EIN DEUTSCHES DIGITALES SIGNATURVERFAHREN AUF DEM WEG ZUM INTERNATIONALEN KRYPTOGRAFISCHEN STANDARD

TECHNISCHE UNIVERSITÄT DARMSTADT

CROSSING

15. Deutscher IT-Sicherheitskongress
16/05/2017

Nina Bindel
TU Darmstadt

ALGORITHMUS VON SHOR, 1994

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

RSA und ECDSA nicht mehr sicher

A digital computer is g
device; that is, it is believ
an increase in computatio
true when quantum mech
factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

QUANTUM COMPUTER REALISTISCH?

- nature.com, 03. 01. 2017:

  „Quantum computers ready to leap out of the lab in 2017"

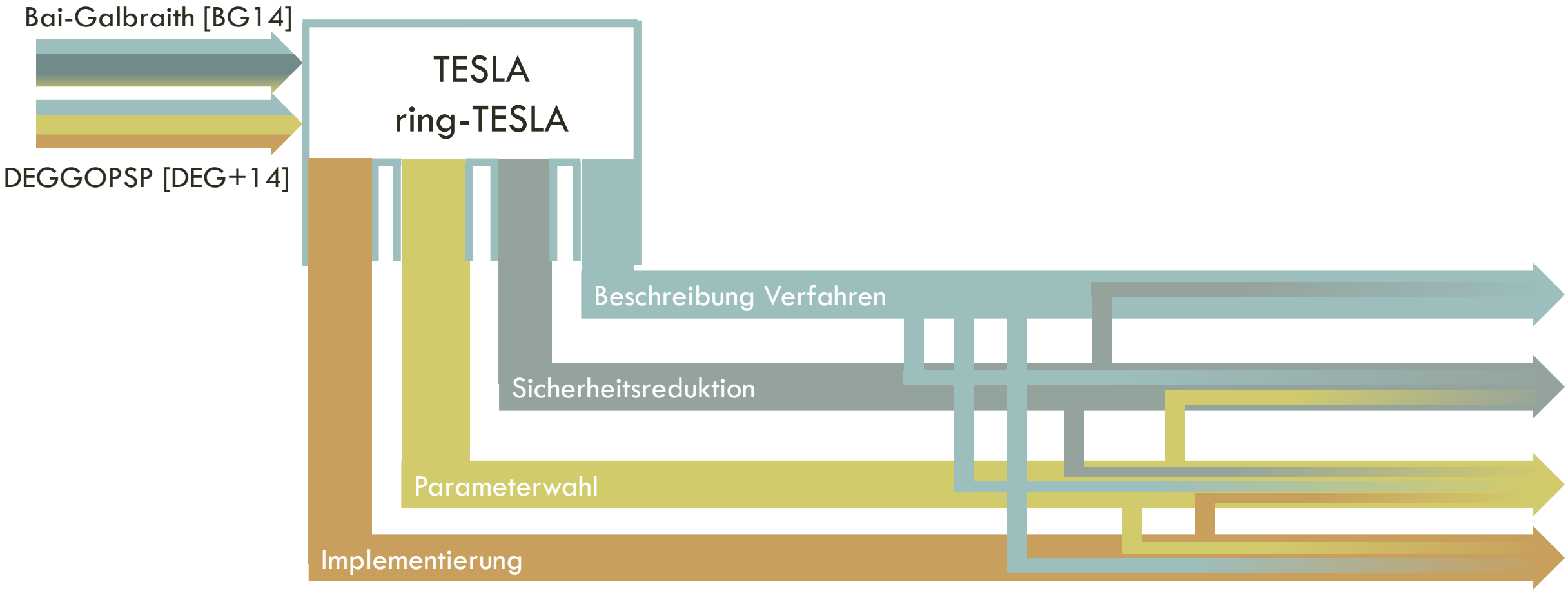
- Abschätzung der EU-Kommision:

  bis 2035 universeller Quantencomputer

BETTER SAFE THAN SORRY

- NSA, 2015 : (Teilweiser) Wechsel von klassischer zu post-quantum Kryptografie
- NIST, 2017: Start des Standardisierungswettbewerbs/Post-Quantum-Projekt

POST-QUANTUM KANDIDAT



UNTERSTÜTZER UND MITAUTOREN

- Sedat Akleylek[1]
- Erdem Alkim[2]
- Johannes Buchmann[3]
- Özgür Dagdelen[4]
- Edward Eaton[5,6]
- Gus Gutoski[6]
- Juliane Krämer[3]
- Giorgia Marson[7]
- Filip Palewa[5,6]
- Peter Schwabe[8]

1 Ondukuz Mayis University, Türkei
2 Ege University, Türkei
3 TU Darmstadt, Deutschland
4 BridginIT GmbH, Deutschland
5 University of Waterloo, Kananda
6 ISARA cooperation, Kanada
7 Ruhr-Universität Bochum, Deutschland
8 Radboud University, The Nedelands

BISHERIGE ENTWICKLUNG VON TESLA

Jul. 2015:
[ABBDP15]
(TESLA)

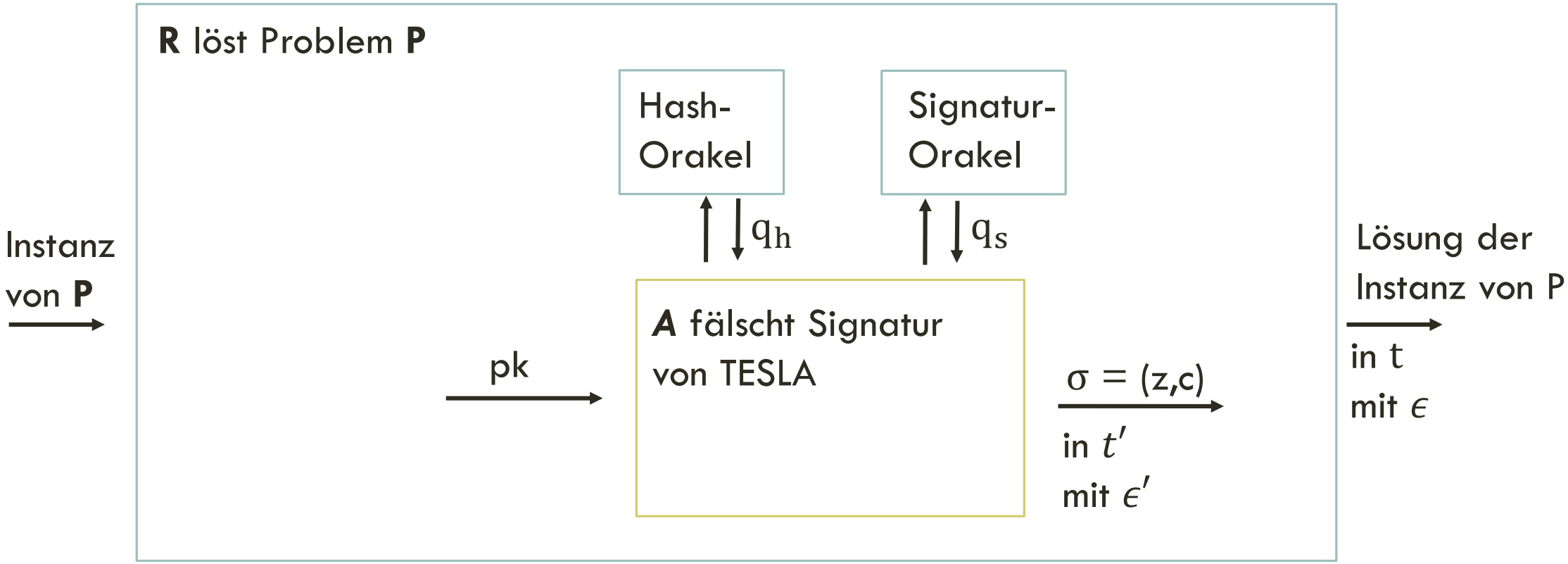
Strikte Reduktion im ROM

Verbesserte Parameter*

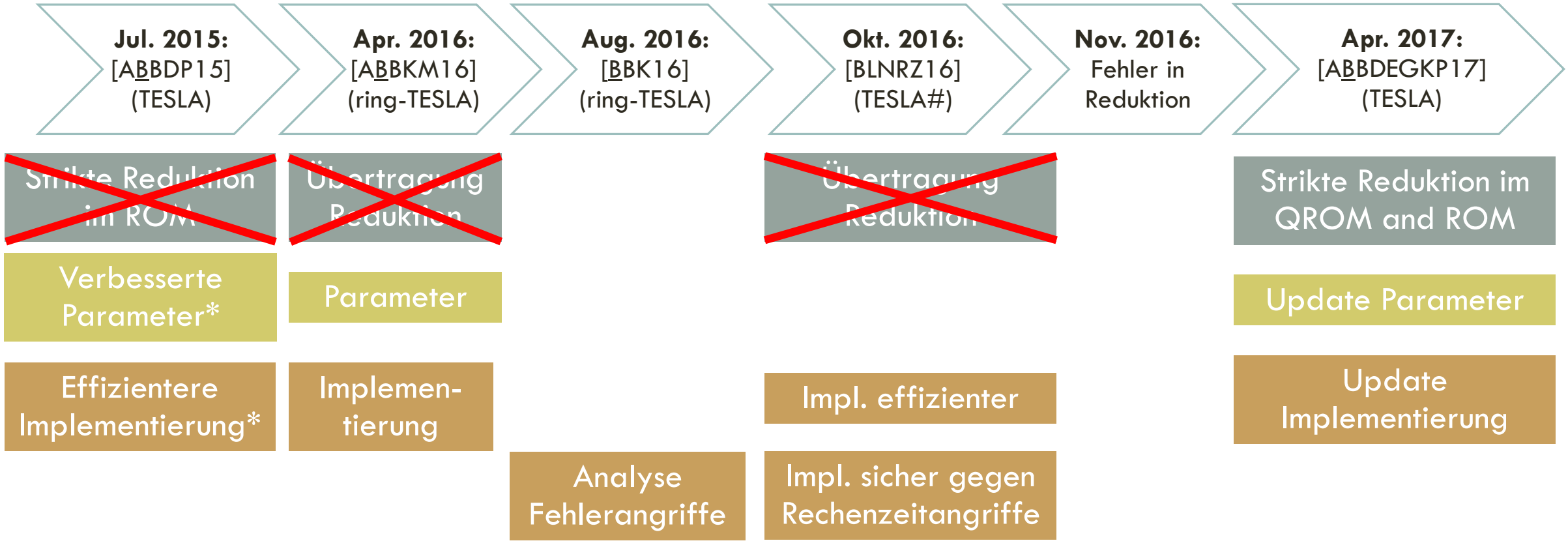
Effizientere Implementierung*

* Im Vgl. zu [BG14] und [DEG+14]

SICHERHEITSREDUKTION



BISHERIGE ENTWICKLUNG VON TESLA



* Im Vgl. zu [BG14] und [DEG+14]

GLIEDERUNG

- Beschreibung Signaturverfahren TESLA & Unterschiede ring-TESLA
- Beschreibung Parameterwahl
- Implementierung & Vergleich
- Geplante nächste Schritte

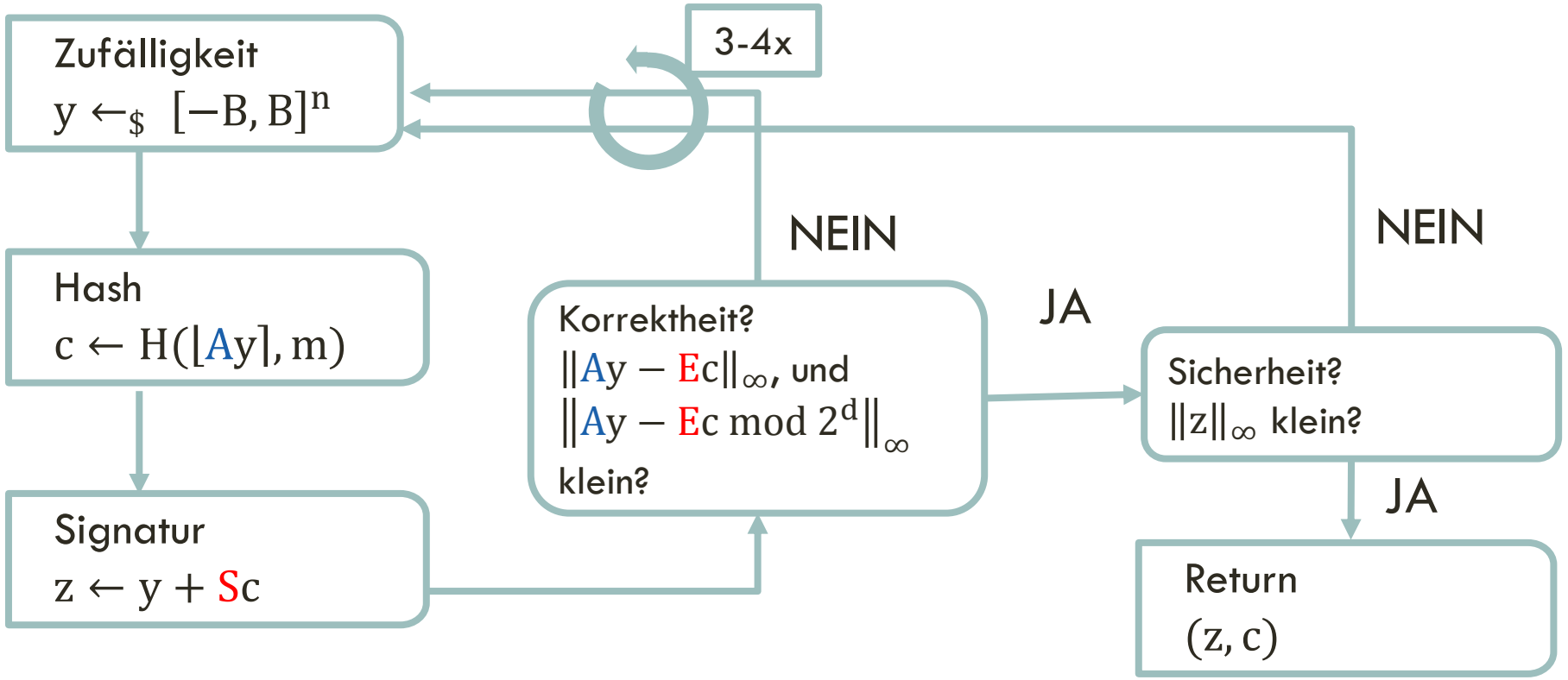
TESLA - SIGNATURERSTELLUNG

$A \leftarrow_{\$} \mathbb{Z}_q^{m \times n}$

$sk = (S, E) \leftarrow_{\sigma} \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^{m \times n}$

$pk = (A, B = AS + E \bmod q)$

Sign(sk, m):



RING-TESLA

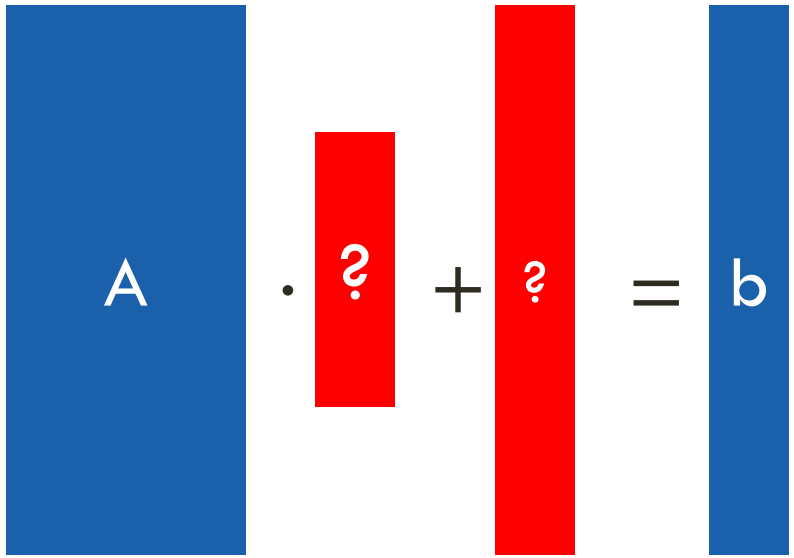
$$A \leftarrow_{\$} \mathbb{Z}_q^{m \times n}$$
$$sk = (S, E) \leftarrow_{\sigma} \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^{m \times n}$$
$$pk = (A, B = AS + E)$$

Rechenintesivste Operation

Großer Speicherplatz

$$a_1, a_2 \leftarrow_{\$} \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$$
$$sk = (s, e_1, e_2) \leftarrow_{\sigma} \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$$
$$pk = (a_1, a_2, b_1 = a_1 s + e_1, b_2 = a_2 s + e_2)$$

LEARNING WITH ERRORS PROBLEM



Gegeben:

$$A \leftarrow_{\$} \mathbb{Z}_q^{m \times n}$$
$$b \leftarrow \mathbb{Z}_q^m$$

Finde:

$$(s,e) \leftarrow_{\sigma} \mathbb{Z}_q^n \times \mathbb{Z}_q^m$$

$$A \cdot s + e = b \bmod q$$

SICHERHEITSREDUKTION TESLA

Theorem

Für entsprechende Parameter gilt: Falls M-LWE (t, ϵ)-schwer ist,

dann ist TESLA $(t', \epsilon', q_h, q_s)$-sicher (EUF-CMA) im „quantum random oracle model“

mit $t \approx t'$ und

$\epsilon' < \epsilon + \text{negl}(\lambda)$.

→ Parameter gewählt sodass

- das Verfahren korrekt,
- die Reduktion strikt und
- das Verfahren sicher ist.

BIT-SICHERHEIT UND BIT-HARDNESS

angestrebtes Sicherheitslevel λ von TESLA = Bit-Hardness η von LWE

~~- Sicherheitsverlust durch Reduktion~~

- Sicherheitsverlust Reduktion LWE auf M-LWE

$\lambda = 96$

wähle LWE-Instanz mit Bit-Hardness

$\eta = 110$

Bit-Hardness = Laufzeitabschätzung schnellster (klassischer oder quantum) Angriffe

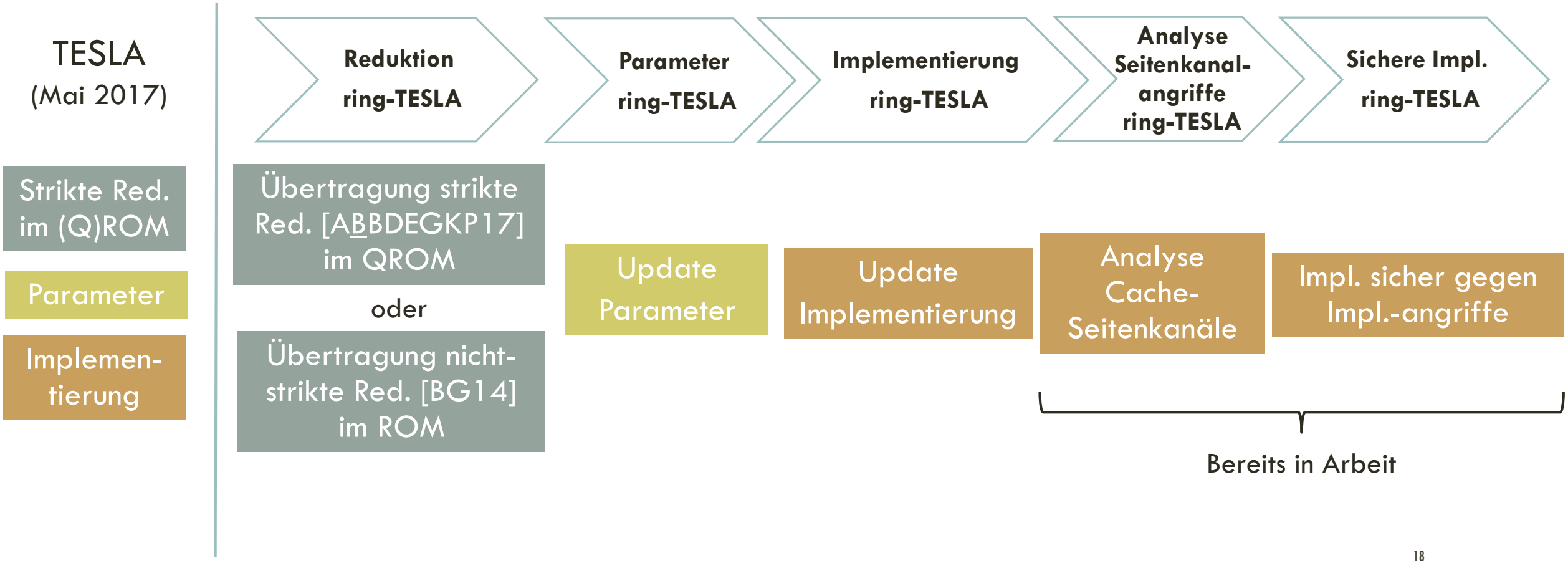
VERGLEICH SICHERHEITSEIGENSCHAFTEN

Signatur-verfahren	Jahr	Problem	ROM?	Strikt?	QROM?	Strikt?
GPV	2008	SIS	✓	✓	✓	✓
GLP	2012	DCK	✓	✗	-	-
GPV-poly	2013	R-SIS	✓	✓	✓	✓
BLISS	2013	R-SIS, NTRU	✓	✗	-	-
BG	2014	SIS, LWE	✓	✗	-	-
TESLA	2017	LWE	✓	✓	✓	✓

VERGLEICH EFFIZIENZ

Verfahren/ Instanziierung	Cycle counts [k-cycles]		Speicherplatz [kB]			Klassische Sicherheit
	Signierung	Verifikation	pk	sk	Sig.	[bit]
GPV	312 800	50 600	27 840	12 064	29	96
TESLA	27 244	5 375	4 808	2 895	1,9	96

GEPLANTE NÄCHSTE SCHRITTE



ZUSAMMENFASSUNG

- Entwicklung und aktuellen Forschungsstand von TESLA:
  - Gitterbasiertes Signaturverfahren
  - Strikte Reduktion von LWE im QROM
  - Parametervorschlag und Implementierung
- Nächste Schritte für ring-TESLA
  - Übertragung Ergebnisse TESLA
  - Sichere Implementierung

…mit dem Ziel der Einreichung beim NIST-PQ-Projekt

DANKE