

signature est un sous-ensemble de la clé privée dépendant du message. Pour vérifier la signature, on hache chacun de ses éléments et on vérifie qu'on obtient le bon sous-ensemble de la clé publique.

La signature de Lamport est simple à mettre en œuvre, mais elle ne peut être utilisée qu'une fois, pour des raisons de sécurité, car elle révèle une partie de la clé privée. Pour signer plusieurs messages, l'Américain Ralph Merkle a inventé ce qu'on nomme aujourd'hui des arbres de hachage, dans lesquels on passe d'un niveau à un autre en appliquant la fonction de hachage. Les arbres de hachage sont couramment utilisés : on les trouve dans la monnaie virtuelle bitcoin et dans les réseaux pair à pair, pour vérifier l'intégrité d'une partie d'un fichier par exemple.

Une autre approche est la cryptographie multivariable, développée dès 1988 sous l'impulsion de deux chercheurs japonais, Tsutomu Matsumoto et Hideki Imai. Elle repose sur la difficulté à résoudre des systèmes d'équations polynomiales à plusieurs inconnues. Au lycée, on apprend à résoudre une équation du second degré à une seule variable. Ce problème devient très difficile lorsque le nombre de variables et le nombre d'équations sont élevés.

Dans le cas d'une signature multivariable, la clé publique est un système d'équations polynomiales ; le message définit le second membre de ce système d'équations, et la signature d'un message n'est autre qu'une solution du système avec second membre. Ainsi, on vérifie la validité d'une signature en vérifiant qu'elle est bien solution du système. La cryptographie multivariable s'applique au chiffrement à clé publique et aux signatures numériques de façon assez efficace.

Cependant, l'inconvénient de cette méthode est que les systèmes d'équations utilisés ont des structures cachées qui, découvertes, constituent des brèches : de nombreux systèmes multivariables ont ainsi été cassés, à commencer par le système de Matsumoto-Imai, contre lequel Jacques Patarin, de l'université Versailles-Saint-Quentin-en-Yvelines, développa une attaque astucieuse en 1995. Un autre cas d'école est la signature numérique Sflash, conçue en 2001 par des chercheurs de la société Schlumberger, et recommandée par le projet européen NESSIE en 2003. Elle a été cassée en 2007 par les cryptographes Vivien Dubois, Pierre-Alain Fouque, Adi Shamir et Jacques Stern.

Enfin, la cryptographie à base de codes correcteurs et celle à base de réseaux reposent sur des problèmes assez voisins : filtrer du bruit. On cache un élément dans un code correcteur d'erreurs (des objets mathématiques très structurés) ou bien dans un réseau euclidien (un arrangement régulier de points dans l'espace à n dimensions) en lui ajoutant du bruit. Il est alors difficile de retrouver l'élément, c'est-à-dire d'enlever le bruit. Dans l'exemple des réseaux, l'élément est un point du réseau, et on le bruite en le déplaçant légèrement : quand la dimension augmente et que le réseau n'est pas trop particulier, il est très difficile de retrouver la perturbation. Cela permet de construire

L'Institut américain des normes et de la technologie a lancé un appel international pour normaliser ces algorithmes postquantiques

assez naturellement un chiffrement à clé publique : c'est ce qu'a fait Robert McEliece dès la fin des années 1970 pour les codes correcteurs. Fondé sur la même idée, le chiffrement à base de réseaux NTRU est peut-être le chiffrement à clé publique le plus rapide du monde.

Malgré leurs similitudes, les codes correcteurs et les réseaux euclidiens ont des différences significatives. Par exemple, on connaît des signatures à base de réseaux très efficaces, contrairement au cas des codes correcteurs. Et les réseaux euclidiens offrent des fonctionnalités que n'a pas la cryptographie traditionnelle : on peut citer le cas du chiffrement complètement homomorphe, qui permet d'effectuer des opérations arbitraires sur des données chiffrées sans que l'on connaisse la clé secrète. Pour toutes ces raisons, la cryptographie à base de réseaux est la méthode postquantique la plus étudiée à l'heure actuelle.

Ces quatre approches postquantiques ont des avantages et des défauts. En février 2016, le NIST (l'Institut américain des normes et de la technologie) a lancé un appel international pour normaliser ces méthodes postquantiques. Cette initiative permettra peut-être de déterminer l'approche la plus adaptée pour remplacer les systèmes de cryptographie à clé publique utilisés aujourd'hui, tel RSA. ■

■ L'AUTEUR



Phong NGUYEN est directeur de recherche à l'Inria et dirige le laboratoire franco-japonais d'informatique du CNRS.

■ BIBLIOGRAPHIE

National Institute of Standards and Technology, **Report on Post-Quantum Cryptography**, Internal Report 8105, 2016.

P. Q. Nguyen et B. Vallée (éd.), **The LLL Algorithm, Survey and Applications**, Springer, 2010.

D. J. Bernstein et al. (éd.), **Post-Quantum Cryptography**, Springer, 2009.

P. Nguyen, **La géométrie des nombres : de Gauss aux codes secrets**, *Dossier Pour la Science*, n° 36, juillet-octobre 2002.





Pourquoi les acteurs nous font vibrer

Gabriele Sofia

Les scientifiques ont montré que lorsque nous regardons un spectacle, notre cerveau et notre corps réagissent d'une façon bien particulière. Nous irions même jusqu'à simuler les actions représentées...

L'ESSENTIEL

■ Des chercheurs ont effectué diverses mesures physiologiques sur des spectateurs pendant qu'ils regardaient une pièce de théâtre ou un spectacle de danse.

■ Ils ont montré que des zones cérébrales essentielles pour comprendre les personnages et l'histoire s'activaient. Leurs résultats suggèrent aussi que le système psychomoteur des spectateurs simule les actions représentées.

■ Cette « résonance physiologique » serait plus intense quand on assiste au spectacle au lieu de le regarder en vidéo.

© Daniel Koehn/Corbis

Avec la découverte des neurones miroirs, les neurosciences commencent à comprendre ce que le théâtre sait depuis toujours ! C'est par cette citation du metteur en scène Peter Brook que débute l'ouvrage intitulé *Les Neurones miroirs*, publié en 2006. Ce livre, écrit par le philosophe Corrado Sinigaglia, de l'université de Milan, et le neuroscientifique Giacomo Rizzolatti, de l'université de Parme, est le premier à décrire ces étonnants neurones qui s'activent de la même façon quand on réalise une action et quand on la regarde faire.

La découverte des neurones miroirs, il y a une vingtaine d'années, a eu un retentissement considérable chez les scientifiques, soulevant de multiples questions et inspirant de nombreuses recherches : ont-ils joué un rôle dans l'apparition du langage ? Sont-ils impliqués dans des troubles tels que la schizophrénie et l'autisme ? Pourrait-on s'en servir pour restaurer des fonctions motrices chez des personnes atteintes de neuropathies ?

Dans le monde du spectacle aussi, ces neurones ont suscité de l'intérêt. Car « ce que le théâtre sait depuis toujours », c'est que chaque action réalisée sur scène a une résonance physique chez le spectateur. En passant au crible le cerveau et le corps de personnes en train de regarder des spectacles de théâtre ou de danse, les

neuroscientifiques ont effectivement trouvé la trace de cette résonance, qui reposerait sur les neurones miroirs, donc, mais aussi sur d'autres mécanismes cérébraux. Les chercheurs commencent ainsi à comprendre pourquoi ces spectacles nous bouleversent.

Quand le spectacle hypnotise

En 2010, Marie-Noëlle Metz-Lutz, de l'Inserm, et ses collègues ont réalisé une étude pionnière, en collaboration avec le Théâtre national de Strasbourg. Les participants étaient allongés dans un appareil d'imagerie par résonance magnétique fonctionnelle (IRMf), tandis qu'ils regardaient une vidéo d'une pièce de théâtre grâce à des lunettes spéciales. Les chercheurs ont montré que plusieurs aires cérébrales particulières s'activaient alors, notamment celles associées à l'empathie et à la théorie de l'esprit (la capacité de se mettre à la place de l'autre), de même que celles associées à la compréhension des métaphores (voir la figure page 41). Ainsi, les spectateurs s'imaginent à la place des personnages, partageant leurs émotions et leurs pensées, et cela se voit dans leur cerveau.

Plus étonnant, l'équipe de Marie-Noëlle Metz-Lutz a observé une baisse de l'activité du précunéus, une zone cérébrale intervenant dans la conscience de soi. Or

L'AUTEUR



Gabriele SOFIA est attaché temporaire d'enseignement et de recherche au département de cinéma

et théâtre de l'université Paul-Valéry, Montpellier 3. Il a coordonné le colloque « Dialogue entre théâtre et neurosciences », de 2009 à 2013, à l'université La Sapienza, à Rome.

on constate aussi cette baisse dans les états d'hypnose et entraînerait une déconnexion des sensations corporelles. Le spectateur serait ainsi tout entier dans le spectacle, au point qu'il s'oublierait lui-même !

Les neurones miroirs accentueraient encore cette immersion dans un film ou une pièce de théâtre, car grâce à eux notre système psychomoteur simule en permanence les actions observées. Ces neurones ont d'abord été découverts par l'équipe de Giacomo Rizzolatti chez des singes, dans le cortex prémoteur, une zone cérébrale qui planifie les mouvements. Des électrodes implantées dans le cerveau des animaux ont révélé que certaines cellules nerveuses – les neurones miroirs – s'activaient de façon similaire quand l'animal prenait un fruit et quand il voyait quelqu'un le prendre.

Par la suite, des expériences d'imagerie cérébrale ont suggéré l'existence de neurones semblables chez l'homme. Cela a été confirmé en 2010. Lors d'expériences du même type, Roy Mukamel, alors à l'université de Californie à Los Angeles (UCLA), et ses collègues ont mesuré l'activité de

plus de 1000 neurones dans le cerveau de 21 patients épileptiques, à qui on avait implanté des électrodes afin de repérer la zone d'où partaient leurs crises. Plusieurs dizaines d'entre eux étaient des neurones miroirs.

Un ballet au bout des doigts

Ces découvertes ne pouvaient qu'inspirer les neuroscientifiques qui s'intéressent au théâtre. Plusieurs équipes ont alors supposé que lorsque nous observons les acteurs, nos neurones miroirs s'activent comme si nous réalisions les mêmes actions, ce qui entraînerait l'envoi de commandes motrices aux muscles. Des neurones spécifiques de la moelle épinière inhiberaient ensuite ces commandes. Les muscles seraient tout de même animés de microcontractions, invisibles à l'œil nu, mais détectables avec des appareils appropriés.

Les chercheurs n'ont pas mesuré directement l'activité des neurones miroirs des spectateurs ni les microcontractions



SE FORMER À L'UPMC C'EST CONSTRUIRE ET PENSER ENSEMBLE VOTRE AVENIR

FAÎTES LE CHOIX DE L'EXCELLENCE

UPMC : UNIVERSITÉ DE RECHERCHE
SCIENTIFIQUE ET MÉDICALE

Une offre complète qui s'adapte à vos besoins

- > Formations qualifiantes inter entreprises
- > Prestations sur mesure, formations intra entreprises
- > Parcours individualisés
- > Accompagnement à la mise en oeuvre de la VAE individuelle ou collective

www.fc.upmc.fr

UPMC
SORBONNE UNIVERSITÉS



SANTÉ

ÉCOLOGIE - BIODIVERSITÉ

CHIMIE ÉLECTRONIQUE

BIOLOGIE

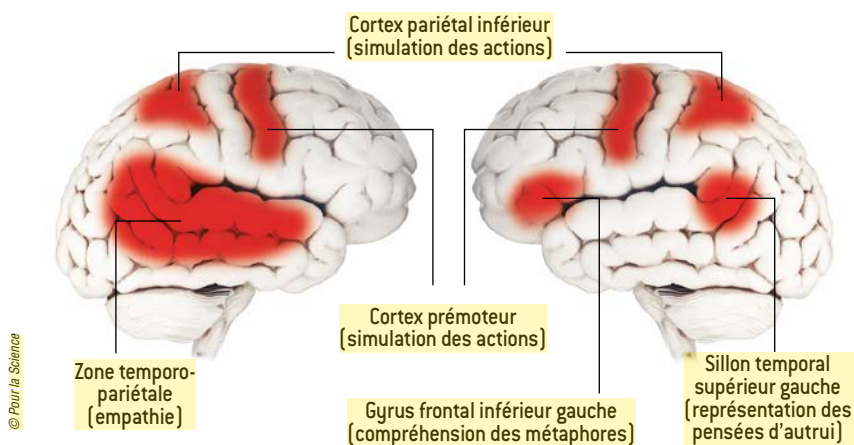
MÉCANIQUE

MATHÉMATIQUES

INFORMATIQUE

Formation continue
Université Pierre & Marie Curie
«Créateur de futurs»

formation.continue@upmc.fr
01 44 27 82 82



DANS LE CERVEAU DU SPECTATEUR, des zones bien particulières s'activent. Ces zones interviennent dans la compréhension des métaphores, l'empathie, la capacité à imaginer ce que pense l'autre. Parallèlement, le précunéus (sur la face médiane du cerveau, non visible sur ces représentations) se désactive en partie, ce qui provoquerait une déconnexion des sensations corporelles. En outre, le spectateur simule mentalement les actions observées grâce à des neurones dits miroirs. Ceux-ci sont situés à divers endroits du cerveau, notamment dans le cortex prémoteur, responsable de la planification des mouvements, et le cortex pariétal inférieur.

musculaires, mais ils ont tout de même observé cette mobilisation de leur système psychomoteur lors d'un spectacle.

Si ces expériences concernaient le domaine de la danse, leurs conclusions sont probablement aussi valables pour le théâtre ou le cinéma. En 2013, Corinne Jola, de l'université d'Abertay en Écosse, a ainsi étudié des sujets qui soit visionnaient un ballet en vidéo, soit y assistaient. Elle a utilisé une technique indirecte, fondée sur la stimulation magnétique transcrânienne, pour évaluer à quel point les spectateurs mobilisaient leur système psychomoteur. Quand une impulsion magnétique est envoyée dans certaines zones cérébrales, le sujet a un léger mouvement rythmique du doigt ou du bras. Or ce rythme change lorsque d'autres phénomènes activent le système psychomoteur. Si ce système simule les actions observées sur scène, on doit donc détecter une telle variation de rythme.

Et c'est bien ce que l'expérience a révélé. Elle a aussi fourni un second résultat intéressant : le rythme a beaucoup plus varié chez les spectateurs présents dans la salle que chez ceux qui ont regardé le spectacle en vidéo, signe que dans le premier cas, le système psychomoteur s'engageait de façon plus intense dans la simulation des actions. Cette résonance particulièrement forte dans le cadre du spectacle vivant est peut-être due à la quantité supérieure d'informations captées par le spectateur quand il est dans la salle : il perçoit alors

Quand le spectateur est dans la salle, il réagit plus intensément, peut-être parce qu'il capte davantage d'informations sur le corps du comédien et la profondeur de l'espace

davantage la posture, l'engagement de tout le corps dans une action, la profondeur de l'espace où se meut le comédien... Bien sûr, le cinéma a d'autres armes, par exemple les gros plans : ces derniers montrent au spectateur des détails difficiles à percevoir au théâtre, tels les mouvements des yeux, ce qui suscite sans doute aussi des réponses physiologiques particulières.

Certaines études suggèrent que pour bien faire « résonner » le cerveau des spectateurs, l'acteur doit construire des intentions précises pour chacune de ses actions – c'est d'ailleurs ce que demandent nombre d'écoles de théâtre, appliquant en cela les théories élaborées par le metteur en scène russe Constantin Stanislavski il y a plus d'un demi-siècle. Dans les expériences de Giacomo Rizzolatti, par exemple, tantôt le chercheur saisissait un fruit placé derrière un écran, tantôt il ne faisait que mimer le geste, aucun fruit n'étant présent. Or les neurones miroirs du singe ne s'activaient que dans le premier cas. En d'autres termes, en l'absence d'intention réelle (comme dans le second cas), ils ne s'activaient pas. Peut-être un acteur professionnel, qui aurait gardé en tête l'objectif de saisir un fruit lorsqu'il mimait le geste, aurait-il été capable d'activer les neurones miroirs du singe...

Les neurones miroirs constituent en tout cas un système très fin de discrimination des intentions – une capacité précieuse pour les animaux sociaux que nous sommes. Des expériences menées par le neurobiologiste Marco Iacoboni, de l'UCLA, en collaboration avec l'équipe de Giacomo Rizzolatti, ont ainsi révélé que lorsque nous voyons une personne saisir une tasse, des neurones miroirs différents s'activent selon que cette personne veut boire ou juste la ranger. C'est ce qui nous rend capables de comprendre son intention, immédiatement et de façon inconsciente.

Les différences d'activation des neurones miroirs résultent d'infimes nuances dans les routines motrices mises en jeu par celui qui effectue l'action – si infimes qu'il est probablement impossible de les planifier consciemment, d'où l'importance des intentions pour un acteur. Quand le personnage souhaite ranger une tasse, par exemple, le comédien qui le joue doit vraiment avoir cette intention en tête, et ce même s'il sait qu'un partenaire l'arrêtera dès qu'il aura posé la main sur l'objet.