NIST PQC STANDARDIZATION

THOMAS ATTEMA & MATTHIEU LEQUESNE

21 April 2022

MITIGATE THE THREAT OF QUANTUM COMPUTERS

Standardize cryptosystems for classical computers believed to be resistant to attacks from both classical and quantum computers

PQC STANDARDIZATION PROCESS

TIMELINE

2016: Call for Submissions

2017 (Round 1):
69 out of 82 submission accepted

2019 (Round 2):
26 candidates

2020 (Round 3):
7 finalists
8 alternates

End 2021:
4/5 primitives selected

2022:
New call for Signatures

2022 – 2023:
Draft Standards

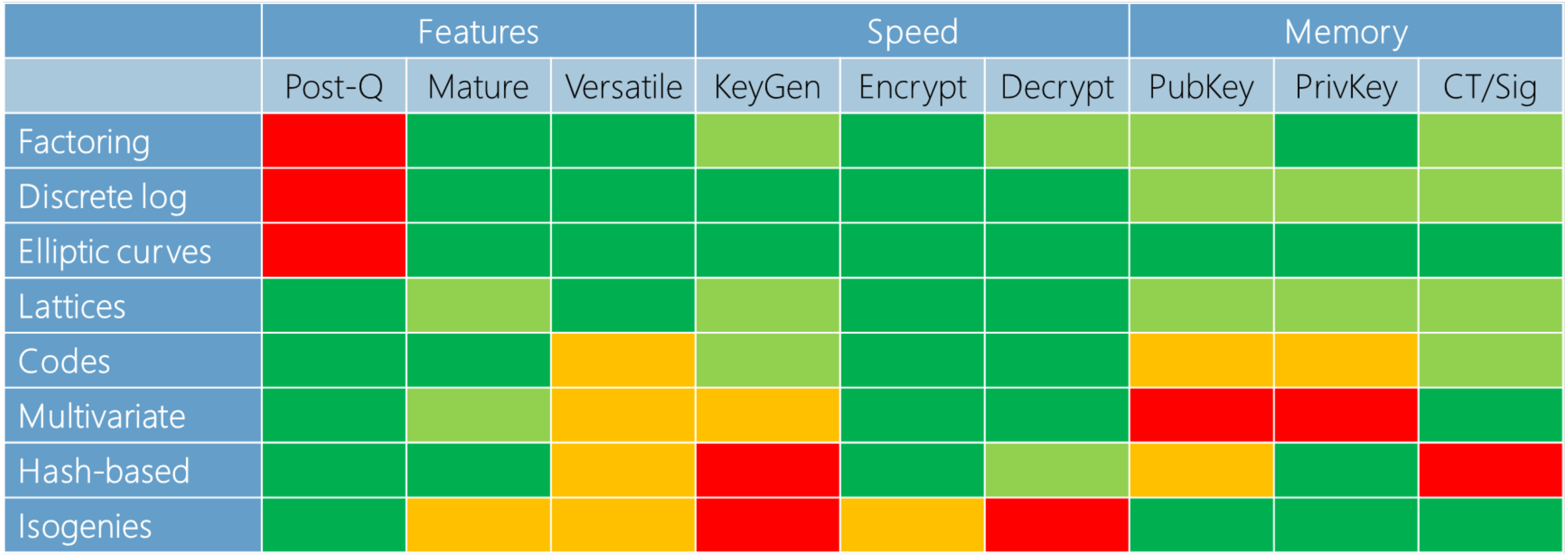
2022:
Round 4 for alternates

2024:
Standards Publication

ROUND 3 FINALISTS

	Signature		Encryption	
	Finalist	Alternate	Finalist	Alternate
Lattice	Dilithium Falcon		Kyber NTRU SABER	FrodoKEM NTRU Prime
Code			McEliece	Bike HQC
Multivariate	Rainbow	GeMSS		
Hash/Symmetric		Picnic SPHINCS+		
Isogeny				SIKE
Total	3	3	4	5

COMPARISON BETWEEN THE TYPES OF PRIMITIVES



OTHER PQC INITIATIVES

Migration zu
Post-Quanten-Kryptografie

Handlungsempfehlungen des BSI

Stand: August 2020

- NBV/BSI recommendations for early adopters
  - FrodoKEM
  - McEliece
- IEEE, ETSI, IETF, ISO, …
- Initiatives in other countries
- …

ATTACK ON RAINBOW
FEBRUARY 21, 2022

- Impact:
  - Still exponential complexity
  - Shift in parameters
  - Only impacts the multivariate schemes

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

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

NEW CALL FOR PQC SIGNATURES
MAIN GOAL: DIVERSIFY THE SIGNATURE PORTFOLIO

- Little diversity in round 3
  - Both multivariate schemes suffered attack improvements (Rainbow and GeMSS)

- NIST might standardize the alternate signature candidate SPHINCS+

- Call opens shortly after coming NIST announcement
  - Submission deadline: January 2023

ISOGENY BASED KEY EXCHANGE BECOMING FASTER

MARCH 18, 2022: ~30% SPEED-UP

Efficient Algorithms for Large Prime Characteristic Fields and Their Application to Bilinear Pairings and Supersingular Isogeny-Based Protocols

Patrick Longa

Microsoft Research, USA
plonga@microsoft.com

IMPROVED DUAL LATTICE ATTACK
APRIL 4, 2022: BY MATZOV – ISRAEL

Report on the Security of LWE:
Improved Dual Lattice Attack

The Center of Encryption and Information Security – MATZOV*†
IDF

OPENSSH 9.0
APRIL 8, 2022 - HYBRID ENCRYPTION BY DEFAULT

- One of the first PQC in production
  - Mitigates *store-now-decrypt-later* attacks
- NTRU Prime - Alternate NIST candidate
  - Neither a conservative choice
  - Nor a NIST finalist

THANK YOU FOR YOUR TIME

TNO innovation for life

CWI