NIST Status Update on the 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

A few things….

- Slack and Bluejeans Q+A
- How to get help
  - Moderator chat on Bluejeans
  - Slack channel (help-desk)
  - Email: conferences@nist.gov or pqc2021@nist.gov
- Talks are being recorded, and will be posted later…
- On Wednesday, there will be a NIST Q+A session
  - Ask questions on the slack channel nist_q-and-a

- (End of conference survey will have a few questions as well)
- Thanks to everybody!

How we got here...

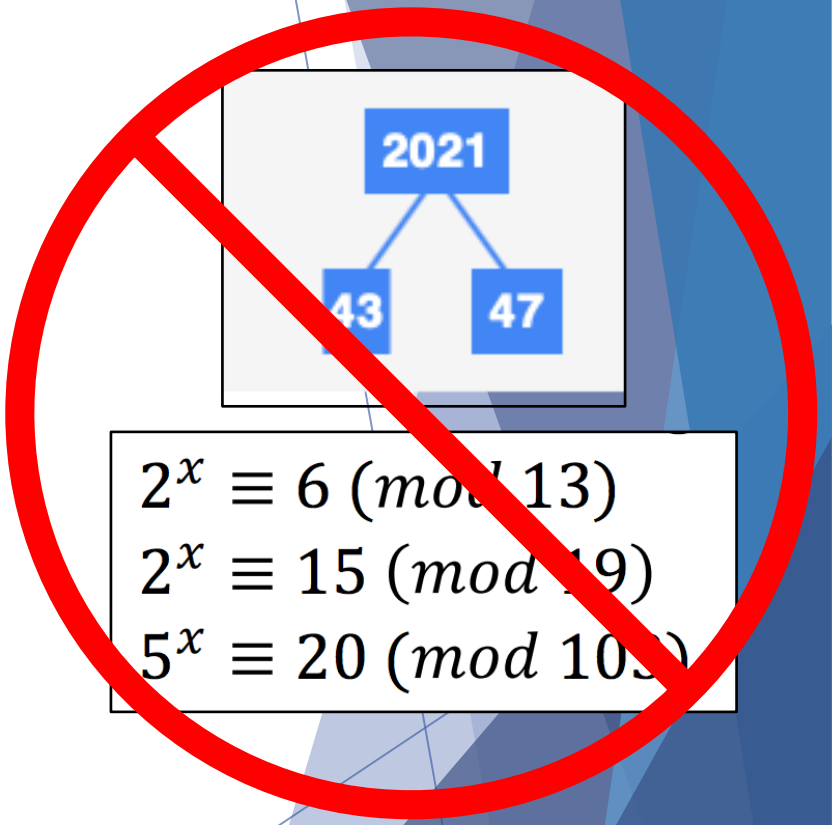
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

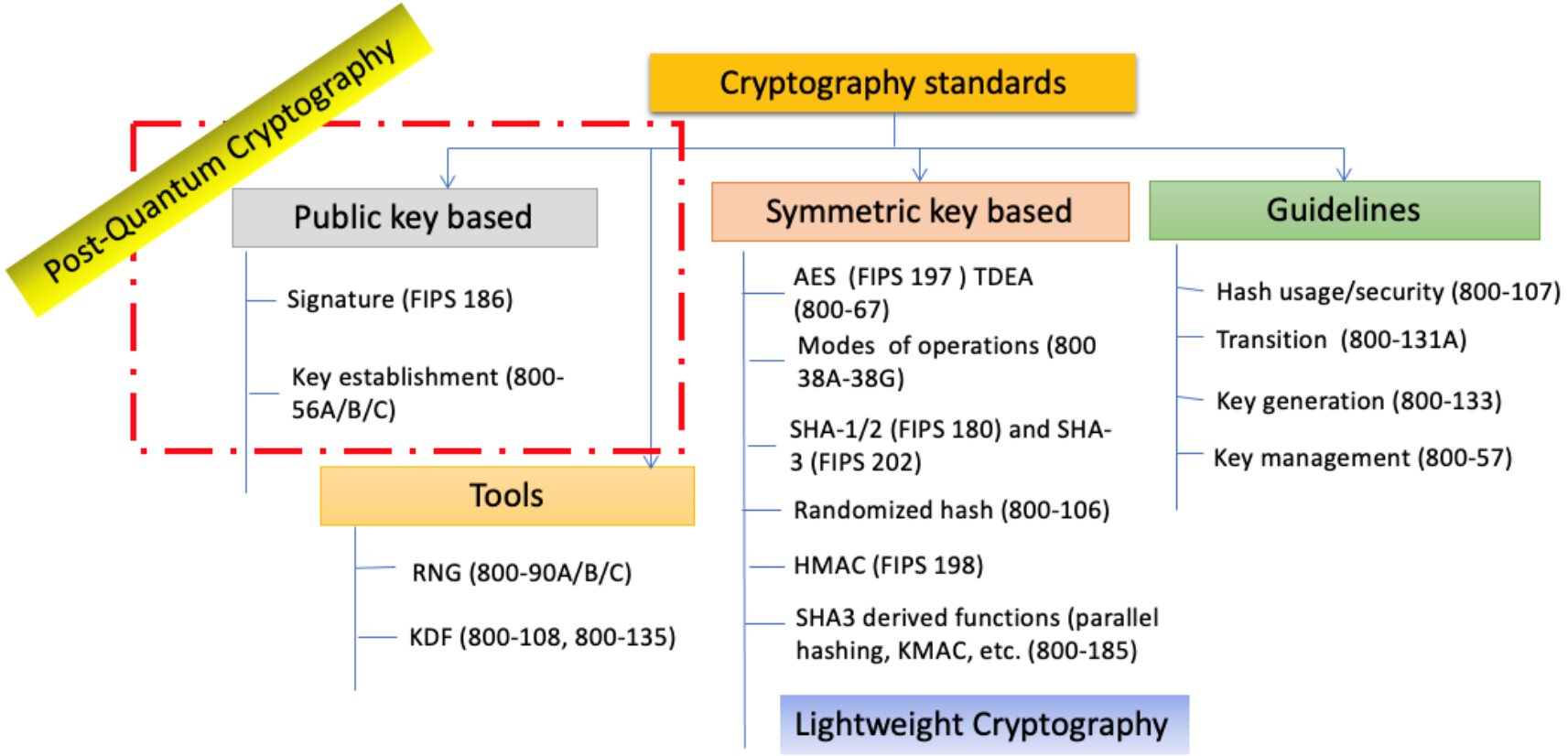
Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms



NIST Crypto Standards



NIST PQC Milestones

- 2015 – NIST Workshop on PQC
- 2016 – NIST report on PQC: NISTIR 8105
- 2016 – NIST announces “competition-like” process
- 2017 – Deadline for submissions
  - 82 submissions received. 69 accepted as 1st round candidates
- 2018 – 1st NIST PQC Standardization Conference
- 2019 – Announced 26 algorithms moving to the 2nd round
  - 1st Round Report: NISTIR 8240
- 2019 – 2nd NIST PQC Standardization Conference
- 2020 – Announced 3rd round 7 Finalists and 8 Alternate candidates
  - 2nd Round Report: NISTIR 8309
- 2021 - 3rd NIST PQC Standardization Conference
- 2022-2023 – Release draft standards and call for public comments

NIST PQC Milestones

- 2015 – NIST Workshop on PQC
- 2016 – NIST report on PQC: NISTIR 8105
- 2016 – NIST announces "competition-like" process
- 2017 – Deadline for submissions
  - 82 submissions received. 69 accepted as 1st round candidates
- 2018 – 1st NIST PQC Standardization Conference
- 2019 – Announced 26 algorithms moving to the 2nd round
  - 1st Round Report: NISTIR 8240
- 2019 – 2nd NIST PQC Standardization Conference

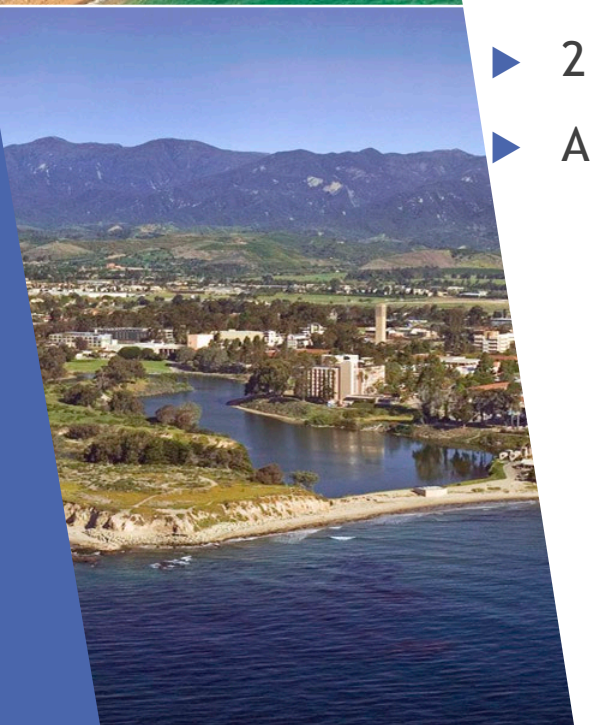
- 2020 – Announced 3rd round 7 Finalists and 8 Alternate candidates
  - 2nd Round Report: NISTIR 8309
- 2021 - 3rd NIST PQC Standardization Conference
- 2022-2023 – Release draft standards and call for public comments

Evaluation Criteria

- **Security** – against BOTH classical and quantum attacks

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)

- **Performance** – measured on a variety of classical platforms
- **Other properties**: Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, Any factors which could hinder adoption, etc…



The First 2 Rounds

- 69 Submissions in the 1st Round ⟹ 26 in the 2nd Round
- The majority were lattice-based or code-based
- Cryptanalysis attacked several schemes
- NIST encouraged several mergers
- The pqc-forum discussion and "Official Comments"
- 2 NIST workshops and status reports (NISTIR 8240 and 8309)
- A lot of research, benchmarking, and real-world experiments

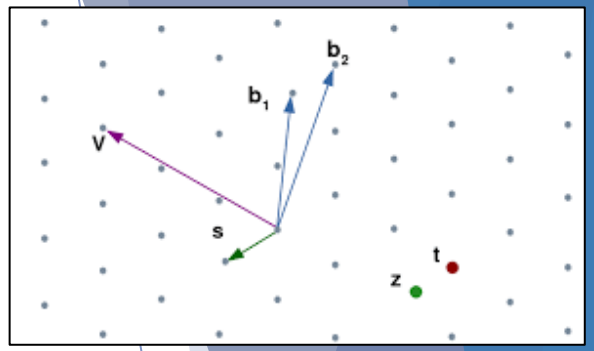
	Signatures		KEM/Encryption		Overall	
	Rd 1	Rd 2	Rd 1	Rd 2	Rd 1	Rd 2
Lattice-based	5	3	21	9	26	12
Code-based	2		17	7	19	7
Multi-variate	7	4	2		9	4
Hash/Symmetric	3	2			3	2
Other	2		5	1	7	1
Total	19	10	45	16	64	26

The 3rd Round

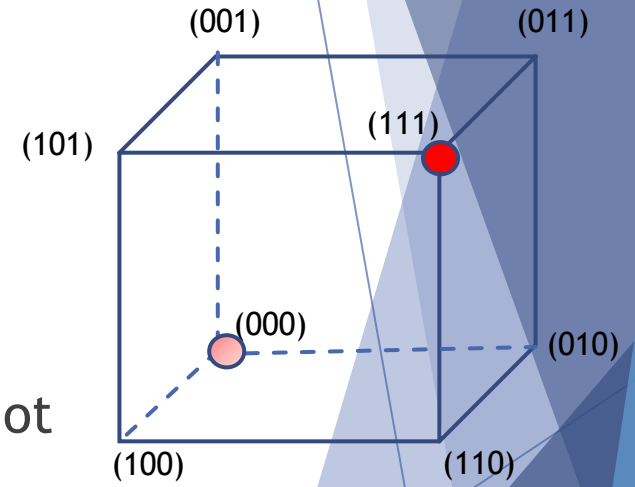
- July 2020: NIST selected 7 **Finalists** and 8 **Alternates**
  - Finalists: most promising algorithms we expect to be ready for standardization at the end of the 3rd round
  - Alternates: candidates for potential standardization, most likely after another (4th) round

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

The KEMs

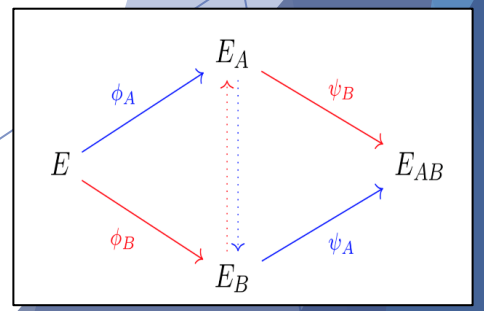


- The finalists **Kyber, NTRU, SABER** are based on structured lattices
  - *NIST expects to select at most one for standardization*
- **Classic McEliece**, the other finalist, is based on codes



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

- The alternates **BIKE** and **HQC** are based on structured codes
- The final alternate **SIKE** is based on isogenies of elliptic curves



The Signatures

- The finalists **Dilithium** and **Falcon** are both based on structured lattices
  - *NIST expects to select at most one for standardization*
- There are two multivariate schemes: the finalist **Rainbow**, and the alternate **GeMSS**
- The alternate **Picnic** is based on some symmetric primitives
- The alternate **SPHINCS+** is based on the security of hash functions

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.*"

An on-ramp for new 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

- 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

Timeline

- The 3rd Round will end sometime close to the end of 2021
  - NIST will announce which finalist algorithms it will standardize
  - NIST will also announce any candidates that will advance on to a 4th round of study
  - The 4th round will similarly be 12-18 months
- NIST will issue a Report on the 3rd Round to explain our decisions
- We expect to release draft standards for public comment in 2022-2023
- The finalized standard will hopefully be ready by 2024

How will NIST makes its selection?

- Using the evaluation criteria: Security, Performance, and Other Properties

- 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

- An important factor during the 3rd round is proving to be IP issues related to the candidates
  - "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.***"

Patents 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

The transition to PQC algorithms

- 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: *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*

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