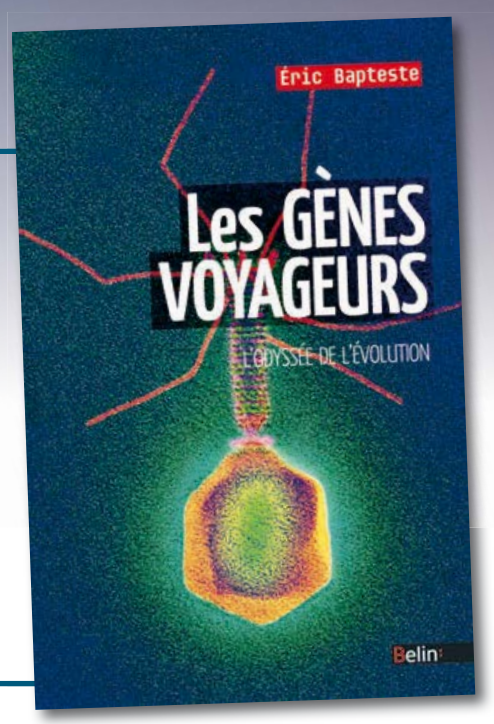
Votre abonnement INTÉGRAL

8,20€ par mois seulement

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

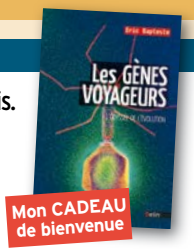


OFFRE SPÉCIALE D'ABONNEMENT

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 nos/an)
+ son hors-série *Dossier Pour la Science* (4 nos/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*** (00GEVO). 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 Acount Number)

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

Type de paiement Paiement récurrent/répétitif

POUR LA SCIENCE

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

❑ (I1A) 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 ❑.

PLS456B Offre réservée aux nouveaux abonnés valable jusqu'au 31.10.2015

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

Si 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.

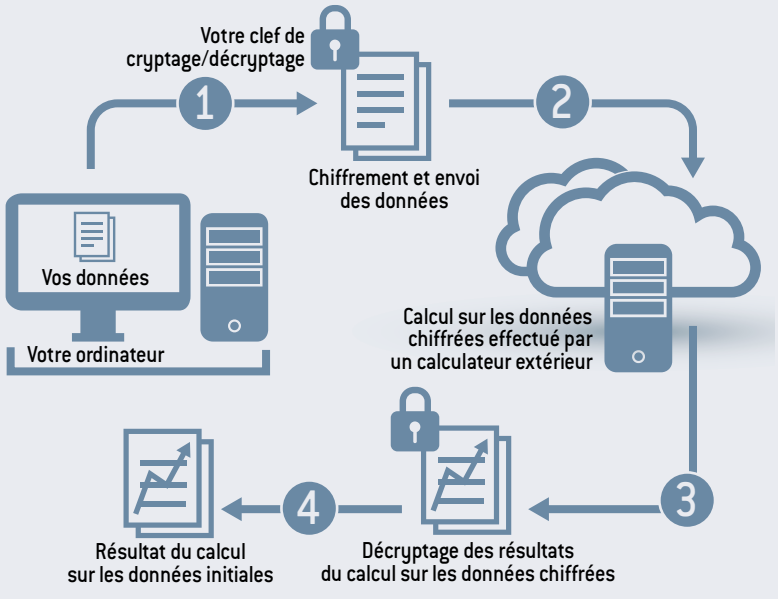
Une méthode très simple : la multiplication

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 © chargé de les sauvegarder. Pour connaître par exemple la moyenne de vos données ou de certaines d'entre elles, vous demandez à © 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 $C\,d_1$, $C\,d_2$,..., $C\,d_n$ est C fois la moyenne de d_1, d_2,..., d_n.

Calcul délocalisé

Avec 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.



Avec ce procédé, vous pouvez faire exécuter par l'opérateur extérieur d'autres types de calculs. Pour connaître le nombre de données qui dépassent un certain nombre B, vous lui demanderez le nombre de données qui dépassent $C\,B$. Le tri de vos données par ordre croissant est aussi faisable, puisque si C est positif, le tri de $C\,d_1, C\,d_2,\ldots, C\,d_n$ exige les mêmes permutations que $d_1, d_2,\ldots, d_n$. Toutes les moyennes pondérées, par exemple la moyenne $(d_1 + 2d_2 + 5d_3 + d_4)/9$, sont aussi possibles sans dévoiler C, car le résultat sur les données multipliées par C est égal à C fois le résultat attendu. Certaines opérations un peu plus compliquées sont envisageables : pour le calcul de $d_1d_2 + d_3d_4 + d_5d_6$, il suffira de diviser le résultat que $\mathcal{O}$ fournit par C^2.

Cependant, vous ne pourrez pas demander $d_1 + d_2d_3$ et, finalement, ce n'est qu'un faible sous-ensemble de calculs que vous saurez faire exécuter à l'extérieur sans avoir à divulguer vos secrets. En particulier, pas question de faire opérer des algorithmes complexes sur vos données, comme l'identification, parmi les nombres confiés, de ceux qui sont des nombres premiers. Remarquons aussi que le chiffrement de vos données en les multipliant par une constante C laisse transparaître certaines informations que vous ne souhaitez peut-être pas que l'opérateur $\mathcal{O}$ connaisse : le numéro de la donnée la plus grande ou la plus petite, les valeurs égales, les données classées, etc.

Le problème sera résolu si vous disposez d'une méthode de chiffrement permettant à la fois de bien masquer toute l'information et autorisant l'exécution d'additions et de multiplications sans rien révéler : avec ces deux opérations, on reconstitue tout calcul.

La solution : des chiffrements pleinement homomorphes

Notons aussi qu'il n'est pas essentiel que l'opération effectuée par $\mathcal{O}$ soit identique à celle que vous voulez au final. En effet, supposons que le chiffrement de la donnée d soit $\mathcal{C}(d)$ et que le déchiffrement (que vous seul savez effectuer) soit l'opération $\mathcal{C}'$: $\mathcal{C}'(\mathcal{C}(d)) = d$. Pour réussir à faire exécuter toutes sortes de calculs par un opérateur extérieur, il suffirait qu'il existe une opération $*_1$ et une opération $*_2$ (pas nécessairement l'addition et la multiplication habituelles) vérifiant :

$\mathcal{C}(d_1 + d_2) = \mathcal{C}(d_1) *_1 \mathcal{C}(d_2)$ (propriété 1)

$\mathcal{C}(d_1 \times d_2) = \mathcal{C}(d_1) *_2 \mathcal{C}(d_2)$ (propriété 2).

En exécutant $*_1$ et $*_2$ à la place de $+$ et $\times$, l'opérateur $\mathcal{O}$ produira à partir des données chiffrées un résultat qui, après le déchiffrement par $\mathcal{C}'$, sera exactement ce que vous voulez.

Par exemple, si vous souhaitez connaître $d_1 + d_2d_3$ sans le calculer vous-même (ce qui est impossible avec la méthode de multiplication par C), vous enverrez vos données cryptées $\mathcal{C}(d_1)$, $\mathcal{C}(d_2)$, $\mathcal{C}(d_3)$ à l'opérateur en lui demandant de calculer $\mathcal{C}(d_1) *_1 (\mathcal{C}(d_2) *_2 \mathcal{C}(d_3))$ et de vous renvoyer le résultat R. Grâce à l'opération $\mathcal{C}'$, vous obtiendrez alors la valeur de $d_1 + d_2d_3$, puisque :

$\mathcal{C}'(R) = \mathcal{C}'[\mathcal{C}(d_1) *_1 (\mathcal{C}(d_2) *_2 \mathcal{C}(d_3))] = \mathcal{C}'[\mathcal{C}(d_1)] + \mathcal{C}'[\mathcal{C}(d_2) *_2 \mathcal{C}(d_3)] = d_1 + \mathcal{C}'[\mathcal{C}(d_2) \times \mathcal{C}'[\mathcal{C}(d_3)]] = d_1 + d_2d_3$.

La méthode fonctionnera pour toute expression, aussi compliquée soit-elle, constituée d'additions et de multiplications. Puisque dès qu'on sait mener des additions

Préserver la confidentialité

Imaginons que l'on souhaite établir une statistique sur un sujet délicat en utilisant Internet et en garantissant à chacune des personnes sondées que les données individuelles contenues dans les réponses ne seront pas divulguées. La procédure est la suivante :

Chaque personne chiffre ses réponses avec la clef publique du collecteur final et les envoie à un calculateur extérieur *(1)*. Ce calculateur traite ces données cryptées et envoie le résultat au collecteur final *(2, 3)*. Ce dernier déchiffre le résultat et obtient la statistique souhaitée *(4)*. Le calculateur extérieur ne peut pas accéder aux informations privées des sujets de l'enquête car il ne dispose pas de la clef privée de déchiffrement, et le collecteur final ne peut pas accéder aux données individuelles car il n'a pas eu accès aux informations chiffrées individuelles transmises.