Craig Gentry, le pionnier

En proposant en 2009 le premier système de cryptage complètement homomorphe, Craig Gentry, aujourd'hui chercheur chez IBM, a révolutionné le domaine. Il a déclenché une multitude de travaux qui, petit à petit, ouvrent des voies pour rendre utilisable son idée, initialement théorique pour l'essentiel. Confier de façon massive des calculs à des opérateurs extérieurs qui ne peuvent pas accéder aux données n'est pas aujourd'hui envisageable. En revanche, peu à peu, il est devenu possible de résoudre des problèmes particuliers n'exigeant qu'une petite quantité de calculs homomorphes (comme pour un vote). Les applications de ces méthodes devraient rapidement s'étendre et aider à accroître la sécurité des réseaux et la protection des données... ce dont on a un grand besoin !

© John D. & Catherine T. MacArthur Foundation

et des multiplications de cette façon, on peut exécuter tout algorithme, le problème des calculs secrets par un tiers se ramène à celui de trouver $\mathscr{C}$, $\mathscr{C}'$, $*_1$, $*_2$, vérifiant les propriétés 1 et 2.

Les méthodes de cryptage vérifiant les propriétés 1 et 2 sont dites « pleinement homomorphes ». Le terme vient du langage mathématique où l'on dénomme homomorphisme les fonctions qui transforment une opération en une autre, comme l'indique par exemple la propriété 1.

Ces homomorphismes jouent un rôle très important en mathématiques et chacun connaît le logarithme qui vérifie $\log(a \times b) = \log(a) + \log(b)$ et qui transforme donc des multiplications en additions (ici, $*_2$ est l'addition habituelle). Avant l'avènement des ordinateurs, c'était le moyen le plus efficace pour mener à la main des calculs numériques, et c'est pourquoi on dressait des tables de logarithmes contenant des millions de données.

En mathématiques, on connaît de nombreux homomorphismes, mais aucun des homomorphismes classiques ne peut servir à concevoir un cryptage $\mathscr{C}$ homomorphe car l'opération de décryptage $\mathscr{C}'$ est alors trop simple ; or une bonne méthode cryptographique est une méthode où il est difficile de trouver $\mathscr{C}'$. Le problème des systèmes de chiffrement pleinement homomorphes n'était donc pas évident au moment où, en 1978, l'idée en a été envisagée par les Américains Ron Rivest et Leonard Adleman et le Grec Michael Dertouzos. On s'est longtemps demandé si de telles méthodes existaient. Le problème a parfois été qualifié de graal de la cryptographie.

Une percée décisive a été réalisée en 2009 par Craig Gentry, de l'université Stanford et aujourd'hui chercheur au centre Thomas Watson d'IBM à New York. Craig Gentry a proposé une méthode qui résout théoriquement le problème et a pour cela reçu une bourse de 625 000 dollars de la fondation MacArthur. La méthode qu'il a initialement proposée n'est pas applicable, car elle exige des calculs trop volumineux au moment du cryptage (la transformation des données avant de les envoyer) et du décryptage. De plus, la taille des données que doit manipuler l'opérateur extérieur $\mathbb{O}$, et donc la quantité de calculs qu'il doit mener, est des millions de fois celle nécessaire quand les données ne sont pas cryptées.

Craig Gentry a fait une percée décisive, pour laquelle il s'est vu attribuer une bourse de 625 000 dollars.

Depuis 2009, une multitude de recherches ont été faites pour trouver des schémas plus économiques. En quelques années, les progrès ont rendu envisageables certaines applications, et l'espoir de méthodes encore plus économiques et faciles à mettre en œuvre suscite de nombreux travaux parmi les spécialistes.

Avant de donner des précisions sur les idées de la percée décisive de Craig Gentry, revenons sur les applications des cryptages pleinement homomorphes ou même partiellement homomorphes.

L'algorithme RSA (conçu en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman) est une méthode de chiffrement à clef publique : pour crypter un message, on utilise la clef publique de son correspondant, et lui seul peut déchiffrer le message grâce à sa clef secrète. C'est un bon algorithme, aujourd'hui très utilisé. Il a la propriété d'être homomorphe pour la multiplication : on en déduit une méthode de chiffrement homomorphe pour l'addition, comme celle évoquée au début de l'article, méthode ayant cette fois l'avantage que les données sont correctement masquées à l'opérateur extérieur.

Une application : les votes secrets

Avec un système additivement homomorphe de ce type, on peut opérer des votes secrets sur le réseau sans se rencontrer. Décrivons un tel procédé.

Il y a trois types d'intervenants : les votants (au plus $N-1$), l'opérateur calculateur, et l'opérateur de dépouillement. L'opérateur de dépouillement choisit un couple clef publique/clef privée et communique la clef publique à chaque votant. Chaque votant choisit alors un nombre entier V de la forme Nk (k entier) s'il veut voter OUI, ou $Nk+1$ (k entier) s'il veut voter NON ; puis il chiffre le nombre V choisi avec la clef publique et transmet le nombre crypté $\mathscr{C}(V)$ à l'opérateur de calcul. Ce dernier fait la somme S de tous les nombres qu'il reçoit et communique S à l'opérateur de dépouillement, lequel déchiffre le résultat grâce à la clef privée, qu'il est seul à connaître. Il trouve ainsi un nombre de la forme $Mk+p$, où p est le nombre de personnes ayant voté NON. Le résultat du vote est alors communiqué à tous.