TeleTrusT-EBCA "PKI-Workshop" 2022

Berlin, 29.09.2022

Konzepte zur technischen Migration auf PQC-Verfahren

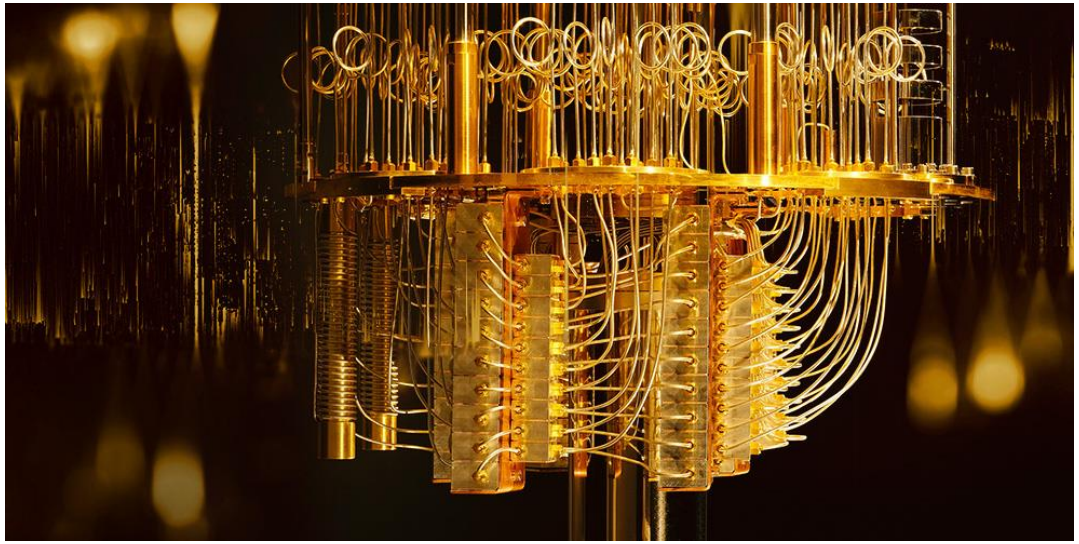
Dr. Christian Tobias, MTG
in Vertretung: Dr. Falko Strenzke, MTG

Agenda

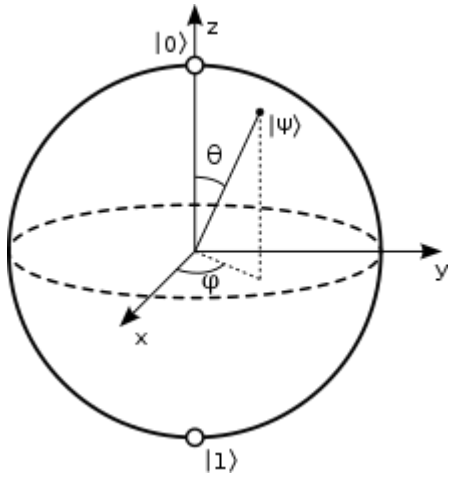
- Herausforderung Quantencomputer
- NIST PQC Competition
- Migration zu PQC
  - Plug and Play?
  - Schlüsselkapselung (KEM)
  - Multi-Algorithmus-Verfahren (aka hybrid)
- Diskussion und Fragen

Quantencomputer – Was ist das eigentlich?

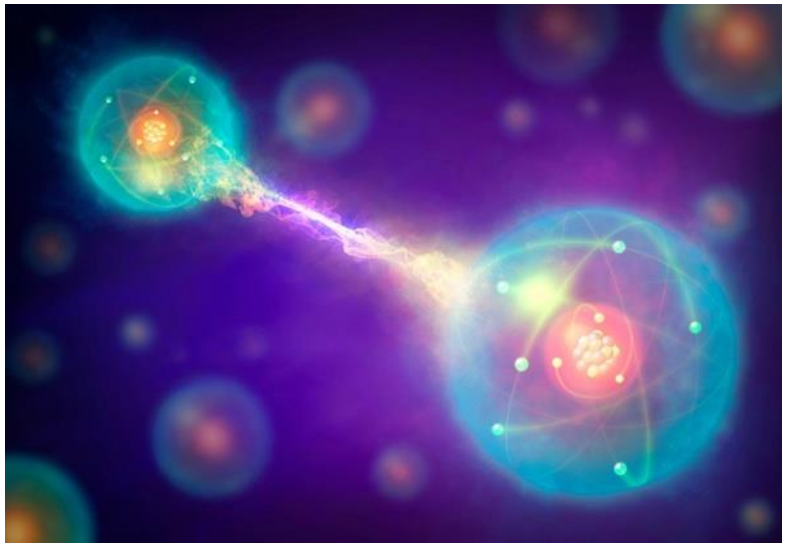
- Ein **Quantencomputer** ist ein Computer, der die Gesetze der Quantenmechanik nutzt.
- Im Unterschied zum klassischen Computer arbeitet er nicht auf der Basis elektrischer, sondern quantenmechanischer Zustände. Hierbei sind besonders das **Superpositionsprinzip** und die **Quantenverschränkung** von Bedeutung.
- Das ermöglicht für ausgewählte Probleme eine exponentielle Beschleunigung der Berechnungen ggü. den aktuellen Computern („klassische Computer“).



Quellehttps://www.ibm.com/blogs/think/de-de/2021/02/erste-forschungsprojekte-mit-dem-ibm-quantencomputer-in-ehningen-gestartet/:



Quellehttps://en.wikipedia.org/wiki/Bloch_sphere:

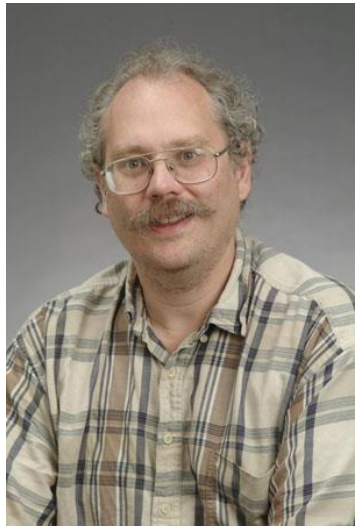


Quelle: http://www.astronomy.com/news/2018/08/distant-quasars-confirm-quantum-entanglement

Die Algorithmen von Shor und Grover

Shor`s Algorithmus

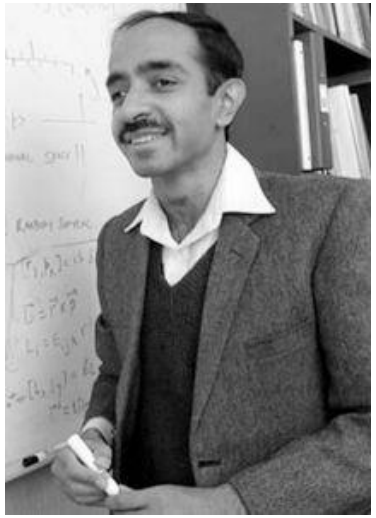
- Benannt nach dem Mathematiker Peter Shor
- Veröffentlicht 1994
- Löst folgende Probleme:
  - Faktorisierung großer Zahlen
  - Berechnung von diskreten Logarithmen
- Damit sind gebrochen:
  - RSA (Verschlüsselung und Signatur)
  - Diffie-Hellman (Schlüsselaustausch)
  - Digital Signature Algorithm (DSA)
  - Etc.



Quelle: https://klein.mit.edu/~shor

Grover‘s Algorithmus

- Benannt nach Lov Kumar Grover
- Veröffentlicht 1996
- Suchalgorithmus auf unstrukturierten Daten
- Die Parameter für symmetrische Algorithmen (Schlüssellänge) und Hashfunktionen (Größe des Hashwerts) müssen angepasst (etwa verdoppelt) werden



Quelle: https://medium.com/

Store Now, Decrypt Later (SDNL)

Utah Data Center

Quelle: https://nsa.gov1.info/utah-data-center/
Abgerufen am 14.04.2022

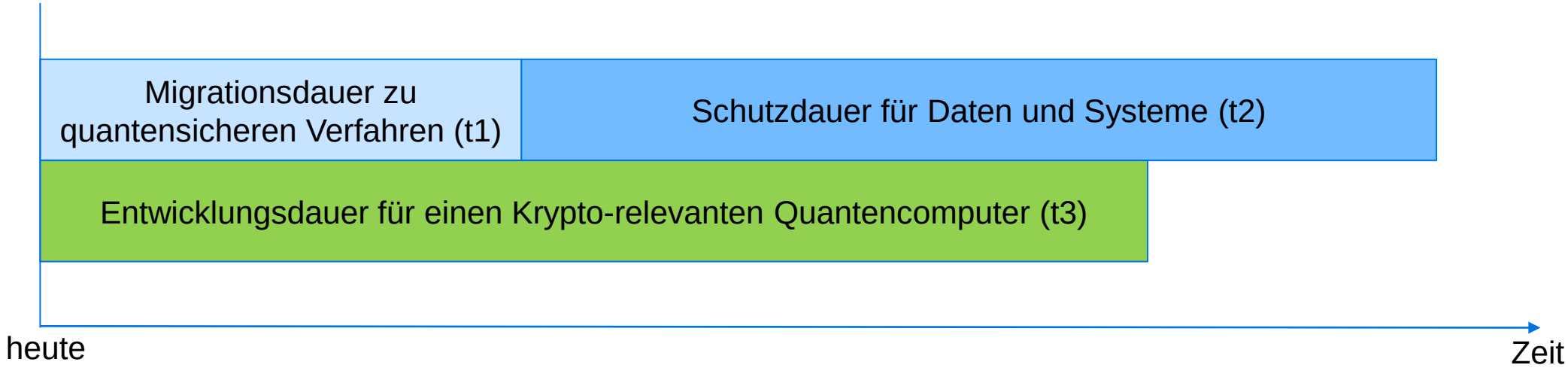
Our Ultimate Target: 256-bit AES

The Advanced Encryption Standard (AES) algorithm is used worldwide to encrypt electronic data on hard drives, email systems, and web browsers. Computer experts have estimated it would take longer than the age of the universe to break the code using a trial-and-error brute force attack with today's computing technology.

In 2004, the NSA launched a plan to use the Multiprogram Research Facility in Oak Ridge, Tennessee to build a classified supercomputer designed specifically for cryptanalysis targeting the AES algorithm. Our classified NSA Oak Ridge facility made a stunning breakthrough that is leading us on a path towards building the first exaflop machine (1 quintillion instructions per second) by 2018. Since the capability to break the AES-256 encryption key within an actionable time period may still be decades away, our Utah facility is sized to store all encrypted (and thereby suspicious) data for safekeeping.

Das Theorem von Mosca

- Daten und Systeme müssen über ihren ganzen Lebenszyklus geschützt bleiben.
- Für Daten bedeutet das, dass für die Verschlüsselung ein Verfahren verwendet werden muss, dass über die komplette Schutzdauer der Daten Vertraulichkeit garantiert.



Informationssicherheit ist nicht mehr gegeben, wenn t3 < t1 + t2

Wann kommt ein kryptografisch relevanter Quantencomputer?

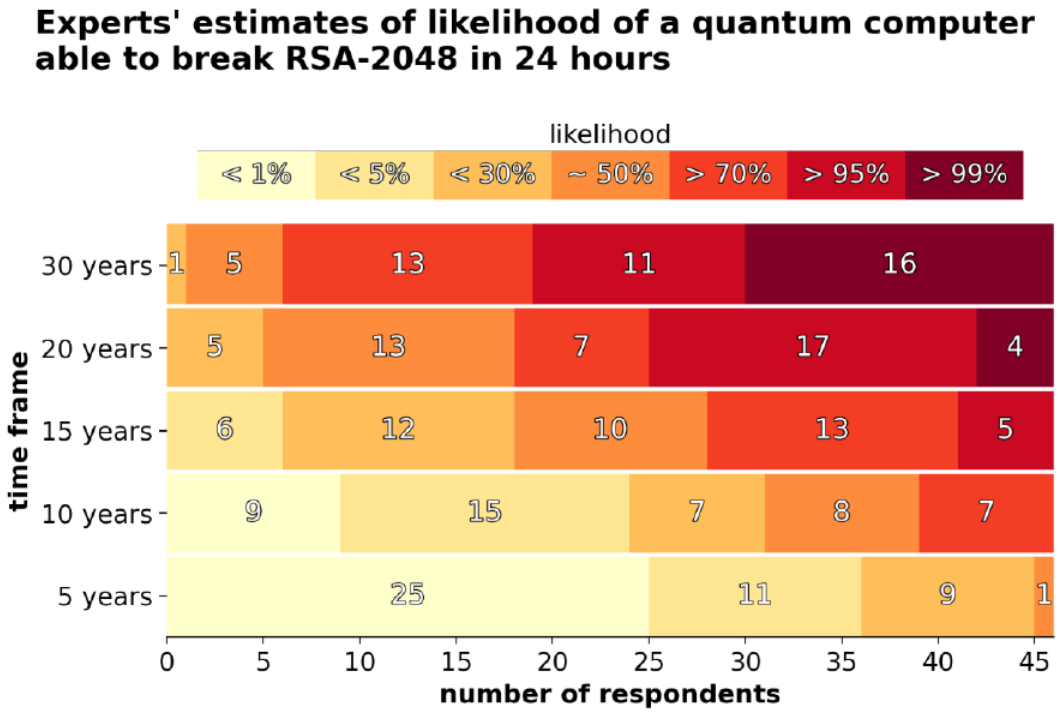


Figure 10 This figure illustrates the central information collected through our survey. The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specified sense of being able to break RSA-2048 in 24 hours—for various time frames, from a short term of 5 years all the way to 30 years.

Quelle: 2021 Quantum Threat Timeline Report, Global Risk Institute, January 2022
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

„Das BSI handelt dazu für den Hochsicherheitsbereich mit der Arbeitshypothese, dass kryptografisch relevante Quantencomputer Anfang der 2030er-Jahre zur Verfügung stehen.“

Quelle: Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen
Bundesamt für Sicherheit in der Informationstechnik (BSI), Oktober 2021

Wunderwaffe Quantencomputer?

- Quantencomputer können spezielle mathematische Probleme wesentlich effizienter lösen als klassische Computer, z.B.
  - Hidden Subgroup Problem: wird in Shor‘s Algorithmus verwendet
  - Suche in unsortierten Daten: wird in Grover‘s Algorithmus verwendet

- Können Quantencomputer alle mathematischen Probleme effizient lösen?
  - **Wahrscheinlich nicht!**

- Können die für Quantencomputer unzugänglichen Probleme zur Konstruktion von kryptografischen Verfahren verwendet werden?
  - **Ja!**
  - **Damit beschäftigt sich die Post-Quantum-Cryptography (PQC)**

NIST PQC Competition (NISTPQC)

- Im Jahr 2016 hat das NIST auf die Notwendigkeit für die Entwicklung quantensicherer Kryptografie hingewiesen und einen Wettbewerb für einen PQC-Standard gestartet:
  - Einreichungen möglich für
    - Digitale Signaturen
    - Verschlüsselung / Schlüsselkapselung (KEM)
  - 82 Einreichungen, davon 69 für die 1. Runde akzeptiert
  - Auswahlkriterien:
    - Sicherheit
    - Größe der Parameter
    - Geschwindigkeit
    - Schutzrechte
    - Etc.

Quelle: Vortrag von Dustin Moody, NIST, https://csrc.nist.gov/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa

NIST PQC Competition (NISTPQC): Erste Ergebnisse

Kategorie	Art	Standard nach Runde 3	Zu Runde 4 zugelassen
Gitter-basiert	KEM	Kyber	
	Digitale Sig.	Dilithium, Falcon	
Hash-basiert	KEM		
	Digitale Sig.	SPHINCS+	
Code-basiert	KEM		Classic McEliece, BIKE, HQC
	Digitale Sig.		
Isogenie-basiert	KEM		~~SIKE~~
	Digitale Sig.		
Multivariat	KEM		
	Digitale Sig.		

Für **National Security Systems (NSS)** durch die **NSA** zugelassene Algorithmen (09/2022):

- Kyber
- Dilithium
- LMS (RFC8554)
- XMSS (RFC8391)
- AES-256
- SHA-384 und SHA-512

Erweiterung Scope der NIST Competition:
Anfang September 2022 hat das NIST einen Aufruf gestartet, weitere Vorschläge für Signaturverfahren einzureichen.

Migration zu PQC: Plug and Play?

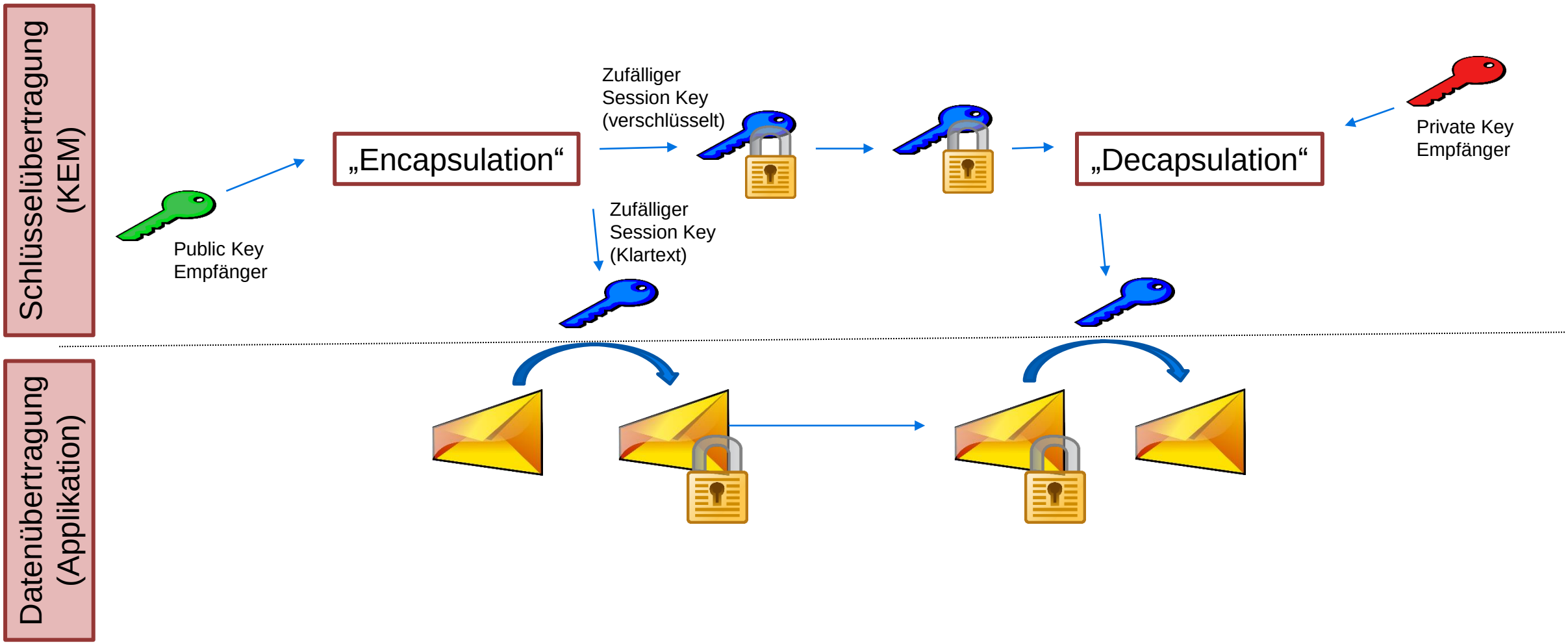
Kryptografische Algorithmen werden als Bausteine in Protokollen wie z.B. TLS verwendet und können mit wenig Aufwand durch die neuen PQC-Verfahren ersetzt werden!

Leider Nein!!!

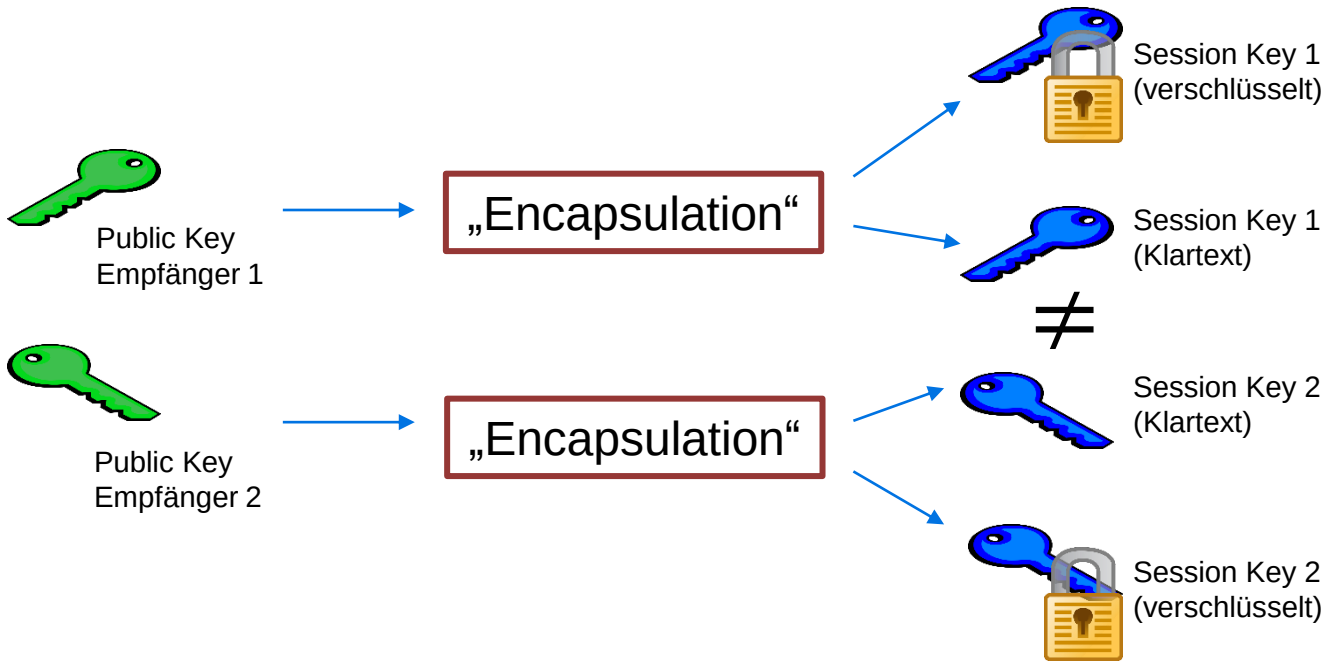
Migration zu PQC:
Herausforderungen (Beispiele)

- Die PQC-Algorithmen unterscheiden sich sehr stark hinsichtlich Performance und Schlüsselgrößen
  - Mit einer Auswahl an 1-2 neuen Verfahren lassen sich nicht alle Anwendungsfälle abdecken.
- Der Übergang zu KEMs macht Anpassungen im Key Management notwendig.
- Die Sicherheit der neuen Verfahren ist noch nicht hinreichend untersucht!
  - Kombination von klassischer Krypto und PQC (hybrider Ansatz)

Migration zu PQC:
Funktionsweise von KEMs



Migration zu PQC: Beispieleinsatz von KEMs



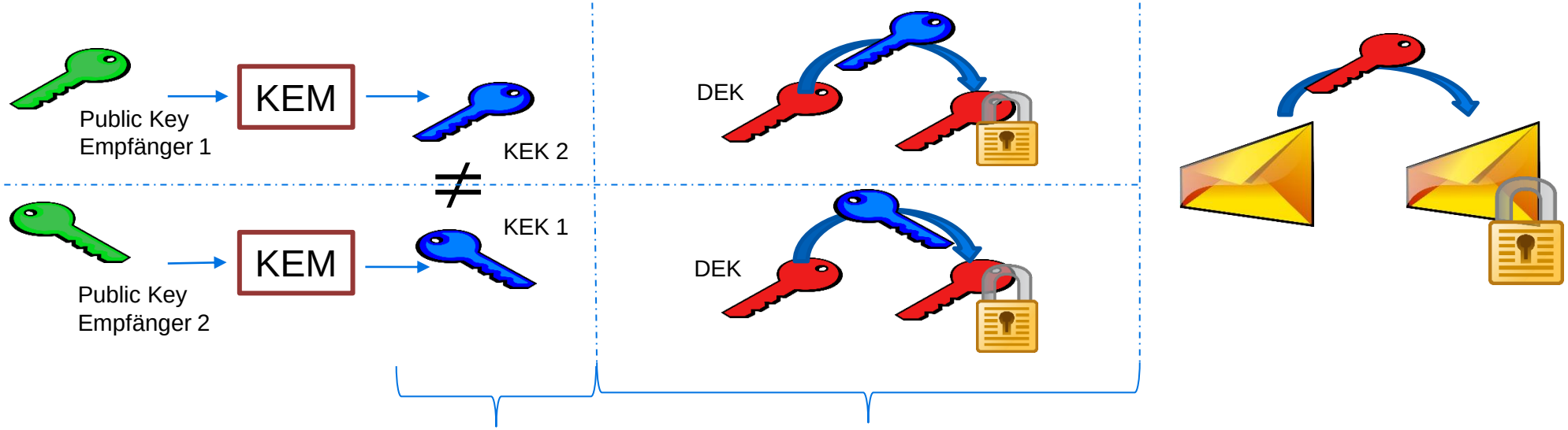
- Der KEM-Algorithmus liefert unabhängige zufällige Session Keys:
  - Bei Eingabe unterschiedlicher Public Keys
  - Bei mehrfachem Aufruf mit demselben Public Key
- Der KEM-Ansatz lässt sich nicht direkt nutzen, um einen Session Key an zwei Empfänger zu senden.
- Dazu ist eine zusätzliche Ebene im Key Management nötig
  - Beispiel: KEM-Trans Verfahren der LAMPS Arbeitsgruppe des IETF.

Migration zu PQC:
KEM-Trans Vorschlag des IETF

Phase 1: Vereinbarung
Key Encryption Key (KEK)

Phase 2: Übertragung
Data Encryption Key (DEK)

Phase 3: Übertragung
Nachricht



Die mit dem KEM vereinbarten Schlüssel sind individuell pro Empfänger.

Zusätzliche Ebene im Key Management: Individuelle Verschlüsselung des DEKs.

Quelle: https://datatracker.ietf.org/doc/draft-perret-prat-lamps-cms-pq-kem/, 20. Mai 2022

Migration zu PQC

- Fortschritte bei der Entwicklung von Quantencomputern schwächen die klassischen Verfahren!
- Die neuen PQC-Verfahren sind noch nicht so gut untersucht:
  - Eurocrypt 2021: Rainbow komplett gebrochen (ePrint 2020/1343)
  - April 2022: Verbesserungen der Dual Lattice Attacks
  - August 2022: SIKE komplett gebrochen (ePrint 2022/975)

Migration zu PQC

- Es könnte einen Zeitraum geben, in dem
  - man klassischen Verfahren nicht mehr voll vertraut und
  - PQC-Verfahren noch nicht hinreichend untersucht sind
- Lösung (hybride Verfahren):
  - Kombinierte Verwendung von klassischer Krypto und PQC
  - Das resultierende Verfahren muss sicher sein, so lange eines der verwendeten Einzelsysteme sicher ist.

Migration zu PQC:
Multi-KEM Verfahren (hybride Verschlüsselung)

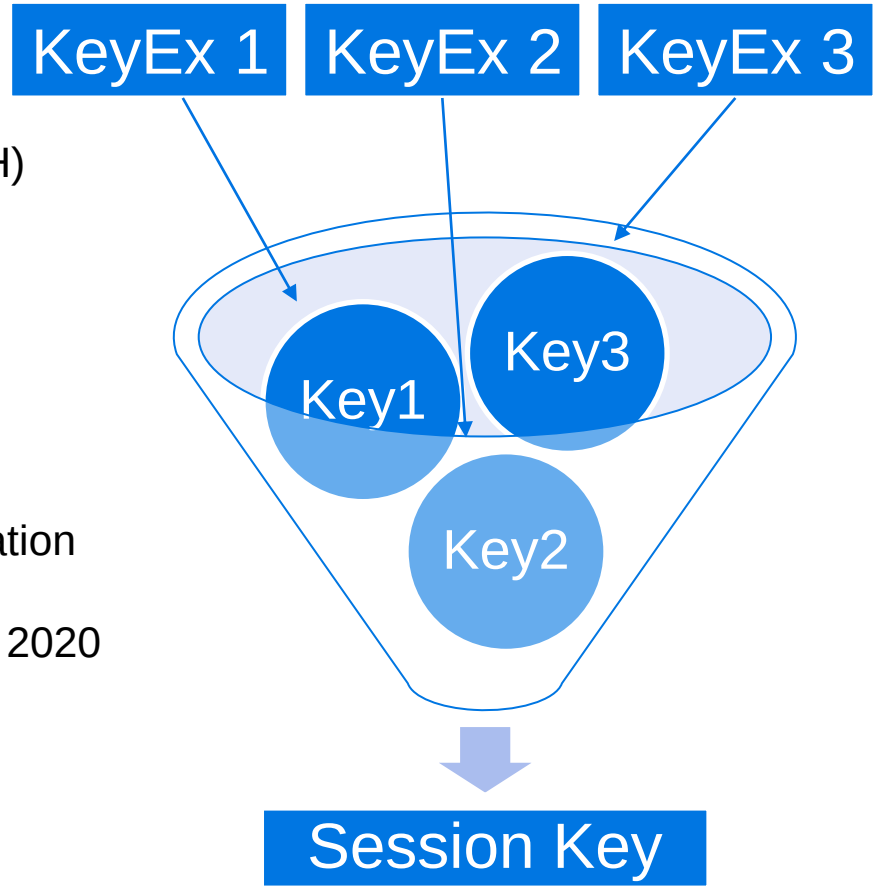
Key Exchange:

- Key Encryption (z.B. RSA-OAEP)
- Key Encapsulation (KEM)
- Key Establishment (z.B. DH, ECDH)

KEM Combiner, z.B.

- ETSI TS 103 744: Quantum-safe Hybrid Key Exchanges, Dec. 2020
- NIST SP 800-56Cr2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes, Aug. 2020

Key Usage



Achtung:

Der Begriff Hybride Verschlüsselung ist mehrfach besetzt.

- In der klassischen Kryptografie für die Übertragung symmetrischer Schlüssel mittels asymmetrischer Verfahren.
- Für die Kombination aus klassischen kryptografischen Verfahren und PQC-Verfahren. Hier sollten alternative Begriffe wie **Multi-Algorithmus Signaturen** oder **Multi-Algorithmus KEMs** verwendet werden.

Migration zu PQC:
A Long Winding Road

- Auch nach der Standardisierung bleibt viel zu tun:
  - Einarbeitung in Protokolle (TLS, SSH, OpenVPN etc.)
  - Einarbeitung in Produkte
  - Überarbeitung regulatorische Anforderungen (z.B. BAIT im Finanzwesen)
  - Migration in Unternehmen:
    - Erstellung Krypto-Inventar
    - Erstellung Migrationsplan (risikobasiert)
    - Migration von Anwendungen und Daten
- Auch wenn der Quantencomputer nicht realisiert werden sollte, PQC wird bleiben!

Kontakt

Dr. Christian Tobias
Christian.Tobias@mtg.de
+49 6151 8000 177

Dr. Falko Strenzke
Falko.Strenzke@mtg.de
+49 6151 8000 24