

Introduction to post-quantum cryptography

Daniel J. Bernstein & Tanja Lange

University of Illinois at Chicago; Ruhr University Bochum; Academia Sinica
&
Eindhoven University of Technology; Academia Sinica

25 August 2022

Cryptography



Sender
"Alice"



Receiver
"Bob"

Jeanette Nuñez picture credit: Public Domain, [Wikimedia](#). Ron DeSantis picture credit: Public Domain, [Wikimedia](#).

Cryptography



Sender
"Alice"



Untrustworthy network
"Eve"



Receiver
"Bob"

- ▶ Motivation #1: Communication channels are spying on our data.
- ▶ Motivation #2: Communication channels are modifying our data.

Cryptography



Sender
"Alice"



Untrustworthy network
"Eve"



Receiver
"Bob"

- ▶ Motivation #1: Communication channels are spying on our data.
- ▶ Motivation #2: Communication channels are modifying our data.
- ▶ Literal meaning of cryptography: "secret writing".
- ▶ Achieves various security goals by secretly transforming messages.
 - ▶ Confidentiality: Eve cannot infer information about the content
 - ▶ Integrity: Eve cannot modify the message without this being noticed
 - ▶ Authenticity: Bob is convinced that the message originated from Alice

The scale of the threat

2012 “[Investigative Report](#) on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE” by the Permanent Select Committee on Intelligence in the U.S. House of Representatives:

Chinese intelligence collection efforts against the U.S. government are growing in “scale, intensity and sophistication.”¹² Chinese actors are also the world’s most active and persistent perpetrators of economic espionage.¹³ U.S. private sector firms and cybersecurity specialists report an ongoing onslaught of sophisticated computer network intrusions that originate in China, and are almost certainly the work of, or have the backing of, the Chinese government.¹⁴ Further, Chinese intelligence services, as well as private companies and other entities, often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data.¹⁵

Cryptographic tools

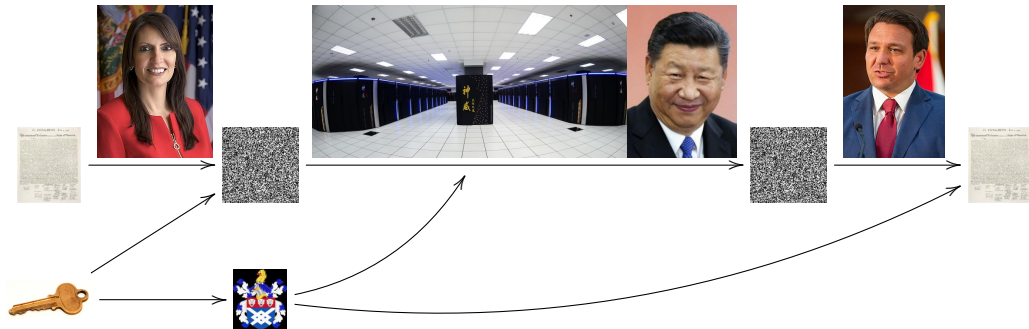
Many factors influence the security and privacy of data:

- ▶ Secure storage, physical security; access control.
- ▶ Protection against alteration of data
⇒ [public-key signatures](#), [message-authentication codes](#).
- ▶ Protection of sensitive content against reading
⇒ [encryption](#) (public-key or symmetric-key).

Many more security goals studied in cryptography

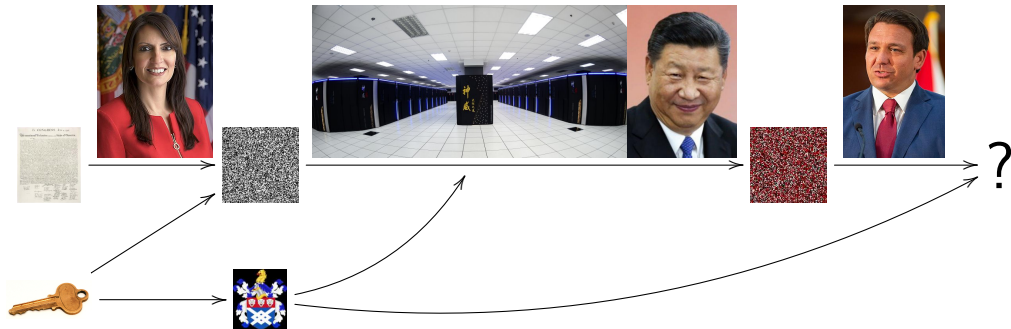
- ▶ Protecting against denial of service.
- ▶ Stopping traffic analysis.
- ▶ Securely tallying votes.
- ▶ Searching in and computing on encrypted data.
- ▶ ...








Public-key signatures



- ▶ Prerequisite: Alice has a private key  and public key .
- ▶ Prerequisite: Everyone knows  as belonging to Alice.
- ▶ Alice signs messages using . Other people verify using .

Public-key signatures



- ▶ Prerequisite: Alice has a private key  and public key .
- ▶ Prerequisite: Everyone knows  as belonging to Alice.
- ▶ Alice signs messages using . Other people verify using .
- ▶ Security goals: Integrity and authenticity.
- ▶ Nobody can produce signatures valid under  without .
- ▶ Modifications to signed message get caught.



Connection Security for qsancus.com

You are securely connected to this site.

Verified by: Cloudflare, Inc.

More Information

Events

[The First USF-QSancus Workshop on Post-Quantum Cryptography](#)

<i>Date</i>	<i>Location</i>	<i>Add. Info</i>
-------------	-----------------	------------------



https://qsancus.com/events/



Connection Security for qsancus.com

You are securely connected to this site.

Verified by: Cloudflare, Inc.

More Information

[General](#)[Media](#)[Permissions](#)[Security](#)

Website Identity

Website: qsancus.com

Owner: This website does not supply ownership information.

Verified by: Cloudflare, Inc.

[View Certificate](#)

Expires on: November 3, 2022

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies

[Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No

[View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

sni.cloudflaressl.com

Cloudflare Inc ECC CA-3

Baltimore CyberTrust Root

Subject Name

Country	US
State/Province	California
Locality	San Francisco
Organization	Cloudflare, Inc.
Common Name	sni.cloudflaressl.com

Issuer Name

Country	US
Organization	Cloudflare, Inc.
Common Name	Cloudflare Inc ECC CA-3

Validity

Not Before	Wed, 03 Nov 2021 00:00:00 GMT
Not After	Wed, 02 Nov 2022 23:59:59 GMT

Subject Alt Names

DNS Name	*.qsancus.com
-----------------	---------------

Subject Alt Names

DNS Name	*.qsancus.com
DNS Name	sni.cloudflaressl.com
DNS Name	qsancus.com

Public Key Info

Algorithm	Elliptic Curve
Key Size	256
Curve	P-256
Public Value	04:24:DB:45:A9:43:24:97:7A:FC:20:E9:C5:61:86:BD:98:1E:32:7D:C...

Miscellaneous

Serial Number	01:DF:45:D4:0E:C1:BE:FD:63:F3:56:7C:E1:9C:30:DB
Signature Algorithm	ECDSA with SHA-256
Version	3
Download	PEM (cert) PEM (chain)

Cryptographic tools used in TLS (<https>)

TLS relies critically on public-key cryptography for two reasons:

- ▶ Making sure the attacker can't pretend to be the server.
This uses signatures: e.g., ECDSA P-256 or RSA-4096.
- ▶ Sending data as scrambled “ciphertexts” that the attacker can't understand.
This uses encryption: e.g., ECDH P-256.

Cryptographic tools used in TLS (<https>)

TLS relies critically on public-key cryptography for two reasons:

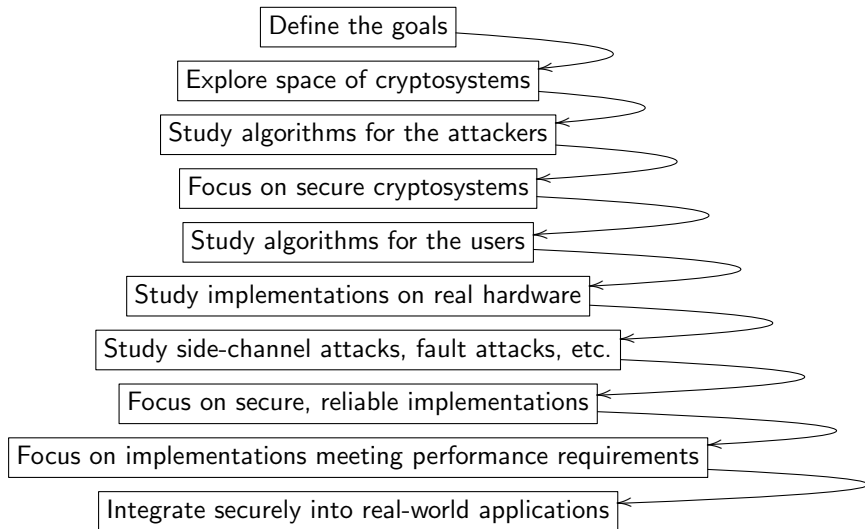
- ▶ Making sure the attacker can't pretend to be the server.
This uses signatures: e.g., ECDSA P-256 or RSA-4096.
- ▶ Sending data as scrambled “ciphertexts” that the attacker can't understand.
This uses encryption: e.g., ECDH P-256.

For speed, TLS combines public-key cryptography with symmetric cryptography:

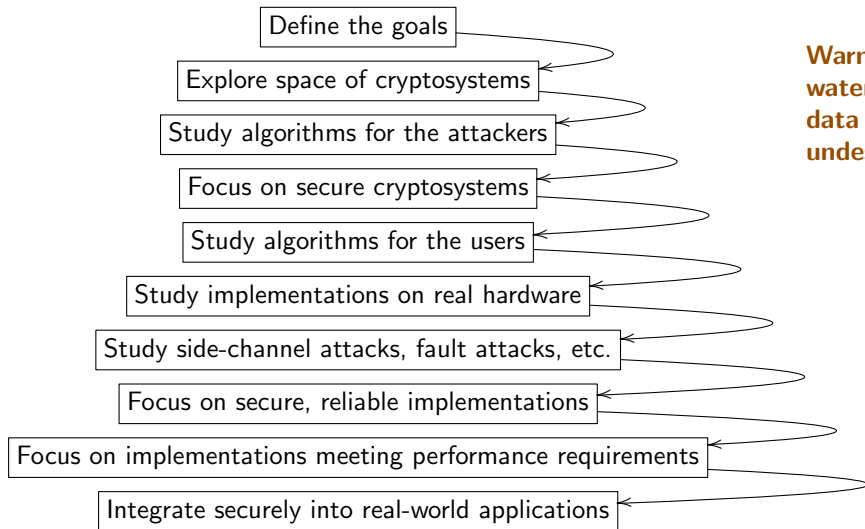
- ▶ Use public-key encryption to exchange a key,
and public-key signatures so the attacker can't substitute a different key.
- ▶ Use symmetric encryption with that key to protect confidentiality of user data.
This uses, e.g., AES.
- ▶ Use symmetric authentication with that key to protect integrity of user data.
This uses, e.g., GCM with SHA-256.

Similar comments for SSH and other popular cryptographic protocols.

Many stages of cryptographic research from design to deployment



Many stages of cryptographic research from design to deployment



Warning:
waterfall
data flow,
undesirable.



Algorithms for Quantum Computation: Discrete Logarithms and Factoring

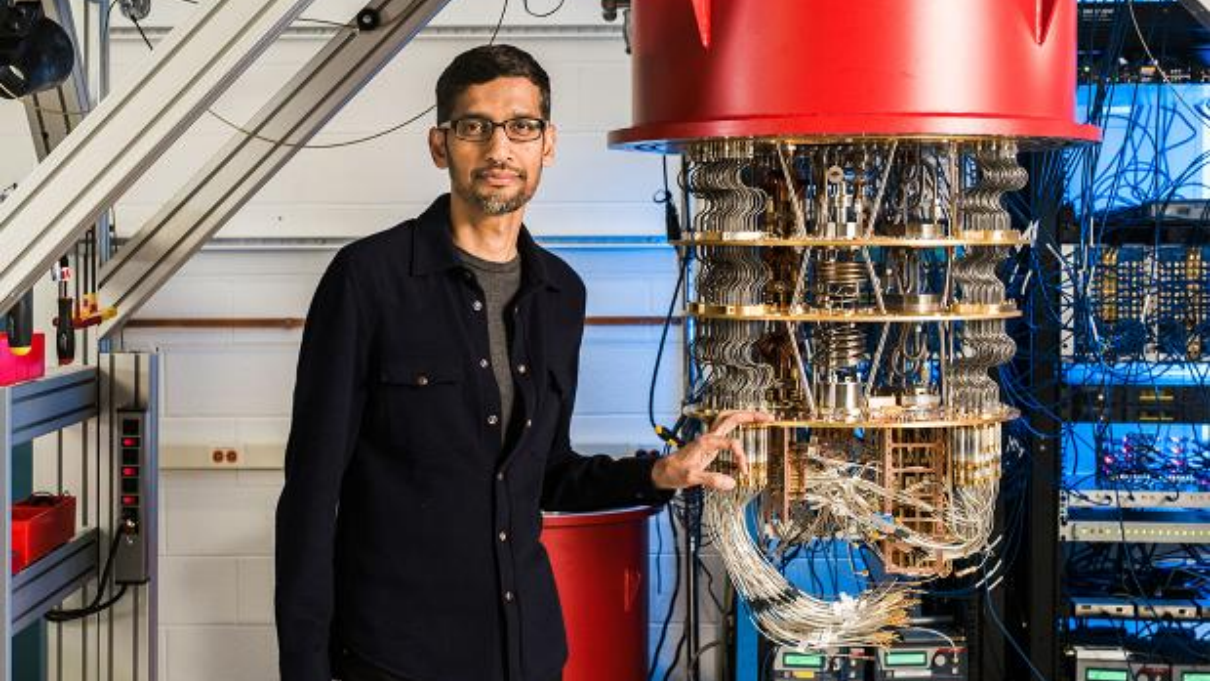
Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

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 computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their compu-

[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 the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

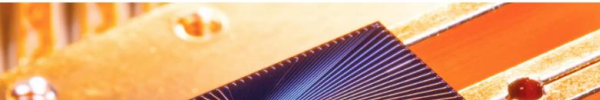
The next part of this paper discusses how quantum computation relates to classical complexity classes. We will



◆ Premium

🏠 > Technology Intelligence

Quantum computing could end encryption within five years, says Google boss



Mr Pichai said a combination of artificial intelligence and quantum would "help us tackle some of the biggest problems we see", but said it was important encryption evolved to match this.

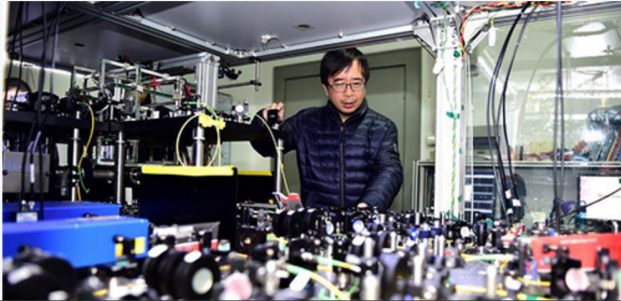
"In a five to ten year time frame, quantum computing will break encryption as we know it today."

This is because current encryption methods, by which information such as texts or passwords is turned into code to make it unreadable, rely upon the fact that classic computers would take billions of years to decipher that code.

Quantum computers, with their ability to be

Chinese researchers expect quantum leap in computing, challenging Google's supremacy

Source: Global Times Published: 2020/8/26 14:58:42



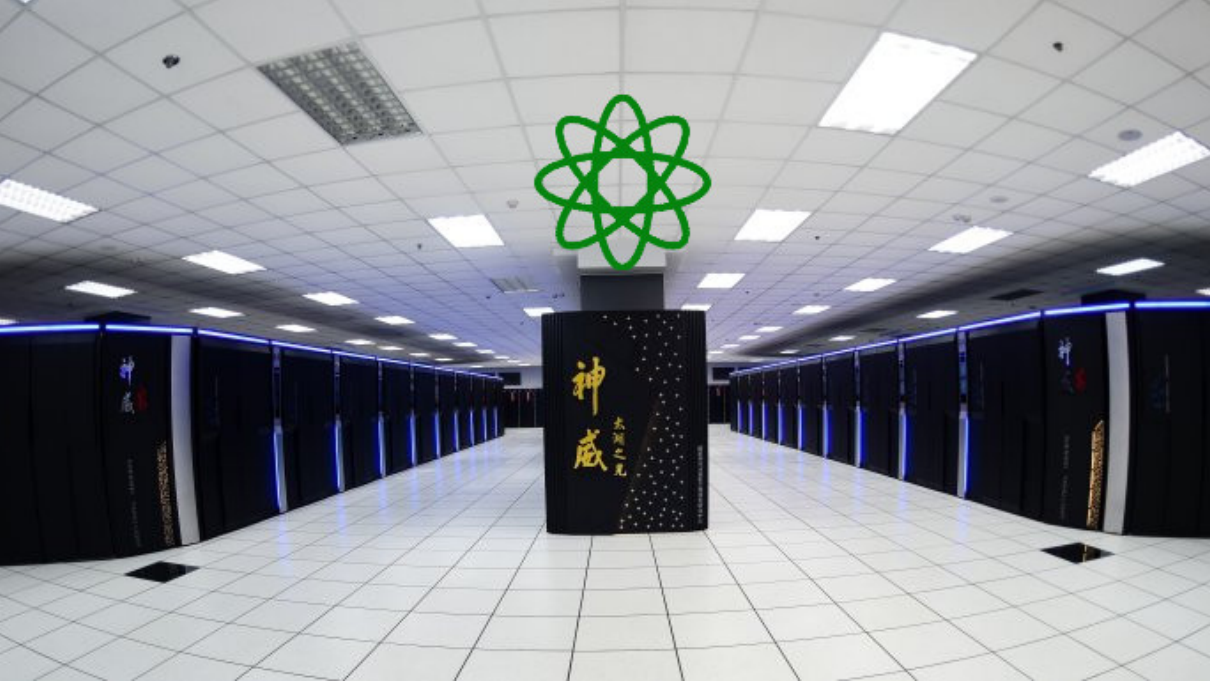
SOURCE / ECONOMY

Chinese researchers achieve quantum advantage in two mainstream routes

By Global Times

Published: Oct 26, 2021 01:18 PM





National Academy of Sciences (US)

4 December 2018: [Report on quantum computing](#)

Don't panic. “Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade.”

National Academy of Sciences (US)

4 December 2018: [Report on quantum computing](#)

Don't panic. “Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade.”

Panic. “Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster.”

“[Section 4.4:] In particular, all encrypted data that is recorded today and stored for future use, will be cracked once a large-scale quantum computer is developed.”

Commonly used systems



Sender
"Alice"



Untrustworthy network
"Eve"



Receiver
"Bob"

Cryptography with symmetric keys

AES-128. AES-192. AES-256. AES-GCM. ChaCha20. HMAC-SHA-256. Poly1305. SHA-2. SHA-3. Salsa20.

Cryptography with public keys

BN-254. Curve25519. DH. DSA. ECDH. ECDSA. EdDSA. NIST P-256. NIST P-384. NIST P-521. RSA encrypt. RSA sign. secp256k1.

Commonly used systems



Sender
"Alice"



Untrustworthy network
"Eve" with quantum computer



Receiver
"Bob"

Cryptography with symmetric keys

**AES-128. AES-192. AES-256. AES-GCM. ChaCha20. HMAC-SHA-256. Poly1305.
SHA-2. SHA-3. Salsa20.**

Cryptography with public keys

**BN-254. Curve25519. DH. DSA. ECDH. ECDSA. EdDSA. NIST P-256. NIST P-384.
NIST P-521. RSA encrypt. RSA sign. secp256k1.**

Post-quantum cryptography

Cryptography under the assumption that the attacker has a quantum computer.

Major categories:

- ▶ **Code-based** encryption: McEliece cryptosystem has survived since 1978. Short ciphertexts and large public keys. Security relies on hardness of decoding error-correcting codes.
- ▶ **Hash-based** signatures: very solid security and small public keys. Require only a secure hash function (hard to find second preimages).
- ▶ **Isogeny-based** encryption: new kid on the block, promising short keys and ciphertexts and non-interactive key exchange. Security relies on hardness of finding isogenies between elliptic curves over finite fields.
- ▶ **Lattice-based** encryption and signatures: possibility for balanced sizes. Security relies on hardness of finding short vectors in some (typically special) lattice.
- ▶ **Multivariate-quadratic** signatures: short signatures and large public keys. Security relies on hardness of solving systems of multivariate equations over finite fields.

Warning: These are categories of mathematical problems;
individual systems may be totally insecure if the problem is not used correctly.

Post-quantum cryptography timeline

- ▶ 1994: Shor's quantum algorithm. 1996: Grover's quantum algorithm.
Many subsequent papers on quantum algorithms: see quantumalgorithmzoo.org.
- ▶ 2003: Daniel J. Bernstein introduces term [Post-quantum cryptography](#).
- ▶ 2006: First International Workshop on Post-Quantum Cryptography. PQCrypto 2006, 2008, 2010, 2011, 2013, 2014, 2016, 2017, 2018, 2019, 2020, 2021, (soon) 2022.
- ▶ 2015: NIST hosts its first workshop on post-quantum cryptography.
- ▶ 2016: NIST announces a standardization project for post-quantum systems.
- ▶ 2017: Deadline for submissions to the NIST competition.
- ▶ 2017 – 69 candidates, lots of cryptanalysis, mostly on immature systems (13 broken).
- ▶ 2019: Second round of NIST competition begins.
- ▶ 2019 – 26 candidates, more cryptanalysis (2 broken).
- ▶ 2020: Third round of NIST competition begins.
- ▶ 2020 – Focus on 15 candidates; even two established systems crumble.
- ▶ 2021 “end of December”: NIST announces first selections.

Post-quantum cryptography timeline

- ▶ 1994: Shor's quantum algorithm. 1996: Grover's quantum algorithm.
Many subsequent papers on quantum algorithms: see quantumalgorithmzoo.org.
- ▶ 2003: Daniel J. Bernstein introduces term [Post-quantum cryptography](#).
- ▶ 2006: First International Workshop on Post-Quantum Cryptography. PQCrypto 2006, 2008, 2010, 2011, 2013, 2014, 2016, 2017, 2018, 2019, 2020, 2021, (soon) 2022.
- ▶ 2015: NIST hosts its first workshop on post-quantum cryptography.
- ▶ 2016: NIST announces a standardization project for post-quantum systems.
- ▶ 2017: Deadline for submissions to the NIST competition.
- ▶ 2017 – 69 candidates, lots of cryptanalysis, mostly on immature systems (13 broken).
- ▶ 2019: Second round of NIST competition begins.
- ▶ 2019 – 26 candidates, more cryptanalysis (2 broken).
- ▶ 2020: Third round of NIST competition begins.
- ▶ 2020 – Focus on 15 candidates; even two established systems crumble.
- ▶ ~~2021~~ 2022 “not later than the end of March” NIST announces first selections.

Post-quantum cryptography timeline

- ▶ 1994: Shor's quantum algorithm. 1996: Grover's quantum algorithm.
Many subsequent papers on quantum algorithms: see quantumalgorithmzoo.org.
- ▶ 2003: Daniel J. Bernstein introduces term [Post-quantum cryptography](#).
- ▶ 2006: First International Workshop on Post-Quantum Cryptography. PQCrypto 2006, 2008, 2010, 2011, 2013, 2014, 2016, 2017, 2018, 2019, 2020, 2021, (soon) 2022.
- ▶ 2015: NIST hosts its first workshop on post-quantum cryptography.
- ▶ 2016: NIST announces a standardization project for post-quantum systems.
- ▶ 2017: Deadline for submissions to the NIST competition.
- ▶ 2017 – 69 candidates, lots of cryptanalysis, mostly on immature systems (13 broken).
- ▶ 2019: Second round of NIST competition begins.
- ▶ 2019 – 26 candidates, more cryptanalysis (2 broken).
- ▶ 2020: Third round of NIST competition begins.
- ▶ 2020 – Focus on 15 candidates; even two established systems crumble.
- ▶ ~~2021~~ 2022 “~~not later than the end of March~~” July NIST announces first selections.
- ▶ 2023/2024?: NIST issues post-quantum standards.

NIST's 5 July 2022 (aka 127 March 2022) announcement

<https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>

The winners:

- ▶ Kyber, a public-key encryption system based on structured lattices
- ▶ Dilithium, a public-key signature scheme based on structured lattices
- ▶ Falcon, a public-key signature scheme based on structured lattices
- ▶ SPHINCS+, a public-key signature scheme based on

NIST's 5 July 2022 (aka 127 March 2022) announcement

<https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>

The winners:

- ▶ Kyber, a public-key encryption system based on structured lattices
- ▶ Dilithium, a public-key signature scheme based on structured lattices
- ▶ Falcon, a public-key signature scheme based on structured lattices
- ▶ SPHINCS+, a public-key signature scheme based on hash functions

NIST's 5 July 2022 (aka 127 March 2022) announcement

<https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>

The winners:

- ▶ Kyber, a public-key encryption system based on structured lattices
- ▶ Dilithium, a public-key signature scheme based on structured lattices
- ▶ Falcon, a public-key signature scheme based on structured lattices
- ▶ SPHINCS+, a public-key signature scheme based on hash functions

Schemes advancing to round 4, so maybe more winners later:

- ▶ BIKE, a public-key encryption system based on codes
- ▶ Classic McEliece, a public-key encryption system based on codes
- ▶ HQC, a public-key encryption system based on codes
- ▶ SIKE, a public-key encryption system based on isogenies

NIST's 5 July 2022 (aka 127 March 2022) announcement

<https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>

The winners:

- ▶ Kyber, a public-key encryption system based on structured lattices
- ▶ Dilithium, a public-key signature scheme based on structured lattices
- ▶ Falcon, a public-key signature scheme based on structured lattices
- ▶ SPHINCS+, a public-key signature scheme based on hash functions

Schemes advancing to round 4, so maybe more winners later:

- ▶ BIKE, a public-key encryption system based on codes
- ▶ Classic McEliece, a public-key encryption system based on codes
- ▶ HQC, a public-key encryption system based on codes
- ▶ ~~SIKE, a public-key encryption system based on isogenies~~

SIKE is not secure, completely broken after NIST's announcement.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.
Used for an experiment with Google servers.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

2016.11: Chrome removes `newhope1024` option.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

2016.11: Chrome removes `newhope1024` option.

2019.04: OpenSSH 8.0 adds `sntrup761` option.

Used if client and server configure it.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

2016.11: Chrome removes `newhope1024` option.

2019.04: OpenSSH 8.0 adds `sntrup761` option.

Used if client and server configure it.

2019.07: Chrome and Cloudflare experiment with `ntruhrss701` and `sikep434`.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

2016.11: Chrome removes `newhope1024` option.

2019.04: OpenSSH 8.0 adds `sntrup761` option.

Used if client and server configure it.

2019.07: Chrome and Cloudflare experiment with `ntruhrss701` and `sikep434`.

2021.05: OpenBSD adds `sntrup761` option for IPsec.

Used if client and server configure it.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

2016.11: Chrome removes `newhope1024` option.

2019.04: OpenSSH 8.0 adds `sntrup761` option.

Used if client and server configure it.

2019.07: Chrome and Cloudflare experiment with `ntruhrss701` and `sikep434`.

2021.05: OpenBSD adds `sntrup761` option for IPsec.

Used if client and server configure it.

2022.02: OpenSSH 8.9 enables `sntrup761` on server by default.

Used if client configures it.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

2016.11: Chrome removes `newhope1024` option.

2019.04: OpenSSH 8.0 adds `sntrup761` option.

Used if client and server configure it.

2019.07: Chrome and Cloudflare experiment with `ntruhrss701` and `sikep434`.

2021.05: OpenBSD adds `sntrup761` option for IPsec.

Used if client and server configure it.

2022.02: OpenSSH 8.9 enables `sntrup761` on server by default.

Used if client configures it.

2022.04: OpenSSH 9.0 enables `sntrup761` on client by default.

Timeline of widely used software adding post-quantum options

2016.07: Chrome adds `newhope1024` option.

Used for an experiment with Google servers.

A patent holder then contacts Google and asks for money—oops!

2016.11: Chrome removes `newhope1024` option.

2019.04: OpenSSH 8.0 adds `sntrup761` option.

Used if client and server configure it.

2019.07: Chrome and Cloudflare experiment with `ntruhrss701` and `sikep434`.

2021.05: OpenBSD adds `sntrup761` option for IPsec.

Used if client and server configure it.

2022.02: OpenSSH 8.9 enables `sntrup761` on server by default.

Used if client configures it.

2022.04: OpenSSH 9.0 enables `sntrup761` on client by default.

These encryption layers are *added* to X25519 encryption (ECC).

If lattices are completely broken, still have pre-quantum security.

US government vs. deployment of post-quantum cryptography

- 2021.07** Matthew Scholl, Chief of the Computer Security Division in NIST's Information Technology Laboratory, on videotape: "Don't let folks start to buy and implement unstandard, unknown, potentially unsecured implementations before we as a general community have agreed upon standardization."
- 2021.08** NSA says: "The intention is to update CNSA to remove quantum-vulnerable algorithms and replace them with a subset of the quantum-resistant algorithms selected by NIST . . . NSA is waiting for the NIST process to be completed and for standards to be published. . . . NSS customers are reminded that NSA does not recommend and policy does not allow implementing or using unapproved, non-standard or experimental cryptographic algorithms. The field of quantum-resistant cryptography is no exception."
- 2021.09** DHS says: Do not use "post-quantum cryptographic industry products until standardization, implementation, and testing of replacement products with approved algorithms are completed by NIST."

HYBRID?



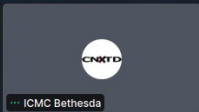
- NSA does not expect to approve post-quantum algorithms with any kind of "but just to be safe, combine with an older algorithm" guidance
- While some argue that deploying a post-quantum algorithm in addition to an existing solution cannot make things less secure, experience shows this to be false
 - CVE 2021-3450 OpenSSL X509_V_FLAG-STRICT
 - Extra check to see if curves were named (relates to NSA discovered Windows CVC 2020-0601)
 - Additional checks shouldn't hurt...but this one overwrote the "The CA isn't valid" result
 - "in cryptographic libraries...system level bugs are a greater security concern than the actual cryptographic procedures" (arXiv 2107.04940)
 - Don't muck with trusted crypto for a temporary fix

Upshot: Don't use temporary hybrids, and invest in implementation robustness before crypto redundancy

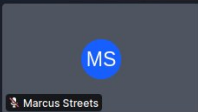
ICMC Bethesda [Screenshare]



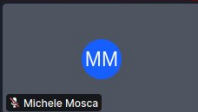
William Layton



ICMC Bethesda



Marcus Streets



Michele Mosca



Urgency of post-quantum recommendations

Screenshot from
8 May 2016

- ▶ All currently used public-key systems on the Internet are broken by quantum computers.
- ▶ Today's encrypted communication can be (and is being!) stored by attackers and can be decrypted later with quantum computer – think of medical records, legal proceedings, and state secrets.
- ▶ Post-quantum secure cryptosystems exist (to the best of our knowledge) but are under-researched – we can recommend secure systems now, but they are big and slow hence the logo of the PQCRYPTO project.
- ▶ PQCRYPTO is an EU project in H2020, running 2015 – 2018.
- ▶ PQCRYPTO is designing a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet.



Standardize now? Standardize later?

Screenshot from
8 May 2016

- ▶ Standardize now!
 - ▶ Rolling out crypto takes long time.
 - ▶ Standards are important for adoption (?)
 - ▶ Need to be up & running when quantum computers come.
- ▶ Standardize later!
 - ▶ Current options are not satisfactory.
 - ▶ Once rolled out, it's hard to change systems.
 - ▶ Please wait for the research results, will be much better!
- ▶ But what about users who rely on long-term secrecy of today's communication?
- ▶ Recommend now, standardize later.
- ▶ Recommend very conservative systems now; users who care will accept performance issues and gladly update to faster/smaller options later.
- ▶ But: standardization takes lots of time, so start standardization processes now.



Initial recommendations of long-term secure post-quantum systems

Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos,
Johannes Buchmann, Wouter Castryck, Orr Dunkelman,
Tim Güneysu, Shay Gueron, Andreas Hülsing,
Tanja Lange, Mohamed Saied Emam Mohamed,
Christian Rechberger, Peter Schwabe, Nicolas Sendrier,
Frederik Vercauteren, Bo-Yin Yang

Issued in 2015 by the PQCRYPTO project.

Initial recommendations

- ▶ **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
 - ▶ AES-256
 - ▶ Salsa20 with a 256-bit key

Evaluating: Serpent-256, ...

- ▶ **Symmetric authentication** Information-theoretic MACs:
 - ▶ GCM using a 96-bit nonce and a 128-bit authenticator
 - ▶ Poly1305

- ▶ **Public-key encryption** McEliece with binary Goppa codes:
 - ▶ length $n = 6960$, dimension $k = 5413$, $t = 119$ errors

Evaluating: QC-MDPC, Stehlé-Steinfeld NTRU, ...

- ▶ **Public-key signatures** Hash-based (minimal assumptions):
 - ▶ XMSS with any of the parameters specified in CFRG draft
 - ▶ SPHINCS-256

Evaluating: HFEv-, ...

Post-Quantum Cryptography: Current state and quantum mitigation



Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing,
Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart.
Evangelos Rekleitis, Angeliki Aktypi, Athanasios-Vasileios Grammatopoulos.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A diagram illustrating a quantum state. A large blue arc is drawn over a background of binary code (0s and 1s). A white arrow points upwards from the center of the arc to the text $\hat{z} = |0\rangle$. Another white arrow points from the bottom right towards the center of the arc, labeled with the quantum state $|\psi\rangle$.

$\hat{z} = |0\rangle$

$|\psi\rangle$

ENISA report: Current state and quantum mitigation (2021)

Chapters

1. Introduction
2. Families of Post-Quantum Algorithms
3. Security Notions and Generic Transforms
4. NIST Round 3 Finalists
5. Alternate Candidates
6. Quantum Mitigation
 - 6.1 Hybrid schemes
 - 6.2 Protective measures for pre-quantum cryptography

Report available from [ENISA's website](#).

US ANSI X9 on post-quantum hybrids

2021: “As we transition from classical cryptography to post-quantum cryptography (PQC), there is a need to understand the proper ways to use both methods simultaneously. PQC methods will not be able to be used as a direct replacement in all cases. And the confidence and broad acceptance of PQC methods will not be as great as classical cryptography.

Simultaneous use of both classical cryptography and PQC methods for both security and acceptance is required during a transition and may be required long term as well. There are improper and insecure ways of implementing a hybrid of classical and PQC methods. Specifying the proper methods of using both are required.” (emphasis added)

French ANSSI on post-quantum hybrids

2022: “Although this new post-quantum toolbox may seem handy for developers, the maturity level of the post-quantum algorithms presented to the NIST process should not be overestimated. Many aspects lack cryptanalytical hindsight or are still research topics, e.g. analysis of the difficulty of the underlying problem in the classical and quantum computation models, dimensioning, integration of schemes in protocols and more importantly the design of secure implementations. This situation will probably last some time after the publication of NIST standards. **Acknowledging the immaturity of PQC is important: ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term.** However, this immaturity should not serve as an argument for postponing the first deployments.” (emphasis added)

What can you do now? Deploy hybrids!

Combine one (or more) pre-quantum schemes with one (or more) post-quantum schemes.

Public-key signatures:

All individual signatures must be valid for the hybrid signature to be valid.

Public-key encryption:

Use multiple systems to jointly generate key for use in symmetric cryptography.

Examples of options to “encrypt the encryption”:

- ▶ Wrap PQC as payload inside pre-quantum (benefit for length fields).
- ▶ Wrap pre-quantum inside PQC (limit the attack surface – quantum attacker cannot even break pre-quantum scheme).

Choice of systems:

- ▶ Different recommendations for rollout in different risk scenarios:
 - ▶ Use most efficient systems with ECC or RSA, to ease usage and gain familiarity. Matches Google and Cloudflare experiments.
 - ▶ Use most conservative systems with ECC or RSA, to ensure that data really remains secure. If you actually have some data you need to protect.
- ▶ Some PQ libraries exist, quality is getting better.

Further information

- ▶ <https://pqcrypto.org> our overview page.
- ▶ PQCrypto 2016, PQCrypto 2017, PQCrypto 2018, PQCrypto 2019, PQCrypto 2020, PQCrypto 2021 with many slides and videos online. PQCrypto 2022 will be online.
- ▶ <https://pqcrypto.eu.org>: PQCRYPTO EU Project.
 - ▶ PQCRYPTO [recommendations](#).
 - ▶ Free software libraries ([libpqcrypto](#), [pqm4](#), [pqhw](#)).
 - ▶ Many reports, scientific articles, (overview) talks.
- ▶ YouTube channel [Tanja Lange: Post-quantum cryptography](#).
- ▶ <https://2017.pqcrypto.org/school>: PQCRYPTO summer school with 21 lectures on video, slides, and exercises.
- ▶ <https://2017.pqcrypto.org/exec> and <https://pqcschool.org/index.html>: Executive school (less math, more perspective).
- ▶ [Quantum Threat Timeline](#) from Global Risk Institute, 2019; [2021 update](#).
- ▶ [Status of quantum computer development](#) (by German BSI).
- ▶ [NIST PQC competition](#).