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