Post-Quantum Cryptography
- Standardization and Transition

Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)
NIST Process Update: Milestones and Timeline

2016
- Determined criteria and requirements
- Announced call for proposals

2017
- Received 82 submissions
- Announced 69 1st round candidates

2018
- 1st round analysis
- Held the 1st NIST PQC standardization Conference

2019
- Announced 26 2nd round candidates
- Held the 2nd NIST PQC Standardization Conference

2020
- Announced 3rd round 7 finalists and 8 alternate candidates

2021
- Hold the 3rd NIST PQC Standardization Conference

2022-2023
- Release draft standards and call for public comments
Considerations in Selecting Algorithms

- **Security**
  - Security levels offered
  - (confidence in) security proof
  - Any attacks
  - Classical/quantum complexity

- **Performance**
  - Size of pk, ciphertext, signature, etc.
  - Speed of KeyGen, Enc/Dec, Sign/Verify
  - Decryption failures

- **Algorithm and implementation characteristics**
  - IP issues
  - Side-channel resistance
  - Simplicity and clarity of documentation
  - Flexible for different platforms and applications

- **Diversity**
  - Based on different assumptions and/or with different properties

- **Other**
  - Official comments/pqc-forum discussion
  - Papers published/presented
Post-Quantum Cryptography

- Some actively researched PQC categories
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key-based signatures
  - Isogeny-based schemes
# First, Second, and Third Round Candidates

<table>
<thead>
<tr>
<th></th>
<th>Signatures</th>
<th>KEM/Encryption</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st round</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Signatures</th>
<th>KEM/Encryption</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2nd round</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lattice-based</td>
<td>3</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Code-based</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Signatures</th>
<th>KEM/Encryption</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3rd round</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lattice-based</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Code-based</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Multi-variate</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Stateless Hash or Symmetric based</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Isogeny</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
Third Round – Lattice Based KEM

- **Crystals-Kyber and Saber**
  - Great performance all-around → **Finalists**

- **FrodoKEM**
  - Conservative/Backup → **Alternate**

- **NTRU**
  - Not quite as efficient, but long & established history, existing standards → **Finalist**

- **NTRUprime**
  - Different design choice and security model → **Alternate**
Third Round – Isogeny and Code-based KEMs

- **SIKE**
  - Newer security problem, an order slower → Alternate

- **Classic McEliece**
  - Oldest design, large public keys but small ciphertexts → Finalist

- **BIKE**
  - Good performance, made some changes → Alternate

- **HQC**
  - Better security analysis/larger keys (than BIKE) → Alternate
• Dilithium and Falcon
  • Both balanced, efficient lattice-based signatures
  • Manageable pk and sig sizes → Finalists

• SPHINCS+ and Picnic
  • SPHINCS+ is stateless hash-based signatures, relatively stable, conservative security, larger sig/slower → Alternate
  • Picnic is based on symmetric-based primitive, not stable yet, but has lots of potential → Alternate

• Rainbow and GeMMS
  • Both have large pk, very small sig
  • Rainbow a bit better → Finalist
  • GeMMS → Alternate
Challenges and Strategies in Transition to PQC

• Public key Cryptography has been used everywhere and two most important usages are for
  • Communication security (IPsec, TLS, etc)
  • Trusted platforms (Code signing)

• Transition is going to be a long journey and full of exciting adventures
  • New features, characters, implementation challenges
  • Not quite drop-in replacements
  • Risk of disruptions in operation and security

• Enable crypto agility is the key for smooth migration
  • A capability allowing to remove some algorithms and to introduce new algorithms in the existing applications and implementations
Initiatives in Transition to PQC

• Prototype PQC candidates in TLS and other protocols

• Stateful Hash Based Signatures for Early Adoption
  • 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))
  • NIST SP 800-208 “Recommendation for Stateful Hash-Based Signature Schemes” published in October 2020
  • ISO/IEC JTC 1 SC27 WG2 Project: Stateful hash-based signatures will be specified in ISO/IEC 14888 Part 4

• Hybrid mode as an approach for migration to PQC
  • Use an existing public key standard, e.g. Diffie-Hellman Key Agreement and a PQC mechanism
  • Each of them establishes a “shared secret value”
  • Derive session keys from both secret values
  • NIST SP 800-56C rev. 2 has incorporated the additional shared secret to key derivation
Transition Preparation and Outreach

  - The paper discussed what we can do now as the first step to prepare for the transition

- NCCoE held a Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms on October 7, 2020
  - About 300 researchers, practitioners, implementers, and policy makers participated workshop
  - Covered experiment implementations on protocols, like TLS, IKE, DNSSEC, and applications like code signing using PQC algorithms
  - Shared transition timeline for specific application community, e.g. financial service
  - Identified some strategies on smooth transition, e.g. dual-signature for PKI
  - Explored hybrid mode in various of protocols e.g. Hybrid mode in TLS 1.3

• NIST announced the 3rd round 7 finalists and 8 alternate candidates in July 2020
• NIST plans to release draft standards for public comments in 2022-2023
• It is the time to prepare for transition and migration

• We will continue open for suggestions and encourage discussions
  • For NIST PQC project, please follow us at https://www.nist.gov/pqcrypto
  • To submit a comment, send e-mail to pqc-comments@nist.gov
  • Join discussion mailing list pqc-forum@nist.gov