PROMETHEUS

PRivacy preserving pOst-quantuM systEms from
advanced crypTograpHic mEchanisms Using latticeS

NIST PQC Project – Current Status

Damien Stehlé, ENS Lyon

Prometheus Industrial Workshop – 28/06/2022

This project has received funding from the European
Union's Horizon 2020 research and innovation programme
under grant agreement No 780701.

PQC project timeline

April 2015: NIST announces future standardization

Nov 2017: Submission ddl, 82 submissions

Dec 2017: Round 1 starts, 69 complete and proper submissions 49 PKE/KEM 20 SIG

(Jan 2018: start of PROMETHEUS)

Jan 2019: Round 2 starts, 26 submissions left 17 PKE/KEM 9 SIG

July 2020: Round 3 starts, 7 finalists, 8 alternates 4(+5) PKE/KEM 3(+3) SIG

Imminent… since the end of 2021: (part of the) selection of future standards

The remaining candidates

7 finalists

PKE/KEM	SIG
Kyber - lattices	**Dilithium** - lattices
McEliece - codes	**Falcon** - lattices
NTRU - lattices	Rainbow* - alg eqs
Saber - lattices	

8 alternates

PKE/KEM	SIG
BIKE - codes	GeMSS - alg eqs
FRODO - lattices	Picnic - hash functions
HQC - codes	SPHINCS+ - hash functions
NTRUPrime - lattices	
SIKE - isogenies	

In bold: candidates coauthored by a Prometheus member
*Rainbow underwent a severe cryptanalysis [Beullens'22]

Purpose of alternates: standardize later, fallback solutions, diversity of assumptions

What about lattices?

Among all types of assumptions, lattices are the most successful:

- ❖ 5 finalists out of 7 (3/4 PKE/KEM and 2/3 SIG)
- ❖ The 3rd SIG finalist and a SIG alternate have suffered significant security losses [Beullens'22]
- ❖ The remaining PKE/KEM finalist has public keys orders of magnitude larger

NIST has stated its intention to standardize at most one lattice PKE/KEM, and at most one lattice SIG:

- ❖ It is likely that one lattice PKE/KEM will be standardized (1/3 chance for PROMETHEUS)
- ❖ It is very likely that one lattice SIG will be standardized (2/2 chances for PROMETHEUS)

Are these algebraic lattices? Yes!

Algebraic lattices are a subclass of lattices coming from algebraic number theory

- ❖ More structure
- ❖ Faster and more compact cryptographic constructions
- ❖ Possibility of dedicated attacks   (yet to be found)

What to use?

- ❖ All 5 lattice NIST finalists rely on algebraic lattices
- ❖ BSI recommends the non-algebraic alternate FrodoKEM (and Classic McEliece)
- ❖ Personal view: the BSI position is hard to justify
  - ❖ 10x larger ciphertexts to prevent against non-existing attacks
  - ❖ algebraic lattices have been around for 25 years without attacks
  - ❖ to get higher security, better increase the parameters of the algebraic finalists

Next steps

“Imminent”: NIST will probably announce one or two standards for each category

On-ramp for SIG: re-opening of the SIG competition, with new candidates

- ❖ NIST wants signatures based on well-established designs/assumptions
- ❖ It wants alternative hardness assumptions
- ❖ Unclear whether non-algebraic lattices will be allowed or not

Draft standards released in 2023 (?)

In the meantime, for critical applications: hybrid implementations
classical + post-quantum

QUESTIONS?