AND THEN THERE WERE FOUR:
THE FIRST NIST PQC STANDARDS

Dustin Moody
NIST PQC Team

Sept. 27, 2023
MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 2023

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

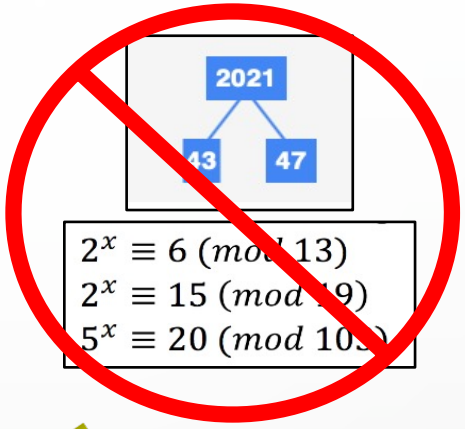
Crypto Technology Group
Computer Security Division
Information Technology Lab

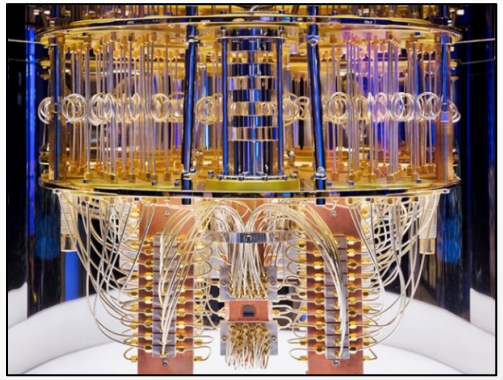
THE QUANTUM THREAT

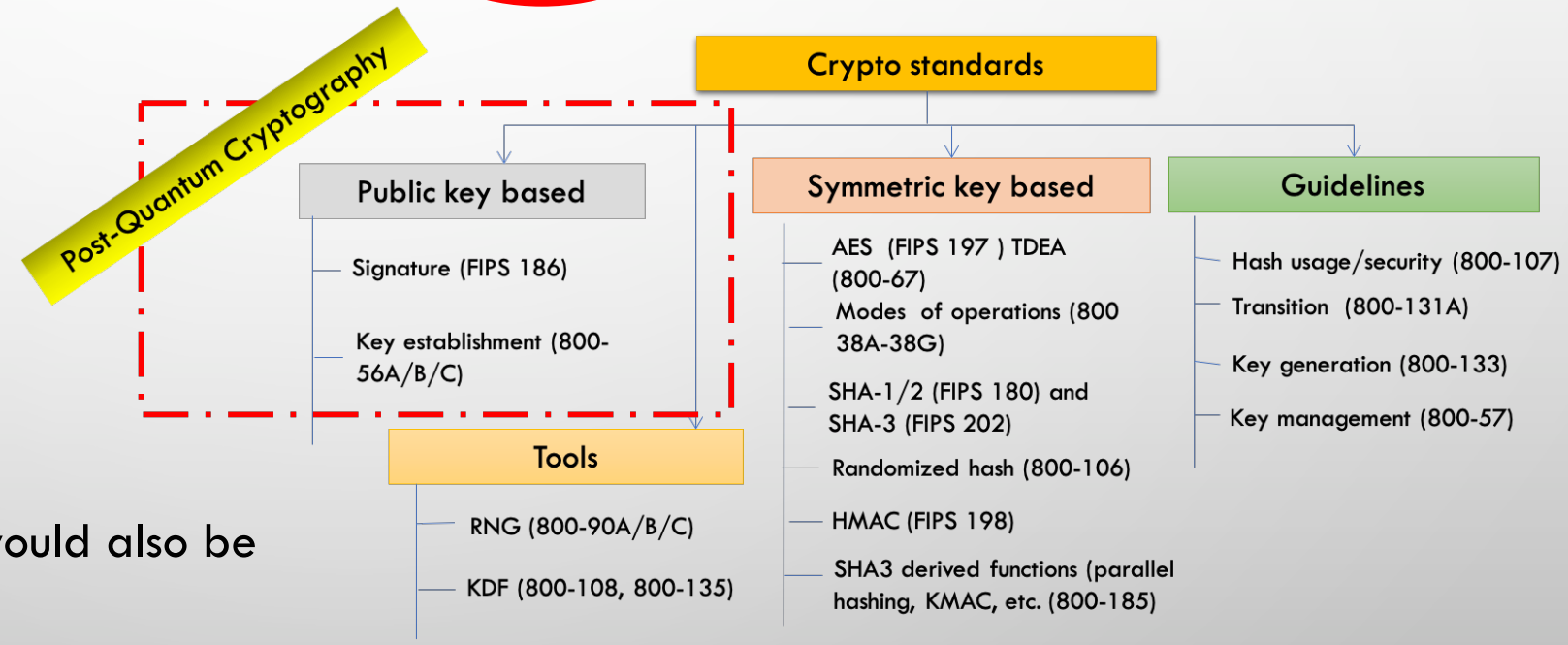
- NIST public-key crypto standards
  - **SP 800-56A**: Diffie-Hellman, ECDH
  - **SP 800-56B**: RSA encryption
  - **FIPS 186**: RSA, DSA, and ECDSA signatures

  all vulnerable to attacks from

  a (large-scale) quantum computer







- Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically

THE PQC "COMPETITION"

- 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 AN OPEN, 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'

ROUND 3 RESULTS

3rd round selection (KEM)	3rd round selection (Signatures)
CRYSTALS-Kyber	**CRYSTALS-Dilithium, Falcon, SPHINCS+**

See NISTIR 8413, *Status Report on the 3rd Round of the NIST PQC Standardization Process,* for the rationale on the selections

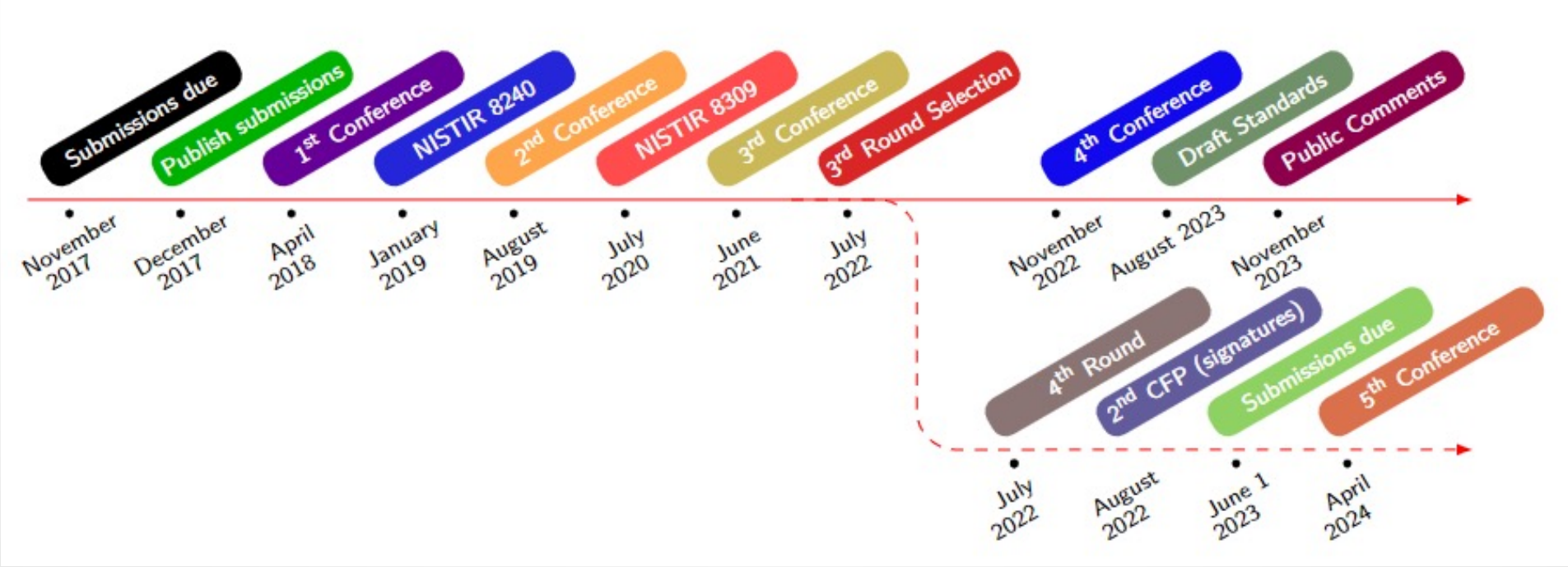
4th round candidates (all KEMs) evaluated for 18-24 months

- ClassicMcEliece
- BIKE
- HQC
- ~~SIKE~~

On-ramp signatures

- NIST issued a new call for additional signatures – preferably for signatures based on non-lattice problems

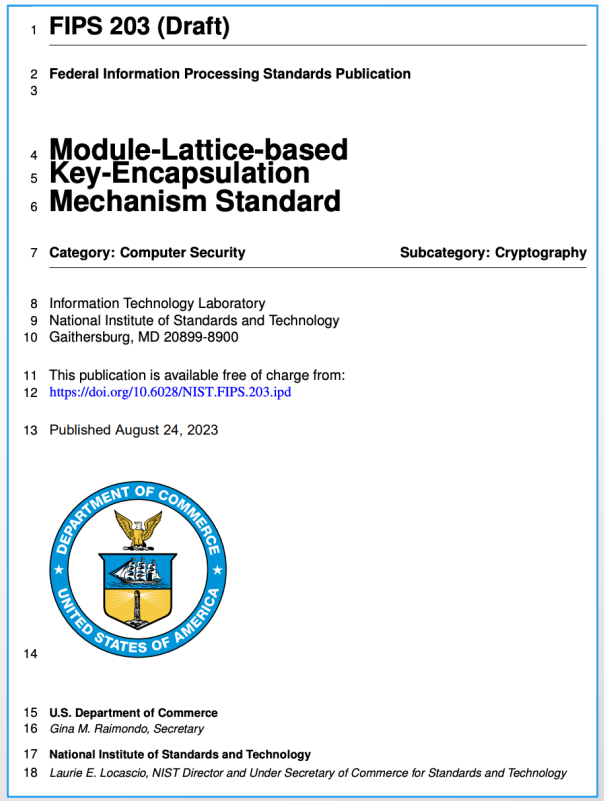
TIMELINE



- The 5th NIST PQC Standardization Conference
  - April 10-12, 2024 in Rockville, Maryland
- Draft standards for public comment released Aug 2023
  - Deadline for comments: November 22, 2023
- **The first PQC standards should be published in 2024**

STANDARDIZATION

- THE 1ST PQC STANDARDS
  - FIPS 203: ML-KEM (KYBER)
  - FIPS 204: ML-DSA (DILITHIUM)
  - FIPS 205: SLH-DSA (SPHINCS+)
  - FN-DSA (FALCON) – UNDER DEVELOPMENT
  - WILL HAVE OTHER DOCS WITH MORE GUIDANCE/DETAILS
- SOME CHOICES MADE
  - WHICH PARAMETER SETS, WHICH HASH FUNCTIONS, OTHER SYMMETRIC PRIMITIVES, ETC
- PLEASE PROVIDE FEEDBACK
  - PQC-FORUM, EMAIL ETC



FIPS 203 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203.ipd

Published August 24, 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

CRYSTALS-DILITHIUM

NIST

- SIGNATURE BASED ON STRUCTURED LATTICES
- ALL OPERATIONS OVER $R = \mathbb{Z}_q[x]/(x^{256}+1)$

KeyGen:

$A \leftarrow R^{n \times m}$

$s \leftarrow S^m$

$t = \text{Round}(As)$

$pk=(A,t)$ $sk=s$

Sign(pk,sk,μ):

$y \leftarrow Y^m$

$w=\text{Round}(Ay)$

$c=\text{Hash}(w,\mu)$

$z=sc+y$

RejectionSample(pk,sk,z)

$\omega = \text{HintVector}(pk,sk,z)$

$\sigma = (z, \omega, c)$

Verify(μ,σ,pk):

$w=\text{UseHintVector}(pk,\sigma)$

check that $c=\text{Hash}(w, \mu)$ and $|z|$ is small

Slide from Round 3 Dilithium update talk

FALCON

- SIGNATURE BASED ON STRUCTURED LATTICES

We work over the cyclotomic ring $\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$.

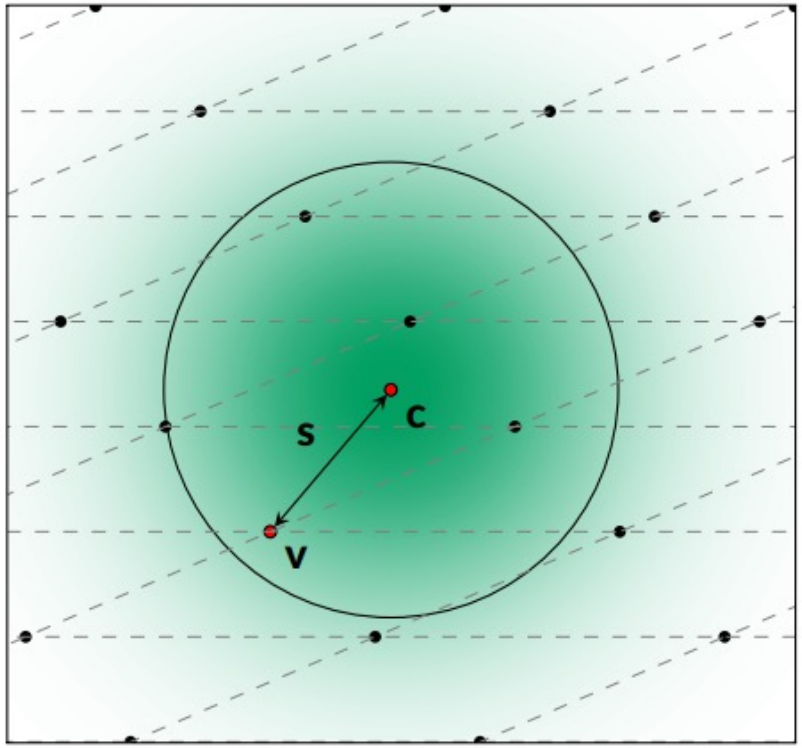
- **Keygen()**
  1. Generate matrices **A**, **B** with coefficients in $\mathcal{R}$ such that
     - $\mathbf{BA} = 0$
     - **B** has small coefficients
  2. pk $\leftarrow$ **A**
  3. sk $\leftarrow$ **B**

- **Sign(m,sk)**
  1. Compute **c** such that $\mathbf{cA} = H(\mathrm{m})$
  2. **v** $\leftarrow$ "a vector in the lattice $\Lambda(\mathbf{B})$, close to **c**"
  3. **s** $\leftarrow \mathbf{c} - \mathbf{v}$

  The signature sig is $\mathbf{s} = (s_1, s_2)$

- **Verify(m,pk sig)**
  Accept iff:
  1. **s** is short
  2. $\mathbf{sA} = H(\mathrm{m})$

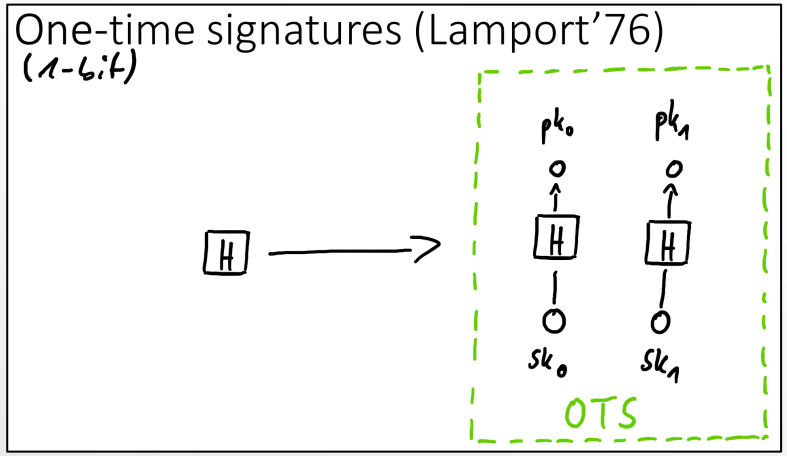
$\Rightarrow$

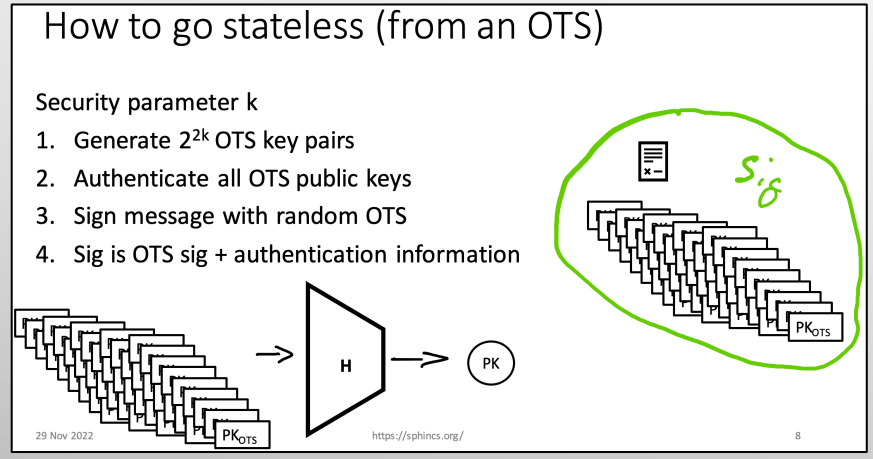


Slide from Round 1 Falcon talk

SPHINCS+

- DIGITAL SIGNATURE BASED ON STATELESS HASH-BASED CRYPTOGRAPHY
- USE ROUND 2 PRESENTATION





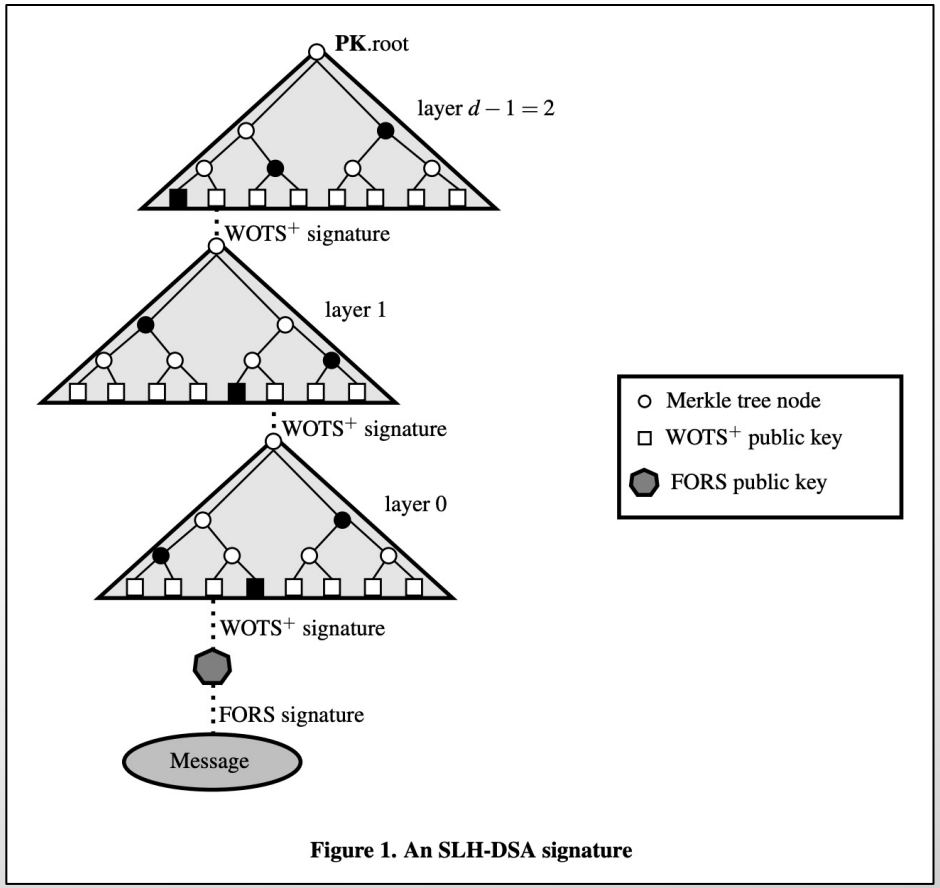


Figure 1. An SLH-DSA signature

Slides from draft FIPS 205 and A. Hulsing's talk at RWPQC 2023

CRYSTALS-KYBER

NIST

- KEM BASED ON STRUCTURED LATTICES
- ALL OPERATIONS OVER $R = \mathbb{Z}_q[x]/(x^n + 1)$

Kyber.CPAPKE: LPR encryption or "Noisy ElGamal"

$\mathbf{A}, \mathbf{s}, \mathbf{e} \leftarrow \chi$ (a Gaussian distribution)

$sk = \mathbf{s}, pk = \mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e}$

$\mathbf{r} \leftarrow \chi$

$\mathbf{e}_1, e_2 \leftarrow \chi'$

$\mathbf{u} \leftarrow \mathbf{A}^T\mathbf{r} + \mathbf{e}_1$

$v \leftarrow \mathbf{t}^T\mathbf{r} + e_2 + \mathrm{Enc}(m)$

$c = (\mathbf{u}, v)$

$m = Dec(v - \mathbf{s}^T\mathbf{u})$

Slide from Round 3 Kyber update talk

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

CONCLUSION

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

- WHAT WILL BE THE INTERSECTION OF THE PQC AND THRESHOLD PROJECTS?

- 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