

Post-Quantum Kryptographie

Es ist Zeit zu handeln

Sebastian Hempel • 13.03.2026



Sebastian Hempel

ITCONSULTING **HEMPEL**

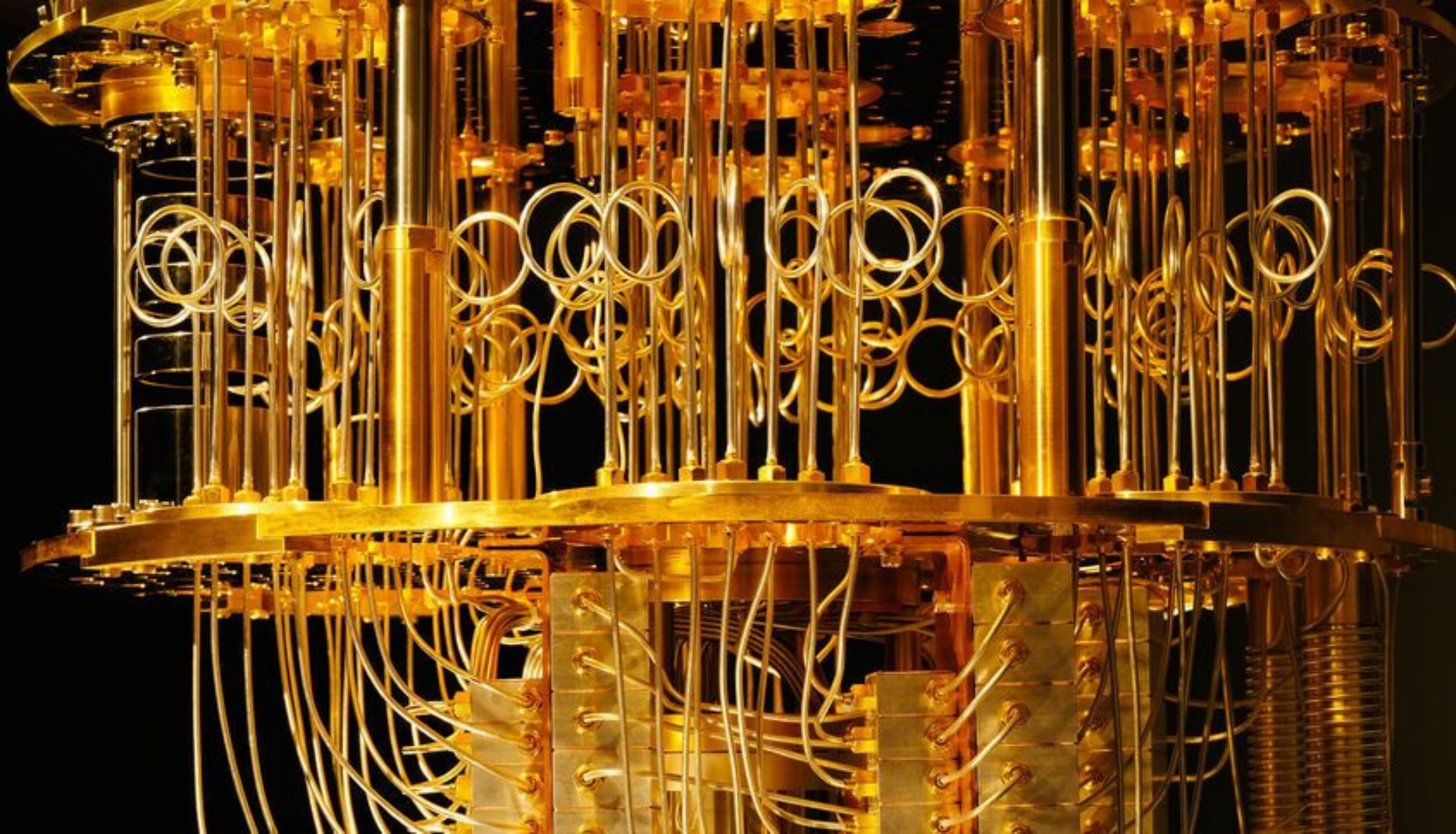
- selbständiger Software-Entwickler seit 2003
- Java, Puppet
- IT-Security
- Linux und OpenSource

<https://it-hempel.de>

@sepp@chaos.social



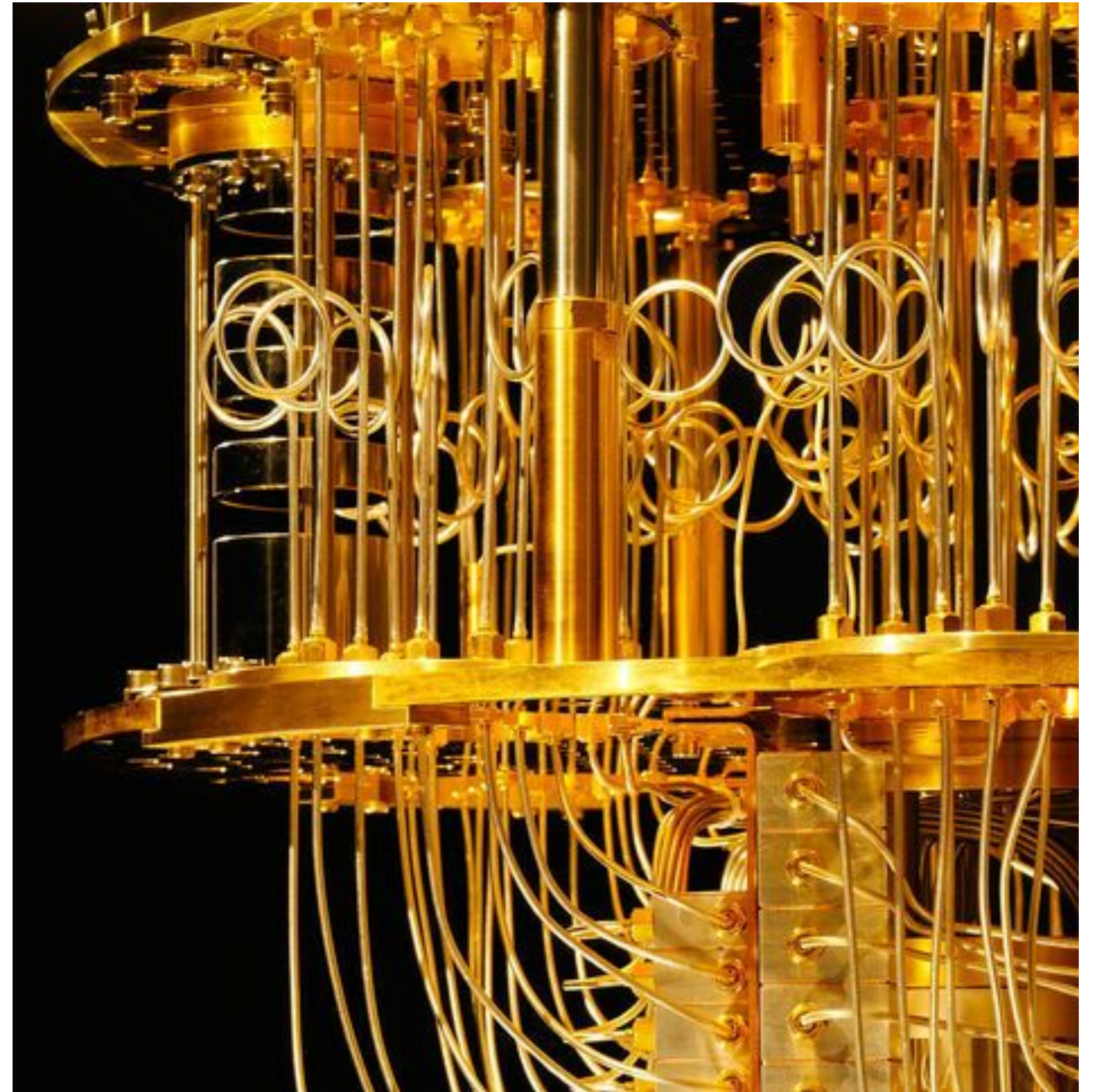
Quantencomputer und Kryptographie



Quantencomputer

Prinzip

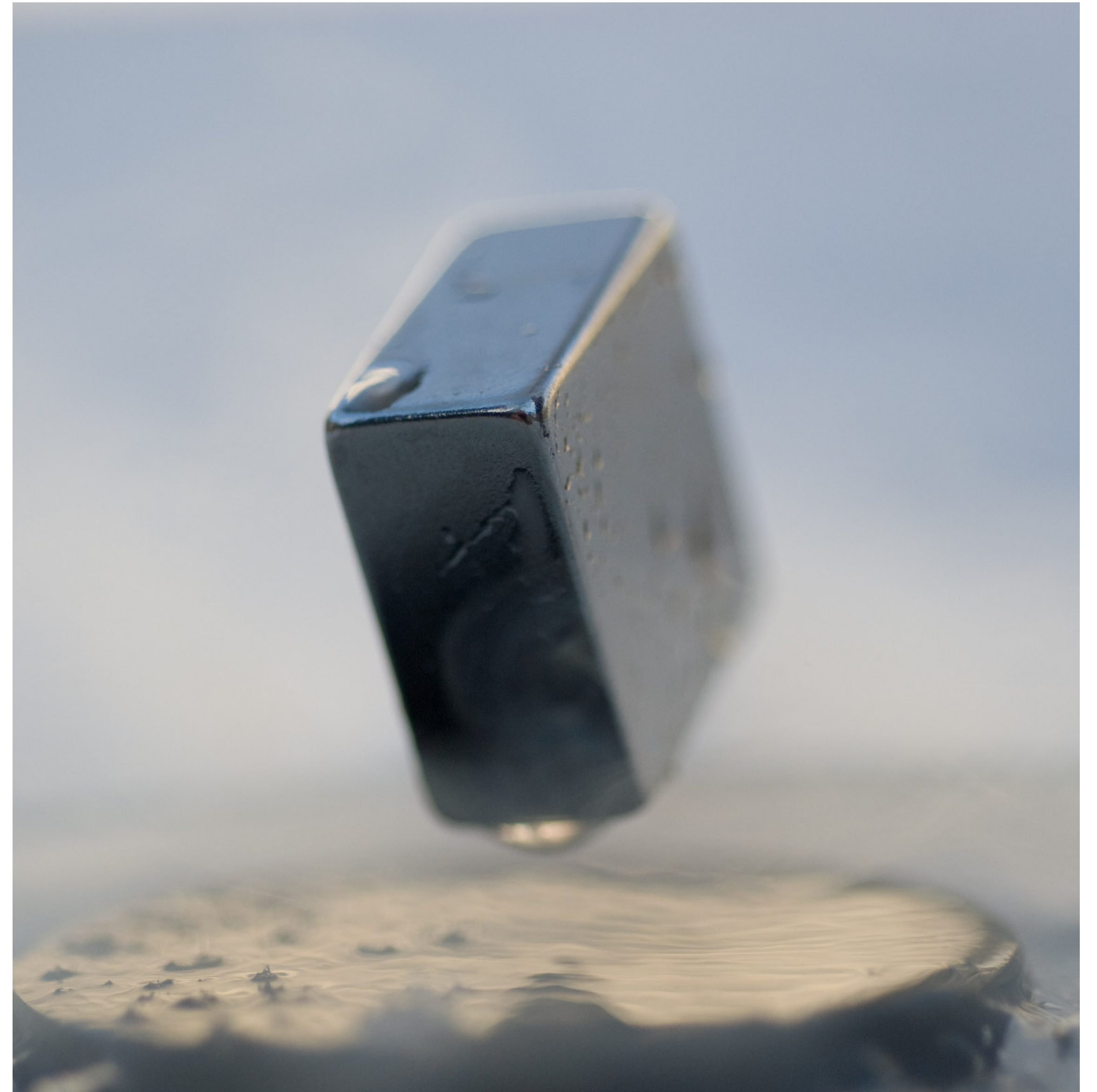
- Bit vs. Qubit
 - 0 oder 1
 - 0, 1 oder alles dazwischen
- Logik vs. Quantenverschränkung
 - und, oder, nicht
 - Quantenmechanik



Quantencomputer

Herausforderungen

- Operation nahe dem absoluten Nullpunkt
- Korrektur von Störungen
 - logische Qubits
- Quantencomputer
 - 7 Qubits (2001, IBM)
 - 53 Qubits (2019, Google)



Levitation of a magnet on top of a superconductor 2 - Wikimedia - CC BY-SA



Kryptografie

Grundlagen

- asymmetrische Verfahren
- Mathematische Probleme
 - Primfaktorzerlegung (RSA)
 - diskreter Logarithmus (ECC)
- keine einfache Lösung / brute force



Gefahr durch Quantencomputer

- mehrere Werte auf einmal
- Shor Algorithmus (1994)
- Schätzung in 2019 für 2048 Bit RSA Schlüssel
 - Quantencomputer: Stunden
 - herkömmliche Computer: mehrere Jahre



Gefahr der Quantencomputer

- Nicht jetzt sondern in der Zukunft
- Zeitraum unbekannt
- Entschlüsselung in der Zukunft



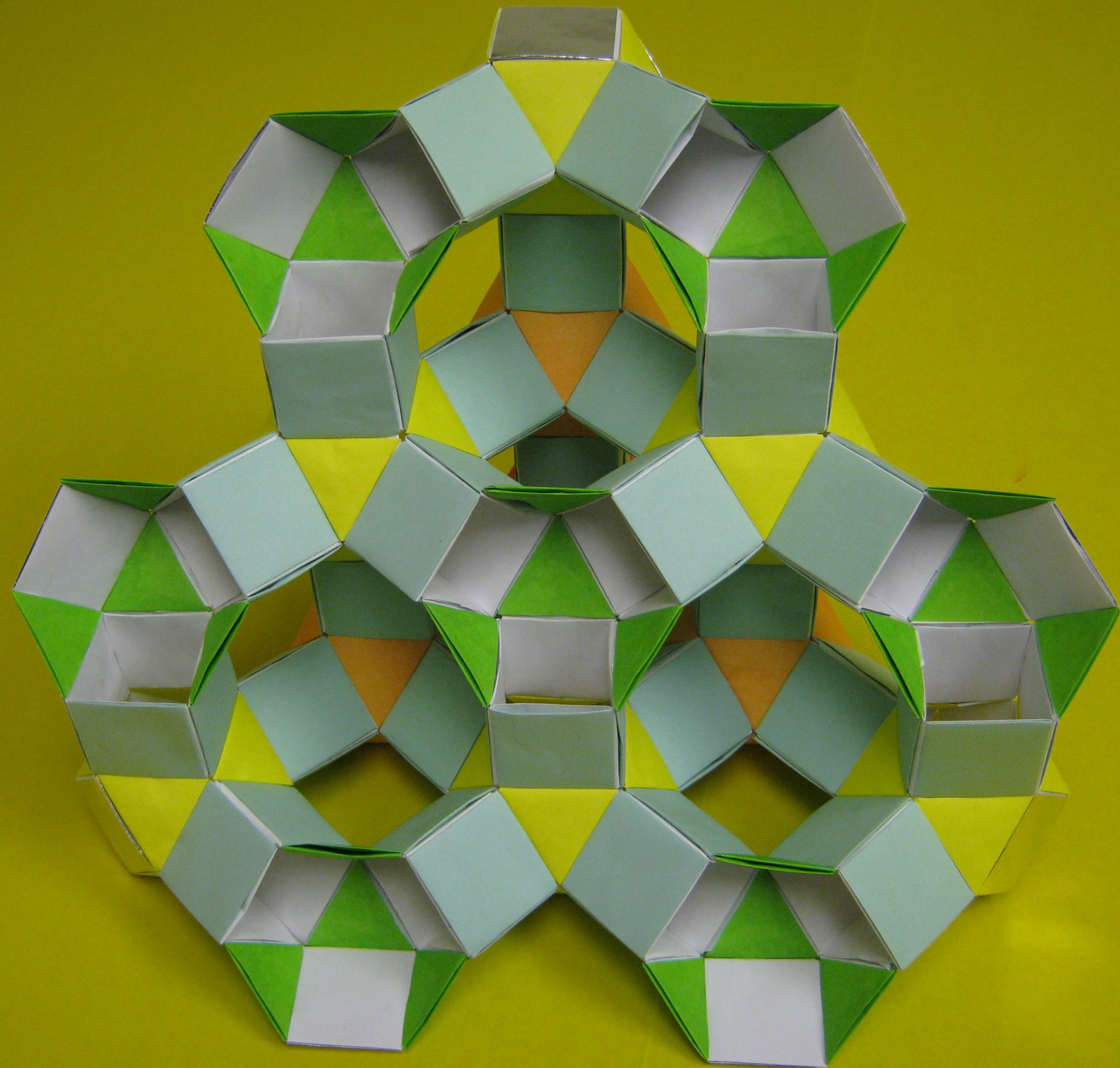
Combining near Worlaby - David Wright - CC-BY

Harvest now - Decrypt later

Harvest now - Decrypt later

- Daten können in der Zukunft gelesen werden
- Gefahr für sensible Daten
 - Gesundheit
 - Firmengeheimnisse
- Schutz muss jetzt angegangen werden - nicht erst in der Zukunft

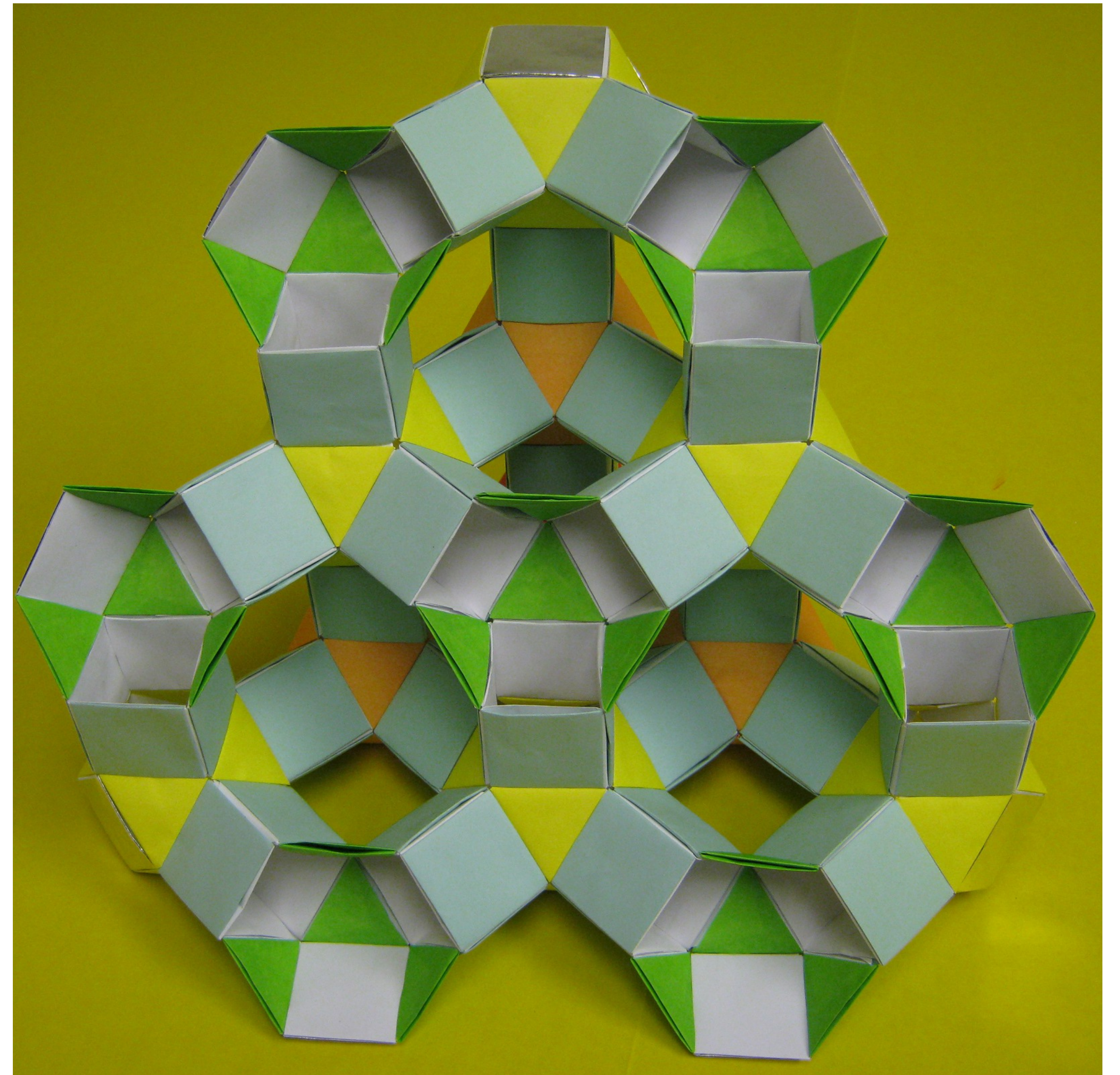
Post Quantum Kryptographie



PQC

post quantum cryptographie

- andere mathematische Probleme
- nicht durch Quanten-Computer lösbar
- ausführbar auf „normalen“ Computern



PQC Verfahren

- Gitterbasierte Kryptographie
 - merdimensionale Gitter
 - kürzester Vektor zwischen zwei Punkten
- Hashbasierte Signaturen
 - z.B. SHA-256
- Codebasierte Verfahren
 - Theorie der fehlerkorrigierenden Codes

NIST Standards

2024

- ML-KEM (FIPS-203)
 - Nachfolger für RSA, ECDH
- ML-DSA (FIPS-204)
- SLH-DSA (FIPS-205)
- FN-DSA (FIPS-206)

The NIST logo is rendered in a bold, black, sans-serif typeface. The letters are thick and closely spaced, with the 'N' and 'I' being particularly prominent due to their height and the sharp angles of the 'N'.

Einsatz von PQC

PQC Sites	März 2025	September 2025	Februar 2026
Cloudflare	26.938	29.195	292.834
Amazon AWS	150	6.333	41.980
Fastly		2.376	11.427
Squarespace	101	94	1.336
Hetzner	12	39	1.227
Google	422	426	1.180

<https://www.netmeister.org/blog/pqc-use-2025-09.html>, <https://www.netmeister.org/blog/pqc-use-2026-02.html>

Einsatz von PQC

Vorraussetzungen

- TLS 1.3
- PQC Zertifikat
- Unterstützung durch Software
- Browser unterstützen PQC bereits
- OpenSSL ab Version 3.5

Einsatz von PQC

Hybride Kryptographie

- Server bietet sowohl PQC als auch herkömmliche Kryptographie an
 - Interoperable Hybrid
 - Composite Hybrid

Einführung von PQC

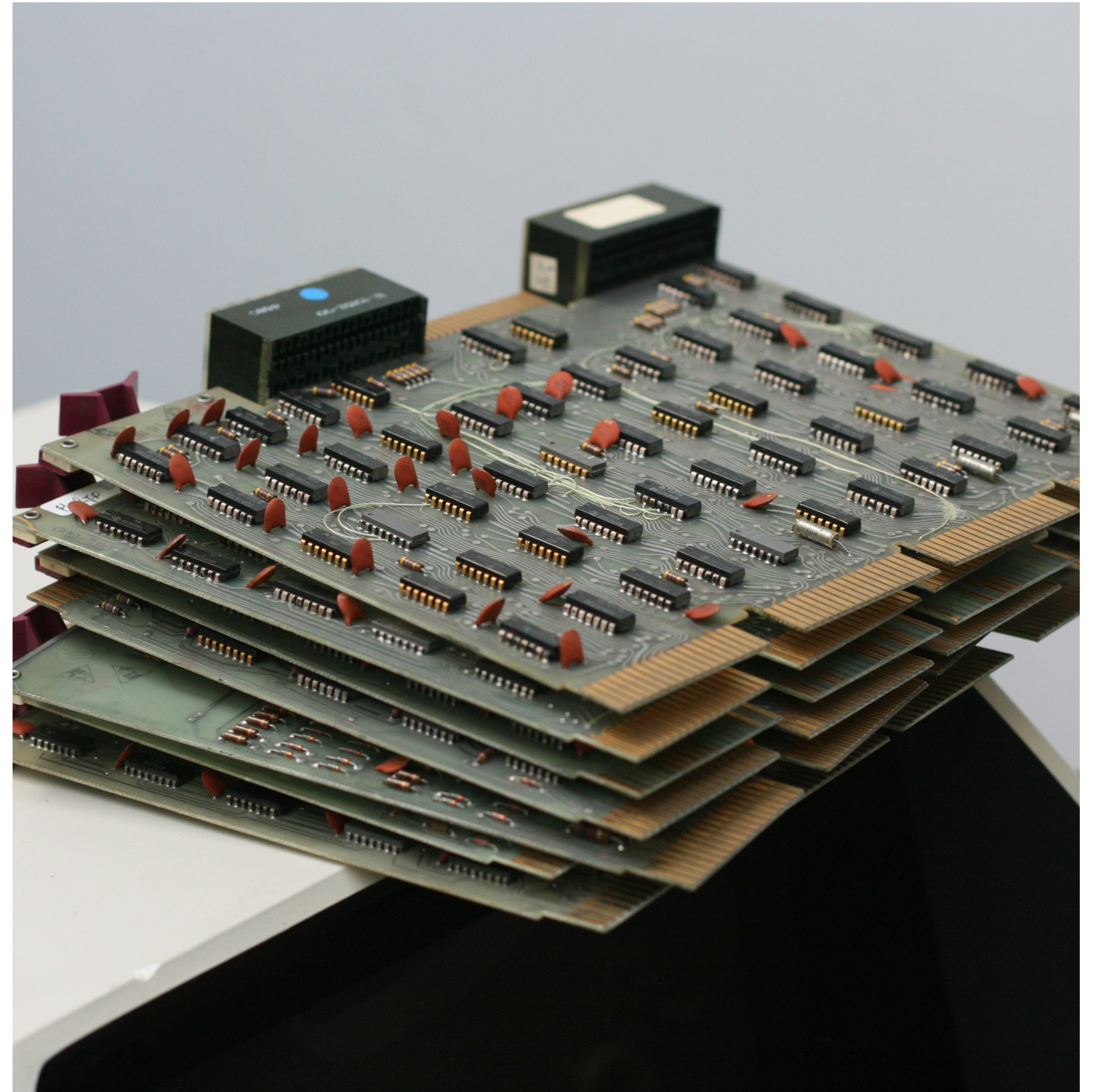
PQC Anforderungen

Höhere Anforderung an Ressourcen

- größere Schlüssel
 - 64 Bytes ECDS → 1.212 Bytes ML-DSA
- größere Signaturen
 - 64 Bytes ECDSA-P256 → 2.420 Bytes MD-DSA
- mehr Computing-Power

Kryptoagilität

- aktuelle Verfahren sind gut „abgehangen“
- PQC Verfahren werden weiterhin untersucht
- Schnelle Reaktion auf Änderung der Verfahren
 - Modularität
 - schnelles Ersetzen und Updaten



Kryptoagilität

- Update von SHA-1 auf SHA-256 dauerte 5 Jahre
- SHA-1 wurde 2017 deprecated
- Das Hash-Verfahren wird aber immer noch verwende



Krypto-Inventar

- Wo wird welche Krypto genutzt?
- Welche Keys Zertifikate gibt es?
 - Laufzeit
- Welche Software wird verwendet?
 - Version
 - unterstützte Kryptographie



Großes Lager mit Kartons - Tim Reckmann - CC BY

Krypto-Inventar

- Tools unterstützen bei Inventarisierung von Software
- Entwickler müssen den Code selbst begutachen
 - Dependencies / Frameworks
 - Quellcode
 - Konfiguration
 - Runtime

Planung

- Priorisierung
 - Kritikalität der Daten
- Software-Updates
- Ersetzung von Systemen

列車時刻表(下り)										H15・10・1	
12:00 J (491A) 名:		17:15 ★ 39A 名: 山博				44:45 331A 名: 姫福下 博					
45 3A		16:30 W ★ 1A 山博		21:30 J (333A) 名: 姫福徳山 博		25:30 ★ 9201A		41:45 ★ 41A 福: 広 ★ 9041A 福徳: 博		48:15 ★ 9203A	
										54:30 J (495A) 静:	
12:30 ★ 3A 博		★ (9111A) 各駅: 岡		三:		35:45 ★ 101A		44:30 J 261A		48:00 ★ (103A) 休日ウヤ (9103A)	
										54:30 ★ 43A 福: 広 ★ 3043A 福・山: 博	
45 07A		12:50 W ★ 5A 山博		16:00 J★ (3083A) 博		21:30 ★ 303A 各駅: 岡		25:00 ★ (105A) 休日ウヤ ★ (9105A)		31:45 (試4911A) 米: 阪	
								35:45 ★ 2007A 姫: 博		41:00 J (401A)	
45 09A		12:30 ★ 9A 博		16:00 J★ (3085A) 山博		21:30 ★ 305A 各駅: 岡		25:00 ★ (109A)		35:45 ★ 111A	
								41:00 J (405A)		44:30 J 265A	
										48:00 ★ (113A) 休日ウヤ (9113A)	
45 15A		12:30 W ★ 11A 徳博		16:00 J★ (3087A) 山博		21:30 ★ 307A 各駅: 岡		25:00 ★ (3117A)		35:45 ★ 71A 姫岡	
								41:00 J (407A)		44:30 J 267A	
45 211A		12:30 ★ 13A 博		16:00 ★ (9213A)		21:30 ★ 309A 各駅: 岡		25:00 J★ (9215A)		35:45 ★ 121A	
								41:00 J (269A)		44:30 J 411A	
45 219A		12:30 W ★ 15A 山博		16:00 J★ (9089A) 山博		21:30 ★ 311A 各駅: 岡		25:00 J★ (9221A)		35:45 ★ 2017A 姫博	
								41:00 J (413A)		44:30 J 271A	
45 225A		12:30 ★ 19A 博		16:00 J★ (9091A) 山博		21:30 ★ 313A 各駅: 岡		25:00 J★ (9227A)		35:45 ★ 123A	
								41:00 J (273A)		44:30 J 415A	
										48:00 ★ (9229A)	
45 231A		12:30 W ★ 21A 徳博		16:00 ★ (9093A) 山博		21:30 ★ 315A 各駅: 岡		25:00 ★ (9233A)		35:45 ★ 73A 姫岡	
								41:00 J (417A)		44:30 J 275A	
										48:00 ★ (9235A)	
										54:30 ★ 53A 福: 広 ★ 9053A 福・山: 博	
										54:30 ★ 55A 福: 広 ★ 9055A 福・徳: 博	
										54:30 ★ 57A 福: 広 ★ 3057A 福・徳: 博	
										54:30 J (9419A) 岡	

Gesetzliche Anforderungen

- EU
 - Pläne für Umstieg bis Ende 2026 erstellen
 - kritische Anwendungen bis Ende 2030
 - komplette Umstellung bis Ende 2035
- NIS-2 (indirekt)
 - „state of the art technology“ / TS-02102
- G7 Cyber Expert Group / BaFin
 - Anforderungen für Finanzbranche

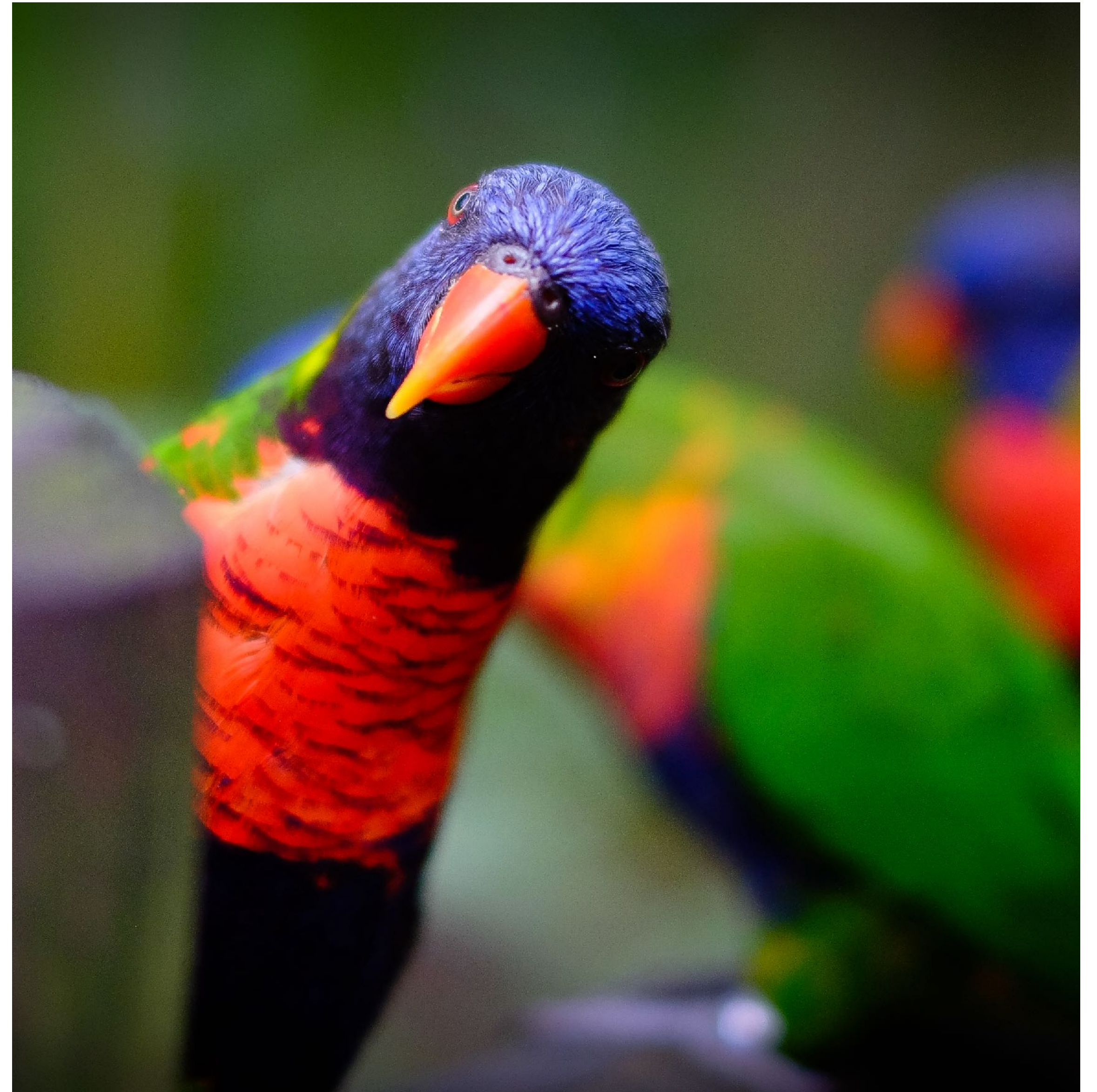


PQC Jetzt

- Gefahr für Daten in der Zukunft
 - Zeitpunkt ungewiss
- Handlung jetzt - vor dem Q-Day
- PQC als Rettung



Fragen?



any questions? - (Matthias Ripp) - CC BY