

Workshop on QKD Systems and
Cybersecurity, 5 Sept 2024

Quantum Computing

- Applications to Cybersecurity
- Quantum Advantage/Supremacy

Quantum Computing Threat Landscape

- Public-key and Symmetric-key Cryptography
- Retrospective Decryption
- Shor's Algorithm
- Grover's Algorithm

PQC as Quantum Computing Threat Mitigation

- Post-Quantum Cryptography
- NIST PQC Standardization Effort
- PQC Transition Recommendations

Cryptographic Agility

- QCs are based on the principles of **quantum mechanics**
 - **Principles:**
 - **Superposition:** a qubit can be in multiple states (0 and 1) simultaneously, allowing QCs to explore a massive number of possible solutions simultaneously, leveraging parallelism to solve complex problems more efficiently
 - **Entanglement:** enables qubits to be interconnected in a way that allows simultaneous processing of large amounts of data, efficient communication of information between qubits, and the implementation of complex algorithms
 - **No-cloning theorem:** prevents the exact copying of an arbitrary unknown quantum state, making eavesdropping harder
 - Use **qubits** (quantum bits) as the smallest unit of information
 - Have their own set of elementary instructions
 - Run **quantum algorithms**
 - An algorithm that can be performed on a QC and takes advantage of the qubit properties
 - Some tasks can be parallelized in ways not possible on classical computers
 - **Parallelization** leads to faster execution

- **QCs have a performance advantage only for selected problems**
 - Solve problems much faster than “classical” computers
 - Solve problems infeasible by “classical” computers
 - Can not speed up all problem solutions
 - ... or the speedup is limited
- **Research question**
 - Find problems that can be solved efficiently with quantum algorithms but not with classical algorithms
- **Quantum-classical hybrid computing**
 - Allows for the efficient use of **quantum resources** for tasks they are best suited for, while utilizing **classical computers** for operations where they excel
 - This approach is practical in the near-term, given the current limitations of quantum hardware
- **Applications**
 - Cryptography, quantum machine learning, drug development, financial modelling, traffic optimization, AI, forecasting

Quantum computers find **applications to cyber security**

- Easily solve math problems, Public Key algorithms (currently used) base their security on
 - Integer factorization
 - Calculating discrete logarithms
- Attack protocols like TLS, VPNs, ...
 - Used for secure browsing, online banking, online shopping, etc.
- Speed up classical cryptographic attacks

Cryptographically Relevant Quantum Computer (**CRQC**)

- A quantum computer of **sufficient size, power and sophistication**
 - Number of qubits, qubit coherence time, gate fidelity, overall error rates, ability to run complex algorithms
- Able to undermine the widely deployed public key-based systems
- **Not a threat to Public Key Cryptography used in real-world systems**
 - A CRQC that could break RSA is **still only theoretical**

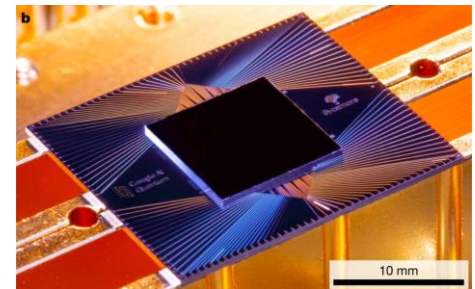
- **Quantum computers exist today**
 - They started small, laboratory-scale and now getting bigger
 - Metrics: qubit count (00s qubits), coherence times (00s msec), and error rates (e.g., 0.1%)
- **Quantum simulators and cloud-based quantum computing platforms (quantum-as-a-service)**
 - Make quantum computing accessible for experimentation, development, and research
 - Develop an understanding, libraries & toolboxes, investigate algorithms & use cases
 - IBM Q Experience, Microsoft Azure Quantum, Google Quantum AI, Amazon Bracket, ...
- **It is impossible to make long term predictions**
 - When (proponents) or even if (skeptics) a **CRQC** will exist
- **The possibility of CRQCs + prudent risk management → proactive action**
 - Uncertain timeline but inevitable threat
 - Long lead time for cryptographic transitions
 - R & D, education and awareness

➤ **Quantum advantage/supremacy**

- A.k.a. “quantum apocalypse/doomsday”
- A demonstration of a QC solving a problem beyond the capabilities of SotA classical computers
 - In any feasible amount of time
 - Irrespective of the usefulness of the problem

➤ **Google’s quantum roadmap**

- 2019: Claimed to have reached quantum supremacy
 - Sycamore processor, 53 qubits
 - 200 sec v. 10K SotA supercomputer years
 - The claim was disputed, still an important proof of PoC
- 2023: Published another result
 - Sycamore processor, 70 qubits
 - 6 seconds v. 47 supercomputer years
- 2025+: Target is 1000 physical qubits ([educational animation](#))



Quantum Computers

➤ IBM's quantum roadmap (as of 2023)

➤ <https://www.ibm.com/quantum>

Development Roadmap

IBM Quantum

	2016–2019 ✓	2020 ✓	2021 ✓	2022 ✓	2023 ✓	2024	2025	2026	2027	2028	2029	2033+
	Run quantum circuits on the IBM Quantum Platform	Release multi-dimensional roadmap publicly with initial aim focused on scaling	Enhancing quantum execution speed by 100x with Qiskit Runtime	Bring dynamic circuits to unlock more computations	Enhancing quantum execution speed by 5x with quantum serverless and Execution modes	Improving quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhancing quantum execution speed and parallelization with partitioning and quantum modularity	Improving quantum circuit quality to allow 7.5K gates	Improving quantum circuit quality to allow 10K gates	Improving quantum circuit quality to allow 15K gates	Improving quantum circuit quality to allow 100M gates	Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing
Data Scientist						Platform						
						Code assistant	Functions	Mapping Collection	Specific Libraries			General purpose QC libraries
Researchers						Middleware						
						Quantum Serverless	Transpiler Service	Resource Management	Circuit Knitting x P	Intelligent Orchestration		Circuit libraries
Quantum Physicist												
	IBM Quantum Experience		QASM3	Dynamic circuits	Execution Modes	Heron (5K)	Flamingo (5K)	Flamingo (7.5K)	Flamingo (10K)	Flamingo (15K)	Starling (100M)	Blue Jay (1B)
	Early	Falcon		Eagle		Error Mitigation	Error Mitigation	Error Mitigation	Error Mitigation	Error Mitigation	Error correction	Error correction
	Canary 5 qubits	Albatross 16 qubits	Penguin 20 qubits	Prototype 53 qubits	Benchmarking 27 qubits	5k gates 133 qubits	5k gates 156 qubits	7.5k gates 156 qubits	10k gates 156 qubits	15k gates 156 qubits	100M gates 200 qubits	1B gates 2000 qubits
						Classical modular 133x3 = 399 qubits	Quantum modular 156x7 = 1092 qubits	Quantum modular 156x7 = 1092 qubits	Quantum modular 156x7 = 1092 qubits	Quantum modular 156x7 = 1092 qubits	Error corrected modularity	Error corrected modularity

➤ EU Flagship Programme “Quantum Technologies”

- 2018 – 2028, EU quantum computer, quantum communications, etc.
- New Strategic Research Agenda on Quantum technologies
 - <https://digital-strategy.ec.europa.eu/en/news/new-strategic-research-agenda-quantum-technologies>
 - <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- Quantum Technologies Flagship
 - A long-term research and innovation initiative
 - Aims to put Europe at the forefront of the quantum revolution
 - Mid-term report (2020)
 - Educational material
- OpenSuperQPlus (2023 – 2026 – 2030)
 - Goal: “ ... a versatile 1,000-qubit quantum-computing system made in Europe”

Scientific and engineering challenges

➤ Quantum decoherence

- Even without a noisy environment qubits will decay on their own
- Due to decoherence, qubit properties are lost
- For actual quantum computations, decoherence must be managed
- Challenge:
 - Prolong coherence times (how long qubits can retain their state) while performing meaningful computations
 - Maintaining coherence for large numbers of qubits over the time needed for complex algorithms is a major challenge

➤ Qubit reliable store

- Must be isolated from their environment (electromagnetic fields, temperature fluctuations, or even cosmic rays)
 - E.g., polarized photons in optical fiber
- Any interaction affect the qubit state
- Often, extreme cooling (e.g., cryogenic temperatures) is required

➤ Qubit reliable manipulation

- To apply logic (gates), qubit interaction must take place in a controlled way
- Small errors accumulate over time
- Difficulty implementing controls -> quantum error correction

- Physical and engineering problems
- Commercial drivers

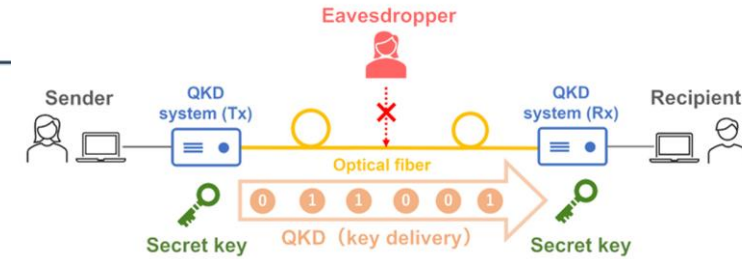
Principal applications

- **Asymmetric key agreement (establishment)**
 - Establish a shared cryptographic key for secure communication
 - In the absence of a pre-established secret
 - Used for message encryption to deter unauthorized access
 - ➔ Confidentiality
- **Digital signatures**
 - Verify the identity of the originator and detect forgery (integrity violation)
 - ➔ Authentication

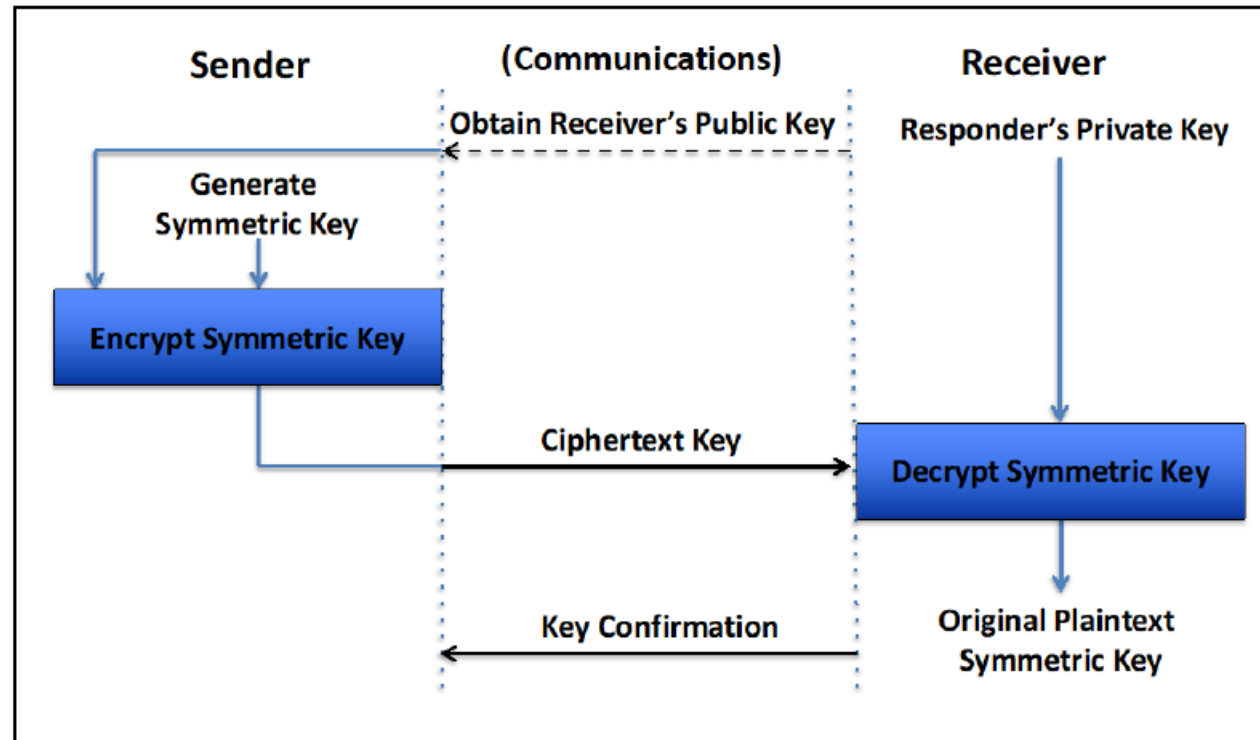
PKC algorithms

- Security is based on difficulty to solve certain **mathematical problems**
- When **properly implemented** and used they cannot be broken
- **Keys of the right size** provide long-term security against **classical computers**

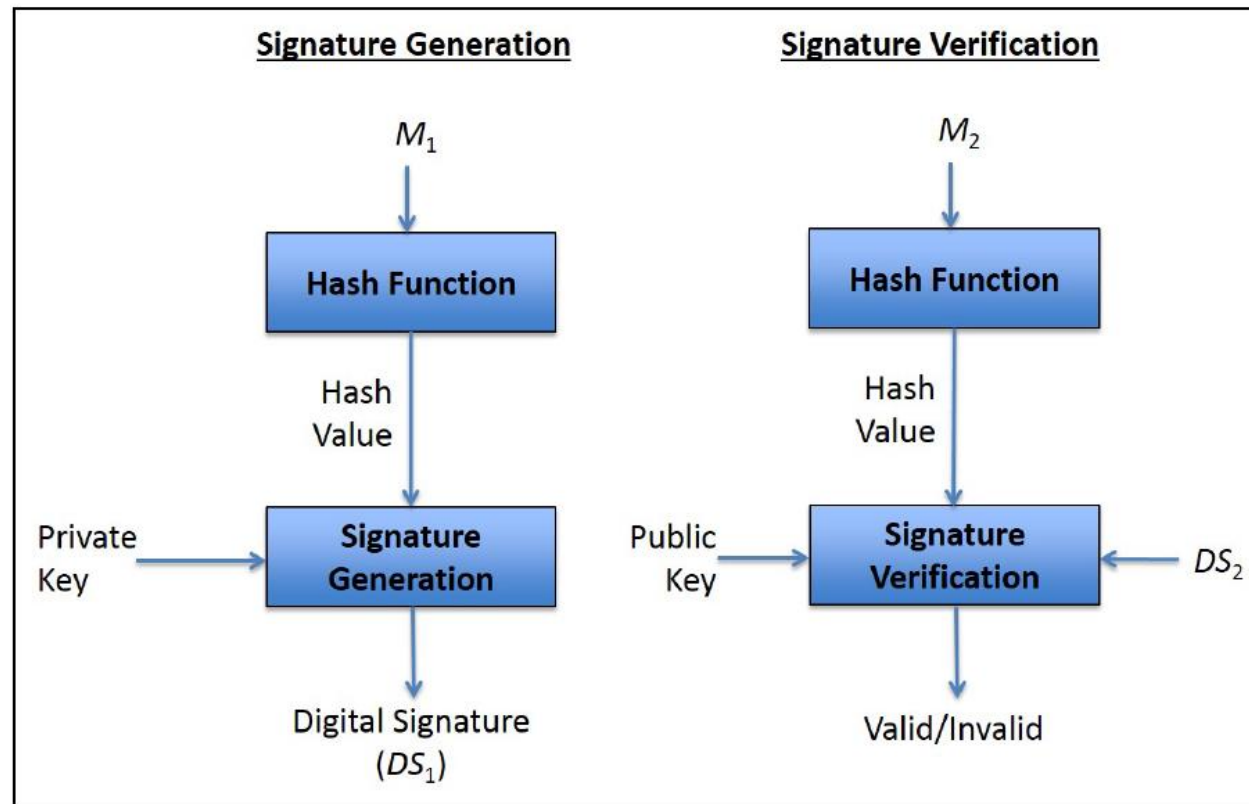
Public Key Cryptography



Key agreement (NIST20)



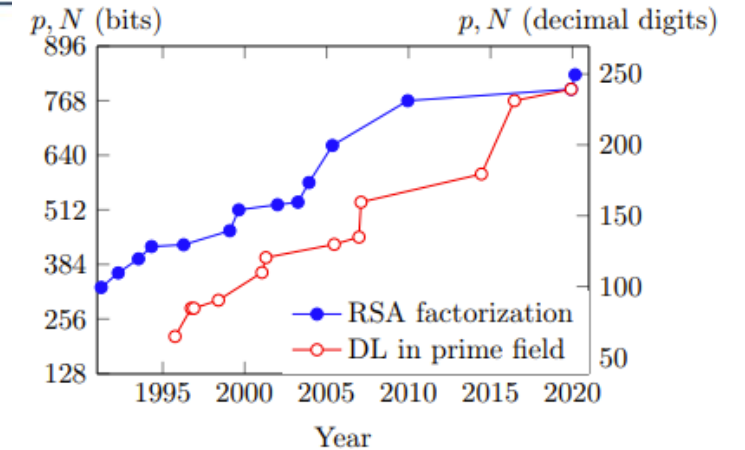
Digital signatures (NIST20)



Public Key Cryptography

RSA Security

- Based on the difficulty of factoring large numbers
- Easy to generate key (prime multiplication)
- Difficult to crack the key (integer factorization)
- RSA factorization records [BOU22]
 - Currently, 829 bits (2020)
 - Much smaller than the RSA keys typically used in practice (2048 bits)
 - Took 2700 years of running powerful computer cores to carry out the computation



A QC can break RSA in “seconds”

- ... as long as the key size is 5 bits ...
- Future versions will be more powerful
- For practical attacks, thousands or even millions of qubits are required
- **QC is not an imminent threat**

Shor's algorithm (1994)

- A **quantum algorithm** for factoring integers
 - One of the **few known quantum algorithms** with a potential **profound impact**
- **Classical computer**: factorization can be performed in **exponential time**
 - The number of steps required to complete the algorithm for a given input **n** is **$O(k^n)$**
 - **n** is placed in the exponent
 - This inefficient algorithm will grow significantly faster than any polynomial function
- **Quantum computer**: factorization can be performed in **polynomial time**
 - The number of steps required to complete the algorithm for a given input **n** is **$O(n^k)$**
 - **n** is placed in the base
- How to factor **2048-bit RSA** integers in **8 hours** using **20 million noisy qubits**, 2021 [GE21]
 - "... in the four years since **2015**, the upper end of the estimate of how many qubits will be needed to factor 2048-bit RSA integers has dropped nearly two orders of magnitude; from a **billion** to twenty million"

Threat to confidentiality

➤ Retrospective decryption

- A.k.a. “harvest now, decrypt later”, and “store now, decrypt later”
- Some data need to be kept secure for long periods (e.g., decades)
 - National security documents, diplomatic communications, ...
- **Adversaries collect encrypted data** hoping to decrypt it in the future
 - Secure key agreement + encrypted data
 - Persistent adversaries (nation state actors?) focus on high-value targets
 - E.g., sensitive data, classified information
 - Impossible to collect everything due to the volumes and costs involved
- **Law enforcement also benefit**
 - Solve cold cases based on breakthroughs in digital forensics
- **Other than CRQC possible breakthroughs:** mathematical, algorithmic or hardware

Symmetric Key Cryptography

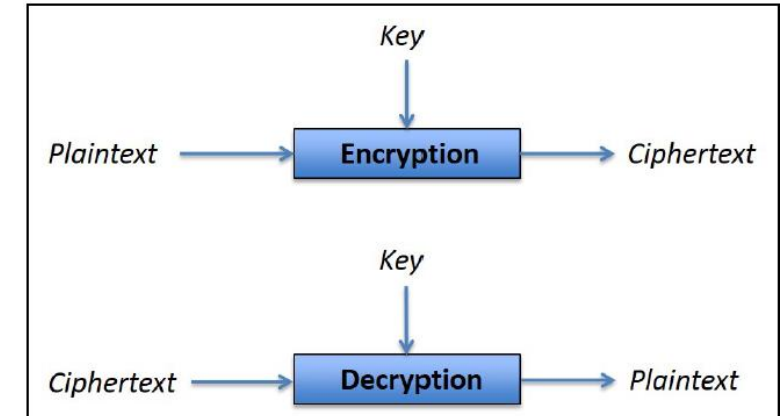
■ Principal applications

➤ Encryption

➤ Bulk encryption

➔ Confidentiality

➤ Construction of other cryptographic primitives



Symmetric algorithms

- Ideally, **security is based on the secrecy and length of the shared key**
- **Keys of the right size** provide long-term security against **classical computers**

Grover's algorithm (1996)

- A quantum algorithm for unstructured search (unsorted database, “digital haystack”)
 - Example application: **Search of the key space in symmetric algorithms**
- Provides only a **moderate quadratic speedup** compared to a search on a classical computer
 - Time for a classical computer to search through a list of size n is proportional to n , complexity is $O(n)$
 - Assume a classical computer needs time T (steps = 1.000.000) to complete a task
 - Time for a QC to search through a list of size n is proportional to \sqrt{n} , complexity is $O(n^{1/2})$
 - A QC solves the same problem in time $T^{1/2}$ (e.g., steps = 1000)
- Can brute-force a 128-bit symmetric key in roughly 2^{64} iterations instead of 2^{128} operations
- Can brute force a 256-bit key in 2^{128} iterations instead of 2^{256} iterations
- The **implementation** of the algorithm on a QC is not straight forward

A CRQC is **not a major threat** for SKC

- Much less severe than the impact of Shor's algorithm on PKC
- SKC algorithms are believed to be secure, provided a sufficiently large key size is used
- **AES-128 / AES-256**
 - Has a security level of **128 / 256** bits against a **classical computer**
 - Has a security level of **64 / 128** bits against a **quantum computer**
 - Security level n means that the best attacks use approximately 2^n operations
- **Doubling the size of the key** is sufficient to maintain an equivalent **security level**
- **Known post-quantum attacks impact [BL17]** →
 - PK algorithms require changes in the fundamental design

Algorithm	Function	Pre-quantum security level	Post-quantum security level
Public key cryptography			
RSA-3072	encryption	128	broken (Shor)
RSA-3072	signature	128	broken (Shor)
DH-3072	key exchange	128	broken (Shor)
DSA 3072	signature	128	broken (Shor)
ECDH 256	key exchange	128	broken (Shor)
ECDSA 256	signature	128	broken (Shor)
Symmetric cryptography			
AES-128	block cipher	128	64 (Grover)
AES-256	block cipher	256	128 (Grover)

CRQC Threat Mitigation

Mitigation measures must be put in place to counter the CRQC threat

- Cryptographic systems have a **long lifecycle**
- Conversion is
 - Slow - new cryptography may take **10-20 years to fully deploy**
 - **A complex and expensive** process

To protect the C-I-A properties of sensitive information

- Set the **cryptographic requirements** early and factor them into **future system designs**
- **Plan** for an eventual **transition** with an **initial focus on hybrid system**

Without effective mitigation, the **threat is unacceptable**

Post-quantum cryptography

- A.k.a. quantum-resistant, quantum-safe cryptography
- PQC algorithms run on
 - **conventional encryption/decryption devices**
 - over conventional communication channels
- **No CRQC is required** to run them
- **Easier to integrate into existing systems**
 - Can be deployed on existing infrastructures (**unlike QKD**)
 - Can interoperate with **existing communications protocols** and **networks**
- **NIST's PQC standardization project**
 - NIST is leading the effort to standardize quantum-resistant algorithms
 - These algorithms are focused on **key exchange** and **digital signatures**, which are the most vulnerable to quantum attacks

PQC algorithms

- Designed with the quantum threat in mind (an adversary with a CRQC)
- Based on current knowledge
 - They are **resistant to attacks from both classical & quantum computers**
 - “... all envisioned and understood quantum computing capabilities”
 - Some algorithms base their security on mathematical constructs than have been studied for longer compared to the rest of the algorithms
 - However, in general, **cryptanalytic efforts are in their early stages**
- **New algorithms will benefit the current ecosystem** of solutions
 - They will **provide alternatives** even for classical computing (and attacks)

Evaluation Criteria

➤ Security

- Resistance to known **attacks** (both classical and quantum)
- Security **proofs** (link to a well-understood hard mathematical problem)
- **Long-term** security (see quantum roadmaps)
- **Side-channel** resistance (e.g., power consumption or timing attacks)

➤ Cost and performance (also for constraint environments)

- **Speed** (key gen, en/de-cryption, signing/verification good enough for practical use in different envs)
- **Memory** and **bandwidth** requirements (size of keys and signatures)
- Computational **efficiency** (CPU cycles, memory, etc. they consume)
- Algorithmic **complexity** (ease of implementation and scaling)

➤ Algorithm and implementation characteristics

- Adaptability to multiple **use cases**
- **Hybridization** capabilities
- Algorithm **maturity** (have withstood cryptanalytic scrutiny for longer)
- Adjustable **parameters** (e.g., key sizes / levels of security to provide different performance trade-offs)

Security strength levels

- Different applications, systems, and environments have varying security needs
- A "one-size-fits-all" approach isn't practical
- Different security levels can ensure that PQC algorithms are applicable across a wide range of use cases
 - From lightweight IoT devices to critical infrastructure
- Help understand how quantum-safe algorithms **compare to classical algorithms**
- **Higher levels require more resources**, and time would be required to attack the system
 - Larger key sizes, longer execution times, and more memory
- **Example: Security Level 1**
 - **Comparable** to breaking the **AES-128** encryption standard using **classical brute-force attacks**
 - Currently considered secure against classical computers but **vulnerable to QC**
 - Suitable for lightweight applications or low-risk environments, such as IoT devices or non-critical systems
 - Performance and efficiency are prioritized

Level	Strength	Example
1	Key search a 128-bit key	e.g., AES-128
2	Collision search a 256-bit hash	e.g., SHA-256
3	Key search a 192-bit key	e.g., AES-192
4	Collision search a 384-bit hash	e.g., SHA-384
5	Key search a 256-bit key	e.g., AES-256

NIST PQC Standardization Effort

Roadmap

Algorithm	Class of Math Problem
CRYSTALS-Kyber	Lattice-based
CRYSTALS-Dilithium	Lattice-based
FALCON	Lattice-based
SPHINCS+	Hash-based
BIKE	Code-based
HQC	Code-based
SIKE	Isogeny-based
Classic McEliece	Code-based

Start (Dec-16)	Due Date	Submissions	Next Round Candidates	Alternate Candidates "second track"	Key Encapsulation Mechanisms	Digital Signatures
1st round	Nov-17	82 (59 + 23)	69		49	20
2nd round	Apr-19		26		17	9
3rd round	Oct-20		7	8 (5 + 3)	4	3
Standardization step	Jul-22				1. CRYSTALS-Kyber	1. CRYSTALS-Dilithium 2. FALCON 3. SPHINCS+
New call for dig sigs	Jun-23					40
4th round (start 7/22) (for alt candidates)	ongoing				1. BIKE 2. Classic McEliece 3. HQC 4. SIKE	
Final version of standards	Aug-24				1. FIPS 203: ML-KEM	1. FIPS 204: ML-DSA 2. FIPS 206: Late 2024? 3. FIPS 205: SLH-DSA

➤ NIST PQC standardization

- NIST issued a new call for **digital signature algorithms** to diversify its portfolio, especially **seeking algorithms not based on structured lattices**
- NIST is expected to provide:
 - Additional **guidance on migrating** to these PQC standards and integrating them into existing system
 - Additional **guidance on hybrid cryptographic schemes** (combining quantum-resistant and classical algorithms)
- **SIKE**
 - Once considered a strong candidate, was broken in July 2022
 - Some researchers believe that restoring security might be possible
 - However, confidence in isogeny-based cryptography has significantly diminished after this breach

Algorithm	Class of Math Problem
CRYSTALS-Kyber	Lattice-based
CRYSTALS-Dilithium	Lattice-based
FALCON	Lattice-based
SPHINCS+	Hash-based
BIKE	Code-based
HQC	Code-based
SIKE	Isogeny-based
Classic McEliece	Code-based

- **Multiple algorithms will eventually be standardized**
 - Proposed algorithms differ considerably in their **performance characteristics**
 - Key size
 - Signature or ciphertext size
 - Computational complexity
 - Security assurance
 - **Not all cryptographic algorithms are suited to every environment/application**
 - Some algorithms will be more suited to particular use-cases than others (e.g., constraint devices)
 - Such mappings will become more evident towards the end of the standardization effort
 - Chosen algorithms are **based on different math problems**
 - **Mitigate the risk** of potential vulnerabilities being found in one class of mathematical problems
 - **Avoiding a single point of failure** (RSA and ECC as historical precedent)
 - Encourage innovation and continued research
 - Allows cryptanalysts to focus on a broad range of mathematical challenges

- **Public-key systems require**
 - **Key-pair generation** algorithm
 - **Signature** schemes: Algorithms for signature generation/verification
 - Only sign a hash of the message
 - **Encryption** schemes: Algorithms for encryption/decryption
 - Only establish a **shared secret** (to later be used by symmetric key algorithms)
- **PQC algorithms**
 - Only good for either signatures or encryption (key encapsulation)
 - Due to the nature of the underlying mathematical problems and the need for optimization in performance and security
 - In contrast, RSA is dual purpose (can be used for both encryption and signatures)
 - Best practice dictates to **use different key pairs** for each operation
 - In PQC, different algorithms and keys should be used for each operation
- **Key sharing mechanisms**
 - **KEX (key exchange)**: typically has one party generating and securely transmitting the key
 - **KEM (key encapsulation)**: a key is generated, encapsulated (encrypted) into a ciphertext and sent to the recipient
 - **Key agreement**: typically involves both parties in the key generation process
- **Quantum-resistant digital certificates** will certify public keys and mitigate MiTM attacks

➤ Standardization

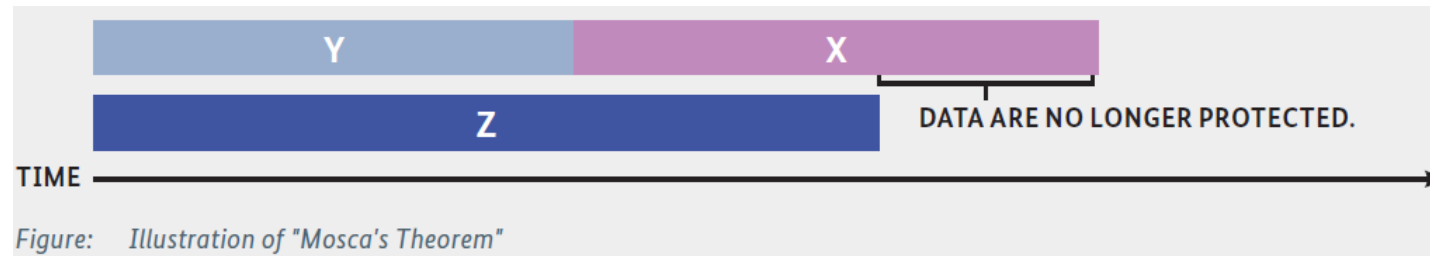
- Several standards organizations, expert groups and NCSAs have made **recommendations** and released reports
- There is **no European standardization process**
- Most western countries and agencies are likely to align with NIST's PQC guidelines

- **BSI** welcomes the NIST process
 - It recommended two schemes in its technical guideline TR-02102-1 (2020)
 - FrodoKEM (lattice-based) and Classic McEliece (code-based) – in hybrid solutions
 - Both **conservative from a security point of view (can serve as a backup)**
 - NIST has already excluded FrodoKEM due to its poor performance (not its security)

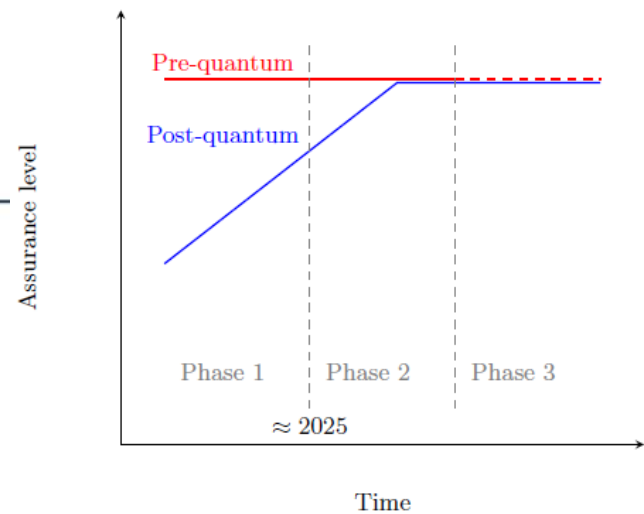
- BSI argues against a proliferation of standards
 - Interoperability
 - Commercial interests
 - Research effort

- **Process (high-level)**
 - Technical **standards** become available
 - Major **products** and **services** adopt the standards
 - States put **regulatory pressure** to organizations to adopt legislation/guidelines
 - Government agencies, critical infrastructure operators, commercial services providers
- **Organizations should**
 - Factor the quantum threat into their **cybersecurity strategy**
 - Identify **priority systems** (create an inventory)
 - Include the transition steps into a **roadmap**
 - Communicate concerns with **national cybersecurity authorities**
 - Consult **transition guidance** produced by **ENISA, NIST, ETSI, NCSAs**, etc.
 - **Alert vendors**
 - **Educate the workforce**
- **Adoption of non-standardized PQC is not recommended**
 - Potential interoperability and compliance issues, added costs and business disruption

Transition: BSI22



- **X**: #years that the data to be protected must remain secured
- **Y**: #years needed to convert the system to Quantum Safe Cryptography
- **Z**: #years it will take for CRQCs to exist
- **X + Y** must be less than **Z**
- **Risk assessment**: "For national security systems, BSI works under the hypothesis that CRQCs will be available in the early 2030s" [BSI22]



➤ Transition: ANSSI roadmap (ANSSI22)

➤ Phase 1 (today)

- **Mandatory** pre-quantum security
- **Optional** PQC (**hybrid** solutions), defense in depth
- No claimed quantum resistance

➤ Phase 2 (not earlier than 2025)

- **Mandatory** pre-quantum security
- **Optional** PQC (**hybrid** solutions), not just a defense in depth measure
- With **claimed quantum resistance**

➤ Phase 3 (probably not earlier than 2030)

- **Optional standalone** post-quantum cryptography with **claimed quantum resistance**
- It is expected that the security assurance level provided by PQ algorithms will be as high as today's pre-quantum assurance level

- Recommendations will adapt to the progress of the processes under way

Other guidelines

➤ NIST

- [Migration to Post-Quantum Cryptography](#)
- Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography (Dec 2023)
 - [NIST SP 1800-38 \(Initial Preliminary Draft\)](#)

➤ ENISA

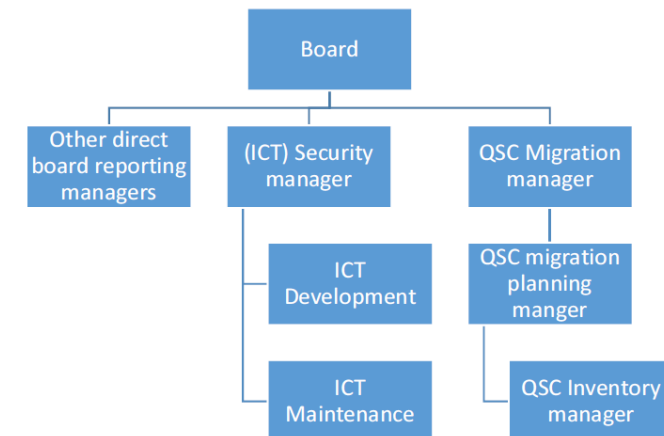
- [Post-Quantum Cryptography: Current state and quantum mitigation \(2021\)](#)
- [Post-Quantum Cryptography - Integration study \(2022\)](#)

➤ European Commission

- [Recommendation on Post-Quantum Cryptography](#)

➤ ETSI (European Telecommunications Standards Institute)

- [Quantum-Safe Cryptography \(QSC\) working group](#)
- Migration strategies and recommendations to Quantum Safe schemes
 - [Technical report TR 103 619, August 2020](#)



Cryptographic primitives are ubiquitous

- Embedded in almost all digital applications and protocols
- Products must be designed with **crypto agility** as a **design requirement**
 - Possibly excluding very short-lived products

Many **crypto primitives** have proven **vulnerable** in the past

- Crypto **attacks** to algorithms
- **Obsolesce of key sizes**

Examples

- RC4 (WEP)
- DES-56 → 3DES-168 → AES-128/192/256 → AES-256 (QCs)
- RSA-512 → RSA-1024 → RSA-2048
- MD5-128 → SHA1-160 → SHA2 → SHA3 (256 – 512)

Crypto-agility is an emergent system property

- The **ability to replace crypto primitives “smoothly”** to respond to newly exposed vulnerabilities
 - No product recall or substitution
- Related to maintainability, **resilience** and survivability
- **Not easy to enforce**
 - Due, for example, to backward compatibility issues

Crypto-agility assumes a comprehensive **cryptography inventory**

- A **record of all cryptography** used in the organization and its context
- A detailed **risk assessment** of all the items in the inventory
- Lessons learned from **high profile cryptographic failures**

Cryptography inventory

- Cryptography-based applications, data processed and purpose
- Infrastructure supporting cryptography

- It includes details about
 - Products and services using cryptography
 - Algorithms and usage modes
 - Keys and key storage arrangements
 - Digital certificates and PKI arrangements
 - Protocols and versions
 - Software libraries versions
 - Roles and responsibilities
 - Data classification/lifespan v. business functions/priorities and risks

- ANSSI views on the Post-Quantum Cryptography transition, Mar. 2022 ([link](#))
- Bernstein and Lange, Post-quantum cryptography – dealing with the fallout of physics success, 2017 ([link](#))
- Boudot et al., The state of the art in integer factoring and breaking public key cryptography, 2022 ([link](#))
- BSI, Quantum-safe cryptography – fundamentals, current developments and recommendations, May 2022 ([link](#))
- ENISA, Post-Quantum Cryptography: Current state and quantum mitigation, May 2021 ([link](#))
- ENISA, Post-Quantum Cryptography - Integration study, Oct. 2022 ([link](#))
- ETSI TR 103 619 V1.1.1, Migration strategies and recommendations to Quantum Safe schemes, Jul. 2020 ([link](#))
- Europol, First Report of the Observatory Function on Encryption, Jan. 2019 ([link](#))
- Europol, Second Report of the Observatory Function on Encryption, Feb. 2020 ([link](#))
- Europol, Third Report of the Observatory Function on Encryption, Jun. 2020 ([link](#))
- Gidney and Ekerä, How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits, 2021 ([link](#))
- NIST SP800-175Br1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms ([link](#))
- NIST IR 8413-upd1, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, Jul. 2022 ([link](#))
- UK NCSC, Preparing for Quantum-Safe Cryptography, Nov. 2020 ([link](#))



HellasQCI - Quantum Communication Infrastructure for Greece



Co-funded by
the European Union

This project is co-funded by the European Union
under the Digital Europe Programme grant agreement No. 101091504.

