Transition vers la cryptographie post-quantique

Benjamin Smith

16/02/2023, Campus Cyber

Inria

What can quantum computers do?

General-purpose quantum computers can run **quantum algorithms** including

1. **Shor's algorithm** (1991)
   - Uses the **quantum Fourier transform** to efficiently detect cycle periods
   - Solves integer factorization and discrete logarithm problems in **polynomial time**
2. **Grover's quantum search algorithm** (1996)
   - Searches an unstructured set of N items in time $\sim \sqrt{N}$
   - Classical computers need time $\sim N$ for the same task

When will quantum computers arrive?

When? For the last 15 years, the answer is typically **"probably in 10 years"**.

Constructing general-purpose quantum processors is a massive challenge for **experimental physics** and **engineering**.

So far: incremental progress.

Shor's algorithm: current (public) record for **integer factorization** is $21 = 3 \times 7$ (in 2012! with 10 qubits)

Progress: IBM announced a 433-qubit machine in 2022.[1]

[1] Source: IBM. Analysis: Olivier Ezratty

Quantum resources

Estimates[2] of actual quantum resources (logical qubits, gates/operations) required to break basic asymmetric cryptography using Shor's algorithm:

Security level	(bits)	RSA/Factoring Key bits	Qubits	Operations	Elliptic Curve Discrete Log Key bits	Qubits	Operations
Legacy	80-bit	1024	2050	5.81×10^{11}	160	1466	2.97×10^{10}
Reduced	112-bit	2048	4098	5.20×10^{12}	224	2042	8.43×10^{10}
Basic	128-bit	3072	6146	1.86×10^{13}	256	2330	1.26×10^{11}
...	192-bit	7680	15362	3.30×10^{14}	384	3484	4.52×10^{11}
Paranoid	256-bit	15360	30722	2.87×10^{15}	512	4719	1.14×10^{12}

[2] *Source: BSI Quantum-safe cryptography (2021)*

Post-quantum cryptography

Post-quantum cryptosystems are designed to

- **run** on today's **conventional hardware**,
- **resist** future conventional adversaries, and
- **resist** future adversaries with powerful **quantum computers**.

Aim: upgrade the crypto in everyday security protocols and products to add quantum-safety.

*This has essentially nothing to do with **quantum cryptosystems** (e.g. QKD), which run on quantum devices and channels, and not on conventional hardware.*

Post-quantum cryptography: when?

Cryptographers are already developing post-quantum cryptosystems.

When should we **transition** to using them?

Transition has to begin **now**.

- Long-term data privacy: adversaries can store now, decrypt later
- Long-term infrastructure: e.g. root certificates can have ten-year lifetimes

Post-quantum cryptosystems: symmetric crypto

Symmetric cryptography: data privacy (encryption) and authenticity (MACs).

Postquantum symmetric cryptography is mostly a reaction to **Grover's algorithm**, which allows "brute-force" search in square-root time. *For example:*

- find n-bit **encryption keys** in $2^{n/2}$ operations instead of 2^n
- find **preimages** of n-bit hashes in $2^{n/2}$ operations instead of 2^n.

Basic response: double existing symmetric key/hash lengths.

Quantum-safe data encryption

Transition case study: **data encryption**.

- **Today:** we use standard **AES-128** (128-bit keys).
- **Quantum safety:** switch to standard AES-256 (256-bit keys).
- **Deployment**: AES-256 is already widely deployed.
- **Confidence**: AES-256 is already a long-term standard, 20 years of analysis
- **Practical consequences**:
  - Key management/storage requirements double
  - Encrypted data: same size
  - Speed and energy: 25-30% performance hit

Conclusion: transition is relatively **manageable**.

Asymmetric/Public-key cryptography in 2022

Asymmetric (public-key) cryptography: fundamental tasks are

Objective	Deployed systems
Key agreement *Prior to symmetric encryption*	Elliptic-curve Diffie–Hellman, RSA key agreement
Signatures *Authentication and identification*	RSA signatures, ECDSA, Ed25519

Virtually all deployed systems depend on the hardness of factoring or discrete logs, so are **totally broken by Shor's algorithm**.

NIST (US National Institute of Standards and Technology) has a **post-quantum standardization project** to select quantum-safe key agreement and signatures.

NIST Round 3 and 4 KEM parameters

Key agreement at today's basic 128-bit security level (NIST Level I):

	Candidate	Paradigm	Public key	Ciphertext
"Pre-quantum"	X25519	ECC	32 B	32 B
New Standard	**Kyber512**	**Lattice-based**	**800** B	**768** B
Future	ClassicMcEliece384464	Code-based	261120 B	128 B
standardization	BIKE	Code-based	1540 B	1572 B
candidates	HQC-128	Code-based	2249 B	4481 B

- Post-quantum key agreements can often run **faster**, but
- they have **much larger** public keys and bandwidth requirements, and
- can present new challenges for secure implementation
  (more memory, more randomness, side-channel defences, …)

NIST Round 3 Signature parameters

Signatures at today's basic 128-bit security level (NIST Level I):

	Candidate	Paradigm	Public key	Signature
"Pre-quantum"	Ed25519	ECC	32 B	64 B
New standards	Dilithium (Level II)	Lattice-based	1312 B	2420 B
	Falcon-512	Lattice-based	897 B	666 B
	SPHINCS+-128s	Hash-based	32 B	7856 B
	SPHINCS+-128f	Hash-based	32 B	17088 B

Quantum-safe signatures typically have **much larger keys and signatures**.

"Round 4": NIST is requesting new alternative signature schemes based on other hard problems.

Post-quantum transition; asymmetric crypto

In theory, we know what to do: replace ECC and RSA post-quantum standards.

In practice, this is a massive real-time scientific experiment:

- **Real-world performance** needs much more study
  e.g. large signatures may need two frames $\implies$ *network performance hit*
- **Low confidence**: new standards are immature, have faced less analysis
- **Side-channel attacks**: a **much larger attack surface** for timing attacks, power analysis, ...
- Improved attacks may imply rapid **parameter changes** to maintain security
- Very few existing **implementations**:
  - **software**: optimizations and potential flaws both poorly understood
  - **hardware**: starting from scratch with a long development cycle

Who is working on post-quantum crypography

Large, high-profile French participation in post-quantum crypto research and standardization (NIST, IETF, IEEE, ...)

Inria teams include

- GRACE (Saclay + Campus Cyber)
- COSMIQ (Paris)
- CAPSULE (Rennes)
- ARIC (Lyon)

Also academic teams in Paris, Limoges, Caen, ...

Companies dedicated to post-quantum crypto include CryptoNext, PQShield, ...

Strategic conclusions: What to do?

When planning your migration to post-quantum cryptography,

1. Follow the **standards** (of course!)
2. Insist on **crypto-agility** (easy modular switching between cryptosystems) to ease inevitable changes as standards evolve
3. Insist on **hybrid solutions** (pre- *AND* post-quantum) until new cryptosystems and software/hardware implementations mature

There are **post-quantum cryptography experts** all around you, don't hesitate to reach out!