Grundlagenforschung als industriell-wissenschaftliches Open Source Projekt

Konditionszahlen der Quantum Algebraic Attack von ausgewählten Kryptosystemen

Sicherheitsniveaus von weltweit genutzten Verschlüsselungen

10/07/2020

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

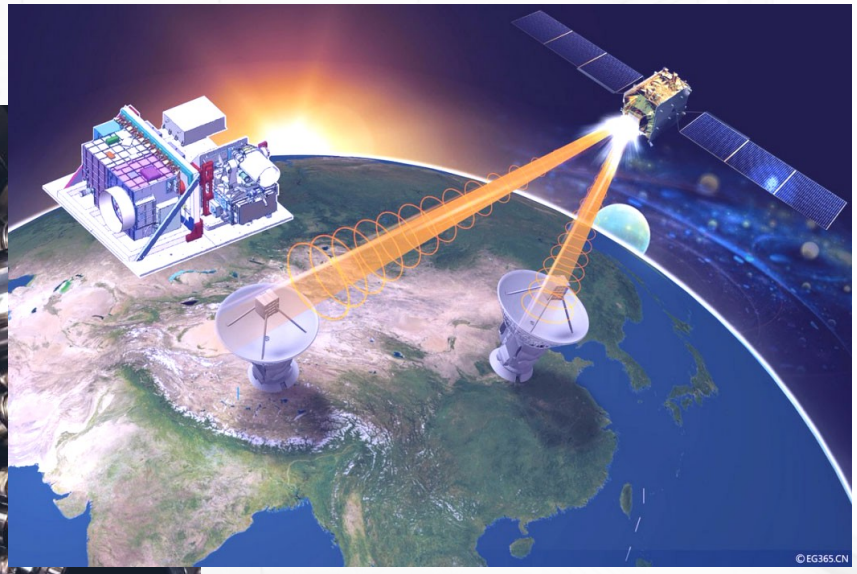
Globaler Industrieller Kontext

Massive globale Förderung der Entwickung von **Quanten-Technologien** bringt

- Hoffnung auf Lösung von Herausforderungen in der Medizin, Umwelt und anderen globalen Problemen

...aber auch

- Bedrohung von globaler Datensicherheit in Kommunikation und Speicherung

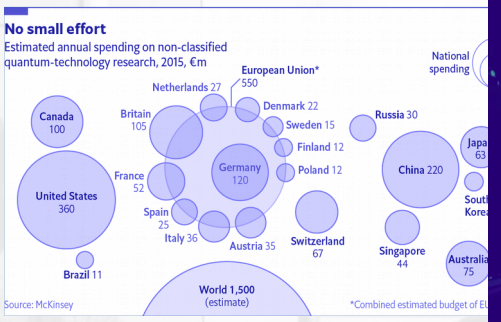


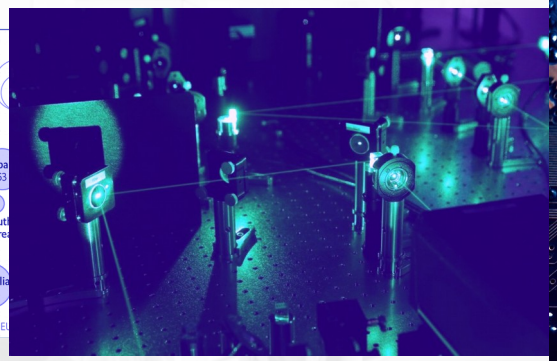
Quantensichere “Threat Intelligence”

Bedrohung

Vertraulichkeit, Integrität und Authentizität von Daten in Kommunikation und Speicherung sind gefährdet [TLS und VPN (Web, Mobile), SSH, PGP (Email), Datenbanken, etc.]

Die internationale Wettrennen in der Entwicklung von Quanten Technologien wird oft als globales Kriegsrennen bezeichnet.





Intelligenz

Parallel wird die Entwicklung Quantensicherer Technologien ebenfalls stark gefördert. Unser Projekt ist in diesem Bereich zu verorten.

Unsere Mission

Grundlagenforschung für "Quantum Threat Intelligence"

- Identifikation Quantensicherer Verschlüsselungen unter den aktuell global genutzten Algorithmen in Bezug auf die 2018 veröffentlichte *Quantum Algebraic Attack* von Chen-Gao.
- Definition von Anforderungen für die Entwicklung neuer Quantensicherer Verschlüsselungs-Algorithmen mit Resistenz gegen die *Quantum Algebraic Attack* von Chen-Gao.

Bemerkung

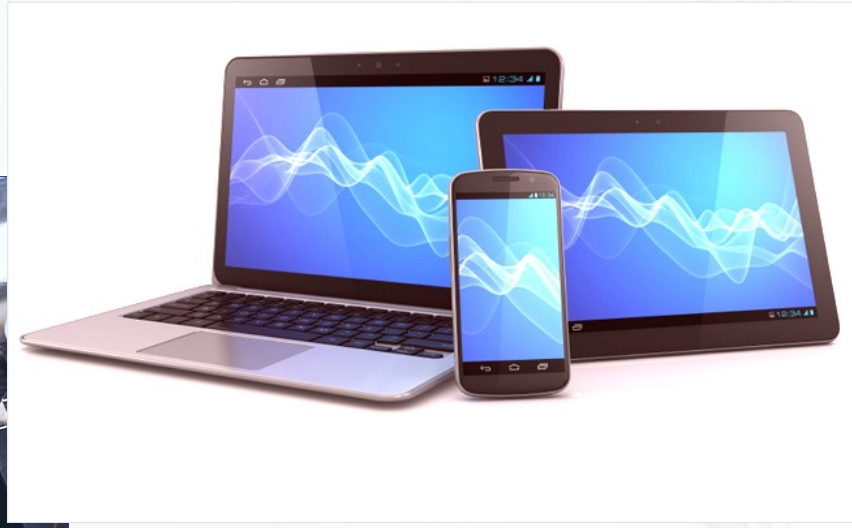
Die *Quantum Algebraic Attack* ist nicht im Scope des NIST Post-Quanten Standardisierungs-Prozesses Seit 2017! (nur für asymmetrische Systeme)

Wir untersuchen die Sicherheitsniveaus von Symmetrishen Kryptosystemen!

Scope unserer Mission

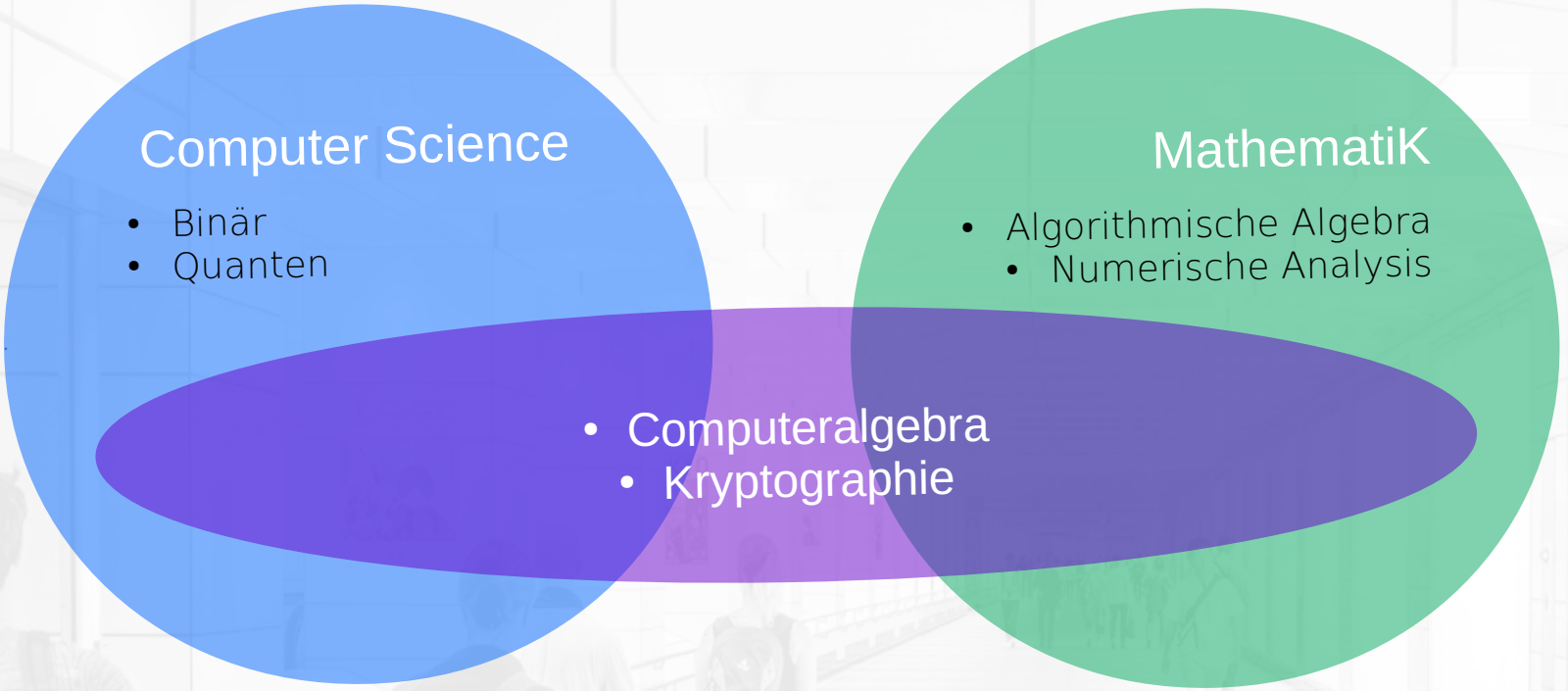
Post-Quanten Sicherheit für binäres und Quantum Computing

- Unsere Betrachtungen beruhen auf **binären und Quantum Computing Aspekten**!
- Deswegen werden unsere Ergebnisse für die Entwicklung von **Quantensicheren binären und Quanten Algorithmen** anwendbar sein.



Komplexität des Themas

Wissenschaftlicher und Technologischer Kontext



Fördern Sie unsere laufende Forschung

Grundlagenforschung als industriell-wissenschaftliches Open Source Projekt

Zwischenergebnisse werden auf Github veröffentlicht, wozu wir jeweils zum Review oder zur Mitarbeit einladen:

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

Paper mit Zwischenergebnissen:
https://github.com/XeniaGabriela/QAA_Condition_Nr/blob/master/official_paper/QAA_on_AES_paper.pdf

Betrachtungen für die aktuellen Untersuchungen:
https://github.com/XeniaGabriela/QAA_Condition_Nr/blob/master/results_nonnenmann_rump/The%20case%20of%20nonzero%20s%20.pdf

Prototype: Sicherheitsniveau von AES

1) Berechnung des Wertes der Konditionszahl κ in der Komplexität der *Quantum Algebraic Attack* von Chen-Gao auf 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) Berechnung des Wertes der Konditionszahlen von weiteren Kryptosystemen im Chen-Gao Paper (Trivium, Keccak, MPKC)

3) Identifikation und Analyse weiterer betroffener Kryptosysteme (Systeme, welche auf ein *Boolean Multivariate Quadratic Equation System (BMQ)* reduziert werden können).

Schritte für Kryptosysteme im Chen-Gao Paper

1) Berechnung der Konditionszahl der Macaulay Matrix der S-Box für AES

a) Für die klassische Definition der Konditionszahl κ einer Matrix gilt:

Singulärwerte = 0 werden mit betrachtet und somit ist κ(AES) = infinity
(siehe "QAA_on_AES_paper.pdf" auf Github)

Kooperation mit Prof. Dr. S. Rump, Institute for reliable computing, TU Hamburg

Done

b) Für die modifizierte Definition einer Konditionszahl κ einer Matrix gilt:

Singulärwerte = 0 werden mit ausgeschloßen und somit muss κ(AES) explizit berechnent werden.
(siehe "the case of nonzero s.pdf" auf Github)

Kooperation mit Mathworks

Ongoing

2) Mit den entwickelten Methoden von Schritt 1b), können die Konditionszahlen von Trivium, Keccak und MPKC berecnet werden.

Polynome der BMQ wurden schon von Chen-Gao identifiziert!

Kooperation mit Mathworks

Open

Kern 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

GI DMV

Feedback and Collaborators

Fachgruppe Computeralgebra

Im August 2020 ist ein Meeting mit anderen Mitgliedern der Computeralgebra Fachgruppenleitung geplant,um weitere Kooperationsmöglichkeiten zu eruieren.