Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Einführung Post-Quanten Kryptographie Omnisecure 2022

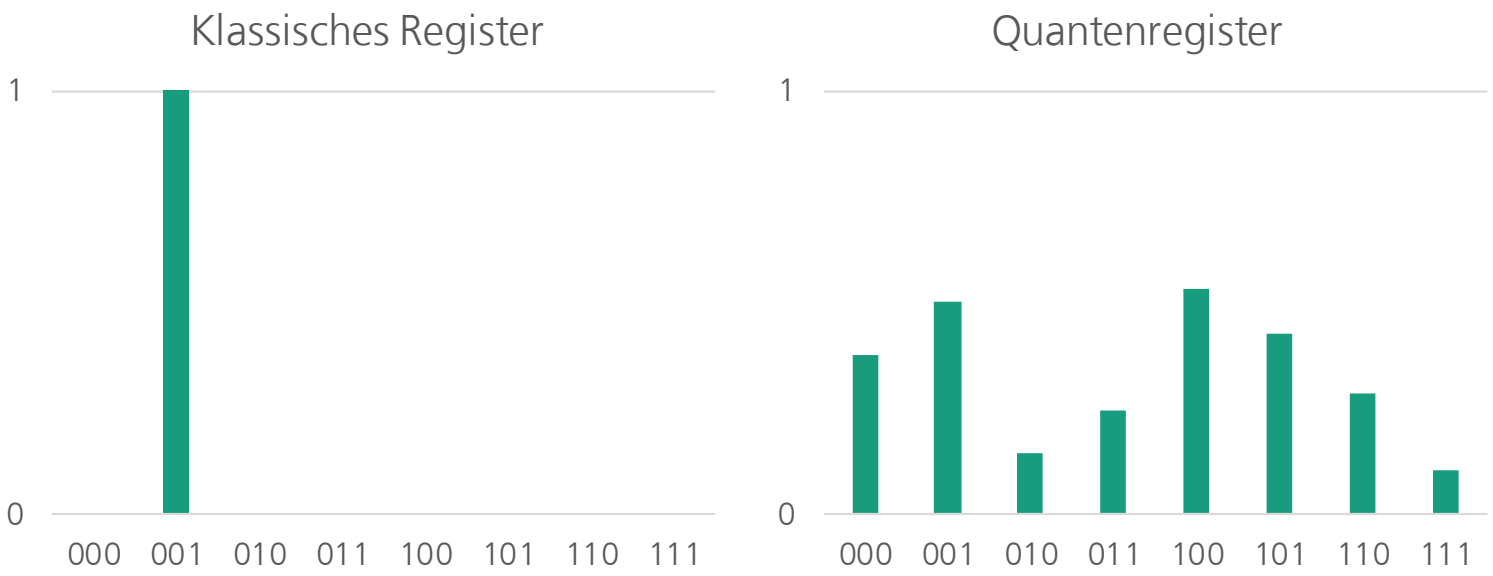
22.06.2022

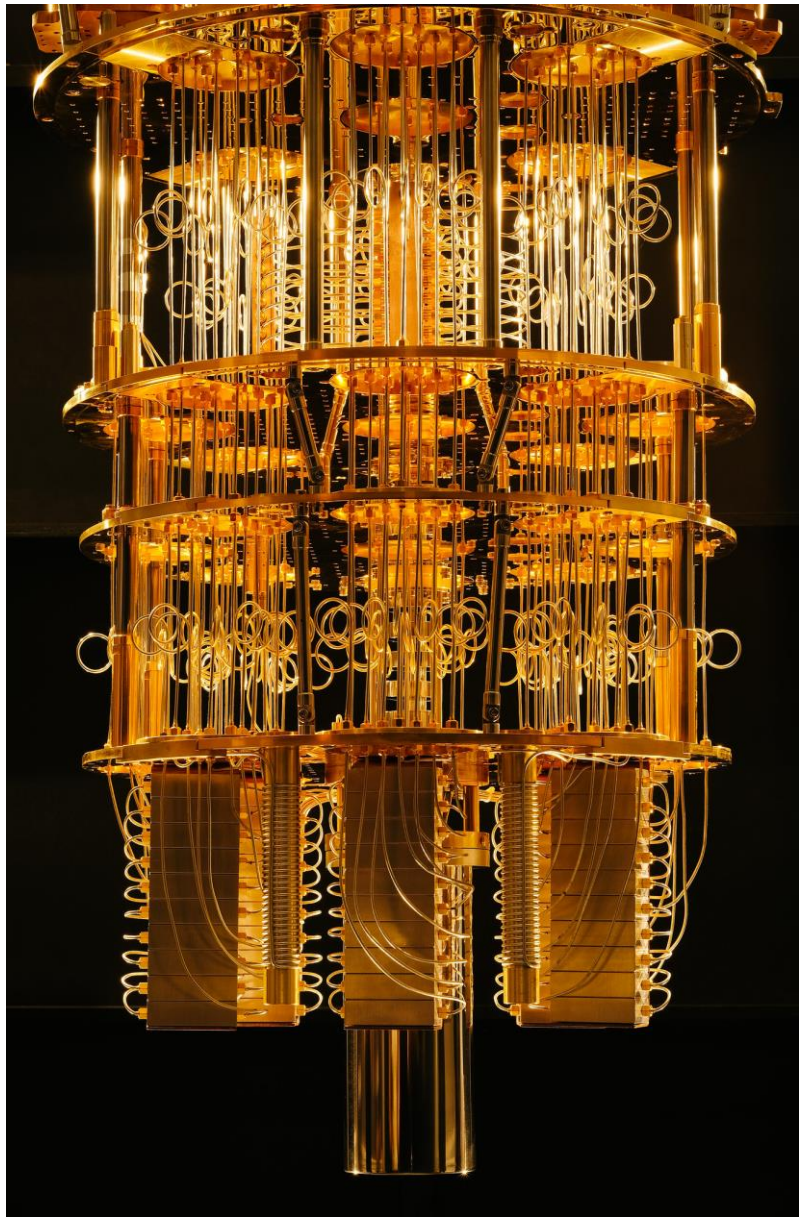
Benjamin Zengin

Quantencomputer

Qubits

- Quantencomputer arbeiten mit Qubits anstatt Bits
- n-Bit Register speichert einen von 2^n Zuständen
- n-Qubit Register speichert Verteilung von 2^n Zuständen





"IBM quantum computer" (CC BY-ND 2.0) by IBM Research

Quantencomputer
Algorithmen

1996: Algorithmus von Grover

Reduziert Laufzeit für Schlüsselsuche symmetrischer Verfahren auf $\sqrt{n}$

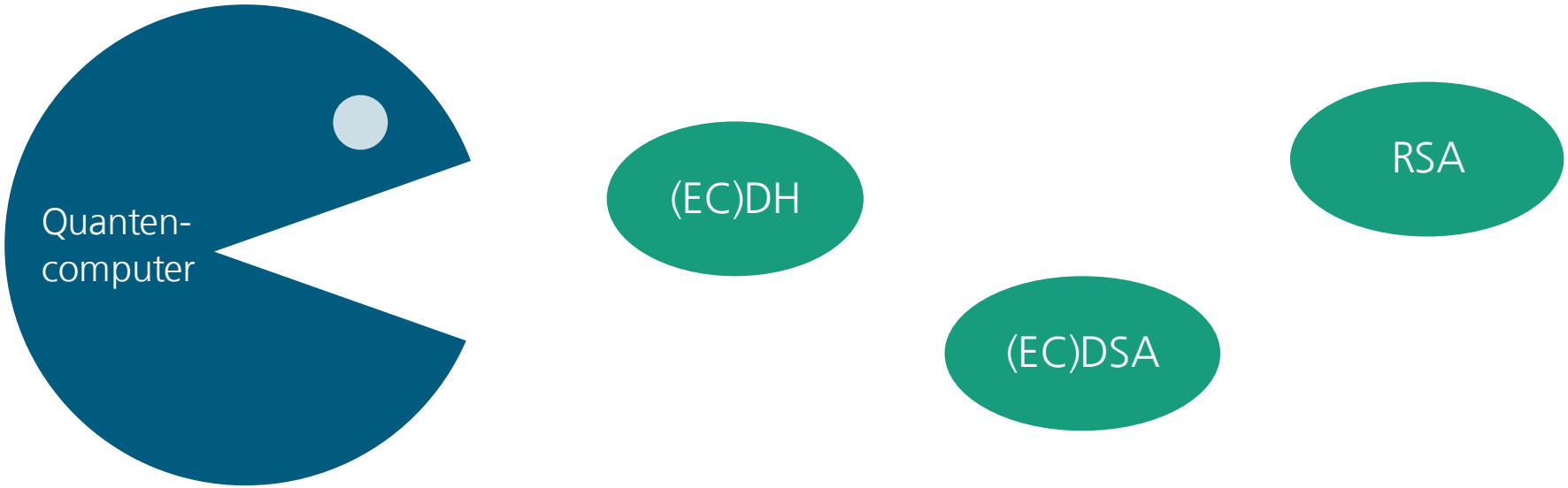
Halbierung der effektiven Schlüssellänge ($\sqrt{2^n} = 2^{n/2}$)

Verdopplung der Schlüssellänge stellt Sicherheitsniveau wieder her

Quantencomputer
Algorithmen

1994: Algorithmus von Shor

- Effiziente Faktorisierung und Berechnung des diskreten Logarithmus
- Bricht jegliche derzeit verwendete asymmetrische Kryptographie



Quantencomputer
Forschung & Entwicklung

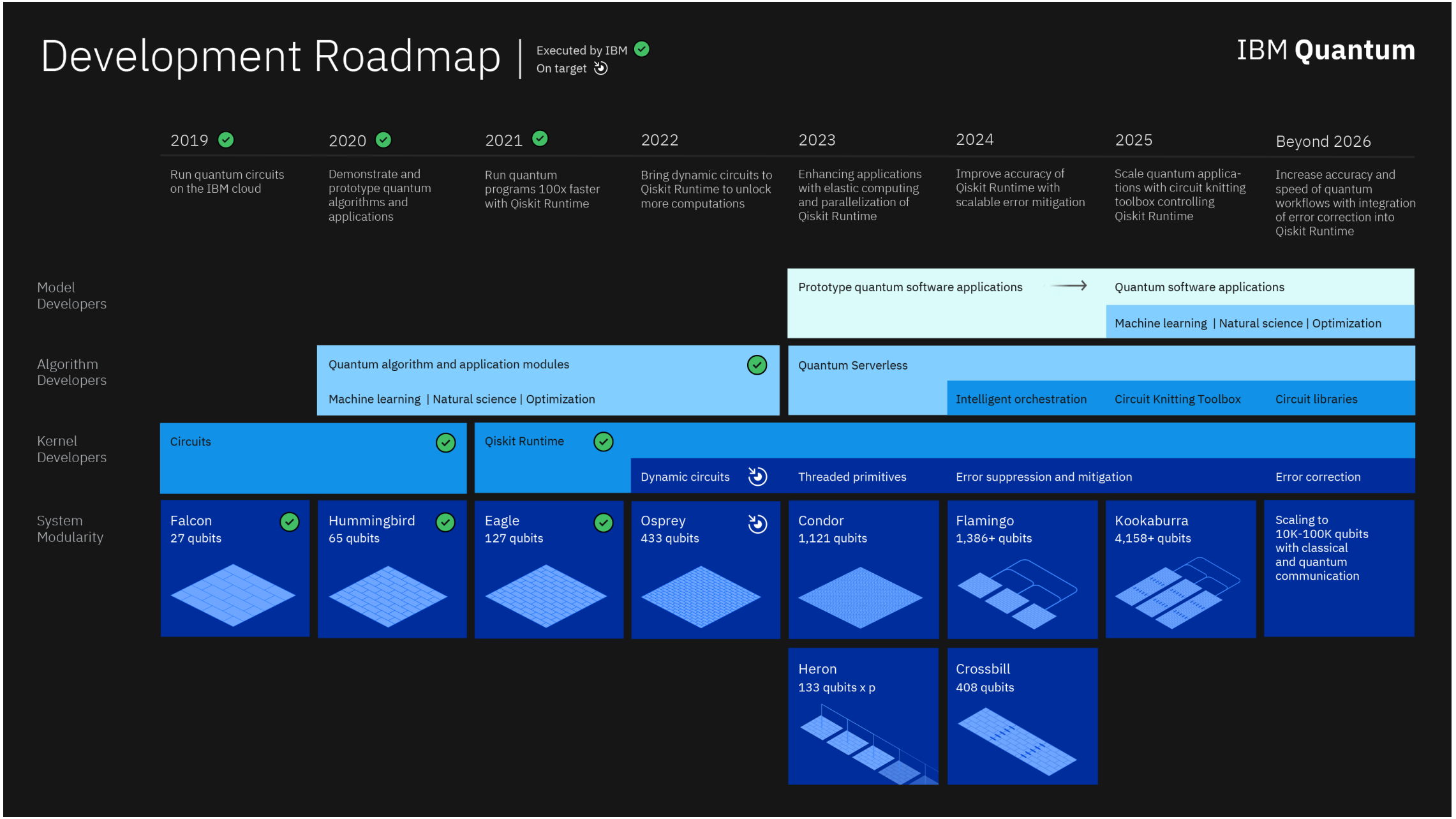
Implementation of Shor's Algorithm on a Linear Nearest Neighbour Qubit Array

Austin G. Fowler, Simon J. Devitt and Lloyd C. L. Hollenberg
Centre for Quantum Computer Technology, School of Physics
University of Melbourne, Victoria 3010, Australia.
(Dated: February 1, 2008)

Shor's algorithm, which given appropriate hardware can factorise an integer N in a time polynomial in its binary length L, has arguable spurred the race to build a practical quantum computer. Several different quantum circuits implementing Shor's algorithm have been designed, but each tacitly assumes that arbitrary pairs of qubits within the computer can be interacted. While some quantum computer architectures possess this property, many promising proposals are best suited to realising a single line of qubits with nearest neighbour interactions only. In light of this, we present a circuit implementing Shor's factorisation algorithm designed for such a linear nearest neighbour architecture. Despite the interaction restrictions, the circuit requires just $2L + 4$ qubits and to first order requires $8L^4$ gates arranged in a circuit of depth $32L^3$ — identical to first order to that possible using an architecture that can interact arbitrary pairs of qubits.

$$2 * 2048 + 4 = 4100$$

Fraunhofer AISEC



How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

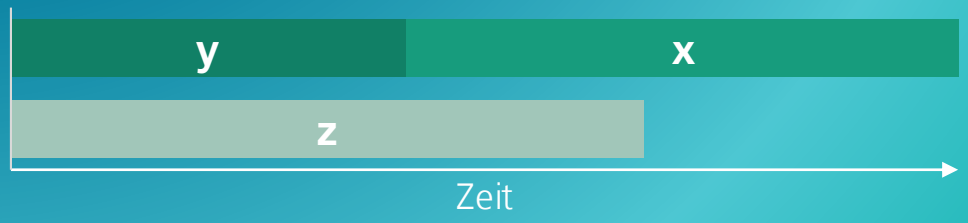
We significantly reduce the cost of factoring integers and computing discrete logarithms in finite fields on a quantum computer by combining techniques from Shor 1994, Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Van Meter et al. 2009, Jones et al. 2010, Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n^2 \lg n$ measurement depth to factor n-bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

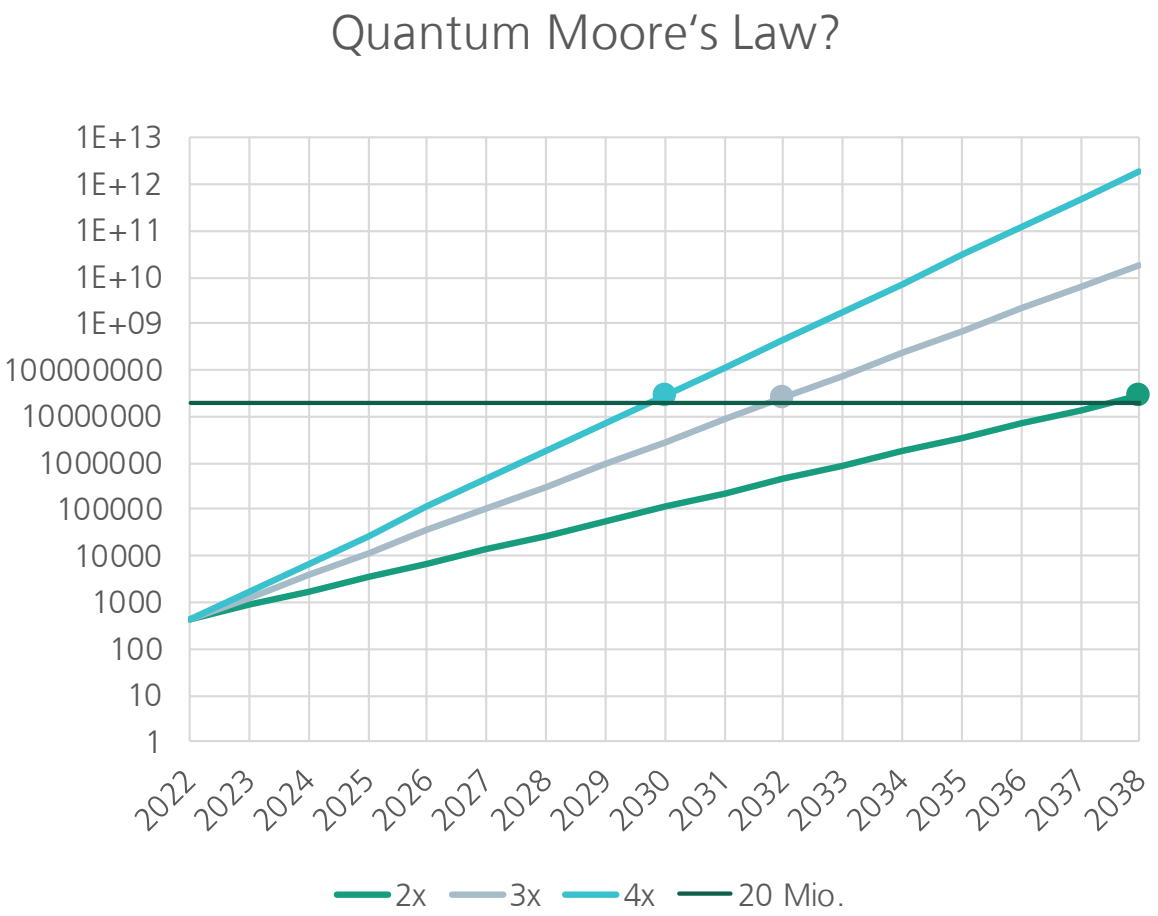
Quantencomputer
Forschung & Entwicklung

„Theorem“ von Michele Mosca [1]

- x = *security shelf-life*
- y = *migration time*
- z = *collapse time*

Wenn x + y > z,
dann haben wir schon heute ein ernsthaftes Problem





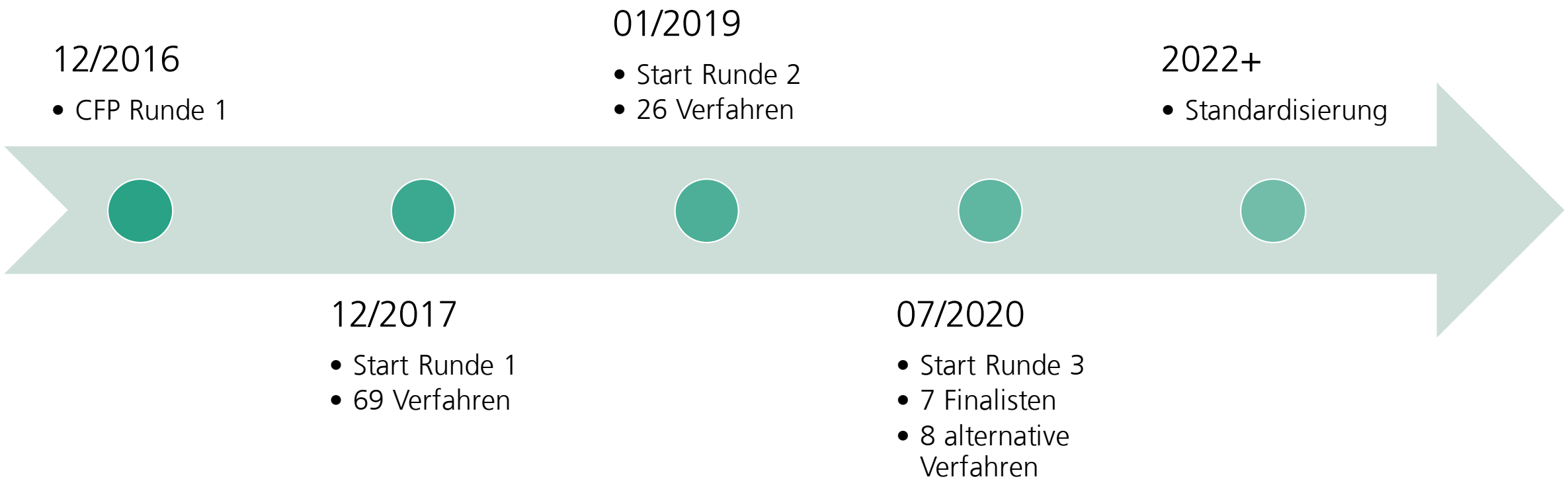
Fraunhofer AISEC

Post-Quantum Kryptographie

Kategorien für alternative asymmetrische Verfahren

Post-Quantum Kryptographie

NIST Standardisierung



Post-Quantum Kryptographie

Vergleich der Verfahren - Signatur

Verfahren	Secret Key	Public Key	Signatur	KeyGen kCycles	Sign kCycles	Verify kCycles
Falcon512	1,28 kB	897 B	657 B	19.872	387	82
Dilithium2	2,54 kB	1,31 kB	2,42 kB	71	195	73
Rainbow-III	611,3 kB	258,4 kB	164 B	56.000	384	20.000
ECDSA	**32 B**	**64 B**	**64 B**	**97**	**133**	**283**

Post-Quantum Kryptographie

Vergleich der Verfahren - Schlüsselaustausch

Verfahren	Secret Key	Public Key	Shared Secret	KeyGen kCycles	Encrypt kCycles	Decrypt kCycles
Kyber90s512	1,63 kB	800 B	736 B	22	29	21
McEliece 348864	6,45 kB	261,12 kB	128 B	36.641	44	135
NTRU-HPS-2048-677	1,24 kB	931 B	931 B	309	84	60
LightSABER	1,57 kB	672 B	736 B	45	62	63
SIKEp434	350 B	197 B	236 B	10.158	15.120	11.077
Frodo-AES-640	19,89 kB	9,62 kB	9,72 kB	1.385	1.862	1.747
ECDH	**32 B**	**64 B**	**64 B**	**245**	**599**	**599**

Kontakt

Benjamin Zengin, M.Sc.
Department Secure Systems Engineering
Tel. +49 89 32299 86 233
benjamin.zengin@aisec.fraunhofer.de

Fraunhofer AISEC
Breite Str. 12
14199 Berlin
www.aisec.fraunhofer.de

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC