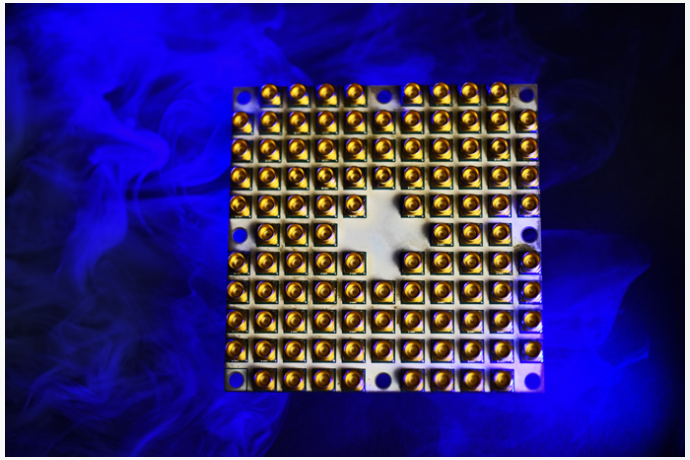
Let's Get Ready to Rumble– The NIST PQC "Competition"

Dustin Moody
NIST

The Rise of Quantum Computing



Intel's 49-qubit chip
"Tangle-Lake"
January 2018

Google's 72-qubit chip
"Bristlecone"
March 2018

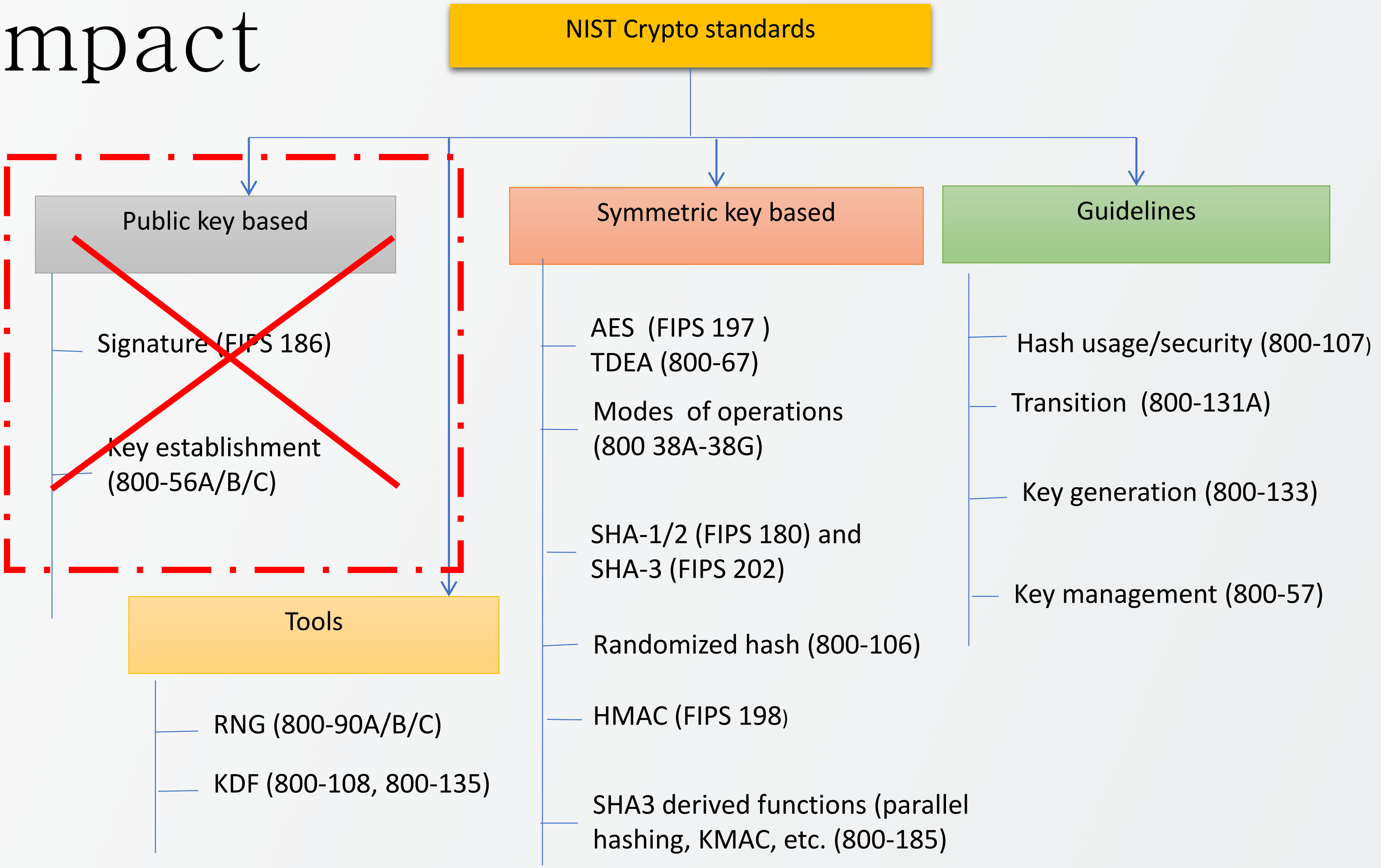
IBM's 50-qubit
quantum computer
November 2017

The Impact

NIST Crypto standards

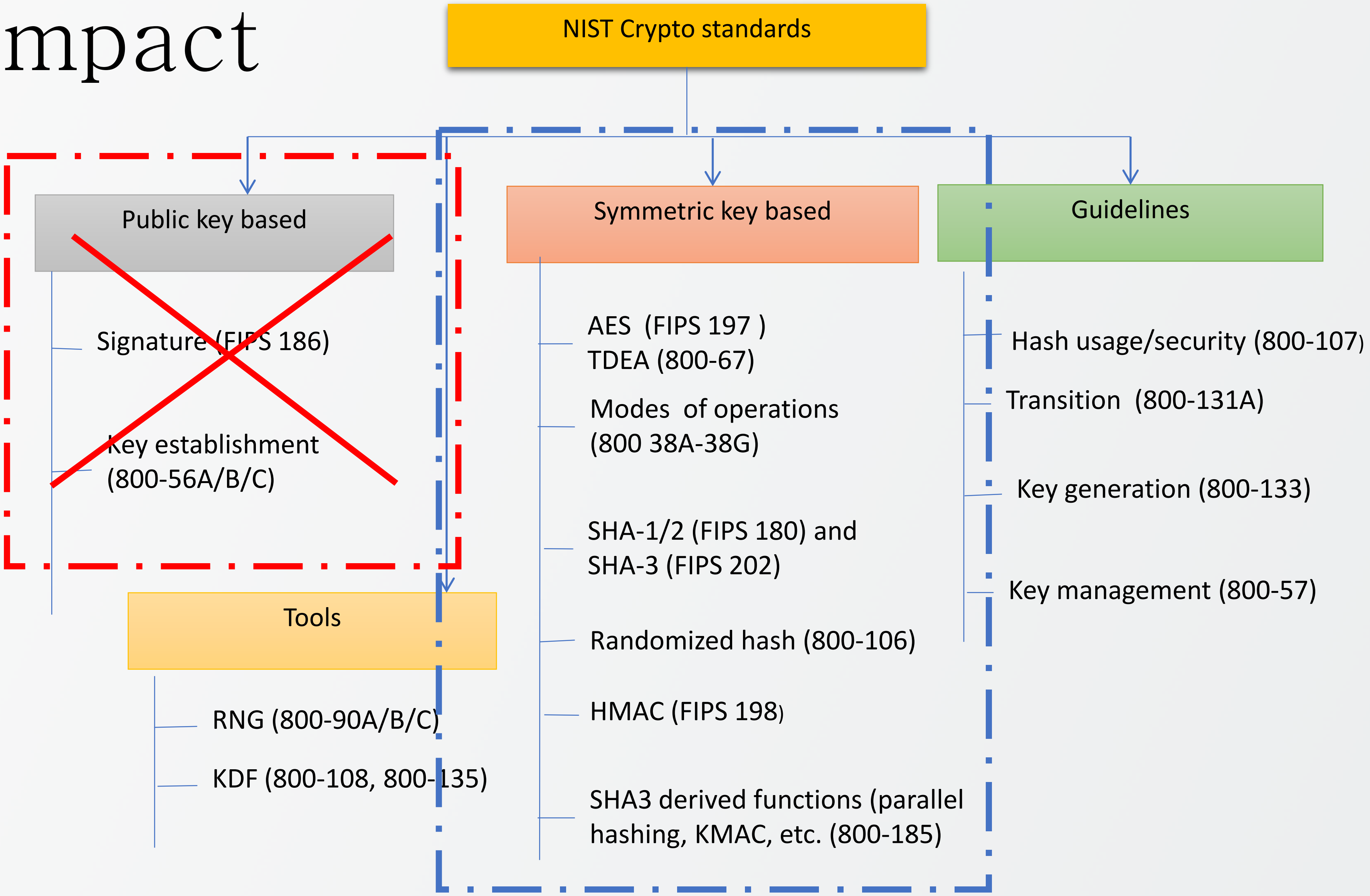
- **Public key based**
  - Signature (FIPS 186)
  - Key establishment (800-56A/B/C)
- **Tools**
  - RNG (800-90A/B/C)
  - KDF (800-108, 800-135)
- **Symmetric key based**
  - AES (FIPS 197)
    TDEA (800-67)
  - Modes of operations (800 38A-38G)
  - SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
  - Randomized hash (800-106)
  - HMAC (FIPS 198)
  - SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)
- **Guidelines**
  - Hash usage/security (800-107)
  - Transition (800-131A)
  - Key generation (800-133)
  - Key management (800-57)

The Impact



NIST Crypto standards
Public key based
Signature (FIPS 186)
Key establishment
(800-56A/B/C)
Symmetric key based
AES (FIPS 197)
TDEA (800-67)
Modes of operations
(800 38A-38G)
SHA-1/2 (FIPS 180) and
SHA-3 (FIPS 202)
Randomized hash (800-106)
HMAC (FIPS 198)
SHA3 derived functions (parallel
hashing, KMAC, etc. (800-185)
Guidelines
Hash usage/security (800-107)
Transition (800-131A)
Key generation (800-133)
Key management (800-57)
Tools
RNG (800-90A/B/C)
KDF (800-108, 800-135)

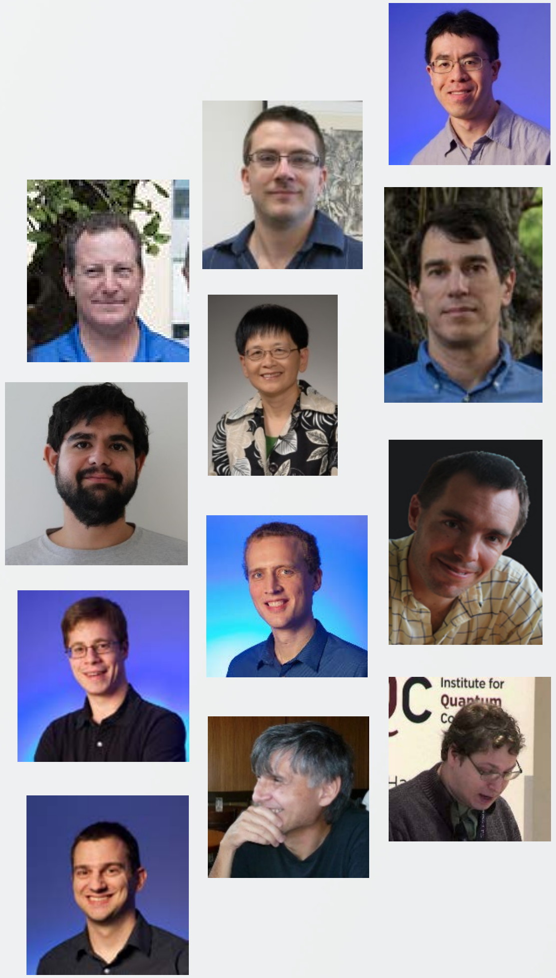
The Impact



NIST Crypto standards
Public key based
Signature (FIPS 186)
Key establishment
(800-56A/B/C)
Tools
RNG (800-90A/B/C)
KDF (800-108, 800-135)
Symmetric key based
AES (FIPS 197)
TDEA (800-67)
Modes of operations
(800 38A-38G)
SHA-1/2 (FIPS 180) and
SHA-3 (FIPS 202)
Randomized hash (800-106)
HMAC (FIPS 198)
SHA3 derived functions (parallel
hashing, KMAC, etc. (800-185)
Guidelines
Hash usage/security (800-107)
Transition (800-131A)
Key generation (800-133)
Key management (800-57)

The NIST PQC Project

- 2009 – NIST publishes a PQC survey
  - Quantum Resistant Public Key Cryptography: A Survey [D. Cooper, R. Perlner]
- 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

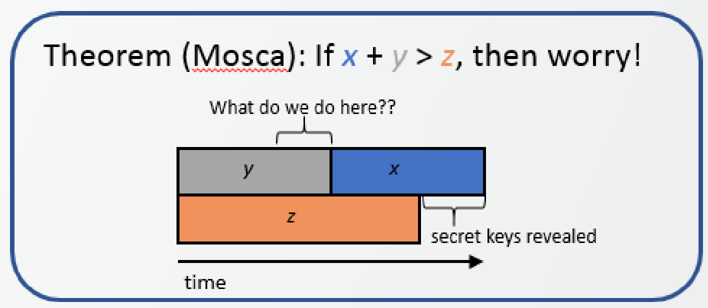


PQC Standardization – when?

- There had been much debate about whether it is too early to look into PQC standardization
- When will a (large-scale) quantum computer be built?

    - **"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."**

      – Dr. Michele Mosca, (April 2015)



- Our experience tells us that we need (at least) several years to develop and deploy PQC standards

The Decision to Move Forward

- Aug 2015 – NSA statement
  - **...** "IAD will initiate a transition to *quantum resistant algorithms* in the **not too distant future ...**"
- Feb 2016 – NIST Report on PQC (NISTIR 8105)
- Feb 2016 – NIST announcement at PQCrypto

- 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"

Timeline

- Aug 2016 – Draft submission requirements & evaluation criteria
- Dec 2016 – Final requirements and criteria
- Nov 2017 – Deadline for submissions
- Apr 2018 – NIST PQC Workshop – submitters' presentations
- 2018/2019 – 2nd Round begins (smaller number of submissions)
  - minor changes allowed
- Aug 2019 – 2nd NIST PQC Workshop
- 2020/2021 - Select algorithms or start a 3rd Round
- 2022-2024 - Draft standards available

- NIST will release reports on progress and selection rationale

Scope

- **Signatures**
  - Public-key schemes for generating/verifying signatures (see FIPS 186-4)
- **Encryption**
  - Key transport from one party to another
  - Exchanging encrypted secret values between two parties to establish shared secret value (see SP 800-56B)
- **Key-establishment (KEMs)**
  - Schemes like Diffie-Hellman key exchange (see SP 800-56A)

Differences with past Competitions

- Post-quantum cryptography is more complicated than AES/SHA-3
  - No silver bullet - each candidate has some disadvantage
  - Not enough research on quantum algorithms to ensure confidence for some schemes
- We do not expect to select just one algorithm
  - Ideally, several algorithms will emerge as “good choices”
- We will narrow our focus at some point
  - This does not mean algorithms are “out”
- Requirements/timeline could potentially change based on developments in the field

Complexities

- Much broader scope – three crypto primitives
- Both classical and quantum attacks
  - Security strength assessment on specific parameter selections
- Consider various theoretical security models and practical attacks
  - Provably security vs. security against instantiation or implementation related security flaws and pitfalls
- Multiple tradeoff factors
  - Security, performance, key size, signature size, side-channel resistance countermeasures
- Migrations into new and existing applications
  - TLS, IKE, code signing, PKI infrastructure, and much more
- Not exactly a competition – it is and it isn’t

The Selection Criteria

- Security - against both classical and quantum attacks
- Performance - measured on various "classical" platforms
- Other properties
  - Drop-in replacements - Compatibility with existing protocols and networks
  - Perfect forward secrecy
  - Resistance to side-channel attacks
  - Simplicity and flexibility
  - Misuse resistance, and
  - More

Security Analysis

- Security definitions (proofs recommended, but not required)
  - IND-CPA/IND-CCA2 for encryption, KEMS
  - EUF-CMA for signatures
  - Used to judge whether an attack is relevant
- Quantum/classical algorithm complexity
  - Classical computers may have the cheapest attacks in practice
  - Stability of best known attack complexity
  - Precise security claim against quantum computation
- Quality and quantity of prior cryptanalysis

Quantum Security

- No clear consensus on best way to measure quantum attacks
- Uncertainties
  - The possibility that new quantum algorithms will be discovered, leading to new attacks
  - The performance characteristics of future quantum computers, such as their cost, speed and memory size
- For PQC standardization, need to specify concrete parameters with security estimates

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

Cost and Performance

- Standardized post-quantum cryptography will be implemented in "classical" platforms
- Ideally, implementable on wide variety of platforms and applications
- May need to standardize more than one algorithm for each function to accommodate different application environments
- Allowing parallel implementation for improving efficiency is certainly a plus
- Preliminary conclusions: efficiency likely OK, but key sizes may pose a significant challenge

Complexities – Part 2

- Assess classical security
  - Many PQC schemes are relatively new. It'll take years to understand their classical security. Let alone quantum security.

- We need to deal with new situations which we haven't considered before, e.g.
  - Decryption failure
  - State management for hash based signatures
  - Public-key encryption vs. key-exchange issues
    - Public-key encryption IND-CCA2
    - Ephemeral key exchange (no key-pair reuse, consider passive attacks, IND-CPA)
  - Auxiliary functions/algorithms, e.g.
    - Gaussian distribution sampling/simulation

Intellectual Property

- “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.”
  - All submitters must declare known patents
  - Reminder: submitters turn in your signed IP statements
- Submissions (and implementations) are freely available for public review and evaluation
- In Round 1, all submissions should be evaluated on their technical merits.

Submissions

- 37 preliminary submissions (early deadline Sep 2017)
- 82 total submissions received
  - 69 accepted as "complete and proper"   (5 since withdrawn)

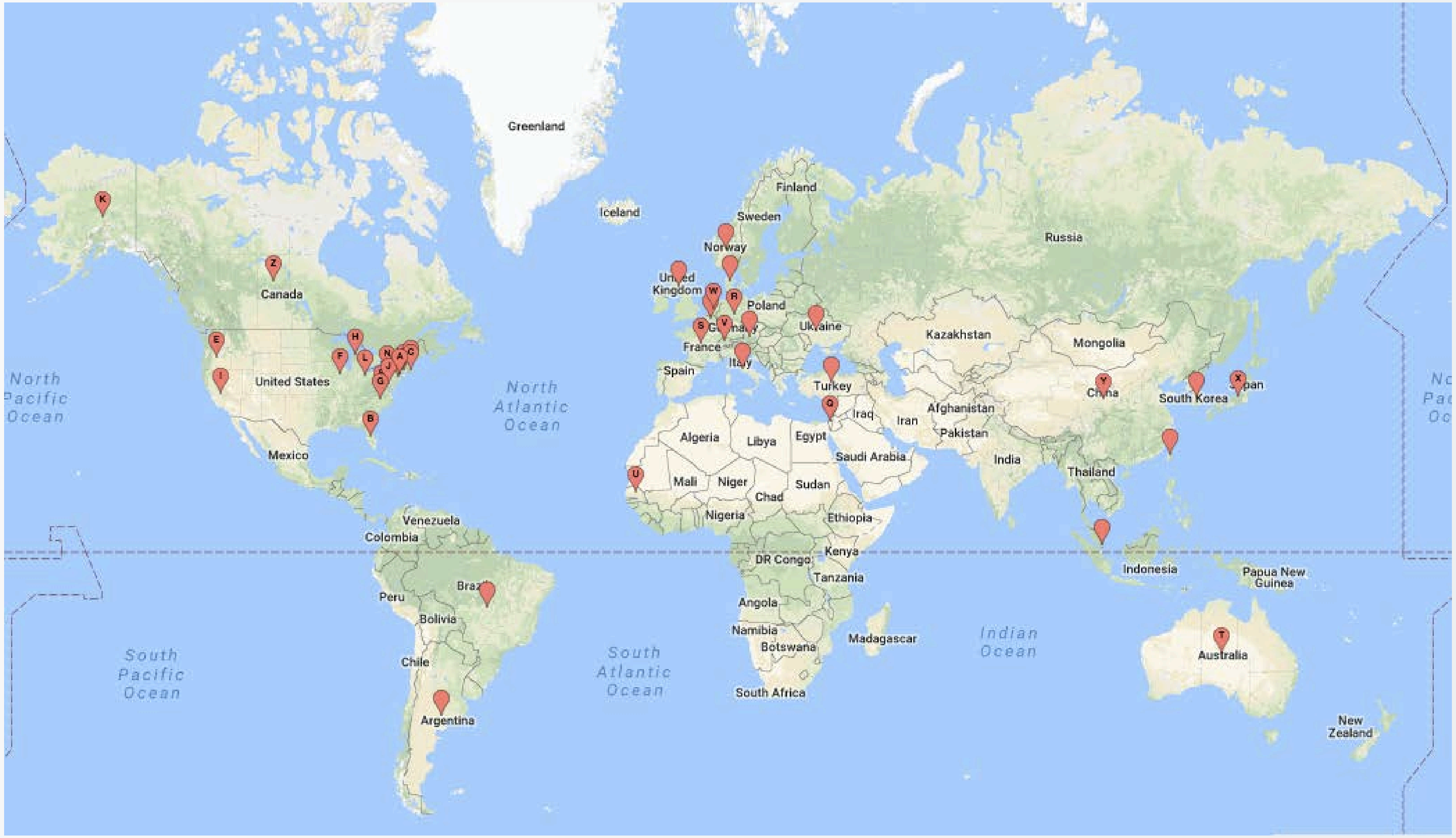
	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric/Hash-based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

Numbers

- We have a total of 278 submitters
  - 67 of those were on more than one submission
    - Distribution: [212, 30, 22, 7, 2, 1, 4, 1]

- Most submissions cover security levels 1,3, and 5.
  - 10 submissions target only the lower levels 1,2,3
    - CFPKM, CompactLWE, Emblem/R.Emblem, NTRU-HRSS-KEM, PQRSA Enc/Sig, QC MDPC-KEM, Gravity-SPHINCS, HiMQ-3, RaCoSS
  - 6 submissions target only the high security levels 4,5
    - Classic McEliece, GuessAgain, Hila5, Mersenne-756839, NTRUprime, KCL

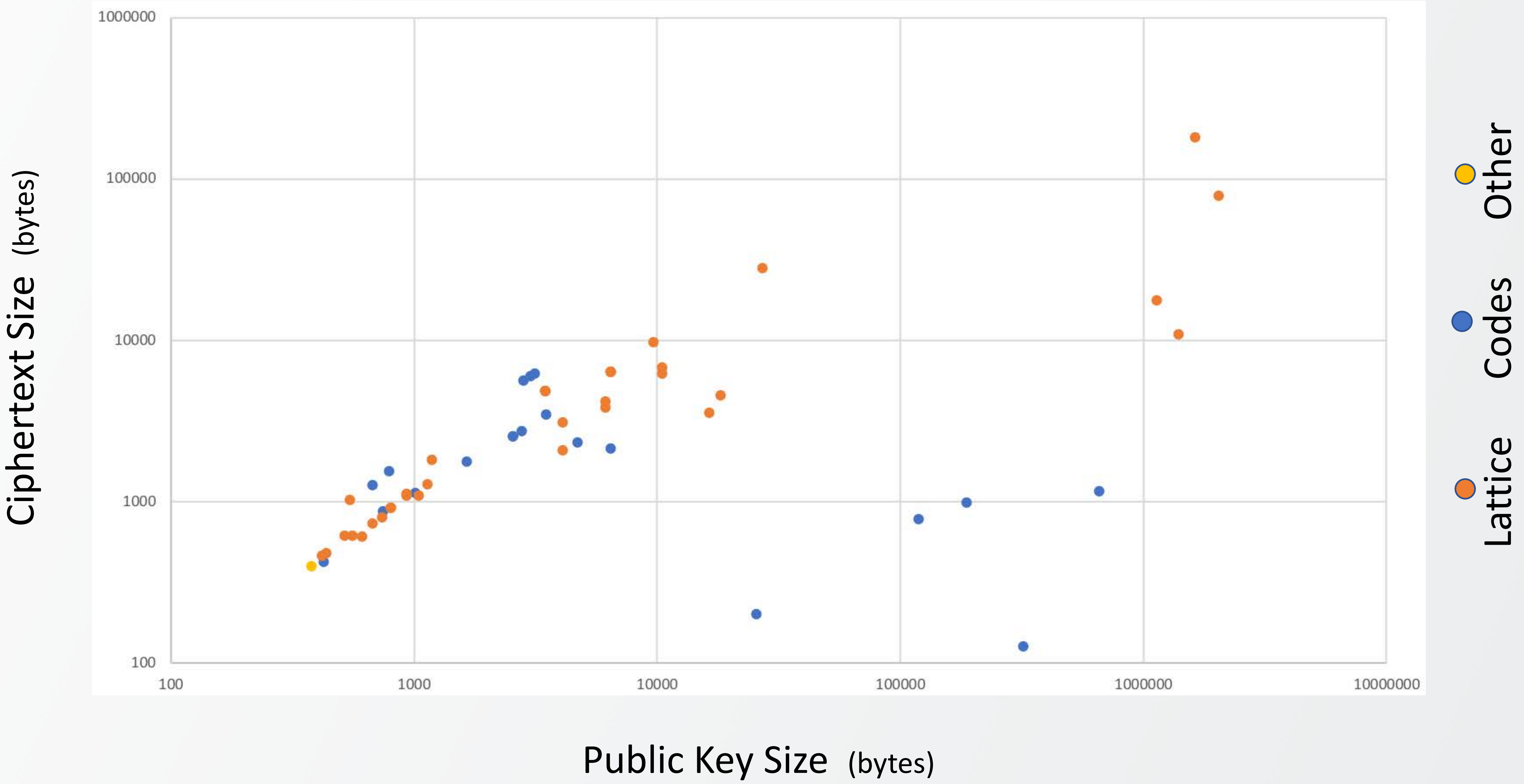
25 Countries, 16 States, 6 Continents



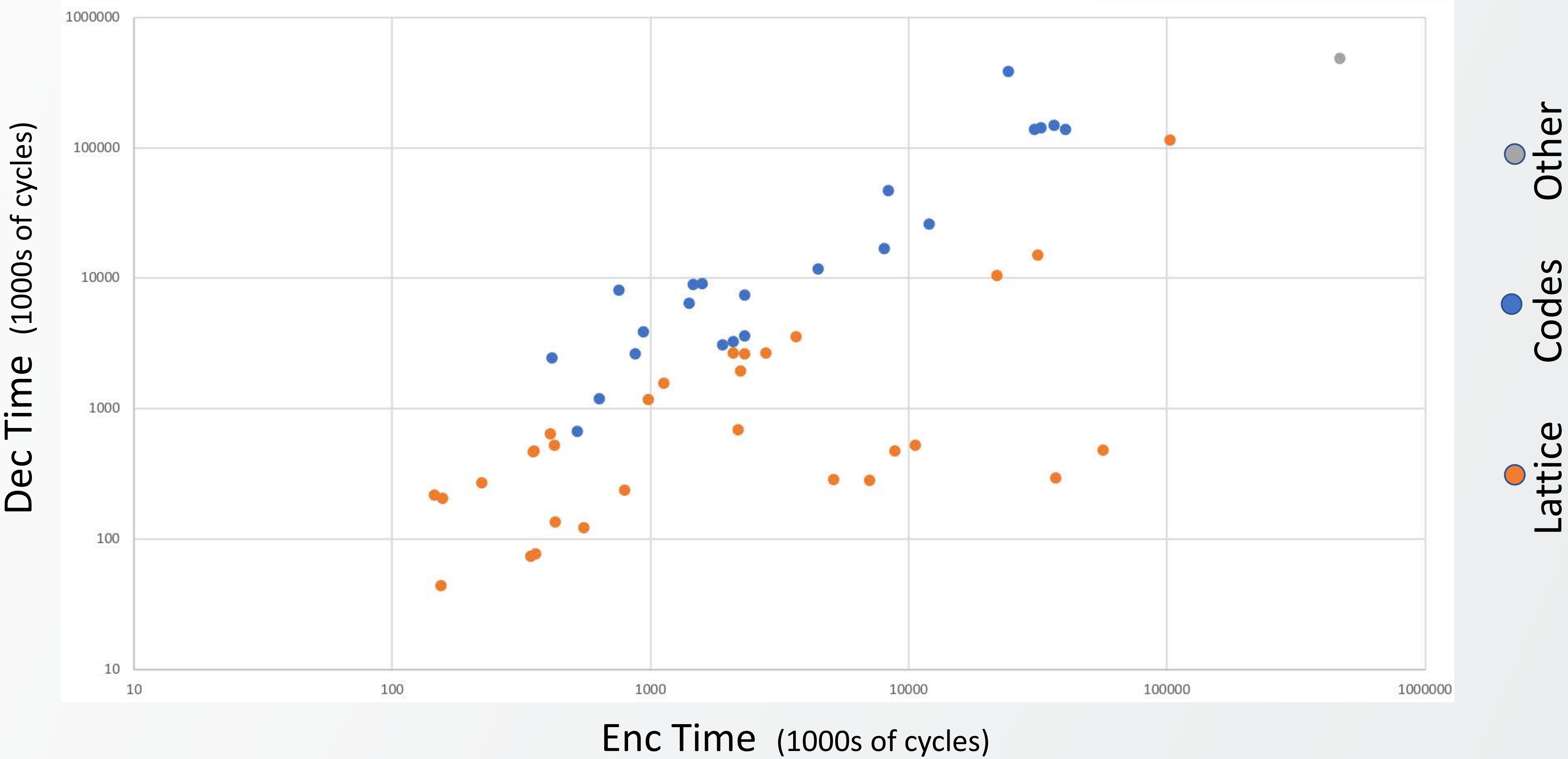
Key Sizes & Performance Graphs

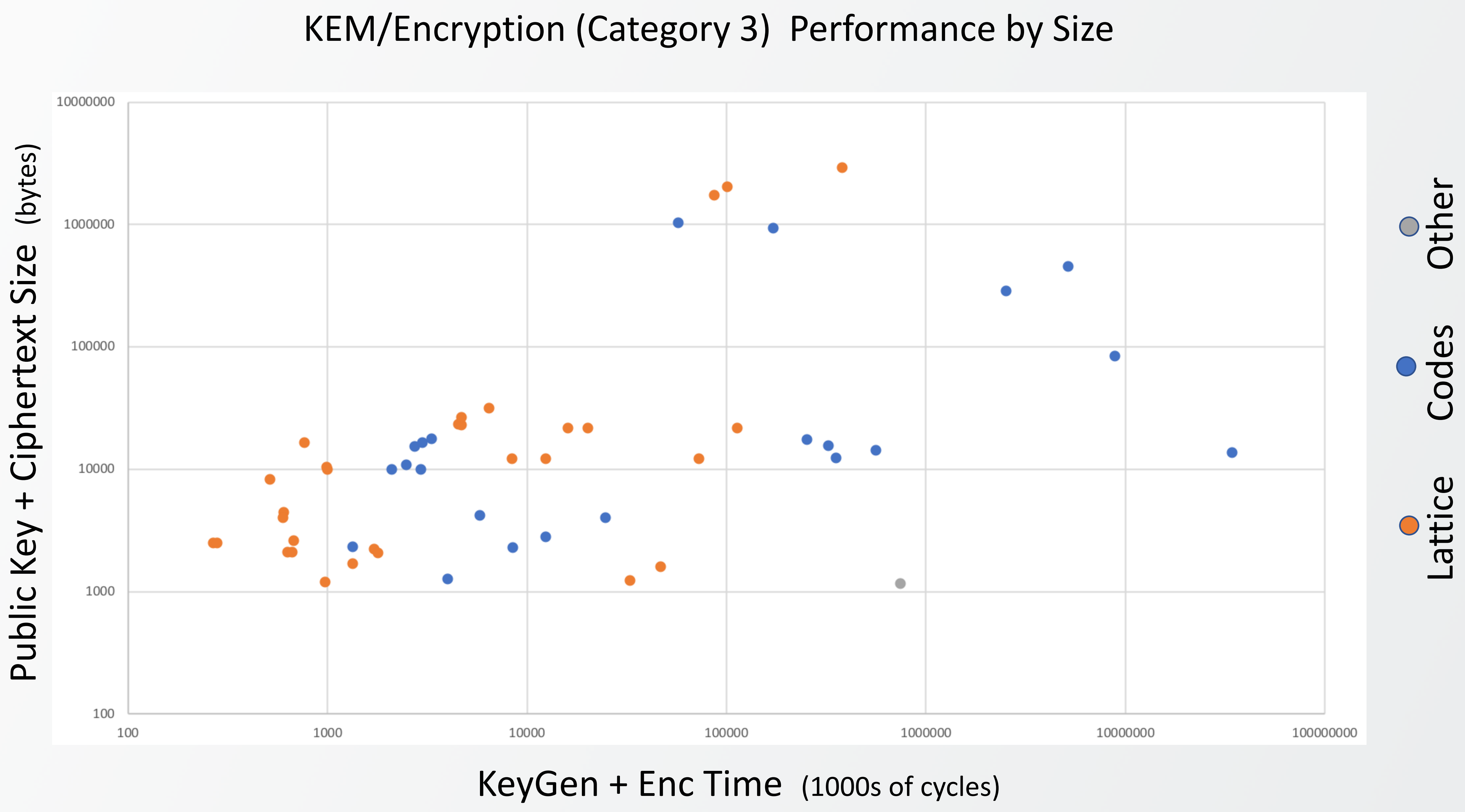
- Reminder: “It is important to note that performance considerations will **NOT** play a major role in the early portion of the evaluation process.”
- Disclaimer – These are from the optimized implementations submitted to us. We know better implementations exist/will exist.
- These charts should mainly be used to see general patterns
  - While performance will vary with implementations, key sizes won’t

KEM/Encryption (Category 1)

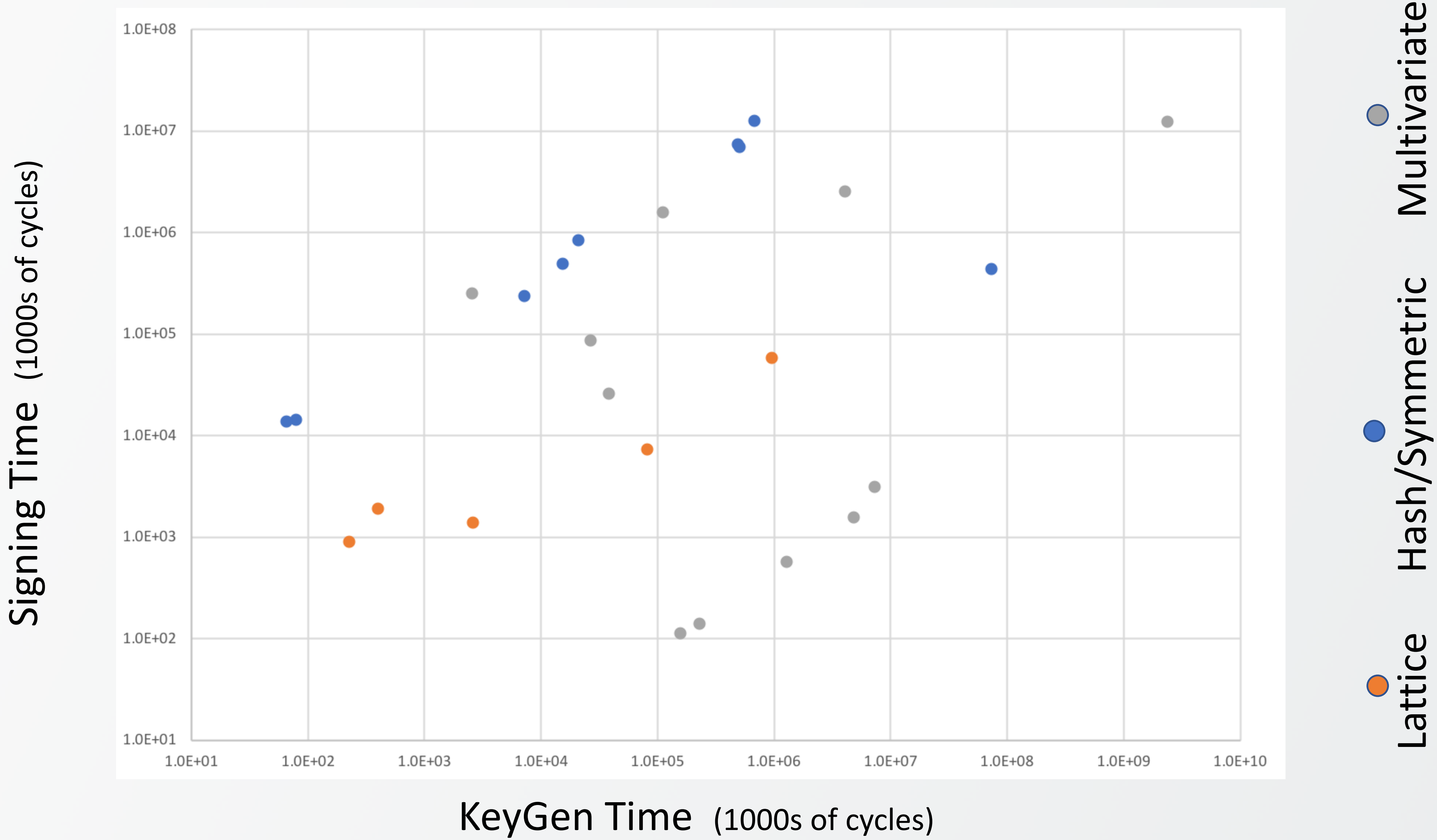


KEM/Encryption (Category 3) Performance

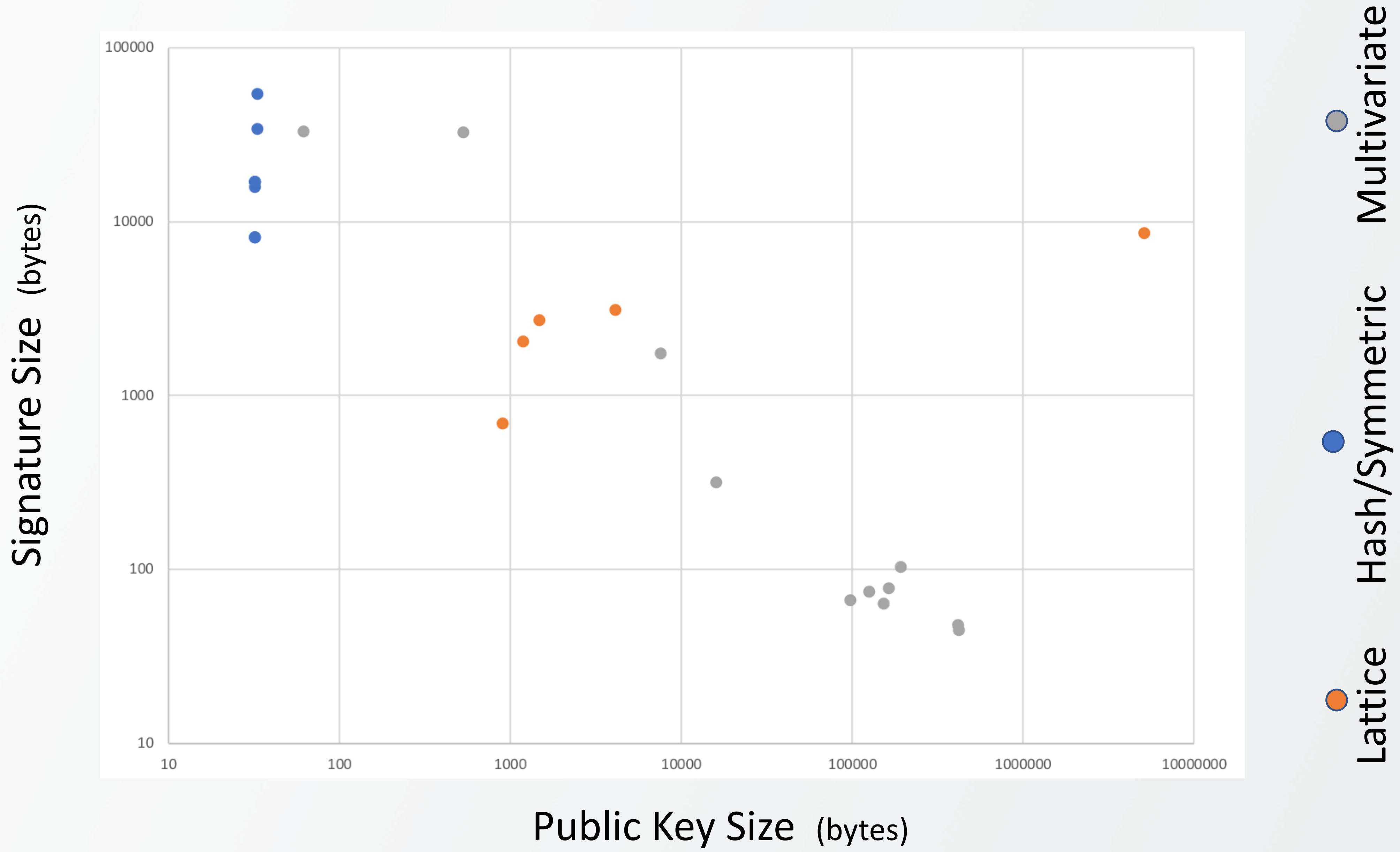



KEM/Encryption (Category 3) Performance by Size
Public Key + Ciphertext Size (bytes)
10000000
1000000
100000
10000
1000
100
100
1000
10000
100000
1000000
10000000
100000000
KeyGen + Enc Time (1000s of cycles)
Other
Codes
Lattice

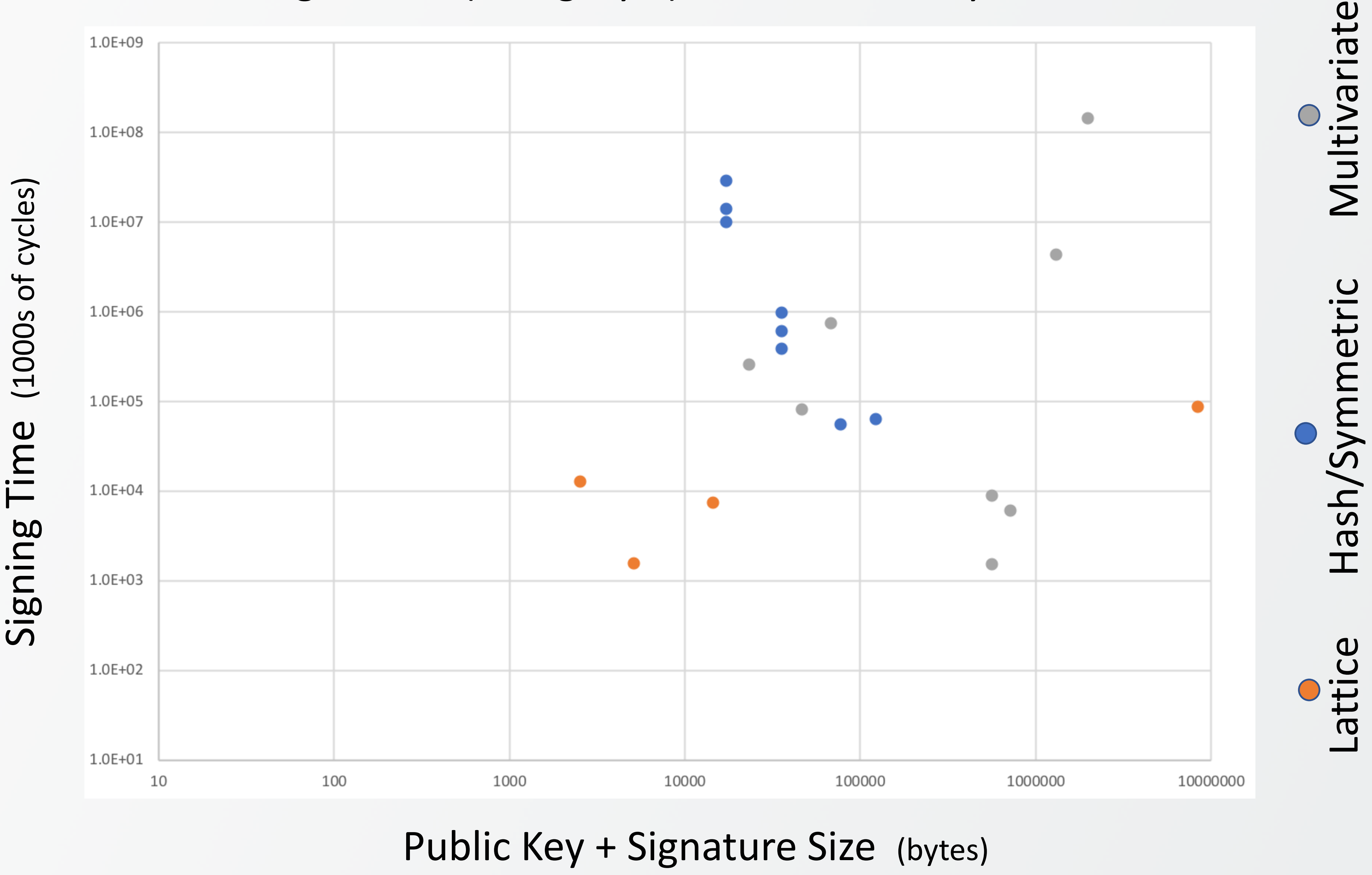
Signatures (Category 1) Performance



Signature (Category 1) Sizes



Signatures (Category 3) Performance by Size



Discussion and Questions

- Since the draft call for proposals was announced, the NIST team has actively interacted with submitters and researchers

- The questions include
  - APIs to support different ancillary functions
  - Using third party libraries
  - Submission format
  - Decryption failure
  - etc.

- The topics discussed at pqc-forum@nist.gov include
  - Quantum vs. classical security strength
  - Security notions (IND-CCA2, IND-CPA, etc.)
  - Random number generation
  - Key exchange vs. key encapsulation (KEMs)
  - Implementation details, (constant-time, etc.....)
  - Official comments on submissions
  - IP/patent issues

- Answers to the common questions and summaries on the major discussion topics are added to the FAQ at www.nist.gov/pqcrypto

Official Comments

- Submit “official comments” on our website using link for each submissions
  - Alternatively, post in the pqc-forum with “Official Comment: NameOfSubmission” in the subject line
- Comments can be minor (bug fixes) or major (breaks)
  - Often are questions, which are answered by submitters
- 38 submissions have received official comments
  - 26 submissions have none
  - 18 submissions have 2 or less
- 210 official comments so far
  - ~60% of these are on 10 submissions.

Transition and Migration

- NIST will update guidance when PQC standards are available
- A “hybrid mode” has been proposed as a transition/migration step towards PQC
  - Such a mode combines a classical algorithm with a post-quantum one
  - Current FIPS 140 validation will only validate the NIST-approved (classical) component
  - The PQC standardization will only consider the post-quantum component
- NIST plans to consider (stateful) hash-based signatures as an early candidates for standardization
  - Only for specific applications like code signing
  - We hope to hear from industry and implementers on the urgency/impact of hash-based signatures

Standards Organizations

- We are aware that many standards organizations and expert groups are working on PQC
  - IEEE P1363.3 has standardized some lattice-based schemes
  - IETF is taking action in specifying stateful hash-based signatures
  - ETSI has released quantum-safe cryptography reports
  - EU expert groups PQCRYPTO and SAFEcrypto made recommendations and released reports
  - ISO/IEC JTC 1 SC27 has already had a 2 year study period for quantum-resistant cryptography and is developing a standing document (SD)

- NIST is interacting and collaborating with these organizations and groups

What's Next?

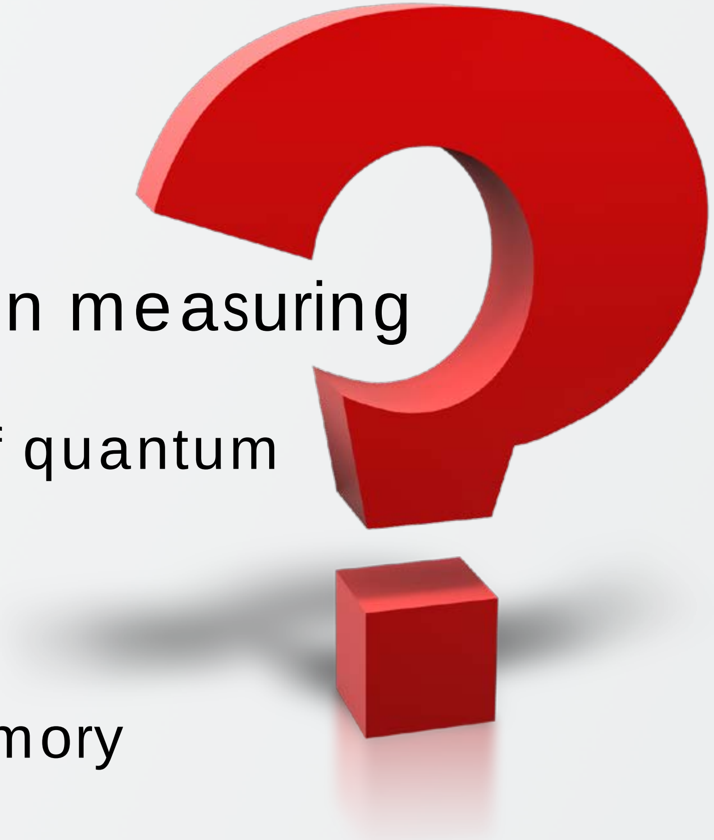
- 2nd NIST PQC Standardization Workshop, Aug 2019
- Sometime before then, we will pick a smaller number of submissions that we feel are the most promising
  - For these, tweaks are allowed in the 2nd Round
- Will be announced on pqc-forum (and our webpage)
- If not selected:
  - Might be eliminated from the standardization process
  - Or might be kept for future consideration, but not in 2nd Round

What does NIST want from you?

- Continue to analyze the submissions
  - Publish and present your work
- Implementations for a variety of platforms
- See how these will fit into applications/protocols
  - Dig into the details – is there anything different from current practice (such as the way to use auxiliary functions)
- Participate in the pqc-forum
- Send us your questions/feedback:

pqc-comments@nist.gov

Questions we have…



- Does NIST need to provide more guidance on measuring the complexity of quantum attacks?
  - Should we specify one or two plausible models of quantum computers?
- Or on complexity of classical attacks?
  - how to deal with attacks with extremely high memory
- How should we handle submissions which are very similar?
  - Keep one? Keep both? Merge them? How?
- What constitutes unacceptable key sizes or performance?

Summary

- Post-quantum crypto standardization will be a long journey
- We have seen many complexities, and know more lie ahead
- Be prepared to transition to new algorithms in 10 years
- 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 for announcements & discussion