Post-Quantum Cryptography: NIST’s Plan for the Future

Dustin Moody
Post Quantum Cryptography Team
National Institute of Standards and Technology (NIST)

The sky is falling?

- When will a quantum computer be built that breaks current crypto?
  - 15 years, $1 billion USD, nuclear power plant (to break RSA-2048) (PQCrypto 2014, Matteo Mariantoni)

- Impact:
  - Public key crypto: FIPS 186-4, SP 800-56A/56B
    - RSA
    - Elliptic Curve Cryptography (ECDSA)
    - Finite Field Cryptography (DSA)
    - Diffie-Hellman key exchange
  - Symmetric key crypto: FIPS 197, SP 800-57
    - AES
    - Triple DES
  - Hash functions: FIPS 180-4, FIPS 202
    - SHA-1, SHA-2 and SHA-3

The sky is falling?

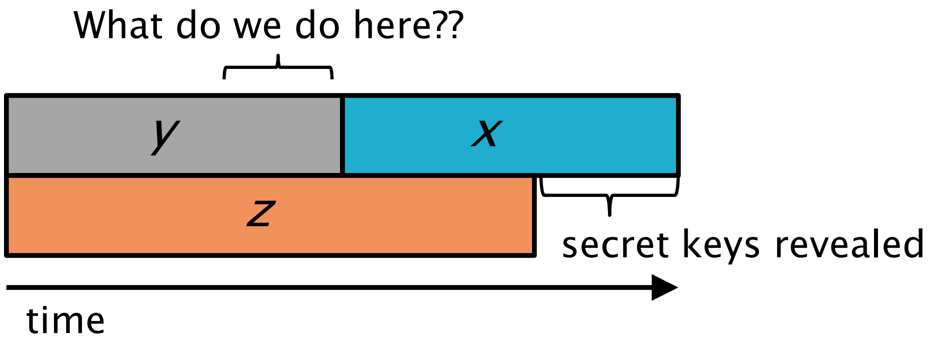
- When will a quantum computer be built?
  - 15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~
  - Symmetric key crypto:
    - AES Need larger keys
    - Triple DES Need larger keys
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3 Use longer output

How soon do we need to worry?

- How long does encryption need to be secure (x years)
- How long to re-tool existing infrastructure with quantum safe solution (y years)
- How long until large-scale quantum computer is built (z years)

Theorem (Mosca): If $x + y > z$, then worry



What do we do here??

secret keys revealed

time

- NSA is transitioning in the “not too distant” future <https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm>
- European PQCrypto project
- ETSI work
- IETF – hash-based signature RFC’s
- NIST report – <http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf>

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

Differences with AES/SHA-3 competitions

- Post-quantum cryptography is more complicated than AES or 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 "pick a winner"
  - Ideally, several algorithms will emerge as 'good choices'
- We may narrow our focus at some point
  - This does not mean algorithms are "out"
- Requirements/timeline could potentially change based on developments in the field

Requirements

- The formal Call will have detailed submission requirements
  - A complete written specification of the algorithms shall be included, consisting of all necessary mathematical operations, equations, tables, diagrams, and parameters that are needed to implement the algorithms. The document shall include design rationale and an explanation for all the important design decisions that are made.

- Minimal acceptability requirements
  - Publicly disclosed and available with no IPR
  - Implementable in wide range of platforms
  - Provides at least one of: signature, encryption, or key exchange
  - Theoretical and empirical evidence providing justification for security claims

Specification

- Implementation
  - Reference version
  - Optimized version
- Cryptographic API will be provided
  - Can call approved hash functions, block ciphers, modes, etc…
- Known Answer and Monte Carlo tests
- Optional – constant time implementation

Intellectual Property

- Signed statements
  - Submitted algorithm
  - Implementations
- Disclose known patent information
- Available worldwide without royalties or any intellectual property restrictions during the analysis phase
  - Submitters can reclaim rights by withdrawing submission from consideration

Evaluation criteria

- To be detailed in the formal Call
  - Security
  - Cost (computational and memory)
  - Algorithm and implementation characteristics
- Draft criteria will be open for public comment
- We strongly encourage public evaluation and publication of results concerning submissions
- NIST will summarize the evaluation results and report publicly

Security Analysis

- Target security levels
  - 128 bits classical security
  - 64/80/96/128 bits quantum security?

- Correct security definitions?
  - IND-CCA2 for encryption
  - EUF-CMA for signatures
  - CK best for key exchange?

- Quantum/classical algorithm complexity
  - Stability of best known attack complexity
  - Precise security claim against quantum computation
  - Parallelism?
  - Attacks on multiple keys?
  - How many chosen ciphertext queries allowed?

- Security proofs

- Quality and quantity of prior cryptanalysis

Cost

- Computational efficiency
  - Hardware and software
    - Key generation
    - Encryption/Decryption
    - Signing/Verification
    - Key exchange
- Memory requirements
  - Concrete parameter sets and key sizes for target security levels
  - Ciphertext/signature size

Algorithm and Implementation Characteristics

- Ease of implementation
  - Tunable parameters
  - Implementable on wide variety of platforms and applications
  - Parallelizable
  - Resistance to side-channel attacks
- Ease of use
  - How does it fit in existing protocols (such as TLS or IKE)
  - Misuse resistance
- Simplicity

Questions

- How is the timeline? Too fast? Too slow?
  - Do we need an ongoing process, or is one time enough?
- How to determine if a candidate is mature enough for standardization?
  - hash-based signatures for code signing
- Should we just focus on encryption and signatures, or should we also consider other functionalities?
- How many "bits of security" do we need against quantum attacks?
- How can we encourage more work on quantum cryptanalysis? Maybe we need "challenge problems"?
- How can we encourage people to study practical impacts on the existing protocols?
  - For example, key sizes may be too big

Conclusion

- NIST is calling for quantum-resistant algorithms
  - We see our role as managing a process of achieving community consensus in a transparent and timely manner
  - Different from (but similar to) AES/SHA-3 competitions
- We don’t have all the answers
- Wanted: Postdocs, guest researchers at NIST
- We would like public feedback
  - Email: pqc-comments@nist.gov
  - PQC forum: pqc-forum@nist.gov