Quand un brevet perturbe l'innovation postquantique

RECHERCHE - Le CNRS refuse de céder sa propriété intellectuelle sur un procédé cryptographique en lice dans un défi mondial de standardisation

A vouloir le beurre et l'argent du beurre, la recherche française pourrait n'avoir ni l'un ni l'autre. Une histoire compliquée de brevet, détenu par le CNRS, est en effet en train de perturber une compétition informatique majeure, au point de handicaper les chances de victoire de chercheurs nationaux, pourtant bien placés.

Cette compétition, organisée par le National Institute of Standards and Technology (NIST), l'organisme de référence américain de standardisation, doit garantir rien de moins que l'avenir de la sécurité des échanges électroniques, sur le Web, les mobiles, les cartes bancaires et autres cartes à puce. Autrement dit, toute la vie numérique sociale et économique.

Une menace plane en effet sur ces technologies utilisant des systèmes cryptographiques de chiffrement et d'authentification robustes pour payer, communiquer, accéder à des services... Jusque-là, ils semblaient solides car ils reposent sur des opérations mathématiques compliquées à réaliser. Par exemple, multiplier deux nombres premiers entre eux pour former un grand nombre est facile à calculer, mais faire l'inverse est difficile (opération dite « de factorisation »). Cette propriété garantit leur solidité, du moins avec les ordinateurs actuels. Or, de nouvelles machines, dites « quantiques », sont en cours de développement et pourraient factoriser plus rapidement, mettant à bas la précieuse sécurité. Des alternatives, déjà déployées, à l'opération de factorisation sont aussi menacées.

En décembre 2016, le NIST a donc lancé un défi à la communauté scientifique pour trouver des algorithmes « postquantiques » résistant à ces nouvelles machines. 82 propositions sont arrivées et la dernière étape de sélection est engagée depuis juillet 2020 pour sept finalistes. *« Nous ferons connaître nos choix fin 2021 ou début 2022 »*, explique Dustin Moody, le responsable de l'équipe de quinze personnes au NIST chargée de cette compétition.

Parmi les derniers finalistes, quatre projets concernent le chiffrement dit « à clé publique », dont deux impliquent des Français, et trois l'authentification, avec dans chacun d'eux des membres français. Un brevet du CNRS, déposé en 2010 et expirant en 2033, serait susceptible de s'appliquer à deux procédés de chiffrement, Saber (essentiellement de l'Université catholique de Louvain en Belgique) et Kyber, plus international avec trois membres français.

C'est de là que vient le problème. *« Ce brevet plombe notre candidature »*, estime Damien Stehlé de l'ENS Lyon, membre de Kyber. Comme lui, plusieurs collègues pensent en effet que, les différences techniques étant minces entre les candidats, c'est l'argument de la propriété intellectuelle qui ferait pencher la balance. *« En cryptographie, les brevets n'ont pas bonne réputation. Certains systèmes ont été brevetés et n'ont jamais servi. D'autres, comme le très connu AES, sorti de mon laboratoire, n'ont pas été brevetés et servent universellement »*, rappelle Frédérik Vercauteren, de l'université de Louvain et contributeur

Un jeu sérieux, Cryptris, réalisé par Kyber, finaliste de la compétition du NIST, destiné à expliquer le fonctionnement de leur algorithme de chiffrement. INRIA/DIGITAL CUISINE/CWI

de Saber. Le déploiement des procédés à base de courbes elliptiques, remplaçant déjà les systèmes de factorisation, a été retardé par des procédures juridiques liées aux brevets. Le très connu système RSA, pourtant breveté et très répandu, n'avait aucun concurrent. Pour éviter d'inévitables procédures juridiques freinant le déploiement, la meilleure option serait, pour le NIST, d'écarter Saber et Kyber...

Le CNRS ne partage pas cette analyse. *« La question des brevets n'est qu'un paramètre d'appréciation des mérites des candidats*, plaide Jean-Luc Moullet, directeur général délégué à l'innovation du CNRS. *C'est une pratique courante en sécurité informatique de déposer des brevets. Il n'est pas anormal qu'il y ait un juste retour de notre activité de recherche et que le CNRS obtienne des licences auprès de grandes entreprises américaines comme les GAFA. »* L'organisme de recherche espère clairement tirer des revenus de cette compétition. Il a ainsi officiellement abandonné toute revendication de son brevet pour les candidats « authentification », *« au regard des faibles perspectives d'exploitation »* sur ces derniers, précise au *Monde* l'organisme. En revanche, pour la partie chiffrement, le CNRS a proposé un taux de rémunération de 1 % du licensing de ce brevet, sans vouloir communiquer l'estimation des revenus potentiels.

« C'est indigne d'un organisme public, estime Mehdi Tibouchi, non-participant à la compétition, cryptographe chez l'opérateur télécoms japonais NTT. *Ce sera dommageable aux utilisateurs et à la communauté scientifique. » « Cela fait craindre que le mieux-disant technique, que j'estime être Kyber, risque d'être écarté. Cette histoire n'améliorera pas l'image du CNRS, qui devrait plutôt négocier l'affichage de la qualité de ses chercheurs, plutôt que de l'argent »*, défend Nicolas Sendrier, chercheur Inria, finaliste lui aussi mais non concerné par le brevet. *« Le CNRS est à côté de la plaque ! »*, tranche Léo Ducas, membre de Kyber, chercheur aux Pays-Bas dans l'organisme public de recherche en mathématiques et informatique CWI.

Un tiers dans l'affaire

La controverse réveille les anciennes querelles sur les finalités de la recherche. D'un côté valoriser financièrement des connaissances, de l'autre les rendre disponibles au plus grand nombre. *« Cette histoire de brevet pourrait saccager dix ans de travail ! »*, regrette Damien Stehlé, pour qui l'intérêt de gagner une telle compétition est de faire reconnaître le savoir-faire de la recherche française et européenne.

Plusieurs courriers pour informer la direction du CNRS de la situation ont été envoyés ou vont l'être, dont l'un, signé le 12 novembre par plus de 60 spécialistes qui y disent craindre que *« cette prise de position du CNRS ne ternisse durablement son image et celle de notre communauté, du fait de décisions stratégiques cruciales que nous subissons sans jamais avoir été consultés ni même informés »*.

« La situation est compliquée car le brevet est détenu par un tiers et non par les candidats. Nous sommes toujours en discussion avec le CNRS », rappelle Dustin Moody, qui reconnaît que ce serait mieux qu'il n'y ait pas de brevet car leur but est de standardiser une solution la plus adaptée aux besoins. Techniquement, mais aussi juridiquement. Or, rien ne dit que le brevet du CNRS s'applique bien à Saber et Kyber. *« Ce n'est pas applicable ! »*, insistent de concert Damien Stehlé et Frédérik Vercauteren. Le premier, avec un de ses collègues, a posté, le 8 octobre sur le forum du NIST consacré à la compétition, une analyse montrant pourquoi. Ironie de l'histoire, il a trouvé un argument de la « bouche » même du CNRS ! Depuis 2017, le brevet du CNRS est contesté par un cabinet d'avocats, Keltie, pour le compte d'un client dont l'identité n'a pas été divulguée. Le 26 octobre, le CNRS a eu gain de cause, mais sa défense a insisté sur le fait que le brevet concernait des procédés ayant une propriété mathématique particulière, qui n'est justement pas celle de Kyber et Saber. ■

DAVID LAROUSSERIE

Le Mexique dénonce le pillage de son patrimoine

ART PRÉCOLOMBIEN - La ministre mexicaine de la culture condamne la vente de 139 pièces par la maison Christie's, à Paris

MEXICO - *correspondance*

La mobilisation de cinq pays latino-américains n'a pas suffi. Mercredi 10 novembre à Paris, 139 pièces d'art précolombien et taïno ont été mises en vente par Christie's. La veille, le communiqué commun des ambassades de Colombie, du Guatemala, du Honduras, du Mexique et du Pérou réclamait pourtant l'annulation de l'événement, dénonçant le *« commerce illégal »* de leur patrimoine historique. Un combat culturel limité par la législation française, qui renvoie à la bonne volonté des collectionneurs.

« Ce genre de transaction encourage le pillage, le trafic illicite et le blanchiment des biens perpétrés par la délinquance organisée », fustige le communiqué des cinq ambassades à Paris. Les enchères se sont déroulées dans les très chics salons de Christie's, situés avenue Matignon, rapportant plus de 3 millions d'euros. Le clou de la vente était une hache maya de 34 cm, réalisée entre 200 et 600 au Mexique, représentant un homme contorsionné avec un serpent dans les bras. La pièce en roche métamorphique a été acquise pour 692 000 euros, soit trois fois son estimation initiale. 71 autres pièces mexicaines ont été mises aux enchères mercredi.

« Le patrimoine culturel n'est pas un objet commercial », déclarait au *Monde* la ministre de la culture mexicaine. Depuis octobre, son gouvernement réclamait l'annulation de la vente. *« Nous exigeons la restitution des pièces. Leur place est dans un musée, car elles représentent l'identité de nos civilisations anciennes, dont certaines sont encore bien vivantes aujourd'hui. »* Le Mexique compte 68 peuples indigènes, qui représentent environ 10 % de ses 126 millions d'habitants.

Casse-tête légal

« Ces ventes sont illégales », dénonce Alejandra Frausto, qui rappelle qu'une loi fédérale, votée en 1972, protège les pièces trouvées dans les zones archéologiques du Mexique. La ministre a adressé, en octobre et novembre, deux lettres à Christie's. *« Ils m'ont répondu que la vente respecte la loi française, qui reconnaît comme propriétaire celui qui possède le bien, favorisant le droit à la propriété au détriment de la protection du patrimoine culturel étranger »*, regrette-t-elle. En conséquence, c'est au justiciable de prouver le caractère illicite des pièces vendues. *« Or, c'est très difficile, avec le trafic illégal, d'identifier le moment de leur sortie du territoire mexicain. Sans compter que de nombreux collectionneurs ont acquis des œuvres avant notre loi de 1972. »*

Un casse-tête légal auquel s'est confronté Mexico à maintes reprises. Sa levée de boucliers, en 2019, contre deux ventes organisées par Millon et Sotheby's s'était aussi soldée par des échecs. Depuis, les déconvenues se multiplient. Paris et Mexico ont pourtant signé, le 1er juillet, une « déclaration d'intention pour le renforcement de la coopération contre le trafic illicite de biens culturels ». Et Alejandra Frausto d'expliquer : *« La déclaration qui renforce la vigilance des deux pays va dans le bon sens. Mais la démarche ne porte pas sur les pièces acquises dans le passé. »*

Pas de quoi décourager la ministre, qui a adressé, début novembre à Christie's, les conclusions d'une étude réalisée par les experts de l'Institut national d'anthropologie et d'histoire (INAH) mexicain. Sur les 87 pièces d'origine mexicaine mises aux enchères mercredi, quinze sont des faux, selon l'INAH. *« Ces ventes favorisent le marché des contrefaçons »*, avertit Alejandra Frausto, qui confie vouloir *« dissuader les acheteurs potentiels »*. Dix des quinze faux présumés ont trouvé acquéreur. En tête, cette représentation d'une chaise à porteurs sculptée de 37 cm de hauteur, présentée par Christie's comme issue de la civilisation Mezcala, dans le sud-est du Mexique, qui s'est vendue 93 750 euros. L'INAH assure pourtant que la pièce est de *« confection récente »*.

De son côté, Christie's indique *« consacrer des ressources considérables à la recherche de la provenance des œuvres proposées à la vente »*. Dans le cas de la vente du 10 novembre, *« ces vérifications ont été effectuées et nous n'avons aucune raison de penser que les biens proviennent d'une source illicite ou que leur vente serait contraire à la loi française »*.

La croisade menée à travers le monde par le gouvernement mexicain a permis de récupérer plus de 5 000 pièces historiques depuis trois ans. *« Mais, à la différence de l'Italie et de l'Allemagne, la France n'a pas rendu d'œuvres appartenant au Mexique »*, se désole la ministre. Les autorités italiennes ont même suspendu, en septembre, la mise aux enchères de 17 pièces préhispaniques. *« Face à une législation française qui nous défavorise, nous cherchons à réveiller les consciences des acheteurs et l'éthique des vendeurs »*, milite Alejandra Frausto. Un demi-échec pour la ministre, qui précise que *« seuls 17 des 26 lots mis aux enchères ce jour-là ont été vendus »*. ■

FRÉDÉRIC SALIBA ET HARRY BELLET