

■ POUR LA

SCIENCE

Juin 2016 - n° 464

science.fr

Édition française de Scientific American



La cryptographie quantique

un système
garanti sans failles ?



POUR LA SCIENCE

www.pourlascience.fr

8 rue Férou - 75278 Paris Cedex 06

Groupe POUR LA SCIENCE

Directrice des rédactions : Cécile Lestienne

Pour la Science

Rédacteur en chef : Maurice Mashaal

Rédactrice en chef adjointe : Marie-Neige Cordonnier

Rédacteurs : François Savatier, Philippe Ribeau-Gésippe, Guillaume Jacquemont, Sean Bailly

Dossier Pour la Science

Rédacteur en chef adjoint : Loïc Mangin

Développement numérique : Philippe Ribeau-Gésippe, assisté de Alice Maestracci

Directrice artistique : Céline Lapet

Maquette : Pauline Bilbault, Raphaël Queruel, Ingrid Leroy

Correction et assistance administrative : Anne-Rozenn Jouble

Marketing & diffusion : Laurence Hay et Ophélie Maillet, assistées de Marie Chaudy

Direction financière et direction du personnel : Marc Laumet

Fabrication : Marianne Sigogne et Olivier Lacam

Directrice de la publication et Gérante : Sylvie Marcé

Anciens directeurs de la rédaction : Françoise Pétry

et Philippe Boulanger

Conseiller scientifique : Hervé This

Ont également participé à ce numéro :

Denis Auroux, Razvan Caracas, Renaud Coulangeon,

Catherine Hordelalay, Anne Dambricourt-Malassé,

Uwe Meierhenrich, Jean-Jacques Perrier, Christophe Pichon,

Daniel da Rocha, Françoise Roques, Daniel Tacquenet

PRESSE ET COMMUNICATION

Susan Mackie

susan.mackie@pourlascience.fr - Tel. : 01 55 42 85 05

PUBLICITÉ France

Directeur de la Publicité : Jean-François Guillotin

jf.guillotin@pourlascience.fr

Tél. : 01 55 42 84 28 • Fax : 01 43 25 18 29

ABONNEMENTS

Abonnement en ligne : <http://boutique.pourlascience.fr>

Courriel : pourlascience@abopress.fr

Téléphone : 03 67 07 98 17

Adresse postale : Service des abonnements - Pour la Science, 19 rue de l'Industrie, BP 90053, 67402 Illkirch Cedex

Tarifs d'abonnement 1 an - 12 numéros

France métropolitaine : 59 euros - Europe : 71 euros

Reste du monde : 85,25 euros

COMMANDES DE LIVRES OU DE MAGAZINES

Pour la Science

628 avenue du Grain d'Or, 41350 Vineuil

pourlasciencevpc@daudin.fr • Tél. : 02 18 54 12 64

DIFFUSION

Contact kiosques : À Juste Titres ; Benjamin Boutonnet

Tel : 04 88 15 12 41

Information/modification de service/réassort :

www.direct-editeurs.fr

SCIENTIFIC AMERICAN

Editor in chief : Mariette DiChristina.

Executive editor : Fred Gutel. Design director : Michael Mrak. Editors :

Ricky Rusting, Philip Yam, Robin Lloyd, Mark Fischetti, Seth Fletcher,

Christine Gorman, Michael Moyer, Gary Stix, Kate Wong.

President : Keith McAllister. Executive Vice President : Michael Florek.

Toutes demandes d'autorisation de reproduire, pour le public français ou francophone, les textes, les photos, les dessins ou les documents contenus dans la revue « Pour la Science », dans la revue « Scientific American », dans les livres édités par « Pour la Science » doivent être adressées par écrit à « Pour la Science S.A.R.L. », 8 rue Férou, 75278 Paris Cedex 06.

© Pour la Science S.A.R.L. Tous droits de reproduction, de traduction, d'adaptation et de représentation réservés pour tous les pays. La marque et le nom commercial « Scientific American » sont la propriété de Scientific American, Inc. Licence accordée à « Pour la Science S.A.R.L. ».

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement la présente revue sans autorisation de l'éditeur ou du Centre français de l'exploitation du droit de copie [20 rue des Grands-Augustins - 75006 Paris].



Maurice Mashaal
rédacteur en chef

Protection quantique

Après avoir marqué la science du XX^e siècle, la physique quantique est bien partie pour marquer aussi le XXI^e. C'est notamment le cas dans le domaine de la protection des données, grâce à l'avènement ces deux dernières décennies d'une « ingénierie quantique », où l'on manipule finement les états quantiques d'atomes ou de photons.

Les méthodes actuelles utilisées pour chiffrer et ainsi protéger des données ou un message doivent leur sécurité au principe suivant : une personne indiscreète ne disposant pas de la clé de décryptage aurait à effectuer des calculs trop volumineux pour qu'elle puisse déchiffrer en temps utile l'information interceptée.

Or ce principe de protection, qui sécurise notamment nos transactions bancaires, est menacé par l'ordinateur quantique, une machine encore hypothétique dont les capacités de calcul dépasseraient de beaucoup celles des ordinateurs classiques.

La cryptographie quantique, un antidote à l'éventuel ordinateur quantique

L'antidote existe cependant : la cryptographie quantique, qui utilise des états d'atomes ou de photons pour communiquer une clé secrète – l'avantage étant que, en vertu des lois quantiques, toute interception serait détectable. Les théoriciens ont même récemment montré que de telles procédures peuvent garantir une sécurité parfaite, que l'adversaire ait ou non un ordinateur quantique [voir pages 26 à 35]. Ces techniques restent toutefois difficiles à mettre en pratique. C'est pourquoi les chercheurs explorent aussi des procédés de chiffrement novateurs, mais non quantiques [voir pages 36-37].

Il en va de la protection de la vie privée et des communications de tous les individus – qu'ils soient honnêtes ou, hélas, malfaisants. Les écoutes illégales, le bras de fer entre Apple et le FBI à propos de l'accès aux données des téléphones et bien d'autres affaires ont montré combien l'enjeu est grand et d'actualité. ■

3 **Édito**

Actualités

- 6 **Savez-vous empiler des oranges en dimension 8 ?**
- 7 **Perturbateurs endocriniens : un flou entretenu**
- 8 **Un bassin féminin de taille modulable**



- 9 **Un élément clé de l'ARN formé sur les comètes ?**
- 11 **Catalyser avec un champ électrostatique**

Retrouvez plus d'actualités sur www.pourlascience.fr

Réflexions & débats

- 14 **Éclairage**
L'Afrique le pied à l'étrier de la science ?
Maurice Mashaal
- 16 **Entretien**
Nouveaux OGM : « Le débat est manipulé »
Yves Bertheau
- 20 **Cabinet de curiosités sociologiques**
Les vertus du canular
Gérald Bronner
- 22 **Homo sapiens informaticus**
La résurrection de l'imparfait du subjonctif
Gilles Dowek
- 24 **Lu sur SciLogs.fr**
La fraude fiscale, une histoire vieille comme le monde
Cécile Michel

Ce numéro comporte deux encarts d'abonnement
Pour la Science brochés sur la totalité du tirage.
En couverture : ©Alex Mit/Shutterstock.com

À LA UNE

26 CRYPTOGRAPHIE

Comment la physique quantique protégera notre vie privée

Artur Ekert et Renato Renner

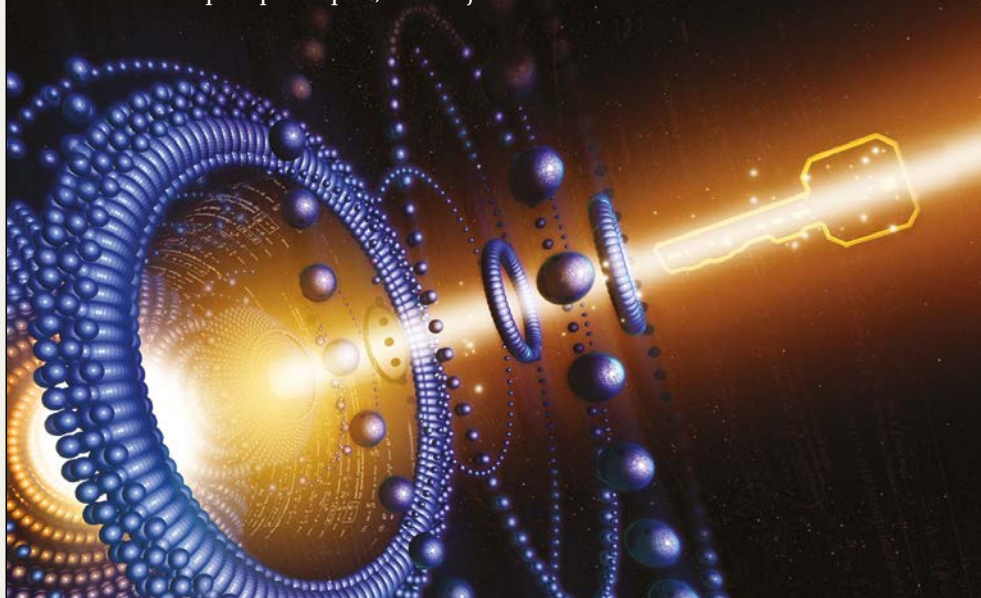
Les méthodes de chiffrement actuelles ne sont pas aussi fiables qu'on le pense. Comment alors protéger nos données et nos communications ? Des recherches récentes montrent que la cryptographie quantique offre des solutions robustes.

36 INFORMATIQUE

La cryptographie de demain

Phong Nguyen

La cryptographie à clé publique utilisée aujourd'hui sera obsolète si l'ordinateur quantique devient une réalité. Toutefois, des méthodes alternatives, dites postquantiques, sont déjà à l'étude.



38 NEUROSCIENCES

Pourquoi les acteurs nous font vibrer

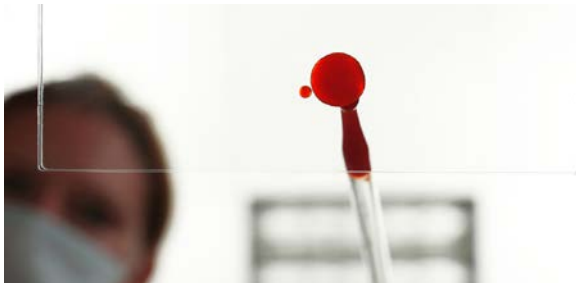
Gabriele Sofia

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...

44 MÉDECINE Une prise de sang contre les cancers

François-Clément Bidard et Stéphanie Descroix

Grâce à la microfluidique – la manipulation des fluides à l'échelle microscopique –, on sait détecter des cellules cancéreuses et de l'ADN tumoral lors d'une simple prise de sang. D'ici quelques années, ces techniques devraient remplacer la biopsie des tumeurs.



52 ASTRONOMIE Une exoplanète aux anneaux géants

Matthew Kenworthy

Des astronomes ont découvert, autour d'une lointaine étoile, une planète dotée d'un immense système d'anneaux, et peut-être une lune.



60 PALÉONTOLOGIE HUMAINE L'incroyable *Homo naledi*

Kate Wong

Petite, le cerveau gros comme une orange, à la fois primitive et proche de nous, une espèce humaine mise au jour en 2013 agite le milieu des paléanthropologues.

70 HISTOIRE DES SCIENCES Comment la mouche a perdu son aile... et la Russie sa découverte

Stéphane Schmitt

La découverte, il y a un siècle, de mutations transformant un organe en un autre a mis deux chercheurs russes sur la piste du rôle des gènes dans l'embryogenèse et l'évolution. Mais la politique s'en est mêlée...

Rendez-vous

78 Logique & calcul

Le nombre π est partout !

Jean-Paul Delahaye

Récemment encore, le nombre π est apparu là où personne ne l'attendait : dans un système simple de collisions, dans la conjecture de Syracuse, dans le jeu de la vie...

84 Science & fiction

Tout l'Univers sur le dos

J. Sébastien Steyer et Roland Lehoucq

86 Art & science

Percer le secret des méduses

Loïc Mangin

89 Idées de physique

La girafe, la paille et la pompe à piston

Jean-Michel Courty et Édouard Kierlik



92 Question aux experts

Les plantes ont-elles des cancers ?

Yves Dessaux

94 Science & gastronomie

Bavarois, aspics et guimauves

Hervé This

96 À lire

98 Bloc-notes

Les chroniques de Didier Nordon

POUR LA
SCIENCE.fr

LETTRE D'INFORMATION



Ne manquez pas
la parution
de votre magazine
grâce à la NEWSLETTER

- Notre sélection d'articles
- Des offres préférentielles
- Nos autres magazines en kiosque



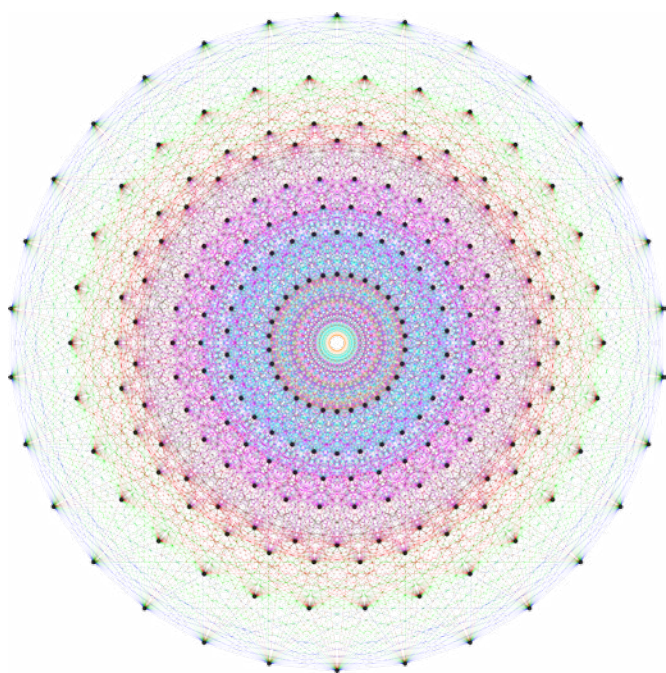
Recevez gratuitement la lettre d'information en inscrivant uniquement votre adresse mail sur www.pourlascience.fr

Actualités

Mathématiques

Savez-vous empiler des oranges en dimension 8 ?

Le problème de l'empilement optimal des sphères dans l'espace ordinaire, à 3 dimensions, a été résolu en 1998. Il vient de trouver une solution en dimensions 8 et 24 !



Shutterstock.com/ixabzy - jgmoxness

L'empilement d'oranges le plus dense est celui que l'on trouve sur les étagères de marchés. Mais qu'en est-il à 8 et 24 dimensions ? À 8 dimensions, la structure optimale est décrite par le groupe de symétrie E_8 , dont une représentation projetée en deux dimensions est donnée à gauche.

Quelle est la meilleure façon d'empiler des sphères identiques, en laissant le moins possible de vides ? Ce problème a été rendu célèbre par Johannes Kepler, qui a conjecturé en 1611 que la configuration la plus dense est la structure pyramidale adoptée sur les étals des marchands de fruits et légumes. La conjecture de Kepler n'a été démontrée qu'en 1998 par Thomas Hales, alors à l'université de Pittsburgh.

S'il est simple de visualiser des tas d'oranges, il en va tout autrement quand on essaye d'imaginer le même problème dans un monde à 4 dimensions ou plus. Or la question de l'empilement des sphères dans un espace multidimensionnel est d'importance, car elle est reliée aux codes correcteurs d'erreurs, utilisés dans les télécommunications

pour reconstituer le signal inévitablement altéré lors de sa transmission.

Un résultat intéressant vient d'être obtenu dans ce domaine : Maryna Viazovska, de l'université Humboldt à Berlin, aidée de plusieurs collègues, a résolu les cas à 8 et 24 dimensions.

Pour les mathématiciens, manipuler des oranges à quatre dimensions ou plus n'est pas un obstacle. Il se ramène à la définition formelle d'une sphère : c'est l'ensemble des points de l'espace – avec autant de dimensions que l'on veut – situés à une distance donnée d'un point particulier, le centre de la sphère. En revanche, l'ajout de dimensions rend le problème de Kepler plus difficile à résoudre, car il augmente le nombre d'arrangements possibles de sphères à examiner.

Une façon de construire les empilements est de partir de l'arrangement hexagonal à deux dimensions. En entassant des couches planes de telle façon que les trous de la couche de dessous, on obtient l'arrangement « naturel » des étagères de fruits, qui est optimal en dimension 3.

Pour construire un empilement en dimension 4, on procède de la même façon, en entassant des arrangements tridimensionnels. Et ainsi de suite. En dimension 8, on obtient un réseau qui présente un grand nombre de symétries, ce qui en facilite l'étude. Ces symétries forment un « groupe » noté E_8 , bien connu des mathématiciens (c'est le plus grand « groupe de Lie complexe de type exceptionnel »), mais aussi des physiciens qui l'étudient parfois dans le cadre des théories

de grande unification en physique des particules.

Si l'on poursuit la procédure jusqu'à 24 dimensions, on obtient un réseau de Leech. Cette structure, découverte en 1965 par John Leech, présente également de nombreuses symétries. Le réseau de Leech est associé au code correcteur de Golay qui a été utilisé pour traiter les images des sondes *Voyager* prises lors de leur survol de Jupiter et Saturne, entre 1979 et 1981.

Mais E_8 et le réseau de Leech sont-ils les empilements les plus denses dans les espaces à 8 et 24 dimensions ? En 2003, Henry Cohn et Noam Elkies, mathématiciens à Cambridge, aux États-Unis, ont montré qu'il est possible de définir des fonctions, dites auxiliaires, qui donnent une estimation de la densité maximale d'empilement pour un espace de dimension