Cybersécurité et la menace quantique

Olivier Blazy

Archimede 2026

Blazy Olivier

Professeur @ Ecole Polytechnique

Olivier.blazy@polytechnique.edu

- Responsible du GT-C2 de 2020-2024
- Auteur du standard HQC @ NIST PQC
- Directeur Scientifique du CIEDS
- Cryptographie, protection de la vie privée, PQ, …

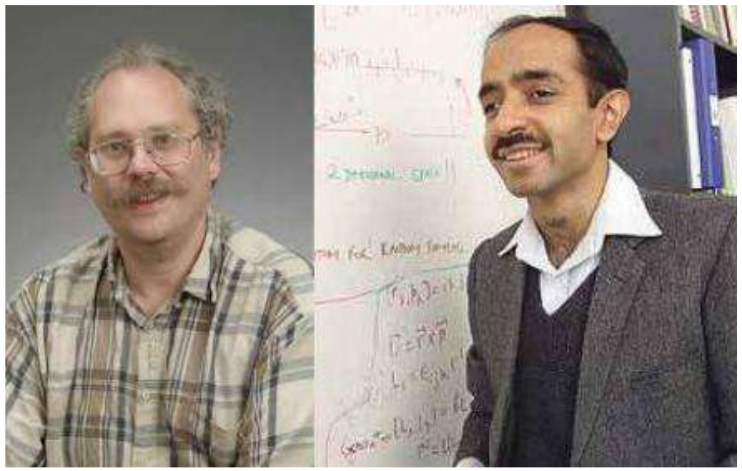
<- Site web

Email ->

L’urgence postquantique: Shor et Grover contre la cryptographie.

1994: Peter Shor a proposé un algorithme quantique qui casse le problème du logarithme discret et la factorization **s’il y a suffisamment de qubits**. (et donc les bases de la crypto moderne RSA, et Diffie Hellman)

1996: Lov Grover a propose un algorithme quantique permettant de chercher en O(√N) dans des ensembles non structures de taille N.



La cryptographie est perdue face au quantique?

Pour appliquer Shor, il faut énormément de qubits (et encore plus de portes quantiques).

Les estimations actuelles disent que pour casser **256** bits de sécurité, il faut envirion ~~**2330**~~ **684** qubits pour le logarithme discret et ~~**3072**~~ **1730** pour RSA.

Les meilleurs ordinateurs actuels promettent... **1223** qubits universels. (atom computing)
Avons-nous déjà perdu?

Non, il y a de fortes contraintes de correction d'erreur pour garantir que ces qubits puissent interagir
Il faut actuellement environ 2^{30+} portes deToffoli

Mais peut-être dans l'avenir ?

L'algorithme de Grover fonctionne bien, mais pour s'en prémunir il suffit de doubler la taille des clés

Le plus gros problème est le collect and decrypt later

2 profils de menace quantique

	Passive	Active
Chiffrement	Collecte maintenant, décrypte plus tard	Accès au clair à la volée
Signature	??	Contrefaçon de signature

Plan de transition **Européen**: 2030 pour les applications à Haut-Risque (sensible dans 10 ans)

Français: ANSSI: pas de certification de nouvelles solutions non PQ dès 2027

Et la cryptographie quantique?

Le Quantique dit que si une information est lue, alors les qubits sont figés.
Donc une signature quantique ne fait pas de sens…

La Distribution Quantique de Clés (QKD) a eu beaucoup de financements mais

French Cybersecurity Agency (ANSSI)

Federal Office for Information Security (BSI)

Netherlands National Communications Security Agency (NLNCSA)

Swedish National Communications Security Authority, Swedish Armed Forces

Executive summary

Quantum Key Distribution (QKD) seeks to leverage quantum effects in order for two remote parties to agree on a secret key via an insecure quantum channel. This technology has received significant attention, sometimes claiming unprecedented levels of security against attacks by both classical and quantum computers.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is

Le Tsunami quantique

Hypothesis	State
RSA, Factorisation	**Cassé**
Courbes Elliptiques	**Cassé**
Isogénie	**Probablement ok, mais bof**
Lattice / Code	**Surement**
Multivarié	**Peut-être**
Fonction de Hachage	**Oui** (mais pas de chiffrement)

Chronologie de la Standardisation NIST.

2016

Call for proposals

2017

Submission Deadline

2018

Several broken proposals

2019

Second Round

2022

Kyber 4th Round

Summer 2022

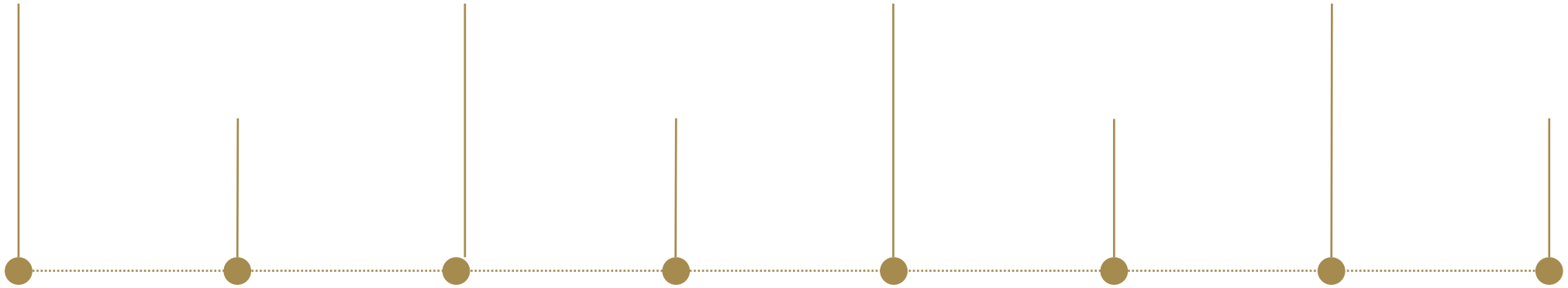
SIDH on a laptop

2024

FIPS for ML-KEM

2025

HQC



Standardization, because rules are fun!
NIST

Chiffrement

Kyber – ML-KEM
Réseaux euclidiens

HQC – HQC-KEM
Codes

Signature

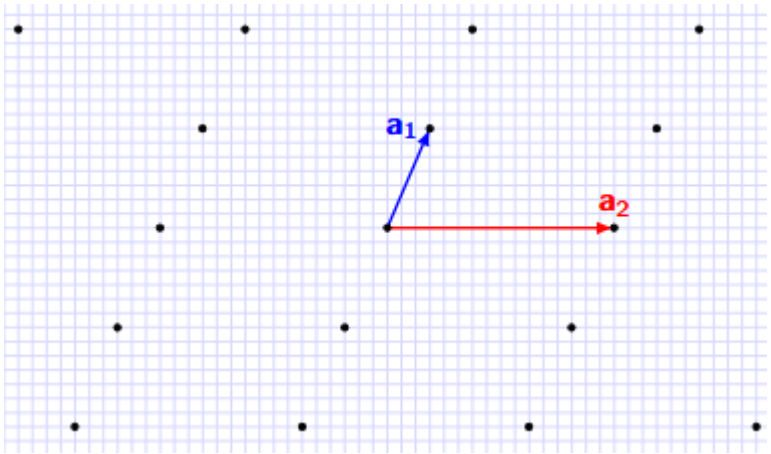
Toutes sur les réseaux

Dilithium	– ML-DSA
Sphincs+	– SLH-DSA
Falcon	– FN-DSA

De nouelles hypothèses, mais des techniques similaires: code/lattices

Syndrome Decoding / Short Integer Solution
Etant donnée une matrice **A**, un vecteur **s**, trouver un petit **x** tel que **Ax** = **s**

Learning with Errors:
Etant donnée **A**, et **c** decider si **c** est proche du span de **A** (**c** = **As** + **e** pour un petit **e**)



Pourquoi l'approche *code-based* reste prometteuse

- Hypothèse bien comprise
- Des décénies d'étude
- Mieux gérées en hardware
- La standardization d'HQC n'est pas un succès isolé mais la culmination de 45 ans d'évolution

Un peu d’histoire

Quick Timeline of Code-based encryption

1978

McEliece

1990s

Niederreiter variant

2003

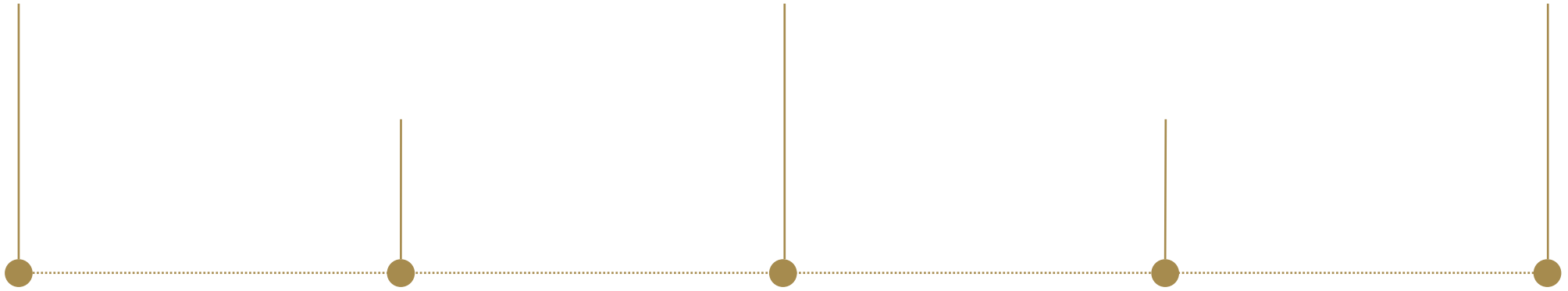
Alekhnovich (provable reductions)

2010s

Structured codes, QC, MDPC

2024

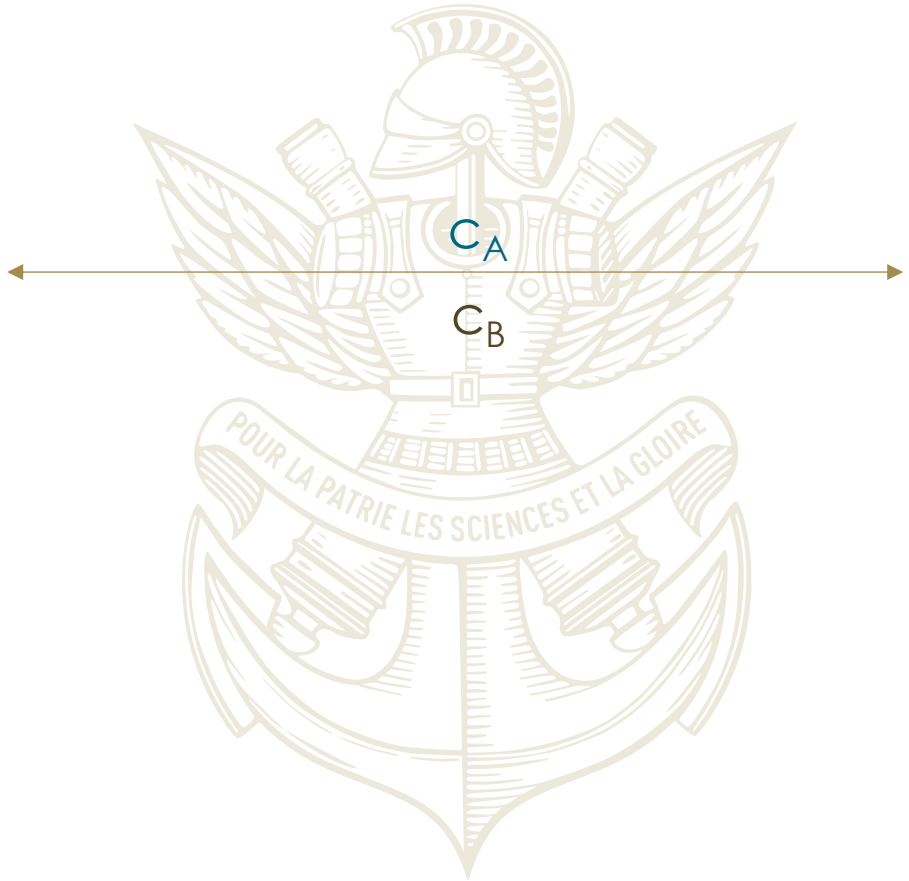
HQC standardization



Diffie Hellman (Courbe Elliptique)

Alice

- $a \leftarrow R$
- $c_A = a\mathbf{P}$
- $ac_B = a(b\mathbf{P})$
- $ab\mathbf{P}$



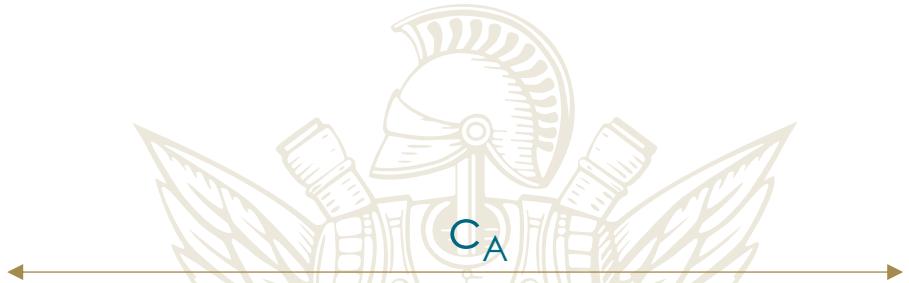
Bob

- $b \leftarrow R$
- $c_B = b\mathbf{P}$
- $bc_A = b(a\mathbf{P})$
- $ab\mathbf{P}$

Diffie Hellman bruité

Alice

- $a \leftarrow R$
- $c_A = aP + e_A$
- $ac_B = a(bP + e_B)$
- $abP + be_A$



Bob

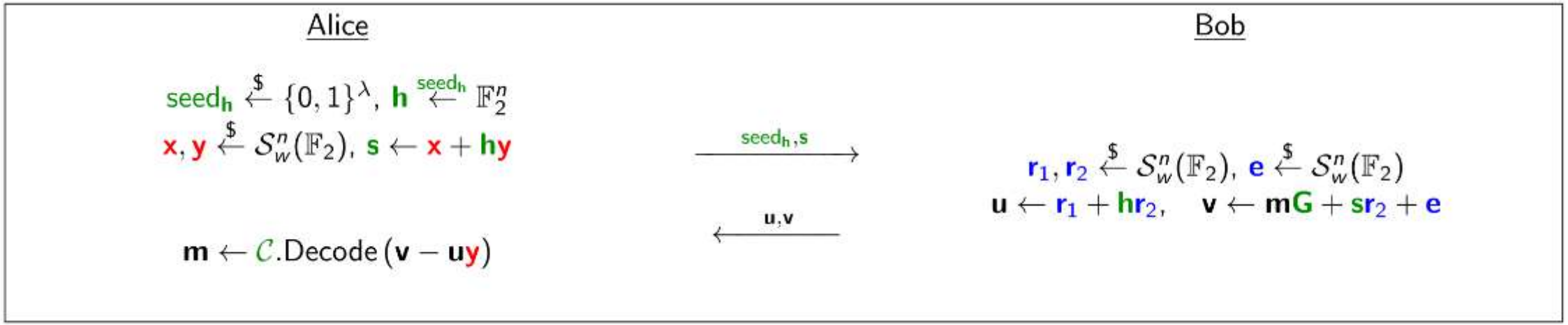
- $b \leftarrow R$
- $c_B = bP + e_B$
- $bc_A = b(aP + e_A)$
- $abP + ae_B$

$$\Delta = ae_B - be_A$$

For a good enough error correcting code G, and any key $\mathbf{K}$:

$$G^{-1}(G(K) + \Delta) = \mathbf{K}$$

HQC in a nutshell (with seed)



Performance

Une Vitesse compétitive

Target lvl	Level I	Level III	Level V
Keygen	75	175	356
Encap	177	405	799
Decap	323	670	1,331

Performance en kilocycles (AVX2)

Des tailles raisonnables

Target lvl	Level I	Level III	Level V
Pk	2,249	4,522	7,245
Chiffré	4,497	9,042	14,484

Taille en octets

Comparaison des schémas à base de code au niveau V

	Pk	C	Keygen	Encap	Decap
HQC	7,245	14,484	356	799	1,331
McEliece	1,044,992	208	674,012	196	273
Kyber	1,568	1,568	73	97	79

Agilité Cryptographique et hybridation X-Wing

Agilité Cryptographique et Hybridation

La migration va être progressive

Combiner des schémas classiques et post-quantiques va permettre une certaine continuité de service mais va demander d'être attentive au design.

Approche Naïve

Si on suppose un KEM classique, et un KEM postquantique

HybridEnc(pk_1,pk_2):

K_1,C_1=Enc(pk_1)
K_2,C_2=Enc(pk_2)
// K=H(K1,K2,C1,C2)
Return C = C_1,C_2

HybridDec(C,sk_1,sk_2)

K'_1=Dec(C_1,sk_1)
K'_2=Dec(C_2,sk_2)
Return K'=H(K'_1,K'_2,C_1,C_2)

Mais: C_2 est trop gros, donc le hasher demande trop de ressources

X-Wing

Une méthoque générique d'hybridation qui ne demande plus de hasher le chiffré post-quantique.

Si le chiffré post-quantum est C2PRI, on utilize: $H(K'_1,K'_2,C_1, pk_1)$.

HQC est naturellement C2PRI.

Perspectives et Q&A

Perspectives and Q&A

Standardization : Bientôt publication du FIPS, et guide de transition

Support hardware en cours

Challenges:

- Réduire encore plus la taille
- Augmenter la resistance au Side-channel
- De meilleures hybridations


Merci
ÉCOLE POLYTECHNIQUE
INSTITUT POLYTECHNIQUE DE PARIS