Le NIST (National Institute of Standards and Technology américain) consacre les chercheurs du Laboratoire Xlim (CNRS/Université de Limoges) et de l'Institut de mathématiques de Bordeaux (Bordeaux INP/CNRS/Université de Bordeaux) comme garants de la sécurité des échanges de données dans le monde entier.

Une équipe de chercheurs du laboratoire Xlim (CNRS/Université de Limoges) **en collaboration avec l'Institut de mathématiques de Bordeaux** (CNRS/Université de Bordeaux/Bordeaux INP), **a été sélectionnée le 11 mars 2025 par le NIST** (National Institute of Standards and Technology) pour **son projet HQC comme second standard de chiffrement post-quantique**.

Explications

Il est retenu désormais que si une faille était découverte dans le ML-KEM, le système qui garantit la sécurité des échanges des données dans le monde dès lors que deux parties communiquent sur un canal public, **c'est bien HQC**, une production de l'Université de Limoges/Université de Bordeaux, **qui prendrait le relais pour continuer à sécuriser nos données**.

Historique

Le choix de HQC vient clôturer un long processus de standardisation qui a débuté en 2017.

Depuis 2015, la National Security Agency (NSA), organisme gouvernemental du département de la Défense aux États-Unis, communique sur le besoin de faire évoluer les outils cryptographiques vers des outils post-quantiques afin de garantir l'intégrité des données échangées lors de nos communications en ligne face au progrès des technologies liées à l'ordinateur quantique susceptible de casser les schémas cryptographiques utilisés actuellement

Dans ce contexte, le NIST a ouvert en juillet 2016 un appel international à contribution afin d'identifier les meilleurs candidats aux futurs standards de cryptographie post-quantique, c'est-à-dire résistants aux ordinateurs quantiques de demain. Cet appel s'est structuré autour de trois grandes classes d'algorithmes : le chiffrement, l'échange de clés et la signature. Pour chacune de ces rubriques, plusieurs alternatives possibles ont été étudiées.

Service Communication - Université de Limoges, 05 55 14 91 10, com@unilim.fr
Service Communication de l'Institut Xlim, info@xlim.fr
Contact presse CNRS, presse@cnrs.fr

Le concours commence en novembre 2017 avec 82 soumissions, dont 69 ont été déclarées recevables. **Parmi ces 69 soumissions, 8 d'entre elles impliquent Philippe Gaborit, professeur à l'Université de Limoges**, au sein du laboratoire Xlim, et ses collaborateurs de l'équipe CRYPTIS, qui bénéficie d'une expertise de plus de 25 ans sur les codes correcteurs d'erreurs au cœur des thématiques post-quantiques.
Cette reconnaissance par le NIST témoigne de l'excellence des recherches menées par les **chercheurs du laboratoire Xlim et de l'Institut de mathématiques de Bordeaux** en matière de cryptographie et de cybersécurité (source : Lettre d'Xlim-Université de Limoges).

a. Vincent Jolivet, président de l'Université de Limoges

« Les équipes de l'université de Limoges, à travers l'Institut Xlim, sont précurseurs depuis des années des recherches en cryptographie. Nos étudiants issus du Master Cryptis sont, pour un grand nombre, en poste dans de nombreuses structures en charge de la sécurité des données, que ce soit dans les Institutions de l'État comme le ministère de l'intérieur ou des armées, mais aussi dans de nombreuses entreprises privées. Cette reconnaissance mondiale de l'algorithme HQC vient confirmer ce que nous savions déjà : notre université dispose des talents et des savoir-faire pour répondre aux grands enjeux de sécurisation des infrastructures numériques de demain et contribuer activement à l'élaboration des standards internationaux en cybersécurité.
Je dis évidemment ma fierté aux équipes de Philippe Gaborit et à ses partenaires pour ce beau résultat. »

b. Antoine Petit, PDG du CNRS

CNRS est très fier de voir consacrée l'excellence des travaux des équipes du laboratoire XLIM et de l'Institut de Mathématiques de Bordeaux. La standardisation de l'algorithme HQC marque non seulement une avancée stratégique pour la sécurité des communications numériques face aux menaces des futurs ordinateurs quantiques mais aussi une reconnaissance internationale de la qualité de l'école française en mathématiques et en cryptographie. »

c. Stéphane Bila, chercheur du CNRS et directeur de l'Institut Xlim

« Cette nouvelle reconnaissance de l'excellence en cryptographie post-quantique est une grande fierté pour l'Institut Xlim. Elle incarne la volonté du laboratoire à rayonner internationalement grâce à des recherches fondamentales de haut niveau et sa capacité à innover. Rappelons-le, il y a plus de 25 ans, la cryptographie post-quantique était peu étudiée et pourtant nos collègues se sont intéressés à ce sujet et ont persévéré. Aujourd'hui, forts de ces années de recherches, leurs travaux sont valorisés de manière remarquable et deviennent le second standard mondial. »

Qu'est-ce que le NIST ?

Le **NIST (National Institute of Standards and Technology)** est une organisation américaine qui établit des standards technologiques utilisés dans le monde entier. Depuis plusieurs années, il mène un processus rigoureux pour sélectionner les meilleurs algorithmes de chiffrement post-quantique afin d'assurer la sécurité des communications à l'avenir.

Fondé en 1901, le NIST est un organe du Département du commerce des États-Unis. C'est l'un des plus anciens laboratoires de sciences physiques du pays. En tant qu'organisme n'ayant pas vocation à réglementer, le NIST développe les standards, les techniques et la métrologie pour un large éventail de technologies.
Distribution électrique intelligente, dossiers médicaux électroniques, horloges atomiques, nanomatériaux avancés, puces informatiques, réseaux mondiaux de communication... de nombreux produits et services dépendent des travaux fournis par le NIST.
Sa mission : promouvoir l'innovation et la compétitivité industrielle des États-Unis, et améliorer la sécurité économique et la qualité de vie des citoyens et résidents du pays grâce au développement des standards, des technologies et, plus largement, de l'ensemble des techniques, indicateurs, méthodes et modèles relatifs à la métrologie. Le NIST se consacre principalement à la science de la mesure, à la traçabilité de haut niveau et au développement et à l'application de standards.

https://www.nist.gov/

Cryptographie post-quantique : enjeux d'avenir et standardisation

La révolution de l'information quantique est en cours et nul ne sait encore jusqu'où elle ira. La montée en puissance des ordinateurs quantiques et l'explosion de nos échanges de données implique que de nouveaux risques de sécurité pourraient apparaître. En effet, le développement d'un ordinateur quantique à grande échelle aurait le potentiel de décrypter les clés de sécurité les plus sophistiquées. Actuellement, la cryptographie est principalement basée sur des problèmes de théorie des nombres comme la factorisation. Les meilleurs algorithmes ont besoin de millions d'années pour factoriser un nombre de 600 chiffres ce qui offre d'importantes opportunités en matière de sécurité. Cependant, la mise au point d'un ordinateur quantique pourrait changer ce paradigme. Si les risques ne sont pas encore concrets, ils doivent être anticipés dès aujourd'hui.
La **cryptographie post-quantique** vise ainsi à anticiper ces risques et à concevoir des systèmes cryptographiques capables de résister aussi bien aux attaques des ordinateurs classiques qu'aux ordinateurs quantiques, tout en restant compatibles avec les protocoles et infrastructures existants.

1. Le projet

Le 11 mars, le NIST a annoncé la sélection de HQC comme second standard de chiffrement post-quantique, parmi les quatre schémas encore en lice (BIKE, HQC, Classic McEliece et SIKE).

HQC repose sur des codes correcteurs d'erreurs, une expertise de plus de 25 ans de l'équipe CRYPTIS de l'Institut Xlim et de l'institut de mathématiques de Bordeaux. Ce nouveau schéma de chiffrement post-quantique s'appuie sur des problèmes mathématiques différents de ML-KEM, l'autre algorithme standardisé pour l'échange de clés en 2022. Ainsi, si une faille était découverte dans ML-KEM, HQC pourrait prendre le relais et continuer à sécuriser nos données.

HQC a été conçu en se basant sur des familles d'algorithmes ayant fait l'objet de dépôts de brevets dès 2010 par les enseignants-chercheurs Philippe Gaborit et Carlos Aguilar-Melchor (Institut Xlim) et détenues conjointement par le CNRS et l'Université de Limoges, puis en collaboration avec l'université de Bordeaux et enfin développé en pratique avec une équipe internationale.

En juillet 2022, le NIST, le CNRS et l'Université de Limoges ont signé un accord de Licence permettant aux opérateurs et utilisateurs finaux des normes cryptographiques d'utiliser cette famille de brevets en cas de standardisation. Cet accord avait été signé afin de favoriser l'adoption rapide et généralisée de ces normes cryptographiques, un objectif commun du NIST et du CNRS.

La standardisation d'HQC constitue une importante reconnaissance du NIST qui témoigne de l'excellence et de la portée mondiale des travaux menés par les chercheurs de l'Institut Xlim, précurseurs en cryptographie post-quantique, et de l'Institut de mathématiques de Bordeaux à travers Gilles Zémor. Le projet a aussi été soutenu par NAQUIDIS une initiative de la région Nouvelle-Aquitaine pour développer les applications du quantique en région Nouvelle-Aquitaine.

Équipe projet (4e tour) :

- Coordinateur : Philippe Gaborit, Université de Limoges

- Carlos Aguilar Melchor, SandBox
- Nicolas Aragon, chercheur de l'Université de Limoges à l'Institut Xlim
- Slim Bettaieb, Technology Innovation Institute, UAE
- Loïc Bidoux, Technology Innovation Institute, UAE
- Olivier Blazy, chercheur de l'École Polytechnique au Laboratoire d'informatique de l'Ecole Polytechnique (CNRS/École Polytechnique)
- Jurjen Bos, Worldline (NL)
- Jean-Christophe Deneuville, ENAC, Université de Toulouse
- Arnaud Dion, ISAE-SUPAERO, Université de Toulouse
- Jérôme Lacan, ISAE-SUPAERO, Université de Toulouse

- Edoardo Persichetti, Florida Atlantic University (US)
- Jean-Marc Robert, chercheur de l'Université de Toulon à l'Institut de mathématiques de Toulon (Université de Toulon)
- Pascal Véron, chercheur de l'Université de Toulon à l'Institut de mathématiques de Toulon (Université de Toulon)
- Gilles Zémor, chercheur de l'université de Bordeaux à l'Institut de mathématiques de Bordeaux

2. Philippe Gaborit

Philippe Gaborit est Ingénieur des Mines de Saint-Etienne, il a obtenu un DEA en mathématiques à l'Université de Lyon puis un doctorat en mathématiques de l'université de Bordeaux, et une HDR en mathématiques à l'Université de Limoges. Il a effectué un post-doctorat à la University of Illinois, à Chicago, et est devenu maître de conférences au département de mathématiques de l'Université de Limoges. Depuis 2008, il est professeur au département d'informatique. Ses recherches portent sur la théorie des codes, la cryptographie, la cryptographie post-quantique, la sécurité et la théorie des nombres. Il est le directeur de 20 thèses soutenues ou en cours sur ces sujets.

« Il y a 25 ans, la thématique de l'ordinateur quantique et ses applications concrètes à la cryptanalyse des systèmes cryptographiques utilisés en pratique s'apparentait davantage à de la science-fiction qu'a un avenir proche »
explique Philippe Gaborit.

3. Médias

a. La Lettre d'Xlim, n°25, décembre 2022

FOCUS

CRYPTOGRAPHIE POST QUANTIQUE

Un accord de licence d'envergure avec le NIST (National Institute of Standards and Technology)

Indéniablement, la révolution de l'information quantique est en cours et nul ne sait encore jusqu'où elle ira. La montée en puissance des ordinateurs quantiques et l'explosion de nos échanges de données laisse supposer que de nouveaux risques de sécurité pourraient apparaître.

En effet, un ordinateur quantique aurait le potentiel de décrypter les clés de sécurité les plus sophistiquées. Si les risques ne sont pas encore concrets, ils doivent être anticipés dès aujourd'hui. Actuellement, la cryptographie est principalement basée sur des problèmes de théorie des nombres comme la factorisation. Les meilleurs algorithmes ont besoin de millions d'années pour factoriser un nombre de 600 chiffres ce qui offre d'importantes opportunités en matière de sécurité. Cependant, l'ordinateur quantique pourrait changer ce paradigme. Si on pouvait construire un ordinateur quantique suffisamment puissant avec assez de qubits (un équivalent quantique des bits des ordinateurs classiques) on pourrait casser facilement les systèmes cryptographiques utilisés actuellement.

Or, nous assistons à une course aux qubits. Si pendant des années le nombre de qubits pour un tel ordinateur a relativement stagné autour d'une dizaine de qubits, depuis plus de 5 ans les grands groupes comme Google, IBM, Microsoft, Intel aux Etats-Unis ou encore ATOS en Europe, se sont intéressés au sujet et le nombre de qubits a ainsi été multiplié par 10. Nous restons cependant encore très loin des milliers de qubits nécessaires pour casser les systèmes cryptographiques.

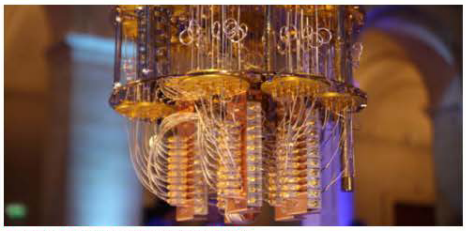

Figure 1 : Ordinateur quantique IBM

La cryptographie post-quantique, une branche de la cryptographie visant à garantir la sécurité de l'information face à un attaquant disposant d'un calculateur quantique, est ainsi devenue un sujet clé de recherche ces dernières années. Elle se distingue de la cryptographie quantique, qui vise à construire des algorithmes cryptographiques utilisant des propriétés physiques, plutôt que mathématiques, pour garantir la sécurité.

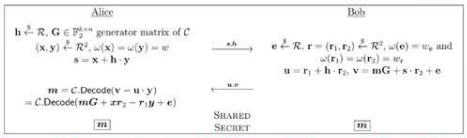

Figure 2 : Variante du protocole HQC pour l'échange de clés utilisée en cryptographie post-quantique

C'est dans ce contexte que le National Institute of Standards and Technology (NIST), agence gouvernementale américaine, a lancé en juillet 2016 un appel international à contribution afin d'identifier les meilleurs candidats aux futurs standards de cryptographie post-quantique, c'est-à-dire résistant aux ordinateurs quantiques de demain. Cet appel s'est structuré autour de trois grandes classes d'algorithmes : le chiffrement, l'échange de clés et la signature. Pour chacune de ces rubriques, l'idée est d'identifier plusieurs types d'alternatives possibles. Le concours a ainsi commencé en novembre 2017 et 82 soumissions ont été réalisées, dont 69 ont été recevables. Parmi ces 69 soumissions, 8 d'entre elles impliquent Philippe Gaborit, professeur à l'Université de Limoges et au sein du laboratoire XLIM, et ses collaborateurs.

L'équipe CRYPTIS bénéficie d'une expertise de plus de 25 ans sur les codes correcteurs d'erreurs au cœur des thématiques post-quantiques. « Il s'agit d'un fait extrêmement rare puisqu'il y a 25 ans, la thématique quantique s'apparentait davantage à de la science-fiction qu'a un avenir proche. » explique Philippe Gaborit.

Après plusieurs années d'analyse du niveau de sécurité et des performances des candidats, le NIST a standardisé dans une première phase quatre candidats. La solution Crystals-Kyber a été retenue pour le chiffrement et l'échange de clés, tandis que Crystals-Dilithium, Falcon et Sphincs+ ont été validés pour la signature. Deux des solutions finalistes s'appuient sur des familles de brevets déposées dès 2010 par les enseignants-chercheurs Philippe Gaborit et Carlos Aguilar-Melchor (Université de Limoges, XLIM), et détenues conjointement par le CNRS et l'Université de Limoges. Ainsi, le 5 juillet 2022, le NIST, le CNRS et l'Université de Limoges ont signé un accord de Licence. Grâce à lui, les opérateurs et les utilisateurs finaux des normes cryptographiques, dérivées des algorithmes PQC sélectionnés par le NIST, n'auront pas besoin d'obtenir une licence distincte sur la famille de brevets concernés du CNRS. Cela favorisera l'adoption rapide et généralisée de ces normes cryptographiques.

De plus, un prolongement de la campagne de standardisation est prévu pour quatre algorithmes : BIKE et HQC qui impliquent l'équipe CRYPTIS, Classic McEliece (tous trois fondés sur les codes correcteurs d'erreur) et SIKE (fondé sur les graphes d'isogénies de courbes elliptiques). En août dernier, SIKE a été craqué, seul trois candidats restent en compétition.

Enfin, cela a permis à l'équipe CRYPTIS d'associer une recherche fondamentale à une recherche plus appliquée en matière de cryptographie post-quantique. Ces activités sont soutenues par Naquidis qui vise à renforcer la thématique quantique en Nouvelle-Aquitaine. En outre, d'autres aspects sont également étudiés. Par exemple, des travaux sont menés sur les questions de protection de la vie privée par Cristina Onete et Olivier Ruatta (XLIM).

CONTACT
Philippe Gaborit- philippe.gaborit@xlim.fr

b. CNRS Innovation, 27 mars 2025

CNRS INNOVATION

Actualités | Expertise | Transfert | Prématuration | Rise | Open | PISE | Premat-Mat | Contact

← Retour aux actualités

Partager

QUANTIQUE

Le NIST standardise HQC : une avancée majeure pour la cybersécurité post-quantique

Publié le 27 mars 2025 | par Jonathan Rangapanaiken

Le National Institute of Standards and Technology (NIST) a annoncé la standardisation de l'algorithme HQC (Hamming Quasi-Cyclic), développé à l'origine par des chercheurs du laboratoire XLIM (CNRS/Université de Limoges) et de l'Institut de Mathématiques de Bordeaux (CNRS/Université de Bordeaux/Bordeaux INP). Cette décision marque une avancée stratégique pour la sécurité des communications numériques face aux menaces des futurs ordinateurs quantiques.

Anticiper la révolution quantique : un enjeu de cybersécurité

L'essor des ordinateurs quantiques pose un défi majeur à la cybersécurité. Ces machines, en exploitant les propriétés de la mécanique quantique, pourraient briser les protocoles de chiffrement classiques, mettant en péril la protection des données sensibles. Afin d'anticiper cette menace, le NIST a initié en 2017 un processus international de sélection des meilleurs algorithmes de cryptographie post-quantique, capables de résister aux attaques quantiques tout en restant compatibles avec les infrastructures existantes.

HQC : un standard complémentaire et robuste

Parmi les nombreuses propositions évaluées, le NIST avait déjà sélectionné en 2022 l'algorithme ML-KEM (anciennement Kyber) pour l'échange de clés. Désormais, HQC rejoint ce standard en tant que second schéma de chiffrement post-quantique.

HQC repose sur les codes correcteurs d'erreurs, une approche cryptographique différente de celle de ML-KEM, ce qui en fait une solution complémentaire. En cas de faille découverte dans l'un des standards, l'autre pourrait assurer la continuité de la sécurité des communications. Cette diversité algorithmique est essentielle pour garantir la robustesse des systèmes face aux cybermenaces futures. Cette décision vient clôturer un long processus de standardisation qui a débuté en 2017.

Une reconnaissance mondiale pour la recherche française

La standardisation de HQC souligne l'excellence de la recherche française en cryptographie. L'algorithme est le fruit de plus de 25 ans d'expertise développée par l'équipe CRYPTIS du laboratoire XLIM et l'Institut de Mathématiques de Bordeaux et se base sur un brevet déposé en 2010 par Philippe Gaborit et Carlos Aguilar de l'équipe CRYPTIS du laboratoire XLIM à l'université de Limoges.

Déjà en 2022, un accord de licence entre le NIST, le CNRS et l'Université de Limoges avait facilité l'intégration des brevets liés à la cryptographie post-quantique dans les standards internationaux. Cette nouvelle standardisation confirme le rôle central de la recherche française dans la sécurisation des infrastructures numériques de demain.

Un impact pour la sécurité numérique

Avec l'adoption officielle de HQC, les entreprises, institutions et gouvernements disposent désormais d'un standard cryptographique supplémentaire pour sécuriser leurs données à long terme. Ce nouveau jalon marque une étape clé dans la transition vers une cryptographie résistante aux attaques quantiques, garantissant ainsi la pérennité et la confidentialité des échanges numériques à l'échelle mondiale.

Source : https://www.cnrsinnovation.com/actualite/le-nist-standardise-hqc-une-avancee-majeure-pour-la-cybersecurite-post-quantique/

4. Présentation Xlim/Université de Limoges/CNRS

a. Xlim

Xlim (CNRS/Université de Limoges / Université de Poitiers) est un institut de recherche pluridisciplinaire qui regroupe plus de 470 personnes et localisé sur 5 sites géographiques à Limoges, Brive, Poitiers et Angoulême. L'institut possède un savoir-faire centré sur l'électronique et les hyperfréquences, l'optique et la photonique, les mathématiques, l'informatique et l'image, la cryptographie, la CAO, dans les domaines du spatial, des réseaux télécom, des environnements sécurisés, de la bio-ingénierie, des nouveaux matériaux, de l'énergie et de l'imagerie.

Xlim
123, avenue Albert Thomas - 87060 LIMOGES CEDEX
Tél. +33(0) 587 50 67 00 --
Site internet : https://www.xlim.fr/

b. Université de Limoges

Au cœur de l'Europe, l'Université de Limoges est un important pôle d'enseignement supérieur pluridisciplinaire, dans un environnement des plus propices à l'épanouissement scientifique. Ouverte, elle est un lieu foisonnant d'interactions, avec une population étudiante multiple, des structures d'accueil efficaces, des équipes proches, des formations fondées sur des recherches de très haut niveau et pour des débouchés bien identifiés. Son excellence scientifique, avec des laboratoires de pointe et des partenariats de grande envergure, contribue à inventer le monde de demain.

Université de Limoges
33 rue François Mitterrand - BP 23204 - 87032 Limoges – France
Tél. +33 (0)5 55 14 91 00
Site internet : https://www.unilim.fr/

c. CNRS

Acteur majeur de la recherche fondamentale à l'échelle mondiale, le Centre national de la recherche scientifique (CNRS) est le seul organisme français actif dans tous les domaines scientifiques. Sa position singulière de multi-spécialiste lui permet d'associer les différentes disciplines scientifiques pour éclairer et appréhender les défis du monde contemporain, en lien avec les acteurs publics et socio-économiques. Ensemble, les sciences se mettent au service d'un progrès durable qui bénéficie à toute la société.

Site internet : https://www.cnrs.fr/fr

5. PORTYQ : une entreprise en appui du projet

Philippe GABORIT, Nicolas ARAGON et Philippe BOUYER ont créé en 2025 la société PORTYQ, spécialisée dans les algorithmes résistants à l'ordinateur quantique (Cryptographie Post-Quantique, PQC).

Afin de défendre les entreprises contre les attaques actuelles et d'accompagner ses clients vers un niveau supérieur de conformité en cybersécurité, PORTYQ propose des services de conseil et de formation. Leurs services s'étendent de l'évaluation de l'infrastructure cryptographique actuelle à l'identification des vulnérabilités et à la recommandation de solutions quantiques sécurisées.

Équipe :

- Nicolas ARAGON (chercheur de l'Université de Limoges à l'Institut Xlim)
- Philippe BOUYER (chercheur du CNRS au Laboratoire Photonique, Numérique & Nanosciences)
- Philippe GABORIT (chercheur de l'Université de Limoges à l'Institut Xlim)
- Aurélien PISSELOUP (Entrepreneur)
- Michel SEYRAC (Entrepreneur)

Partenaires :

- Institut Optique Graduate School
- Université Paris Saclay
- Xlim
- CNRS
- Université de Limoges
- Naquidis Center
- Bpi France
- Région Nouvelle-Aquitaine
- Aquitaine Science Transfert
- Avrul
- Alienor Trasnfert

PORTYQ
1 avenue d'Ester - 87069 Limoges
06 11 29 31 33
contact@portyq.com
Site internet : https://portyq.com/

6. Master CRYPTIS

Fondé en 1986, le Master CRYPTIS est le plus ancien master de France en cryptologie et cybersécurité. Depuis sa création, plus de 1000 étudiants ont été formés sur le site de la Faculté des Sciences et Techniques de l'Université de Limoges, créant ainsi un important réseaux d'anciens étudiants.

L'équipe enseignante de ce master est constituée de chercheurs et de spécialistes du domaine reconnus internationalement. 20% de cours de M2 sont assurés par des professionnels reconnus dans leur domaine.

Le master CRYPTIS bénéficie d'un excellent taux d'insertion professionnelle des ses étudiants : 96% trouvent un emploi dans les deux mois suivant le stage, avec un salaire moyen 41k€ brut annuel (chiffres 2023).

Site internet : https://www.cryptis.fr/