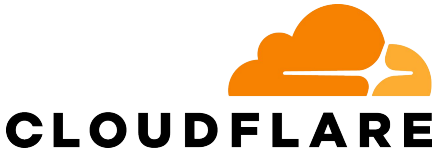

New Post-Quantum Signatures on the Horizon

Bas Westerbaan & Thom Wiggers

NIST Signatures

- 1st PQC Competition
  - Announced 2016
  - First round started 2017
  - Finalists selected July 2022
    - Dilithium
    - Falcon
    - SPHINCS+
  - Draft standards expected soon

Quick recap: the current choices

	Sizes (bytes)		Speed compared to P-256		Note
	Sig.	**Pub. key**	**Sign**	**Verify**	
Dilithium2	2,420	1,312	2.5	0.3	General purpose, but large sizes.
Falcon512	666	897	5 ⚠	0.3	Fast signing requires floating point arithmetic, which is vulnerable to timing attacks. Not suitable for online signatures.
SPHINCS⁺-128s	7,856	32	3,000	1.7	Security well understood. No need for hybrid.
SPHINCS⁺-128f	17,088	32	200	4	
XMSS_20_128 ⚠	900	32	10	2	128 bit variants not standardized. No non-repudiation. Requires keeping state.

WebPKI drop-in with just Dilithium: **+17kB** (including 2 SCTs)
Dilithium for handshake and Falcon for rest: **+9kB**.

Quick recap: coping mechanisms

- Suppressing intermediates (part 2, part 3).
  Ship yearly list of intermediates to clients. Saves ~2–3 kB.
- AuthKEM (aka KEMTLS)
  Use KEM in leaf cert. Big change to TLS. Saves ~3 kB.
- Merkle Tree Certificates
  Replace all certs/SCTs/OCSP by single authentication path (~700b). Requires delayed issuance & update mechanism on clients. Big change to WebPKI. Only handshake signature remains.

(Most combinations of these approaches are possible)

Better PQ signature would be great and NIST agrees

- NIST signatures on-ramp
  - Diversity cryptographic assumptions
    - Dilithium / Falcon both based on structured lattices
  - Announced mid 2022
  - 1st round started July 2023 ← You are here
  - First standards expected ?? (well after 2025)

"We are most interested in a general-purpose digital signature scheme which is not based on structured lattices
• We may be interested in other signature schemes targeted for certain applications. For example, a scheme with very short signatures."

- Dustin Moody (NIST), "NIST PQC: LOOKING INTO THE FUTURE", Fourth PQC Standardization Conference [Virtual]

40 submissions

- Code-based
  - Enhanced pqsigRM
  - FuLeeca
  - LESS
  - MEDS
  - Wave
- Isogenies
  - SQISign
- Lattices
  - EHT
  - EagleSign
  - HAETAE
  - HAWK
  - HuFu
  - Raccoon
  - Squirrels
- MPC-in-the-Head
  - CROSS
  - MIRA
  - MQOM
  - MiRitH
  - PERK
  - RYDE
  - SDitH
- Symmetric
  - AIMer
  - Ascon-Sign
  - FAEST
  - SPHINCS-alpha
- Multivariate
  - 3WISE
  - Biscuit
  - DME-Sign
  - HPPC
  - MAYO
  - PROV
  - QR-UOV
  - SNOVA
  - TUOV
  - UOV
  - VOX
- Other
  - ALTEQ
  - KAZ-Sign
  - PREON
  - Xifrat1-Sign.I
  - eMLE-Sig 2.0

40 submissions: the first eliminations (July 19th)

- Code-based
  - Enhanced pqsigRM
  - ~~FuLeeca~~
  - LESS
  - MEDS ⚠️
  - Wave
- Isogenies
  - SQIsign
- Lattices
  - EHT
  - ~~EagleSign~~
  - HAETAE
  - HAWK
  - HuFu
  - Raccoon
  - Squirrels
- MPC-in-the-Head
  - CROSS
  - MIRA
  - MQOM
  - MiRitH
  - PERK
  - RYDE
  - SDitH
- Symmetric
  - AIMer
  - Ascon-Sign
  - FAEST
  - SPHINCS-alpha
- Multivariate
  - ~~3WISE~~
  - ~~Biscuit~~ ❓
  - DME-Sign
  - ~~HPPC~~
  - MAYO
  - PROV
  - QR-UOV
  - SNOVA
  - TUOV
  - UOV
  - VOX
- Other
  - ALTEQ ⚠️
  - ~~KAZ Sign~~
  - PREON
  - ~~Xifrat1-Sign.I~~
  - ~~eMLE-Sig 2.0~~

Submissions: verification < 5ms

- Code-based
  - Enhanced pqsigRM
  - ~~LESS~~
  - ~~Wave~~
- Isogenies
  - ~~SQIsign~~
- Lattices
  - EHT
  - HAETAE
  - HAWK
  - HuFu
  - Raccoon
  - Squirrels
- MPC-in-the-Head
  - CROSS
  - ~~MIRA~~
  - MQOM
  - MiRitH
  - PERK
  - RYDE
  - SDitH
- Symmetric
  - AIMer
  - Ascon-Sign
  - FAEST
  - SPHINCS-alpha
- Multivariate
  - DME-Sign
  - MAYO
  - ~~PROV~~
  - ~~QR-UOV~~
  - ~~SNOVA~~
  - TUOV
  - UOV
  - VOX
- Other
  - ~~PREON~~

Note: based on current, often not exactly optimized, performance metrics.

Submissions: signature < 3000 bytes

- Code-based
  - Enhanced pqsigRM
- Lattices
  - EHT
  - HAETAE
  - HAWK
  - HuFu
  - ~~Raccoon~~
  - Squirrels
- MPC-in-the-Head
  - ~~CROSS~~
  - ~~MQOM~~
  - ~~MiRitH~~
  - ~~PERK~~
  - ~~RYDE~~
  - ~~SDitH~~
- Symmetric
  - ~~AIMer~~
  - ~~Ascon-Sign~~
  - ~~FAEST~~
  - ~~SPHINCS-alpha~~
- Multivariate
  - DME-Sign
  - MAYO
  - TUOV
  - UOV
  - VOX

Certificate usage: public key + sig < 4 KB (Dilithium)

- Code-based
  - ~~Enhanced pqsigRM~~
- Lattices
  - EHT
  - HAETAE
  - HAWK
  - ~~HuFu~~
  - ~~Squirrels~~
- Multivariate
  - DME-Sign
  - MAYO
  - ~~TUOV~~
  - ~~UOV~~
  - ~~VOX~~

Certificate usage

Scheme	Category	Parameterset	NIST level	Pk bytes	Sig bytes	pk+sig	Sign (cycles)	Verify (cycles)
EdDSA ⚠	Pre-Quantum	Ed25519	Pre-Q	32	64	96	42,000	130,000
DME-Sign	Multivariate	2^32	1	1,449	32	1,481	50,000	25,000
MAYO	Multivariate	one	1	1,168	321	1,489	460,978	175,158
Falcon	Lattices	512	1	897	666	1,563	1,009,764	81,036
HAWK	Lattices	512	1	1,024	555	1,579	85,372	148,224
[illegible]	Code-based	[illegible]	[illegible]	[illegible]	1,100	[illegible]	[illegible]	[illegible]
HAETAE	Lattices	120	2	992	1,463	2,455	6,253,166	387,594
Dilithium	Lattices	II	2	1,312	2,420	3,732	333,013	118,412

SCT / root usage: sig < 666 bytes (Falcon)

- Code-based
  - Enhanced pqsigRM
- Lattices
  - EHT
  - ~~HAETAE~~
  - HAWK
  - ~~HuFu~~
  - ~~Squirrels~~
- Multivariate
  - DME-Sign
  - MAYO
  - TUOV
  - UOV
  - VOX

SCT / root usage

Scheme	Category	Parameterset	NIST level	Pk bytes	Sig bytes	pk+sig	Sign (cycles)	Verify (cycles)
DME-Sign	Multivariate	2^32	1	1,449	32	1,481	50,000	25,000
EdDSA ⚠️	Pre-Quantum	Ed25519	Pre-Q	32	64	96	42,000	130,000
TUOV	Multivariate	Is	1	65,552	80	65,632	272,394	570,194
UOV	Multivariate	Is-pkc	1	66,576	96	66,672	109,314	276,520
UOV	Multivariate	Is-classic	1	412,160	96	412,256	109,314	58,274
VOX	Multivariate	128	1	9,104	102	9,206	664,265	168,567
TUOV	Multivariate	Ip	1	42,608	112	42,720	220,792	491,120

(...)

SCT / root usage (cntd.)

Scheme	Category	Parameterset	NIST level	Pk bytes	Sig bytes	pk+sig	Sign (cycles)	Verify (cycles)
			(...)					
UOV	Multivariate	lp-pkc	1	43,576	128	43,704	105,324	224,006
UOV	Multivariate	lp-classic	1	278,432	128	278,560	105,324	90,336
EHTv3 / EHTv4	Lattices	v3-1	1	83,500	169	83,669	189,500,000	2,050,000
MAYO	Multivariate	two	1	5,488	180	5,668	563,900	91,512
MAYO	Multivariate	one	1	1,168	321	1,489	460,978	175,158
HAWK	Lattices	512	1	1,024	555	1,579	85,372	148,224
Falcon	Lattices	512	1	897	666	1,563	1,009,764	81,036

Concrete instances

- Only DME-Sign. Adds 3kB compared to P-256.
  (Completely mitigated by abridged compression.)
  Will DME-Sign survive the weekend?
- MAYO using the *one* variant for leaf/intermediate and *two* for the rest. Adds 3.3kB.
  Signing time much worse than P-256, but still <0.3ms.
  More trust in security than DME-Sign, but still uncertain.
- UOV `Is-pkc` for SCTs and roots and HAWK512 for the rest. Adds 3.2kB.
  66kB for stored UOV public keys. HAWK relies on Falcon's assumptions and then some.
- UOV `Is-pkc` for SCTs and roots and Dilithium2 for the rest. Adds 7.4kB.
  Relatively conservative choice.
- Bonus: SQISign only. Adds <0.5kB.
  Signing time of >1s, and verification time of >35ms.

Wrapping up

- Still no perfect drop-in post-quantum signatures on the horizon.
  But: several schemes, whose additional cost is much easier to mitigate for TLS/WebPKI, than the currently available schemes.
- We're very early in the process: performance metrics and security are still very uncertain.

Explore for yourself:

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