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.

L'opérateur calculateur, qui ne connaît pas la clef de déchiffrement, ne peut pas connaître les votes individuels ; l'opérateur de dépouillement, qui n'a pas eu connaissance des nombres transmis individuellement, ne peut pas lui non plus connaître les votes individuels. Les votants peuvent contrôler le travail de l'opérateur de calcul, s'ils acceptent de se communiquer les $\mathcal{C}(V)$, ce qui ne compromet pas le secret du vote. Avec un tel système, même si les votants sont séparés par des milliers de kilomètres et ne communiquent que par messages, aucun vote ne circule de manière lisible, et personne ne sait comment les autres ont voté. On peut encore perfectionner de tels systèmes, comme l'explique un article de Véronique Cortier et Steve Kremer *(voir la bibliographie)*.

Ce type d'applications de la cryptographie partiellement homomorphe est aujourd'hui arrivé à maturité et le système de vote *Helios* est un logiciel libre développé par les chercheurs de l'université Harvard et de l'université catholique de Louvain. On l'a utilisé pour l'élection du recteur de l'université catholique de Louvain et plusieurs fois lors d'élections étudiantes. L'Association internationale des chercheurs en cryptographie (IACR) l'utilise pour choisir les membres de son bureau. Il est fondé sur le système de chiffrement *El Gamal,* qui est additivement homomorphe.

Une arithmétique « secrète »

Voici maintenant la description d'une version du chiffrement pleinement homomorphe de Craig Gentry. Cette version est due à Marten van Dijk, Craig Gentry, Shai Halevi et Vinod Vaikuntanathan. Les idées sont simples et n'impliquent que des calculs élémentaires effectués avec des entiers.

La méthode utilise le fait que, pour créer un système de chiffrement pleinement homomorphe, il suffit de définir un système qui chiffre les bits, des 0 et des 1, et de savoir faire exécuter par l'opérateur extérieur un nombre quelconque d'opérations logiques du type XOR (OU exclusif) et ET entre de tels bits chiffrés.

Vers des machines à voter sûres ?

La question de savoir s'il faut développer l'utilisation de machines à voter est particulièrement délicate, et elle exige que des cryptologues compétents et des techniciens très qualifiés s'en occupent… ce qui n'est pas toujours le cas. Des appels à la prudence ont été émis par de nombreuses personnalités et mouvements. En France, un rapport du Sénat datant de 2014 préconisait le maintien du moratoire sur les machines à voter décidé en 2007. La CNIL a aussi exprimé des réserves sur le vote électronique.

Les incidents et problèmes semblent trop nombreux pour qu'on envisage aujourd'hui de remplacer au niveau national le bulletin de vote, l'isoloir et l'urne fermée à clef par des ordinateurs s'échangeant des messages et que les citoyens devraient manipuler pour effectuer leurs devoirs électoraux.

Le site *Ordinateurs de vote* (www.ordinateurs-de-vote.org/) et le récent rapport *Ethics and electronic voting* de Chantal Enguehard (https://hal.archives-ouvertes.fr/hal-01016256/document) détaillent les raisons et les faits montrant qu'il faut être prudent et patient.

Cependant, rien n'interdit de chercher à concevoir des méthodes de vote aussi rigoureuses que possible, permettant des contrôles *a posteriori* tout en garantissant l'anonymat des votes. Le calcul homomorphe présenté dans le présent article semble une voie sérieuse : il donne des garanties convenables concernant la protection du secret des votes et autorise le contrôle et le recalcul des résultats, tout en permettant à chacun d'être certain que son bulletin est pris en compte.

Le système *Helios* de vote par Internet (https://vote.heliosvoting.org/), fondé sur le calcul homomorphe et développé par l'université Harvard et l'université catholique de Louvain, est disponible gratuitement et librement. L'association internationale des chercheurs en cryptographie (IACR) l'utilise pour choisir les membres de son bureau… ce qui est un argument sérieux pour croire en ses qualités.

Il faut se méfier de toutes les solutions précipitées en la matière, et il ne faut renoncer à aucune des garanties données par les procédures classiques de vote. Il ne fait cependant pas de doute qu'il y aurait des avantages à pouvoir voter de chez soi, et que si c'était possible de manière sûre, le coût de l'organisation d'élections en serait, à terme, considérablement réduit.

MACHINE À VOTER électronique utilisée à Aulnay-sous-Bois en 2007.

DR