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

**DILITHIUM, FALCON, SPHINCS+**

**BUT WHAT ABOUT A SECOND COMPETITION FOR SIGNATURES?**
Quick recap: the current choices

<table>
<thead>
<tr>
<th>Sizes (bytes)</th>
<th>Speed compared to P-256</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig.</td>
<td>Pub. key</td>
<td>Sign</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>-----</td>
</tr>
<tr>
<td><strong>Dilithium2</strong></td>
<td>2,420</td>
<td>1,312</td>
</tr>
<tr>
<td><strong>Falcon512</strong></td>
<td>666</td>
<td>897</td>
</tr>
<tr>
<td><strong>SPHINCS⁺-128s</strong></td>
<td>7,856</td>
<td>32</td>
</tr>
<tr>
<td><strong>SPHINCS⁺-128f</strong></td>
<td>17,088</td>
<td>32</td>
</tr>
<tr>
<td><strong>XMSS_20_128</strong></td>
<td>900</td>
<td>32</td>
</tr>
</tbody>
</table>

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
  • 1\textsuperscript{st} 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
  - SQI-sign

- 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.1
  - 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

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Category</th>
<th>Parameterset</th>
<th>NIST level</th>
<th>Pk bytes</th>
<th>Sig bytes</th>
<th>pk+sig</th>
<th>Sign (cycles)</th>
<th>Verify (cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EdDSA</td>
<td>Pre-Quantum</td>
<td>Ed25519</td>
<td>Pre-Q</td>
<td>32</td>
<td>64</td>
<td>96</td>
<td>42,000</td>
<td>130,000</td>
</tr>
<tr>
<td>DME-Sign</td>
<td>Multivariate</td>
<td>$2^{32}$</td>
<td>1</td>
<td>1,449</td>
<td>32</td>
<td>1,481</td>
<td>50,000</td>
<td>25,000</td>
</tr>
<tr>
<td>MAYO</td>
<td>Multivariate</td>
<td>one</td>
<td>1</td>
<td>1,168</td>
<td>321</td>
<td>1,489</td>
<td>460,978</td>
<td>175,158</td>
</tr>
<tr>
<td>Falcon</td>
<td>Lattices</td>
<td>512</td>
<td>1</td>
<td>897</td>
<td>666</td>
<td>1,563</td>
<td>1,009,764</td>
<td>81,036</td>
</tr>
<tr>
<td>HAWK</td>
<td>Lattices</td>
<td>512</td>
<td>1</td>
<td>1,024</td>
<td>555</td>
<td>1,579</td>
<td>85,372</td>
<td>148,224</td>
</tr>
<tr>
<td>FulDec</td>
<td>Code-based</td>
<td></td>
<td>1</td>
<td>5,000</td>
<td>1,100</td>
<td>2,150</td>
<td>6,253,166</td>
<td>387,594</td>
</tr>
<tr>
<td>HAETAE</td>
<td>Lattices</td>
<td>120</td>
<td>2</td>
<td>992</td>
<td>1,463</td>
<td>2,455</td>
<td>6,253,166</td>
<td>387,594</td>
</tr>
<tr>
<td>Dilithium</td>
<td>Lattices</td>
<td>II</td>
<td>2</td>
<td>1,312</td>
<td>2,420</td>
<td>3,732</td>
<td>333,013</td>
<td>118,412</td>
</tr>
</tbody>
</table>
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

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

(...)

# SCT / root usage (cntd.)

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