RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

PQC TRANSITION IN FRANCE
ANSSI VIEWS

Mélissa Rossi, ANSSI, France

Real World Post-Quantum Crypto March 26th 2023 Tokyo

National cybersecurity authority role of ANSSI in crypto

Advisory

Promote the use of state-of-the-art cryptographic standards.


GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES

RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

- National guidelines on crypto
  « Guide des mécanismes cryptographiques »
- European guidelines on crypto (SOG-IS)
  Goal: harmonized crypto evaluation scheme
  « Agreed Cryptographic Mechanisms » (ACM)
- Shared analysis of selected scientific and technical topics
  Technical Position Papers

Regulatory

Supervise the evaluation and delivery of security labels for cryptographic products.

In the French scheme, security evaluations comprise cryptographic evaluation tasks.

e.g. CC certificates

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Quantum threat and Post-Quantum Cryptography (PQC)

➢ It is **hard to predict** if cryptographically relevant quantum computers will ever exist in the future.

Because of the retroactive **“store now, decrypt later"** attack :
➔ Prudence dictates to take the quantum threat into account as soon as possible in some cases
… **long before knowing** if (or when) the development of a cryptographically relevant quantum computer will become achievable in the future.

➢ QKD: Why ANSSI considers that QKD represents a less promising avenue? See *ANSSI position paper on QKD*.

➢ PQC: The most promising avenue to thwart the quantum threat.

Initial technical recommendation report (published in 2022) *ANSSI views on post quantum transition*

➔ A new updated position paper with more details will be published in Summer 2023.

We present here the updated content.

Advances in post-quantum cryptography

Key role of the ongoing NIST standardization process for PQC proposals as a catalyst.

- Strong involvement of the crypto research community
- Focus on a restricted number of KEMs and signatures while preserving the diversity.

Beyond the NIST objective to derive standards, the past four rounds of the standardization campaign **provide a variety of algorithms and solid (although recent) analysis**.

High academic and industrial interest in France: many collaborative projects on design, security analysis of the primitives, cryptanalysis…

Nov 30th 2022: First diplomatic telegram sent from FR to USA encrypted with PQC (FrodoKEM)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline of the talk

1. Initial transition recommendations
2. Our recommendations on post-quantum schemes
3. Our recommendations on hybridation modes
4. Update on the certificate delivery process

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline of the talk

1. Initial transition recommendations
2. Our recommendations on post-quantum schemes
3. Our recommendations on hybridation modes
4. Update on the certificate delivery process

Initial recommendations

Even if the post-quantum algorithms have gained a lot of attention,
and **NIST standards are announced,**
➡ they are **still not mature enough to solely ensure the security.**

Immaturity on different levels:

- the study of the **difficulty of the underlying problem** in the classical and quantum computation models is still under analysis (regularly moving)
- the **choice of parameters** still requires research
- the **integration** of PQC schemes **in protocols** still requires formal proofs
- the vast domain of **secure implementations** (side-channel attacks) remains to be analyzed

➡ several post-quantum schemes have suffered from classical attacks in the past years, e.g.

- W. Beullens. Breaking Rainbow takes a weekend on a laptop. In Y. Dodis and T. Shrimpton, editors, Advances in Cryptology – CRYPTO 2022
- W. Castryck and T. Decru. An efficient key recovery attack on SIDH, eprint archive 2022/975

ANSSI strongly recommends avoiding any drop-in replacement of pre-quantum with post-quantum.

No endorsement of any direct jump.

Single exception: systems where the cryptographic security only relies on hash-based signatures (e.g. software updates)

[Aligned with BSI's *Recommendations on PQC*]

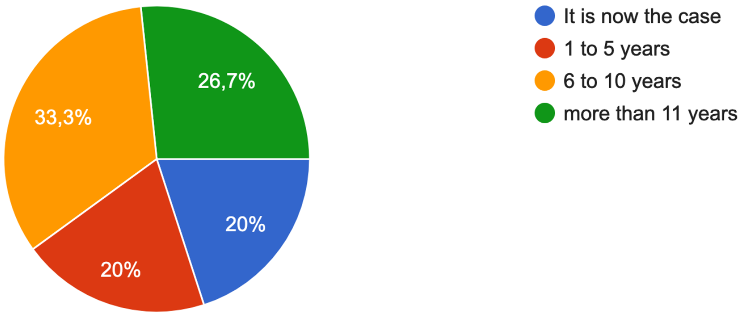
Perception of PQC maturity by crypto researchers

I have asked ∼15 PQC researchers about their perception of PQC maturity.

- Schemes' design is recent:
  ➡Some researchers believe that they might be more vulnerable now because they are recent.
- Cryptanalysis is also recent:
  ➡Some also think that PQC schemes might be more vulnerable in the future with improved cryptanalysis.

There is a clear higher confidence in lattice-based schemes.

How many years do you think we have to wait for gaining a stable classical assurance level for PQC (similar to RSA 2048) ?



15 researchers: not very significative

Initial recommendations: hybridation

Hybridation, hybridation, hybridation.

Hybridation for KEMs and Signatures: post-quantum mechanisms constructed over a recognized pre-quantum scheme.

- Preservation of the pre-quantum security
- Extra protection against the quantum threat
- Low performance penalty over drop-in replacement

➔ Hybridation with pre-shared keys is a possible valid solution.

[Aligned with BSI's *Recommendations on PQC*]

For mitigating the quantum threat, ANSSI strongly recommends to use hybrid protocols in the short and medium term.

Single exception: systems where the cryptographic security only relies on hash-based signatures (e.g. software updates)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Initial recommendations: strategic transition agenda

Acknowledging the immaturity of PQC is important,

but it should not serve as an argument for postponing the first deployments.

ANSSI encourages any company or entity to **consider a progressive transition strategy towards quantum-resistant cryptography.**

ANSSI encourages any progress towards **crypto-agility**.

ANSSI recommends to **start transitioning with hybrid quantum-resistant cryptography as soon as possible** for security products aimed at offering a **long-lasting protection of information (after 2030)**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Initial recommendations on symmetric cryptography

ANSSI encourages to use a conjectured post-quantum security level on **symmetric primitives** consistent with the selected post-quantum PKC algorithm.

- In practice AES-256 for block ciphers and SHA2-384 for hash functions.

- Grover’s algorithm quadratically speeds up the exhaustive search of secret keys in symmetric algorithms.
- More evolved quantum attacks can also speed up certain attacks on hash functions (collision finding attacks).

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline of the talk

1. Initial transition recommendations
2. Our recommendations on post-quantum schemes
3. Our recommendations on hybridation modes
4. Update on the certificate delivery process

Detailed recommendations on post-quantum schemes

ANSSI traditionally **does not provide any closed list of recommended algorithms** in order to avoid proscribing innovative state-of-the-art algorithms that could be well-suited for some particular use cases.

The following detailed recommendations are not exclusive.

Lattice-based KEMs

Crystals-Kyber
- competitive performance, relevant for many use cases
- based on structured lattices problems
- relatively simple design

FrodoKEM
- more conservative variant (based on an unstructured lattice problem)
- simple design as well

Recommendations

(1) **Do not modify the parameters** of the standardized instance unless justified.
(2) Use the **highest security level** as possible, preferably level-5 (i.e. equivalent to AES 256).
(3) Use **ephemeral keys** as much as possible. It prevents many attacks like decryption failure ones.
(4) Use the **semantically secure version** (IND-CCA) that will be standardized by NIST.
There are some cases, like in provable authenticated protocols, where the IND-CPA version in static mode may still be secure. But no decryption oracle (even in side-channel) must be available.

Lattice-based Signatures

Crystals-Dilithium

- competitive performance
- based on structured lattices problems
- relatively simple design

Falcon

- more compact and efficient
- based on structured lattices problems
- needs particular (floating points) instructions

Recommendations

(1) **Do not modify the parameters** of the standardized instance unless justified.
(2) Use the **highest security level** as possible, preferably level-5 (i.e. equivalent to AES 256).
(3) Pay attention to stick to the design in order to avoid misuse attacks. Gaussian distributions in Falcon play an important role in the security and they should not be replaced.
(4) For Falcon, side-channel countermeasures are difficult to apply and research has proved that side-channel attacks may defeat unprotected implementations of Falcon.

Hash-based Signatures

XMSS/LMS

- Conservative signature option (minimalist security hypothesis)
- Potentially limited number of possible signatures per key pair
- Stateful

SPHINCS+

- stateless variant of XMSS
- Conservative signature option (minimalist security hypothesis)
- Less competitive in terms of performance and compactness

Recommendations

(1) **Do not modify the parameters** of the standardized instance unless justified
(2) Use the **highest security level** as possible, preferably level-5 (i.e. equivalent to AES 256).
(3) Hybridation is optional for these signatures.
(4) For XMSS/LMS, the state is a very critical data and should be protected in integrity.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline of the talk

1. Initial transition recommendations
2. Our recommendations on post-quantum schemes
3. Our recommendations on hybridation modes
4. Update on the certificate delivery process

Hybridation of KEMs

Combine the security of several post-quantum and pre-quantum KEMs.

Let n key encapsulation schemes $\mathtt{KEM}_i = (\mathsf{KeyGen}_i, \mathsf{Encaps}_i, \mathsf{Decaps}_i)\ 1 \leq i \leq n$
Let $\mathscr{K}_i$ be $\mathtt{KEM}_i$ key space.
Let $\mathscr{C}_i$ be $\mathtt{KEM}_i$ ciphertext space.
Let $\tilde{\mathscr{K}} := \mathscr{K}_1 \times \cdots \times \mathscr{K}_n$ and $\tilde{\mathscr{C}} := \mathscr{C}_1 \times \cdots \times \mathscr{C}_n$

Let $W : \tilde{\mathscr{K}} \times \tilde{\mathscr{C}} \to \mathscr{K}$ be a **key combiner**.

$\widetilde{\mathsf{KeyGen}}()$

for $i = 1 \ldots n$ **do**
$\quad (sk_i, pk_i) \leftarrow_\$ \mathsf{KeyGen}()$
$\overrightarrow{sk} = (sk_i)_{1 \leq i \leq n}$
$\overrightarrow{pk} = (pk_i)_{1 \leq i \leq n}$
return $(\overrightarrow{sk}, \overrightarrow{pk})$

$\widetilde{\mathsf{Encaps}}\left(\overrightarrow{pk} = (pk_i)_{1 \leq i \leq n}\right)$

for $i = 1 \ldots n$ **do**
$\quad (c_i, k_i) \leftarrow_\$ \mathsf{Encaps}(pk_i)$
$\vec{c} = (c_i)_{1 \leq i \leq n}$
$\vec{k} = (k_i)_{1 \leq i \leq n}$
$k = W(\vec{k}, \vec{c})$
return $(\vec{c}, k)$

$\widetilde{\mathsf{Decaps}}\left(\overrightarrow{sk} = (sk_i)_{1 \leq i \leq n}, \vec{c} = (c_i)_{1 \leq i \leq n}\right)$

for $i = 1 \ldots n$ **do**
$\quad k_i \leftarrow_\$ \mathsf{Decaps}(sk_i, c_i)$
$\vec{k} = (k_i)_{1 \leq i \leq n}$
$k = W(\vec{k}, \vec{c})$
return k

IND-CPA robustness: $\exists i$ such that $\mathtt{KEM}_i$ is IND-CPA $\Longrightarrow$ $\widetilde{\mathtt{KEM}}$ is IND-CPA.

IND-CCA robustness: $\exists i$ such that $\mathtt{KEM}_i$ is IND-CCA $\Longrightarrow$ $\widetilde{\mathtt{KEM}}$ is IND-CCA.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Hybridation modes: pre-shared keys

An extra key psk can be pre-shared and stored by both parties.

$\widetilde{\text{Encaps}}\left(\overrightarrow{pk} = (pk_i)_{1 \le i \le n}, psk\right)$

for $i = 1 \ldots n$ **do**
$\quad (c_i, k_i) \leftarrow_\$ \text{Encaps}(pk_i)$
$\vec{c} = (c_i)_{1 \le i \le n}$
$\vec{k} = (k_i)_{1 \le i \le n}$
$k = W(psk, \vec{k}, \vec{c}\,)$
return $(\vec{c}, k)$

$\widetilde{\text{Decaps}}\left(\overrightarrow{sk} = (sk_i)_{1 \le i \le n}, \vec{c} = (c_i)_{1 \le i \le n}, psk\right)$

for $i = 1 \ldots n$ **do**
$\quad k_i \leftarrow_\$ \text{Decaps}(sk_i, c_i)$
$\vec{k} = (k_i)_{1 \le i \le n}$
$k = W(psk, \vec{k}, \vec{c}\,)$
return k

This technique alone with $n = 1$ is called **Type 1 hybridation**.

➡ Relies on the symmetric paradigm

➡ Good **intermediate solution** but ANSSI raises the following warnings:

(1) The **confidentiality and integrity of the pre-shared key** is a crucial pre-requisite.

(2) Each pre-shared key must only be shared by two parties and not by a group of three or more parties.

(3) Fails to ensure perfect forward secrecy (PFS) against quantum adversaries.

Hybridation modes: key combiners

1 $W(\vec{k}, \vec{c}) = (k_1 | k_2 | \ldots | k_n)$

Cat

Concatenation does not provide IND-CPA-robustness

2 $W(\vec{k}, \vec{c}) = k_1 \oplus k_2 \oplus \ldots \oplus k_n$

XOR

XOR is robust for IND-CPA but not robust for IND-CCA.

Mix and match attack

$\mathscr{A}(pk_1, pk_2, c_1^*, c_2^*, k^*)$: // $k^* = k_1 \oplus k_2$ if $b = 0$ or random if $b = 1$

$(c_1, k_1) \leftarrow \mathsf{Encaps}_1(pk_1)$

$(c_2, k_2) \leftarrow \mathsf{Encaps}_2(pk_2)$

$k' \leftarrow \widetilde{\mathsf{Decaps}}(\vec{sk}, (c_1, c_2^*))$ // $k' = k_1 \oplus k_2^*$

$k'' \leftarrow \widetilde{\mathsf{Decaps}}(\vec{sk}, (c_1^*, c_2))$ // $k'' = k_1^* \oplus k_2$

if $k^* = k_1 \oplus k_2 \oplus k' \oplus k''$ **then return** 0 //$k_1 \oplus k_2 \oplus k' \oplus k'' = k_1^* \oplus k_2^*$

else return 1

- F. Giacon, F. Heuer, and B. Poettering. KEM combiners. pages 190–218, PKC 2018.

Hybridation modes: key combiners

3 $W(\vec{k}, \vec{c}) = \mathsf{PRF}(k_1 \oplus k_2 \oplus \ldots \oplus k_n, \vec{c})$

XOR then PRF

XOR then PRF is robust for IND-CPA but no proof for IND-CCA robustness.

4 $n = 2$

$$W(\vec{k}, \vec{c}) = \mathsf{PRF}(\mathsf{dualPRF}(k_1, k_2), \vec{c})$$

for arbitrary n:

nested dual PRF

Dual-PRF

DualPRF is robust for IND-CCA under the **dualPRF hypothesis.**

- the dualPRF hypothesis is new.
- cannot be obtained from standard PRF constructions.
- non-trivial constructions but ongoing research.

- Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. Hybrid key encapsulation mechanisms and authenticated key exchange. PQCRYPTO 2019

Hybridation modes: [ETSI's Hybrid Key Combiners]

5 $W(\vec{k}, \vec{c}) = \mathrm{KDF}(0^{|\mathrm{salt}|}, k_1 | k_2 | \ldots | k_n, \vec{c}, L)$

Cat then KDF

Cat then KDF is robust for IND-CPA under mild hypothesis on the KDF
- can be proved IND-CCA in the ROM
- no proof in the QROM.
- can be proved without ROM but with strong hypothesis on the KDF.
- $\vec{c}$ should be included in the input.

6 $W(\vec{k}, \vec{c}) = (r_1 | r_2 | \ldots | r_n)$

CASCADE

$$(w_1, r_1) = \mathrm{KDF}(0^{|\mathrm{salt}|}, k_1, \vec{c}_1, d + \ell)$$
$$(w_2, r_2) = \mathrm{KDF}(0^{|\mathrm{salt}|}, w_1 | k_2, \vec{c}_2, d + \ell)$$
$$\vdots$$
$$r_n = \mathrm{KDF}(0^{|\mathrm{salt}|}, w_{n-1} | k_n, \vec{c}_n, d + \ell)$$

CASCADE is robust for IND-CPA in the ROM
- no proof IND-CCA in the QROM.
- can be proved IND-CCA without ROM but with strong hypothesis on the KDF.
- $\vec{c}$ should be included in the input.

- Matthew Campagna and Adam Petcher. Security of hybrid key encapsulation. Cryptology ePrint Archive, Report 2020/1364, 2020. https://eprint.iacr.org/2020/1364
- Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. Hybrid key encapsulation mechanisms and authenticated key exchange. PQCRYPTO 2019

Hybridation modes

In general, as for any cryptographic function, ANSSI recommends to use **standards or well-studied modes with validated security proofs.**

➡ The implementation security (side-channel resistance) of the hybridation mode is also very important to avoid attacks that would bypass certain key encapsulations.

	IND-CPA robustness	IND-CCA robustness
CAT	×	×
XOR	✓	×
XOR then PRF	✓	(×)
Dual-PRF	✓	(✓)
CAT then KDF	✓	(✓)
CASCADE	✓	(✓)

For **IND-CCA robustness**:
- research is still ongoing
- the modes did not pass the « test of time »

In addition, XOR and XOR then PRF may be relevant to achieve **IND-CPA robustness.**

Cat then KDF and CASCADE seem as good options.
➡ Drafted for being included at a protocol level (TLS, IKE).

- D. Stebila, S. Fluhrer, and S. Gueron. Hybrid key exchange in TLS 1.3 (draft IETF). https://www.ietf. org/id/draft-ietf-tls-hybrid-design-03.html.
- C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van-Geest, O. Garcia-Morchon, and V. Smyslov. Multiple Key Exchanges in IKEv2 https://datatracker.ietf.org/doc/ draft-ietf-ipsecme-ikev2-multiple-ke/.

Hybrid Signatures

The solutions for hybrid signatures are less diverse.
The signature scheme below is proved secure in the existential unforgery under chosen message attacks model (EUF-CMA).

Let n signature schemes $\mathtt{SIG}_i = (\mathsf{KeyGen}_i, \mathsf{Sign}_i, \mathsf{Verif}_i)$ $1 \leq i \leq n$

$\widetilde{\mathsf{KeyGen}}()$

for $i = 1 \ldots n$ **do**
  $(sk_i, pk_i) \leftarrow_{\$} \mathsf{KeyGen}()$
$\overrightarrow{sk} = (sk_i)_{1 \leq i \leq n}$
$\overrightarrow{pk} = (pk_i)_{1 \leq i \leq n}$
return $(\overrightarrow{sk}, \overrightarrow{pk})$

$\widetilde{\mathsf{Sign}}\left(\overrightarrow{sk} = (sk_i)_{1 \leq i \leq n}, m\right)$

for $i = 1 \ldots n$ **do**
  $\sigma_i \leftarrow \mathsf{Sign}(sk_i, m)$

return $\widetilde{\sigma} = (\sigma_i)_{1 \leq i \leq n}$

$\widetilde{\mathsf{Verif}}\left(\overrightarrow{pk} = (pk_i)_{1 \leq i \leq n}, m, \vec{\sigma}\right)$

for $i = 1 \ldots n$ **do**
  if $\mathsf{Verif}(pk_i, m, \sigma_i) = 0$ **then return** 0
return 1

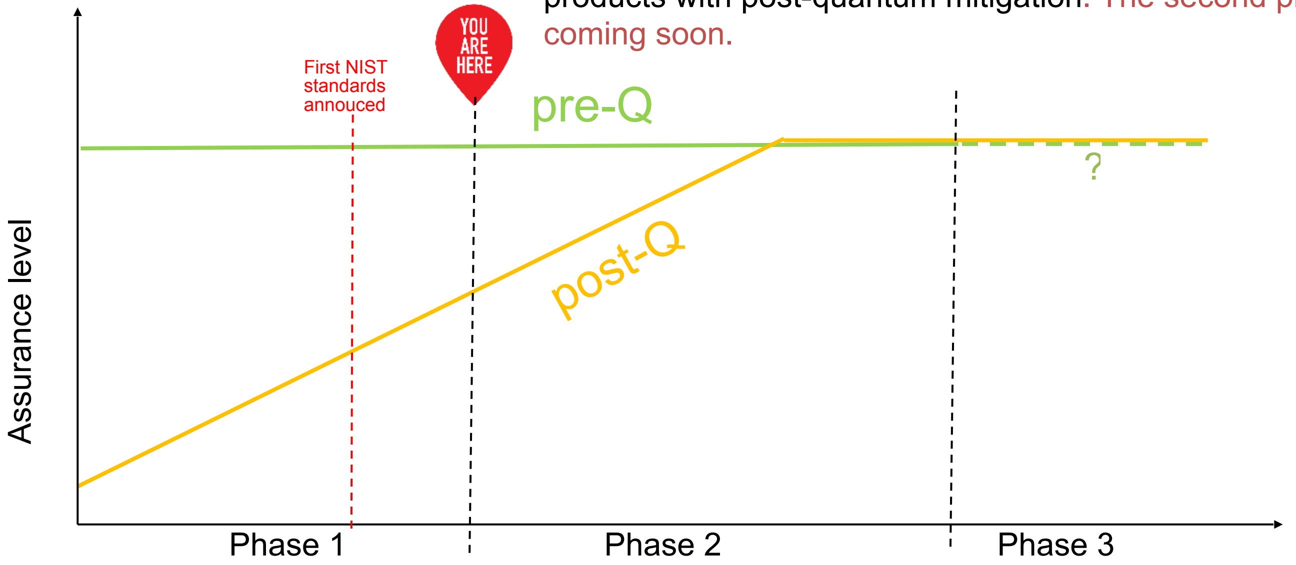
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline of the talk

1. Initial transition recommendations
2. Our recommendations on post-quantum schemes
3. Our recommendations on hybridation modes
4. Update on the certificate delivery process

3-phase transition

➢ The experimental phase is close to the end. Many industries have prototyped their transition and project to commercialize products with post-quantum mitigation. The second phase is coming soon.



Hybrid PQC as a defense-in-depth add-on.	**Hybrid PQC as post-quantum mitigation.**	**TBD depending on the context and PQC assurance level**
Security visa evaluation will only include pre-quantum assurance (no degradation of the security).	Security visa evaluation will include hybrid PQC analysis and mention the post-quantum assurance.	Probably optional hybridation.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Update on the security certificate delivery process

ANSSI is **updating its agenda on certificate delivery.**

The evaluation centers (ITSEFs) are currently developing skills on:

- evaluation of hybrid mechanisms,
- evaluation of a number of well-known PQC algorithms.
- side-channel evaluation of a number of well-known PQC algorithms.

Phase-2 Certificates

In addition to the classical state-of-the-art assurance recognition, the certification report will soon be able to **mention the presence of state-of-the-art post-quantum protection.**

➡ First results are expected in **2024-2025.**

For developers willing to evaluate their products: please contact the ITSEFs for more information

Thank you for your attention