Conception et analyse d’un système de vote électronique satisfaisant aux exigences de sécurité modernes.

Le vote électronique est un domaine concret qui nécessite de nombreuses propriétés de sécurité. Tout d’abord, il est nécessaire d’authentifier les votants légitimes et de s’assurer qu’ils ne puissent pas disposer de plusieurs voix : on parle d’éligibilité. Il faut ensuite pouvoir calculer le résultat du vote de manière vérifiable, c’est-à-dire fournir une preuve qu’il est cohérent avec les bulletins reçus. Enfin, tout cela ne doit jamais compromettre le secret du vote.

Pour chacune de ces problématiques, la cryptographie fournit des solutions acceptables, mais il n’existe pas encore de protocole de vote électronique qui réponde simultanément à toutes. Pour faire face à ce défi, nous avons d’abord étudié la phase de dépouillement (ou tally), qui consiste à obtenir le résultat à partir des bulletins émis. En effet, la littérature ne permet jusque-là que de faire des dépouillements très basiques, comme d’obtenir le nombre de fois que chaque choix a été effectué. En utilisant des techniques de Multi-Party Computation, nous avons proposé de nouvelles méthodes de dépouillement pour des systèmes de vote plus complexes comme Single Transferable Vote, Condorcet ou encore le Jugement Majoritaire. Pour ces méthodes, l’usage était de révéler en clair l’ensemble des choix effectués par tous les votants, ce qui donne trop d’informations au regard du secret du vote. Notre contribution est donc de proposer des méthodes de dépouillement « tally-hiding », qui ne révèlent rien de plus que le résultat. Afin de pouvoir traiter la phase de tally séparément, et garantir que ses propriétés de sécurité ne soient pas dégradées par les autres phases du protocole de vote, nous avons établi la sécurité de nos protocoles de tally dans un exigeant cadre de composition, dit « UC framework ». Cela a nécessité des preuves cryptographiques qui permettent de réduire les propriétés de sécurité comme le secret du vote à des hypothèses de sécurité comme le problème Diffie-Hellman Décisionnel.

Parallèlement à nos recherches sur le tally-hiding, nous nous sommes intéressés à des propriétés de sécurité plus complexes comme le cast-as-intended (le votant peut-il être sûr que son bulletin contient bien la bonne intention de vote, même quand son appareil de vote est compromis ?) et la coercion-resistance (un votant ne doit pas pouvoir convaincre l’attaquant du contenu de son vote, même s’il collabore avec lui durant la phase de vote). Concernant la coercion-resistance, bien que cette notion ait presque vingt ans, il n’y a pas encore de définition (cryptographique) précise dans la littérature. Motivés par les attaques que nous avons trouvées sur tous les schémas dit « coercion-resistant », nous proposons une nouvelle définition de la coercion-resistance, ainsi qu’un schéma qui respecte cette notion. Nous nous efforcerons par la suite de prouver cryptographiquement que notre schéma respecte notre notion de coercion-resistance.