Des nombres et des énigmes

Êtes-vous prêts pour des énigmes difficiles ? Ana Retchman, maîtresse de conférences à l'université de Strasbourg, et Sébastien Kernivinen, enseignant en mathématiques, à Rennes, vous en proposent 14. Elles sont extraites, pour la plupart, des *Défis du calendrier 2018*, d'Ana Retchman.

Suite des énigmes page 81. Solutions page 106.


Ana Retchman


Sébastien Kernivinen

ÉNIGME 1

Jusqu'à quel nombre N est-il possible de colorier en rouge ou bien en bleu les nombres entiers de 1 à N sans que deux nombres quelconques distincts de la même couleur ne redonnent, en les additionnant, un nombre de la même couleur ? Indice : c'est un cube !

ÉNIGME 2

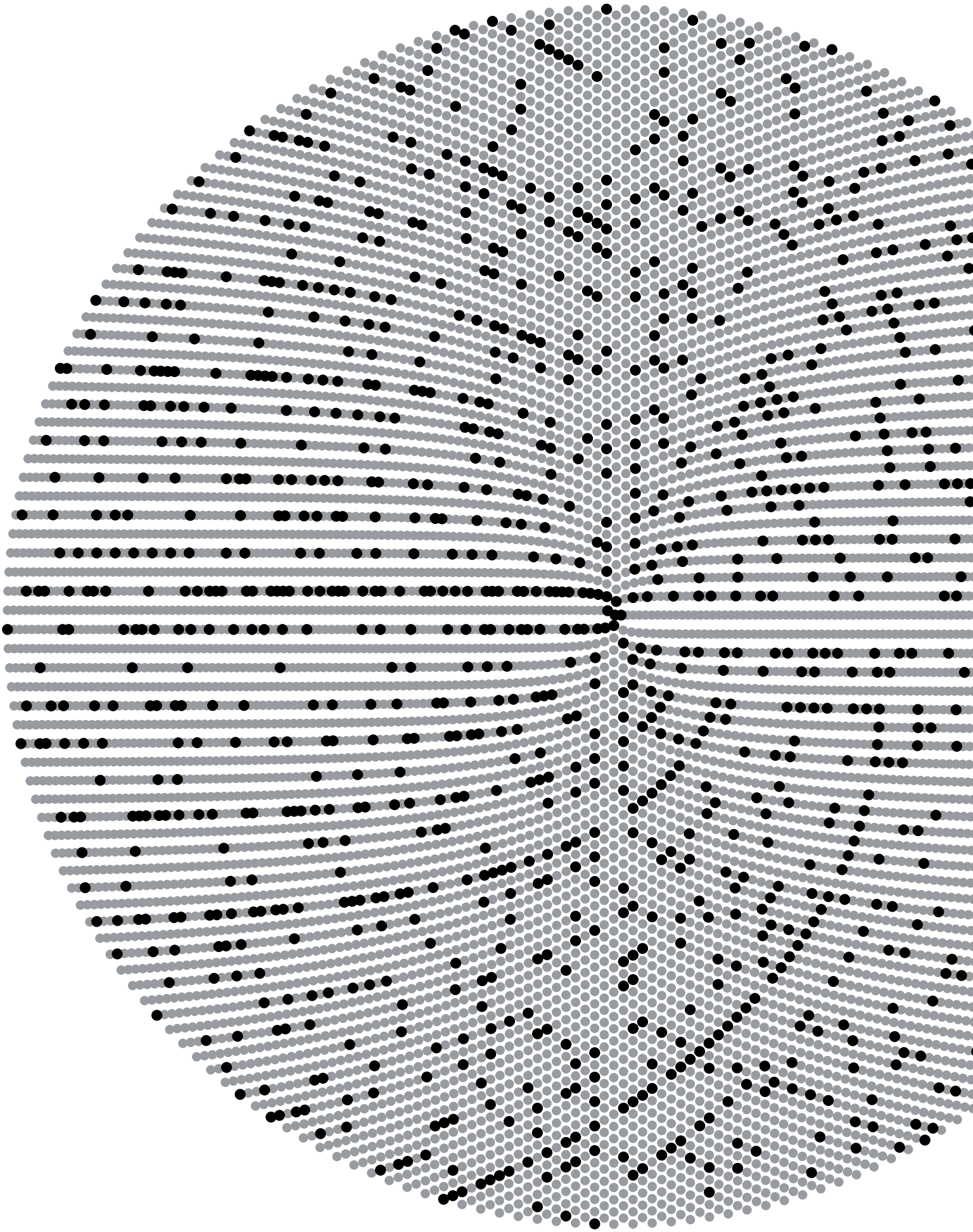
Combien y a-t-il de « randonnées » partant du nombre entier 1 et arrivant au nombre entier 10 en ajoutant successivement ou bien 1 ou bien 2 à chaque pas ?

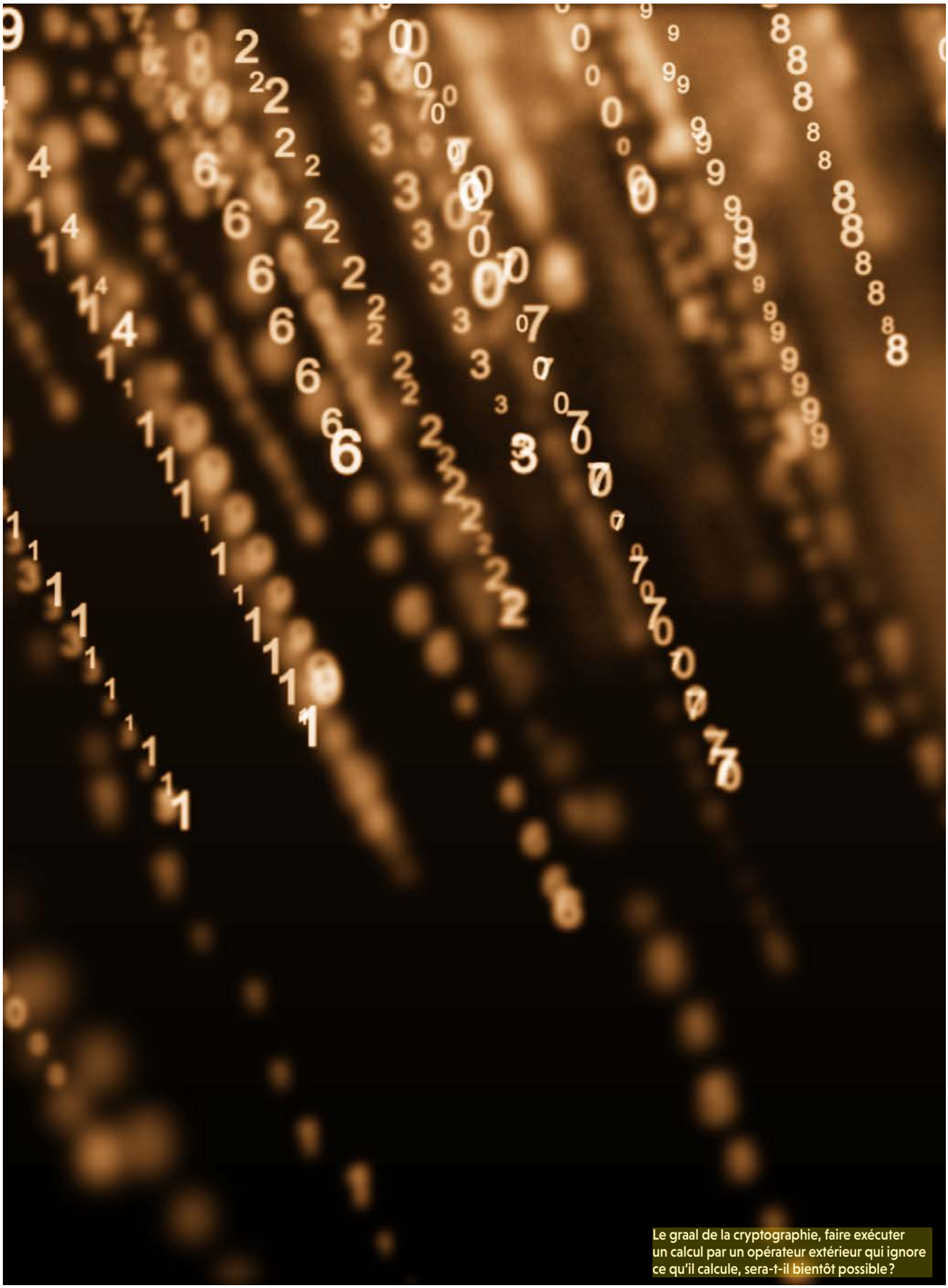
ÉNIGME 3

Trouvez dix entiers positifs distincts tels que chacun d'entre eux divise la somme de ces dix nombres.

ÉNIGME 4

Quels sont les nombres rationnels positifs r tels que $r+\frac{1}{r}$ soit un entier ?





Le graal de la cryptographie, faire exécuter un calcul par un opérateur extérieur qui ignore ce qu'il calcule, sera-t-il bientôt possible ?

L'ESSENTIEL

- Comment calculer et manipuler des données sans les connaître?
- Pour des calculs simples, les solutions sont faciles. Mais on est vite limité, par exemple pour identifier parmi des nombres ceux qui sont premiers.
- On peut aller plus loin avec les méthodes de chiffrement pleinement homomorphe que les travaux de Craig Gentry ont rendues possibles.
- Avec des versions partielles, on peut déjà sécuriser des votes électroniques. Mais des progrès restent nécessaires pour rendre «pleinement» utilisable le chiffrement pleinement homomorphe.

L'AUTEUR

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

Une nouvelle merveille cryptographique !

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. On peut parler de prodige !

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, vous devez les connaître!

Eh bien, non! C'est tout l'enjeu des systèmes de chiffrement homomorphe: un tiers peut 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

Si les calculs à effectuer sont simples, il est facile d'imaginer une solution. Vous choisissez un nombre C que vous seul connaissez. Vous multipliez toutes vos données par C, et ce sont ces données que vous transmettez à l'opérateur extérieur (noté $\mathbb{O}$) chargé de les sauvegarder. Pour connaître par exemple la moyenne de vos données ou de certaines d'entre elles, vous demandez à $\mathbb{O}$ 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,..., Cd_n est C fois la moyenne de d_1, d_2,..., d_n.

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 CB. Le tri de vos données par ordre croissant est aussi faisable, puisque si C est positif, le tri de Cd_1, Cd_2,..., Cd_n exige les mêmes permutations que d_1, d_2,..., 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 $\mathbb{O}$ 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 $\mathbb{O}$ 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.

DES CHIFFREMENTS PLEINEMENT HOMOMORPHES

Notons aussi qu'il n'est pas essentiel que l'opération effectuée par $\mathbb{O}$ soit identique à celle que vous voulez au final. En effet, supposons que le chiffrement de la donnée d soit $\mathscr{C}(d)$ et que le déchiffrement (que vous seul savez effectuer) soit l'opération $\mathscr{C}'$: $\mathscr{C}'(\mathscr{C}(d))=d$. 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:

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

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

En exécutant $*_1$ et $*_2$ à la place de + et $\times$, l'opérateur 2 produira à partir des données chiffrées un résultat qui, après le déchiffrement par $\mathscr{C}'$, 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 chiffrées $\mathscr{C}(d_1)$, $\mathscr{C}(d_2)$, $\mathscr{C}(d_3)$ à l'opérateur en lui demandant de calculer $\mathscr{C}(d_1)*_1(\mathscr{C}(d_2)*_2\mathscr{C}(d_3))$ et de vous renvoyer le résultat R. Grâce à l'opération $\mathscr{C}'$, vous obtiendrez alors la valeur de $d_1+d_2\,d_3$, puisque:

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

La méthode fonctionnera pour toute

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 clé secrète et vous les envoyez à l'opérateur extérieur (1). L'opérateur effectue des calculs avec les données chiffrées et vous envoie les résultats (chiffrés) sans avoir eu connaissance de la clé (2, 3). Vous déchiffrez les résultats reçus grâce à la clé 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.