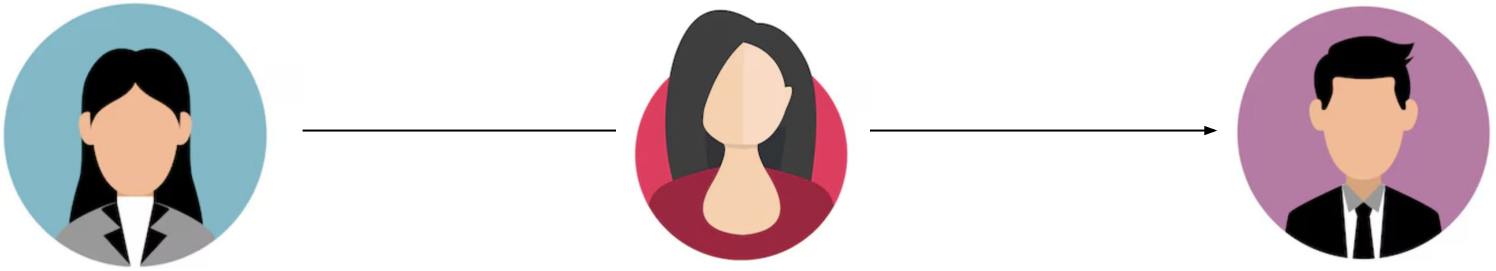
Post Quantum Cryptography

Where We Are and What Lies Ahead

Dr. Ishaani Priyadarshini
School of Electrical Engineering and Computer Science
Washington State University, Everett

VICEROY CySER
Virtual Seminar, October 28, 2025

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

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.

Cryptographic Tools used in TLS (https)

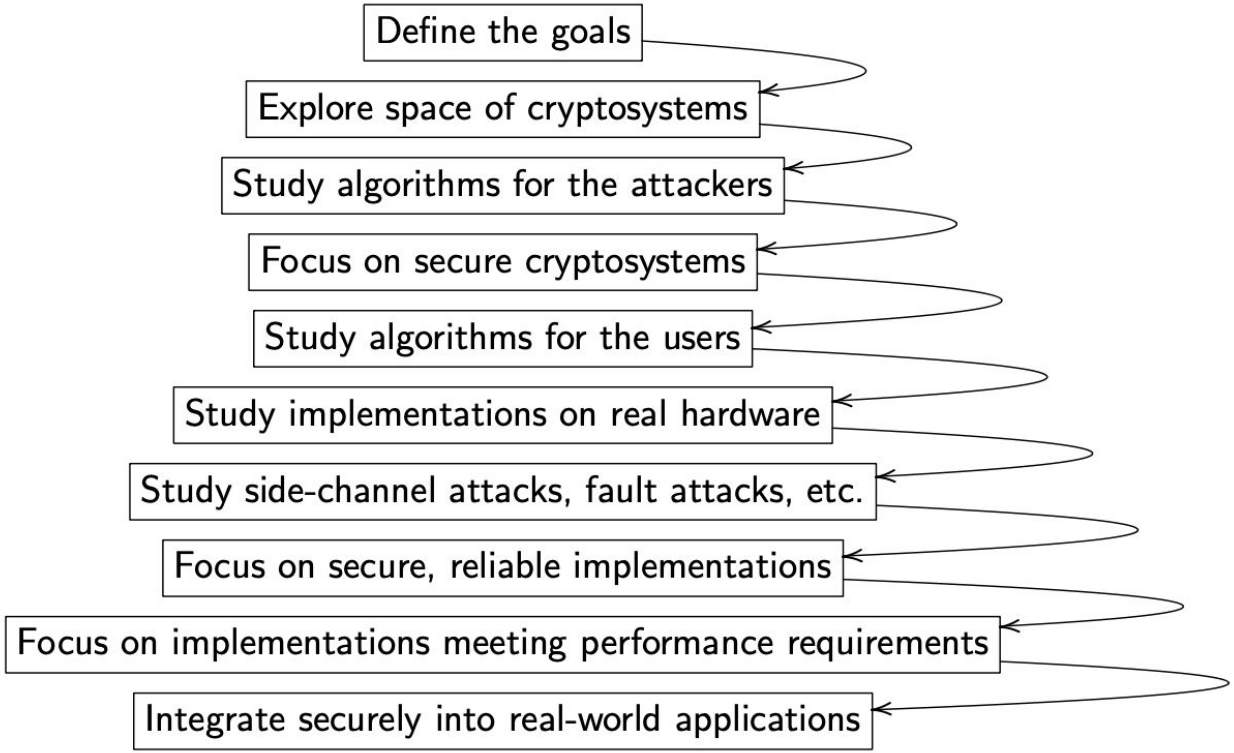
TLS relies critically on public-key cryptography for two reasons

- 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.

Many stages of cryptographic research from design to deployment



Advancements in Quantum Computation

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

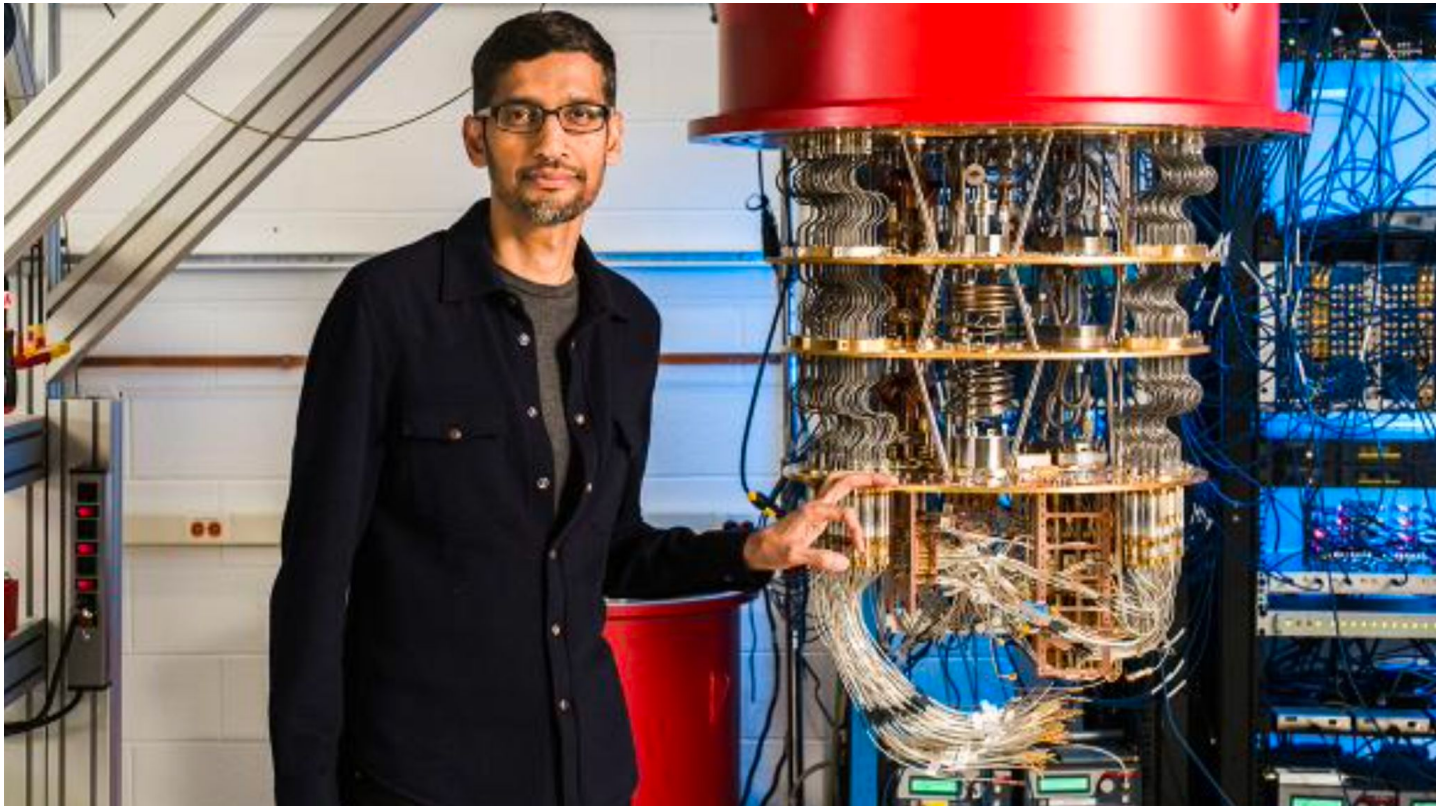
[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give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

Universal quantum computers are coming, and are scary

- Quantum Computing- From theory to cryptographic threat
  - Massive global research effort – rapid progress from theory to prototypes
  - Mark Ketchen, IBM (2012): This isn't 50 years away – maybe 10–15 years.
  - 2022–2027: Universal quantum computers become practical
- Shor's Algorithm – The Cryptographic Breaker
  - Solves key hard problems in polynomial time:
    - Integer factorization → RSA broken
    - Discrete log in finite fields → DSA broken
    - Discrete log on elliptic curves → ECDSA broken
    - All current Internet public-key systems collapse
- Grover's Algorithm – The Partial Threat
  - Speeds up brute-force search (√N improvement)
    - AES-128 ⇒ 2^{64} operations
    - AES-256 ⇒ 2^{128} operations
    - Symmetric encryption survives with larger keys

Advancements in Quantum Computation



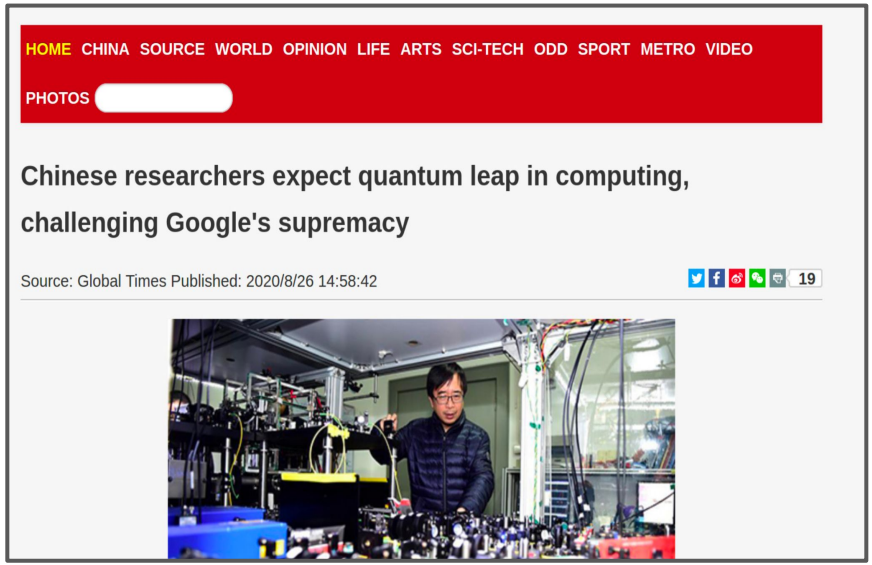
Advancements in Quantum Computation

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.

Advancements in Quantum Computation



A Little Breaking News — Quantum Computing and PQC

Quantum Echoes: Quantum Algorithm 13,000 Times Faster Than Supercomputer

2025-10-27 · From Sebastian Gerstl | Translated by AI · 3 min Reading Time ·

The team at Google Quantum AI has designed an algorithm for quantum computers that, according to a study, significantly outperforms supercomputers for certain tasks for the first time.

NEWS

Lattice Brings Post-Quantum Cryptography to Low-Power FPGAs

October 21, 2025 by Duane Benson

The new low-power FPGAs include CNSA-2.0 compliance and hardware root of trust for post-quantum cryptographic security.

Post-quantum cryptography a.k.a quantum-resistant algorithms: Cryptography designed under the assumption that the attacker (not the user!) has a large quantum computer.

National Academy of Sciences (US)

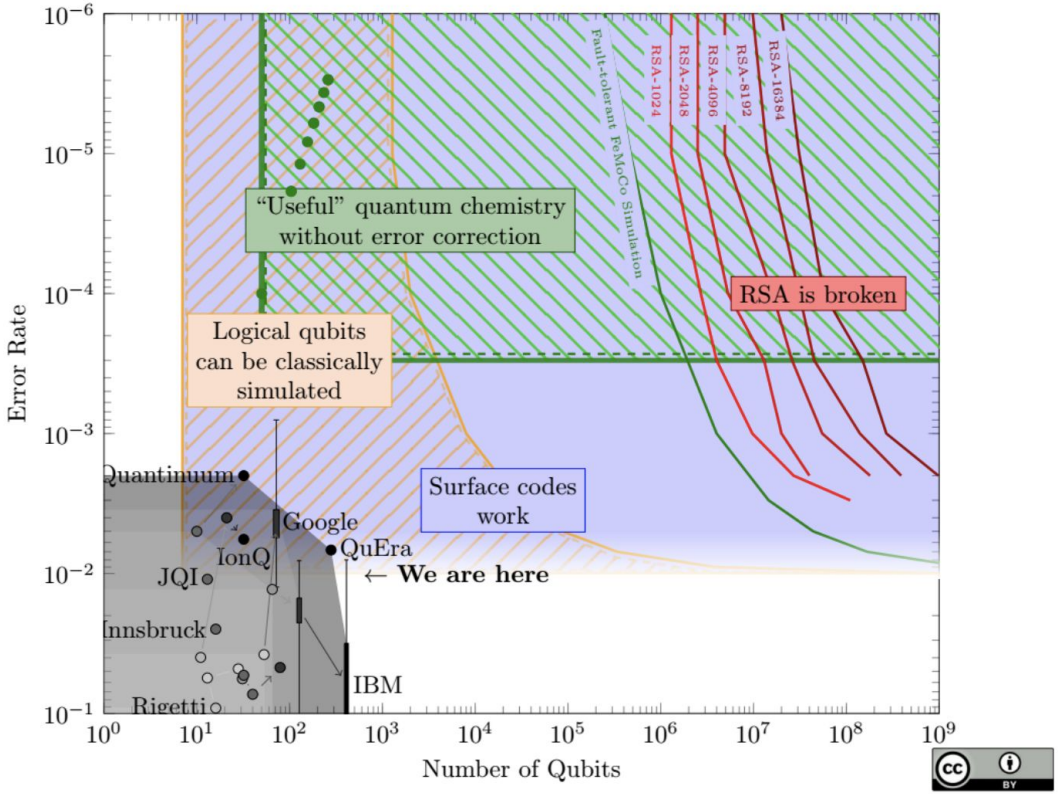
4 December 2018: Report on quantum computing

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."

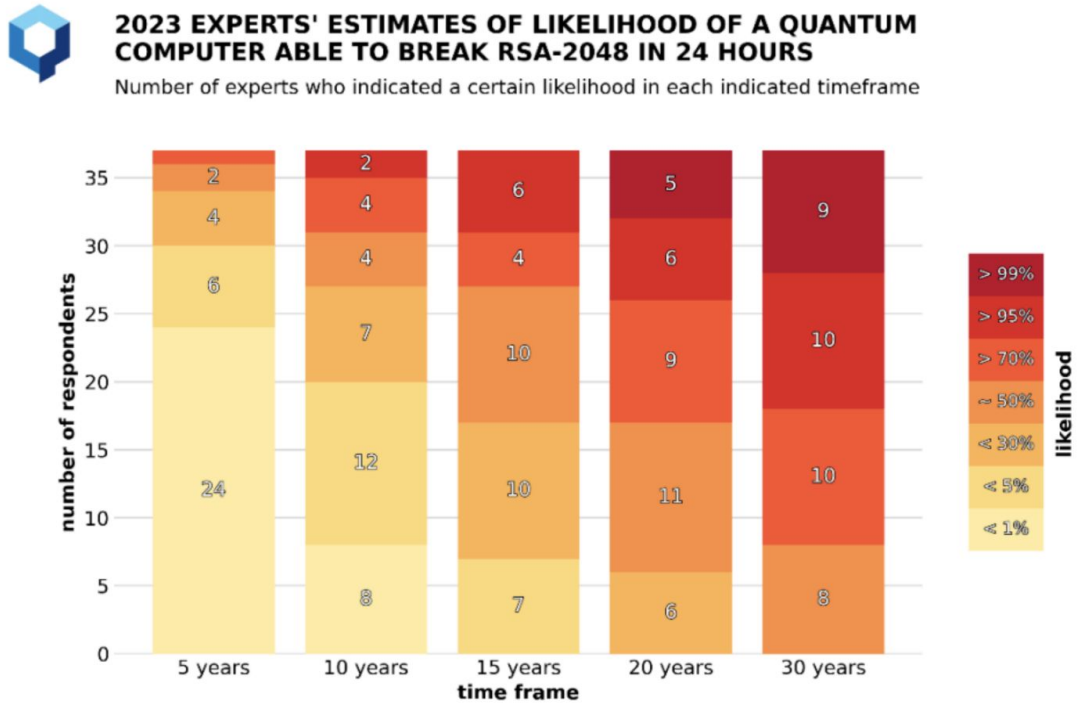
"[Section 4.4:] In particular, all encrypted data that is recorded today and stored for future use, will be cracked once a large-scale quantum computer is developed."

Landscape of Quantum Computing



When will a cryptographically relevant quantum computer be built?

≥ 50% of experts surveyed think there's ≥ 50% chance of a cryptographically relevant quantum computer by 2038.



Post-quantum cryptography

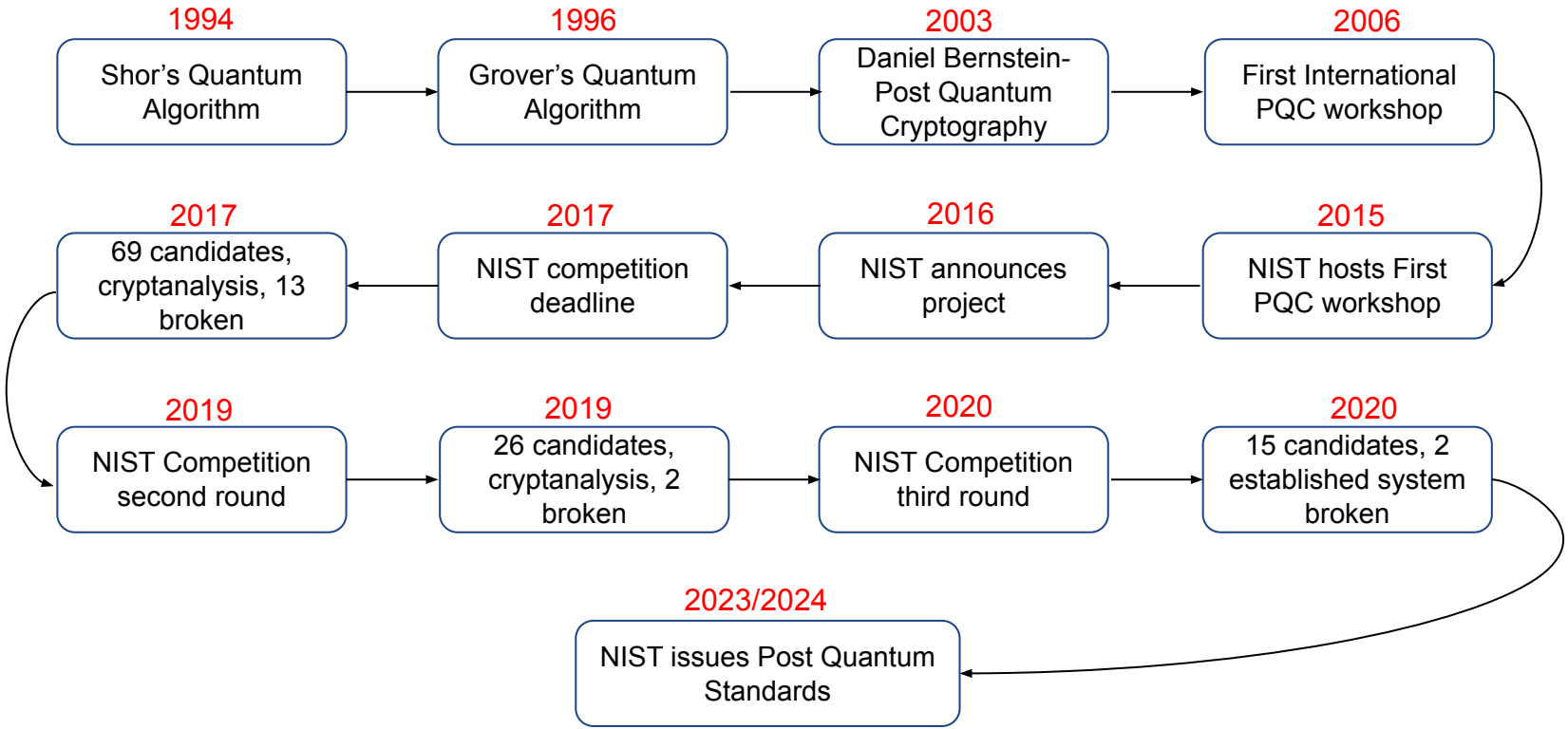
Cryptography under the assumption that the attacker has a quantum computer.

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



NIST 2022 Announcement

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)

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."

Strategic Timing for Post-Quantum Standardization

- 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.

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.”*

French ANSSI on post-quantum hybrids

2022

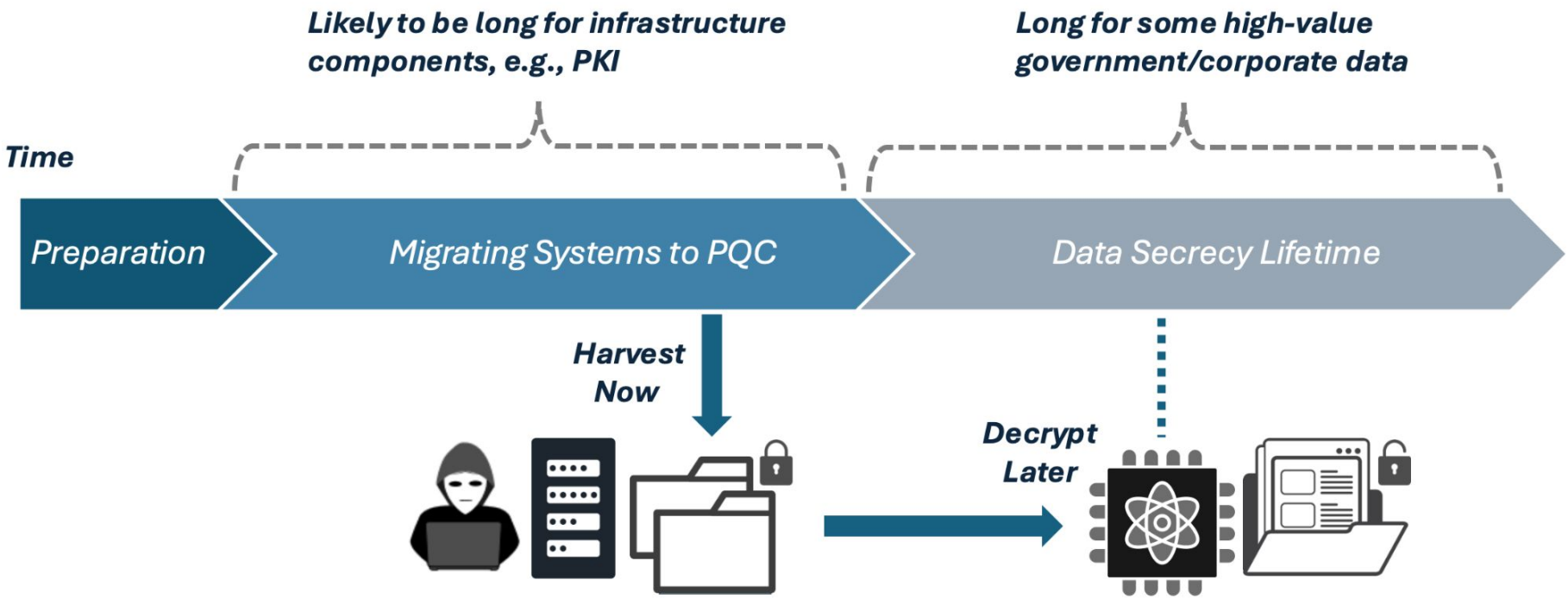
“Although this new post-quantum toolbox may seem handy for developers, the maturity level of the post-quantum algorithms presented to the NIST process should not be overestimated. Many aspects lack cryptanalytical hindsight or are still research topics, e.g. analysis of the difficulty of the underlying 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.”*

Hybrid Approaches to Post-Quantum Migration

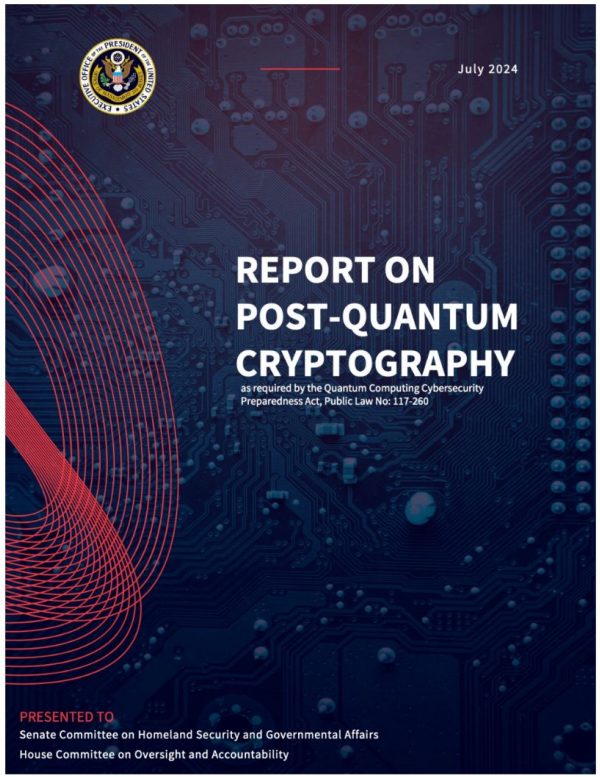
Combine one (or more) pre-quantum schemes with one (or more) post-quantum schemes.

- **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.

Migration Considerations



Migration Considerations



Estimated cost to migrate US government to PQC between 2025–2035:

$7.1 billion

Quantum Vulnerable Algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Organizations may continue using public key algorithms at the 112 bit security level as they migrate to post-quantum cryptography.

Post Quantum Algorithms

Digital Signature Algorithm Family	Parameter Sets	Security Strength	Security Category
ML-DSA [FIPS204]	ML-DSA-44	128 bits	2
	ML-DSA-65	192 bits	3
	ML-DSA-87	256 bits	5
SLH-DSA [FIPS205]	SLH-DSA-SHA2-128[s/f] SLH-DSA-SHAKE-128[s/f]	128 bits	1
	SLH-DSA-SHA2-192[s/f] SLH-DSA-SHAKE-192[s/f]	192 bits	3
	SLH-DSA-SHA2-256[s/f] SLH-DSA-SHAKE-256[s/f]	256 bits	5
LMS, HSS [SP800208]	With SHA-256/192 With SHAKE256/192	192 bits	3
	With SHA-256 With SHAKE256	256 bits	5
XMSS, XMSS^{MT} [SP800208]	With SHA-256/192 With SHAKE256/192	192 bits	3
	With SHA-256 With SHAKE256	256 bits	5

Key Establishment Scheme	Parameter Sets	Security Strength	Security Category
ML-KEM [FIPS203]	ML-KEM-512	128 bits	1
	ML-DSA-768	192 bits	3
	ML-DSA-1024	256 bits	5

The Road Ahead: From Classical Cryptography to Quantum Readiness

- Modern security relies on public-key cryptography — RSA, ECC, and DSA — for confidentiality, integrity, and authentication.
- Shor’s and Grover’s algorithms fundamentally break these assumptions, endangering all Internet-scale encryption.
- NIST launched the Post-Quantum Cryptography initiative (2016); the first lattice- and hash-based standards (ML-DSA, ML-KEM, SLH-DSA, LMS/HSS/XMSS) were finalized in 2022–2024.
- The migration will be gradual, using hybrid deployments that combine classical and post-quantum systems to maintain trust and continuity.
- Migration timelines are long, data lifetimes even longer — meaning the time to begin preparing is now, before “harvest now, decrypt later” becomes a real-world event.

References

- NIST PQC Standardization Project (2022–2024)
- National Academy of Sciences Report on Quantum Computing (2018)
- ANSI X9 and ANSSI PQC Hybrid Recommendations (2021–2022)
- CNSA 2.0 / NSA Post-Quantum Transition Guidance
- Bernstein et al., Post-Quantum Cryptography (Springer, 2009)

Thank You

Advancing security for a quantum future