

■ POUR LA

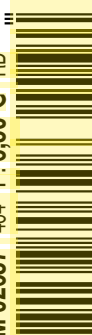
SCIENCE

Juin 2016 - n° 464

lascience.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. ■