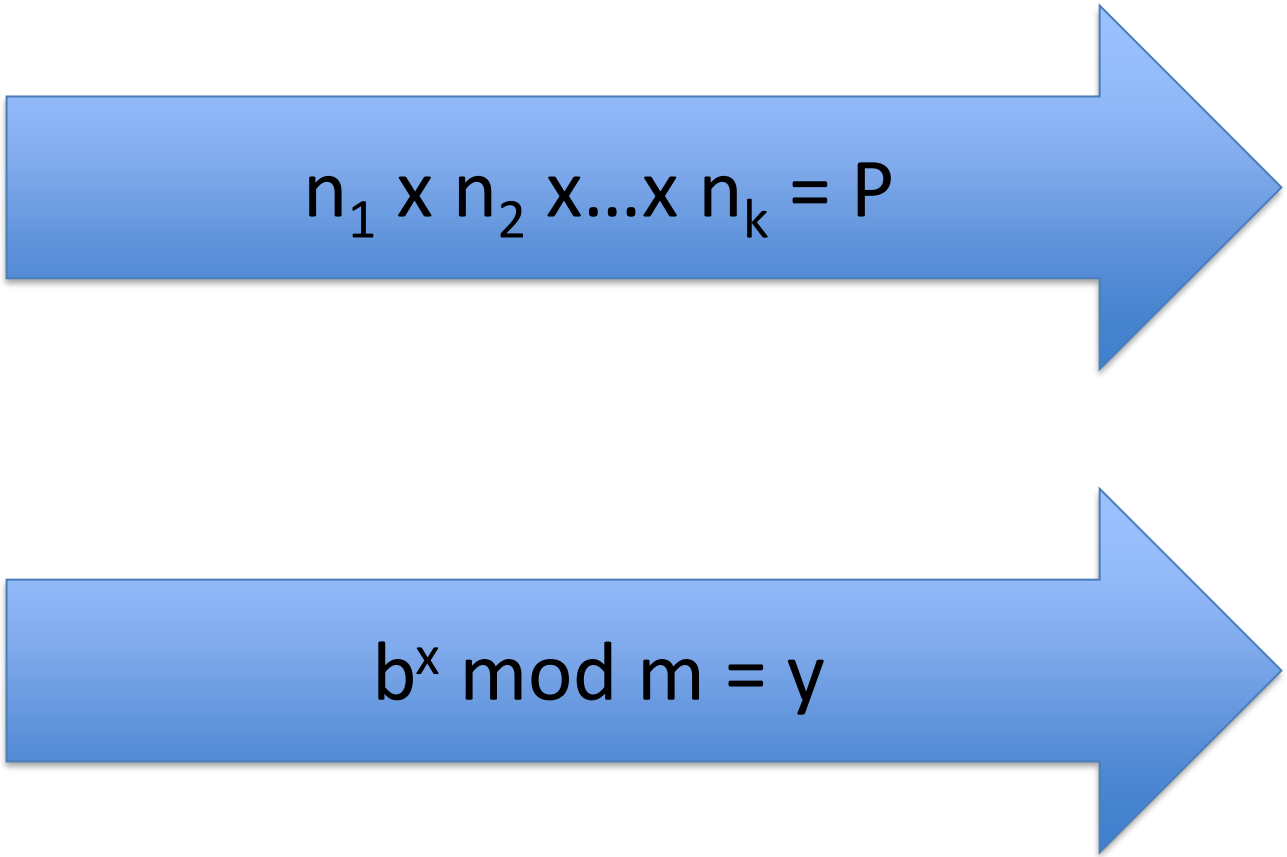
Security preparedness under the GDPR: the (possible) PQC impact

Giuseppe D'Acquisto
Italian Data Protection Authority

Engineering Data Protection In The Wake of PQC
December 8th 2025

One-Way Functions



Classical Security Strategy

- Increase key lengths to maintain security.
- Examples:
  - RSA 1024 → RSA 2048 → RSA 4096
  - DES → AES-128 → AES-256
- Works if attackers are limited to classical computation paradigms.
- Provides time “safety margin” against brute-force attacks.

Quantum Computing Challenge

- Shor's algorithm: speedup for factorization and discrete logarithms.
- Grover's algorithm: speedup for brute-force search (k bit keys work as k/2).
- Qubits: superposition allows simultaneous evaluation of many computational paths.
- Quantum algorithms amplify correct outcomes; formerly infeasible problems become solvable.

Quantum Asymmetry

- Attackers can “harvest now, decrypt later” once quantum computers exist.
- Long-lived encrypted data is vulnerable to future quantum decryption.
- This this creates asymmetry: attackers live in the future, defenders in the past.
- A proactive planning to protect long-term confidentiality.

Engineering Implications

- Simply increasing key lengths is no longer sufficient.
- Quantum-resistant strategies are required.
- Three complementary strategies:
  1. Crypto agility (short term)
  2. Post-quantum cryptography (long term)
  3. Data-protection-driven controls (always)

Crypto Agility

- Ability to swap algorithms and key types without redesign.
- Supports gradual migration to stronger or post-quantum schemes.
- Requires parallel testing, piloting and staged deployment.
- Ongoing capability, not a one-time patch.

Post-Quantum Cryptography

- Lattice-based schemes resist quantum attacks (e.g. Learning With Errors, Shortest Vector Problem).
- Complexity remains exponential even under quantum parallelization.
- NIST post-quantum schemes:
  - CRYSTALS-Dilithium (signature)
  - Falcon (signature)
  - SPHINCS+ (hash-based signature)
  - CRYSTALS-Kyber (key encapsulation mechanism)

Data Protection Engineering

- Mitigate “harvest now” risk via strong governance and principled controls.
- Data minimization: keep only what is necessary; delete or anonymize the rest.
- Segregation/splitting: partition data to reduce compromise risk.
- Multiparty computation: compromise of a share does not break overall security.

Conclusions

- Quantum computing arrival is inevitable; timing and scale uncertain.
- Confidentiality today must outlast current cryptography.
- Act now: map cryptography, ensure agility, embed post-quantum readiness.
- Core principle: control data, not only encryption. Delete, minimize, isolate now!