COMMUNIQUÉ DE PRESSE

Accord de licence entre le NIST, le CNRS et l'Université de Limoges : le rayonnement international de l'excellence de la recherche française.

Le 5 juillet 2022, le NIST, le CNRS et l'Université de Limoges signent 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.

La sécurité de nos données et de nos échanges électroniques est aujourd'hui assurée grâce à des algorithmes de cryptographie robustes face aux attaques des meilleurs ordinateurs actuels. Cependant, le développement à venir de l'ordinateur quantique fait peser une menace sur la sécurité des systèmes de communication et d'authentification utilisés de manière généralisée dans notre vie quotidienne – sur le web et les réseaux mobiles, les cartes à puce, les documents d'identité, systèmes embarqués dans l'aéronautique, les transports, ou encore les objets connectés – imposant un changement de paradigme cryptographique.

Dans ce contexte, le *National Institute of Standards and Technology* (NIST), agence gouvernementale américaine, a lancé en juillet 2016 un appel international à contributions afin d'identifier les meilleurs candidats aux futurs standards de cryptographie post-quantique, c'est-à-dire résistant aux ordinateurs quantiques de demain.

L'analyse du niveau de sécurité et des performances des candidats a permis au NIST de retenir en phase finale quatre candidats permettant l'échange de clés cryptographiques. Il a été observé que deux des solutions finalistes pourraient s'appuyer sur des familles de brevets[1] déposées dès 2010 par les enseignants-chercheurs Philippe Gaborit et Carlos Aguilar-Melchor (Université de Limoges et laboratoire CNRS Xlim), et détenues conjointement par le CNRS et l'Université de Limoges.

Soucieux de l'intérêt général d'un processus de standardisation à vocation mondiale, le CNRS et l'Université de Limoges, soutenus par France Brevets, se sont entendus sur les termes d'un accord de licence dont les parties prenantes se félicitent. L'accord permet ainsi de valoriser une propriété intellectuelle issue des résultats de la recherche publique française.

Grâce à l'accord de licence annoncé entre le NIST, le CNRS et l'Université de Limoges, les opérateurs et les utilisateurs finaux des normes cryptographiques dérivées des algorithmes PQC sélectionnés n'auront pas besoin d'obtenir une licence distincte sur cette famille de brevets du CNRS. Cela favorisera l'adoption rapide et généralisée de ces normes cryptographiques, un objectif commun du NIST et du CNRS.

« Cet accord de licence, fruit d'un processus de concertation entre les parties prenantes impliquées, consacre au niveau mondial l'excellence de la recherche fondamentale française. Elle illustre tout particulièrement la qualité de l'école française en mathématiques et en cryptographie. » se réjouit Antoine Petit, Président-Directeur Général du CNRS.

[1] Notamment les brevets EP11712927.0 et US13/579682

« Nous sommes fiers que les chercheurs de notre Université contribuent à définir le futur de la sécurité numérique. L'équipe de recherche MATHIS du laboratoire XLIM confirme l'impact global de ses travaux en cryptographie post-quantique. » se félicite Isabelle Klock-Fontanille, Présidente de l'Université de Limoges.

« Le NIST est heureux de franchir cette étape importante dans la cryptographie post-quantique (PQC) et reconnaît que la participation et la coopération de partenaires internationaux comme celles du CNRS ont été importantes pour en assurer le succès », a déclaré Charles Romine, Directeur du laboratoire des technologies de l'information du NIST. *« Nous nous réjouissons de poursuivre nos travaux sur l'avenir du quantique, un sujet partagé sur lequel nous apprécions collaborer avec le CNRS. La méthode ouverte, transparente et inclusive que le NIST utilise pour standardiser les nouveaux algorithmes de cryptage profite à tous et cultive la confiance dans ces technologies. »*

Contacts presse :

CNRS - priscilla.dacher@cnrs.fr
NIST - charles.boutin@nist.gov
Université de Limoges - com@unilim.fr