Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Standardisierung von Post-Quanten-Kryptografie

Dr. Stephan Ehlen

Bundesamt für Sicherheit in der Informationstechnik, Referat KM 21

Omnisecure, Berlin, 24. Januar 2024

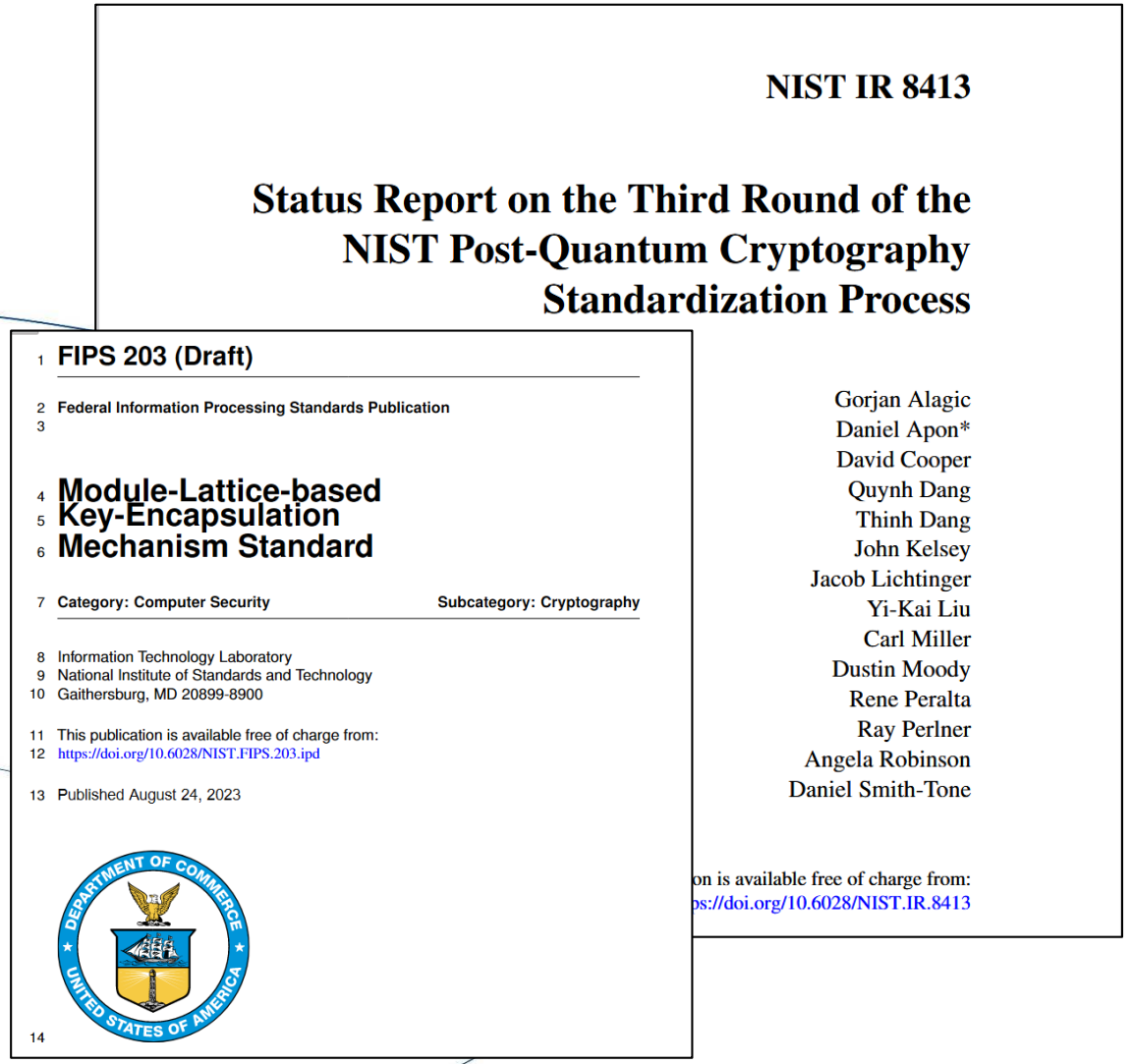
Standardisierung: NIST-Prozess („A long and winding road“)

Standardisierung: NIST-Prozess

August 2023: Drafts für FIPS 203, 204, 205:
1 KEM: **ML-KEM** (CRYSTALS-Kyber)

3 Signaturverfahren:
ML-DSA (CRYSTALS-Dilithium)
SLH-DSA (SPHINCS+),
Falcon (später),

Aktuell:
- Weitere Ausschreibung für Signaturverfahren
- 4. Runde (BIKE, HQC, Classic McEliece, ~~SIKE~~)



NIST IR 8413

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Daniel Apon*
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone

on is available free of charge from:
ps://doi.org/10.6028/NIST.IR.8413

FIPS 203 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

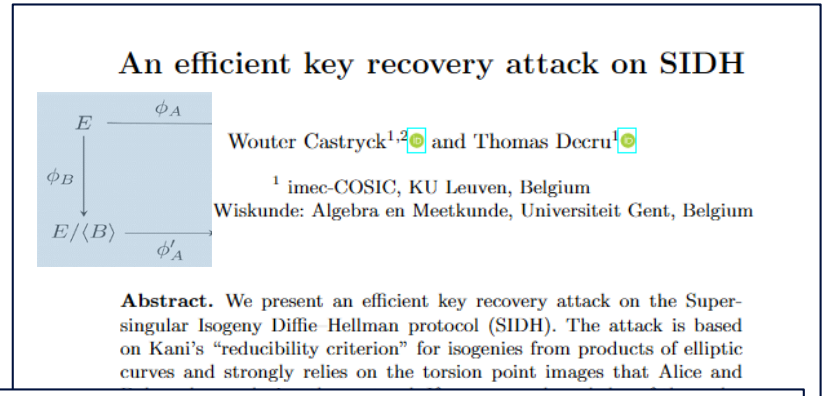
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203.ipd

Published August 24, 2023

DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA

Entwicklungen während des NIST-Prozesses

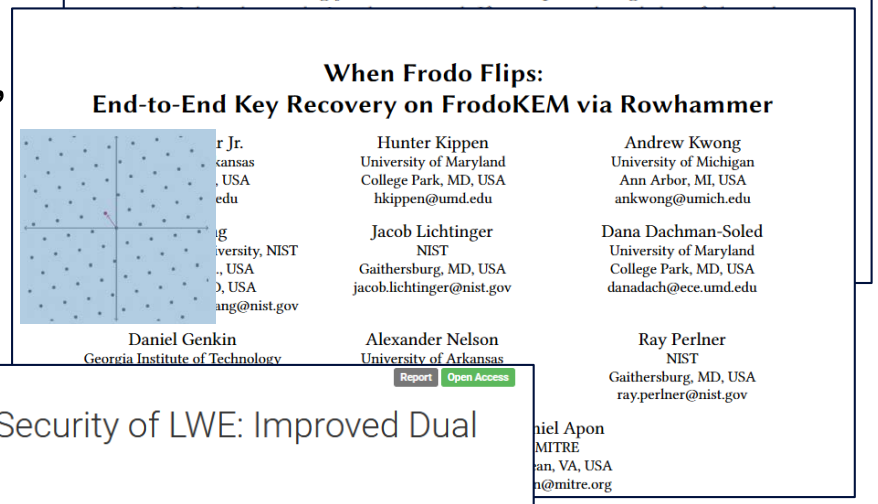
- Viel Aufmerksamkeit und Forschungsaktivität
- Einige Verfahren komplett gebrochen
- Beullens 2022: “Breaking Rainbow Takes a Weekend on a Laptop”
- Castryck, Decru 2022: “An Efficient Key Recovery Attack on SIDH”
- Verbesserte Gitterangriffe
- Seitenkanalattacken


An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

Abstract. We present an efficient key recovery attack on the Supersingular Isogeny Diffie Hellman protocol (SIDH). The attack is based on Kani’s “reducibility criterion” for isogenies from products of elliptic curves and strongly relies on the torsion point images that Alice and


When Frodo Flips:
End-to-End Key Recovery on FrodoKEM via Rowhammer

Hunter Kippen
University of Maryland
College Park, MD, USA
hkippen@umd.edu

Andrew Kwong
University of Michigan
Ann Arbor, MI, USA
ankwong@umich.edu

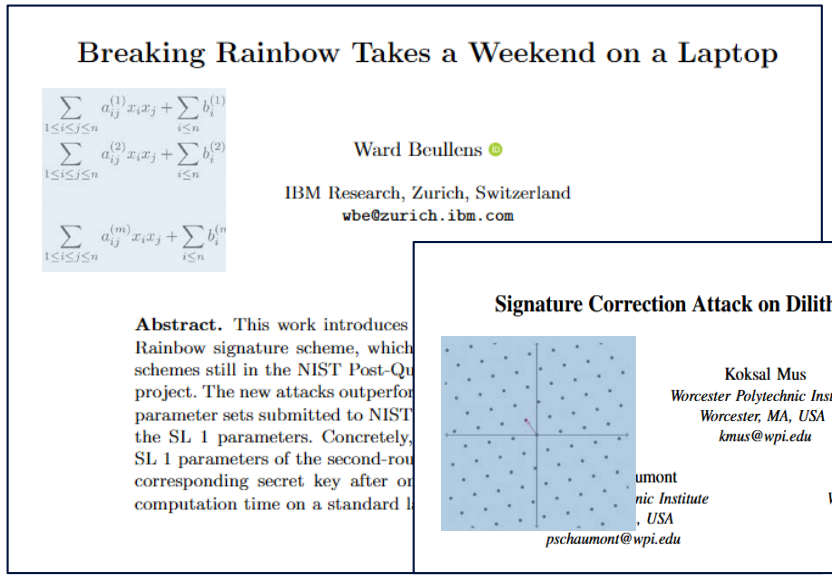
Jacob Lichtinger
NIST
Gaithersburg, MD, USA
jacob.lichtinger@nist.gov

Dana Dachman-Soled
University of Maryland
College Park, MD, USA
danadach@ece.umd.edu

Daniel Genkin
Georgia Institute of Technology

Alexander Nelson
University of Arkansas

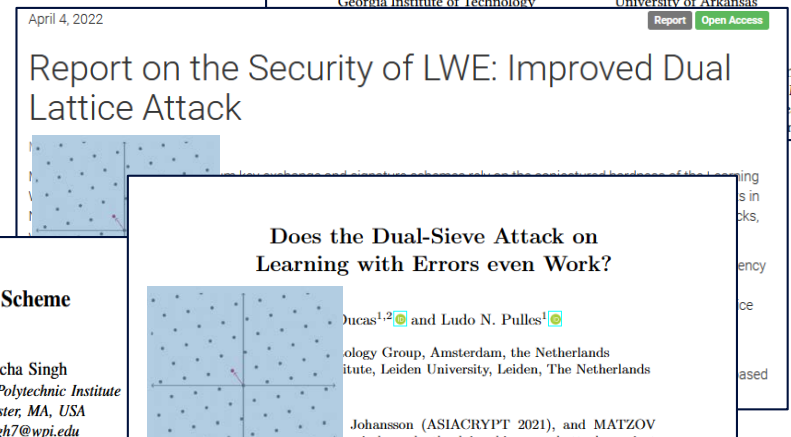
Ray Perlner
NIST
Gaithersburg, MD, USA
ray.perlner@nist.gov


Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces
Rainbow signature scheme, which
schemes still in the NIST Post-Qu
project. The new attacks outperfor
parameter sets submitted to NIST
the SL 1 parameters. Concretely,
SL 1 parameters of the second-rou
corresponding secret key after o
computation time on a standard l


April 4, 2022
Report
Open Access
Report on the Security of LWE: Improved Dual Lattice Attack

Signature Correction Attack on Dilithium Signature Scheme

Koksal Mus
Worcester Polytechnic Institute
Worcester, MA, USA
kmus@wpi.edu

Richa Singh
Worcester Polytechnic Institute
Worcester, MA, USA
rsingh7@wpi.edu

Berk Sunar
Worcester Polytechnic Institute
Worcester, MA, USA
sunar@wpi.edu

pschaumont@wpi.edu

Does the Dual-Sieve Attack on
Learning with Errors even Work?

Johansson (ASIACRYPT 2021), and MATZOV
follow up work in this line adding new practical improvements.
However, from a theoretical perspective, all of these works are painfully specific to Learning with Errors, while the principle of the Dual-Sieve attack is more general (Laarhoven & Walter, CT-RSA 2021). More critically, all of these works are based on heuristics that have received very little theoretical and experimental attention.

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Post-Quanten-Kryptografie - Empfehlungen

- Seit 2020 empfiehlt das BSI erste Post-Quanten-Verfahren
- Im Jahr 2021 hat das BSI den Leitfaden Kryptografie quantensicher gestalten veröffentlicht

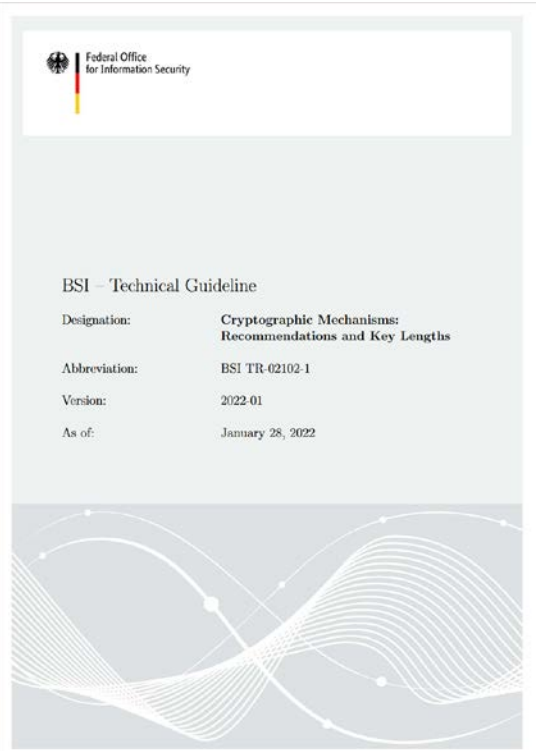
- Empfohlene Verfahren in der TR-02102-1:
  - FrodoKEM
  - Classic McEliece
  - Hashbasierte Signaturverfahren

→ https://www.bsi.bund.de/PQ-Migration

BSI-Empfehlungen: Ausblick 2024/2025

- Schlüsselkapselung:
  - FrodoKEM und Classic McEliece
  - ML-KEM *(nach* Prüfung des finalen Standards*)*
- Signaturverfahren:
  - ML-DSA *(nach* Prüfung des finalen Standards*)*
  - SLH-DSA *(nach* Prüfung des finalen Standards*)*
  - LMS/HSS und XMSS/XMSS^MT
- *Parameter: NIST level 3 und 5*
- PQC nur in *hybriden Lösungen*,

  also PQC + “klassisch”, außer für hashbasierte Signaturen


Federal Office for Information Security

BSI – Technical Guideline

Designation:	Cryptographic Mechanisms: Recommendations and Key Lengths
Abbreviation:	BSI TR-02102-1
Version:	2022-01
As of:	January 28, 2022

Standardisierung: ISO/IEC, IETF/IRTF

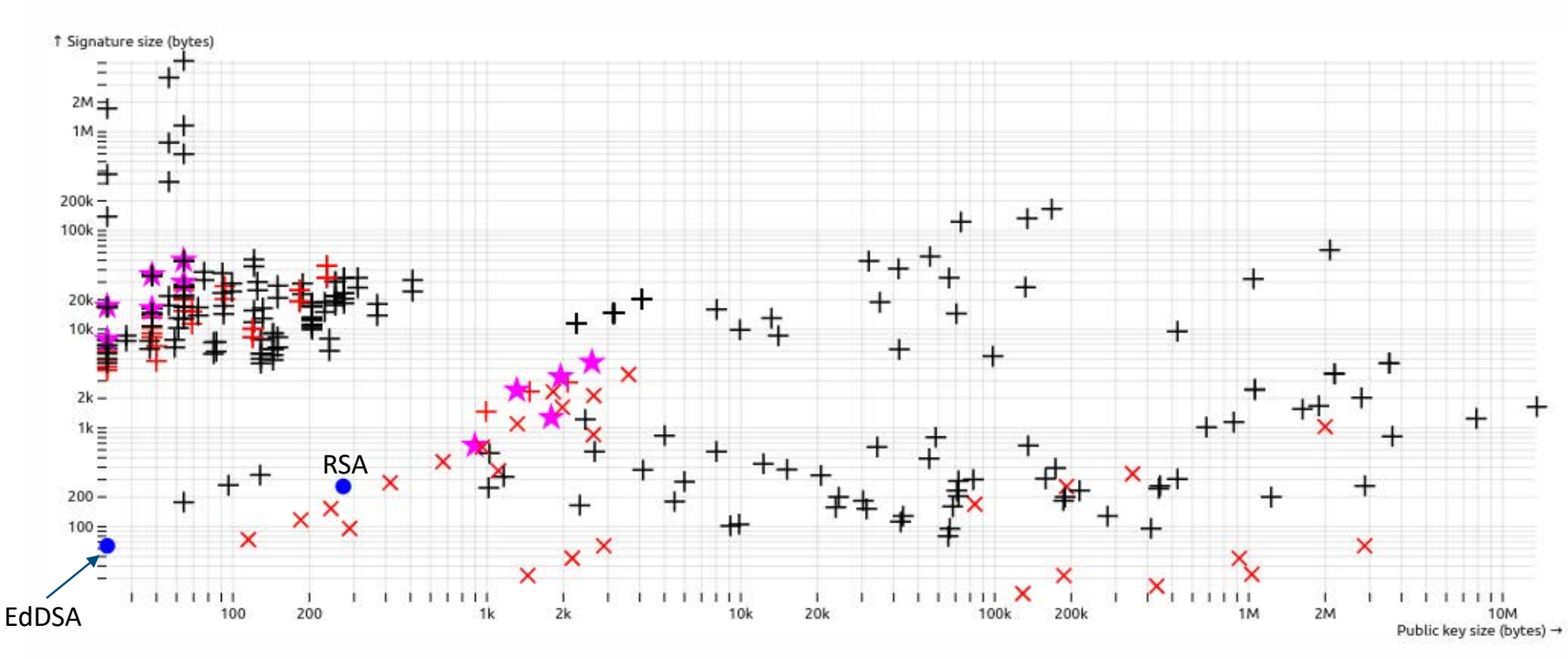
- ISO/IEC 18033-2 (AMD2):
  Standardisierung (auf BSI-Initiative) von PQ-Verfahren zur Schlüsseleinigung
  - **FrodoKEM, Classic McEliece** und **CRYSTALS-Kyber**

- Viele Standardisierungs-Aktivitäten in IETF/IRTF, z.B.:
  - Neue Arbeitsgruppe Post-Quantum Use In Protocols (pquip)
  - OpenPGP: **draft-wussler-openpgp-pqc** (aus BSI-Projekt entstanden, call for adoption)
  - draft-ounsworth-pq-composite-sig (derzeit nicht von LAMPS adoptiert)
  - LAMPS: draft-lamps-pq-composite-kem
    draft-ietf-lamps-cms-kyber, draft-ietf-lamps-cms-sphincs-plus, draft-ietf-lamps-dilithium-certificates, draft-ietf-lamps-kyber-certificates
  - X.509: **draft-gazdag-x509-hash-sigs** (Kooperation BSI-genua, call for adoption kommt)
  - TLS 1.3: draft-ietf-tls-hybrid-design
  - IKEv2: RFC9370
  - CFRG: **draft-ounsworth-cfrg-kem-combiners** (BSI-Beteiligung)

NIST-Verfahren für weitere Signaturverfahren

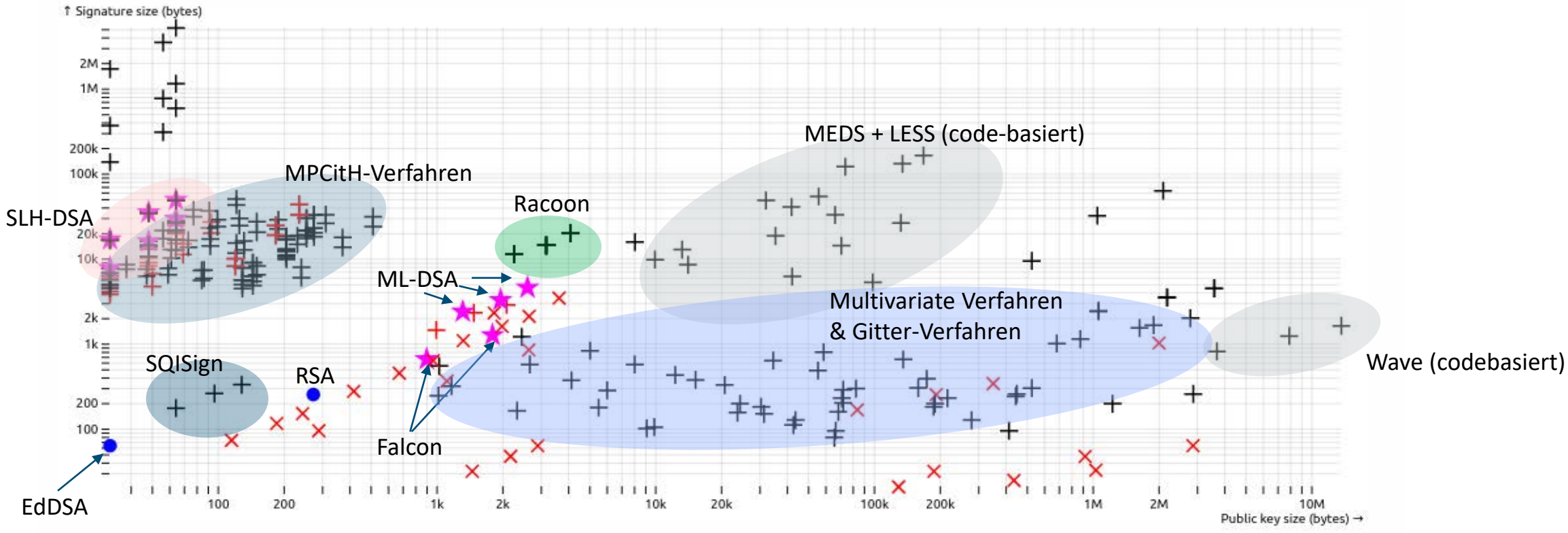
- NIST hat dazu aufgerufen, weitere Signaturverfahren einzureichen
- Hintergrund: Suche nach effizienten Verfahren, die nicht auf strukturierten Gittern beruhen
- Es sind aktuell 40 Verfahren in der ersten Runde, einige schon gebrochen
- Davon:
  - Code-basiert: 6
  - Isogenie-basiert: 1
  - Gitter-basiert: 7
  - MPC-in-the-Head: 7
  - Multivariat: 10
  - Auf symmetrischen Primitiven beruhend: 4
  - Andere: 5

NIST-Verfahren für weitere Signaturverfahren



Quelle: https://pqshield.github.io/nist-sigs-zoo/

NIST-Verfahren für weitere Signaturverfahren



x: gebrochen

Quelle: https://pqshield.github.io/nist-sigs-zoo/

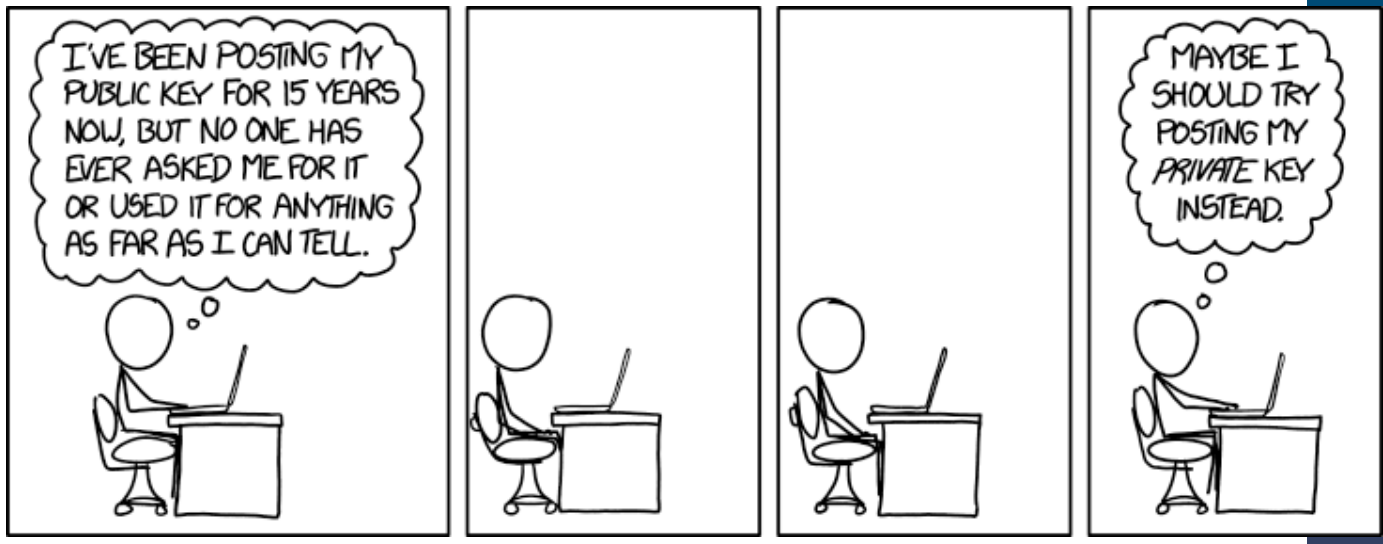
Fazit

Deutschland
Digital•Sicher•BSI•

- Der kryptografische Umbruch hat begonnen.
- Aber: es gibt auch bei der Standardisierung noch sehr viele Aufgaben zu lösen.
- Kryptoagilität sollte ein Designkriterium sein!
- Umstellung auf hybride Verfahren anstatt Ersatz der klassischen Verfahren.
- Inventur, Risikobewertung und Planung sind bereits jetzt möglich.

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•



Kontakt

Dr. Stephan Ehlen

stephan.ehlen@bsi.bund.de

quantum@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de