Post-Quantum

Cryptography Conference

ANSSI plan for post-quantum transition

Jérôme Plût
ANSSI

ANSSI views on post-quantum transition

Jérôme Plût—jerome.plut@ssi.gouv.fr

Agence nationale de la sécurité des systèmes d'information

2023-11-07 PKIC Post-Quantum Cryptography Conference

1. Quantum threat and quantum-safe cryptography

2. Role of ANSSI in cybersecurity and cryptography

3. Transition to post-quantum cryptography
   - End goal: quantum-safe cryptography
   - A three-phase transition plan

4. Technical guidelines
   - Position on post-quantum algorithms
   - Position on hybridisation schemes

1. Quantum threat and quantum-safe cryptography

What can a quantum computer do?

- **Shor's algorithm:** A large quantum computer could solve the *discrete logarithm* and *factorization* problems in *polynomial time* (i.e. very efficiently).
  - This breaks: RSA, (EC)DSA, (EC)DH.
  - *i.e.* essentially all currently-used asymmetric cryptography!

- **Grover's algorithm:** An *extremely* large quantum computer could solve the *exhaustive search* problem in *square-root time* (i.e. somewhat efficiently).
  - This is a generic attack against any possible cryptographic algorithm (in particular, all symmetric-key cryptography is affected).
  - However, the attack remains inefficient (only less so).

- A limited number of **other special cases**, e.g. possibly cube-root collision search.

Evaluation of the quantum threat

Cryptographically useful quantum computers don't exist...

Evaluation of the quantum threat

Cryptographically useful quantum computers **probably** don't exist **right now**...

- $\mathbb{P}(\text{quantum computer}) \geqslant 2^{-128}$ so security analysis **must** take it into account.
- Deployment of quantum-immune cryptography *might* take longer than concretization of the quantum threat.
- In fact, threat is already present, due to *retroactive attacks*.

Retroactive attacks

- Against *confidentiality* in general: « store now, decrypt later »;
  - ☞ Affects asymmetric encryption (encrypted emails)...
  - ☞ but also key exchange (TLS).
- Against *authenticity* in limited cases:
  - ☞ possible future forged software updates for already-existing devices (« verify now, forge later » ?).
  - ☞ authenticated key exchanges are **not** affected now (but still need to eventually transition to quantum-safe cryptography).

How to resist quantum computing?

- Extreme position: *ditch cryptography entirely* and rely on physical security:
  - "quantum cryptography", *i.e. quantum key distribution*.
  - Currently: *this is science-fiction* (at any practical scale).

- Symmetric cryptography is only affected by Grover's algorithm.
  - In general, *doubling key sizes everywhere* is sufficient
  - (Whether this is necessary is still debated!).

- **All currently used asymmetric cryptography is totally broken** by a large enough quantum computer.
  - Solution: abandon discrete logarithm (& factorization)
  - and use algorithms relying on **other** mathematical problems instead.

Post-quantum cryptography

(is actually a subfamily of classical asymmetric cryptography!).

2. Role of ANSSI in cybersecurity and cryptography

Advisory role

ANSSI is (among other things):

- editor of **national technical guidelines** for cryptography in security products.
  - Available online (in French only, sorry!):

`ssi.gouv.fr/guide/mecanismes-cryptographiques/`

  - rules and « best practices »;
  - regularly updated, trying to remain up-to-date with research.
- contributor to **European guidelines (SOG-IS)**.
- **not** a standardization agency.

Regulatory role

ANSSI supervises the evaluation and delivery of **security visas** for security products which use cryptography.

- Security visas are *required* for governmental use.
  - In particular, conformance with the national guidelines is needed.
- Accepted security visas are published online: `ssi.gouv.fr/en/products/certified-products`
- Analysis of the products is performed by ITSEF companies.
  - Theoretical analysis of cryptography included in the product;
  - also practical attacks (including side-channel).
- ITSEF analyses (and ITSEFs themselves) are reviewed by ANSSI technical teams.

Accepted algorithms

- No closed “white list” of accepted algorithms.
  - Goal: do not stifle using innovative algorithms for particular use cases.
- A list of criteria for each family of algorithms:
  - ☞ for block ciphers, key size and block size,
  - ☞ for discrete logarithm, modulus size and selection process,
- For unusual algorithms: *ad-hoc analysis* is required.
  - ☞ An exotic block cipher matching the key and block sizes of AES256 is *not* automatically approved!

3. Transition to post-quantum cryptography

End goal: quantum-safe cryptography

- Goal: eventually replace all pre-quantum algorithms with "equivalent" *post-quantum* algorithms...
  - ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition
  - ssi.gouv.fr/uploads/2023/09/follow_up_position_paper_on_post_quantum_cryptography.pdf
- ...**without security loss** at any point.
  - *Is post-quantum cryptography mature enough?*
- We don't believe in quantum key distribution in most cases:
  - ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications

Families of post-quantum algorithms

Families of post-quantum algorithms

- Lattices:
  - all-purpose family (key encapsulation, signatures, etc.);
  - began (in a large scale) in 2005.
- Codes:
  - share some features of lattices;
  - initiated in late 1970s;
  - increased interest as post-quantum schemes.
- Multivariate:
- Isogeny graphs:
  - These two families currently have only a limited number of use cases.
- Hash-based signatures:
  - (Will be discussed later).

NIST post-quantum standardization process

- Started in 2016.
- Helped the cryptography research community focus on a number of targets.
- After three rounds, in 2022, the following algorithms were retained:

	Key encapsulation	Signature
Lattices	Kyber	Dilithium
		FALCON
Hash-based		SPHINCS+

- In addition, three code-based KEM candidates remain in round 4.

Maturity of post-quantum cryptography

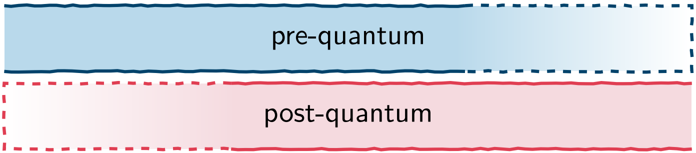
The maturity level of post-quantum cryptography should not be over-estimated.

- It is (roughly) comparable to that of RSA in the mid-1990s.
- About the algorithms themselves:
  - difficulty of the problem itself (vs. classical or quantum adversary),
  - dimensioning and algorithm choice...
- ... but also about algorithm *implementations*:
  - side-channel attacks,
  - integration in protocols...

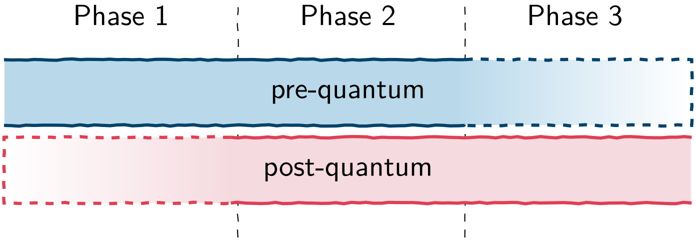
Post-quantum cryptography will not become immediately mature with the publication of the NIST standards.

PQC deployment should be initiated as soon as possible, even before PQC algorithms are fully mature.

The three-phase transition plan



The three-phase transition plan



Phase 1 (current): defence in depth

Phase 1 (current): defence in depth

- Post-quantum algorithms[1] **must** be hybridized with well-known pre-quantum algorithms.
- Post-quantum safety is **recommended** for data with long lifetimes.

- Hybridisation mandate applies to top-level (user-facing) products: parts of the product (e.g. libraries, components) may of course be specialized for post-quantum algorithms.
- Relative *freedom* in the choice of post-quantum algorithm:
  - preferably a *stable, well-studied* specification:
    - ☞ e.g. NIST finalist or trusted alternate.
    - ☞ (Very few exceptions are expected in practice, e.g. FrodoKEM).
  - desired post-quantum security level: matching the security level for symmetric algorithms (preferably NIST level 5 $\approx$ AES256).

[1] **except hash-based signatures**

Hybridisation

Hybridisation

- Combine *well-studied* pre-quantum schemes with more risky *post-quantum* schemes…
- … as a combination which is as secure as *the strongest* part.
  - *i.e.* such that there exists a mathematical proof that breaking the combination requires breaking *both* parts.

The combination preserves the known pre-quantum security, while adding extra protection against the quantum threat.

  - ☞ Specific examples to be given later in this talk.
- **Cost**: the sum of pre-quantum and post-quantum parts.
  - Pre-quantum part is typically lightweight (relative to post-quantum part) in bandwidth (public key/ciphertext/signature size).
- Hybridisation with pre-shared (symmetric) keys is allowed.

Crypto-agility

A system is *crypto-agile* if it is possible to update its cryptographic algorithms during its lifetime.

- This allows building now systems which will be updated with secure post-quantum algorithms.
- Requires dimensioning the system for planned future updates.

Phase 2: building post-quantum confidence

Phase 2: building post-quantum confidence

Start date: $\geqslant$ **2025**.

- Hybridisation **remains mandatory**.
- Post-quantum safety becomes **mandatory** in some cases.

- ANSSI gives a list of *criteria* for post-quantum algorithms.
- The list of accepted algorithms (in practice) might differ from the set of NIST standards.
- Hybridisation remains necessary to guarantee pre-quantum non-regression.

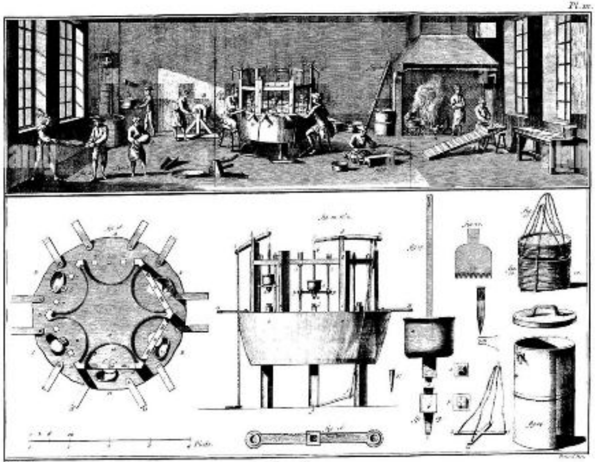
Phase 3: standalone post-quantum cryptography

Phase 3: standalone post-quantum cryptography

Start date: $\geqslant$ **2030**.

- Some post-quantum algorithms may now be used **without hybridisation**.
- Post-quantum safety likely becomes **mandatory in most/all cases**.

4. Technical guidelines



Epinglier

Lattice-based key exchange

CRYSTALS-Kyber	FrodoKEM
Structured lattices	Unstructured lattices
Efficient, relevant for many use cases	Conservative security-wise

Recommendations:

- *Do not modify the parameters* from the standardized versions.
- Use the *highest security level* possible, preferably level 5 ($\approx$ AES256).
- Use *ephemeral keys* if possible: this prevents e.g. decryption failure attacks.
- Use the *actively secure (IND-CCA)* version as documented in the NIST process.

Lattice-based signatures

CRYSTALS-Dilithium	FALCON
Structured lattices	Structured lattices
Good performance	More compact
Simple design	Requires floating-point operations

Recommendations:

- *Do not modify the parameters* from the standardized versions.
- Use the *highest security level* possible, preferably level 5 ($\approx$ AES256).
- For Falcon:
  - Gaussian distributions play an important security role and *should not* be replaced.
  - Falcon is vulnerable to side-channel attacks and countermeasures are hard to implement.

Hash-based signatures

- These algorithms have a *security proof* relying on various security features of a hash function.
- They can already be used **without hybridisation** provided that the conditions for the security proof are respected.

- Performance is a major issue:
  - signature size are large,
  - some signatures (e.g. XMSS) have **stateful private keys**: the number of signatures per key is **bounded**.
- The realistic use cases are *limited*
  - typical case: software updates (infrequent, inherently stateful, not constrained in size, vulnerable to retroactive attacks).

Hash-based signatures

XMSS, LMS	SPHINCS+
stateful	**stateless** variant of XMSS
Limited number of signatures per private key	Larger signatures, less efficient

- All three schemes are considered as conservative security-wise.
- *Do not modify the parameters* from the standardized versions.
- Use the *highest security level* possible, preferably level 5 ($\approx$ AES256).
- May already be used **without hybridisation**.
- The state of XMSS/LMS private keys is **critical** and must be safely managed.
  - The state must be protected in *integrity* and against *re-use*.
  - Forbids e.g. redundancy of private key storage!

"Poor man's hybridisation": pre-shared keys

Pre-quantum algorithm + pre-shared (symmetric) key.

- Simple **stop-gap** solution.
- The security of the pre-shared key **(confidentiality and integrity)** is crucial.
- Each pre-shared key may be shared by only *two* parties.
- Perfect forward secrecy is not ensured against quantum adversaries.

Hybridisation for confidentiality: key combiners

- Protocol combining several key exchanges (pre-quantum or post-quantum) into a single key exchange.
- IND-CPA security: the combined key exchange is IND-CPA as soon as *any* of its components is.
  - (likewise for IND-CCA).
  - Proof work is still ongoing!

	IND-CPA	IND-CCA	
CAT	✗	✗	
XOR	✓	✗	
XOR-then-PRF	✓	(✗)	
Dual-PRF	✓	(✓)	
CAT-then-KDF	✓	(✓)	TLS v1.3 draft
CASCADE	✓	(✓)	≈IKEv2 draft (RFC9370)

Hybridisation for authenticity: signature combiner

Combining signatures by concatenation is secure (EUF-CMA).

The verifier **must** verify both signatures.

- Whether defining a new “combined” signature algorithm or manually checking two signatures is a choice depending on the use case.

Post-Quantum

Cryptography Conference

PKI

Consortium