Cryptography in a *Post-Quantum* World

http://indianajones.wikia.com/wiki/Raiders_of_the_Lost_Ark

Dustin Moody, Lily Chen

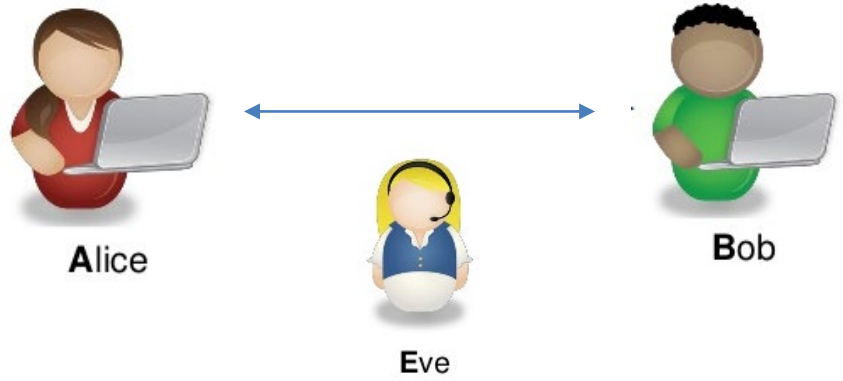
National Institute of Standards and Technology (NIST)

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

Cryptography

Alice and Bob want to communicate

- Beware of Eve



Symmetric-key crypto

- Alice and Bob have a shared key
- Example: AES (encryption)

Public-key crypto

- Alice has never met Bob, but wants to send him a message
- Example: RSA (encryption and signatures)

Classical vs Quantum Computers

The security of crypto relies on intractability of certain problems to modern computers

- Example: RSA and factoring

Quantum computers

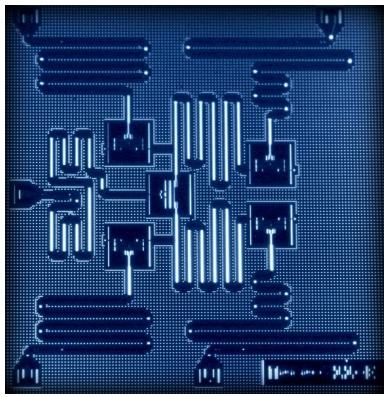
- Exploit quantum mechanics to process information
- Use quantum bits = “qubits” instead of 0’s and 1’s
- Superposition – ability of quantum system to be in multiples states at the same time
- Potential to vastly increase computational power beyond classical computing limit

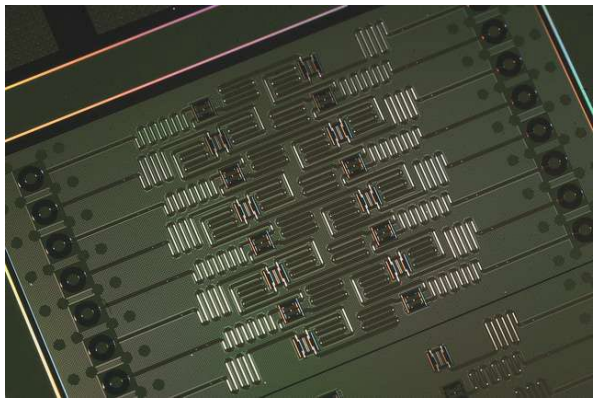
Quantum Computers

Difficulties

- When a measurement is made on quantum system, superposition collapses
- Quantum states are very fragile and must be extremely well isolated
- Intersection of many developing fields: superconductors, nanotechnology, quantum electronics, etc…

1998 – 2 qubits
2000 – 4, 5, and then 7 qubits
2006 – 12 qubits
2011 – 14 qubits
2017 – 20, 49 qubits ?? (Google)
Measuring qubits is not best metric

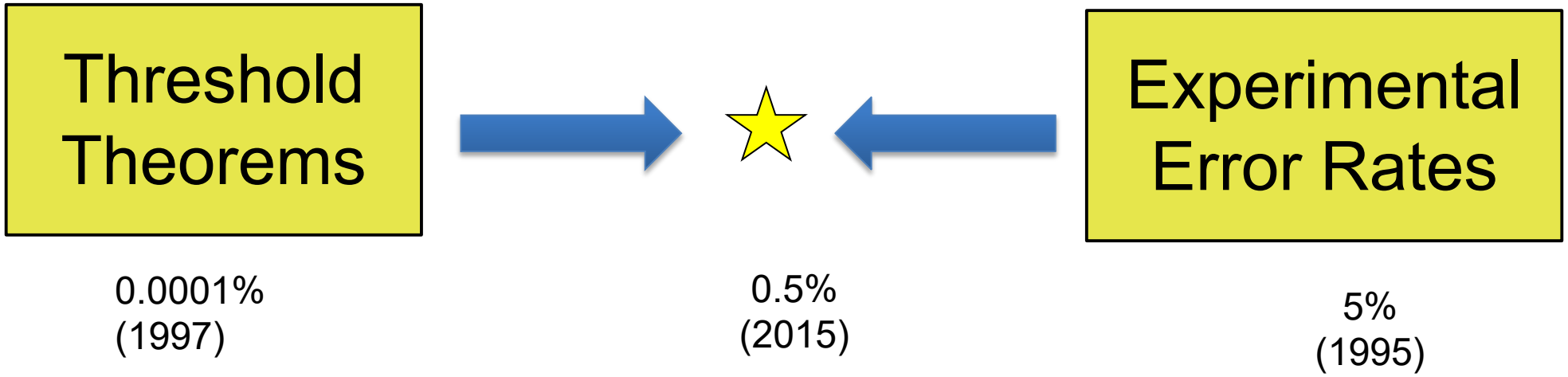




Intel's 5 qubit and 16 qubit processors

Threshold Theorem

If error per quantum computation can be brought below (roughly) 0.5%, arbitrarily long quantum computations can be performed by correcting errors as you go

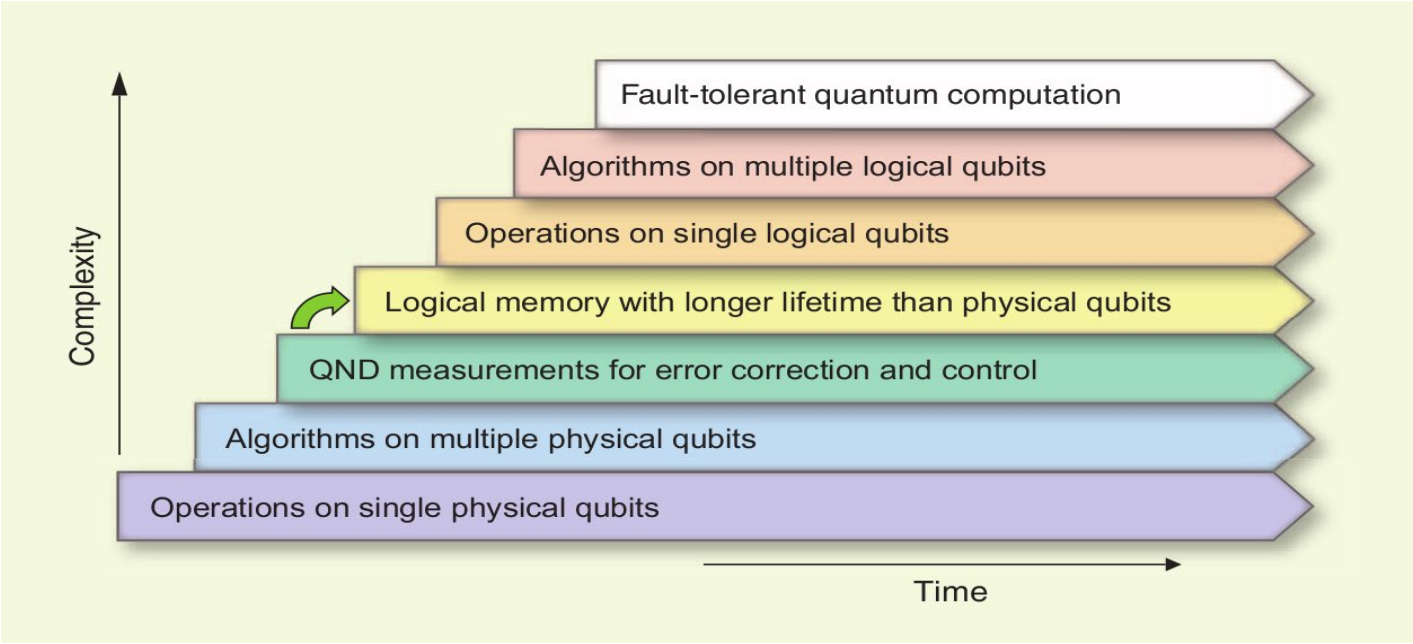


Theorists improve error correction schemes to tolerate higher error rates

Experimentalists achieve lower error rates

Quantum Computing Progress

A lot of progress, but still a long way to go



[Image credit: M. Devoret and R. Schoelkopf]

Quantum Algorithms

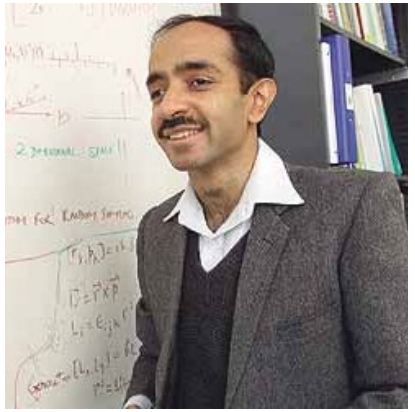
1994, Peter Shor created a quantum algorithm that would give an exponential speed-up over classical computers

- Factoring large integers
- Finding discrete logarithms

Grover's algorithm – polynomial speed-up in unstructured search, from O(N) to O($\sqrt{N}$)

Simulating the dynamics of molecules, superconductors, photosynthesis, among many, many others

- see http://math.nist.gov/quantum/zoo

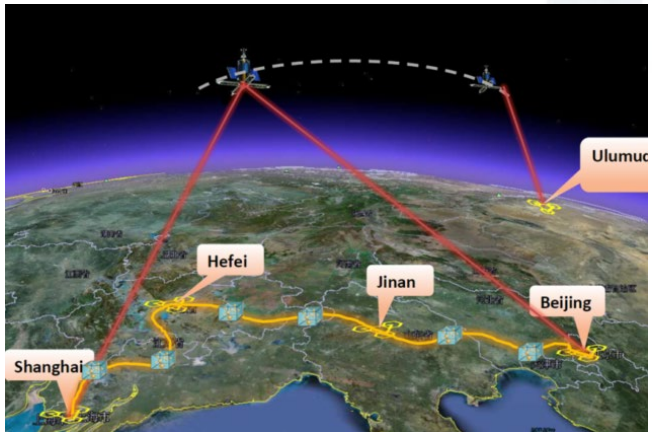


Quantum Cryptography

Quantum cryptography – using quantum computers to do cryptography
- Security is mostly based on physical assumptions (quantum mechanics)

Best example: **Quantum Key Distribution** (QKD)

- Using quantum communication to establish a shared key between 2 parties
- If an eavesdropper tries to learn any information, the observation causes the key exchange to have errors that can be detected
- Security can be proven without imposing any restrictions on the abilities of the eavesdropper, which isn't possible with classical crypto
- Being developed commercially around the world



Limitations

Best example: **Quantum Key Distribution** (QKD)

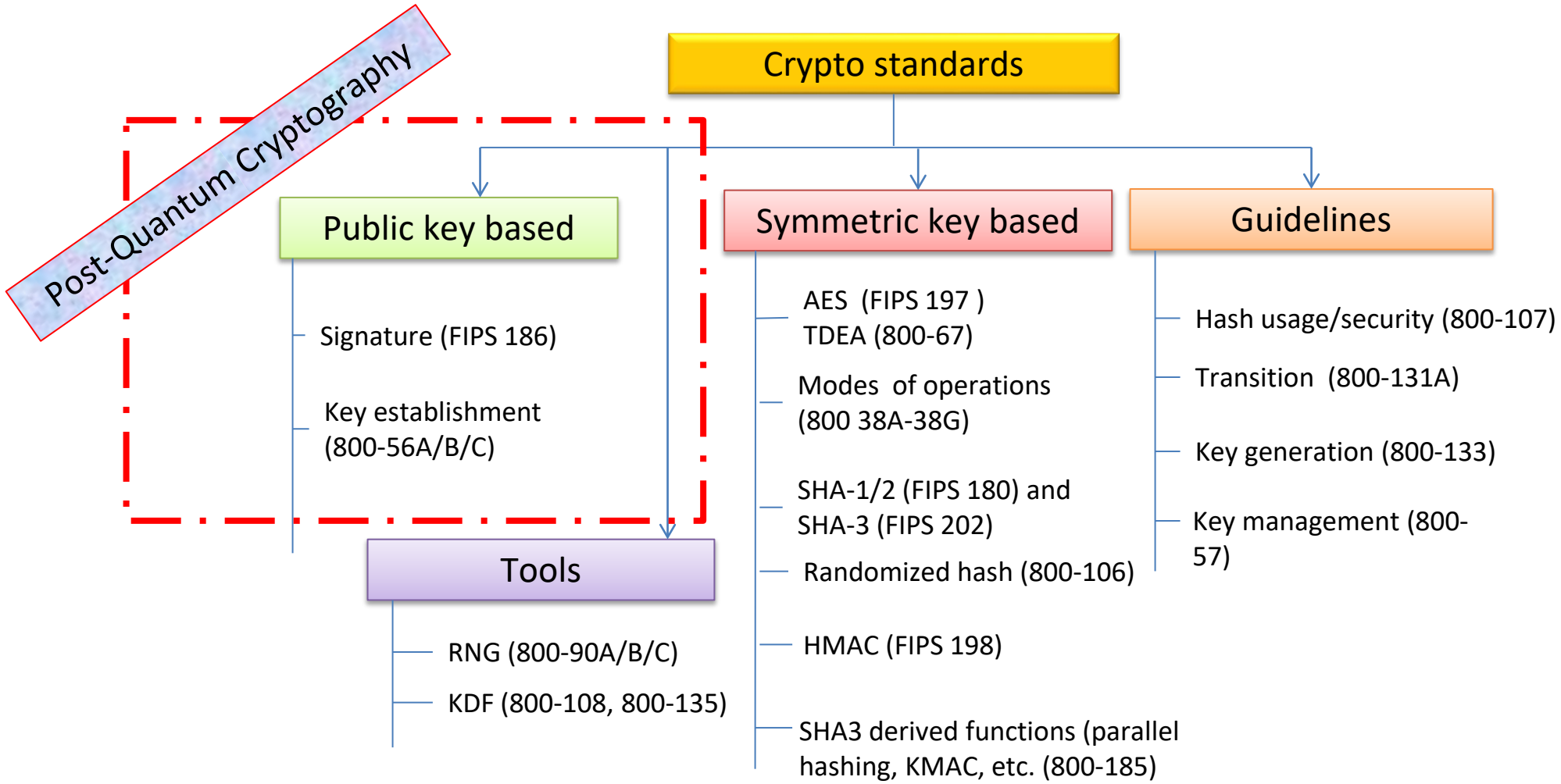
- Using quantum communication to establish a shared key between 2 parties
- If an eavesdropper tries to learn any information, the observation causes the key exchange to have errors that can be detected
- Security can be proven without imposing any restrictions on the abilities of the eavesdropper, which isn't possible with classical crypto
- Being developed commercially around the world

Drawbacks

- Specialized equipment (doesn't run on classical computers)
- Not cheap
- Not easily scalable

→ The Cryptographic Technology Group at NIST is NOT focusing on QKD

NIST Cryptography Standards



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

The Sky is Falling?

If a large-scale quantum computer could be built then….

Public key crypto:

- RSA
- ECDSA (and Elliptic Curve Cryptography)
- DSA (and Finite Field Cryptography)
- Diffie-Hellman key exchange

Symmetric key crypto:

- AES
- Triple DES

Hash functions:

- SHA-2 and SHA-3

The Sky is Falling?

If a large-scale quantum computer could be built then….

Public key crypto:

- ~~RSA~~
- ~~ECDSA (and Elliptic Curve Cryptography)~~
- ~~DSA (and Finite Field Cryptography)~~
- ~~Diffie-Hellman key exchange~~

Symmetric key crypto:

- AES
- Triple DES

Hash functions:

- SHA-2 and SHA-3

The Sky is Falling?

If a large-scale quantum computer could be built then….

Public key crypto:

- ~~RSA~~
- ~~ECDSA (and Elliptic Curve Cryptography)~~
- ~~DSA (and Finite Field Cryptography)~~
- ~~Diffie-Hellman key exchange~~

Symmetric key crypto:

- AES — Need longer keys
- Triple DES — Need longer keys

Hash functions:

- SHA-2 and SHA-3 — Use longer output

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

PQC Standardization – Is it too early?

It has been a long debate among researchers and practitioners on whether it is too early to look into PQC standardization

When will a large-scale quantum computer be built?

- "There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."

– Dr. Michele Mosca, U. of Waterloo

Our experience tells that we need at least several years to developing and deploying PQC standards

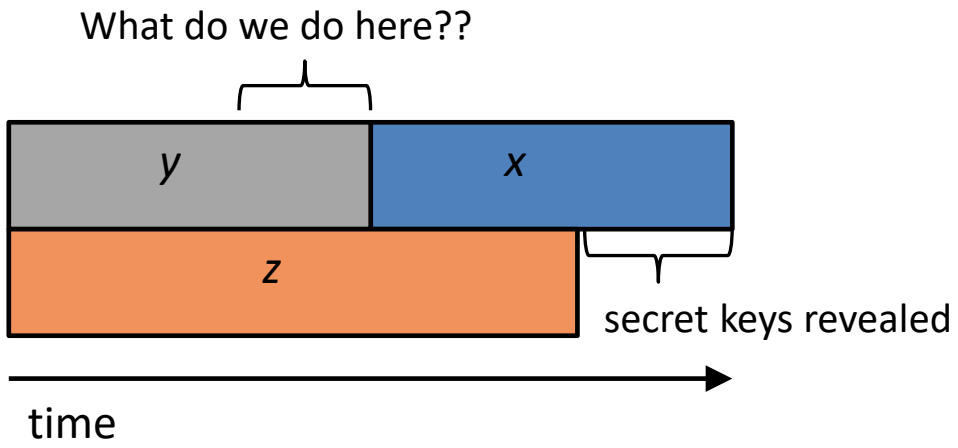
How soon do we need to worry?

How long does your information need to be secure (*x* years)

How long to re-tool existing infrastructure with quantum safe solution (*y* years)

How long until a large-scale quantum computer is built (*z* years)

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



NSA IAD Announcement August 2015

NSA's Information Assurance Directorate updated its list of Suite B cryptographic algorithms

- "IAD will initiate a transition to quantum resistant algorithms in the **not too distant future**. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."

Standardization is the first step towards the transition

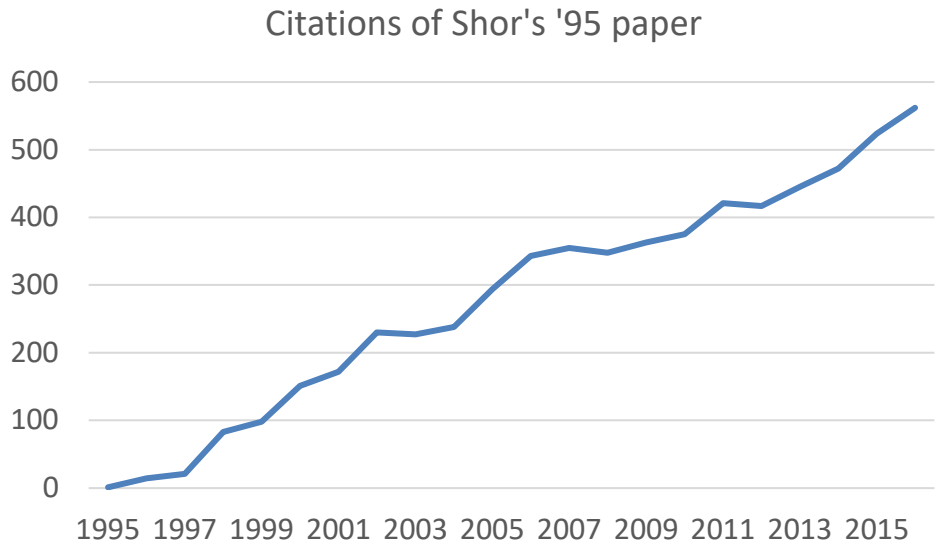
Post-Quantum Cryptography (PQC)

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
- Standardization
- Usability and interoperability

  (IKE, TLS, etc… use public key crypto)



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

Possible Replacements

Lattice-based

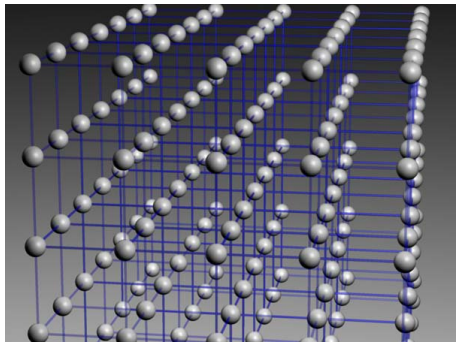
Code-based

Multivariate

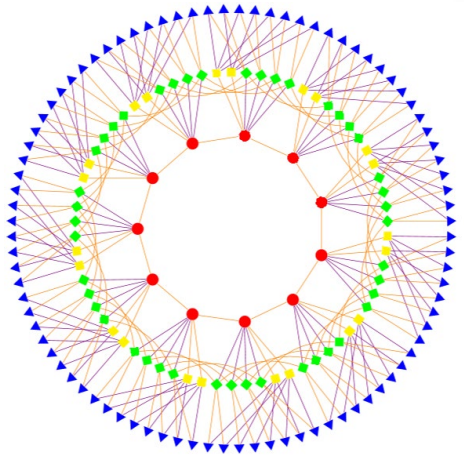
Others

- Hash-based signatures
- Isogeny-based signatures
- Etc….

All have their pros and cons



01010111 01101001 01101011
01101001 01110000 01100101
01100100 01101001 01100001



$$
\begin{aligned}
f_1(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1,\\
f_2(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2,\\
&\vdots\\
f_m(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m,
\end{aligned}
$$

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

Really, a lot more questions than answers

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 MDPC	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

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

PQC Standardization – A big decision to move forward

Considering the time to develop/deploy PQC standards and the backward secrecy required for information, **it is the time** to look into standardization

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

What we have done so far – The first mile in a long journey

- ~ 2012 – NIST begins PQC project
  - Research and build NIST team
- April 2015 – 1st NIST PQC workshop
- Aug 2015 – NSA statement
- Feb 2016 – NIST Report on PQC (NISTIR 8105)
- Feb 2016 – NIST preliminary announcement of standardization plan
- Aug 2016 – Draft submission requirements and evaluation criteria released for public comments
- Sep 2016 – Comment period ends
- Dec 2016 – Announcement of finalized requirements and criteria(Federal Register Notice)
- Nov 2017 – Deadline for submissions

NIST PQC team – The most significant in the first mile

Consists of 10+ NIST researchers in crypto, quantum information, quantum algorithms

Hold bi-weekly seminars (internal and invited speakers)

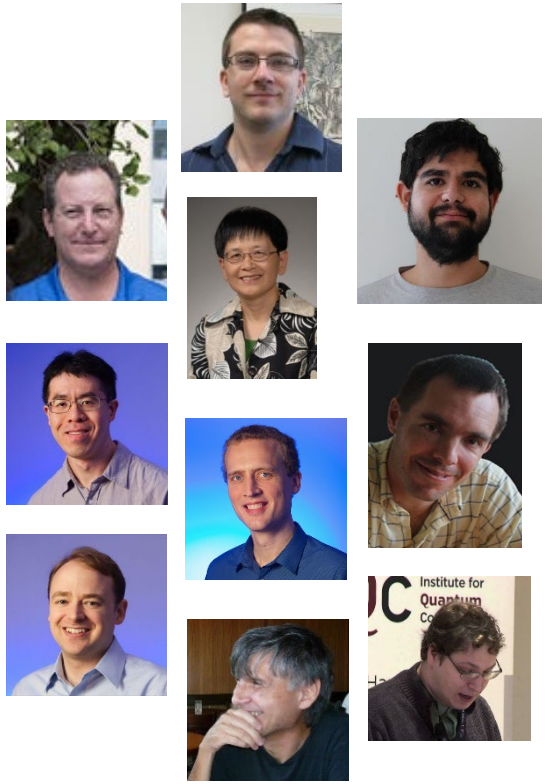
Publish results at PQcrypto and other journals/conferences

Engage with research community (presentations and discussion forums)

Work with industry and standards organizations (ETSI, IETF, ISO/IEC SC27)

Reach government agencies for raising awareness of upcoming cryptography transition

Collaborate with QuiCS (Joint Center for Quantum Information and Computer Science) at the University of Maryland, as well as University of Waterloo



NIST's ~~PQC Contest~~ Standardization Plan

Timeline	
Nov. 30, 2017	Submission deadline
April 2018	Workshop – Submitters' presentations
3-5 years	Analysis phase - NIST reports on findings and more workshops/conferences
2 years later	Draft standards available for public comments

- NIST will post "complete and proper" submissions
- NIST PQC Standardization Conference (with PQCrypto, Apr 2018)
- Initial phase of evaluation (12-18 months)
  - Internal and public review
  - No modifications allowed
- Narrowed pool will undergo a second round (12-18 months)
  - Second conference to be held
  - Minor changes allowed
- Possible third round of evaluation, if needed
- NIST will release reports on progress and selection rationale

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

Complexities of PQC Standardization

- Much broader scope – three crypto primitives
  - Signatures, Encryption, Key agreement
- Against both classical and quantum attacks
  - Security strength assessment on specific parameter selections
- Consider various theoretical security models and practical attacks
  - Provably security vs. security against instantiation or implementation related security flaws and pitfalls
- Multiple tradeoff factors
  - Security, performance, key size, signature size, side-channel resistance countermeasures
- Migrations into new and existing applications
  - TLS, IKE, code signing, PKI infrastructure, and much more
- Not exactly a competition – it is and it isn't

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

Minimal acceptability requirements

- Publicly disclosed and freely available during the process
  - Signed statements, disclose patent info
- 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
- Concrete values for parameters meeting target security levels

The selection criteria

Secure against both classical and quantum attacks

Performance - measured on various "classical" platforms

Other properties

- Drop-in replacements - Compatibility with existing protocols and networks
- Perfect forward secrecy
- Resistance to side-channel attacks
- Simplicity and flexibility
- Misuse resistance, and
- More

Security Analysis

Security definitions

- IND-CCA2 for encryption, EUF-CMA for signatures, CK best for key exchange?
- Used to judge whether an attack is relevant

Quantum/classical algorithm complexity

- Stability of best known attack complexity
- Precise security claim against quantum computation
- Parallelism?

Security proofs (not required but considered as support material)

Quality and quantity of prior cryptanalysis

Quantum Security – How to assess it?

- Currently, NIST crypto standards specify parameters for classical security levels at 112, 128, 192, 256 bits
- For PQC standardization, need to specify concrete parameters with security estimates
  - Led to the bits of quantum security requirements in the draft CFP
- No clear consensus on best way to measure quantum attacks
- Uncertainties
  - The possibility that new quantum algorithms will be discovered, leading to new attacks
  - The performance characteristics of future quantum computers, such as their cost, speed and memory size

Quantum Security Strength Categories

	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)

Computational resources should be measured using a variety of metrics

- Number of classical elementary operations, quantum circuit size, etc…
- Consider realistic limitations on circuit depth (e.g. 2^{40} to 2^{80} logical gates)
- May also consider expected relative cost of quantum and classical gates.

These are understood to be preliminary estimates

Cost and Performance

Standardized post-quantum cryptography will be implemented in "classical" platforms

Ideally, implementable on wide variety of platforms and applications

May need to standardize more than one algorithm for each function to accommodate different application environments

- from extremely processing constrained devices to limited communication bandwidth

Allowing parallel implementation for improving efficiency is certainly a plus

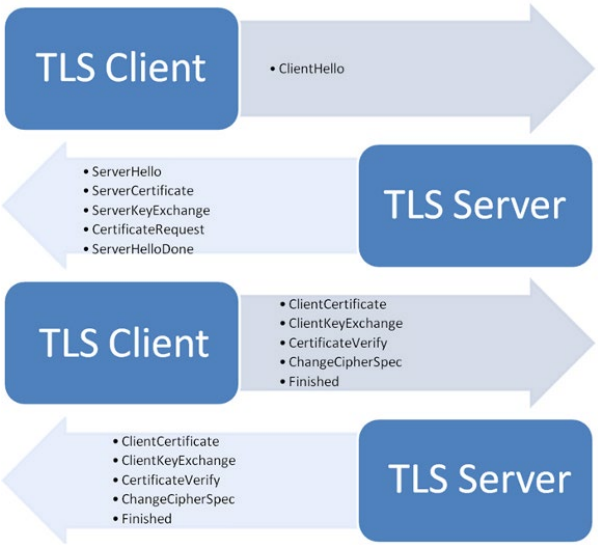
Preliminary conclusions: efficiency likely OK, but key sizes may pose a significant challenge

Drop-in Replacements

We're looking for quantum-resistant drop-in replacements for existing applications, e.g. Internet Key Exchange (IKE) and Transport Layer Security (TLS)

- Key establishment
  - Ideally, we'd like to have something to replace Diffie-Hellman key exchange
  - Practically, we have to look into some schemes such as encryption with one-time public key, which are not quite drop-in replacements
- Signatures
  - We'd like to have signatures with reasonable public key size, signature size, and fast signature verification
  - Practically, we shall prepare to handle probably larger public keys, or/and larger signatures, (and to handle a stateful situation)

We need to be realistic about what we can get for the quantum-resistant counterpart for existing applications



Challenges

Uncertainties – Quantum Security

- The possibility that new quantum algorithms will be discovered, leading to new attacks
- The performance characteristics of future quantum computers, such as their cost, speed and memory size

Assess classical security

- Most of PQC schemes are relatively new
- It takes years to understand their classical security

We need to deal with new situations which we haven't considered before, e.g.

- Decryption failure
- State management for hash based signatures
- Public-key encryption vs. key-exchange issues
  - Public-key encryption IND-CCA2
  - Ephemeral key exchange (no key-pair reuse, consider passive attacks, IND-CPA)
- Auxiliary functions/algorithms, e.g.
  - Gaussian simulation

We have to move away from many things we have been used with existing schemes

Transition and Migration

NIST will update guidance when PQC standards are available

- SP 800-57 Part I specifies “classical” security strength levels 128, 192, and 256 bits are acceptable through 2030

Even with the upcoming PQC transition, still required to move away from weak algorithms/key sizes:

- Anything with “classical” security strength less than 112 bits should NOT be used anymore

A “hybrid mode” has been proposed as a transition/migration step towards PQC cryptography

- Such a mode combines a classical algorithm with a post-quantum one
- Current FIPS 140 validation will only validate the NIST-approved (classical) component
- The PQC standardization will only consider the post-quantum component

Interactions with Standards Organizations

We are aware that many international/industry standards organizations and expert groups are working on or planning to work on post quantum cryptography standards/recommendations

- IEEE P1363.3 has standardized some lattice-based schemes
- IETF is taking action in specifying stateful hash-based signatures
- ETSI released quantum-safe cryptography report
- EU expert groups PQCrypto and SafeCrypto made recommendations and released reports
- ISO/IEC JTC 1 SC27 has already had three six months study periods for quantum-resistant cryptography

NIST is interacting and collaborating with these organizations and groups

NIST plan to consider hash-based signatures as an early candidates for standardization, but probably just for specific applications like code signing

Summary

Quantum computers have HUGE potential

Post-quantum cryptography standardization is going to be a long journey

After the first mile, we have observed many complexities and challenges

Be prepared to transition to new algorithms in 10 years

We will continue to work with the community towards PQC standardization

See www.nist.gov/pqcrypto

Sign up for the pqc-forum for announcements and discussion