ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

KRYPTO-AGILITÄT

Michael Kreutzer, Michael Waidner, Leonie Wolf
ATHENE | TU Darmstadt | Fraunhofer SIT
7. Februar 2024

MOTIVATION FÜR KRYPTO-AGILITÄT

- Innovation in der Kryptografie
- Nationale Standards
- Sicherheit von kryptografischen Verfahren erodiert (Bedrohungen)

INNOVATION IN DER KRYPTOGRAFIE
Z. B. ERWEITERTE SCHUTZMÖGLICHKEITEN

Forward Secrecy:
Trotz Kompromittierung des Langzeitschlüssels ist vergangene (möglicherweise aufgezeichnete) Kommunikation sicher.

- In TLS 1.2 teilweise integriert
- In TLS 1.3 durch Sessionkeys integriert

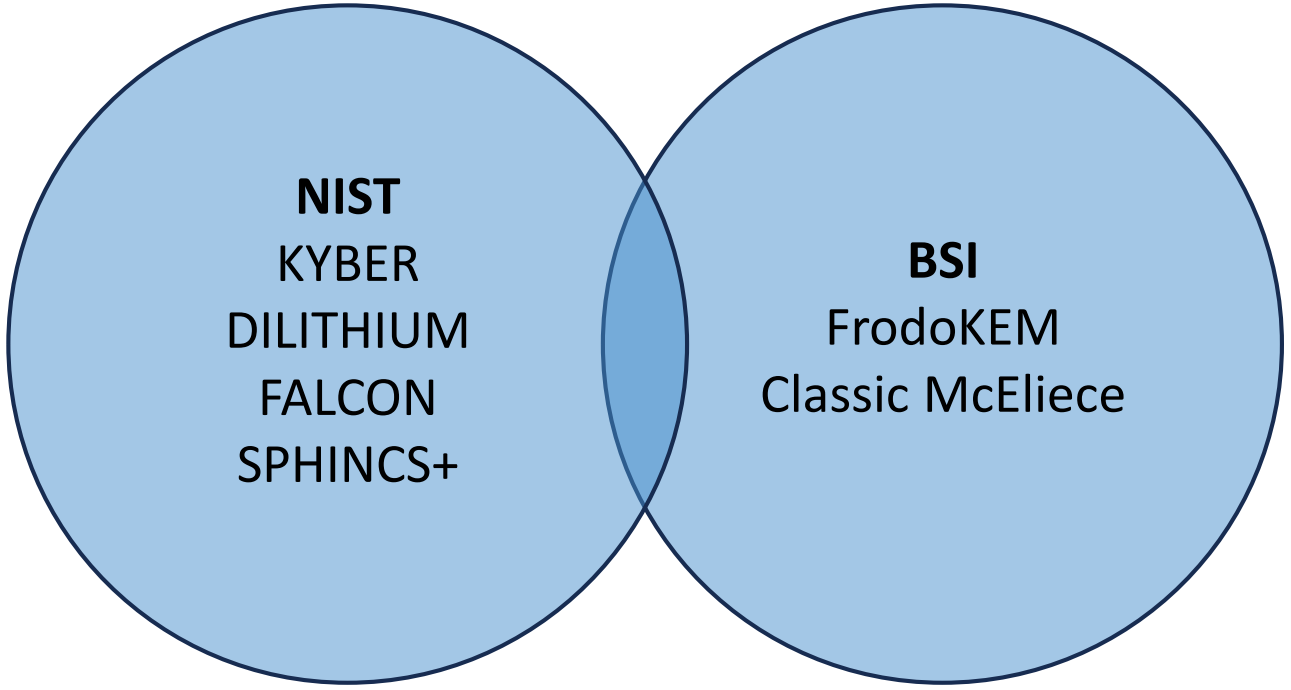
Tabelle: https://en.wikipedia.org/wiki/Transport_Layer_Security

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
RSA	Yes	Yes	Yes	Yes	Yes	No
DH-RSA	No	Yes	Yes	Yes	Yes	No
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes
ECDH-RSA	No	No	Yes	Yes	Yes	No
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
DH-DSS	No	Yes	Yes	Yes	Yes	No
DHE-DSS (forward secrecy)	No	Yes	Yes	Yes	Yes	No
DHE-ECDSA (forward secrecy)	No	No	No	No	No	Yes
ECDH-ECDSA	No	No	Yes	Yes	Yes	No
ECDHE-ECDSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
DHE-EdDSA (forward secrecy)	No	No	No	No	No	Yes
ECDH-EdDSA	No	No	Yes	Yes	Yes	No
ECDHE-EdDSA (forward secrecy)[74]	No	No	Yes	Yes	Yes	Yes
PSK	No	No	Yes	Yes	Yes	Yes
PSK-RSA	No	No	Yes	Yes	Yes	No
DHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes
ECDHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes
SRP	No	No	Yes	Yes	Yes	No
SRP-DSS	No	No	Yes	Yes	Yes	No
SRP-RSA	No	No	Yes	Yes	Yes	No
Kerberos	No	No	Yes	Yes	Yes	?
DH-ANON (insecure)	No	Yes	Yes	Yes	Yes	No
ECDH-ANON (insecure)	No	No	Yes	Yes	Yes	No
GOST R 34.10-2012	No	No	No	No	Yes	Yes

NATIONALE STANDARDS

Z. B. inkompatible Standards in Post-Quanten Kryptografie

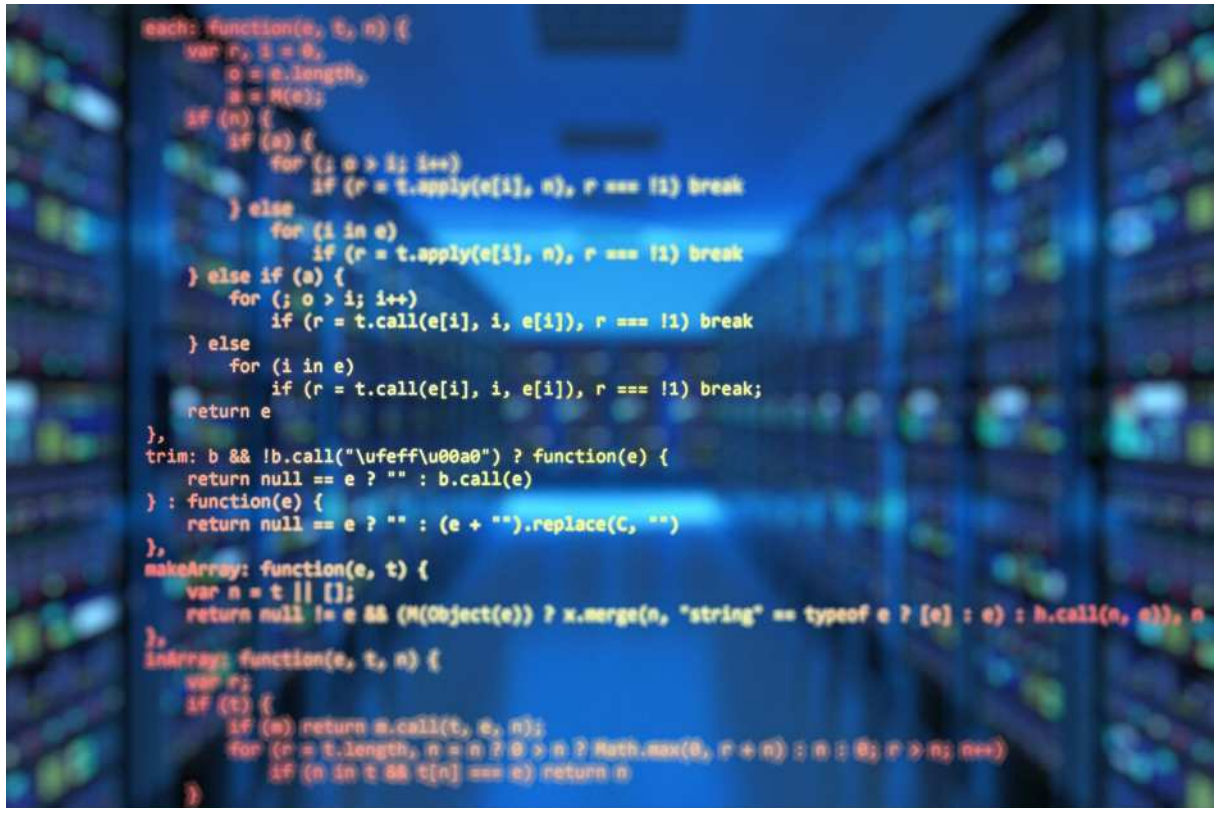
- NIST PQC: CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALON, SPHINCS+
- BSI bisher empfohlen: FrodoKEM, Classic McElliece



KRYPTOGRAFIE ERODIERT

4 Bedrohungskategorien:

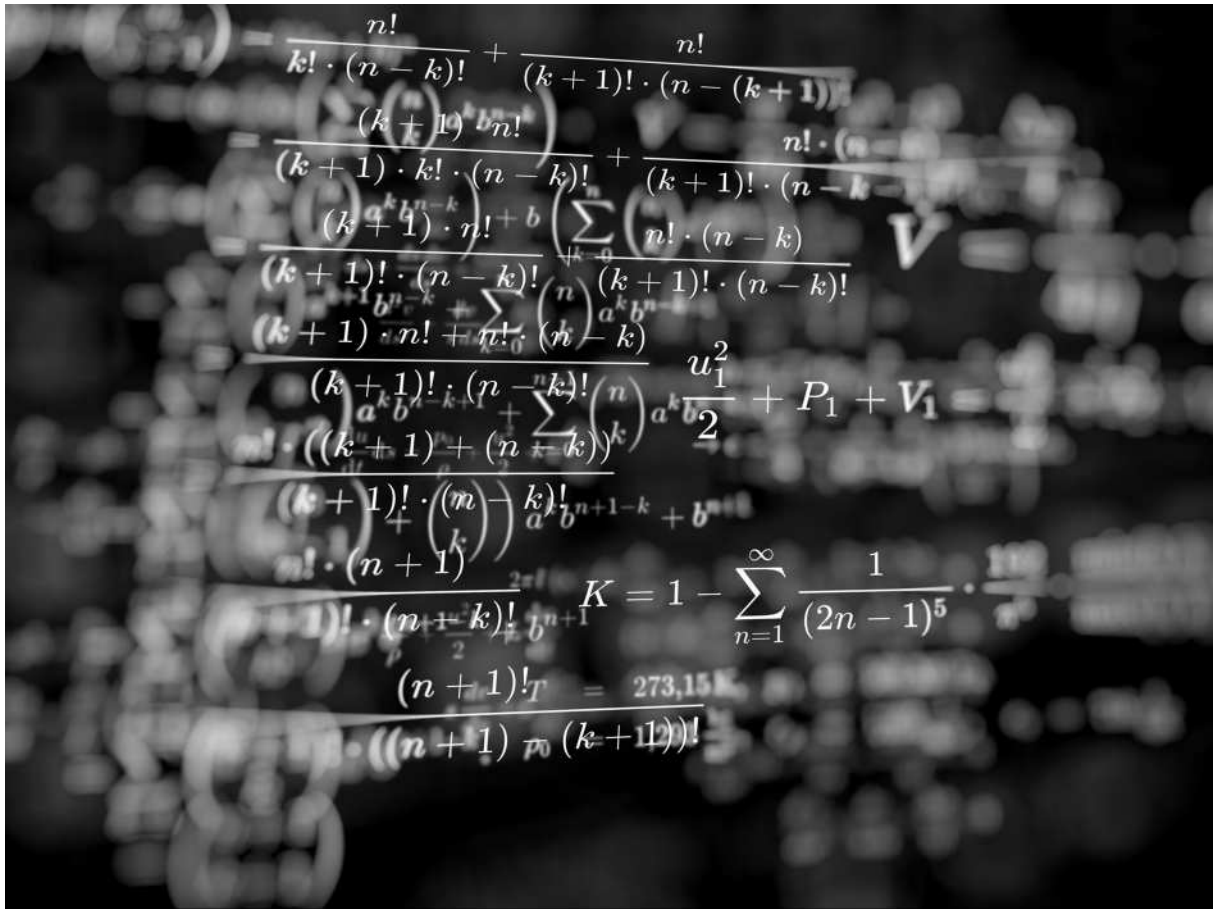
- Implementierungsfehler
  → PS3: Zufallszahl = feste Zahl



KRYPTOGRAFIE ERODIERT

4 Bedrohungskategorien:

- Implementierungsfehler
- Mathematische Fortschritte
  → SIKE

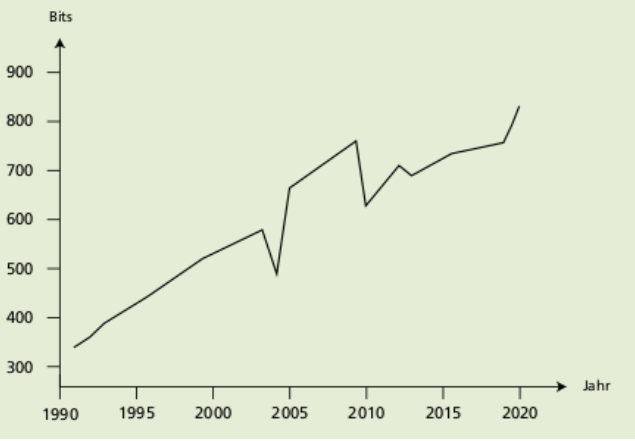


KRYPTOGRAFIE ERODIERT

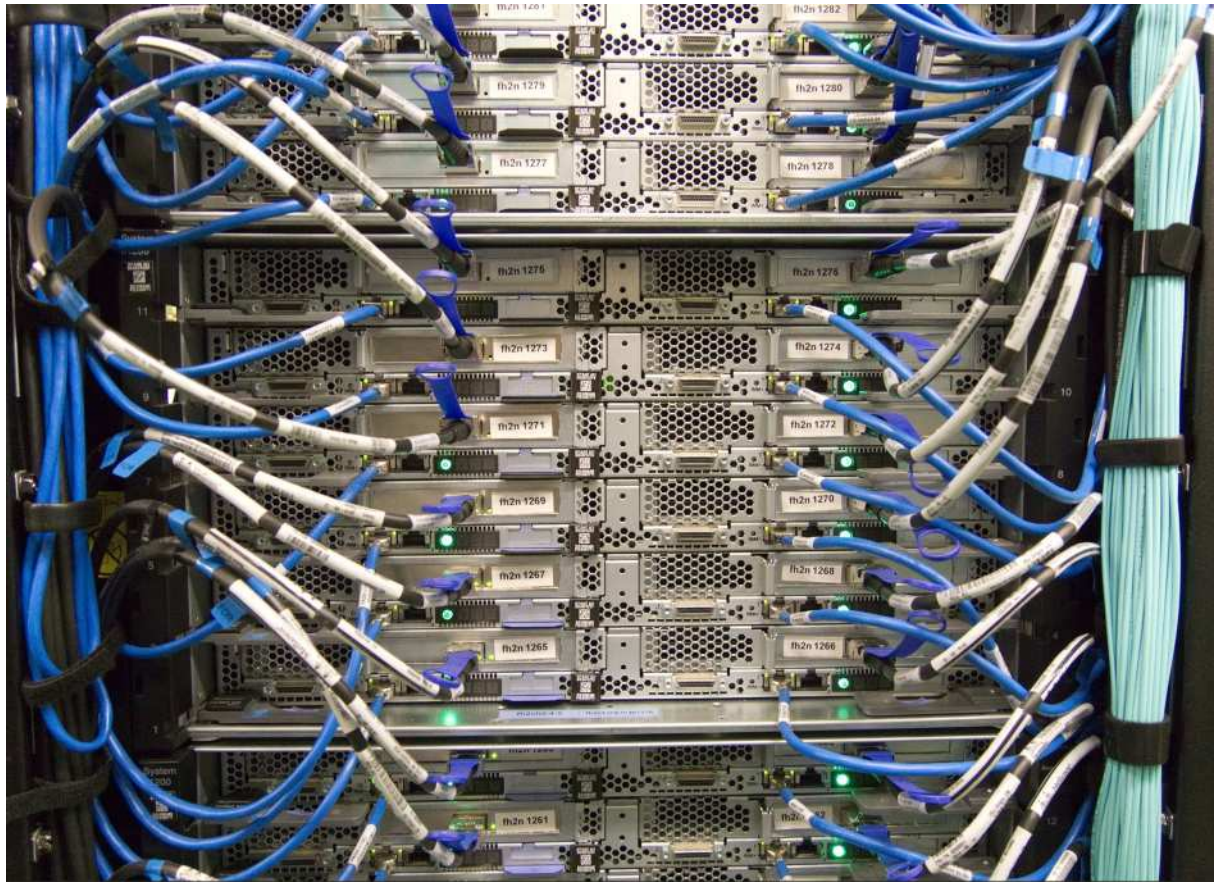
4 Bedrohungskategorien:

- Implementierungsfehler
- Mathematische Fortschritte
- Steigerung der Rechenleistung

→ RSA-Challenge



Nach Zahlen von:
https://en.wikipedia.org/wiki/RSA_Factoring_Challenge



KRYPTOGRAFIE ERODIERT

4 Bedrohungskategorien:

- Implementierungsfehler
- Mathematische Fortschritte
- Steigerung der Rechenleistung
- Quantencomputer

WAS IST KRYPTO-AGILITÄT?

Bundesamt
für Sicherheit in der
Informationstechnik

6.2 Kryptoagilität

Bei der Neu- und Weiterentwicklung von Anwendungen sollte vor allem darauf geachtet werden, die kryptografischen Mechanismen möglichst flexibel zu gestalten, um auf Entwicklungen reagieren, kommende Empfehlungen und Standards umsetzen und möglicherweise in Zukunft Algorithmen, die nicht mehr das gewünschte Sicherheitsniveau garantieren, austauschen zu können („Kryptoagilität"). Dies gilt insbesondere aufgrund der Bedrohung durch Quanten-

→ Einfach?
→ Schnell?

→ Kryptografische Algorithmen sollen einfach und schnell ausgetauscht werden können.

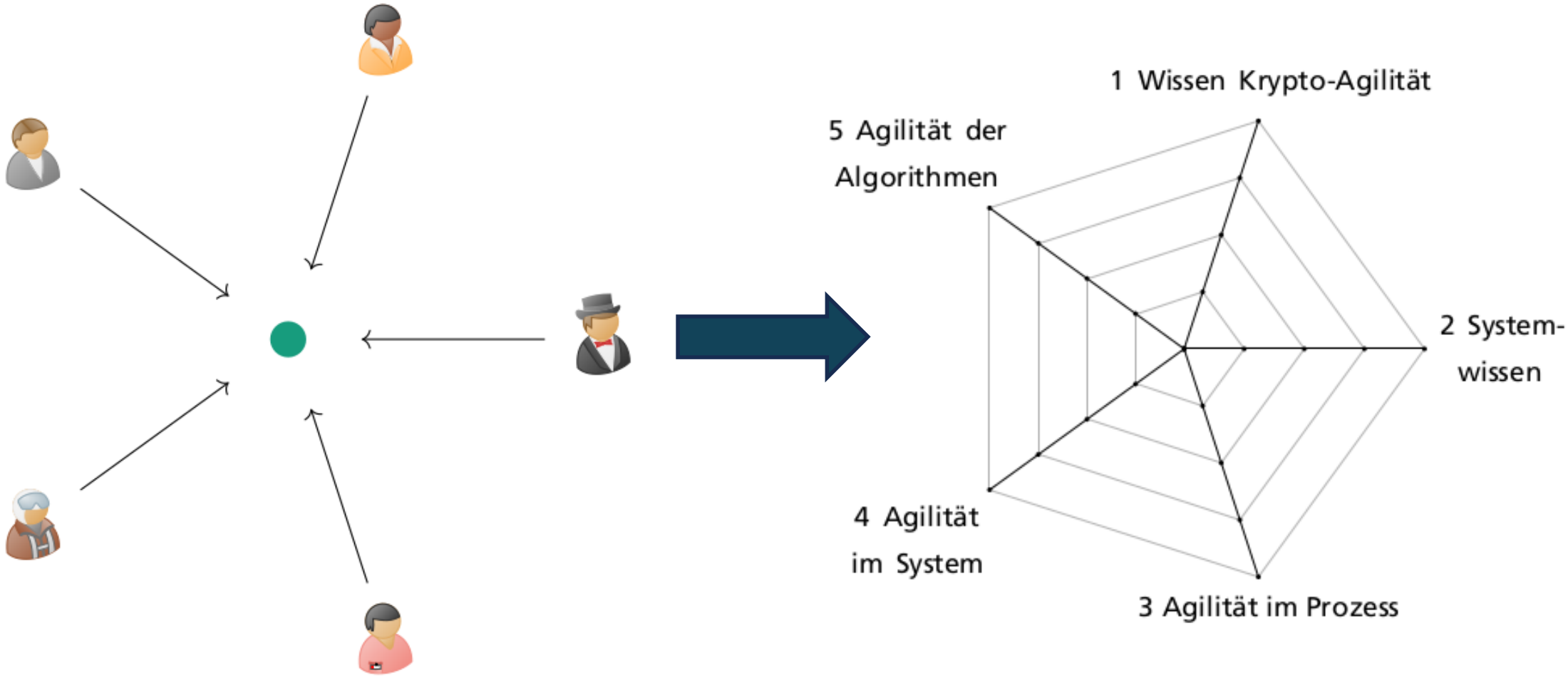
NIST

Impact of Quantum Computing Technology on Classical Cryptography

From time to time, the discovery of a cryptographic weakness, constraints imposed by dependent technologies, or advances in the technologies that support cryptanalysis make it necessary to replace a legacy cryptographic algorithm. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Many information systems lack *crypto agility*—that is, they are not designed to encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure. As a result, an organization may not possess complete control over its cryptographic mechanisms and processes so that it can make accurate alterations to them without involving intense manual effort.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

WAS IST KRYPTO-AGILITÄT?



https://www.sit.fraunhofer.de/fileadmin/folien/casc-presentation.pdf?_=1665582038

Hohm, Julian, Andreas Heinemann, and Alexander Wiesmaier. "Towards a maturity model for crypto-agility assessment." *International Symposium on Foundations and Practice of Security*. Cham: Springer Nature Switzerland, 2022.

WAS IST KRYPTO-AGILITÄT?

Technische Perspektiven:

- Agilität der Algorithmen
  - Austausch von Algorithmen, Modularer Aufbau, Schnittstellen
  - Mehrere kryptografische Algorithmen zur Auswahl (mit Aushandlungsprozess)
  - Einheitliche Schnittstellen für Kryptografie
- Agilität im System
  - Speicher-, Rechen-, Bandbreitenkapazitäten (auch für PQC)
  - Hard- und Software unabhängig
  - Rückwärtskompatibilität
- Prozess?

WAS IST KRYPTO-AGILITÄT?

Governance Perspektiven:

- Prozess
  - Updatebarkeit (Testen, Ausnahmen für Devices mit kurzer Lebensdauer?)
  - Guidelines (Effektivität)
- Systemwissen
  - Nutzung von Kryptografie
  - Zugänge/Verantwortlichkeiten für Systeme
- Wissen Krypto-Agilität
  - Theoretisches/Praktisches Wissen
  - Konzept für Umsetzung von Krypto-Agilität (+ Migration zu PQC)

→ Ganze muss Lieferkette mitgedacht werden

BEISPIEL: PLUG & CHARGE KRYPTO-AGIL (1/2)

ISO 15118: Norm für Plug & Charge, nicht krypto-agil.

→ PQC-Erweiterung: QuantumCharge

Lebensdauer:

→ Ladesäulen: 10+ Jahre

→ E-Autos: bis zu 35 Jahre

Signierung & Verifikation auf Embedded Devices.

→ Wenig Speicherplatz für lange Schlüssel & Signaturen.

→ Prozessoren nicht optimiert auf z. B. Lattice-Operationen.

Kern, D., Krauß, C., Lauser, T., Alnahawi, N., Wiesmaier, A., & Niederhagen, R. (2023, May). QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging. In International Conference on Applied Cryptography and Network Security (pp. 85-111). Cham: Springer Nature Switzerland.

BEISPIEL: PLUG & CHARGE KRYPTO-AGIL (2/2)

	aktuell	Krypto-agil
Norm	ISO 15118	QuantumCharge
Algorithmen	ECDSA, EdDSA, ...	Generische Alg.-Schnittstelle für Kyber, FALCON, ...
Protokolle	TLS, basierend auf ECC	Generische Version von TLS
Speicher	Kleine Schlüssel und Signaturen (ECDSA: 32 Byte und 64 Byte).	Große Schlüssel und Signaturen (DILITHIUM: 2528 Byte und 2420 Byte).
Prozessoren	Optimiert für ECC	Optimiert z. B. für Lattice-Operationen

Kern, D., Krauß, C., Lauser, T., Alnahawi, N., Wiesmaier, A., & Niederhagen, R. (2023, May). QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging. In International Conference on Applied Cryptography and Network Security (pp. 85-111). Cham: Springer Nature Switzerland.

PQC-VERFAHREN: UNTERSCHIEDLICHE STÄRKEN

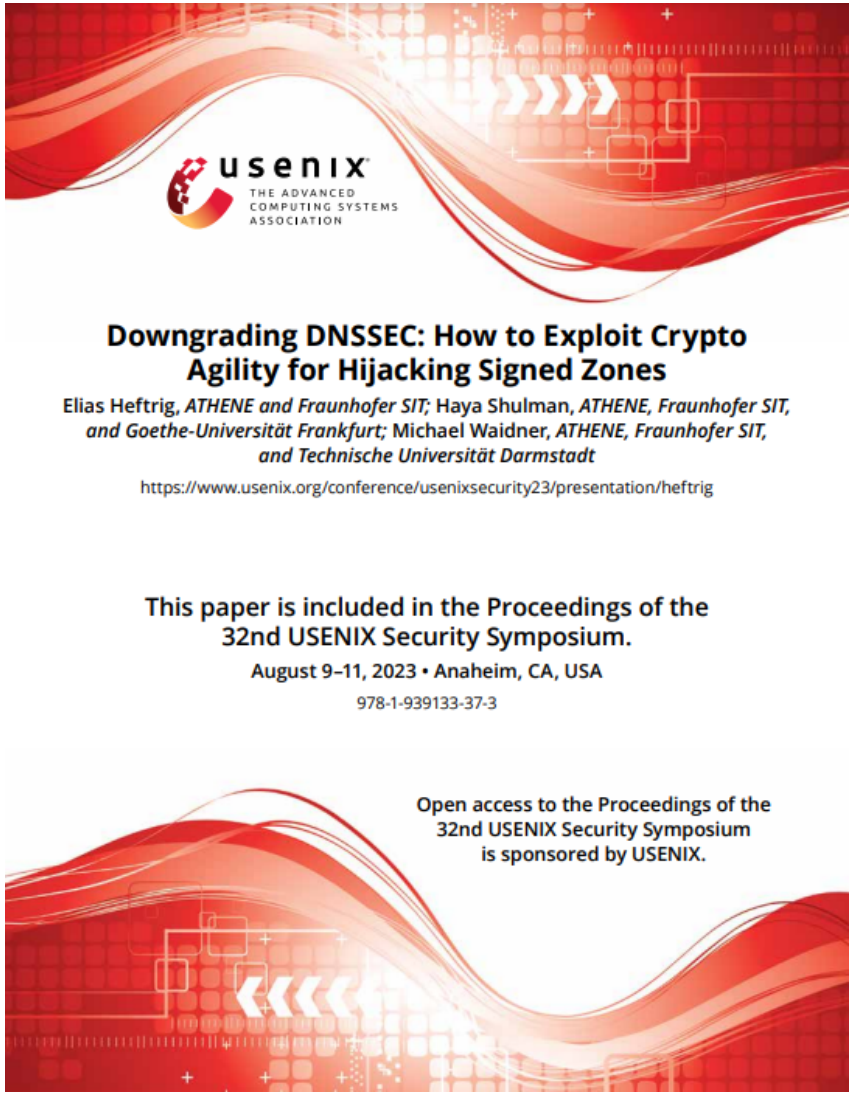
ECC UND RSA → FLEXIBEL EINSETZBAR, PQC → ZOO VON VERFAHREN

KEM	Codebasiert	Gitterbasiert
Schlüssel	--	+
Ciphertext	+	-
Performance	+	++
Beispiele	Classic McEliece	KYBER, FrodoKEM….

SIG	Gitterbasiert	Hashbasiert
Schlüssel	+	++
Signatur	+	--
Performance	-	--
Beispiele	DILITHIUM, FALCON…	SPHINCS+

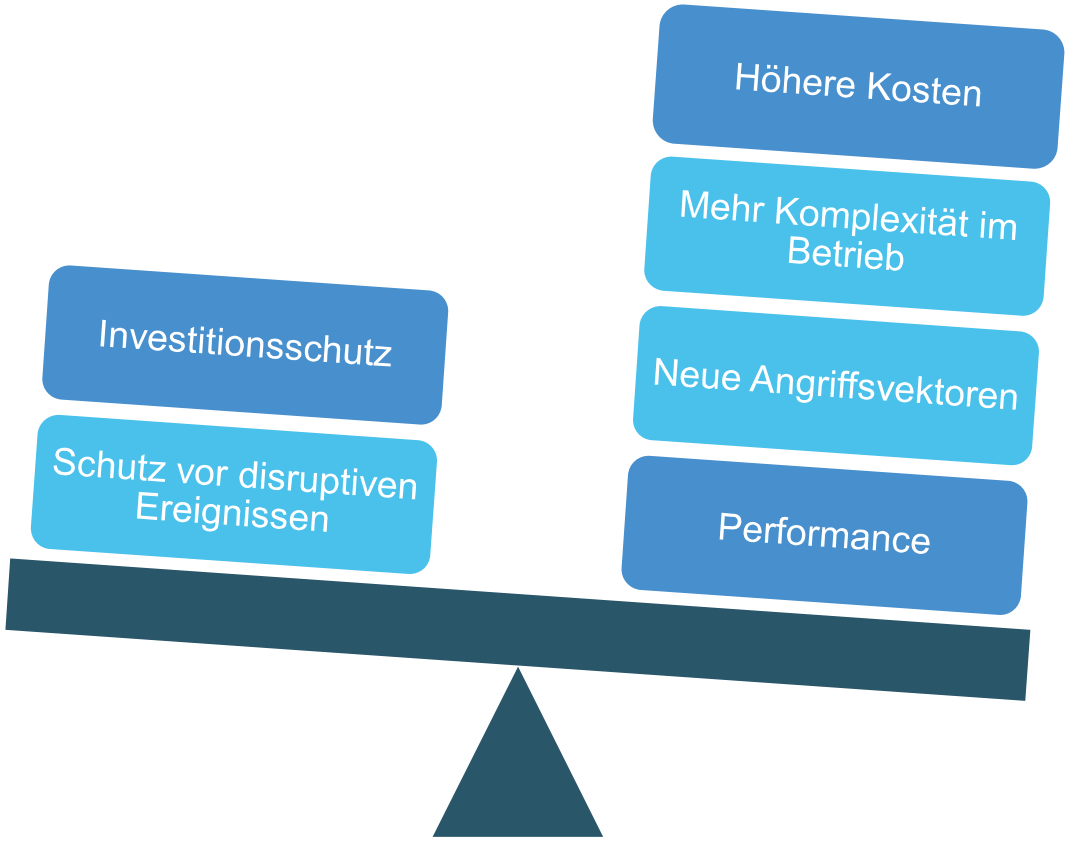
NEUE ANGRIFFSVEKTOREN

Fehlerhaft umgesetzte Krypto-Agilität



Heftrig, Elias, Haya Shulman, and Michael Waidner. "Downgrading DNSSEC:
How to Exploit Crypto Agility for Hijacking Signed Zones." *Proceedings of the 32nd USENIX Conference on Security Symposium*. 2023.

SCHLECHTES IMAGE VON KRYPTO-AGILITÄT?



תודה רבה!

Merci beaucoup!

çok teşekkürler

谢谢

Thank you very much!

Dank je wel!

Vielen Dank!

Muchas gracias

ありがとうございます

Dziękuję!

Grazie mille!

شكرا لك

zor spas