Communiqué de presse national **01/04/2026**

Sous embargo jusqu'au 01/04/2026, à 08h45 heure de Paris

Cryptographie sur ADN : une nouvelle approche franco-japonaise fait ses preuves

- Une équipe de scientifiques franco-japonais a développé une méthode cryptographique qui utilise l'ADN comme vecteur.
- L'ADN présente l'avantage de permettre la génération et le partage de grandes clefs aléatoires, indépendamment de la distance émetteur-récepteur.
- Cette méthode offre des garanties de sécurité que l'on pensait jusqu'ici réservées aux seules approches de cryptographies quantiques.

Utiliser l'ADN comme méthode pour crypter des messages sensibles devient possible. Une équipe pluridisciplinaire a développé une approche de chiffrement sur ADN permettant de générer et de partager des clés aléatoires pour coder des messages, et ce, quelle que soit la distance entre l'expéditeur et son destinataire. La démarche vient d'être testée pour la première fois en conditions réelles à l'occasion du déplacement du président de la République au Japon[1], le 1er avril 2026. Ces travaux ont été réalisés au sein d'une collaboration entre le CNRS[2], l'Université de Tokyo, l'Université de Limoges, IMT Atlantique et l'École supérieure de physique et de chimie industrielles de la ville de Paris (ESPCI Paris - PSL), avec le soutien de l'ANR et France 2030[3]. Ils font l'objet d'une prépublication sur une archive ouverte[4].

La protection des communications confidentielles, un enjeu majeur à l'ère du numérique

Aujourd'hui, le chiffrement des données sensibles repose principalement sur des méthodes dites « conditionnelles », dont la sécurité repose sur l'hypothèse qu'aucun acteur extérieur ne dispose d'une puissance de calcul suffisante pour briser le code. D'autres approches dites « inconditionnelles » existent cependant, comme le chiffrement de Vernam (ou méthode OTP - « *One-Time Pad* »)[5]. Bien qu'elle offre une sécurité parfaite, au sens où elle garantit que la sécurité ne dépend pas de la puissance de calcul d'un acteur adverse, cette approche impose plusieurs contraintes : la clé qui permet de chiffrer le message doit être partagée à l'avance entre l'expéditeur et le destinataire. Elle doit également être aussi longue que le contenu du message lui-même, utilisée une seule fois, et « parfaitement » aléatoire, c'est-à-dire impossible à prédire. Or, produire et partager de grandes clés aléatoires à usage unique reste très difficile avec les méthodes existantes, en particulier lorsque l'expéditeur et le destinataire sont séparés par des distances importantes.

L'ADN pour crypter des messages

C'est là que l'ADN devient intéressant. Chaque molécule d'ADN est composée de quatre bases chimiques (A, T, C et G), et les chimistes sont capables de synthétiser commercialement de longues chaines dont l'ordre des bases est statistiquement aléatoire. Ces séquences d'ADN peuvent ensuite être copiées à l'identique, à l'aide de processus enzymatiques, et ainsi partagées entre un expéditeur et un destinataire[6].

Concrètement, les scientifiques préparent des ensembles d'ADN dupliqués - d'origine entièrement synthétiques[5] -, dont une copie est conservée chez l'expéditeur et l'autre par le destinataire. Les fragments d'ADN qu'ils contiennent vont permettre aux correspondants de générer des clés de chiffrement parfaitement aléatoires, mais qui seront pourtant identiques 2 à 2. Ceci est réalisé juste avant la communication, grâce à de puissantes machines de séquençage, qui vont lire les molécules pour assembler une clé numérique binaire (composée de 0 et de 1) qui permet de coder, d'envoyer et de décoder un message allant jusqu'à plusieurs centaines de mégaoctets.

Une méthode fiable, sécurisée et performante même à longue distance

Les points forts de cette approche ? L'ADN présente une densité de stockage et une stabilité remarquable : correctement conservé, le polymère peut rester intact pendant des milliers d'années et il suffit de quelques milligrammes pour stocker des exaoctets d'information binaire, soit l'équivalent d'un million de disques durs. De plus, la génération de clés cryptographiques partagées via l'ADN a l'avantage d'être indépendante de la distance entre l'émetteur et le récepteur. Autrement dit, rien n'empêcherait d'utiliser cette méthode entre la Terre et la Lune - ou au-delà.

Mais surtout cette approche sur ADN rend plus accessible la seule méthode cryptographique dont on peut prouver mathématiquement qu'elle est à sécurité inconditionnelle, c'est-à-dire indépendante de la puissance de calcul d'un adversaire. En testant différents scénarios, les scientifiques ont démontré que même si l'ADN utilisé pour générer les clés était intercepté, le canal resterait inviolable : puisqu'il n'existe que deux copies de chaque séquence d'ADN, - une pour l'expéditeur et une pour le destinataire -, toute clé partiellement volée ne serait jamais réutilisée par les correspondants. De même, si l'intercepteur tentait d'amplifier la clé pour en obtenir plusieurs copies avant de la restituer aux utilisateurs, cette manipulation se traduirait par des anomalies dans le nombre de copies, détectables par les correspondants qui décideraient alors de ne plus utiliser ces clés.

Par ses différents atouts et sa fiabilité, cette approche ouvre de nouvelles perspectives pour la protection des communications les plus sensibles, qu'il s'agisse d'échanges diplomatiques, militaires ou scientifiques. À plus long terme, elle pourrait également trouver des applications dans des contextes extrêmes, notamment les communications spatiales ou les infrastructures numériques critiques où la fiabilité et l'inviolabilité des échanges constituent des enjeux majeurs.

Bibliographie

Synchronized DNA sources for unconditionally secure cryptography. Sandra Jaudou*, Hélène Gasnier*, Elias Boudjella*, Marc Canève, Victoria Bloquert, Vasily Shenshin, Tilio Pilet, Sacha Gaucher, Soo Hyeon Kim, Philippe Gaborit, Gouenou Coatrieux, Matthieu Labousse, Anthony Genot, and Yannick Rondelez. *contributions équivalentes

Lien HAL : https://hal.science/hal-05560338

Notes :

1- La démonstration se fera lors de la visite du Président au « Laboratory for Integrated Micro-Mechatronics Systems » (Université de Tokyo/CNRS) basé à Tokyo.
2- Du laboratoire Gulliver (CNRS/ESPCI PARIS – PSL). D'autres scientifiques du Laboratory for Integrated Micro-Mechatronic Systems (CNRS/Université de Tokyo) sont impliqués, dont l'un des porteurs du projet, Anthony

Genot, aujourd'hui décédé (https://www.insis.cnrs.fr/fr/cnrsinfo/hommage-anthony-genot-une-intelligence-en-resonance-avec-lavenir).

3- Dans le cadre du PEPR MoleculArXiv, piloté par le CNRS : https://pepr-molecularxiv.fr/ et du projet ANR DNA Sec, porté par IMT Atlantique.
4- https://hal.science/hal-05560338
Ces travaux n'ont pas encore été validés par une revue scientifique à comité de lecture.
5- Le chiffrement de Vernam, ou méthode « One-time pad » (OTP), est un système de chiffrement symétrique utilisant une clé aléatoire de même longueur que le message, utilisée une seule fois. Lorsqu'il est appliqué correctement, il offre une sécurité théoriquement parfaite, car le message chiffré ne révèle aucune information sans la clé.
6- L'ADN utilisé en cryptographie est issu d'un processus de fabrication synthétique qui s'inspire uniquement du principe de codage de l'ADN, sans aucun lien biologique, fonctionnel ou génétique avec l'ADN des organismes vivants.

Contacts :

Chercheur CNRS | Yannick Rondelez | yannick.rondelez@espci.fr

Chercheur CNRS | Matthieu Labousse | matthieu.labousse@espci.fr

Presse CNRS | Elisa Doré | T +33 1 44 96 53 16 | elisa.dore@cnrs.fr