Post-Quantum Cryptography

and Security in a Quantum Computing Era

Bo-Yin Yang, Academia Sinica

Nuvoton IoT Tech Forum 2022.06.28

“Postquantum” Cryptography

Genesis of the Discipline (2003–04)

I call it postquantum cryptography, for cryptography that survives post the quantum computing apocalypse. . . . Daniel J. Bernstein.

Definition of “Postquantum Cryptography”

Cryptosystems, in particular public-key cryptosystems, that stay secure even when the *attacker* has quantum computers.

We are only assumed to use **classical** computers

How long do you think before there are quantum computers, ones that can break RSA? . . . From the audience, CHES 2004

*I think quantum computers will arrive in ten to fifteen years, but **probably not for every man on the street**. . . . Isaac Chuang*

“Postquantum” Cryptography

Genesis of the Discipline (2003–04)

> *I call it postquantum cryptography, for cryptography that survives post the quantum computing apocalypse. . . . Daniel J. Bernstein.*

Definition of “Postquantum Cryptography”

Cryptosystems, in particular public-key cryptosystems, that stay secure even when the *attacker* has quantum computers.

We are only assumed to use **classical** computers

> *How long do you think before there are quantum computers, ones that can break RSA? . . . From the audience, CHES 2004*
>
> *I think quantum computers will arrive in ten to fifteen years, but **probably not for every man on the street**. . . . Isaac Chuang*

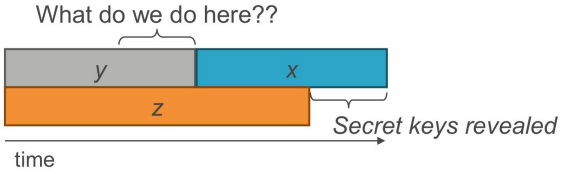
Experts today estimates 10–15 years to Cryptographically Relevant Quantum Computers.

How soon do we need to worry?

Depends on:

- How long do you need encryption to be secure? (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance? (*z* years)

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



What to do about Quantum Supremacy (2019)

Impending Arrival of Quantum Computing

Google Published about its 53-bit Quantum Computer

- Quantum Supremacy refers to a computation that classical computers cannot do ...
- Which happens to be simulating a quantum computer!
- The entire machine is liquid-He cooled (under $4^{\circ}K$)

Other entities (IBM, China) announced their own

Has Quantum Computing arrived? What impact must we prepare for?

Alert: Not A Faster Computer

It's Different, Occasionally Excels, **Including Breaking Crypto**

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in com-

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was

Why Postquantum Cryptography (PQC)

Almost All Network Transactions Are Encrypted

Every `https://` access uses Public-Key Cryptography (RSA, ECC...)

Quantum Computing (Shor's Algorithm) Breaks Cryptosystems

RSA, ECC (Elliptic Curve Cryptography, including ECDSA) etc.

- RSA depends on Factoring
- ECC depends on Discrete Logarithms on Elliptic Curve Groups

Why Postquantum Cryptography (PQC)

Almost All Network Transactions Are Encrypted

Every `https://` access uses Public-Key Cryptography (RSA, ECC…)

Quantum Computing (Shor's Algorithm) Breaks Cryptosystems

~~RSA, ECC (Elliptic Curve Cryptography, including ECDSA)~~ …all broken

Quantum Computers Don't Solve All Hard Problems

- Decoding a Random (error-correcting) Code
- Solving a Multivariate Quadratic (MQ) system of equations
- Find Short Vectors in Lattices, Inverting One-Way Functions in Symmetric Crypto

Cryptosystems based on these aren't broken by quantum computing.

Cryptosystems Surviving Quantum Computing are **PostQuantum**

McEliece (Codes), NTRU, LPR (Lattices), Unbalanced-Oil-and-Vinegar (MQ), etc.

Why Postquantum Cryptography (PQC)

Post Quantum(-Apocalypse) Cryptography, not Post “Quantum Cyptography”

nuvoTon

Cryptosystems Surviving Quantum Computing are PostQuantum

McEliece (Codes), NTRU, LPR (Lattices), Unbalanced-Oil-and-Vinegar (MQ), etc.

Why Postquantum Cryptography (PQC)

Post Quantum(-Apocalypse) Cryptography, not Post “Quantum Cyptography”

nuvoTon

Cryptosystems Surviving Quantum Computing are PostQuantum

McEliece (Codes), NTRU, LPR (Lattices), Unbalanced-Oil-and-Vinegar (MQ), etc.

PQC does not come after Quantum Crypto!

- PQC: Enemies have expensive Quantum Equipment
- Quantum Crypto: Everyone has expensive Quantum Equipment

Why Postquantum Cryptography (PQC)

Post Quantum(-Apocalypse) Cryptography, not Post “Quantum Cyptography”

Cryptosystems Surviving Quantum Computing are **PostQuantum**

McEliece (Codes), NTRU, LPR (Lattices), Unbalanced-Oil-and-Vinegar (MQ), etc.

PQC does **not** come after Quantum Crypto!

- PQC: Enemies have expensive Quantum Equipment
- Quantum Crypto: Everyone has expensive Quantum Equipment

PQC is ready **now**

- RSA was 18 years old when standardized(1994), ECC was 20(2005).
- McEliece, the oldest PQC, was proposed in 1978 and is now 43.

Why Postquantum Cryptography (PQC)

Post Quantum(-Apocalypse) Cryptography, not Post "Quantum Cyptography"

Cryptosystems Surviving Quantum Computing are **PostQuantum**

McEliece (Codes), NTRU, LPR (Lattices), Unbalanced-Oil-and-Vinegar (MQ), etc.

PQC does **not** come after Quantum Crypto!

- PQC: Enemies have expensive Quantum Equipment
- Quantum Crypto: Everyone has expensive Quantum Equipment

PQC is ready **now**, can be deployed on **today's** equipment

- McEliece, the oldest PQC, was proposed in 1978 and is now 43.

Why Postquantum Cryptography (PQC)

Post Quantum(-Apocalypse) Cryptography, not Post "Quantum Cyptography"

Cryptosystems Surviving Quantum Computing are **PostQuantum**

McEliece (Codes), NTRU, LPR (Lattices), Unbalanced-Oil-and-Vinegar (MQ), etc.

PQC does **not** come after Quantum Crypto!

- PQC: Enemies have expensive Quantum Equipment
- Quantum Crypto: Everyone has expensive Quantum Equipment

PQC is ready **now**, can be deployed on **today's** equipment

- McEliece, the oldest PQC, was proposed in 1978 and is now 43.

Usually Quantum Crypto = Quantum Key Distribution (QKD)

U.S. National Security Agency taken a position against QKD/QC

Why Postquantum Cryptography (PQC)

Post Quantum(-Apocalypse) Cryptography, not Post "Quantum Cyptography"

Cryptosystems Surviving Quantum Computing are **PostQuantum**

McEliece (Codes), NTRU, LPR (Lattices), Unbalanced-Oil-and-Vinegar (MQ), etc.

PQC does **not** come after Quantum Crypto!

- PQC: Enemies have expensive Quantum Equipment
- Quantum Crypto: Everyone has expensive Quantum Equipment

PQC is ready **now**, can be deployed on **today's** equipment

- McEliece, the oldest PQC, was proposed in 1978 and is now 43.

Usually Quantum Crypto = Quantum Key Distribution (QKD)

U.S. National Security Agency taken a position against QKD/QC, that it is overpriced, unnecessary, and doesn't deliver on its security promises.

Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

Synopsis

NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

What are Quantum Key Distribution (QKD) and Quantum Cryptography (QC)?

Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link. Published theories suggest that physics allows QKD or QC to detect the presence of an eavesdropper, a feature not provided in standard cryptography.

Quantum-resistant algorithms are implemented on existing platforms and derive their security through mathematical complexity. These algorithms used in cryptographic protocols provide the means for assuring the confidentiality, integrity, and authentication of a transmission—even against a potential future quantum computer. The National Institute of Standards and Technology (NIST) is presently conducting a rigorous selection process to identify quantum-resistant (or post-quantum) algorithms for standardization[1]. Once NIST completes its selection process, NSA will issue updated guidance through CNSSP-15.

Understanding the QKD/QC story

Quantum key distribution and Quantum cryptography vendors—and the media—occasionally state bold claims based on theory—e.g., that this technology offers "guaranteed" security based on the laws of physics. Communications needs and security requirements physically conflict in the use of QKD/QC, and the engineering required to balance these fundamental issues has extremely low tolerance for error. Thus, security of QKD and QC is highly implementation-dependent rather than assured by laws of physics. Although we refer to QKD only to simplify discussion below, similar statements can be made for QC.

Technical limitations

1. **Quantum key distribution is only a partial solution.** QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if

Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

Synopsis

NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

What are Quantum Key Distribution (QKD) and Quantum Cryptography (QC)?

Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link. Published theories suggest that physics allows QKD or QC to detect the presence of an eavesdropper, a feature not provided in standard cryptography.

Quantum-resistant algorithms are implemented on existing platforms and derive their security through mathematical complexity. These algorithms used in cryptographic protocols provide the means for assuring the confidentiality, integrity, and authentication of a transmission—even against a potential future quantum computer. The National Institute of Standards and Technology (NIST) is presently conducting a rigorous selection process to identify quantum-resistant (or post-quantum) algorithms for standardization. When NIST completes its selection process, NSA will issue updated guidance through CNSSP-15.

Quantum key distribution and Quantum cryptography vendors—and the media—occasionally state bold claims based on theory—e.g., that this [illegible] conflict in [illegible] security of [illegible] discussion [illegible]

1. **Quantum key distribution is only a partial solution.** QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if

Synopsis:
NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

NSA on Quantum Key Distribution (QKD)

Technical limitations

- QKD requires special purpose equipment (not just any computer).
- QKD increases infrastructure costs and insider threat risks.
- QKD poses a significant challenge to secure and validate.
- QKD increases the risk of denial of service.
- QKD is only a partial solution.
  - provide no authentication, actually needs an authenticated channel
    - in modern crypto, authentication $\Leftrightarrow$ can exchange keys $\Leftrightarrow$ do secure communications.

NSA on Quantum Key Distribution (QKD)

Technical limitations

- QKD requires special purpose equipment (not just any computer).
- QKD increases infrastructure costs and insider threat risks.
- QKD poses a significant challenge to secure and validate.
- QKD increases the risk of denial of service.
- QKD is only a partial solution.
  - provide no authentication, actually needs an authenticated channel
    - in modern crypto, authentication $\Leftrightarrow$ can exchange keys $\Leftrightarrow$ do secure communications.

NSA's Suggestion: Postquantum (Quantum-Resistant) Cryptography

- Follow the NIST (National Institute for Standards and Technology) Process for Post-Quantum Cryptography Standardization

NSA on Quantum Key Distribution (QKD)

Technical limitations

- QKD requires special purpose equipment (not just any computer).
- QKD increases infrastructure costs and insider threat risks.
- QKD poses a significant challenge to secure and validate.
- QKD increases the risk of denial of service.
- QKD is only a partial solution.
  - provide no authentication, actually needs an authenticated channel
    - in modern crypto, authentication $\Leftrightarrow$ can exchange keys $\Leftrightarrow$ do secure communications.

NSA's Suggestion: Postquantum (Quantum-Resistant) Cryptography

- Follow the NIST Process for Post-Quantum Cryptography Standardization

Other Security Agencies Also Do Not Endorse QKD

British, Dutch, German, French, EU's ENISA ...

NIST Competition leads the Way

Brief Timeline Leading Up To the NIST Open Call

1994 Shor's Algorithm

1999 IBM's 7-qubit factorization of 15

2003 "Post-Quantum Cryptography (PQC)" coined

2006 First International Workshop on Post-Quantum Cryptography

2015 NIST PQC workshop, NSA PQC announcements

2016 NIST Calls for a PQC standard competition

NIST in Charge

Slides, D. Moody, National Institute of Standards and Technology, 2019.05.10

NIST Competitions*

- Block Cipher
  - AES – 15 candidates, 2 rounds, 5 finalists, 3 years + 1 year for standard
- Hash Function
  - SHA-3 – 64 submissions, 51 accepted, 3 rounds, 14 2nd round candidates, 5 finalists, 5 years + 3 years for standard
- *Post-Quantum Cryptography*
  - No Name? – 82 submissions, 69 accepted, 2 (or 3) rounds, 26 2nd round candidates, 2017-2020ish + 2? Years for standard
- Lightweight Crypto
  - 57 submissions, 2019-2022ish

Taiwan in NIST Round 3

Finalists: May be standardized after this Round

Key Establishment Methods	Basis	Signatures	Basis
Classic McEliece	Code	Crystals-Dilithium	Lattice
Crystals-Kyber	Lattice	Falcon	Lattice
NTRU	Lattice	Rainbow	Multivariate
Saber	Lattice		

Alternates: May be standardized after a Possible 4th Round

Key Establishment Methods	Basis	Signatures	Basis
BIKE	Code	GeMSS	Multivariate
FrodoKEM	Lattice	Picnic	Symmetric
HQC	Code	SPHINCS+	Symmetric
NTRU Prime	Lattice		
SIKE	Isogenies		

Recommendation I: What PQC To Use?

If Pressed **today**

I would suggest

- Classic McEliece for long term secrets
  - 43 years and the asymptotic security level remains the same
- NTRU Prime for most secret transmissions
  - Used by the ultra-paranoid secure-connections library `OpenSSH`.
    - `OpenSSH` is used in $> 50\%$ of live IPv4 addresses on the internet.
- Hash-based signatures for state matters
  - SPHINCS+ (Alternate in NIST Round 3, well understood and secure).
  - LMS (Also well understood and secure, but *different*)
- Use Prequantum-Postquantum Hybrids

Stateful Hash Function Signatures

There are high-speed digital signatures XMSS and LMS, which everyone believes to be secure under some reasonable sounding conditions.

Older Hash-Based Digital Signatures and their Limitations

- Limited Number of Uses
- Need to keep a Persistent State

Ready-to-Go

- They are NIST standards as described in SP 800-208

Recommendation II: Transitioning Now

A Long Term Security Officer for your Institution

Need someone specifically in charge of moving to Long Term Security for big institutions

First Task: Inventory the Current Systems

- Replace all security-related systems for which source is unavailable.
- Find all uses of traditional crypto (RSA, ECC, etc.)
- Find and replace ≤ 128-bit (and maybe 128-bit) symmetric crypto
  - Must Replace: MD5, SHA-1 (by SHA-2 or SHA-3) 3DES (by ChaCha20 or AES-256); Optional: AES-128 (by AES-256)

Second Task: Shift for Long Term Security

- Classic McEliece (in Hybrid Mode) to encrypt long-term secrets
- NTRU Prime (in Hybrid Mode) to encrypt short-term transmissions
- SPHINCS+ or XMSS to sign presidential and state announcements

Recommendation III: Key Continuity

Assume Each Transmission Protected by a Shared Secret

Each time the two parties establish a key via traditional crypto (RSA, ECC ...), mix the newly established "shared key" with the last prior shared key, and use that as the next real new shared key.

- For stronger security, update stored shared key
- By "mix" we usually mean "apply a hash function".
- Establish initial shares out of band when setting up a new device
- Do not discard a shared key until a new one is established.

What Does Key Continuity Gain Us?

Security: Attacker cannot read our continuing conversation without

- having our previous shared key, *and*
- being able to break the key establishment method

Cost: Hash functions are secure, efficient and easy to implement.

Recommendations IV: Start Now

There is little time to lose

nuvoTon

We shouldn't wait for NIST

- It takes years (maybe a decade) to build and transition systems.
- Key Continuity is cheap and useful
- This will be good for the institution anyway

What is Already Available

- Open Source software is available
- Verification Efforts underway
- No Patent problems in each of the named cryptosystems

That's All, and for Your Further Reading

- BSI, German Federal Office for Information Security, Status of quantum computer development, version 1.2.
- E. Grumbling, M. Horowitz, eds. Quantum Computing: Progress and Prospects, National Academy of Sciences.
- M. Mosca, M. Piani, Quantum threat timeline, Global Risk Institute,
- National Institute for Standards and Technology, Post-Quantum Initiative.
- ENISA Report: Post-Quantum Cryptography: Current state and quantum mitigation
- Post-Quantum Mini-School, Taipei 2020

Progress on Quantum Attacks

C. Gidney, M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, `https://arxiv.org/abs/1905.09749`