A Quantum World and how NIST is preparing for future crypto

Dustin Moody
Post Quantum Cryptography Team
National Institute of Standards and Technology (NIST)
pqc@nist.gov

Cryptography today and NIST Standards

- Basic crypto applications:
  - Encryption, Signatures, Key-establishment, …
- Public key cryptosystems
  - RSA
    - Signature FIPS 186-4
    - Key-transport SP 800-56B
  - Elliptic Curve Cryptography
    - Signature (ECDSA) FIPS 186-4
    - Key-establishment (EC-DH) SP 800-56A
  - Finite Field Cryptography FIPS 186-4, SP 800-56A
- Symmetric key crypto:
  - AES FIPS 197
  - Triple DES SP 800-67
- Hash functions:
  - SHA-1, SHA-2 and SHA-3 FIPS 180-4, FIPS 202

Impacts of Quantum Computing

- Shor's Algorithm
  - Factors large numbers
  - Solves Discrete Log Problem
- Grover's Algorithm
  - Quadratic speed-up in searching databases

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

Impacts of Quantum Computing

- Shor's Algorithm
  - Factors large numbers
  - Solves Discrete Log Problem
- Grover's Algorithm
  - Quadratic speed-up in searching databases
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - Elliptic Curve Cryptography (ECDSA)
    - Finite Field Cryptography (DSA)
    - Diffie-Hellman key exchange
  - Symmetric key crypto:
    - AES
    - Triple DES
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3

Impacts of Quantum Computing

- Shor's Algorithm
  - Factors large numbers
  - Solves Discrete Log Problem
- Grover's Algorithm
  - Quadratic speed-up in searching databases

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - Finite Field Cryptography (DSA)
    - Diffie-Hellman key exchange

  - Symmetric key crypto:
    - AES
    - Triple DES

  - Hash functions:
    - SHA-1, SHA-2 and SHA-3

Impacts of Quantum Computing

- Shor's Algorithm
  - Factors large numbers
  - Solves Discrete Log Problem
- Grover's Algorithm
  - Quadratic speed-up in searching databases
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - Diffie-Hellman key exchange
  - Symmetric key crypto:
    - AES
    - Triple DES
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3

Impacts of Quantum Computing

- Shor's Algorithm
  - Factors large numbers
  - Solves Discrete Log Problem
- Grover's Algorithm
  - Quadratic speed-up in searching databases

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~

  - Symmetric key crypto:
    - AES
    - Triple DES

  - Hash functions:
    - SHA-1, SHA-2 and SHA-3

Impacts of Quantum Computing

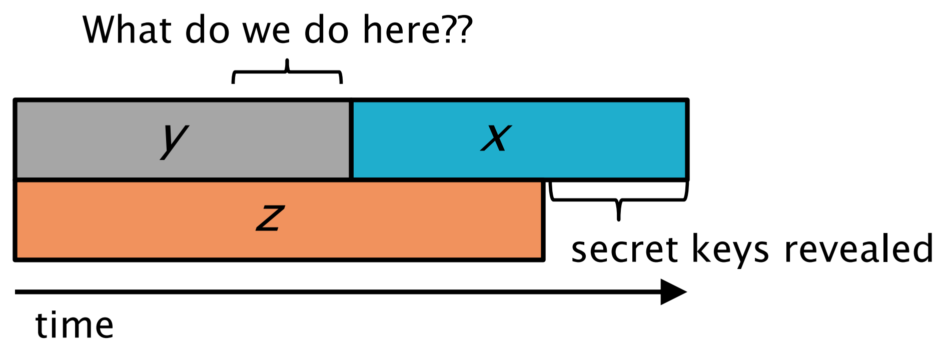
- Shor's Algorithm
  - Factors large numbers
  - Solves Discrete Log Problem
- Grover's Algorithm
  - Quadratic speed-up in searching databases
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman 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

Post-Quantum Cryptography

- Cryptosystems which run on classical computers, and are considered to be resistant to quantum attacks

- 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 1: If $x + y > z$, then worry



Practical Questions

- Which are most important in practice?
  - Public and private key sizes
  - Key pair generation time
  - Ciphertext size
  - Encryption/Decryption speed
  - Signature size
  - Signature generation time
  - Signature verification time
- Not a lot of benchmarks in this area

Observations

- For most of the potential PQC replacements, the times needed for encryption, decryption, signing, verification are acceptable
- Some key sizes are significantly increased
  - For most protocols, if the public keys do not need to be exchanged, it may not be a problem
- Some ciphertext and signature sizes are not quite plausible
- Key pair generation time for the encryption schemes is not bad at all
- **No easy "drop-in" replacements**
- Would be nice to have more benchmarks

Security

- What does security mean?
  - Breaking the cryptosystem is computationally hard, e.g., requires 2^{256} operations
- Show security against known attacks
- How to protect against unknown attacks?
  - Security proofs (based on mathematical conjectures)
    - Many PQC systems use new assumptions, often with special structure
- How to measure the complexity of a quantum attack?
- How well do these cryptosystems perform with other protocols in the real world?
- Are there concrete estimates of security (e.g. 128 bits)?

The NIST PQC Project

- Objectives
  - Examine quantum-resistant public key cryptosystems
  - Monitor quantum computing progress and applicability of known quantum algorithms
- Biweekly seminars since 2012
- Publications and presentations
  - Journals, conferences, workshops
- Collaboration:
  - Hosting academic visitors
  - CryptoWorks 21(U. of Waterloo)
  - Joint Center for Quantum Information and Computer Science, University of Maryland
- NIST Workshop on Cybersecurity in a Post-Quantum World

  http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm