

Protocole de Vote Universellement Vérifiable

GRECC (Groupe de Recherche en Complexité et Cryptographie)
Département d'informatique, École normale supérieure
45, rue d'Ulm – 75230 Paris Cedex 05

1 Encadrement

Ce stage se déroulerait de 4 à 6 mois au sein GRECC, dans le département d'informatique de l'École normale supérieure, sous la direction de David Pointcheval (chargé de recherche CNRS au département d'informatique de l'ENS) – <http://www.di.ens.fr/~pointche> – David.Pointcheval@ens.fr

2 Vote électronique

2.1 Généralités

Les élections et les référendums nécessitent le déplacement de tous les participants au vote. Or, il est difficile de convaincre tout le monde de faire ce déplacement, alors qu'il serait si facile de voter de chez soi, de façon électronique. Les avantages seraient multiples : un plus grand nombre de participants, dépouillement automatisé et donc plus rapide, etc. Cependant, une telle procédure nécessite au moins les deux propriétés suivantes :

- *vérifiabilité* : chacun veut être en mesure de vérifier que son vote a été considéré et que le scrutin final est correct.
- *anonymat* : chacun veut conserver le secret de son vote.

Ces deux propriétés semblent contradictoires, car pour vérifier le résultat du scrutin, il faut voir toutes les étapes du calcul. Mais en fait, les calculs cryptographiques, et notamment les calculs sur des valeurs chiffrées, permettent ces opérations sans pour autant *ouvrir* les enveloppes et donc rompre le secret des votes.

De nombreuses autres propriétés sont également souhaitables, pour apporter les mêmes garanties que les méthodes de vote à bulletins secrets papier :

- *incoercibilité* : nul ne peut contraindre qui que ce soit de voter contre son choix.
- *incorruptibilité* : l'achat de vote n'est pas possible (où un corrupteur récompense un votant en l'échange de la preuve du contenu de son vote).

La différence essentielle entre ces deux notions est que, dans la première, le votant n'est pas co-opératif avec le mal-honnête ; alors que dans le cas de la corruption, le votant veut bien voter ce qu'on lui dit, en échange d'une récompense.

2.2 Nouveau protocole de vote

Notre équipe a récemment proposé un nouveau protocole de vote électronique [1] qui présente toutes les propriétés ci-dessus, notamment

- chacun peut vérifier que le scrutin final, ainsi que des scrutins partiels, sont corrects ;

- cependant, le vote de chacun reste secret ;
- des modules permettent d’apporter l’incoercibilité et l’incorrupibilité.

Ce protocole utilise du chiffrement homomorphe. C’est-à-dire que chacun chiffre son vote v dans un cryptogramme $c = E(v)$. Ce dernier est alors envoyé à l’autorité. La propriété homomorphe garantit que le déchiffré du produit des cryptogrammes vaut la somme des messages clairs (les votes) :

$$D(\prod c_i) = \sum v_i.$$

Ainsi, tout le monde peut effectuer le produit de tous les cryptogrammes, puis l’autorité déchiffre ce produit. On obtient alors de résultat du scrutin.

Le chiffrement homomorphe utilisé permet de plus un scrutin à candidats multiples (nombre de protocoles se limitent à la situation du référendum avec une simple alternative OUI/NON).

Ce protocole de vote a déjà été implémenté : <http://www.di.ens.fr/~pointche/vote>.

Cependant, cette implémentation n’est pas complète pour une véritable utilisation. En effet, le processus brièvement expliqué ci-dessus présente l’inconvénient que l’autorité a le pouvoir de déchiffrer chaque vote. Or, on n’a aucune raison de faire confiance à une quelconque autorité. Dans la description originale [1], il est proposé de distribuer la phase de déchiffrement : pour déchiffrer un cryptogramme, au moins t autorités doivent co-opérer. On utilise pour cela des techniques de calculs secrets multi-parties.

3 Objectifs du Stage

Tel que présenté dans [1], le protocole est parfaitement adapté à un usage pratique, notamment dans un environnement Internet via une interface Web. Les calculs à effectuer sont assez simples comme l’atteste la maquette déjà effectuée.

Le but de ce stage est de distribuer la phase cruciale pour la sécurité : le calcul du scrutin.

Ainsi, après une bonne compréhension des différentes primitives cryptographiques mises en œuvre (chiffrement, signature, preuves de connaissance, calcul secret multi-partie, etc), il sera demandé de distribuer le processus de déchiffrement, actuellement effectué par un serveur seul, parmi plusieurs serveurs.

Un tel stage permettra de se familiariser avec de nombreuses notions de cryptographie. Il nécessite cependant certaines compétences en programmation (en C et si possible en Java).

Références

- [1] O. Baudron, P.A. Fouque, D. Pointcheval, G. Poupard, et J. Stern. Practical Multi-Candidate Election System. Dans *PODC '01*. ACM, 2001.
Disponible sur <http://www.di.ens.fr/~pointche/pub.html>.