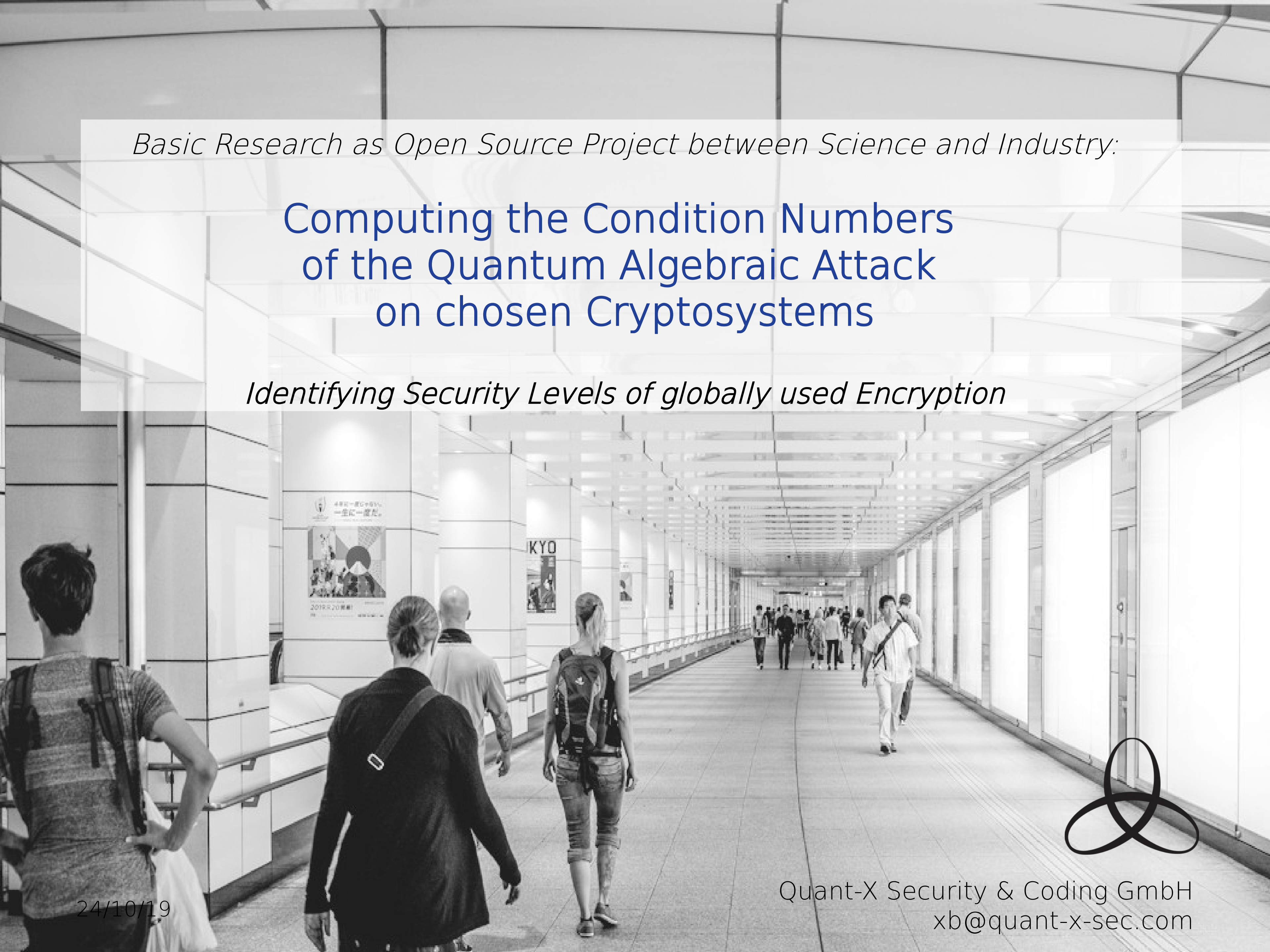
Basic Research as Open Source Project between Science and Industry:

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

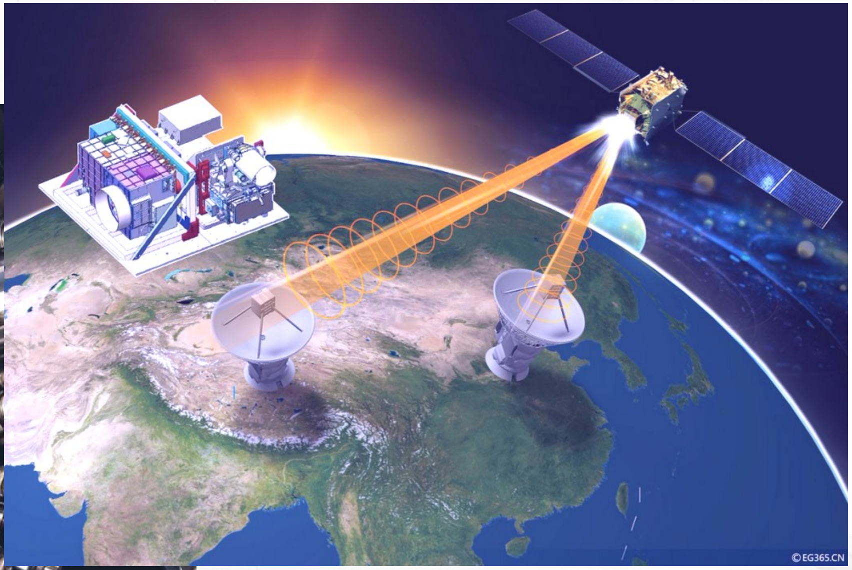
Global Industrial Context

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

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

but also

- threats to global data security on the other side

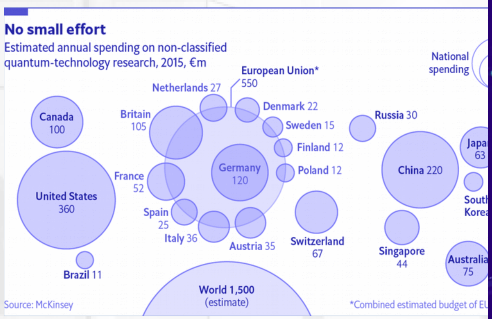


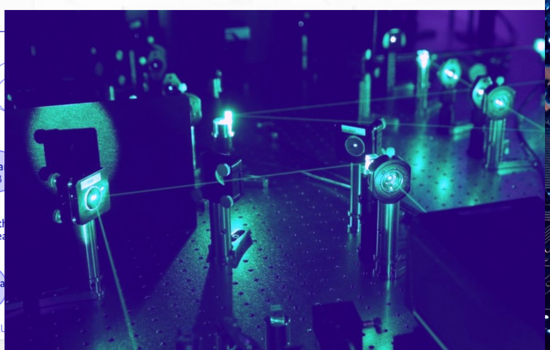
Post-Quantum Threat Intelligence

Threat

Confidentiality, Integrity and Authenticity of data in transport and 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

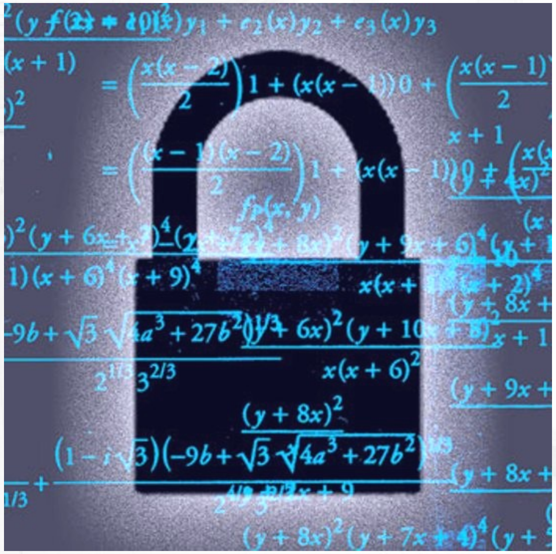
Basic Research for Post-Quantum Threat Intelligence by

- 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)

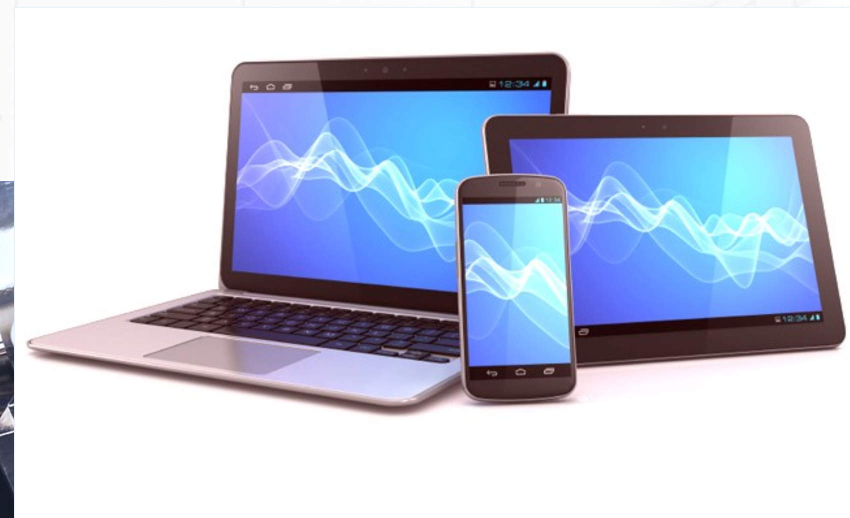
We investigate the security levels of symmetric crypto systems!



Scope of our Mission

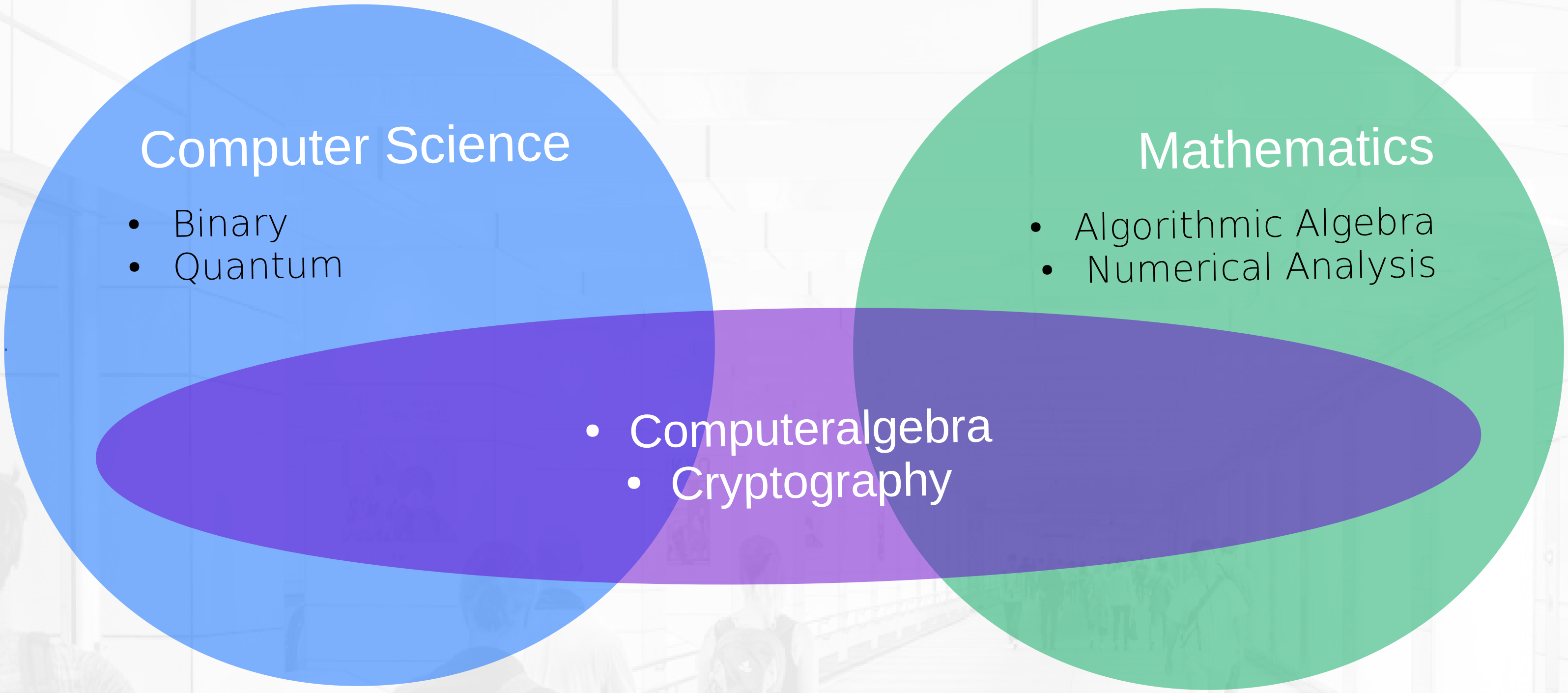
Post-Quantum Security for Binary and Quantum Technologies

- 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



Ongoing Research in Need for Funding

Basic Research as Open Source Project between Science and Industry

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

Overview:
https://github.com/XeniaGabriela/QAA_Condition_Nr

Paper with achieved Results:
https://github.com/XeniaGabriela/QAA_Condition_Nr/blob/master/official_paper/QAA_on_AES_paper.pdf

Considerations for ongoing Research:
https://github.com/XeniaGabriela/QAA_Condition_Nr/blob/master/results_nonnenmann_rump/The%20case%20of%20nonzero%20s%20.pdf

Prototype: Security Level of AES

1) Compute the value of the condition number κ in the complexity of the Quantum Algebraic Attack by Chen-Gao on AES.

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	$2^{78.53} c\kappa^2$

2) Compute the value of the condition number of crypto systems in the Chen-Gao paper (Trivium, Keccak, MPKC)

3) Investigate more affected crypto systems (crypto systems which can be reduced to a Boolean Multivariate Quadratic Equation System).

Steps for Crypto Systems in Chen-Gao Paper

1) Compute the condition number of the Macaulay Matrix of the S-Box for AES

a) For the classical notion of a condition number κ

Done

including zero singular values, $\kappa(\mathrm{AES}) = \text{infinity}$
(see "QAA_on_AES_paper.pdf" on Github)

Cooperation with Prof. Dr. S. Rump, Institute for reliable computing, TU Hamburg

b) For the modified notion of a condition number

Ongoing

excluding zero singular values, $\kappa(\mathrm{AES})$ has to be explicitly computed
(see "the case of nonzero s.pdf" on Github)

Cooperation with Mathworks

2) With identified mechanisms of step 1b), compute the condition numbers of Trivium, Keccak and MPKC.

Open

Polynomials are already identified by Chen-Gao!

Cooperation with Mathworks

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

Feedback and Collaborators

Fachgruppe Computeralgebra

In August 2020 we will have a meeting with the Computeralgebra Professionals Group Germany's Speaker to identify potential further cooperation on the topic.