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 Japon1, le 1er avril 2026. Ces travaux ont été réalisés au sein d'une collaboration entre le CNRS2, 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 20303. Ils font l'objet d'une prépublication sur une archive ouverte4.*

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 importante

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 destinataire6.

Concrètement, les scientifiques préparent des ensembles d'ADN dupliqués - d'origine entièrement synthétiques5 -, 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