

P. 24
MÉDECINE

UNE NOUVELLE VISION DE L'AUTO-IMMUNITÉ

Stephani Sutherland

À propos des maladies auto-immunes, le coupable a longtemps été tout désigné : un système immunitaire détraqué. On s'aperçoit qu'il ne constitue qu'une partie de l'équation.

P. 34
MÉDECINE

LES FEMMES SUREXPOSÉES?

Melinda Wenner Moyer

Près de quatre personnes sur cinq atteintes de troubles auto-immuns sont des femmes. Pourquoi une telle disproportion? Une explication serait à chercher du côté de l'histoire évolutive de la grossesse.

P. 40
IMMUNOLOGIE

« IL Y A UN FORT PARALLÈLE ENTRE AUTO-IMMUNITÉ ET CANCER »

Entretien avec Frédéric Rieux-Laucat

Malgré la complexité et la multiplicité des maladies auto-immunes, on commence à percevoir certains points communs entre ces pathologies, voire avec d'autres comme le cancer et le Covid-19.

P. 80
LOGIQUE & CALCUL
DES SUITES FRACTALES D'ENTIERS

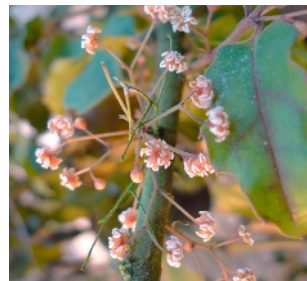
Jean-Paul Delahaye

Une suite numérique fractale est une suite de nombres dont une partie la reproduit entièrement. La construction de tels objets stimule la créativité de nombreux passionnés.

P. 86
ART & SCIENCE
Un climat photogénique
Loïc Mangin

P. 88
IDÉES DE PHYSIQUE
Oxygène à gogo
Jean-Michel Courty
et Édouard Kierlik

P. 92
CHRONIQUES
DE L'ÉVOLUTION
À la recherche
de la fleur ancestrale
Hervé Le Guyader



P. 96
SCIENCE & GASTRONOMIE
Comment faire briller
le chocolat
Hervé This

P. 98
À PICORER

A

CTUALITÉS

P.6 Échos des labos

P.18 Livres du mois

P.20 Disputes environnementales

P.22 Les sciences à la loupe

DES RETRAITS SÉCURISÉS GRÂCE À LA RELATIVITÉ RESTREINTE

Quand, lors d'un retrait d'argent au distributeur, on entre son code secret, il y a un risque de se le faire voler. Mais grâce à un protocole sécurisé, il est possible de s'authentifier sans dévoiler d'information exploitable par un fraudeur.



Comment confirmer votre identité à un distributeur de billets sans taper votre code secret ? Un protocole sécurisé, reposant sur la relativité restreinte, a été mis en œuvre.

Quand vous retirez de l'argent à un distributeur, vous devez taper un code secret pour confirmer votre identité. Cette opération est un point faible du système. De toute évidence, vous devez entrer votre code à l'abri de regards indiscrets. Mais plus difficiles à détecter, certains escrocs équipent des distributeurs de faux claviers ou de faux lecteurs de cartes qui enregistrent toutes vos informations. Existe-t-il une solution pour sécuriser cette étape d'identification ? En 1985, Shafi Goldwasser, du MIT, et ses collègues ont introduit le concept de preuve à divulgation nulle de connaissance. Dans

le cas du distributeur, ce protocole permet de confirmer votre identité sans révéler d'informations (votre code secret) qu'un tiers mal intentionné pourrait exploiter, mais, pour des raisons techniques, il était difficile de le mettre en œuvre. Cependant, Sébastien Designolle, avec ses collègues de l'université de Genève et de l'université McGill à Montréal, vient d'en faire une démonstration concrète en s'appuyant sur la relativité restreinte.

En quoi consiste une preuve à divulgation nulle de connaissance ? Imaginez que vous ayez inventé une machine révolutionnaire et que vous craigniez qu'on vous vole vos idées. Comment prouver à autrui que vous avez bien construit l'objet

sans en révéler les détails ? C'est là qu'intervient la preuve à divulgation nulle de connaissance. Elle consiste en un « fournisseur de preuve » et un « vérificateur ». Ce dernier, grâce à un jeu de questions-réponses, s'assure que le fournisseur de preuve a bien en sa possession ce qu'il affirme. Mais à la fin, le vérificateur n'a aucun détail sur la machine à part la garantie qu'elle existe.

La plupart des protocoles conventionnels de preuve à divulgation nulle d'information impliquent de résoudre des problèmes mathématiques difficiles telle la décomposition de grands nombres en leurs facteurs premiers. La robustesse du système dépend donc de la puissance des ordinateurs utilisés pour élucider le problème mathématique. Or les progrès techniques peuvent mettre en péril ces approches. En 1988, Avi Wigderson, à l'institut des études avancées de Princeton, et ses collègues ont montré