What was NIST thinking?

Round 2 of the NIST PQC “Competition”

Dustin Moody
NIST Crypto Standards

• Areas:
  • Block ciphers, hash functions, message authentication codes (MACs), digital signatures, key-establishment, post-quantum (signatures + key establishment), random bit generation, etc...

• FIPS, SP’s, and NISTIRs

• NISTIR 7977 – NIST’s process for developing crypto standards
  • Cooperation with other SDO’s

• Principles:
  • Transparency, openness, balance, integrity, technical merit, global acceptability, usability, continuous improvement, innovation and intellectual property

• Stakeholders:
  • Primarily the US federal government, broader industry and public/private organizations
NIST Competitions*

• **Block Cipher**
  • AES – 15 candidates, 2 rounds, 5 finalists, 3 years + 1 year for standard

• **Hash Function**
  • SHA-3 – 64 submissions, 51 accepted, 3 rounds, 14 2nd round candidates, 5 finalists, 5 years + 3 years for standard

• **Post-Quantum Cryptography**
  • No Name? – 82 submissions, 69 accepted, 2 (or 3) rounds, 26 2nd round candidates, 2017-2020ish + 2? Years for standard

• **Lightweight Crypto**
  • 57 submissions, 2019-2022ish
The NIST PQC Project

- 2009 – NIST publishes a PQC survey
  - Quantum Resistant Public Key Cryptography: A Survey [R. Perlner, D. Cooper]
- 2012 – NIST begins PQC project
  - Research and build team
  - Work with other standards organizations (ETSI, IETF, ISO/IEC SC 27)
- April 2015 – 1st NIST PQC Workshop
A competition by any other name

• Feb 2016 – NIST Report on PQC ([NISTIR 8105](#))
• Feb 2016 – NIST announcement at PQCrypto in Japan
• Dec 2016 – Final requirements and evaluation criteria published
• Nov 2017 – Deadline for submissions

• Scope:
  • Digital Signatures  (FIPS 186)
  • Public-key encryption/KEMs (SP 800-56A and SP 800-56B)

• Expected outcome: a few different algorithms
Evaluation Criteria

**Security** – against both classical and quantum attacks

<table>
<thead>
<tr>
<th>Level</th>
<th>Security Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>At least as hard to break as AES128 (exhaustive key search)</td>
</tr>
<tr>
<td>II</td>
<td>At least as hard to break as SHA256 (collision search)</td>
</tr>
<tr>
<td>III</td>
<td>At least as hard to break as AES192 (exhaustive key search)</td>
</tr>
<tr>
<td>IV</td>
<td>At least as hard to break as SHA384 (collision search)</td>
</tr>
<tr>
<td>V</td>
<td>At least as hard to break as AES256 (exhaustive key search)</td>
</tr>
</tbody>
</table>

• NIST asked submitters to focus on levels 1,2, and 3. (Levels 4 and 5 are for very high security)

**Performance** – measured on various classical platforms

**Other properties:**
• Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, etc...
The 1\textsuperscript{st} Round Candidates

- 82 submissions received.
- 69 accepted as “complete and proper” (5 withdrew)

<table>
<thead>
<tr>
<th></th>
<th>Signatures</th>
<th>KEM/Encryption</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based</td>
<td>5</td>
<td>21</td>
<td>26</td>
</tr>
<tr>
<td>Code-based</td>
<td>2</td>
<td>17</td>
<td>19</td>
</tr>
<tr>
<td>Multi-variate</td>
<td>7</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Symmetric-based</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>19</strong></td>
<td><strong>45</strong></td>
<td><strong>64</strong></td>
</tr>
</tbody>
</table>
Overview of the 1\textsuperscript{st} Round

• Began Dec 2017 – 1\textsuperscript{st} Round Candidates published
• Resources:
  • Internal and external cryptanalysis
  • The 1\textsuperscript{st} NIST PQC Standardization Workshop
  • Research publications
  • Performance benchmarks
  • Official comments
  • The pqc-forum mailing list

• Ended Jan 30, 2019 – 2\textsuperscript{nd} Round Candidates Announced
Breaks and attacks

• Dec 21 – Submissions publicly posted
• 3 weeks later – 12 schemes broken or significantly attacked
• 5 withdrawals
  • Edon-K, HK17, RankSign, RVB, SRTP
• April 2018 – 4 more schemes broken/attacked

• NIST lacked full confidence in security of:
  • CFPKM, Compact-LWE, DAGS, DME, DRS, GuessAgain, Giophantus, Lepton, McNie, pqsigRM, RaCoSS, RLCE, Walnut-DSA
Performance considerations

• “Performance considerations will NOT play a major role in the early portion of the evaluation process.”

• PQRSA and DualModeMS were too inefficient

• Evaluation resources
  • NIST’s internal numbers
  • Preliminary benchmarks – SUPERCOP, OpenQuantumSafe, etc...
  • We hope to get more benchmarks for Round 2
The PQC-forum

- Sign up at www.nist.gov/pqcrypto
- Official channel for announcements and discussion of NIST PQC

- 1261 members
- 926 posts
Official Comments

• Can be submitted on pqc-forum or our website
• Way to keep track of comments on particular submission

• Round 1 - Over 300 official comments
  • 60% of comments on about 10 submissions
  • About half of submissions had 2 or fewer comments

• Round 2 – official comments “start over”
The 1st NIST PQC Standardization Conference

- April 11-13, 2018 in Ft. Lauderdale, Florida co-located with PQCrypto 2018

- There were 52 presentations, covering 60 algorithms, with 345 attendees
  - Most presentations were only 15 minutes
Signed statements required from submitters (posted on our webpage)

From the CFP:

“NIST does not object in principle to algorithms or implementations which may require the use of a patent claim, where technical reasons justify this approach, but will consider any factors which could hinder adoption in the evaluation process.”

For Round 1 – schemes evaluated on their technical merits
  • Later on in process, IP concerns may play a larger role

For Round 2 – only need new IP statements if new team members, or if IP status has changed.
NIST’s Process

- **Dec 2017** – Check submissions for completeness
- **Jan to Sep 2018** – Detailed internal presentations on submissions
- **Apr 2018** – 1st Workshop – submitter’s presentations
- **Sep to Nov 2018** – Review and make preliminary decisions
  - Compare similar type schemes to each other
- **Dec 2018** – Final decision and start report (NISTIR 8240)
  - Very hard decisions
  - Report focused on candidates that advanced on
# Apples and Oranges

<table>
<thead>
<tr>
<th>Encryption/KEMs</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crystals-Kyber</td>
<td>Lattice MLWE</td>
</tr>
<tr>
<td>KINDI</td>
<td>Lattice MLWE</td>
</tr>
<tr>
<td>Saber</td>
<td>Lattice MLWR</td>
</tr>
<tr>
<td>FrodoKEM</td>
<td>Lattice LWE</td>
</tr>
<tr>
<td>Lotus</td>
<td>Lattice LWE</td>
</tr>
<tr>
<td>Lizard</td>
<td>Lattice LWE/RLWE</td>
</tr>
<tr>
<td>Emblem/R.emblem</td>
<td>Lattice LWE/RLWE</td>
</tr>
<tr>
<td>KCL</td>
<td>Lattice LWE/RLWE/LWR</td>
</tr>
<tr>
<td>Round 2</td>
<td>Lattice LWR/RLWR</td>
</tr>
<tr>
<td>Hila5</td>
<td>Lattice RLWE</td>
</tr>
<tr>
<td>Ding’s key exchange</td>
<td>Lattice RLWE</td>
</tr>
<tr>
<td>LAC</td>
<td>Lattice RLWE</td>
</tr>
<tr>
<td>Lima</td>
<td>Lattice RLWE</td>
</tr>
<tr>
<td>NewHope</td>
<td>Lattice RLWE</td>
</tr>
<tr>
<td>Three Bears</td>
<td>Lattice IMLWE</td>
</tr>
<tr>
<td>Mersenne-756839</td>
<td>Lattice ILWE</td>
</tr>
<tr>
<td>Titanium</td>
<td>Lattice MP-LWE</td>
</tr>
<tr>
<td>Ramstake</td>
<td>Lattice LWE like</td>
</tr>
<tr>
<td>Odd Manhattan</td>
<td>Lattice Gener1c</td>
</tr>
<tr>
<td>NTRU Encrypt</td>
<td>Lattice NTRU</td>
</tr>
<tr>
<td>NTRU-HRSS-KEM</td>
<td>Lattice NTRU</td>
</tr>
<tr>
<td>NTRUprime</td>
<td>Lattice NTRU</td>
</tr>
</tbody>
</table>
Mergers

• NIST encouraged mergers of similar submissions

  • Round5 = Round2 + Hila5
  • Rollo = Lake + Locker + Ouroboros-R
  • NTRU = NTRUEncrypt + NTRU-HRSS-KEM
  • LEDAcrypt = LEDAkem + LEDApkc

• NIST is still open to future mergers
Biting the Bullet (1)

- NIST wanted to keep diversity, but reduce numbers
Biting the Bullet (2)

- NIST wanted to keep diversity, but reduce numbers

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Type</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crystals-Kyber</td>
<td>Lattice</td>
<td>MLWE</td>
</tr>
<tr>
<td>KINDI</td>
<td>Lattice</td>
<td>MLWE</td>
</tr>
<tr>
<td>Saber</td>
<td>Lattice</td>
<td>MLWR</td>
</tr>
<tr>
<td>FrodoKEM</td>
<td>Lattice</td>
<td>LWE</td>
</tr>
<tr>
<td>Lotus</td>
<td>Lattice</td>
<td>LWE</td>
</tr>
<tr>
<td>Lizard</td>
<td>Lattice</td>
<td>LWE/RLWE</td>
</tr>
<tr>
<td>Emblem/R.embled</td>
<td>Lattice</td>
<td>LWE/RLWE</td>
</tr>
<tr>
<td>KCL</td>
<td>Lattice</td>
<td>LWE/RLWE/LWR</td>
</tr>
<tr>
<td>Round 2</td>
<td>Lattice</td>
<td>LWR/RLWR</td>
</tr>
<tr>
<td>Hila5</td>
<td>Lattice</td>
<td>RLWE</td>
</tr>
<tr>
<td>Ding’s key exchange</td>
<td>Lattice</td>
<td>RLWE</td>
</tr>
<tr>
<td>LAC</td>
<td>Lattice</td>
<td>RLWE</td>
</tr>
<tr>
<td>Lima</td>
<td>Lattice</td>
<td>RLWE</td>
</tr>
<tr>
<td>NewHope</td>
<td>Lattice</td>
<td>RLWE</td>
</tr>
<tr>
<td>Three Bears</td>
<td>Lattice</td>
<td>MLWE</td>
</tr>
<tr>
<td>Mersenne-756839</td>
<td>Lattice</td>
<td>ILWE</td>
</tr>
<tr>
<td>Titanium</td>
<td>Lattice</td>
<td>MP-LWE</td>
</tr>
<tr>
<td>Ramstake</td>
<td>Lattice</td>
<td>LWE like</td>
</tr>
<tr>
<td>Odd Manhattan</td>
<td>Lattice</td>
<td>Generic</td>
</tr>
<tr>
<td>NTRU Encrypt</td>
<td>Lattice</td>
<td>NTRU</td>
</tr>
<tr>
<td>NTRU-HRSS-KEM</td>
<td>Lattice</td>
<td>NTRU</td>
</tr>
<tr>
<td>NTRUprime</td>
<td>Lattice</td>
<td>NTRU</td>
</tr>
</tbody>
</table>
Biting the Bullet (3)

- NIST wanted to keep diversity, but reduce numbers

<table>
<thead>
<tr>
<th>Signatures</th>
<th>Type</th>
<th>Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRYSALS-Dilithium</td>
<td>Lattice</td>
<td>Fiat-Shamir</td>
</tr>
<tr>
<td>qTesla</td>
<td>Lattice</td>
<td>Fiat-Shamir</td>
</tr>
<tr>
<td>Falcon</td>
<td>Lattice</td>
<td>Hash then sign</td>
</tr>
<tr>
<td>pqNTRUSign</td>
<td>Lattice</td>
<td>Hash then sign</td>
</tr>
<tr>
<td>Gravity-SPHINCS</td>
<td>Symm</td>
<td>Hash</td>
</tr>
<tr>
<td>SPHINCS+</td>
<td>Symm</td>
<td>Hash</td>
</tr>
<tr>
<td>Picnic</td>
<td>Symm</td>
<td>ZKP</td>
</tr>
<tr>
<td>GeMMS</td>
<td>MultVar</td>
<td>HFE</td>
</tr>
<tr>
<td>Gui</td>
<td>MultVar</td>
<td>HFE</td>
</tr>
<tr>
<td>HIMQ-3</td>
<td>MultVar</td>
<td>UOV</td>
</tr>
<tr>
<td>LUOV</td>
<td>MultVar</td>
<td>UOV</td>
</tr>
<tr>
<td>Rainbow</td>
<td>MultVar</td>
<td>UOV</td>
</tr>
<tr>
<td>MQDSS</td>
<td>MultVar</td>
<td>Fiat-Shamir</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signatures</th>
<th>Type</th>
<th>Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRYSALS-Dilithium</td>
<td>Lattice</td>
<td>Fiat-Shamir</td>
</tr>
<tr>
<td>qTesla</td>
<td>Lattice</td>
<td>Fiat-Shamir</td>
</tr>
<tr>
<td>Falcon</td>
<td>Lattice</td>
<td>Hash then sign</td>
</tr>
<tr>
<td>SPHINCS+</td>
<td>Symm</td>
<td>Hash</td>
</tr>
<tr>
<td>Picnic</td>
<td>Symm</td>
<td>ZKP</td>
</tr>
<tr>
<td>GeMMS</td>
<td>MultVar</td>
<td>HFE</td>
</tr>
<tr>
<td>LUOV</td>
<td>MultVar</td>
<td>UOV</td>
</tr>
<tr>
<td>Rainbow</td>
<td>MultVar</td>
<td>UOV</td>
</tr>
<tr>
<td>MQDSS</td>
<td>MultVar</td>
<td>Fiat-Shamir</td>
</tr>
</tbody>
</table>
A brief intermission

• Dec 4 – pqc-forum post saying we are close to end of 1st round
• Dec 13 – NIST decided to announce 2nd Round candidates at RWC
• Dec 22 – US government shutdown begins
  • NIST employees cannot work in any way, shape or form
• Jan 9-11 – Real World Crypto in San Jose, CA
  • NIST did not attend and announce as planned
• Jan 28 – NIST is back at work!
• Jan 30 – 2nd Round Announcement
  • 1st Round Report, NISTIR 8240 (https://doi.org/10.6028/NIST.IR.8240)
The Round 2 Candidates

• KEMs/Encryption: Lattices
  • Crystals-Kyber
  • FrodoKEM
    • Uses algebraically unstructured lattices, relies on standard LWE. Results in larger key sizes, and slightly slower performance than other (ring-based) lattice schemes.
  • LAC
    • Based on poly-variant of LWE. Uses modulus $q=251$. Good performance. Category 5 parameters have problems. Needs constant-time implementation.
  • NewHope
    • Based on ring LWE, with power-of-2 cyclotomic ring. Good performance.
The Round 2 Candidates

• KEMs/Encryption: Lattices
  • NTRU
    • Merger of 2 good submissions. Been around longer than other submissions. Based on “NTRU assumption”. NTRU lattices have more structure than other lattice schemes.
  • NTRU Prime
    • 2 versions (streamlined and LPRime). Uses irreducible, non-cyclotomic polynomials and inert prime $q$. Good performance. Different cost model used than other submissions. Only level 5 parameters.
  • Round 5
    • Merger, mostly based on Round2. Uses prime cyclotomic rings, based on (ring) LWR. Good performance and low bandwidth. Previous issue with decryption failure.
  • Saber
    • Based on module LWR, and power-of-2 cyclotomic ring. Good performance and low bandwidth. Parameters may not fit known security reductions.
  • Three Bears
    • Novel design (variant of module LWE over the integers). Fast arithmetic. Newer security assumption.
The Round 2 Candidates

• KEMs/Encryption: Code-based
  • Classic McEliece
  • NTS-KEM
    • Very, very similar to Classic McEliece, but with some different design choices. Needs constant time implementation.
  • BIKE
    • 3 versions. Based on quasi-cyclic MDPC codes. Ephemeral use only. Similar key size and performance to lattice schemes. More analysis needed of particular security assumption.
  • HQC
    • Low decryption failure rate (necessary for CCA security). As a result, slightly larger key and ciphertext sizes. More analysis needed of particular security assumption.
The Round 2 Candidates

- **KEMs/Encryption: Code-based (and Isogeny)**
  - **Rollo**
    - Merger of 3 rank-based schemes using LRPC codes. 2 schemes are ephemeral, 1 targets CCA security. Newer security assumption.
  - **LEDAcrypt**
    - Merger. Based on quasi-cyclic LDPC codes, which have more structure than QC-MDPC codes. New parameters with low decryption rates. Needs more analysis.
  - **RQC**
    - Rank-based scheme. No decryption failures. As a result, slower speeds and ciphertext size. Security problem needs more analysis, as it is newer.
  - **SIKE**
The Round 2 Candidates

• **Signatures: Lattices**
  - **Crystals-Dilithium**
    - Fiat-Shamir idea, based on module LWE. Good performance.
  - **Falcon**
    - Uses the NTRU lattice. Good performance. Complicated to implement.
  - **qTesla**
    - Based on ring LWE. Good performance. More analysis needed of particular security assumption.

• **Symmetric-based**
  - **Sphincs+**
    - Stateless hash-based scheme. Security well understood, relying only on pre-image resistance of the hash function. Small public keys, but large signatures. Signing is slower.
  - **Picnic**
The Round 2 Candidates

• Signatures: Multivariate
  • GeMSS
    • An HFEv- “big-field” scheme. Very small signatures. As a result, some performance sizes/times are larger. Better tradeoffs may be found.
  • LUOV
    • “Small-field” scheme based on UOV. Low bandwidth. Some of the techniques introduced need more analysis.
  • MQDSS
    • Based on provably secure reduction to MQ problem, using Fiat-Shamir. (Actual parameters don’t fit the reduction). Smaller public keys, and larger signature sizes. Needs more research and optimization.
  • Rainbow
    • Generalization of UOV, adding in structure to be more efficient. Somewhat well-studied. The implementation could be improved.
Tweaks

• Submission teams had until March 15 to send us their revised/merged submission
  • No major re-designs, must meet all the same acceptance criteria
  • NIST will decide whether tweaks are acceptable (working with the submitters)

• Many teams asked for more time, so 2 week extension granted

• We will post the tweaked candidates as soon as possible
• Most common tweaks: updated parameters, optimizations
The Second Round (and beyond)

- Aug 22-24, 2019 – 2\textsuperscript{nd} NIST PQC Standardization workshop, co-located with CRYPTO in Santa Barbara, CA
  - Deadline for paper submission: May 31, 2019

- Expected to last 12-18 months, after possibly a 3\textsuperscript{rd} Round

- Overall timeline: we still expect draft standards around 2022ish
  - (but reserve the right to change this!)
Stateful Hash-based signatures

• NIST plans to approve stateful hash-based signatures
  • 1) XMSS, specified in RFC 8931
  • 2) LMS, currently specified in draft, and in the RFC editor queue

• In Feb 2019, NIST issued a request for public input on how to mitigate the potential misuse of stateful HBS schemes. Comments are due by April 1, 2019.

• NIST expects to have a Special Publication (SP) published in 2019
What NIST wants

• Performance (hardware+software) will play more of a role
  • More benchmarks
  • For hardware, NIST asks to focus on Cortex M4 (with all options) and Artix-7

• Continued research and analysis on **ALL** of the 2\textsuperscript{nd} round candidates

• See how submissions fit into applications/protocols. Any constraints?
Other NIST happenings

• NIST has a lightweight crypto project
  • 57 submissions received
  • Workshop on Nov 4-6, 2019 at NIST

• Threshold Crypto workshop
  • March 11-12, 2019

• FIPS 186-5 (and SP 800-186) – ECC and Digital Signatures
  • Expected to be released for public comment by May 2019
Summary

• Round 2 has started
  • 26 candidate algorithms
    (17 encryption/KEM, 9 signatures)

• We will continue to work in an open and transparent manner with the crypto community for PQC standards

• Check out: www.nist.gov/pqcrypto
  • Sign up for the pqc-forum

• Talk to us: pqc-comments@nist.gov