The Homestretch:

the beginning of the end

of the NIST PQC 3rd Round

Dustin Moody

NIST PQC team

National Institute of Standards and Technology
U.S. Department of Commerce

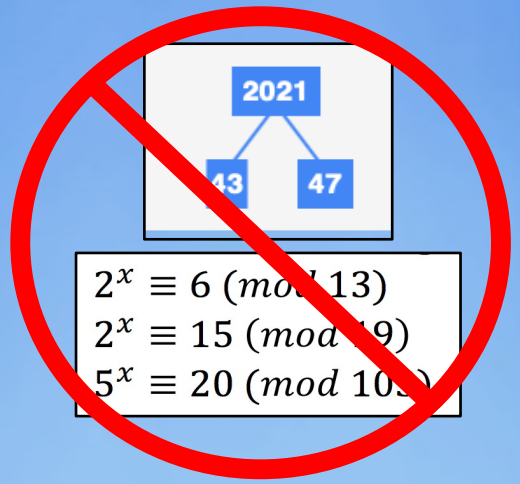
Cryptographic Technology Group
Computer Security Division
Information Technology Lab

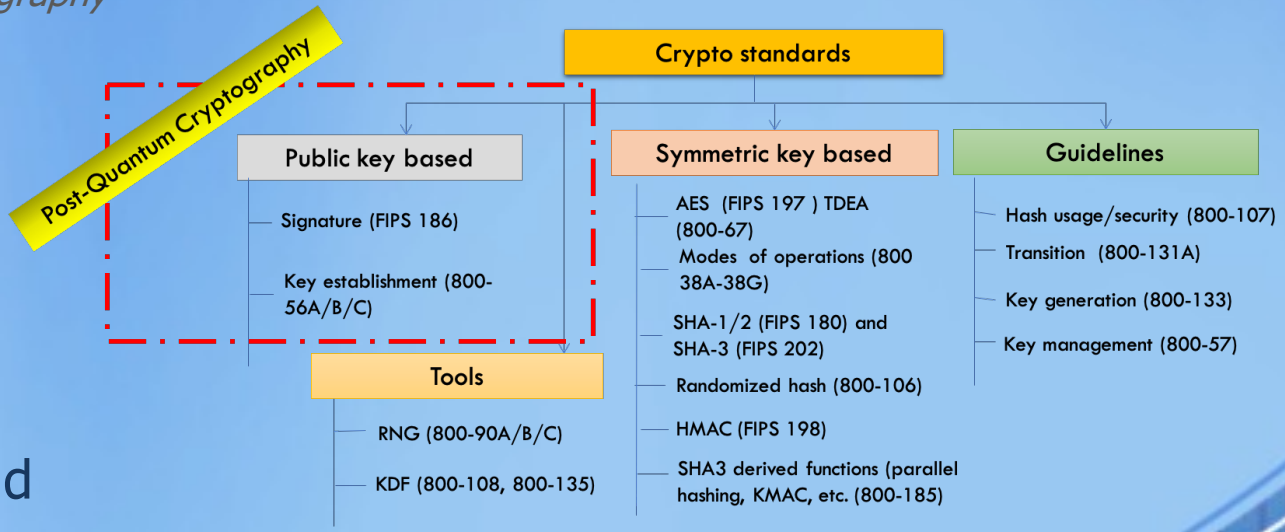
Outline

- Motivation
- A look back
- Where we are now
- What lies ahead

Why we're here

- NIST public-key crypto standards
  - **SP 800-56A**: *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*
  - **SP 800-56B**: *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*
  - **FIPS 186**: *The Digital Signature Standard*
- vulnerable to attacks from a (large-scale) quantum computer





- Shor's algorithm would break RSA, ECDSA, (EC)DH, DSA
- Symmetric-key crypto standards would also be affected, but less dramatically

Not too long ago….

- April 2015 – NIST workshop: Cybersecurity in a post-quantum world

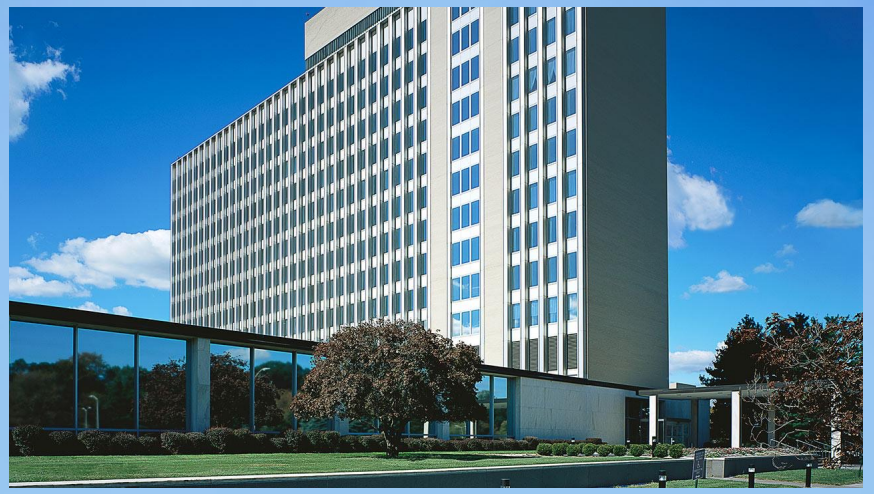
NIST Workshop on Cybersecurity in a Post-Quantum World
April 2 – April 3, 2015

NIST solicits papers, presentations, case studies, panel proposals, and participation from any interested parties, including researchers, systems architects, vendors, and users. NIST will post the accepted papers and presentations on the workshop web site and include these in a workshop handout. However, no formal workshop proceedings will be published. NIST encourages presentations and reports on preliminary work that participants plan to publish elsewhere. Topics for submissions should include, but are not limited to, the following:

Security Status of Approved Public Key Cryptographic Algorithms

- How does the development of quantum computers affect the security of currently deployed public key algorithms? (E.g., encryption (for key transport), digital signatures, and key agreement)
- How would quantum computers affect other services which rely on public key infrastructure? (E.g. TLS, IPSec, etc.)
- Are there other concerns with the existing public key algorithms that would motivate the development of alternative cryptosystems?
- Are there other advanced computing technologies that could threaten the existing cryptosystems?

Short Term Actions



Not too long ago….

- Aug 2015 – NSA bulletin

- "IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."

  https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

Not too long ago….

- Feb 2016 – NIST Report on PQC

NIST

Search CSRC

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

PUBLICATIONS

NISTIR 8105

Report on Post-Quantum Cryptography

Date Published: April 2016

Author(s)

Lily Chen (NIST), Stephen Jordan (NIST), Yi-Kai Liu (NIST), Dustin Moody (NIST), Rene Peralta (NIST), Ray Perlner (NIST), Daniel Smith-Tone (NIST)

Abstract

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will

DOCUMENTATION

Publication:

NISTIR 8105 (DOI)

Local Download

Supplemental Material:

Press Release (other)

Comments received on Draft NISTIR 8105 (pdf)

Related NIST Publications:

1 Introduction

In the last three decades, public key cryptography has become an indispensable component of our global communication digital infrastructure. These networks support a plethora of applications that are important to our economy, our security, and our way of life, such as mobile phones, internet commerce, social networks, and cloud computing. In such a connected world, the ability of individuals, businesses and governments to communicate securely is of the utmost importance.

Many of our most crucial communication protocols rely principally on three core cryptographic functionalities: public key encryption, digital signatures, and key exchange[1]. Currently, these functionalities are primarily implemented using Diffie-Hellman key exchange, the RSA (Rivest-Shamir-Adleman) cryptosystem, and elliptic curve cryptosystems. The security of these depends on the difficulty of certain number theoretic problems such as Integer Factorization or the Discrete Log Problem over various groups.

In 1994, Peter Shor of Bell Laboratories showed that quantum computers, a new technology leveraging the physical properties of matter and energy to perform calculations, can efficiently solve each of these problems, thereby rendering all public key cryptosystems based on such assumptions impotent [1]. Thus a sufficiently powerful quantum computer will put many forms of modern communication—from key exchange to encryption to digital authentication—in peril.

The discovery that quantum computers could be utilized to solve certain problems faster than classical computers has inspired great interest in quantum computing. Is quantum complexity fundamentally different from classical complexity? When will large-scale quantum computers be built? Is there a way to resist both a quantum and a classical computing adversary? Researchers are working on these questions.

In the twenty years since Shor's discovery, the theory of quantum algorithms has developed significantly. Quantum algorithms achieving exponential speedup have been discovered for several problems relating to physics simulation, number theory, and topology. Nevertheless, the list of problems admitting exponential speedup by quantum computation remains relatively small. In contrast, more modest speedups have been developed for broad classes of problems related to searching, collision finding, and evaluation of Boolean formulae. In particular, Grover's search algorithm proffers a quadratic speedup on unstructured search problems. While such a speedup does not render cryptographic technologies obsolete, it can have the effect of requiring larger key sizes, even in the symmetric key case. See Table 1 for a summary of the impact of large-scale quantum computers on common cryptographic algorithms, such as RSA and the Advanced Encryption Standard (AES). It is not known how far these quantum advantages can be pushed, nor how wide is the gap between feasibility in the classical and quantum models.

[1] NIST standardized digital signature schemes in [FIPS 186-4], as well as public key-based key establishment schemes in [SP800-56A] (using key exchange) and [SP800-56B] (using public key encryption).

Not too long ago….

- Feb 2016 – 7th PQCrypto in Fukuoka, Japan
- NIST announced a call for (public-key) quantum-resistant algorithms

Call for Proposals

- NIST is calling for quantum-resistant cryptographic algorithms for new public-key crypto standards
  - Digital signatures
  - Encryption/key-establishment
- We see our role as managing a process of achieving community consensus in a **transparent** and timely manner
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as 'good choices'
- We may pick one (or more) for standardization
  - Only algorithms publicly submitted considered

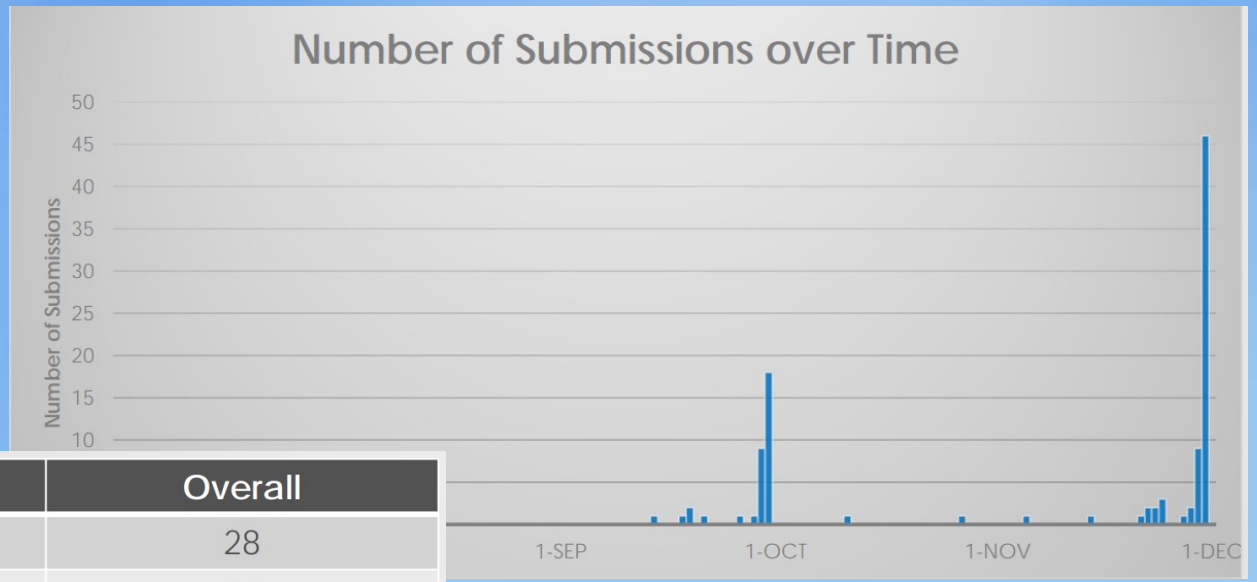
Timeline

- Fall 2016 – formal Call For Proposals
- Nov 2017 – Deadline for submissions
- 3-5 years – Analysis phase
  - NIST will report its findings
- 2 years later – Draft standards ready

- Workshops
  - Early 2018 – submitter's presentations
  - One or two during the analysis phase

Not too long ago….

- Dec 2016 – Final requirements published in the *Call for Proposals*
- Nov 2017 – Submission deadline



	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	**23**	**59**	**82**

MINIMAL ACCEPTABILITY REQUIREMENTS

- Publicly disclosed and freely available during the process
  - Signed statements, disclose patent info
- Implementable in wide range of platforms
- Provides at least one of: signature, encryption, or key establishment
- Theoretical and empirical evidence providing justification for security claims
- Concrete values for parameters meeting target security levels

Security Strength Categories

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

- Computational resources should be measured using a variety of metrics
- NIST asked submitters to focus on levels 1,2, and 3
  - Levels 4 and 5 for high security
- These are understood to be preliminary estimates

The 1st Round

- Dec 20, 2017 – Jan 30, 2018
- Initially, 69 → 64 candidates
  - 278 distinct submitters
- Apr 2018, 8th PQCrypto + 1st NIST PQC Standardization conference in Florida
- Research, cryptanalysis, pqc-forum, official comments, benchmarking, mergers
- In the end, 26 schemes selected to move on
  - NISTIR 8240, NIST Report on the 1st Round

The 2nd Round

- Jan 30, 2018 – July 22, 2020
- Started with 26 candidates
- 2nd NIST PQC standardization conference in California, PQCrypto in Chongqing

- Schemes broken/attacked: LAC, LedaCrypt, Round5, Rollo, RQC, LUOV, MQDSS, qTESLA

- 15 schemes selected to move on
  - NISTIR 8309, NIST Report on 2nd Round

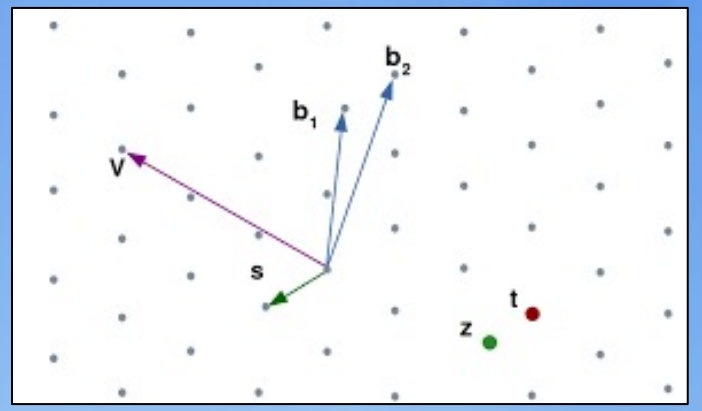
	Signatures	KEMs/Encryption	Total
Lattice-based	3	9	12
Code-based	0	7	7
Multi-variate	4	0	4
Symmetric-based	2		2
Other	0	1	1
Total	**9**	**17**	**26**

So where are we now?

- 3rd Round: 7 Finalists and 8 Alternates
  - **Finalists**: most promising algorithms we expect to be ready for standardization at the end of the 3rd round
  - **Alternates**: candidates for potential standardization, most likely after another (4th) round

	Finalists	Alternates
KEMs/Encryption	Kyber NTRU SABER Classic McEliece	Bike FrodoKEM HQC NTRUprime SIKE
Signatures	Dilithium Falcon Rainbow	GeMSS Picnic SPHINCS+

The Lattice KEMs

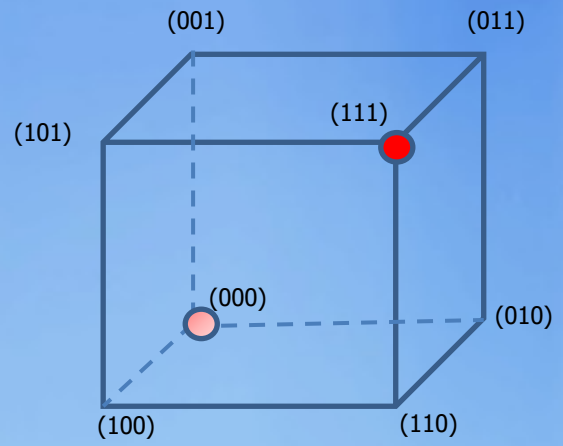


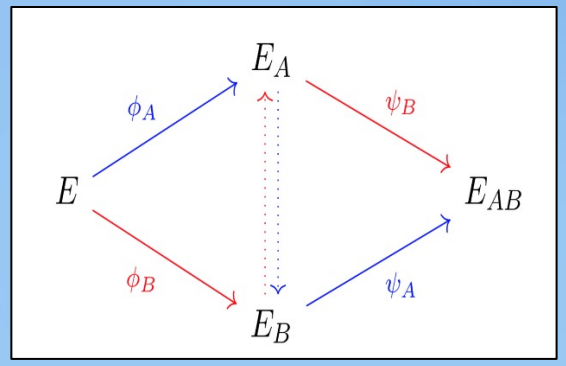
- The finalists **Kyber, NTRU, SABER** are based on structured lattices
  - Kyber and SABER are based on module-LWE/LWR
  - NTRU is based on the NTRU problem
  - NTRU recently added a category 5 parameter set
  - All three have good performance (in terms of efficiency and key/ciphertext sizes)
  - *NIST expects to select at most one for standardization*

- The alternates **NTRUprime** and **FrodoKEM** are based on lattices
  - NTRUprime uses structured lattices, while FrodoKEM does not

The Other KEMs

- **Classic McEliece**, the other finalist, is code-based
  - Been around since 1978
  - Very large public keys, but very small ciphertexts
- The alternates **BIKE** and **HQC** are based on structured codes
  - Both have much smaller key sizes than Classic McEliece
- The final alternate **SIKE** is based on isogenies of elliptic curves
  - Small key/ciphertext sizes, a bit slower than other candidates





The Signatures

- The finalists **Dilithium** and **Falcon** are both based on structured lattices
  - Dilithium is Fiat-Shamir style, while Falcon is hash then sign
  - Both have good performance
  - *NIST expects to select at most one for standardization*

- The alternate **Picnic** is based on zero-knowledge proofs and a block cipher
- The alternate **SPHINCS+** is based on the security of hash functions
  - The security of SPHINCS+ is very well understood

- There are two multivariate schemes: the finalist **Rainbow**, and the alternate **GeMSS**
  - Both have large public keys, and very small signature sizes

The state of the signatures

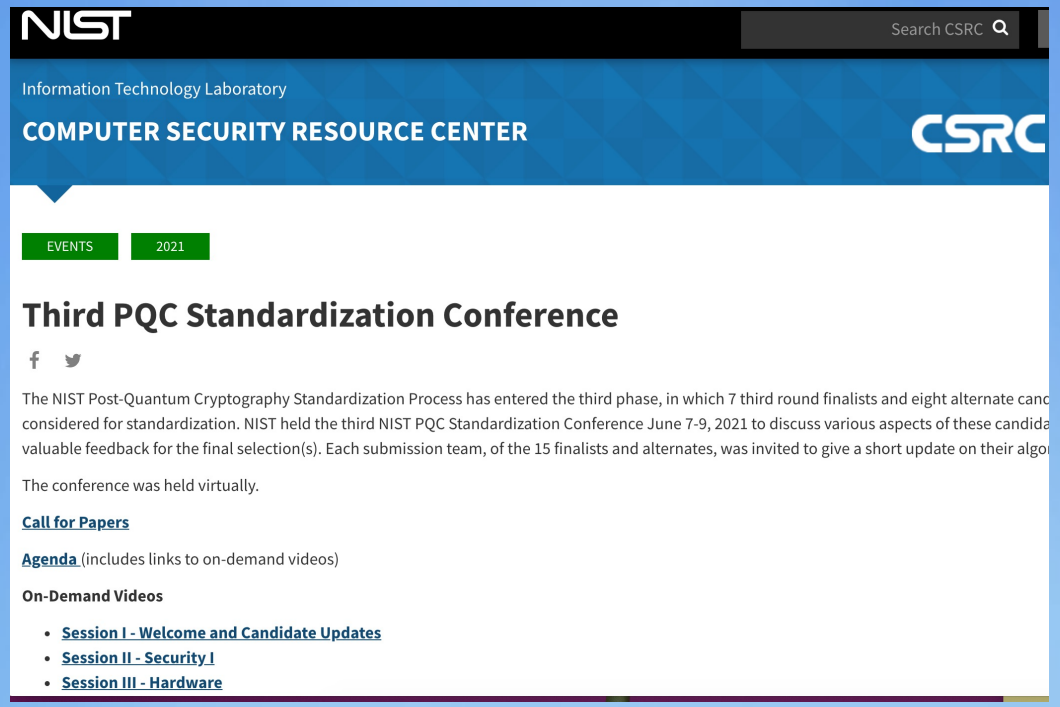
- Cryptanalytic results during the 3rd round have created some concerns about the security of both multivariate schemes **Rainbow** and **GeMSS**

- Jan 2021 pqc-forum post from NIST:
  - "NIST sees **SPHINCS+** as an extremely conservative choice for standardization. If NIST's confidence in better performing signature algorithms is shaken by new analysis , **SPHINCS+** could provide an immediately available algorithm for standardization at the end of the third round. "

  - "NIST is pleased with the progress of the PQC standardization effort but recognizes that current and future research may lead to promising schemes which were not part of the NIST PQC Standardization Project. *NIST may adopt a mechanism to accept such proposals at a later date. In particular, NIST would be interested in a general-purpose digital signature scheme which is not based on structured lattices.*"

The 3rd NIST PQC Conference

- June 2021, held virtually
  - Over 400 participants
  - 38 accepted papers
  - 15 candidate team updates
  - Video, slides, papers posted at our website



- Announcements:
  - 4th round
  - on-ramp for signatures

- Ongoing research:
  - Hardware and software implementations, side-channel analysis, cryptanalysis of 3rd round candidates, PQC in applications and protocols, formal verification, security, variants of candidates, etc

What lies ahead….

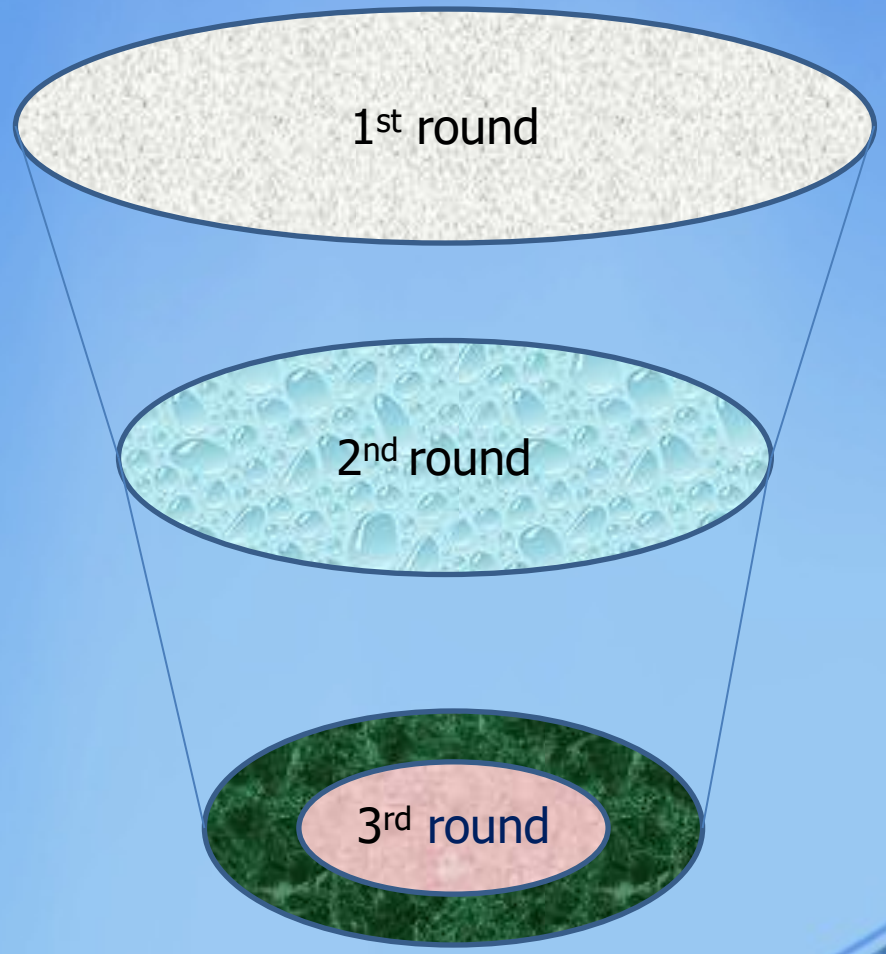
- The 3rd Round will end sometime close to the end of 2021
  - NIST will announce which finalist algorithms it will standardize
    - (As mentioned previously, also potentially SPHINCS+)
  - This will include algorithms which will be able to be used by most applications
  - NIST will issue a Report on the 3rd Round to explain our decisions
- NIST will also announce any candidates advancing to 4th round
  - The 4th round will similarly be 12-18 months
  - These algorithms will be for a diversified portfolio, or for applications with different performance needs
- We expect to release draft standards for public comment in 2022-2023
- The first set of standards will hopefully be finalized by 2024

An on-ramp for signatures

- At the conclusion of the 3rd Round, NIST will issue a new Call for Proposals
  - There will be a deadline for submission, likely 6 months – 1 year
  - This will be much smaller in scope than main NIST PQC effort
  - The main reason for this call is to diversify our signature portfolio
- 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.
- The more mature the scheme, the better.
- NIST will decide which (if any) of the received schemes to focus attention on

How will NIST make its decisions?

- Using the evaluation criteria:
- Security
  - Security levels offered
  - (confidence in) security proof
  - Any attacks
  - Classical/quantum complexity
- Performance
  - Size of parameters
  - Speed of KeyGen, Enc/Dec, Sign/Verify
  - Decryption failures
- Algorithm and implementation characteristics
  - IP issues
  - Side channel resistance
  - Simplicity and clarity of documentation
  - Flexible
- Other
  - Official comments/pqc-forum discussion
  - Papers published/presented



How will NIST make its decisions?

- For the lattice KEMs, the main decision will be **Kyber/NTRU/Saber**
- Similarly for lattice signatures, the main decision will be **Dilithium/Falcon**
- Any other algorithms selected will be their own distinct decision

- We very much want analysis to continue on **ALL** of the finalists

- As we are moving closer to our selection, IP issues are an important factor
  - "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.***"

Patent and IPR issues

- This is a very complicated area
- We acknowledge the impact of encumbered technology on adoption

- NIST is actively engaging to try to resolve known IPR issues on the candidates
- When we have something concrete, we will share it

- **Note: it may not be possible for NIST to resolve all IP concerns**

- In light of the above, NIST believes the discussion should be around the impact of IP, and how we should factor these issues into our decision-making
  - *NIST would very much appreciate feedback on the impact of potentially selecting algorithms which may be encumbered*

Research Challenges

- Many important topics to be studied:
  - Security proofs in both the ROM and QROM
  - Does the specific ring/module/field choice matter for security?
    - Or choice of noise distribution?
    - Does "product" or "quotient" style LWE matter?
  - Finer-grained metrics for security of lattice-based crypto (coreSVP vs. real-world security)
  - Are there any important attack avenues that have gone unnoticed?
  - Side-channel attacks/resistant implementations for finalists and alternates
  - More hardware implementations
  - Ease of implementations – decryption failures, floating point arithmetic, noise sampling, etc.
- Specific algorithm questions
  - Decoding analysis for BIKE, category 1 security levels for Kyber/Saber/Dilithium, algebraic cryptanalysis of cyclotomics for lattices, etc…

Analysis still needed

- There has been much discussion over the past several months
  - Security of lattice based candidates
    - (See pqc-forum posts)
  - Security of code-based candidates
    - See the recent post by NIST on pqc-forum
    - There is a multi-cipher text attack scenario not explicitly covered by the security definitions given in the CFP. How should NIST deal with this?
    - A 2nd question on concrete number of bit operations needed to perform an ISD attack that may be applicable to the code-based schemes. NIST would like more analysis.
  - Use cases with hard performance constraints
    - Do the candidates fit on highly constrained platforms?
  - Other issues?

The transition to PQC

- NIST will issue guidance on the transition
- An update from last year on SP 800-56C Rev. 2 allows for a "hybrid mode" to combine shared secrets for key-establishment
  - In other words, you can combine an unapproved (i.e. a PQC) algorithm with a NIST-approved algorithm and still receive FIPS validation

- NIST SP 800-208, *Recommendation for Stateful Hash-based Signature Schemes*, was published
  - The SP approves certain parameter sets for XMSS and LMS

- The National Cybersecurity Center of Excellence (NCCoE) released a whitepaper and project description for Migration to PQC

Conclusion

- We can start to see the end?
- NIST is grateful for everybody's efforts
- Check out www.nist.gov/pqcrypto
  - Sign up for the pqc-forum for announcements & discussion
  - Contact us at: pqc-comments@nist.gov