NIST status update on Elliptic Curves and Post-Quantum Crypto

Dustin Moody

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

Elliptic Curve Crypto in NIST Standards

- **FIPS 186-4**, *Digital Signature Standard*
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - 15 recommended curves
  - Also has DSA, RSA signatures

- **SP 800-56A**, *Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography*
  - Elliptic Curve Diffie Hellman (ECDH)
  - Elliptic Curve authenticated key agreement (ECMQV)

Changes in FIPS 186-5

- New requirement to publish seeds for DSA signatures
- X9.31 RSA signatures removed
- Larger key sizes (2048 bits or more) for RSA signatures allowed
- More elliptic curve details added
  - New SP 800-186 has most of them
  - New elliptic curves specified (Edwards25519 and Edwards448)
- The EdDSA signature algorithm is included
- Deterministic version of ECDSA included
- Various minor improvements/corrections to algorithms in appendices

DSA signatures

- Two of the domain parameters for DSA are prime numbers *p* and *q*, where $p - 1 = h \cdot q$
  - These primes are supposed to be generated deterministically, from a random *seed*
- Recent research showed that DSA primes could be generated in such a way that there is a trapdoor
  - With knowledge of the trapdoor, one can compute discrete logs efficiently, which breaks the security of DSA
  - It seems hard to detect if such a trapdoor is present
- Recommended remedy: publish the seed
  - The trapdoor primes have to be specially constructed; publishing the seed shows this wasn't done
- **FIPS 186-5 makes publishing the seeds mandatory**

RSA signatures

- FIPS 186-4 includes RSA signatures using X9.31 and PKCS #1
- ANSI X9.31 was withdrawn, so we have also withdrawn it
  - It included PRNGs -- we have updated guidance in the SP 800-90 series
- FIPS 186-4 required RSA key sizes of length 1024, 2048, or 3072 bits
- **FIPS 186-5 to allow any key size with (even) length $\geq$ 2048**

Elliptic Curve Crypto in FIPS 186

- FIPS 186-4 included an elliptic curve analogue of DSA, called ECDSA
  - Mostly referred to ANSI X9.62 for specific details
  - Included specifications of the NIST curves

- ANSI X9.62 was withdrawn, so for FIPS 186-5 we added back in the details needed to implement ECDSA
  - X9.142 is under development, which will specify ECDSA

- In addition, **we are adding new elliptic curve signature algorithms** (deterministic ECDSA and EdDSA) **and new elliptic curves** (Edwards25519 and Edwards448).

- We will put many of the elliptic curve details in a new document SP 800-186.

Deterministic Signatures

- The past decade has seen some attacks which resulted from bad random number generation in signature schemes
- Deterministic signatures desired (for some applications)
  - Deterministic schemes need to be carefully protected against side-channel attacks, particularly in hardware implementations
- **Two deterministic schemes to be added in FIPS 186-5**
  1. Deterministic ECDSA: Following IETF RFC 6979, instead of generating the per-message-secret *k* randomly, generate it deterministically, and follow the rest of ECDSA unchanged.
  2. EdDSA (see the next slides)

Edwards Curves

- The NIST curves are all in Weierstrass form
- For example, the prime curves look like:

$$y^2 = x^3 - 3x + b$$

- Recent research in ECC found a new model: Edwards curves

$$x^2 + y^2 = 1 + dx^2y^2$$

- Edwards curves can be implemented faster, and in a uniform way providing easier constant time implementations

EdDSA

- IETF RFC 8032 specified an Edwards curve digital signature algorithm, known as EdDSA.
  - Based off of Schnorr signatures
- 2 sets of parameters:
  - Ed25519, providing approximately 128 bits of security (uses Edwards version of Curve25519)
  - Ed448, which provides approximately 224 bits of security
- EdDSA is deterministic – care must be taken against side channel attacks
- Also includes a “pre-hash” version, which signs *Hash*(*M*), not *M*

- Note: Curve25519/X25519 not currently in SP800-56A, possibly added in future

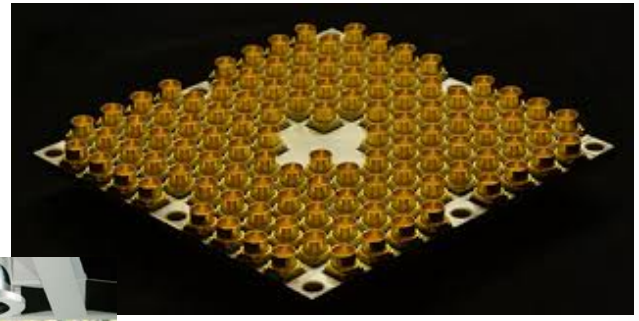
ECC - Looking forward

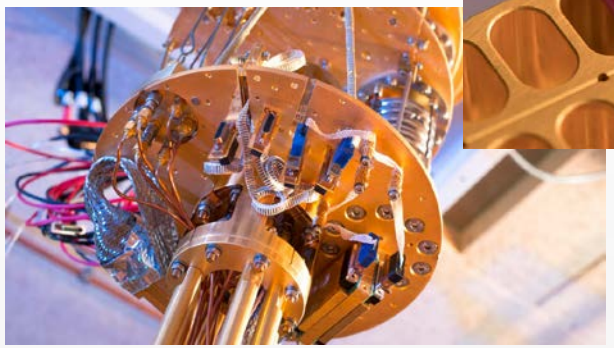
- No more major changes expected for FIPS 186-5 and SP 800-186
- The draft versions for public comment will be available by May
- Send questions or comments to:

dustin.moody@nist.gov

The Quantum Threat

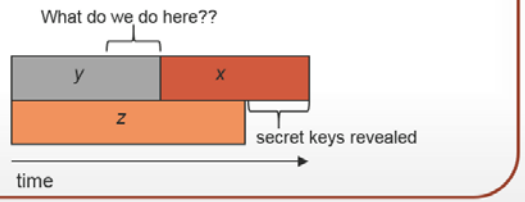
- Quantum computers
- Impact on cryptography
  - Shor's algorithm
    - RSA, Elliptic-Curve crypto dead
  - Grover's algorithm
    - Need longer AES keys/hash outputs
- Why worry now?





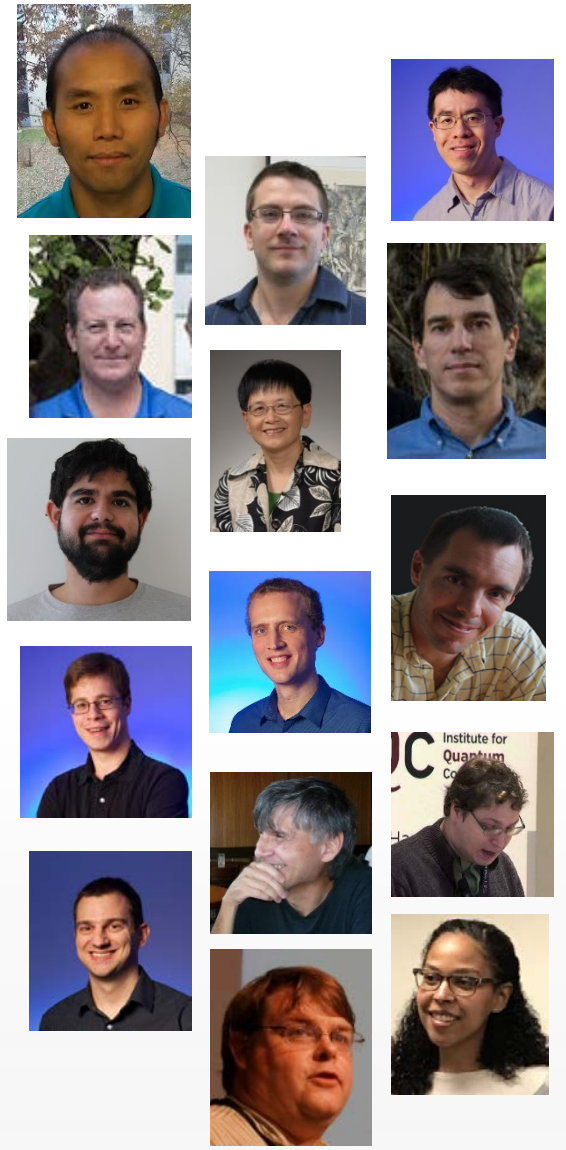
- How long does your information need to be secure (*x* years)
- How long to re-tool with a quantum safe solution (*y* years)
- How long until a large-scale quantum computer is built (*z* years)

Theorem: If *x* + *y* > *z*, then worry!



The NIST PQC Project

- **Post Quantum Cryptography**
  - Cryptosystems which run on classical computers, and are considered to be resistant to quantum attacks
- NIST public-key crypto standards vulnerable to quantum attacks:
  - FIPS 186-5, *The Digital Signature Standard* (RSA, DSA, ECDSA)
  - SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography* (DH, ECDH, MQV)
  - SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes using Integer Factorization Cryptography* (RSA)
- In 2016, NIST announced a competition-like process to select quantum-resistant public-key algorithms for standardization
  - A small number will likely be selected for each functionality
- Scope: Digital signatures, Public-key encryption, Key-establishment mechanisms (KEMs)



Timeline

- 2009 – NIST publishes PQC survey: Quantum Resistant Public Key Cryptography: A Survey [D. Cooper, R. Perlner]
- 2012 – NIST establishes PQC project
- April 2015 – 1st NIST PQC Workshop
- 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 of PQC "competition"
- Dec 2016 – Final submission requirements and evaluation criteria published
- Nov 2017 – Submission deadline
- Dec 2017 – 1st Round candidates announced
- April 2018 – 1st NIST PQC Standardization Conference (slides)
- Jan 2019 – 2nd Round candidates announced
- 2022-2024 – Draft standards available

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)

  - NIST asked submitters to focus on levels 1,2, and 3. (Levels 4 and 5 are for very high security)
- **Performance** – measured on various classical platforms
- **Other properties**:
  - Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, etc…

The Submissions

- 82 total submissions received from 25 Countries, 6 Continents (and 16 states)
  - A total of 278 submitters
- 69 accepted as “complete and proper” (5 since withdrawn)
- Most submitted schemes (or previous versions) have been published previously – In general, no big surprises

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

The 1st Round

- Evaluation and analysis phase lasting about a year
  - Security proofs (IND-CPA/IND-CCA2 and EUF-CMA)
  - Quantum/classical algorithm complexity for attacks
  - Precise claims against quantum computation
    - Lots of uncertainty here, but we still need concrete parameters and security estimates
  - Cryptanalysis
    - Many schemes attacked or broken
- Performance testing
  - Libraries like SUPERCOP and OpenQuantumSafe
  - Side-channel resistance
- IP concerns
- Official Comments and the pqc-forum
- Merging submissions

The Selection Process

- Used evaluation criteria: Security, Cost and Performance, Algorithm and Implementation characteristics
- Security arguments in submission, external analysis, internal NIST cryptanalysis
- NIST studied each submission in detail
- Implemented attacks. Attacks that called security into question.
- Overall quantity, quality and maturity of analysis on each scheme
- While performance was not the key factor, we did note apparent performance characteristics. External and internal benchmarks.
- Some unique and elegant designs. Diversity of algorithms important.
- Compared schemes against similar schemes, in cases where there were many

The 2nd Round Candidates

- Encryption/KEMs (17)

- BIKE
- Classic McEliece
- CRYSTALS-KYBER
- FrodoKEM
- HQC
- LAC
- LEDAcrypt (merger of LEDAkem/pkc)
- NewHope
- NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM)
- NTRU Prime
- NTS-KEM
- ROLLO (merger of LAKE/LOCKER/Ouroboros-R)
- Round5 (merger of Hila5/Round2)
- RQC
- SABER
- SIKE
- Three Bears

- Digital Signatures (9)

- CRYSTALS-DILITHIUM
- FALCON
- GeMSS
- LUOV
- MQDSS
- Picnic
- qTESLA
- Rainbow
- SPHINCS+

NIST Report on the 1st Round: https://doi.org/10.6028/NIST.IR.8240

What's Next

- 2nd Round Candidate teams may make tweaks
  - Deadline: March 15, 2019
  - NIST will publish accepted updated submissions shortly thereafter
- 2nd NIST PQC Standardization Conference
  - August 22-24, 2019 in Santa Barbara, CA
  - Co-located with CRYPTO 2019
  - Call for Papers – deadline May 31, 2019
- More analysis….
- Either 3rd Round or Selection of algorithms for standardization

PQC Summary

- 26 Candidates advance into the 2nd Round

- Post-quantum crypto standardization will be a long journey
- Be prepared to transition to new algorithms in 10 years
  - Facilitate crypto-agility

- 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

- Send us comments or questions at pqc-comments@nist.gov
  - For example, what constitutes unacceptable key sizes or performance?