*Basic Research as Open Source Project between Science and Industry:*

# Computing the Condition Numbers of the Quantum Algebraic Attack on chosen Cryptosystems

*Identifying Security Levels of globally used Encryption*

24/10/19

Quant-X Security & Coding GmbH
xb@quant-x-sec.com

# Global Industrial Context

Massive global funding for the development of **Quantum Technologies** brings

- hope for solving health care, environmental and other global problems

but also

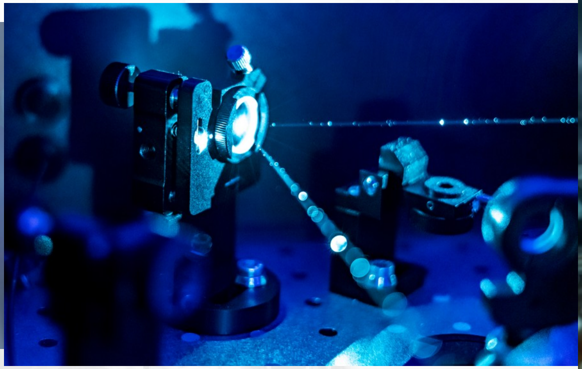
- threats to global data security on the other side

# Post-Quantum Threat Intelligence

## Threat

Confidentiality, Integrity and Authenticity of data in transport and in rest are in danger. [TLS and VPN (Web, Mobile), SSH, PGP (Email), Databases, etc.]

The international competition in the development of Quantum Technologies it is often called a war race.



## Intelligence

In parallel, the development of Quantum Secure Technologies is massively funded as well.

# Our Mission

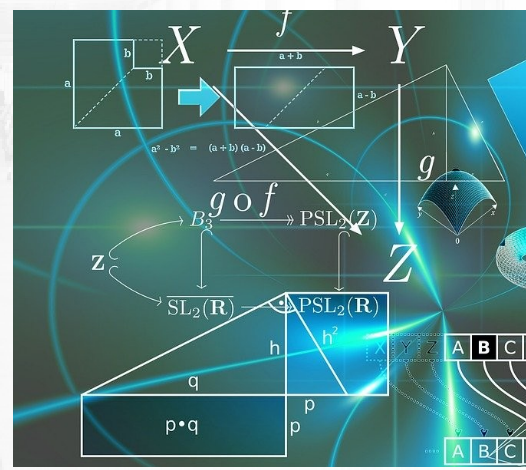
Basic Research for Post-Quantum Threat Intelligence by

- Identifying Quantum Secure Encryption among globally algorithms wrt. recently published *Quantum Algebraic Attack* by Chen-Gao
- Refining requirements for the development of new Quantum Secure Encryption Algorithms, resisting the quantum algebraic attack

## Remark

The *Quantum Algebraic Attack* is not in the scope of the NIST Post-Quantum standardization process which started in 2017! (only for asymmetric systems)

We investigate the security levels of symmetric crypto systems!



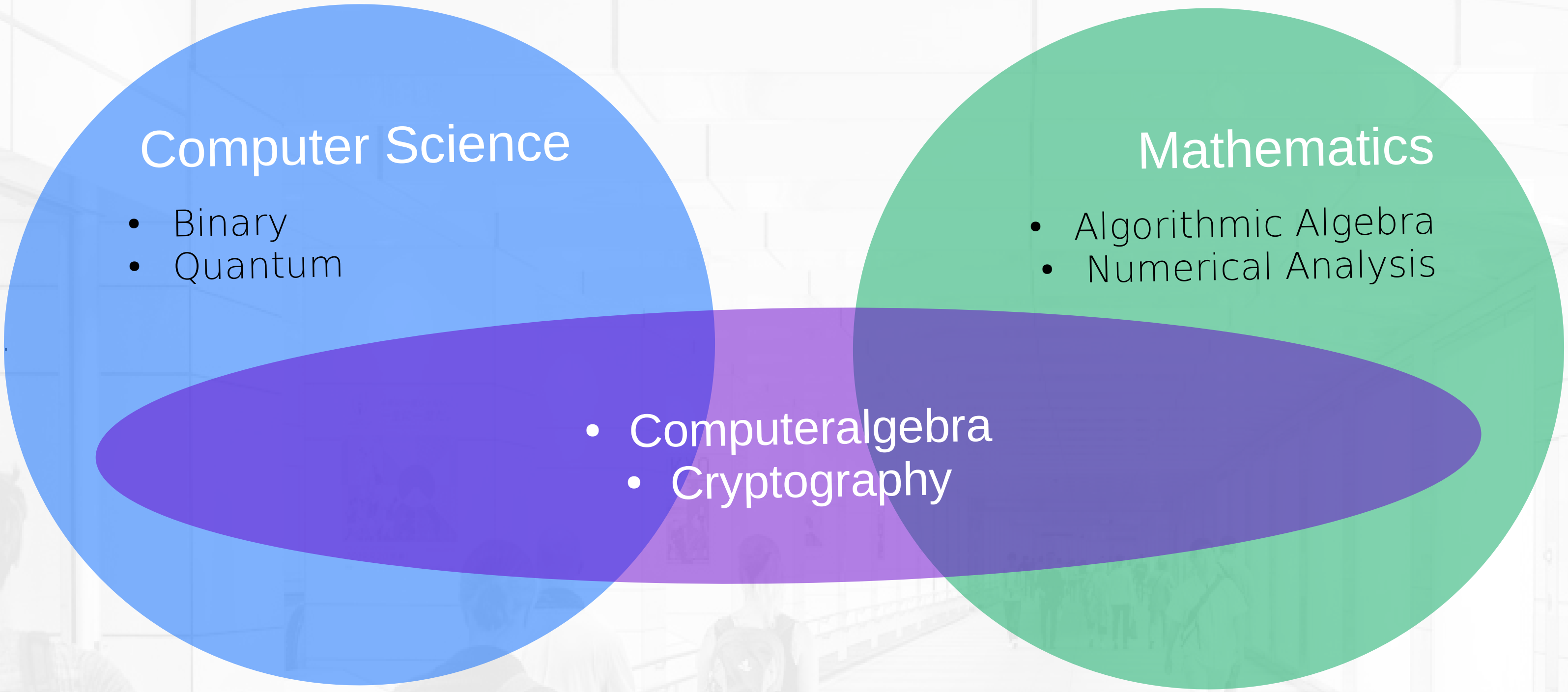
# Scope of our Mission

## Post-Quantum Security for Binary and Quantum Technologies

- Our results cover both, the **binary and quantum computing aspects**!
- Therefore our results will bring benefit to the development of **quantum resistant binary and quantum technologies**.

# Complexity of the Topic

## Scientific and Technological Context



# Security Level Computation

The condition number $\kappa$ in the complexity of the Quantum Algebraic Attack by Chen-Gao is the condition number of the Macaulay matrix defined in their paper.

The computation of $\kappa$ is not trivial due to the size of the matrix, which cannot be handled by classical methods on classical computing systems anymore.

| AES | $N_k$ | $N_r$ | #Vars | #Eqs | T-Sparseness | Complexity |
|---|---|---|---|---|---|---|
| AES-128 | 4 | 4 | 1792 | 4400 | 101376 | $2^{68.61}c\kappa^2$ |
| AES-128 | 4 | 6 | 2624 | 6472 | 151680 | $2^{70.68}c\kappa^2$ |
| AES-128 | 4 | 8 | 3456 | 8544 | 201984 | $2^{72.16}c\kappa^2$ |
| AES-128 | 4 | 10 | 4288 | 10616 | 252288 | $2^{73.30}c\kappa^2$ |
| AES-192 | 6 | 12 | 7488 | 18096 | 421248 | $2^{76.59}c\kappa^2$ |
| AES-256 | 8 | 14 | 11904 | 29520 | 696384 | $2^{78.53}c\kappa^2$ |

# Security Level Estimations

The joint work of Jianqiang Li, Jintai Ding, Vlad Gheorghiu, Andr´as Gily´en, Sean Hallgren,

*Limitations of the Macaulay matrix approach for using the HHL algorithm to solve multivariate polynomial systems,*

offers security level estimations for affected cryptosystems: Chen/Gao's algorithm is exponential in the Hamming weight (number of one's) of the solution (the secret key). As a good randomly generated symmetric secret key has equally many zero's as one's, we can assume that in this case the Hamming weight is about half the size of the key, for AES 256 this would be 128.

[https://indico.physik.uni-muenchen.de/event/84/attachments/248/553/S2C.Li.slides.pdf](https://indico.physik.uni-muenchen.de/event/84/attachments/248/553/S2C.Li.slides.pdf)

## Remark

Thanks to the participants of the Industrial Computeralgebra Conference 2021 for this hint!

# Research Results

*Open Source Project between Science and Industry*

Results are published on Github, where we invited collaborators and reviewers:

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

Computeralgebra Magazine Publication:
*https://fachgruppe-computeralgebra.de/data/CA-Rundbrief/car67.pdf*

Scientific Paper:
*https://github.com/Quant-X-Security-Coding-GmbH/QAA_Condition_Number/blob/main/official_paper/QAA_on_AES_paper.pdf*

# Core Team

## Xenia Bogomolec

- CEO Quant-X Security & Coding
- Information Security Specialist
- Fachreferentin Industrie Fachgruppe Computeralgebra

## Dr. Peter Nonnenmann

- Independent Scientific Researcher
- Quantum Theory
- Computer Science

Fachgruppe Computeralgebra

DMV

# Feedback and Collaborators

Fachgruppe Computeralgebra

And the friendly essential support of

- Prof. Dr. Siegfried Rump (Head of the Institute for for Reliable Computing, TU Harburg
- Christoph Stockhammer, MathWorks