

Quantum Technology Transfer Catalysers

How we enable the integration of quantum technologies in classical infrastructures

<https://quant-x-sec.com> | xb@quant-x-sec.com

image source: midjourney

10/08/23

xb@quant-x-sec.com



QUANT-X SECURITY & CODING

mastering digital complexity

Who We are

Founded in 2019 / Located at Hanover, Germany / 10 employees: Men and Women of Letters

IT EXPERTS / CONSULTING

- Information Security
- Project Management
- Software Engineering
- IT Operations

RESEARCH & DEVELOPMENT

- Software Engineering
- Security Analyses & Proofs



QUANT-X SECURITY & CODING

xb@quant-x-sec.com



Quantum Technology Related Activities

“Preserve confidentiality, integrity and availability of data in the future”

- Quantum and Post-Quantum Security Integration
- Quantum and Post-Quantum Security Migration
- Quantum Security Proofs and Validation
- Quantum Algorithm Feasibility Studies

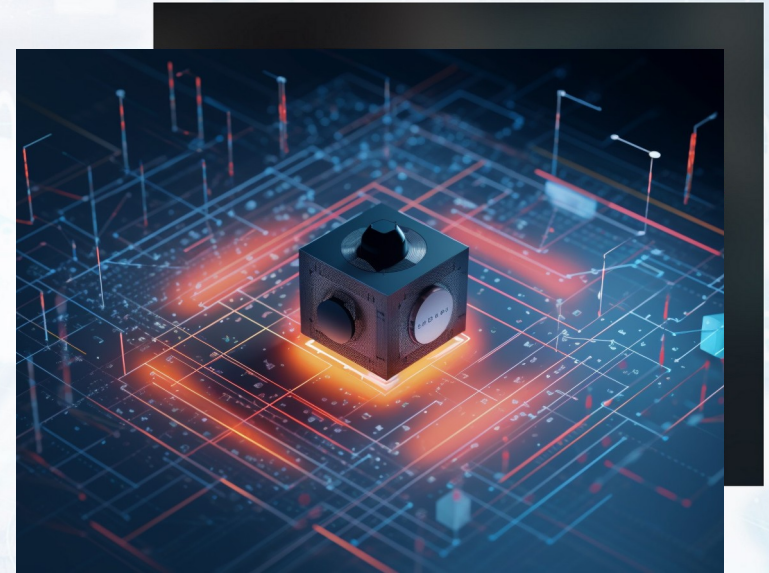


image source: midjourney



R&D - Quantum and Post-Quantum Integration

[Project](#)[Partners](#)[Associated Partners](#)[Contact](#)[DE](#)

QUANTUM SECURE DIGITAL IDENTITIES



<https://quant-id.de/>

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Dieses Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KISQ108K gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei Quant-ID.



Fraunhofer
IPMS

MTG



image source: iStock

Quantum and Post-
Quantum Security

OAuth / OpenID Connect

Associated

ROLAND
HEDBERG

GUISEPPE
DE MARCO



Fraunhofer IPMS:
QRNG development

Quant-X:

- Project coordination
- QRNG entropy proof and validation
- IAM protocol adjustments
- Software engineering
- Operations of end user applications
- Statistics

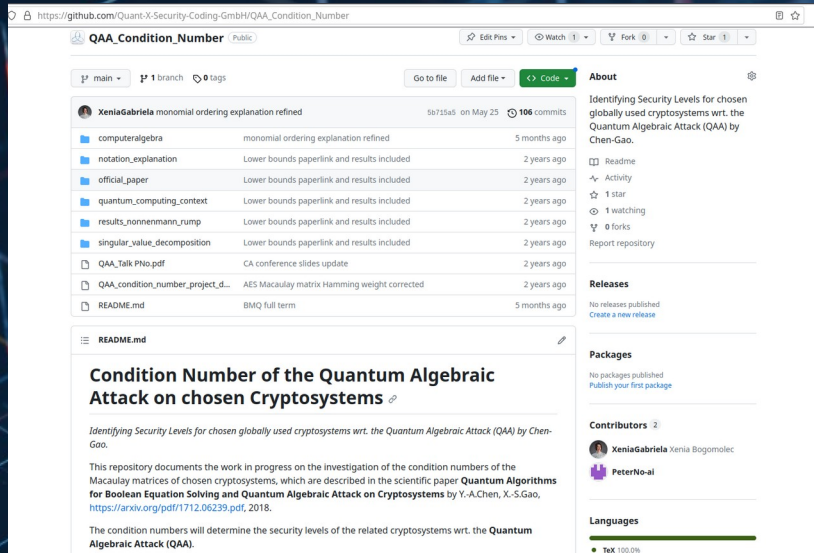
MTG AG:

- PQC-PKI
- HW-SW APIs

University of Regensburg:

- PQC-Analyses
- QRNG entropy proof and validation lead

Quantum Algorithms – QAA / HHL



https://github.com/Quant-X-Security-Coding-GmbH/QAA_Condition_Number

QAA_Condition_Number Public

1 branch 1 tag

Go to file Add file Code

About

Identifying Security Levels for chosen globally used cryptosystems wrt. the Quantum Algebraic Attack (QAA) by Chen-Gao.

106 commits

5 months ago

2 years ago

2 years ago

2 years ago

2 years ago

2 years ago

2 years ago

2 years ago

2 years ago

5 months ago

computeralgebra monomial ordering explanation refined

notation_explanation Lower bounds paperlink and results included

official_paper Lower bounds paperlink and results included

quantum_computing_context Lower bounds paperlink and results included

results_nonnenmann_rump Lower bounds paperlink and results included

singular_value_decomposition Lower bounds paperlink and results included

QAA_Talk_PhD.pdf CA conference slides update

QAA_condition_number_project_d... AES Macaulay matrix Hamming weight corrected

README.md BMQ full term

Condition Number of the Quantum Algebraic Attack on chosen Cryptosystems

Identifying Security Levels for chosen globally used cryptosystems wrt. the Quantum Algebraic Attack (QAA) by Chen-Gao.

This repository documents the work in progress on the investigation of the condition numbers of the Macaulay matrices of chosen cryptosystems, which are described in the scientific paper [Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems](https://arxiv.org/pdf/1712.06239.pdf) by Y.-A.Chen, X.-S.Gao, <https://arxiv.org/pdf/1712.06239.pdf>, 2018.

The condition numbers will determine the security levels of the related cryptosystems wrt. the Quantum Algebraic Attack (QAA).

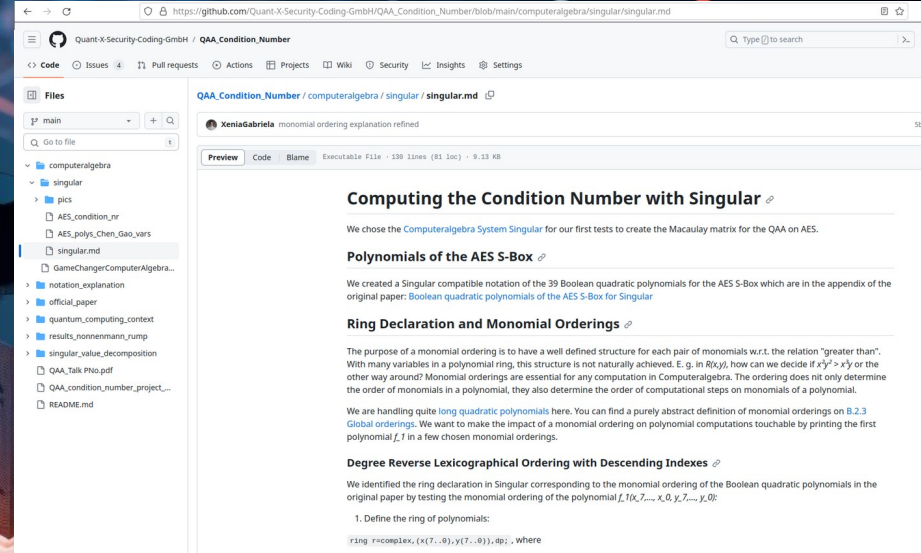
Contributors

XeniaGabriela Xenia Bogomolec

PeterNo-ai

Languages

Text 100.0%



https://github.com/Quant-X-Security-Coding-GmbH/QAA_Condition_Number/blob/main/computeralgebra/singular/singular.md

Quant-X-Security-Coding-GmbH / QAA_Condition_Number

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

Files

main

Go to file

computeralgebra

singular

pics

AES_condition_nr

AES_polys_Chen_Gao_vars

singular.md

GameChangerComputerAlgebra...

notation_explanation

official_paper

quantum_computing_context

results_nonnenmann_rump

singular_value_decomposition

QAA_Talk_PhD.pdf

QAA_condition_number_project...

README.md

Computing the Condition Number with Singular

We chose the [Computeralgebra System Singular](#) for our first tests to create the Macaulay matrix for the QAA on AES.

Polynomials of the AES S-Box

We created a Singular compatible notation of the 39 Boolean quadratic polynomials for the AES S-Box which are in the appendix of the original paper: [Boolean quadratic polynomials of the AES S-Box for Singular](#)

Ring Declaration and Monomial Orderings

The purpose of a monomial ordering is to have a well defined structure for each pair of monomials w.r.t. the relation "greater than". With many variables in a polynomial ring, this structure is not naturally achieved. E.g. in $R[x,y]$, how can we decide if $x^2y^2 > x^3y$ or the other way around? Monomial orderings are essential for any computation in Computeralgebra. The ordering does not only determine the order of monomials in a polynomial, they also determine the order of computational steps on monomials of a polynomial.

We are handling quite [long quadratic polynomials](#) here. You can find a purely abstract definition of monomial orderings on [B.2.3 Global orderings](#). We want to make the impact of a monomial ordering on polynomial computations touchable by printing the first polynomial f_1 in a few chosen monomial orderings.

Degree Reverse Lexicographical Ordering with Descending Indexes

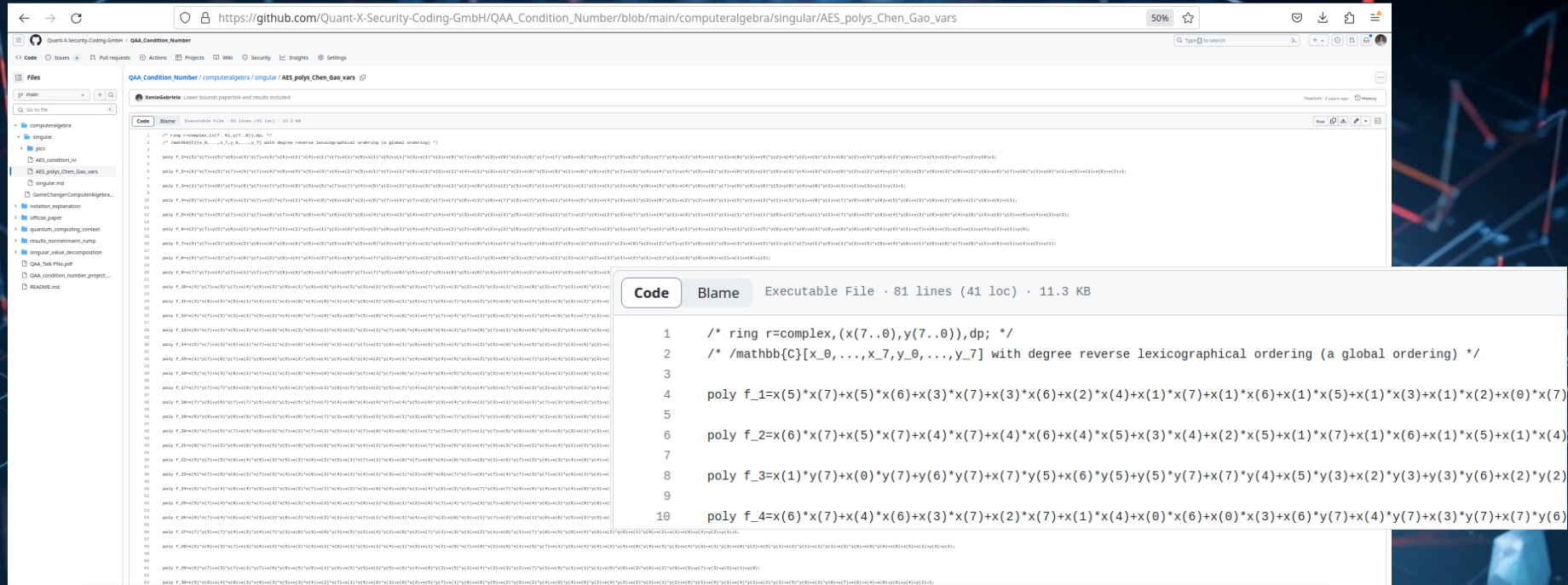
We identified the ring declaration in Singular corresponding to the monomial ordering of the Boolean quadratic polynomials in the original paper by testing the monomial ordering of the polynomial $f_1(x, y, z, \dots, x_0, y, z, \dots, y, 0)$:

1. Define the ring of polynomials:

```
ring r=complex, (x(7..8), y(7..8)), dp;
```

Focus: What we can achieve with Computeralgebra

Quantum Algorithms – QAA AES Quadratic Polynomials



The screenshot shows a GitHub repository for 'Quant-X-Security-Coding-GmbH/QAA_Condition_Number'. The file 'AES_polys_chen_gao_vars' is selected, showing a list of quadratic polynomials in a Singular ring. The polynomials are defined over a complex field and involve variables x_0 through x_7 and y_0 through y_7 . The polynomials are:

- $\text{poly } f_1 = x(5)*x(7)+x(5)*x(6)+x(3)*x(7)+x(3)*x(6)+x(2)*x(4)+x(1)*x(7)+x(1)*x(6)+x(1)*x(5)+x(1)*x(3)+x(1)*x(2)+x(0)*x(7)$
- $\text{poly } f_2 = x(6)*x(7)+x(5)*x(7)+x(4)*x(7)+x(4)*x(6)+x(4)*x(5)+x(3)*x(4)+x(2)*x(5)+x(1)*x(7)+x(1)*x(6)+x(1)*x(5)+x(1)*x(4)$
- $\text{poly } f_3 = x(1)*y(7)+x(0)*y(7)+y(6)*y(7)+x(7)*y(5)+x(6)*y(5)+y(5)*y(7)+x(7)*y(4)+x(5)*y(3)+x(2)*y(3)+y(3)*y(6)+x(2)*y(2)$
- $\text{poly } f_4 = x(6)*x(7)+x(4)*x(6)+x(3)*x(7)+x(2)*x(7)+x(1)*x(4)+x(0)*x(6)+x(0)*x(3)+x(6)*y(7)+x(4)*y(7)+x(3)*y(7)+x(7)*y(6)$

Next Step: Macaulay Matrix

First industry sector: Biotechnology (Genome Sequencing)

- Database with tech specs of genome sequencing instrument types, library preps and species
- APIs for connecting instruments, service providers and users
- Broker platform for library preps and genome sequencing jobs
- Genome sequencing capacity manager for service providers and the integrated broker platform
- Genome sequencing job search engine by sample species, type of genome analysis, desired delivery date etc.



image source: iStock

Next Step: Betatest.

We are looking for Betatest users (genome sequencing providers and users)!



Contact us if your are interested in cooperation.

Thank you!
Questions?

<https://quant-x-sec.com> | xb@quant-x-sec.com

10/08/23

xb@quant-x-sec.com



QUANT-X SECURITY & CODING

mastering digital complexity