

- > 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 $d_1, d_2, \dots, d_n$.

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 $Cd_1, Cd_2, \dots, Cd_n$ exige les mêmes permutations que $d_1, d_2, \dots, d_n$.

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.

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:

$$\begin{aligned}\mathcal{C}(d_1 + d_2) &= \mathcal{C}(d_1) *_1 \mathcal{C}(d_2) \quad (\text{propriété 1}) \\ \mathcal{C}(d_1 \times d_2) &= \mathcal{C}(d_1) *_2 \mathcal{C}(d_2) \quad (\text{propriété 2}).\end{aligned}$$

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 $\mathcal{C}'$, 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 chiffrées $\mathcal{C}(d_1), \mathcal{C}(d_2), \mathcal{C}(d_3)$ 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:

$$\begin{aligned}\mathcal{C}'(R) &= \mathcal{C}'(\mathcal{C}(d_1) *_1 (\mathcal{C}(d_2) *_2 \mathcal{C}(d_3))) = \\ &= \mathcal{C}'(\mathcal{C}(d_1)) + \mathcal{C}'(\mathcal{C}(d_2) *_2 \mathcal{C}(d_3)) = \\ &= d_1 + \mathcal{C}'(\mathcal{C}(d_2) \times \mathcal{C}(d_3)) = d_1 + d_2d_3.\end{aligned}$$

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.

