THE NIST PQC STANDARDS: LIGHT AT THE END OF THE TUNNEL

Dustin Moody
Computer Security Division
NIST
NIST DEVELOPED THE FIRST ENCRYPTION STANDARDS IN 1970S

- DATA ENCRYPTION STANDARD (DES), PUBLISHED 1977 AS FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 46

OVER 40 YEARS, NIST CONTINUES TO EVOLVE ITS CRYPTOGRAPHIC STANDARDS

- ENABLE TO RESPOND THE GROWING APPLICATION DEMAND
- ENHANCE SECURITY STRENGTH TO AGAINST MORE SOPHISTICATED ATTACKS

Nearly all commercial laptops, cellphones, Internet routes, VPN servers, and ATMs use NIST Cryptography
QUANTUM ALGORITHMS

1994 – SHOR’S ALGORITHM

• A QUANTUM ALGORITHM GIVING AN EXPONENTIAL SPEED-UP OVER CLASSICAL COMPUTERS
  • FACTORING LARGE INTEGERS
  • FINDING DISCRETE LOGARITHMS

1996 – GROVER’S ALGORITHM

• POLYNOMIAL SPEED-UP IN UNSTRUCTURED SEARCH, FROM $O(N)$ TO $O(\sqrt{N})$
THE QUANTUM THREAT

- 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
HOW SOON DO WE NEED TO WORRY?
"The United States must prioritize the transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."
THE OMB ‘MIGRATING TO PQC’ MEMO

- PRIORITIZE INVENTORY OF CRYPTOGRAPHIC SYSTEMS
  - FOCUS ON HIGH VALUE ASSETS AND HIGH IMPACT SYSTEMS
  - ANNUALLY SUBMIT RESULTS TO ONCD AND CISA UNTIL 2035
    - ONCD/CISA WILL RELEASE TOOLS AND PROCEDURES FOR INVENTORY
    - MORE SPECIFICS PROVIDED…..
- ANNUAL ASSESSMENT OF FUNDING REQUIRED FOR MIGRATION
- AGENCIES SHOULD HAVE ALREADY DESIGNATED A MIGRATION LEAD
  - OMB WILL COORDINATE GOVERNMENT-WIDE RESPONSE
- TESTING PRE-STANDARDIZED PQC ALGORITHMS ENCOURAGED
- NIST WILL CREATE A WORKING GROUP TO DEVELOP BEST PRACTICES

"THE UNITED STATES MUST PRIORITIZE THE TRANSITION OF CRYPTOGRAPHIC SYSTEMS TO QUANTUM-RESISTANT CRYPTOGRAPHY, WITH THE GOAL OF MITIGATING AS MUCH OF THE QUANTUM RISK AS IS FEASIBLE BY 2035."
IN SEPT 2022, NSA ANNOUNCED CNSA 2.0 ADVISORY TO PREPARE NATIONAL SECURITY SYSTEMS FOR THE TRANSITION TO PQC

NSA EXPECTS THE TRANSITION TO QR ALGORITHMS FOR NSS TO BE COMPLETE BY 2035 IN LINE WITH NSM-10.
THE NIST PQC “COMPETITION”

• IN 2016, 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 A 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’
1. **SECURE** 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>

2. **PERFORMANCE** - MEASURED ON VARIOUS "CLASSICAL" PLATFORMS

3. **OTHER PROPERTIES**
   - DROP-IN REPLACEMENTS - COMPATIBILITY WITH EXISTING PROTOCOLS AND NETWORKS
   - PERFECT FORWARD SECRECY
   - RESISTANCE TO SIDE-CHANNEL ATTACKS
   - SIMPLICITY AND FLEXIBILITY
   - MISUSE RESISTANCE, ETC…
THE FIRST THREE ROUNDS

ROUND 1 (DEC ‘17 – JAN ‘18)
- 69 CANDIDATES AND 278 DISTINCT SUBMITTERS
- SUBMITTERS FROM >25 COUNTRIES, ALL 6 CONTINENTS
- APR 2018, 1ST NIST PQC CONFERENCE
- ALMOST 25 SCHEMES BROKEN/ATTACKED
- NISTIR 8240, NIST REPORT ON THE 1ST ROUND

ROUND 2 (JAN ‘18 – JUL ‘20)
- 26 CANDIDATES
- AUG 2019 – 2ND NIST PQC CONFERENCE
- 7 SCHEMES BROKEN/ATTACKED
- NISTIR 8309, NIST REPORT ON THE 2ND ROUND

ROUND 3 (JUL ‘20 – JUL ‘22)
- 7 FINALISTS AND 8 ALTERNATES
- JUNE 2021 – 3RD NIST PQC CONFERENCE
- NISTIR 8413, NIST REPORT ON THE 3RD ROUND

<table>
<thead>
<tr>
<th>Type</th>
<th>Signatures</th>
<th>KEMs/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>Total</td>
<td><strong>19</strong></td>
<td><strong>45</strong></td>
<td><strong>64</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Signatures</th>
<th>KEMs/Encryption</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based</td>
<td>3</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Code-based</td>
<td>0</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Multi-variate</td>
<td>4</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Symmetric-based</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td><strong>9</strong></td>
<td><strong>17</strong></td>
<td><strong>26</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Signatures</th>
<th>KEMs/Encryption</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based</td>
<td>2</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Code-based</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Multi-variate</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Symmetric-based</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td><strong>6</strong></td>
<td><strong>9</strong></td>
<td><strong>15</strong></td>
</tr>
</tbody>
</table>
### ROUND 3 RESULTS

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

See [NISTIR 8413](https://csrc.nist.gov/publication/199528), Status Report on the 3rd Round of the NIST PQC Standardization Process, for the rationale on the selections.

**4th round candidates (all KEMs)**
- ClassicMcEliece
- BIKE
- HQC
- SIKE

**On-ramp signatures**
- NIST issued a new call for additional signatures – preferably for signatures based on non-lattice problems
THE SELECTED ALGORITHMS

- **CRYSTALS-KYBER**
  - KEM BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY

- **CRYSTALS-DILITHIUM**
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY, RELATIVELY SIMPLE IMPLEMENTATION
  - NIST RECOMMENDS IT BE THE PRIMARY SIGNATURE ALGORITHM USED

- **FALCON**
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - SMALLER BANDWIDTH, BUT MUCH MORE COMPLICATED IMPLEMENTATION
  - THE FALCON STANDARD WILL COME OUT AFTER THE OTHERS

- **SPHINCS+**
  - DIGITAL SIGNATURE BASED ON STATELESS HASH-BASED CRYPTOGRAPHY
  - SOLID SECURITY, BUT PERFORMANCE NOT AS GOOD IN COMPARISON TO DILITHIUM/FALCON
• The 5th NIST PQC Standardization Conference
  • April 10-12, 2024 in Rockville, Maryland

• Draft standards for public comment will be in summer 2023
• The first PQC standards should be published in 2024
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
AN ON-RAMP FOR SIGNATURES

• Scope:
  • NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.
  • NIST may also be interested in signature schemes that have short signatures and fast verification.
  • Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.

• The more mature the scheme, the better.
• NIST will decide which (if any) of the received schemes to focus attention on

No on-ramp for KEMs currently planned.
THE ONRAMP NUMBERS

- 50 submissions received by the final deadline
  - There were 23 signatures (and 59 KEMs) submitted in 2017
  - 262 distinct submitters

- 40 submissions accepted as ‘complete and proper’
  - From 5 continents and 28 countries

- For complete specs (including code):
  see www.nist.gov/pqcrypto

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice</td>
<td>7</td>
</tr>
<tr>
<td>Code-based</td>
<td>6</td>
</tr>
<tr>
<td>Multivariate</td>
<td>11</td>
</tr>
<tr>
<td>MPC in the head</td>
<td>6</td>
</tr>
<tr>
<td>Symmetric</td>
<td>4</td>
</tr>
<tr>
<td>Isogeny</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>40</strong></td>
</tr>
</tbody>
</table>
THE PQC STANDARDS WILL BE FIPS

- Each algorithm will be its own document
- Will have some SP’s which contain more guidance/details
- All the algorithms will be given a standardized name
  - ML-KEM (KYBER), ML-DSA (DILITHIUM), NL-DSA (FALCON) and SLH-DSA (SPHINCS+)

SOME CHOICES NEED TO BE MADE

- Which parameter sets to include
- Which hash functions, other symmetric primitives, etc?
- How to allow for any potential changes from the Round 3 specifications?
  - Submission teams may submit suggested changes
  - Any changes by NIST (or suggested by teams) will be discussed publicly

PLEASE PROVIDE FEEDBACK

- PQC-forum, email etc
Stateful hash-based signatures were proposed in 1970s

- Rely on assumptions on hash functions, that is, not on number theory complexity assumptions
- It is essentially limited-time signatures, which require state management

NIST specification on stateful hash-based signatures

- NIST SP 800-208 “Recommendation for Stateful Hash-Based Signature Schemes”

Internet Engineering Task Force (IETF) has released two RFCs on hash-based signatures

- RFC 8391 “XMSS: eXtended Merkle Signature Scheme” (By Internet Research Task Force (IRTF))
- RFC 8554 “Leighton-Micali Hash-Based Signatures” (By Internet Research Task Force (IRTF))

ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

- Stateful hash-based signatures will be specified in ISO/IEC 14888 Part 4
- It is in the 1st Working Draft stage

Stateful hash-based signatures from SP 800-208 are allowed for signing software/firmware updates in CNSA 2.0
• THERE HAS BEEN MUCH DISCUSSION ON HYBRID/COMPOSITE MODES
  • NIST SP800-56C REV. 2 ALLOWS FOR A CERTAIN HYBRID MODE
  • WE WILL WORK WITH THE COMMUNITY IN DIFFERENT STAGES OF MIGRATION TO ASSURE SECURITY

• NIST WILL PROVIDE TRANSITION GUIDELINES TO PQC STANDARDS
  • NIST HAS PROVIDED SUCH GUIDANCE BEFORE
    • EXAMPLES: TRIPLE DES, SHA-1, KEYS < 112 BITS
  • TIMEFRAME WILL BE BASED ON RISK ASSESSMENT OF QUANTUM ATTACKS
WE ARE AWARE THAT MANY STANDARDS ORGANIZATIONS AND EXPERT GROUPS ARE WORKING ON PQC

- ASC X9 HAS DONE STUDIES AND WRITTEN WHITE PAPERS
- IEEE P1363.3 HAS STANDARDIZED SOME LATTICE-BASED SCHEMES
- IETF HAS STANDARDIZED STATEFUL HASH-BASED SIGNATURES LMS/XMSS AND IS CURRENTLY DOING NEW WORK GEARED TO THE PQC MIGRATION
- ETSI HAS RELEASED QUANTUM-SAFE CRYPTOGRAPHY REPORTS
- EU EXPERT GROUPS PQCRYPTO AND SAFECRYPTO MADE RECOMMENDATIONS AND RELEASED REPORTS
- ISO/IEC JTC 1 SC27 HAD A STUDY PERIOD FOR QUANTUM-RESISTANT CRYPTOGRAPHY AND RELEASED A STANDING DOCUMENT (SD)

- NIST IS INTERACTING AND COLLABORATING WITH THESE ORGANIZATIONS AND GROUPS

- SOME COUNTRIES HAVE BEGUN STANDARDIZATION ACTIVITIES
WHAT CAN ORGANIZATIONS DO NOW?

• PERFORM A QUANTUM RISK ASSESSMENT WITHIN YOUR ORGANIZATION
  • INVENTORY INFORMATION ASSETS AND THEIR CURRENT CRYPTO PROTECTION
  • IDENTIFY WHAT ‘X’, ‘Y’, AND ‘Z’ MIGHT BE FOR YOU – DETERMINE YOUR QUANTUM RISK
  • PRIORITIZE ACTIVITIES REQUIRED TO MAINTAIN AWARENESS, AND TO MIGRATE TECHNOLOGY TO QUANTUM-SAFE SOLUTIONS

• EVALUATE VENDOR PRODUCTS WITH QUANTUM SAFE FEATURES
  • KNOW WHICH PRODUCTS ARE NOT QUANTUM SAFE
  • ASK VENDORS FOR QUANTUM SAFE FEATURES IN PROCUREMENT TEMPLATES

• DEVELOP AN INTERNAL KNOWLEDGE BASE AMONGST IT STAFF

• TRACK DEVELOPMENTS IN QUANTUM COMPUTING AND QUANTUM SAFE SOLUTIONS

• ESTABLISH A ROADMAP TO QUANTUM READINESS FOR YOUR ORGANIZATION

• ACT NOW – IT WILL BE LESS EXPENSIVE, LESS DISRUPTIVE, AND LESS LIKELY TO HAVE MISTAKES CAUSED BY RUSHING AND SCRAMBLING
CONCLUSION

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

• 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