UNIVERSITATEA LUCIAN BLAGA DIN SIBIU
HPI Hasso Plattner Institut
CLUJ IT
Sibiu IT Cluster
SID 2025
Sibiu Innovation Days
06-07 November, Sibiu - RO
EMERGING DISRUPTIVE TECHNOLOGIES:
Balancing Innovation, Risks, and Societal Impact

A study on cryptographic algorithms adapted for the quantum computing era

Introduction, Key Algorithms, and Cybersecurity Implications

Introduction – Quantum Computing and Cybersecurity

- Quantum computers use superposition and entanglement for computation.
  - Superposition → a quantum system can explore many possibilities at once.
  - Entanglement → qubits influence each other instantly, allowing correlations classical bits cannot achieve.
- **Shor's algorithm with a performant quantum computer can break RSA and ECC.**
- **Major threat to security of communications, finance, internet, military and sensitive data.**

What is Shor's algorithm ?

- Shor's algorithm is a quantum algorithm developed by Peter Shor in 1994.
- It is famous because it can efficiently solve two problems that classical computers cannot:

1. Integer Factorization

- Breaking down a large number NNN into its prime factors.
- Example: finding that 187 = 11 × 17.
- For large numbers (2048-bit RSA keys), classical computers would take billions of years.
- Shor's algorithm can do it in polynomial time on a sufficiently large quantum computer.

2. Discrete Logarithm Problem (DLP)

- The core math behind Elliptic Curve Cryptography (ECC).
- Shor's algorithm can compute discrete logarithms exponentially faster than classical methods.
- Shor's algorithm is the reason why current public-key cryptography (RSA, ECC, DSA) will be completely broken by quantum computers once they reach a large enough scale.

Cryptographic Algorithms Used Today in Industry - Asymmetric

- Asymmetric cryptography is based on a pair of keys: a **public key**, shared with anyone, and a **private key**, kept secret. Data encrypted with one key can only be decrypted with the other.
- **Public-Key Cryptography (Asymmetric).**
  - **RSA**
    - Widely used for encryption, digital signatures, and SSL/TLS certificates.
    - Security relies on the hardness of integer factorization.
    - Vulnerable to Shor's algorithm → easily broken by a large quantum computer. → Factor RSA-2048 in hours or minutes.
  - **Elliptic Curve Cryptography (ECC)**
    - Includes algorithms like ECDSA, ECDH.
    - Common in mobile devices, TLS, blockchain (e.g., Bitcoin, Ethereum).
    - Security relies on Elliptic Curve Discrete Logarithm Problem (ECDLP).
    - Vulnerable to Shor's algorithm → completely breakable with quantum power.

Cryptographic Algorithms Used Today in Industry - Symmetric

- **Symmetric cryptography** uses the **same secret key** for both encryption and decryption. It is generally faster and more efficient than asymmetric cryptography, but it requires a secure method to share the secret key between parties.
  - **AES (Advanced Encryption Standard)**
    - Industry standard for data encryption (128/192/256-bit keys).
    - Quantum attacks (Grover's algorithm) reduce effective security:
      - AES-128 → equivalent to 64-bit security.
      - AES-256 → equivalent to 128-bit security (still considered secure).
  - **SHA-2 / SHA-3 (Hash Functions)**
    - Used for integrity, digital signatures, blockchain mining.
    - Quantum attacks reduce security (Grover's algorithm):
    - Collision resistance halved.
    - Still secure if larger output sizes are used (e.g., SHA-256 → upgrade to SHA-512 for safety).

What Is Post-Quantum Cryptography (PQC)?

- Designed to resist classical and quantum computer attacks.
- Replaces vulnerable algorithms (RSA, ECC) with quantum-safe alternatives.
- Post-Quantum Cryptography is standardized by NIST PQC project.
- PQC will avoid the apocalypse of internet, secure communication (eg. military), finance, and sensitive data.

Main Families of Post-Quantum Algorithms

1. Lattice-Based (Kyber, Dilithium, Falcon).
2. Hash-Based (SPHINCS+).
3. Multivariate Polynomial (Rainbow, broken).
4. Code-Based (Classic McEliece).
5. Isogeny-Based (SIKE, broken).

Lattice-Based Cryptography

- Examples: CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon.
  - **CRYSTALS-Kyber**: A **post-quantum key encapsulation mechanism (KEM)** designed for secure key exchange. It is efficient, fast, and resistant to quantum attacks, and has been selected by NIST as the standard for public-key encryption in the post-quantum era.
  - **CRYSTALS-Dilithium**: A **post-quantum digital signature scheme** based on lattice problems. It provides strong security against quantum adversaries, while remaining practical for real-world applications.
  - **Falcon**: Another **post-quantum digital signature scheme**, also lattice-based, optimized for **very small signatures and high efficiency**, making it suitable for constrained environments like embedded systems.
- High efficiency and strong security proofs.
- **Used for encryption, key exchange and digital signatures.**

Hash-Based Signatures

- Example: SPHINCS+.
  - **SPHINCS+**: A **post-quantum digital signature scheme** based on **hash functions** rather than lattices. It is highly secure and conservative, designed to remain secure even if other post-quantum approaches are broken, but it produces larger signatures and is less efficient compared to lattice-based alternatives.
- Based on hash function security.
- Robust but less efficient (large signatures).

Code-Based Cryptography

- Example: Classic McEliece.
  - **Classic McEliece**: A **post-quantum public-key encryption scheme** based on error-correcting codes. It has been studied for decades and is considered one of the most secure options against quantum attacks. Its main drawback is the **very large public key size**, but it offers excellent performance in encryption and decryption speed.
- Uses error-correcting codes.
- Very secure but large public keys.

Multivariate Polynomial Cryptography

- Example: Rainbow.
- Uses multivariate quadratic equations.
- Some schemes broken, not always reliable.

Isogeny-Based Cryptography

Example: SIKE.

Based on elliptic curve isogenies.

Recently broken, no longer recommended.

Potential Consequences Without PQC

- Encrypted communications can be decrypted.
- Digital signatures forged (identity theft).
- Harvest now, decrypt later attacks.
- Collapse of trust in digital infrastructures.

Potential Consequences Without PQC for internet

- TLS/HTTPS would fail
- Today, when you visit a website, your browser uses RSA or ECC to establish a secure connection.
- If those algorithms are broken, attackers could impersonate websites, read or alter communications, and inject malware.

Potential Consequences Without PQC for bank transactions

- Digital signatures could be forged
- Software updates, bank transactions, and blockchain systems (Bitcoin, Ethereum) all rely on ECC or RSA signatures.
- Quantum computers could forge these signatures → fake updates, counterfeit transactions, or fraudulent contracts would look valid.

Potential Consequences Without PQC for Identity verification

- Identity verification breaks down
- Public-key certificates (SSL/TLS, code signing, email encryption) would no longer prove who is who.
- Anyone could masquerade as a bank, government, or service provider.

Potential Consequences Without PQC for encrypted data

- Long-term encrypted data becomes vulnerable
- Sensitive archives (medical, military, financial records) encrypted with current standards could be decrypted by future quantum computers.
- The trust model of the digital world (where cryptography guarantees confidentiality, authenticity, and integrity) would collapse, because we could no longer be sure that communications, transactions, or digital identities are genuine and secure.

Classical vs. Post-Quantum Cryptography - overview

Current Algorithm (Industry Standard)	Quantum Status	Recommended PQC Replacement	Notes
RSA (encryption, signatures, TLS)	Broken by Shor's algorithm	**CRYSTALS-Kyber (encryption), CRYSTALS-Dilithium (signatures)**	Kyber is NIST's chosen KEM, Dilithium is NIST's main signature scheme.
ECC (ECDH, ECDSA, EdDSA, etc.)	Broken by Shor's algorithm	**Kyber (key exchange), Dilithium/Falcon/SPHINCS+ (signatures)**	ECC is widely used in TLS, mobile, blockchain.
DSA (Digital Signature Algorithm)	Broken by Shor's algorithm	**Dilithium, Falcon, SPHINCS+**	DSA is less common today but still present in legacy systems.
AES-128	Weakened by Grover's algorithm (effective 64-bit)	AES-256	Symmetric crypto remains safe with longer keys.
SHA-2 (SHA-256)	Weakened (effective 128-bit)	SHA-512 / SHA-3	Hashes are not fully broken, just need longer output.
SHA-3	Resistant (weakened but still safe)	Still secure	Future-proof but can use larger sizes for safety.
Classic key exchange (Diffie–Hellman)	Broken by Shor's algorithm	**Kyber**	DH is not quantum-safe.

Implementation Roadmap

- Milestone 1: December 31, 2026. Member States are required to lay the groundwork for national PQC transition.
  - This includes: identifying stakeholders, completing inventories that support cryptographic asset management and dependency maps. It's important to include the supply chain, and create a national awareness and communication program

- Milestone 2: December 31, 2030. Implement next steps. By this date, a quantum-safe upgrade path is required, supporting PQC transition for all high-risk use cases. Resources should be allocated, and there needs to be dialogue with the private sector regarding services, PQC training alongside international collaboration.

- Milestone 3: December 31, 2035. In line with the USA's NSM-10 and the NCSC recommendations, by this date PQC transition for medium-risk use cases is required, and either hybrid or fully standardized and tested PQC should be completed for as many systems as possible.

4U Assessment

1. Unworkable – What problems exist today that current solutions cannot address?

- Current public-key cryptography (RSA, ECC) will **become unworkable in the quantum era**, since quantum computers running Shor's algorithm can break them.
- PQC addresses this **fundamental gap** — without it, secure communication, digital signatures, and authentication would no longer be reliable.

2. Unavoidable – Is adoption inevitable?

- Yes. Once large-scale quantum computers are available, **migration to PQC will be unavoidable** to protect critical infrastructure, finance, healthcare, defense, and personal data.
- Standards (e.g., NIST PQC algorithms) are already being defined, showing inevitability of global adoption.

3. Urgent – Is it a priority right now?

- Yes. The "**harvest now, decrypt later**" threat means attackers can already store encrypted data today and decrypt it once quantum machines are available.
- Migration to PQC takes years (standards, software, hardware updates), so preparing now is urgent to avoid future crises.

4. Underserved – Are current solutions insufficient?

- Definitely. Current systems rely almost entirely on RSA/ECC, which are not quantum-safe.
- PQC is still **under-deployed** in practice, with only pilots and early implementations in industry.
- Organizations often lack expertise, tools, and readiness for PQC transition — leaving this need underserved.

Conclusion

- Quantum computing threatens current cryptography.
- PQC algorithms (Kyber, Dilithium, SPHINCS+, Falcon, McEliece) are critical.
- Immediate adoption ensures Cybersecurity resilience.
- Avoid apocalypse