PRESS RELEASE

License Agreement between the NIST, the CNRS and the University of Limoges: The International Impact of French Research Excellence

On July 5, 2022, the NIST, the CNRS and the University of Limoges signed a license agreement. As a result, implementers and end users of cryptographic standards derived from the selected PQC algorithms will not need a separate license under the CNRS patent family. This will promote the timely and widespread adoption of these cryptographic standards, a shared goal of NIST and the CNRS.

The security of our data and electronic communications is ensured by cryptographic algorithms that can resist attacks from today's best computers. However, the coming development of the quantum computer poses a security threat to the communication and authentication systems widely used in our everyday lives—on the web and mobile networks, chip-enabled cards, identity documents, onboard systems in aviation, transportation, and connected objects—subsequently imposing a change of cryptographic paradigm.

In this context, the National Institute of Standards and Technology (NIST), an American governmental agency, launched an international call for contributions in July 2016 to identify the best candidates for future post-quantum cryptography standards, in other words that are capable of resisting the quantum computers of the future.

After analysis of the security level and performance of the candidates, the NIST selected four of them for a final phase, enabling the exchange of cryptographic keys. It has been observed that two of the finalist solutions may be based on patent families[1] submitted in 2010 by the academics Philippe Gaborit and Carlos Aguilar-Melchor (University of Limoges and the joint research unit CNRS Xlim), and that are jointly held by the CNRS and the University of Limoges.

Concerned about the general interest of a global standardisation process, the CNRS and the University of Limoges agreed, with the support of France Brevets (an investment fund fully dedicated to patent promotion), on the terms of a license agreement that has been positively received by the stakeholders. The agreement promotes an intellectual property that emerged from results achieved by French public research.

As a result of the license agreement announced between NIST, the CNRS and the University of Limoges, implementers and end users of cryptographic standards derived from the selected PQC algorithms will not need a separate license under the CNRS patent family. This will promote the timely and widespread adoption of these cryptographic standards, a shared goal of NIST and the CNRS.

"This license agreement grew out of a consultation process between the stakeholders, and establishes the global excellence of French basic research. It especially illustrates the quality of the French school of mathematics and cryptography," enthuses CNRS Chairman and CEO Antoine Petit.

"*We feel proud that researchers from our University have been contributing to define the future of digital security. The MATHIS research team from the XLIM laboratory confirms the global impact of*

[1] Especially patents EP11712927.0 and US13/579682

their work in post-quantum cryptography." says Isabelle Klock-Fontanille, President of the University of Limoges.

"*NIST is pleased to achieve this milestone in post-quantum cryptography (PQC) and recognizes that the participation and cooperation of international partners, including the expertise from CNRS France, were important to this success,"* said Charles Romine, director of NIST's Information Technology Laboratory. *"We look forward to continued work in preparing for a quantum future and appreciate CNRS's collaboration in this achievement, in which we all share. The open, transparent and inclusive method that NIST is using to standardize new encryption algorithms benefits everyone and cultivates trust and confidence in these technologies.*"

Press contacts
CNRS: Priscilla.dacher@cnrs.fr
NIST: charles.boutin@nist.gov
University of Limoges: com@unilim.fr