A Quantum World and how NIST is preparing for future crypto

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
  - Factorization based – RSA
    - Signature FIPS 186-4
    - key transport, SP 800-56B
  - Discrete Logarithm based
    - Elliptic Curve Cryptography (ECDSA FIPS 186-4, EC-DH, SP 800-56A)
    - Finite Field Cryptography (DSAFIPS 186-4, DH 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, Draft FIPS 202

Impacts of Quantum Computing

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

- Impact:
  - Public key crypto:
    - RSA
    - ECDSA
    - 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 database

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ECDSA
    - 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 database

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~ECDSA~~
    - 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 database

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~ECDSA~~
    - ~~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 database

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~ECDSA~~
    - ~~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 database

- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~ECDSA~~
    - ~~DSA~~
    - ~~Diffie-Hellman key exchange~~

  - Symmetric key crypto:
    - AES Need larger key size
    - Triple DES Need larger key size

  - 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

- PQC needs time to be ready for applications
  - Efficiency
  - Confidence – cryptanalysis
  - Usability and interoperability (IKE, TLS, etc… use public key crypto)

- Status of quantum computers

The NIST PQC Project

- Objectives
  - Examine quantum-resistant public key cryptosystems
  - Monitor quantum computing progress and applicability of known quantum algorithms

- NIST PQC team
  - Dr. Lily Chen
  - Dr. Stephen Jordan
  - Dr. Yi-kai Liu
  - Dr. Daniel Smith-Tone
  - Dr. Dustin Moody
  - Dr. Rene Peralta
  - Mr. Ray Perlner

Possible PQC Replacements

- Lattice-based
  - NTRU Encrypt and NTRU Sign
  - (Ring-based) Learning with Errors
- Code-based
  - McEliece encryption and CFS signatures
- Multivariate
  - HFE, sFlash, psFlash, Quartz,
- Many more….
  - hash-based signatures
  - isogeny-based schemes
  - etc...

- All have their pros and cons

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/verification time

- Not a lot of benchmarks in this area

Encryption Schemes

Algorithm	KeyGen Time (RSA sign=1)	Decrypt Time (RSA sign=1)	Encrypt Time (RSA sign=1)	Public Key Size (bits)	Private Key Size (bits)	Ciphertext Size (bits)	Time* Scaling	Key* Scaling
NTRUEncrypt	10	0.1	0.1	~3000	~4000	~3000	k^2	k
McEliece	5	1	0.02	651264	1098256	1660	k^2	k^2
Quasi-Cyclic McEliece	5	1	0.02	4801	9602	9602	k^2	k
RSA	50	1	0.02	1024	1024	1024	k^6	k^3
DH	0.5	0.5	0.5	1024	480	1024	k^4	k^3
ECC	0.1	0.1	0.1	320	480	320	k^2	k

- **Disclaimer** – these are rough estimates for comparison purposes only, not benchmarks. Numbers are for 80 bits of security.

* Time and key scaling ignore log *k* factors

Signature Schemes

Algorithm	KeyGen Time (RSA sign=1)	Sign Time (RSA sign=1)	Verify Time (RSA sign=1)	Limited Lifetime ?	Public Key Size	Private Key Size	Signature Size (bits)	Time* Scaling	Key * Scaling
Winternitz-Merkle signatures	200 10000 500000	1 1 2	0.2 0.2 0.2	2^{20} 2^{30} 2^{40}	368 368 368	15200 22304 29344	17024 18624 20224	k^2	k^2
GLP signatures (lattice-based)	0.01	0.5	0.02		11800	1620	8950	k^2	k
CFS signature (code based)	5	2000	0.02		9437184	~15000000	144	exp(o(k))	exp(o(k))
Psflash signature (multivariate)	50	1	0.1		576992	44400	296	k^3	k^3
Quartz signature (multivariate)	100	2	0.05		126000	11500	80	k^3	k^3
RSA	50	1	0.02		1024	1024	1024	k^6	k^3
DSA	0.5	0.5	0.5		1024	480	320	k^4	k^3
ECDSA	0.1	0.1	0.1		320	480	320	k^2	k

- **Disclaimer** – these are rough estimates for comparison purposes only, not benchmarks. Numbers are for 80 bits of security.

* Time and key scaling ignore log *k* factors

Observations

- For the 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 size and signature size 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
  - Try all known attacks, show that they are infeasible
- How to protect against unknown attacks?
  - New attacks, new discoveries in mathematics?
  - Try to argue that these are "unlikely"
    - Security proofs (based on mathematical conjectures)
      - Newer PQC systems use new assumptions
    - Design cryptosystems to defeat common classes of attacks

Attacks on PQC systems

- General-purpose Algorithms
  - Lattice basis reduction
    - Practical performance beats theoretical guarantees
  - Grobner basis reduction
    - General algorithm for solving multivariate systems of equations
- Specialized attacks:
  - "Learning a parallelepiped"
    - Breaks old versions of NTRUSign
    - NTRUSign can be repaired using perturbations; is this secure?
  - Differential attacks
    - Break certain multivariate cryptosystems (e.g., SFLASH)
    - HFE, unbalanced oil/vinegar are still ok
  - Lattice reduction attacks
    - Break some versions of McEliece using LDPC codes
    - Standard McEliece is still ok

Open Questions on Security

- Many cryptosystems use lattices/codes/equations with special structure. Does this affect security?
- 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. 112 bits)?

The NIST PQC Project Update

- Biweekly seminars since 2012
  - Look into the latest results
  - Discuss progress and impact
- 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 will organize a PQC workshop in 2015

Selected Publications and Presentations

- R. Perlner, D. Smith-Tone, A Classification of Differential Invariants for Multivariate Post-quantum Cryptosystems, PQCrypto 2013
- D. Smith-Tone, Quantum-Resistand Multivariate Public Key Cryptography, Dagstuhl Quantum Cryptanalysis Workshop
- Y. Liu, Building One-time Memories from Isolated Qubits, Qcrypt 2013
- L. Chen, Practical Impacts of Quantum Computing, ETSI Quantum-Safe Crypto Workshop
- Y. Liu, Evaluating the Security of Post-Quantum Cryptosystems, ETSI Quantum-Safe Crypto Workshop
- S. Jordan, Partial-indistinguishability Obfuscation with Braids, IQIM seminar
- S. Jordan, Super-polynomial Quantum Speedups Tutorial, Lorentz Center
- S. Jordan, Quantum Algorithms for Quantum Field Theories, Science