TNO innovation for life

NIST – PQC STANDARDISATION

DRS IR MARAN VAN HEESCH

maran.vanheesch@tno.nl

Source image: NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST

EXCITEMENT DURING SUMMER!!

NIST

CSRC MENU

Search CSRC

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

UPDATES 2022

PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

July 05, 2022

Summary

NIST has completed the third round of the Post-Quantum Cryptography (PQC) standardization process, which selects public-key cryptographic algorithms to protect information through the advent of quantum computers. A total of four candidate algorithms have been selected for standardization, and four additional algorithms will continue into the fourth round.

THE FOUR CANDIDATES TO BE STANDARDIZED

Algorithms to be Standardized	
Public-Key Encryption/KEMs	**Digital Signatures**
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS$^+$

MIGRATION PLAN

Ramping up

1.become familiar with subject
2.create awareness
3.form a project group

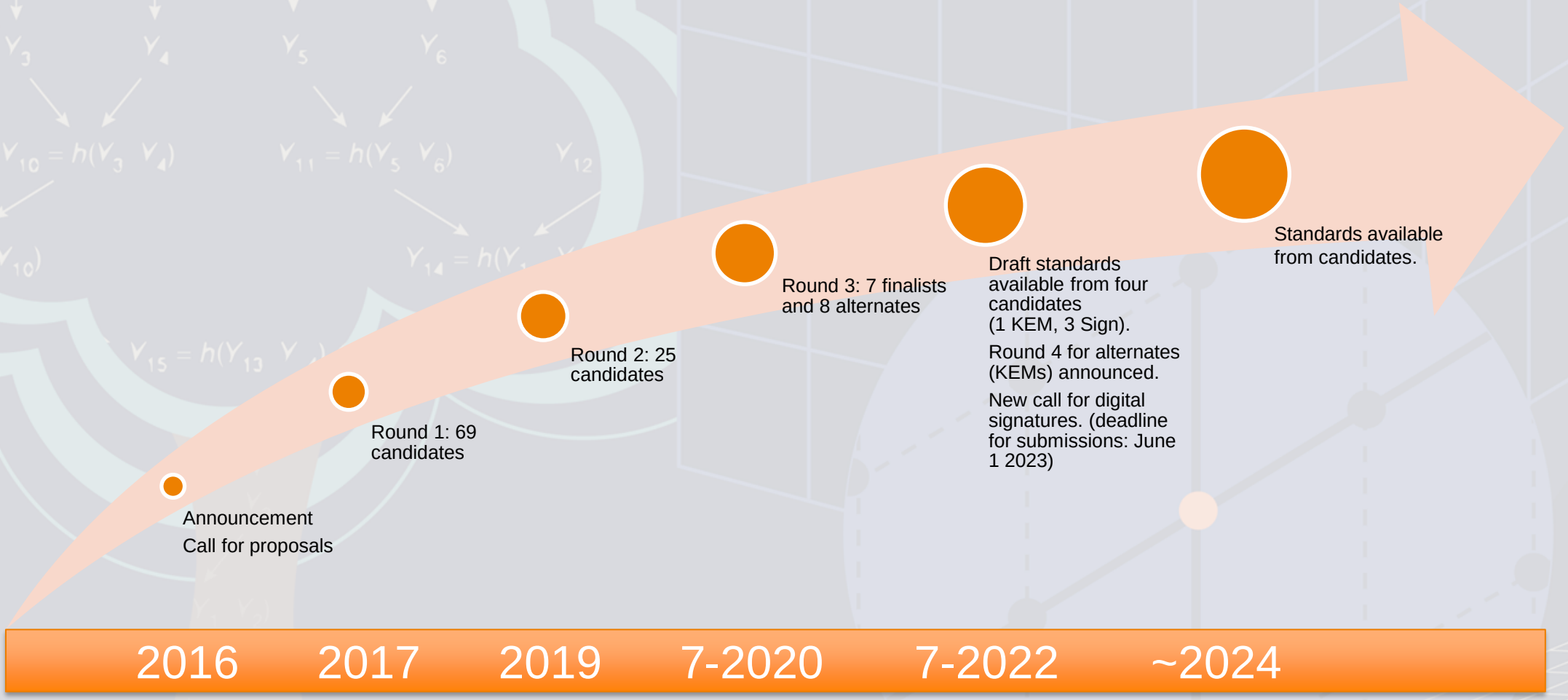
Initial no-regret moves

1.create a list of assets to be migrated
2.migration planning
3.migrate symmetric cryptography and hash functions

Replace asymmetric crypto

1.selection of algorithms
2.hybrid solutions
3.quantum-safe only solutions

REALISTIC STANDARDISATION TIMELINE



FOURTH ROUND CANDIDATES

PQC Fourth Round Candidate Key-Establishment Mechanisms (KEMs)

The following candidate KEM algorithms will advance to the fourth round:

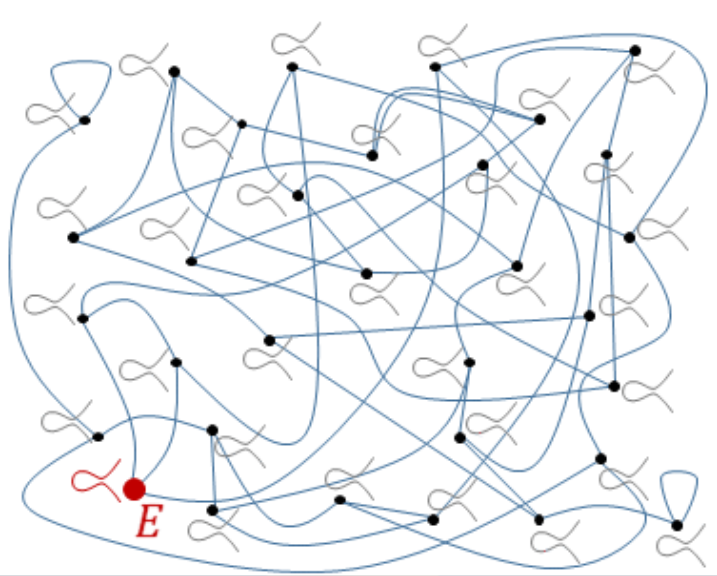
Public-Key Encryption/KEMs
BIKE
Classic McEliece
HQC
SIKE

FOURTH ROUND CANDIDATES

PQC Fourth Round Candidate Key-Establishment Mechanisms (KEMs)

The following candidate KEM algorithms will advance to the fourth round:

Public-Key Encryption/KEMs
BIKE
Classic McEliece
HQC
SIKE



The SIKE algorithm is broken (taking only hours), but was still in the running in the fourth round of the NIST standardization effort.

Research is still required!

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

COULDA BEEN A CONTENDER —

Post-quantum encryption contender is taken out by single-core PC and 1 hour

Leave it to mathematicians to muck up what looked like an impressive new algorithm.

DAN GOODIN - 8/2/2022, 2:31 PM

Figure: https://www.esat.kuleuven.be/cosic/elliptic-curves-are-quantum-dead-long-live-elliptic-curves/

THE FOUR CANDIDATES TO BE STANDARDIZED - A CLOSER LOOK

Algorithms to be Standardized	
Public-Key Encryption/KEMs	**Digital Signatures**
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS$^+$



MIGRATION PLAN

Ramping up

1.become familiar with subject
2.create awareness
3.form a project group

Initial no-regret moves

1.create a list of assets to be migrated
2.migration planning
3.migrate symmetric cryptography and hash functions

Replace asymmetric crypto

1.selection of algorithms
2.hybrid solutions
3.quantum-safe only solutions

WHICH SIGNATURE SCHEME TO CHOSE?

Signature scheme	Primitive	Time to sign	Time to verify	Signature size	Implementation difficulty	Maturity
Dilithium	Lattices					
Falcon	Lattices					
SPHINCS$^+$	Hash-based					

good | fair | poor | bad

Maran van Heesch maran.vanheesch@tno.nl

Leo Ducas l.ducas@cwi.nl

Thomas Prest thomas.prest@pqshield.com

Andreas Hülsing andreas@huelsing.net