AND THEN THERE WERE FOUR: THE FIRST NIST PQC STANDARDS

Dustin Moody
NIST PQC Team

Sept. 27, 2023
MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 2023
NIST public-key crypto standards
- **SP 800-56A**: Diffie-Hellman, ECDH
- **SP 800-56B**: RSA encryption
- **FIPS 186**: RSA, DSA, and ECDSA signatures

All vulnerable to attacks from a (large-scale) quantum computer.

Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically.
NIST CALLED FOR QUANTUM-RESISTANT CRYPTOGRAPHIC ALGORITHMS FOR NEW PUBLIC-KEY CRYPTO STANDARDS
  - DIGITAL SIGNATURES
  - ENCRYPTION/KEY-ESTABLISHMENT

OUR ROLE: MANAGING A PROCESS OF ACHIEVING COMMUNITY CONSENSUS IN AN OPEN, TRANSPARENT, AND TIMELY MANNER

DIFFERENT AND MORE COMPLICATED THAN PAST AES/SHA-3 COMPETITIONS

THERE WOULD NOT BE A SINGLE “WINNER”
  - IDEALLY, SEVERAL ALGORITHMS WILL EMERGE AS ‘GOOD CHOICES’
ROUND 3 RESULTS

<table>
<thead>
<tr>
<th>3rd round selection (KEM)</th>
<th>3rd round selection (Signatures)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRYSTALS-Kyber</td>
<td>CRYSTALS-Dilithium, Falcon, SPHINCS+</td>
</tr>
</tbody>
</table>

See [NISTIR 8413](https://nvlpubs.nist.gov/nistpubs/ers/er08413.pdf), Status Report on the 3rd Round of the NIST PQC Standardization Process, for the rationale on the selections.

4th round candidates (all KEMs) evaluated for 18-24 months
- ClassicMcEliece
- BIKE
- HQC
- SIKE

On-ramp signatures
- NIST issued a new call for additional signatures — preferably for signatures based on non-lattice problems
• The 5th NIST PQC Standardization Conference
  • April 10-12, 2024 in Rockville, Maryland

• Draft standards for public comment released Aug 2023
  • Deadline for comments: November 22, 2023

• The first PQC standards should be published in 2024
THE 1ST PQC STANDARDS

- FIPS 203: ML-KEM (KYBER)
- FIPS 204: ML-DSA (DILITHIUM)
- FIPS 205: SLH-DSA (SPHINCS+)
- FN-DSA (FALCON) – UNDER DEVELOPMENT
  - WILL HAVE OTHER DOCS WITH MORE GUIDANCE/DETAILS

SOME CHOICES MADE

- WHICH PARAMETER SETS, WHICH HASH FUNCTIONS, OTHER SYMMETRIC PRIMITIVES, ETC

PLEASE PROVIDE FEEDBACK

- PQC-FORUM, EMAIL ETC
• SIGNATURE BASED ON STRUCTURED LATTICES

• ALL OPERATIONS OVER $R = \mathbb{Z}_q[x]/(x^{256} + 1)$

**KeyGen:**

- $A \leftarrow R^{n \times m}$
- $s \leftarrow S^m$
- $t = \text{Round}(As)$
- $pk=(A,t)$  $sk=s$

**Sign(pk,sk,μ):**

- $y \leftarrow y^m$
- $w=\text{Round}(Ay)$
- $c=\text{Hash}(w,μ)$
- $z=sc+y$
- $\text{RejectionSample}(pk,sk,z)$
- $ω = \text{HintVector}(pk,sk,z)$
- $σ = (z, ω, c)$

**Verify(μ,σ,pk):**

- $w=\text{UseHintVector}(pk,σ)$
- check that $c=\text{Hash}(w, μ)$ and $|z|$ is small
• SIGNATURE BASED ON STRUCTURED LATTICES

We work over the cyclotomic ring $\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$.

Keygen():
1. Generate matrices $A, B$ with coefficients in $\mathcal{R}$ such that
   - $BA = 0$
   - $B$ has small coefficients
2. $pk \leftarrow A$
3. $sk \leftarrow B$

Sign($m, sk$):
1. Compute $c$ such that $cA = H(m)$
2. $v \leftarrow \text{a vector in the lattice } \Lambda(B), \text{ close to } c$
3. $s \leftarrow c - v$

The signature $\text{sig} = (s_1, s_2)$

Verify($m, pk, \text{sig}$):
Accept iff:
1. $s$ is short
2. $sA = H(m)$
• DIGITAL SIGNATURE BASED ON STATELESS HASH-BASED CRYPTOGRAPHY
• USE ROUND 2 PRESENTATION

One-time signatures (Lamport’76) ($\mathcal{A} \mathcal{L} \mathcal{H}$)

How to go stateless (from an OTS)

Security parameter $k$
1. Generate $2^k$ OTS key pairs
2. Authenticate all OTS public keys
3. Sign message with random OTS
4. Sig is OTS sig + authentication information

Figure 1. An SLH-DSA signature

Slides from draft FIPS 205 and A. Hulsing’s talk at RWPQC 2023
KEM BASED ON STRUCTURED LATTICES

ALL OPERATIONS OVER $R = \mathbb{Z}_q[x]/(x^n + 1)$

Kyber.CPAPKE: LPR encryption or “Noisy ElGamal”

$A, s, e \leftarrow \chi$ (a Gaussian distribution)

$sk = s$, $pk = t = As + e$

$r \leftarrow \chi$
$e_1, e_2 \leftarrow \chi'$
$u = A^T r + e_1$
$v = t^T r + e_2 + \text{Enc}(m)$
$c = (u, v)$

$m = \text{Dec}(v - s^T u)$
THE KEMS IN THE 4TH ROUND

- **Classic McEliece**
  - NIST is confident in the security
  - Smallest ciphertexts, but largest public keys
  - We’d like feedback on specific use cases for Classic McEliece

- **BIKE**
  - Most competitive performance of 4th round candidates
  - We encourage vetting of IND-CCA security

- **HQC**
  - Offers strong security assurances and mature decryption failure rate analysis
  - Larger public keys and ciphertext sizes than BIKE

- **SIKE**
  - The SIKE team acknowledges that SIKE (and SIDH) are insecure and should not be used
CONCLUSION

• THE BEGINNING OF THE END IS HERE!
• OR IS IT THE END OF THE BEGINNING?

• WHAT WILL BE THE INTERSECTION OF THE PQC AND THRESHOLD PROJECTS?

• NIST IS GRATEFUL FOR EVERYBODY’S EFFORTS

• CHECK OUT www.nist.gov/pqcrypto
  • SIGN UP FOR THE PQC-FORUM FOR ANNOUNCEMENTS & DISCUSSION
  • SEND E-MAIL TO pqc-comments@nist.gov