Bundesamt
für Sicherheit in der
Informationstechnik

Digitale Souveränität trotz Quantencomputer

Dr. Manfred Lochter, BSI

Themen

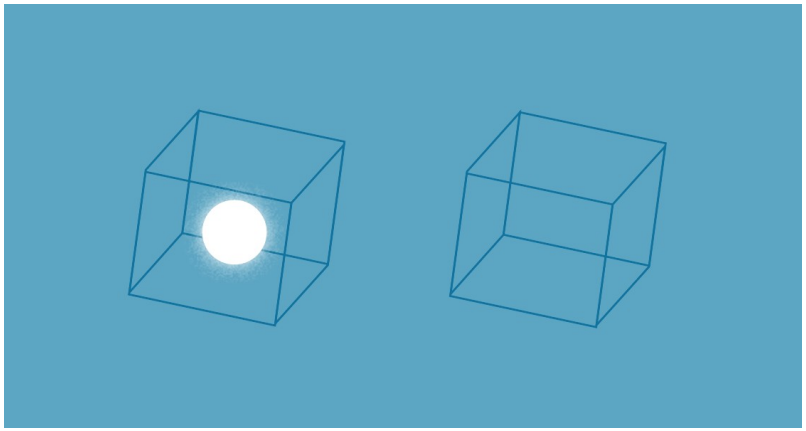
Kryptografische Auswirkungen von Quantencomputern
Kryptoagilität, „hybride“ Lösungen
Der NIST-Prozess
Aktivitäten des BSI
QKD und Zufall

TR-02102-1

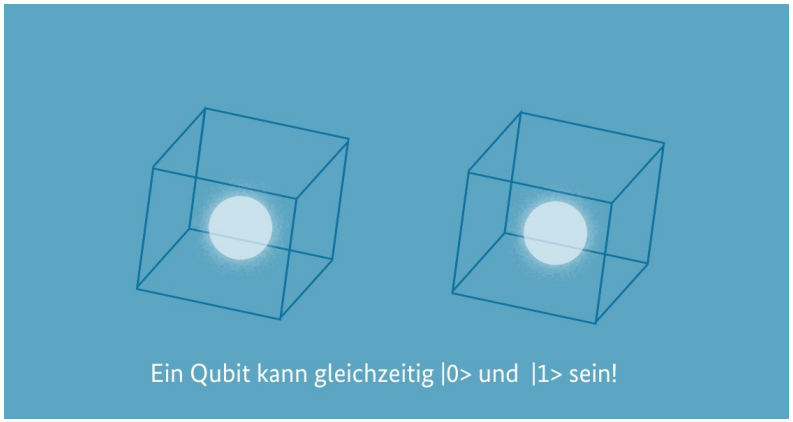
"Aus Sicht des BSI steht bei der Auswahl von neuen Verfahren Sicherheit an erster Stelle. Zur Schlüsseleinigung sind die im NIST-Prozess vorgeschlagenen Verfahren **FrodoKEM und Classic McEliece** die konservativste Wahl.
Mit Hinblick auf die Dauer des NIST-Prozesses hat sich das BSI entschieden, nicht auf die Entscheidung von NIST zu warten.
Wir beabsichtigen vielmehr, in der neuen Version unserer Technischen Richtlinie TR-02102-1 zu Algorithmen und Schlüssellängen die beiden genannten Verfahren als grundsätzlich geeignet (in hybriden Lösungen) zu empfehlen.
Diese Empfehlung wird gegebenenfalls angepasst, wenn die Entwicklung im NIST-Prozess weiter fortgeschritten ist."
(Arne Schönbohm, 16.12.2019, Tagesspiegel Background)

Quantencomputer und Quantentechnologien

Herkömmliche Computer rechnen auf Bits



Quantencomputer rechnen auf verschränkten (logischen) Qubits



→Potentielle Quantencomputer können parallel auf 2^n Zuständen operieren!

Verbreitung von Kryptografie

Früher

Meist Regierungs-anwendungen

Heute

TLS, Reisedokumente Gesundheitskarte, Bankwesen, elektronische Identitäten, ...
Oft mit Smartcards als Sicherheitsanker.

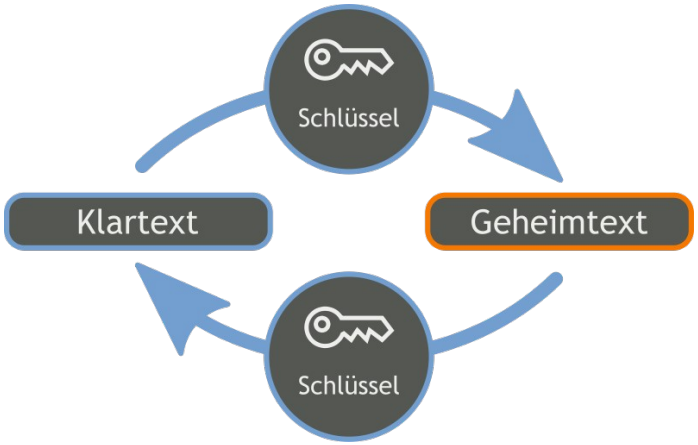
Zukünftig

Ubiquitär, zunehmende Vernetzung, möglichst kostengünstige Produkte, lange Lebensdauer und erforderliche Rückwärtskompatibilität (IoT, Industrie 4.0, C2C, Blockchain,...)

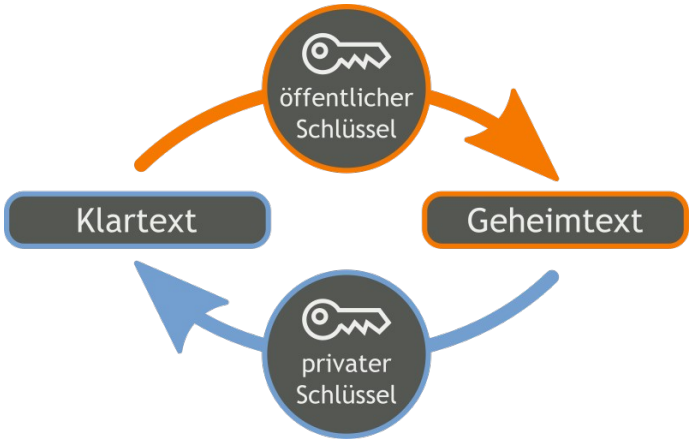
State-of-the-Art-Kryptografie

Kombination aus symmetrischer und asymmetrischer Kryptografie.

Symmetrisch:
Verfahren wie AES-128/256 zur Verschlüsselung oder zum Hashen (SHA-256/384).



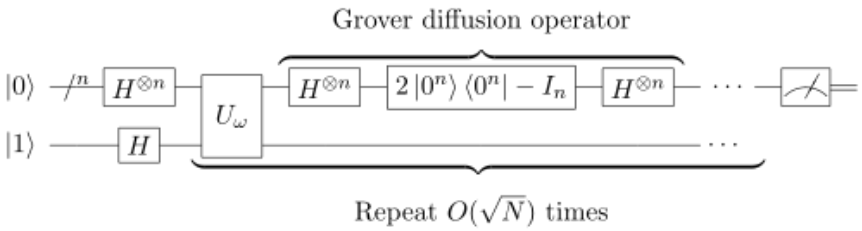
Asymmetrisch:
Schlüsseleinigung und Authentisierung mit digitalen Signaturen auf Basis des RSA-Verfahrens oder von elliptischen Kurven.

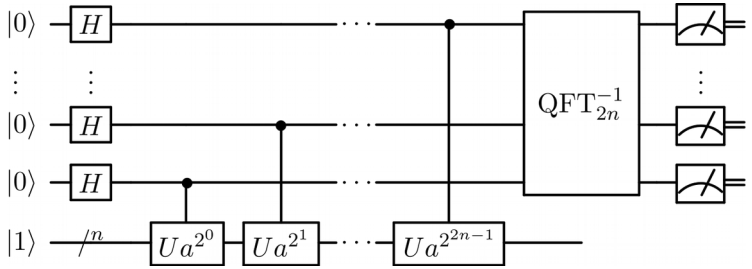


Kryptografische Auswirkungen von Quantencomputern

Grover,1996:
Die Schlüssellänge symmetrischer Verfahren würde sich grob halbieren.

Shor,1994:
Quantencomputer würden die heute verwendeten Public-Key-Verfahren (RSA, ECC,…) brechen.





Bundesamt für Sicherheit in der Informationstechnik

Kryptografische Auswirkungen von Quantencomputern

Auswirkungen von Quantencomputern treten zu unterschiedlichen Zeitpunkten ein.

- Schlüsseleinigung: Speichern und später entschlüsseln!
- Signatur: Kurzfristige Authentisierung oder langfristige Gültigkeit?

Selbst ohne Quantencomputer ist die Sicherheit der verwendeten Algorithmen nicht garantiert!

- Alternativen sind notwendig.
- Diese sollten flexibel und sicher austauschbar sein.

Auslöser?

NSA: CNSS-Advisory (2015)

Chinas Quantensatellit Micius startete am 16. August 2016. (AFP)

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

National strategy for quantum technologies

A NEW ERA FOR THE UK

UK: National Strategy for Quantum Technologies (2015)

Bundesamt für Sicherheit in der Informationstechnik

Politische Auswirkungen

Konkrete Aufträge für das BSI

- Wechsel zu quantensicherer Kryptografie
- Zufall
- QKD
- NIST Prozess
- Prüfkriterien
- ...

Bundesamt
für Sicherh
Informatior

Wann kommen Quantencomputer?

"Mit 1/5 Wahrscheinlichkeit wird es in 10 Jahren einen Quantencomputer geben, der RSA-2048 innerhalb eines Tages bricht."
(Michele Mosca, November 2019)

Wann?

With “concerted program” we mean that an industrialized nation pools a lot of its research and development effort into such a project, comparable with the Apollo and Manhattan programs in the US. Assuming that the current technical challenges are met - somewhat better operations, sparse use of voluminous periphery, larger chip areas, interchip connects and upgrades to cryogenic technology—it seems to be possible to have a computer with a Million planar transmons and a physical error rate of 1:10000. This would allow to attack 2048 Bit RSA in a few hundred hours.
(www.bsi.de/qcstudie)

Neue Version der BSI-Studie unter www.bsi.bund.de/qcstudie verfügbar

Wann?

Arbeitshypothese für den Hochsicherheitsbereich:

“Anfang der 2030er Jahre gibt es mit einer signifikanten Wahrscheinlichkeit einen kryptografisch relevanten Quantencomputer”

Konsequenzen

- Neubewertung und Weiterentwicklung von Produkten erforderlich
- Änderung von Zulassungsanforderungen
- Möglicherweise Beschränkung von Einsatzmöglichkeiten
- Berücksichtigung von Kryptoagilität bei Beschaffungszyklen
- Internationale Abstimmung erforderlich

Handlungsbedarf jetzt!

Risk management

- **Auch wenn es nie Quantencomputer geben wird**
- Langlebige Informationen
- Langlebige Systeme

Planung, Standardisierung, Produkte

- Sind PQ-Algorithmen auf den gegenwärtigen Platformen lauffähig?
- Kompatibilität mit Standardprotokollen?
- Märkte

„Enabling mechanisms“

- Hybride Schlüsseleinigung und Signatur sowie hashbasierte Signaturen
- Kryptografische Agilität

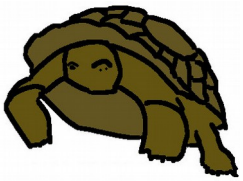
Post-Quantum-Kryptografie

= Algorithmen für die **heute** keine Angriffe mit Quantencomputern bekannt sind

- Abgrenzung zur Quantenkryptografie
- „Beweisbare Sicherheit“
- Schlüsseleinigung: Gitter (New Hope, Frodo), Codes, …
- BSI TR-02102
- Signaturen zur Authentisierung
- Hashbasierte Signaturen
- In gemanagten Systemen existieren weitere AdHoc-Lösungen.

Standardisierung

PQCRYPTO
ICT-645622



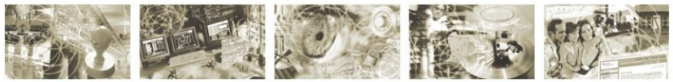
SAFE crypto

NIST

ETSI

IETF

Bundesamt
für Sicherheit in der
Informationstechnik



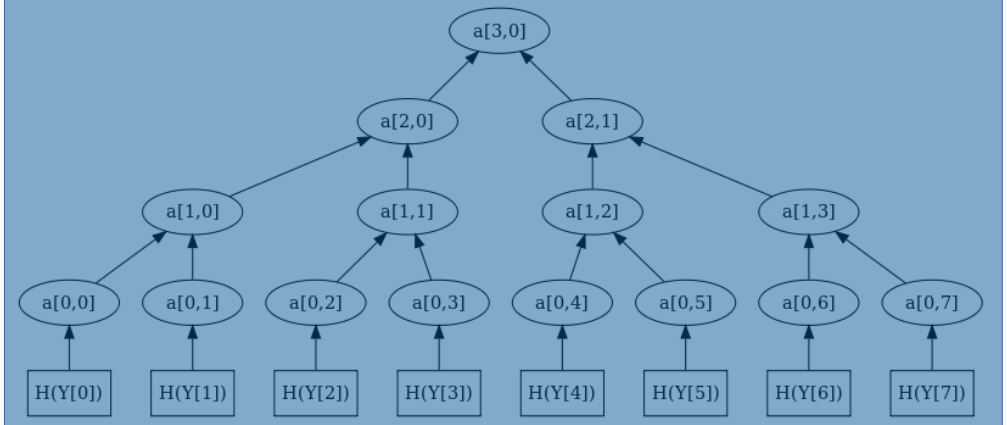
Technische Richtlinien des BSI

https://www.cacrnet.org.cn

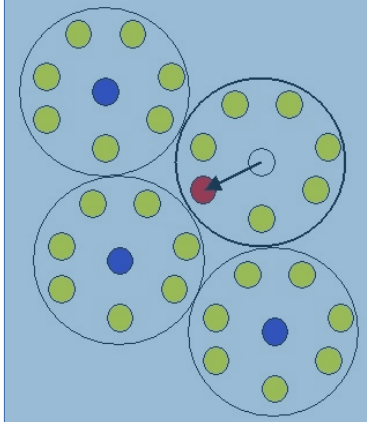
NIST-Standardisierung

"A long and winding road"

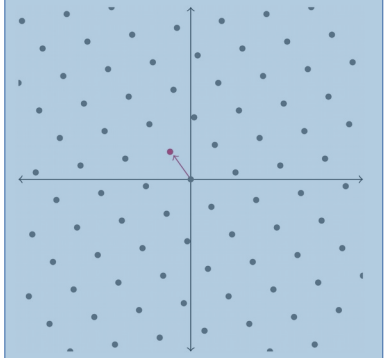
Kandidaten



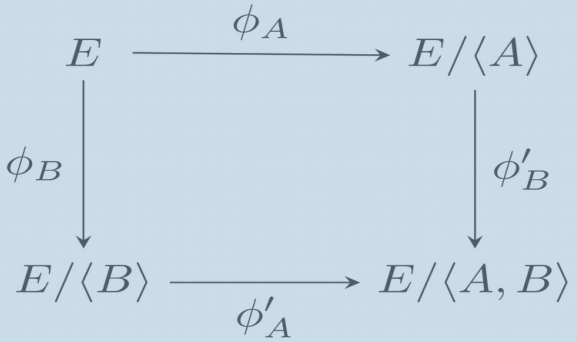
Hash-based



Code-based



Lattice-based



Isogeny-based

$$f_1(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{i\le n} b_i^{(1)} x_i + c^{(1)} = d_1$$

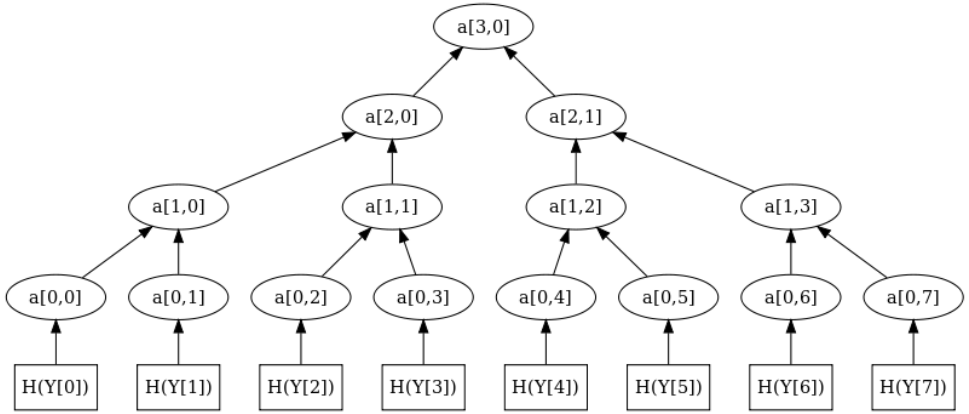
$$f_2(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(2)} x_i x_j + \sum_{i\le n} b_i^{(2)} x_i + c^{(2)} = d_2$$

$$\vdots$$

$$f_m(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{i\le n} b_i^{(m)} x_i + c^{(m)} = d_m$$

Multivariate

Hashbasierte Signaturen



- Hashbasierte Signaturen empfohlen (SatDSiG).
- Zustandsbehaftete Varianten (XMSS RFC 8391, LMS RFC 8553) sind standardisiert und werden wahrscheinlich durch NIST übernommen.
- Draft SP liegt zur Kommentierung vor. Hashbasierte Signaturen werden voraussichtlich 2021 in der TR-02102 detailliert empfohlen.

Hashbasierte Signaturen sind aus Sicht des BSI ein wesentlicher Baustein für Kryptoagilität!

Lösung: Quantenkryptografie?

Quantum Key Distribution (QKD): Schlüsseleinigung auf Basis quantenmechanischer Prinzipien

- QKD benötigt einen authentischen klassischen Kanal.
- Und Zufall
- „Unconditionally Secure“
- Sie bietet noch keine Ende-zu-Ende-Sicherheit.
- Weitere Untersuchungen und Prüfkriterien sind erforderlich.
- Das BSI hat die Erstellung eines Protection Profiles für QKD ausgeschrieben
- AIS 20/31
- Workshop mit Fraunhofer IOF Jena, Januar 2020
- QuNET, Q.Link.X

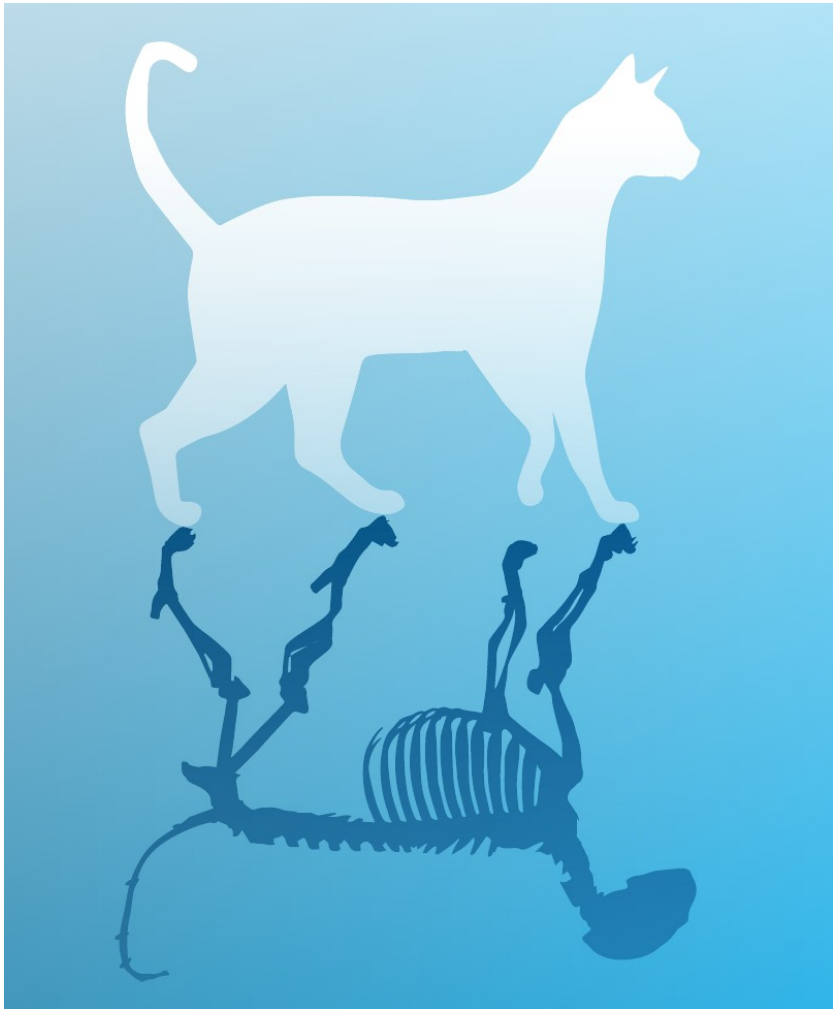
BMBF-Förderprogramm

“Das BMBF hat … eine "Richtlinie zur Förderungvon Forschungsvorhaben zum Thema 'Post-Quanten-Kryptografie'" veröffentlicht. Themenschwerpunkte für die Förderung sind "Quantencomputer-resistente Verfahren und ihre Sicherheitseigenschaften", "Effiziente, sichere Soft- und Hardware für quantencomputer-resistente Verfahren" sowie "Lösungen für eine einfache Migration zu quantencomputer-resistenten Verfahren". Das BSI begrüßt das Förderprogramm des BMBF…”

(Ausschuss Digitale Agenda, Stellungnahme des BSI)

Fazit

- Kryptografischer Umbruch wird (und muss) kommmen!
- Schon heute sind Gegenmaßnahmen möglich.
- Standards entwickeln sich.
- Agilität muss ein Designkriterium sein.
- Mit unerwarteten Seiteneffekten ist zu rechnen.

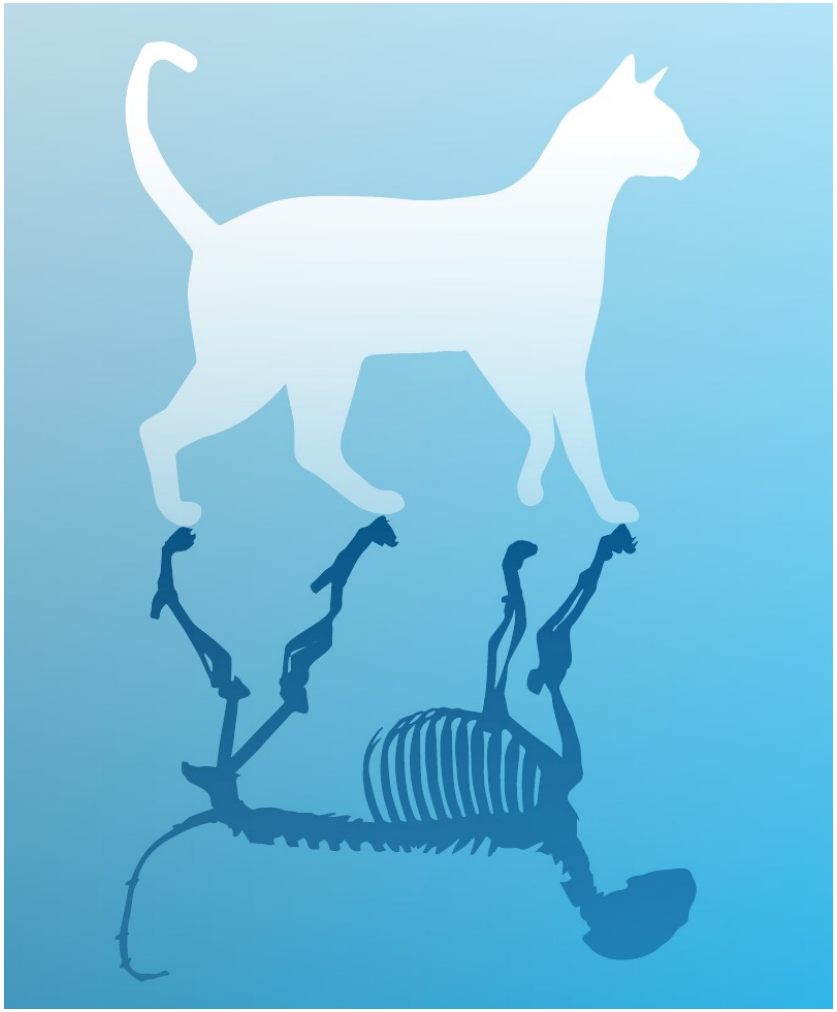


Conclusion

Don‘t panic!
(Corporal Jones)

If everything's under control,
you're going too slow.

(attributed to Mario Andretti)



Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Dr. Manfred Lochter

Manfred.lochter@bsi.bund.de
Tel. +49 (0) 228 95825643

BSI
Referat KM 21
Postfach 200363
53133 Bonn
www.bsi.bund.de

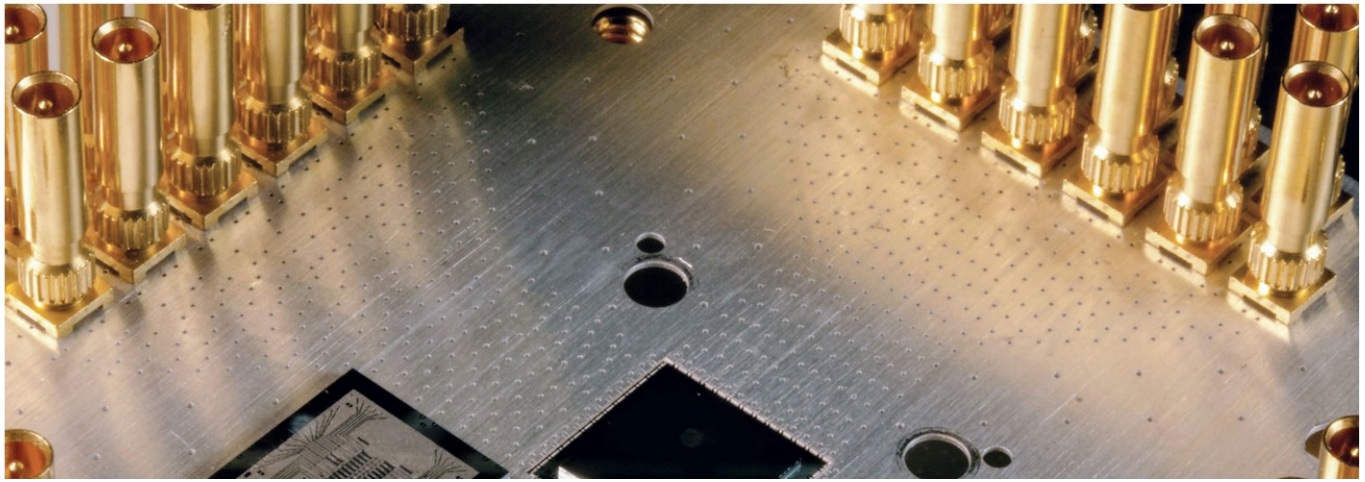
Bundesamt
für Sicherheit in der
Informationstechnik

Neven‘s Law?

ABSTRACTIONS BLOG

A New Law to Describe Quantum Computing’s Rise?

Neven’s law states that quantum computers are improving at a “doubly exponential” rate. If it holds, quantum supremacy is around the corner.



Wirtschaftliche Auswirkungen

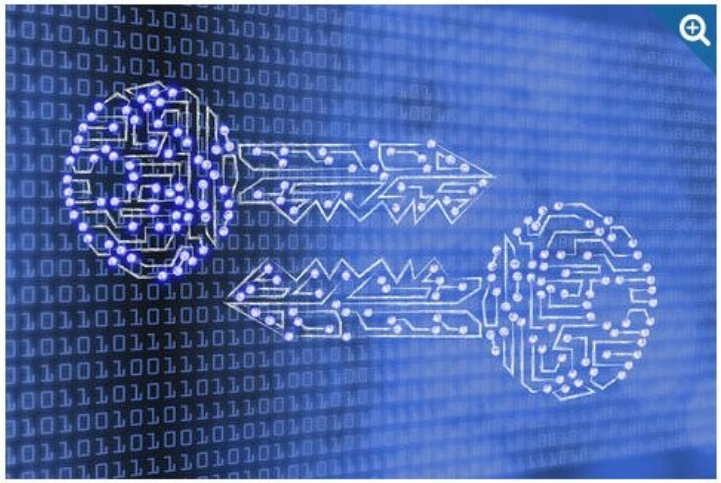
NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study

An international competition led to the voluntary standard that today protects millions of IT systems.

September 19, 2018

GAITHERSBURG, Md.—The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has released a study that estimates a $250 billion economic impact from the development of its Advanced Encryption Standard (AES) over the past 20 years.

AES is a cryptographic algorithm used to encrypt and



MEDIA CONTACT

Jennifer Huergo
jennifer.huergo@nist.gov
(301) 975-6343

ORGANIZATIONS

Information Technology Laboratory

Innovation & Industry Services