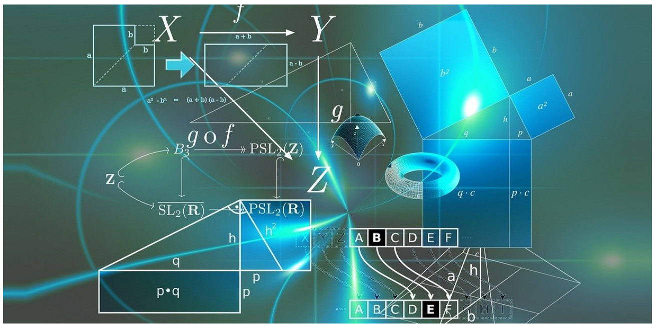
1) The realization of adequately potent quantum computers.
2) The condition number κ of the Macaulay matrix derived from the BMQ of a specific affected cryptosystem.

An "Adequately potent quantum computer" in terms of number of stable qubits can only be determined for a cryptosystem if its κ is known.

Chen and Gao computed the runtime complexity of the QAA for the four previously mentioned cryptosystems. The complexity constant c of the *HHL algorithm* contributes to the runtime complexity linearly. The condition number κ is contained as a quadratic term.

Computing or estimating the values of the specific κ of a cryptosystem is the next step to identify whether it is prone to the QAA when sufficiently potent quantum computers are available.

Chen and Gao say: *"Condition numbers of equation systems are generally difficult to estimate, and estimating the condition numbers for these cryptosystems is an interesting future work"* ([1], page 3).


X
f
Y
g
$g \circ f$
B_3
$\mathrm{PSL}_2(\mathbf{Z})$
Z
$\mathrm{SL}_2(\mathbf{R})$
$\mathrm{PSL}_2(\mathbf{R})$
$a^2 - b^2 = (a+b)(a-b)$
h
q
p
p•q
A B C D E F
a
b
b^2
a^2
q·c
p·c

Dr. Peter Nonnenmann is currently working on a solution to create the Macaulay matrix of the cryptosystem AES and compute its condition number κ. You can read more about the progress in our official paper on github [6](open source industrial-scientific project).

Impact on Block Cipher Design

The very innovative design of the QAA has a considerable impact on how we might design cryptosystems in the future. E. g. in the case of a block cipher, we always have a symmetric key, from which sub keys are derived for the rounds of the block encryption. In classical settings and even wrt. Grover's search, the complexity of the sub key derivation function adds to the runtime complexity of the whole encryption algorithm.

For the QAA, we have a different situation: The key derivation function has has no impact on the runtime complexity, because:

1) The key and the expanded key are considered key variables in the BMQ.
2) The derived sub keys are considered state variables in the BMQ.

So for secure cryptography wrt. the QAA, we will need cryptosystems which cannot be reduced to a BMQ or cryptosystems which can be reduced to a BMQ but have a specified Macaulay matrix with a large condition number κ.

We have received the friendly support from industry (Mathworks) and scientists (Prof. Dr. Siegfried Rump, Head of the Institute for Reliable Computing, TU Harburg amongst others).

Interested contributers are welcome to join us!

References

[1] Y. A. Chen, X. S. Gao, Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems, *https://arxiv.org/pdf/1712.06239v3.pdf*, 2018.

[2] 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.

[3] M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt, Applying Grover's algorithm to AES: quantum resource estimates, *https://arxiv.org/abs/1712.06239*, 2018.

[4] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, J. Schanck, Estimating the cost of eneric quantum pre-image attacks on SHA-2 and SHA-3s, *https://eprint.iacr.org/2016/992.pdf* QCrypt, 2016.

[5] A.W. Harrow, A. Hassidim, S. Lloyd, Quantum algorithm for linear systems equations, *Physical Review Letters, 103(15)*: 150502, 2009.

[6] Open source industrial-scientific project initiated by Quant-X Security & Coding GmbH
P. Nonnenmann, X. Bogomolec, and various temporary contributers Feasibility of the Quantum Algebraic Attack on AES, *https://github.com/XeniaGabriela/QAA_Condition_Nr-/blob/master/official_paper/QAA_on_AES_paper.pdf*: 2020.