L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

Computerworld UK staff, **The eight security backdoors that helped kill faith in security**, 2017 : www.computerworlduk.com/security/7-security-backdoors-that-heped-kill-faith-in-security-3634220/

Absolute poker and UltimateBet cheating scandals, World Casino Index, 2016 : www.worldcasinoindex.com/guide/absolute-poker-and-ultimatebet-cheating-scandals/

Safest poker sites, Ultimate Bet Review, 2016 : www.safestpokersites.com/ultimate-bet/

P. Bellanger, **La Souveraineté numérique**, Stock, 2014.

N. Perlroth *et al.*, **NSA able to foil basic safeguards of privacy on Web**, *The New York Times*, 5 septembre 2013.

F. Daignière, **F5 BIG-IP remote root authentication bypass vulnerability**, 2012 : www.trustmatta.com/advisories/MATTA-2012-002.txt

qu'Apple, sans l'avouer, a cédé aux injonctions du FBI et qu'il sait les contourner ! Il y a bien une porte dérobée ou un équivalent dans les téléphones d'Apple.

Les grandes firmes informatiques prétendent défendre la sécurité des systèmes et appareils qu'elles vendent et affirment refuser de placer des portes dérobées dans leurs machines et logiciels. Il serait naïf de les croire : il est certain que cela n'a pas toujours été le cas, et la collaboration entre les géants d'Internet et les autorités américaines a été prouvée à maintes reprises, en particulier à la suite des révélations du lanceur d'alerte Edward Snowden. La NSA *(National Security Agency)*, grâce au programme de surveillance PRISM, a eu un accès direct aux données d'Apple, de Facebook, de Microsoft, de Google, d'AOL et de Skype, et il est vraisemblable que c'est encore le cas aujourd'hui.

Le temps des illusions est fini

Quand vous utilisez ces services, soyez certains que vos informations seront soigneusement rangées dans les immenses entrepôts de données de la NSA, dont la capacité de stockage est colossale. Le centre de la NSA récemment construit dans l'Utah aurait des capacités se comptant en centaines d'exaoctets (1 exaoctet = 10^{18} caractères). Certains médias évoquent même des yottaoctets (10^{24} octets), même si cela semble peu vraisemblable, du moins dans un avenir proche.

Une autre histoire un peu plus ancienne que celle des téléphones d'Apple montre que les autorités américaines (mais elles ne sont sans doute pas les seules), ne se contentent pas de demander publiquement qu'on leur communique les clés d'accès des portes dérobées concernant des appareils dont on prétend qu'ils n'en ont pas, mais qu'elles en insèrent secrètement !

En cryptographie, disposer de programmes qui engendrent rapidement des suites pseudoaléatoires est important, car ces méthodes servent comme composants de base à de nombreux algorithmes de chiffrement de données. Le NIST (*National Institute of Standards and Technology*, l'institut américain des normes et de la technologie) publie des conseils et des normes sur le sujet. Ces normes étaient largement suivies. Or la norme du *Dual Elliptic Curve Deterministic Random Bit Generator* (Dual-EC-DRBG) a été, sans qu'il ne subsiste aucun doute, manipulée par la NSA. Ce générateur contient une porte dérobée qui permet aux détenteurs de clés appropriées de contrôler la production des bits censés être pseudo-aléatoires et donc de casser les méthodes de chiffrement qui les utiliseraient.

Dès 2007 paraissaient des études suspectant l'existence d'une porte dérobée dans le Dual-EC-DRBG. Pourtant, le NIST l'indiquait parmi quatre méthodes recommandées pour des usages cryptographiques, ce qu'il a cessé de faire seulement en 2014. À nouveau, ce sont les révélations d'Edward Snowden qui ont permis de connaître le fin mot de l'histoire. Elles indiquent que la NSA avait travaillé sur la normalisation du Dual-EC-DRBG, jusqu'à devenir le responsable unique de sa formulation.

Le *New York Times*, qui a analysé les documents d'Edward Snowden, affirme même que la NSA dépense 250 millions de dollars par an (parfois en payant simplement les entreprises concernées) pour insérer dans les produits cryptographiques des portes dérobées ou des faiblesses lui permettant de casser les chiffrements. On comprend bien que la réputation du NIST en a pâti et que, dorénavant, ses normes sont considérées avec méfiance. C'est plus généralement le cas de nombreux produits et matériels américains, dont on sait qu'ils sont souvent conçus pour faciliter les tâches d'espionnage généralisé de la NSA.

La situation de domination et d'intrusion généralisée de systèmes étrangers (notamment américains) dans le monde numérique est un danger non seulement pour la vie privée de tous, mais aussi pour les entreprises dont les secrets techniques et commerciaux risquent de tomber dans des mains concurrentes ou adverses. Pierre Bellanger, dans un excellent livre sur le sujet *(voir la bibliographie)*, évoque avec raison un grave problème de « souveraineté numérique ». ■

Retrouvez la rubrique Logique & calcul sur www.pourlascience.fr

OFFRE DÉCOUVERTE | ABONNEZ-VOUS À POUR LA SCIENCE

1 AN - 12 Nos
59€
24% d'économie

2 ANS - 24 Nos
110€
29% d'économie

3 ANS - 36 Nos
159€
32% d'économie

BULLETIN D'ABONNEMENT

POUR LA SCIENCE

À renvoyer accompagné de votre règlement à : Pour la Science - Service abonnements - 19 rue de l'industrie - BP 90 053 - 67 402 Illkirch cedex

PAS474B

❑ **OUI, je m'abonne à *Pour la Science* en formule Découverte :**

- ❑ **1 an • 12 numéros • 59€** au lieu de ~~78,50€~~ **(D1A59E)**
- ❑ **2 ans • 24 numéros • 110 €** au lieu de ~~157 €~~ **(D2A110E)**
- ❑ **3 ans • 36 numéros • 159 €** au lieu de ~~235,50€~~ **(D3A159E)**

MES COORDONNÉES

Nom : _____

Prénom : _____

Adresse : _____

_____

Code postal : _____

Ville : _____

Tél. : _____
Pour le suivi client (facultatif)

MON MODE DE RÈGLEMENT

❑ Par chèque à l'ordre de *Pour la Science*

❑ Par carte bancaire

N° _____

Date d'expiration _____ Clé _____

Signature obligatoire

Mon e-mail pour recevoir la newsletter *Pour la Science* (à remplir en majuscule). _____@_____

Grâce à votre email nous pourrons vous contacter si besoin pour le suivi de votre abonnement. À réception de votre bulletin, comptez 5 semaines pour recevoir votre n° d'abonné. Passé ce délai, merci d'en faire la demande à pourlascience@abopress.fr

J'accepte de recevoir les informations de *Pour la Science* ❑ OUI ❑ NON et de ses partenaires ❑ OUI ❑ NON

Délai de livraison: dans le mois suivant l'enregistrement de votre règlement. Offre réservée aux nouveaux abonnés, valable jusqu'au 31/07/17 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site www.pourlascience.fr. Conformément à la loi "Informatique et libertés" du 6 janvier 1978, vous disposez d'un droit d'accès et de rectification aux données vous concernant en adressant un courrier à *Pour la Science*.

SCIENCE & FICTION

Ralentir la lumière avec la Force

Depuis quelques années, contrôler la lumière jusqu'à la figer sur place n'est plus l'apanage de personnages de fiction. Les physiciens ont trouvé le moyen de la ralentir en laboratoire !

Roland LEHOUCQ et Jean-Sébastien STEYER. Illustration : Marc BOULAY

L'introduction du film *Star Wars : Le Réveil de la Force* (J. J. Abrams, 2015) montre une scène étonnante : Kylo Ren, le successeur de Dark Vador, utilise la Force pour stopper le tir de pistolet laser de Poe Dameron, le meilleur pilote de la Résistance. Par « stopper », il faut comprendre « arrêter en l'air » le pinceau lumineux émis par l'arme. Une fois le héros capturé, Kylo Ren retourne dans son vaisseau et la lumière stoppée redémarre.

Jouer ainsi avec la vitesse de la lumière n'est pas une première dans les œuvres de fiction. Dans son roman *Le Maître de la lumière*, publié en 1933, Maurice Renard narre une banale histoire de pièce hantée. Mais on n'y trouve nul fantôme. La clé du mystère est l'étrange « luminite » : « la lumière cheminant dans cette matière à une vitesse extrêmement freinée, on voit, de part et d'autre des plaques de luminite, ce qui se trouvait là jadis. Et plus la plaque est épaisse, plus le passé qu'elle montre est lointain, sur une face comme sur une autre. »

On retrouve la même idée dans la nouvelle *Lumière des jours enfuis* de l'écrivain britannique Bob Shaw (1966) où le « verre lent » est un matériau que la lumière met des années à traverser. Le procédé invoqué pour expliquer le phénomène est « un tunnel en spirale enroulé à l'extérieur du rayon de capture de chaque atome du verre ». L'argument ne paraît pas très scientifique, même si les mots utilisés veulent montrer le contraire. Dans sa série de romans de fantasy burlesque, *Les Annales du Disque-monde* (à partir de 1983), Terry Pratchett ne s'embarrasse pas de détails techniques pour justifier que, dans son univers, la lumière ne se propage qu'à quelques centaines de kilomètres par heure : c'est tout simplement à cause de « l'intensité plutôt embarrassante du champ de magie ».

GRÂCE À LA « FORCE », Kylo Ren, l'un des méchants du film *Star Wars : Le Réveil de la Force* (2015), est capable de stopper un tir de pistolet laser.

Dans notre monde, est-il possible de ralentir la lumière ? Avant de répondre à cette question, il faut se rappeler que la lumière est une onde électromagnétique et qu'on peut lui associer plusieurs vitesses. La vitesse de phase est la vitesse de l'onde porteuse, autrement dit celle à laquelle les maxima et les minima d'une onde électromagnétique sinusoïdale se déplacent. Dans tous les milieux matériels, la vitesse de phase d'une telle onde dépend de sa fréquence. Ces milieux sont dits dispersifs.

Superposer des ondes de diverses fréquences permet d'obtenir une onde plus complexe dont on définit la vitesse de groupe comme celle de l'enveloppe de l'onde. Pour une impulsion lumineuse utilisée dans les communications, la vitesse de groupe est celle du maximum de l'amplitude de l'impulsion et aussi celle à laquelle l'énergie se propage. Cette distinction entre vitesse de phase et vitesse de groupe a été proposée en 1880 par le physicien français Georges Gouy. En effet, ces vitesses sont *a priori* différentes, sauf dans le vide où elles se confondent et valent environ 300 000 kilomètres par seconde.

Lorsque la lumière traverse un milieu transparent, sa vitesse de phase est inférieure