

# Abonnez-vous à

■ POUR LA

# SCIENCE



## **+** En CADEAU de bienvenue :

### **Les gènes voyageurs, d'Éric Baptiste**

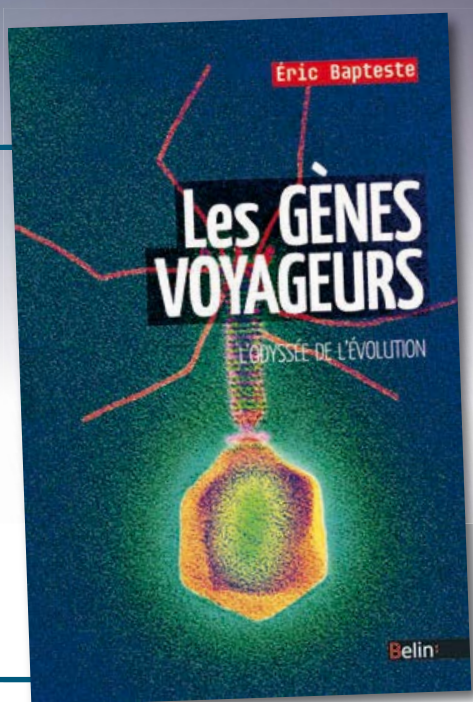
Savez-vous que l'échangisme est une pratique très répandue chez les microbes ? Que des organismes comme les plantes ou les animaux deviennent en partie ce qu'ils mangent ? Que les bactéries sont impliquées dans des guerres qui durent des millions d'années et qu'elles entretiennent une vie sociale intense ? Ces phénomènes biologiques sont provoqués par des voyages de gènes inattendus, qui transforment la majeure partie du vivant. Une découverte récente qui pourrait bien révolutionner les sciences de l'évolution...

Éditions Belin - Paru en 2013 - 192 pages - Prix unitaire : 20,40 €

Votre abonnement  
**INTÉGRAL**

**8,20€**  
**par mois**  
**seulement**

le magazine  
+ le hors-série chez vous  
+ l'accès numérique illimité à  
toutes les archives  
sur **www.pourlascience.fr**



# OFFRE SPÉCIALE D'ABONNEMENT

POUR LA  
**SCIENCE**

À découper ou à photocopier et à retourner accompagné de votre règlement dans une enveloppe non affranchie à :  
Groupe Pour la Science - Service Abonnements - Libre réponse 90 382 - 75 281 Paris cedex 06

## 1. MA FORMULE

☐ **OUI**, je m'abonne à l'offre « Intégrale » à 8,20€ par mois.

Je reçois le magazine *Pour la Science* (12 n°/an)

+ son hors-série *Dossier Pour la Science* (4 n°/an)

+ mon livre. Je bénéficie aussi de l'accès numérique illimité aux archives sur **www.pourlascience.fr**.

Mon e-mail obligatoire pour l'accès aux contenus numériques (à remplir en majuscules)

@

À réception de votre bulletin, comptez 5 semaines pour recevoir votre n° d'abonné. Passé ce délai, merci d'en faire la demande à abonnements@pourlascience.fr

## 2. MES COORDONNÉES

Nom :

Prénom :

Adresse :

Code postal : \_\_\_\_\_ Ville : \_\_\_\_\_

Pays : \_\_\_\_\_

Tél. : \_\_\_\_\_

Pour le suivi client (facultatif)

## 3. MON MODE DE RÈGLEMENT

☐ (IPVI) Je règle par prélèvement **8,20€ par mois\*** et reçois en cadeau le livre *Les gènes voyageurs* (OGEVO). Je remplis l'autorisation ci-dessous en joignant impérativement un IBAN/BIC.

\*Pour la France métropolitaine et d'outre-mer. Pour l'Europe (pays de la zone SEPA) : 9,60€ par mois. Abonnement en reconduction tacite dénonçable à tout moment auprès du service abonnement avec un préavis de 3 mois. Conditions complètes sur **www.pourlascience.fr**

### AUTORISATION DE PRÉLÈVEMENT PAR MANDAT SEPA

En signant ce mandat SEPA, j'autorise Pour la Science à transmettre des instructions à ma banque pour le prélèvement de mon abonnement dès réception de mon bulletin. Je bénéficie d'un droit de rétractation dans la limite de 8 semaines suivant le premier prélèvement. Plus d'informations auprès de mon établissement bancaire.

### 1 - COORDONNÉES DU TITULAIRE DU COMPTE

Nom, prénom

Adresse

Numéro et nom de la rue

Code postal

Ville

Pays

### 2 - COORDONNÉES BANCAIRES

IBAN

Numéro d'identification international du compte bancaire - IBAN (International Bank Account Number)

BIC

Code international d'identification de votre banque - BIC (Bank Identifier Code)

Type de paiement

Paiement récurrent/répétitif

### 3 - Date et signature obligatoires

À

Date

Signature :

### NOM DU CRÉANCIER

Pour la Science - 8 rue Férou - 75006 Paris

ICS N° FR92ZZZ426900

N° de référence unique de mandat (RUM)

Partie réservée au service abonnement. Ne rien inscrire

☐ (ITA) Je préfère régler mon abonnement d'un an en **une seule fois 99€\*\*** sans bénéficier du cadeau.

\*\* Offre valable en France métropolitaine et d'outre-mer. Pour l'étranger, participation aux frais de port à ajouter : Europe 16€ - autres pays 35€.

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

☐ Par carte bancaire N°

Date d'expiration

Clé

Signature obligatoire

En application de l'article 27 de la loi du 6 janvier 1978, les informations ci-dessus sont indispensables au traitement de votre commande. Elles peuvent donner lieu à l'exercice du droit d'accès et de rectification auprès du groupe Pour la Science. Par notre intermédiaire, vous pouvez être amené à recevoir des propositions d'organismes partenaires. En cas de refus de votre part, merci de cocher cette case ☐.

POUR LA  
**SCIENCE**

## LOGIQUE & CALCUL

### Déléguer un calcul sans divulguer ses données

*Vous confiez des calculs à un tiers, il les effectue et vous transmet les résultats, mais sans avoir pu connaître ni les données du calcul ni ses résultats : un nouveau miracle cryptographique !*

Jean-Paul DELAHAYE

**S**i vous êtes prudent, vous chiffrez vos données avant de les confier à un service de sauvegarde extérieur, dans le « cloud » par exemple. Comment demander alors à ce service de prendre les données d'un fichier et d'en calculer la moyenne, ou d'en extraire des informations particulières ? Pour calculer et manipuler des données, il semble qu'il faille les connaître.

Eh bien, non ! C'est tout l'enjeu des systèmes de chiffrement homomorphe : vous permettez à un tiers de calculer avec vos données qu'il ne connaît pas, et il produit un résultat qui lui est illisible, mais que vous savez déchiffrer.

#### Une méthode très simple : la multiplication

Si les calculs à effectuer sont simples, il est facile d'imaginer une solution. Vous choisissez un nombre  $C$  que vous serez le seul à connaître. Vous multipliez toutes vos données par  $C$ , et ce sont ces données que vous transmettez à l'opérateur extérieur  $\textcircled{C}$  chargé de les sauvegarder. Pour connaître par exemple la moyenne de vos données ou de certaines d'entre elles, vous demandez à  $\textcircled{C}$  de calculer la moyenne sur les données dont il dispose et de vous transmettre le résultat. Puis vous divisez le résultat par  $C$  : vous avez votre moyenne, car la moyenne de  $Cd_1, Cd_2, \dots, Cd_n$  est  $C$  fois la moyenne de  $d_1, d_2, \dots, d_n$ .

#### Calcul délocalisé

**A**vec les chiffrements dits homomorphes, un opérateur calcule sur des données chiffrées dont il n'a pas connaissance. Une fois le calcul achevé, il ne peut pas connaître le résultat trouvé, que seul le commanditaire du calcul déchiffre.

Vous chiffrez vos données avec une clef secrète et vous les envoyez à l'opérateur extérieur (1). L'opérateur effectue des calculs avec les données cryptées et vous envoie les résultats (cryptés) sans avoir eu connaissance de la clef (2, 3). Vous déchiffrez les résultats reçus grâce

à la clef secrète (4) : vous avez ainsi connaissance des résultats d'un calcul que vous n'avez pas fait, résultats auxquels l'opérateur n'a pas pu avoir accès. Pour des calculs simples, des séries d'additions et de soustractions, la mise au point d'applications réelles telles que les systèmes de vote est possible.

