CRAIG GENTRY, LE PIONNIER

© John D. & Catherine T. MacArthur Foundation

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 !

> son correspondant, et lui seul peut déchiffrer le message grâce à sa clé 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.

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 clé publique/clé privée et communique la clé 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 clé publique et transmet le nombre chiffré $\mathscr{C}(V)$ 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 clé 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 clé 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 $\mathscr{C}(V)$, 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'expliquent Véronique Cortier et Steve Kremer dans un article de 2013.

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.

La clé secrète du système, que l'utilisateur doit garder pour lui, comme le C de l'exemple du début de l'article, est ici un long nombre entier impair p, mettons de 500 chiffres binaires. Dans toute la description de la méthode, la taille des entiers manipulés est importante; les opérations ne sont pas faisables à la main, mais ce n'est aujourd'hui pas un problème, puisque n'importe quel téléphone peut manipuler des nombres de plusieurs millions de chiffres.

Un multiple «approximatif» de p est un nombre de la forme $qp+e$, où e est un nombre d'une vingtaine de chiffres binaires introduisant une sorte de bruit. Retrouver p à partir de la donnée d'un ou plusieurs multiples approximatifs de p nécessite des calculs si longs qu'ils sont impossibles à réaliser pratiquement en un temps raisonnable. C'est sur cette impossibilité pratique que se fonde le chiffrement pleinement homomorphe que nous décrivons. Si q comporte beaucoup de chiffres (par exemple plusieurs millions de chiffres binaires), un attaquant

ignorant p ne peut pas faire la différence entre $qp+e$ et un nombre quelconque de même taille.

De ce fait, chiffrer un bit b (b=0 ou 1) par $\mathscr{C}(b)=pq+b+2r$ où r a une vingtaine de chiffres et q plusieurs millions est une bonne méthode : celui qui connaît p n'a aucun mal à retrouver q en faisant la division par p.

Le reste de la division est $b+2r$, qui est pair si b=0 et impair si b=1. Ainsi, celui qui connaît p saura sans mal déchiffrer $\mathscr{C}(b)$. Et celui qui ne connaît pas p ne voit dans $\mathscr{C}(b)$ qu'un nombre quelconque dont il ne tire rien. Ce système de chiffrement est homomorphe pour le XOR et le ET et est donc pleinement homomorphe. Le vérifier est une simple question d'arithmétique. En voici les détails, que vous pouvez passer si vous trouvez cela fastidieux.

Soient b_1 et b_2 deux bits. Chiffrons-les : $\mathscr{C}(b_1)=c_1=q_1p+2r_1+b_1$ et $\mathscr{C}(b_2)=c_2=q_2p+2r_2+b_2$ avec des entiers r_1 et r_2 d'une vingtaine de chiffres, p d'environ 500 chiffres et q_1 et q_2 de plusieurs millions de chiffres. Celui qui connaît p peut calculer le reste de la division par p de : $c_1+c_2=(q_1+q_2)p+2(r_1+r_2)+(b_1+b_2)$. Ce reste est $2(r_1+r_2)+(b_1+b_2)$; puisque $2(r_1+r_2)$ est pair, connaître le reste donne la parité de (b_1+b_2) c'est-à-dire le XOR entre b_1 et b_2. Additionner $\mathscr{C}(b_1)$ et $\mathscr{C}(b_2)$ donne donc, si l'on connaît p, le XOR entre b_1 et b_2 (b_1+b_2 n'est impair que si l'un ou l'autre est impair, mais pas les deux, et est pair dans les deux autres cas). On peut donc faire calculer à un opérateur extérieur des XOR sans qu'il connaisse ni les données b_1 et b_2, ni le résultat qu'il calcule. C'est la propriété d'homomorphisme additif. Notons que le «bruit» sur c_1+c_2 est passé de r_1 et r_2 à $2(r_1+r_2)$, il a donc à peu près doublé.

Pour la multiplication, l'opérateur extérieur calcule : $c_1c_2=(q_1q_2p+2q_1r_2+q_1b_2+2q_2r_1+q_2b_1)p+2(2r_1r_2+r_1b_2+r_2b_1)+b_1b_2$.

La division par p donne le reste $2(2r_1r_2+r_1b_2+r_2b_1)+b_1b_2$ et donc la parité de b_1b_2, c'est-à-dire le ET entre b_1 et b_2 (b_1b_2 est impair si b_1 et b_2 le sont). C'est la propriété d'homomorphisme multiplicatif. Notons cependant que le bruit sur le résultat est maintenant de l'ordre de $4r_1r_2$.

NETTOYER LE « BRUIT »

Cette méthode est donc parfaite à un détail près. Plus on fera de calculs successifs de XOR et de ET, plus le bruit introduit par les $2r$ augmentera en taille et cela en particulier à cause des ET. Ce n'est pas grave si l'on n'effectue que quelques opérations, mais cela devient très ennuyeux si le bruit atteint la taille de p, car alors on ne peut plus retrouver (b_1+b_2) et b_1b_2.

En effet, si le bruit devient supérieur à p, le reste n'est plus comme il faut (car le quotient augmente de 1 ou plus) pour connaître la somme et le produit des deux bits codés. La méthode n'est bonne qu'à la condition d'opérer >

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 clé 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 de vote par Internet Helios (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