Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

THESIS / THÈSE

MASTER EN SCIENCES INFORMATIQUES

Sécurisation du vote électronique sur internet

Jeanmoye, Francis

Award date:
2005

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 20. Apr. 2024

FACULTÉS UNIVERSITAIRES NOTRE-DAME DE LA PAIX, NAMUR

INSTITUT D'INFORMATIQUE

RUE GRANDGAGNAGE 21, B-5000 NAMUR (BELGIUM)

SÉCURISATION DU VOTE ÉLECTRONIQUE SUR INTERNET

Francis Jeanmoye

Mémoire présenté en vue de l'obtention du grade de licencié en informatique

Année Académique 2004-2005

Résumé

Ce mémoire a pour but de définir les critères de sécurité qui doivent impérativement être respectés lors d'une élection, de chercher les failles dans différents protocoles existants et, au vu de celles-ci, de tenter d'en définir un qui réponde à tous les critères fixés.

Nous ne polémiquerons pas, dans ce mémoire, sur le bien-fondé de l'utilisation de l'Internet dans les procédures de votes, d'autres l'ont fait avant nous et une large littérature existe déjà à ce sujet.

Nous ne parlerons pas non plus de la fiabilité du transport des données et du matériel nécessaire à l'organisation d'une telle élection ; nous ferons donc abstraction de toute contingence matérielle pour nous centrer uniquement sur le protocole proprement dit ; les informations devant voyager sur la toile, les données des messages sont donc vulnérables aux attaques externes et un protocole permettant la tenue d'une telle élection ne doit souffrir d'aucune faille de sécurité.

Nous présenterons d'abord les différentes manières d'utiliser l'électronique dans une élection, en marquant la différence entre le vote électronique (« e-voting ») tel que nous le connaissons en Belgique, et le vote par l'Internet (« i-voting »).

Quelques solutions commerciales et autres existent déjà sur le marché ; nous analyserons quelques-unes d'entre elles afin d'en déceler les points forts et les points faibles, et verrons d'après cette analyse si les protocoles que celles-ci proposent peuvent être qualifiés de protocoles sécurisés ou non.

A partir d'un protocole simpliste, nous élaborerons différentes améliorations de celui-ci, arriverons à certaines conclusions à propos de ces différentes évolutions et tenterons d'arriver à un protocole qui respecte les 6 critères que nous nous serons fixés comme base pour un vote sécurisé.

Pour conclure, nous envisagerons la possibilité d'utiliser un tel protocole dans la vie réelle.

Summary

The goal of this thesis is to define some security rules that should absolutely be respected during an election, to find the flaws in different existing protocols and, thanks to these, we will try to build a protocol that meets all the defined criteria.

We won't discuss, in this thesis, about the validity of using the Internet for election procedures, other people did this before and there is a wealth of material on this subject.

We won't either speak about the reliability of data transport nor about the material needed to realize such an election; we will consider that the material needed is available and we will focus on the protocol itself; all the data have to travel on the net, so they are easily reachable by external attacks; thus, a protocol allowing the performance of such an election must be absolutely flawless.

We will first show different ways of using electronics to perform elections, showing the different between electronic voting (e-voting), like the system used in Belgium, and Internet voting (I-voting).

Some commercial solutions are already available; we will analyse some of them to find which are strong and weak points, and, after analysing these, tell if these may be qualified as secure protocols or not.

From a simplistic protocol, we will build, step by step, different improvements of this one, we will also build conclusions about some protocol families and we will attempt to create a protocol responding to all the fixed criteria.

As conclusion, we will consider the possibility to implement such a protocol in the real life.

Avant-Propos

Ce mémoire de fin d'étude a représenté une charge de travail conséquente, bien plus que nous ne l'imaginions au départ ; la profusion d'information obtenue lors de nos recherches nous ont demandé un gros travail de lecture et de sélection avant même que de commencer le travail proprement dit.

Grâce à l'aide, aux interventions et au soutien de certaines personnes, ce travail a enfin pu être finalisé.

Je remercie vivement les personnes suivantes :

M. John SEIBEL, Président de la société TrueBallot.com

M. Ivan FONT, Marketing Manager de la société Scytl.com

M. Jean RAMAEKERS professeur et promoteur aux F.U.N.D.P.

M^{elle} Isabelle LINDEN, coordinateur pédagogique et doctorante aux F.U.N.D.P.

Merci également à toutes les personnes qui, par un mot, une phrase, une suggestion, une idée, m'ont permis d 'avancer dans mon mémoire.

Je ne pourrai jamais assez remercier ma famille, qui, pendant ces trois ans où je suis redevenu étudiant, m'a supporté, m'a aidé et encouragé afin que j'atteigne le but final de cette licence à horaire décalé. Sans leur soutien, je ne sais pas si j'aurais pu surmonter certains moments de découragement.

Table des matières

Introduction

Internet est partout : dans les maisons, les écoles, les bureaux, les administrations, les commerçants ; depuis quelques années, l'essor d'Internet l'a rendu indispensable pour un grand nombre de personnes.

Aujourd'hui, de plus en plus, de nombreuses opérations s'effectuent par le biais de la toile : achats en ligne, réservations, demandes de documents, gestion de comptes en banque ... .

Et qu'en est-il au sujet des élections. Est-il envisageable que, d'ici quelques années, des procédures complètement automatisées permettent de voter à distance, sans bulletin de papier, et d'obtenir les résultats fiables endéans les quelques minutes qui suivent la clôture des votes ?

Alors que l'informatique apporte des solutions dans toutes les opérations quotidiennes fastidieuses, ajoutant à la facilité la performance et l'absence d'erreur, il semble que, pour ce qui est des élections, la chose ne soit pas aussi aisée.

Certains projets existent, des produits sont déjà commercialisés et des essais à grande échelle ont déjà été effectué. Ces produits sont-ils fiables ? Offrent-ils autant, ou même plus de garanties que les élections dites « classiques », où le grand nombre d'acteurs, la profusion de petites entités, la défiance entre personnes travaillant ensemble le temps d'une élection rendent très fortement improbable une fraude à grande échelle ? Nous regarderons de plus près les solutions proposées leurs atouts et leurs faiblesses.

Le matériel existe, les liaisons existent, les systèmes de liaison sécurisées entre entités existent, les moyens de chiffrement existent ; le tout est de les faire travailler ensemble pour une même cause : un vote sécurisé sur Internet.

Il existe aussi une polémique au sujet du vote électronique sur Internet ; est-il judicieux ou non d'accepter le vote à partir de n'importe quel endroit, sans surveillance ? Un tel système ne risque-t-il pas d'amener à des dérives, telles que de contraindre une électeur à voter pour un candidat, en assistant à son vote ? Des opposant au système existent [*PourEVA*]. Ces discussions sortent du cadre de ce mémoire et nous n'en parlerons pas.

Nous allons donc tâcher, en considérant que nous avons le matériel ad hoc, les liaisons sécurisées (mais sujettes à des attaques)et les protocoles de chiffrement, de construire un protocole qui permette l'organisation d'élections sécurisées sur Internet.

Chapitres

Chapitre I. E-Voting, I-Voting

A. Système d'élection

Avant de parler du vote électronique, il est bon de rappeler le fonctionnement d'une élection avec bulletin de vote en papier.

En vue de définir les exigences à appliquer pour la création de systèmes de vote électronique, nous devons d'abord nous baser sur l'existant, les élections que nous pourrions dénommer "élections avec bulletin de vote en papier".

1. Qu'est ce qu'un système d'élection classique?

Fig 1 *Bureau de vote*

Rappelons qu'une élection est un choix de candidats effectué par la voie des suffrages. Le suffrage dit "universel direct", est un système par lequel le corps électoral est constitué de tous les citoyens qui votent directement pour les candidats à élire.

Quels sont les différents acteurs d'une élection :

- ☑ Les électeurs : l'ensemble des personnes qui ont le droit de voter ; ceux-ci constituent le corps électoral.
- ☑ Les votants : ce sont les électeurs qui participent à l'élection, et qui font donc usage de leur droit de vote, en remplissant en secret et anonymement un bulletin de vote qu'ils placent ensuite dans une urne.
- ☑ Les candidats : ce sont les personnes qui se présentent sur les listes et pour lesquelles les électeurs sont invités à voter et à faire leur choix
- ☑ Les membres du bureau de vote : ce groupe de personnes est chargé du bon déroulement de l'élection en ce qui concerne les votants du bureau dont il s'occupent. Ils sont chargés de noter chaque électeur venant voter et de l'authentifier, afin d'être certain qu'il est autorisé à voter et qu'il ne vote qu'une seule fois. Ils vérifient aussi que le bulletin de chaque votant soit placé dans l'urne prévue à cet effet.

Fig 2 *Isoloir*

- ☑ Les membres des équipes de dépouillement : lorsque l'élection est terminée, les urnes sont ouvertes et les votes des bulletins sont comptabilisés. La somme des résultats obtenus par les différentes équipes de dépouillement donnera le résultat de l'élection.

Avant de pouvoir procéder à une élection, il faut établir la liste des personnes qui pourront participer à celle-ci, selon des critères qui sont variables d'une élection à l'autre, mais qui doit être figée avant de commencer l'opération du vote proprement dit.

Quant au matériel proprement dit, il se compose principalement de :

- ☑ Bulletins de votes : chaque électeur se présentant au bureau de vote pour voter en reçoit un ; il se rend dans l'isoloir pour le compléter en secret avant de le déposer dans l'urne.
- ☑ Urnes : dans chaque bureau de vote se trouve une urne, que les votants remplissent avec leur bulletin de vote. De cette manière, le vote de chacun sera traité de manière anonyme.

2. *Schéma d'un système d'élection classique*

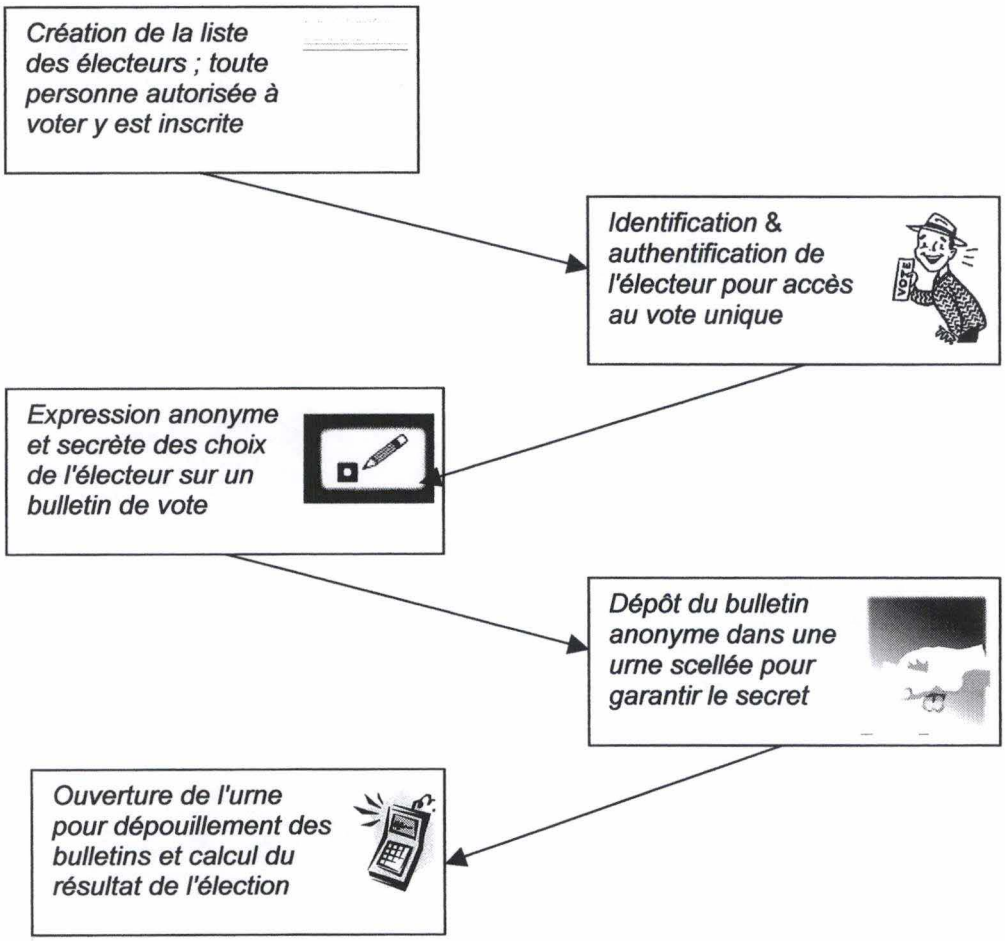


Fig 3 *Schéma d'une élection classique*

De tels systèmes d'élections dit "classiques", sont depuis très longtemps en fonction et peuvent être considérés comme corrects si l'ensemble des intervenants humains (votants, membres du bureau de vote, membres des équipes de dépouillement) sont tous de confiance et effectuent leur tâche sans erreur.

Si tel est le cas, nous avons alors un système d'élection répondant à différentes caractéristiques qui sont les bases de tous systèmes d'élections officielles, c'est-à-dire:

- *Anonyme :* il est impossible de connaître l'identité de l'électeur à partir d'un bulletin de vote (afin d'éviter les collusions et les contraintes)
- *Secret :* le vote de chaque électeur est inconnu et confidentiel;
- *Correct :* tous les votes exprimés sont interprétés et comptabilisés correctement;
- *Honnête :* personne ne peut voter plus d'une fois ou changer le vote d'une autre;
- *Complet :* tous les électeurs doivent voter ou justifier leur absence (ce dernier point n'étant pas requis pour toutes les élections, mais, puisque nous sommes en Belgique et que ce point est exigé lors des élections belges, nous le signalons);

Au départ de la procédure d'élection, les électeurs sont identifiés mais nous ne pouvons connaître la valeur de leurs votes et si nous connaissons un vote, par exemple au moment du dépouillement, nous ne pouvons pas le rattacher à l'électeur.

Après la clôture de l'élection, tous les identifiants des électeurs et tous les choix des votes peuvent être publiquement connus, mais la relation entre électeur et vote est impossible et inconnue.

La validité des systèmes "classiques" repose donc uniquement sur des valeurs humaines avec le respect de procédures strictes et l'exécution correcte des tâches prévues Le respect de celles-ci repose entre autres sur la surveillance mutuelle qu'exercent l'un sur l'autre les membres des bureaux de vote et de dépouillement ainsi qu'aux différents observateurs.

3. Vote informatisé

Dans beaucoup de domaines, l'arrivée de l'informatique a permis une accélération du travail ; celle-ci a aussi permis de supprimer les erreurs dues à des facteurs humains, permettant ainsi d'obtenir un résultat plus digne de confiance, ainsi qu'une plus grande sécurité. Toutes ces qualités seraient les bienvenues dans un système d'élections.

Il serait trop simpliste de qualifier, par défaut, une méthode d'élection utilisant la technologie informatique, plus sécurisant et aussi correcte qu'un système d'élection classique reposant exclusivement sur des intervenants humains. Il faudra donc fournir différentes preuves attestant de la validité des modèles d'élections utilisant cette technologie *[The Bell].*

Il faudra donc pouvoir fournir des preuves qui devront être évaluables objectivement, notamment la confiance en la validité de l'information qui circule dans l'architecture informatique mise en place. Cette vérification peut intervenir à deux niveaux : une auto-vérification dans le système lui-même

une vérification par l'électeur

a) Vérification par le système d'élection

Problème

Comment un système d'élection électronique peut-il prouver que le vote reçu dans l'urne est le même que celui "noirci" sur le bulletin de vote par l'électeur?

Le votant n'a pas la possibilité de savoir et de contrôler si le vote qu'il a exprimé est arrivé dans l'urne électronique via le canal de communication avec la même valeur qu'à l'origine.

Solutions proposées

Certaines architectures de systèmes d'élections électroniques proposent une impression d'un ticket-preuve sur lequel l'électeur peut vérifier si le vote est identique à celui qu'il a exprimé sur un terminal de vote informatisé ; l'électeur doit ensuite placer son ticket dans une urne "classique" au bureau de vote tandis que son vote électronique est transféré, par un autre canal de communication, dans une urne électronique. L'urne classique pourra toujours être utilisée en cas de contestation afin de vérifier la validité du vote électronique.

Cette architecture propose une solution utilisant deux canaux de communications indépendants pour le bulletin de vote; un via le vote électronique, et un autre via l'impression du bulletin papier et le placement de celui-ci dans une urne traditionnelle. Nous sommes ici en présence d'une solution utilisant 2 canaux indépendants.

Critique

Malgré la redondance de canaux, cette solution n'apporte pas de "confiance en l'information" objective en cas de problème.

En effet, si une différence est observée entre les résultats fournis par le vote électronique et les résultats des votes sur ticket papier, il n'y aura pas de solution au travers du système ainsi défini. Il faudra donc de manière subjective ou par une règle établie donner la préférence à un des deux résultats. Cette manière de procéder n'est donc pas la panacée ; une décision extérieure au système est nécessaire afin de solutionner le problème. De plus, un système tel que celui-ci augmente les possibilités de fraudes pour modifier ou faire annuler une élection.

Conséquence

Afin d'obtenir un modèle qui puisse prendre les décisions adéquates, il s'agit de multiplier le nombre de canaux indépendants (au minimum 3) ; plus il existe de ces canaux, plus grande sera la confiance en ce modèle d'organisation.

Mais tous ces canaux sont-ils réellement indépendants ? En admettant que le vote soit corrompu par un élément perturbateur à l'intérieur même du terminal avant son envoi, la multiplication des canaux d'envoi n'augmenteront pas la fiabilité de l'élection.

Quant aux modèles utilisant un seul canal de communication, il reposent sur une confiance absolue dans le bon fonctionnement des différents acteurs du système (matériel et humain), mais n'offrent aucune solution objective de vérification, à moins d'offrir une possibilité de retracer le trajet complet d'un vote.

Problème

Comment un système d'élection électronique peut-il prouver que l'urne électronique ne contient que les votes placés par les votants, et qu'aucun ajout n'a été effectué ?

Le votant n'a pas la possibilité de savoir et de contrôler si tous les votes qui sont dans l'urne électronique proviennent de votants.

Solutions proposées

Certaines architectures de systèmes d'élections électroniques proposent un comptage des votants et, en parallèle, un comptage des votes. Pour que l'élection soit correcte, le nombre de vote doit être équivalent au nombre de votants.

Critique

S'il est vrai que ce contrôle permet d'accentuer la robustesse du système, il a toutefois une limite : qui peut être certain qu'un vote se trouvant dans la liste des votes à l'issue de l'élection correspond au choix d'un votant ? Il se pourrait qu'un système « oublie » de comptabiliser des votes, et remplace ceux-ci par d'autres.

Conséquence

Afin d'obtenir un modèle qui puisse prouver que tous les votes sont des votes « valides », c'est-à-dire des votes qui ont été mis dans l'urne par des votants, il faut que le système puisse prouver que tous les votes appartiennent à des électeurs ; un système peut l'affirmer, il ne peut en aucun cas le prouver, puisque, pour prouver, il faudrait pouvoir comparer ; la seule personne à même de vérifier qu'un vote est correct, c'est le votant ; lui seul sait pour qui il a voté.

b) Vérification par l'électeur

Afin de prouver que le système d'élection électronique reflète la réalité des votees introduits par les participants, il faudrait que ce système puisse permettre au votant d'avoir la certitude que ce qui paraît avoir eu lieu s'est déroulé tel qu'annoncé :

☑ La présence de son vote dans l' « urne »

☑ La comptabilisation de son vote à l'issue du scrutin.

La possibilité de vérification de ces informations augmente la confiance que l'on peut placer dans un système d'élections électroniques.

Ces vérifications ne sont aucunement obligatoires, mais du fait même de leur existence, est un moyen efficace de dissuasion contre d'éventuelles fraudes, puisque personne n'a la possibilité de savoir quel électeur effectuera une vérification, ni quand celle-ci aura lieu.

Il est très important, pour la qualité d'un système de vote électronique, que seul l'électeur soit susceptible d'effectuer cette vérification ; aucune autre personne ne peut avoir le droit de consulter ces informations ; si ces informations pouvaient être fournies à d'autres personnes que l'électeur, il existerait des risques de collusion ou de contrainte pour l'électeur.

Il est donc primordial qu'aucune information, hormis le vote lui-même, ne soit commune entre l'organisateur de l'élection et l'électeur lui-même.

c) Confiance de l'électeur

Quelles raisons poussent un électeur à avoir confiance en une élection classique, alors qu'il est réticent à croire en la validité d'un vote électronique ? Tout d'abord, l'électeur est souvent convaincu qu'un système d'élection traditionnel peut être faussé si un nombre suffisant de personnes participant à l'organisation de l'élection sont corrompues. Néanmoins, le fait qu'une énorme quantité de bulletins de vote sur support papier soient comptabilisés et vérifiés en des endroits différents par des gens différents représente un obstacle difficilement surmontable pour une fraude massive.

Par contre, ce même électeur est souvent convaincu qu'une fraude dans les systèmes et réseaux informatique pourrait modifier des millions d'enregistrements de votes électroniques en très peu de temps ; il faudra donc le convaincre de la validité, de la résistance aux attaques, de la robustesse d'un système de vote électronique afin que celui-ci soit accepté par un électorat à priori réticent.

B. E-Vote

Plusieurs pays européens - dont la Belgique - sont déjà bien avancés dans le vote électronique E-Vote. Ce système est une « copie électronique » de la procédure de vote classique. La caractéristique principale de l'E-Vote est que ce vote électronique n'utilise pas de connexions réseau. Le principal atout d'un tel système est d'obtenir un comptage plus rapide des votes, diminuant ainsi la charge de travail des assesseurs.

La Belgique a une grande expérience dans ce type d'élection, utilisant des cartes magnétiques pour remplacer le traditionnel bulletin de vote papier. Ce vote se caractérise par une grande similitude avec le vote traditionnel, à ceci près que le bulletin de vote est remplacé par une carte magnétique, que le crayon est remplacé par un écran tactile, et que l'urne qui reçoit la carte effectue une lecture de celle-ci pour le comptage total.

Un autre système, de la firme NEDAP (NV Nederlandische Apparatenfabriek NEDAP, fabricant de machines à voter depuis 1975), est utilisé pour des élections officielles dans plusieurs pays européens comme les Pays-Bas, l'Allemagne, la France ; notons toutefois que l'Irlande, suite à un rapport indépendant concernant ce système, commandé par le premier ministre, a abandonné le projet de vote électronique pour les élections européennes de 2004. Nous étudierons de manière plus approfondie ce système dans le chapitre « Analyse de l'existant ». [*NEDAP*] [*Irlande*]

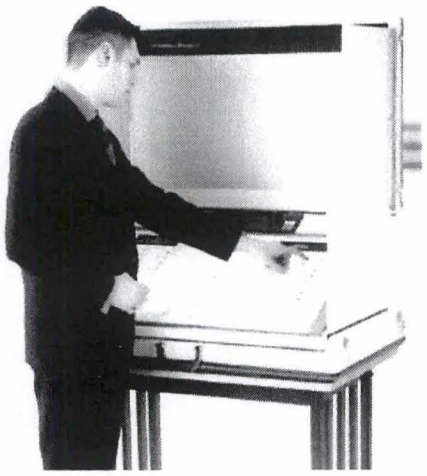


Fig 4 *Machine à voter NEDAP*

C. I-Vote

Depuis quelques temps déjà, des solutions d'élections électroniques utilisant des architectures connectées au réseau Internet ou dites "en ligne", sont proposées par des sociétés privées telles que : "Election.com" (devenu « Accenture eDemocracy services »), "SafeVote", "VoteHere", "CyberVote", etc

L'architecture présentée utilise à chaque fois les techniques de chiffrement et de sécurisation de l'information pour répondre aux règles de secret et d'intégrité des votes exprimés.

Jusqu'à présent, à part quelques expériences (Genève 2003, Mérignac et Vandoeuvre 2002, Canberra 2003, ...) , seules des initiatives d'élections privées ou des référendums emploient de telles architectures.

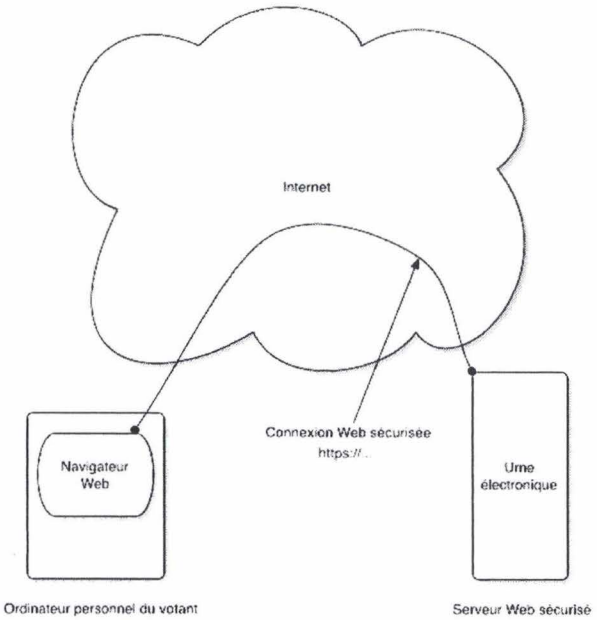


Fig 5 *Voter par l'Internet : Schéma*

Nous sommes peut-être arrivés à un tournant important dans l'histoire du vote électronique au travers d'un réseau car, de plus en plus, les Etats s'y intéressent, commandant des études de faisabilité, ou vont même jusqu'à organiser des élections parallèles lors d'élections officielles réelles (élections primaires présidentielles du parti Démocrate dans l'état d'Arizona, organisées par la société privée Election.com en mars 2000) [*Arizona 2000*]

De grands débats idéologiques sont également initiés pour répondre aux interrogations apportées par le vote électronique à distance telles que:

- ☑ Le vote à distance est-il propice aux influences ou aux corruptions d'électeurs?
- ☑ Le vote à distance est-il un remède contre l'abstention?
- ☑ Une nouvelle démocratie: "La cyber-Démocratie" ou E-Démocratie.

Par exemple, depuis plusieurs années, est organisé un "Forum IDémocratie" au mois de mai à Issy-les-Moulineaux. Des "tables rondes" réunissant les spécialistes et acteurs du vote électronique, tant institutionnels que privés, entraînent entre autres des discussions sur des sujets tels que ceux présentés ci-dessus. [*Forum Mondial IDémocratie*]

L'Europe suit également le mouvement avec la mise en place du projet E-POLL qui a pour but de fournir un système global de vote électronique pour les élections démocratiques, les rendant plus simples à organiser et plus accessibles aux citoyens. Le système a été testé à petite échelle en 2002 en France (en 2004 en Italie.[*E-Poll*]

La Commission européenne a suivi avec intérêt le projet "EU-Studentvote" qui, du 9 au 23 mai 2002, avec l'aide de la société Election.com, organisa la première élection en ligne à l'échelle européenne et qui permit à 82.000 étudiants d'élire le 'Conseil étudiant européen', qui a vocation d'être l'organe de représentation étudiante auprès des institutions européennes.*[EU-StudentVote]*

La société à capitaux américains "Election.com", avant d'être reprise par Accenture.com, a été active pendant plus de 25 ans sur le marché de l'organisation d'élections et en a coordonné plus de 600 à ce jour. *[Election.com].*

La société organisait, gérait et proposait tous types d'élections sur Internet pour toutes elections politiques, privées ainsi que pour les associations sans but lucratif.

L'objectif d'Election.com était de permettre l'augmentation de la participation d'électeurs au processus démocratique de leur pays, de leur région, de leurs sociétés ou associations grâce à l'utilisation d'un simple navigateur WEB sur Internet.

Aux Etats-Unis, il est fréquent de confier les tâches d'organisation d'élections à des sociétés privées spécialisées comme "Election.com".

Pour l'organisation des élections primaires Présidentielles du parti Démocrate dans l'état d'Arizona, la société "Election.com" implémenta un système qui offrait 3 options ou possibilités de votes aux électeurs démocrates.

- ☑ Option 1 : Le vote classique papier dans un bureau de vote.
- ☑ Option 2 : Le vote sur un ordinateur connecté au réseau mais dans un bureau de vote.
- ☑ Option 3 : Le vote par Internet à partir de l'ordinateur de l'électeur.

L'élection, organisée en mars 2000, a été la première élection ayant valeur légale et utilisant une technique de vote à distance.

Rappelons que toute architecture de vote électronique à distance ou par Internet nécessite trois phases :

1. Constitution du corps électoral

Les électeurs doivent être enregistrés dans une base de données centralisée et doivent être en possession d'un code qui leur permettra un accès personnel (Identification, code secret PIN, biométrique,...) pour participer à l'élection.

2. Vérification du droit de vote, et vote proprement dit

Au moment du vote, l'électeur doit être identifié pour lui envoyer un bulletin de vote électronique. L'ordinateur de l'électeur ou la station de vote transmet le vote chiffré aux serveurs de l'élection.

3. Comptabilisation des votes

A la fin de l'élection, l'ordinateur de dépouillement comptabilise les votes tout en respectant les règles d'anonymat de l'électeur.

Différentes sociétés privées et institutions publiques se sont déjà attelées à la tâche et proposent différents systèmes que nous nous proposons d'analyser.

Chapitre II. Analyse de l'existant

Nous nous contenterons, dans ce chapitre, de passer en revue une partie des produits disponibles sur le marché. Les produits « e-voting » ne faisant pas partie du corps de ce travail, Nous nous focaliserons sur les produits « I-voting », qui, de plus en plus, sont présents en force sur le marché, pour tout type d'élection.

A. Election.com

[*Election.com*]

1. Présentation

Cette société, active dans le domaine du vote électronique depuis 1998, n'existe plus en temps que telle et fait maintenant partie de la société de consultance Accenture ; c'est entre autres elle qui s'est occupée de l'organisation des élections primaires présidentielles du parti Démocrate dans l'état d'Arizona en 2000, et et qui a aidé au déroulement de la première élection en ligne à l'échelle européenne (EU-StudentVote) qui permit à 82.000 d'étudiants d'élire le « Conseil étudiant européen ». [EU-StudentVote]

L'authentication de l'électeur est basée sur un code d'identification personnel (PIN) envoyé par la poste, et différentes informations personnelles (pour l'élection en Arizona, les données privées demandées à l'électeur étaient sa date de naissance ainsi que les quatre derniers chiffres de son numéro de sécurité sociale).

2. Remarques

Comme le choix entre le vote papier et le vote électronique reste à l'électeur, il faut que le responsable du bureau de vote vérifie que celui-ci ne s'est pas déjà présenté à un autre bureau pour voter, ou qu'il n'ait d'abord voté sur Internet de chez lui avant de se présenter au bureau. Et lorsque l'électeur choisit de voter sur papier et qu'il n'a pas déjà voté, il faut donner au système l'identité de l'électeur afin d'empêcher celui-ci de voter à plusieurs reprises.

Lorsqu'il vote de manière électronique, l'électeur ne possède aucune information qui lui permettrait de retrouver son vote ; il ne possède pas non plus de trace papier, pas plus que n'en possèdent les bureaux de vote, ce qui empêche tout recomptage. C'est entre autres sur ce point que se bat Rebecca Mercuri. [*Mercuri*].

Puisqu'il est possible à un électeur de voter à partir d'un lieu quelconque, il est tout à fait plausible d'imaginer qu'une personne puisse voter pour une autre, si celle-ci lui a fourni les informations nécessaires à l'identification. Une tel système est la porte ouverte à toutes sortes de marchandages, d'achats, ou même d'extorsions de droits de votes.

Les systèmes et bases de données informatiques pour l'identification des électeurs, la réception des votes et le dépouillement des résultats sont séparés et indépendants ; il n'y a donc pas de lien entre l'identité de l'électeur et le vote exprimé. De plus, aucune preuve papier du vote de l'électeur n'est fournie ; il n'y a donc aucun moyen, si ce n'est la bonne foi de la compagnie, de prouver qu'un vote d'un électeur n'a pas été altéré : le résultat de l'élection n'est donc pas vérifiable.

Une élection hybride, laissant le choix à l'électeur jusqu'au jour du scrutin, devant le bureau de vote, entre le vote papier et le vote électronique demande une gestion «humaine » des électeurs ; pour chaque électeur choisissant le vote papier, le responsable du bureau de vote doit vérifier que celui-ci n'a pas déjà voté électroniquement ; il doit aussi enlever manuellement l'électeur qui choisit le vote papier de la liste des électeurs n'ayant pas voté. Ces manipulations, on peut le concevoir aisément, sont un facteur de risque important ; une « erreur », volontaire ou non, peut facilement arriver.

B. VoteHere.net

[VoteHere.net]

1. Présentation

Présente sur le marché depuis 1998, cette société propose une gamme de produits e-Voting et i-Voting, sous le nom de VHTi (acronyme de « VoteHere Technology Inside »).

Fig 6 *Reçu*

La société part du principe que, pour qu'une élection soit valable, sa validité doit être prouvable de bout en bout. C'est cette vérification qui est effectuée par VHTi.

Chaque électeur, à l'issue de son vote, reçoit un reçu ; celui-ci reprend différentes informations qui permettront à l'électeur de vérifier, à l'issue du scrutin, si son vote a bien été pris en compte, et aussi s'il n'a pas été altéré. Du fait de cette possibilité de vérification, il serait risqué de tenter de modifier le scrutin, vu que personne ne sait qui va vérifier son vote.

La transmission du vote utilise sensiblement le même principe que les tickets de loterie ; il en possède deux caractéristiques intéressantes :

- ☑ Tout d'abord, puisque le billet est pré-imprimé, le jeu ne peut pas être changé une fois l'impression effectuée. Contrairement aux machines à sous, les billets gagnants sont connus au moment de l'impression.
- ☑ Deuxièmement, un joueur qui a gratté une case ne peut faire marche arrière ; il est impossible de « dé-gratter » une case.

VHTi utilise des propriétés semblables pour s'assurer qu'un vote est en toute certitude pris en compte. Au moment du vote, le système crée un set de codes pour le vote, sensiblement pareil à un de ces tickets à gratter, immédiatement après le vote, mais avant de délivrer l'accusé de réception. L'ordre de ces

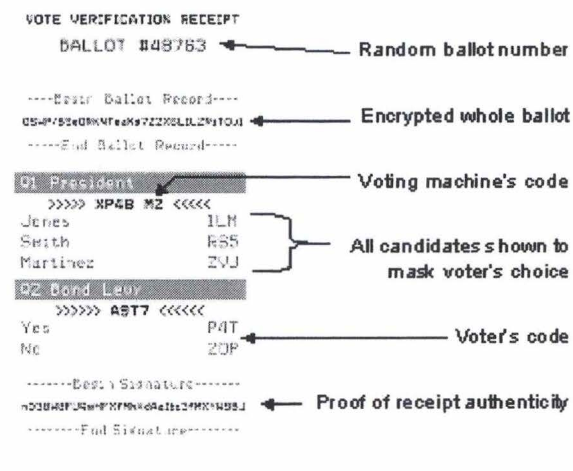


Fig 7 *Reçu (détails)*

opérations est d'une importance primordiale pour que chaque électeur ait le contrôle de son propre vote.

Ensuite, le système prouve à l'électeur que le « ticket à gratter » a été préparé en respectant scrupuleusement son vote, et délivre un accusé de réception que ce dernier peut emporter. Après cette opération, la machine transmet le « ticket à gratter » de l'électeur à l'urne électronique à partir de laquelle s'effectuera le décompte final. L'électeur a la possibilité, grâce à son accusé de réception, de vérifier s'il retrouve bien son vote dans l'urne électronique, s'il a bien été pris en compte, et s'il n'a pas été altéré.

Voici, plus détaillées, les différentes étapes qui permettent la transmission sécurisée du vote d'un électeur. Pour la simplicité de l'explication, nous allons supposer que l'élection ne propose que deux candidats, mais celle-ci serait la même pour un plus grand nombre de possibilités de choix.

1. L'électeur vote pour le candidat B.
2. La machine crée un « bulletin de vote » (du type ticket à gratter) semblable à celui qui figure ci-dessous. Notez que chaque case a la même valeur pour le candidat choisi (candidat B), alors que, pour le candidat non sélectionné (candidat A), les cases sont remplies au moyen de valeurs aléatoires.

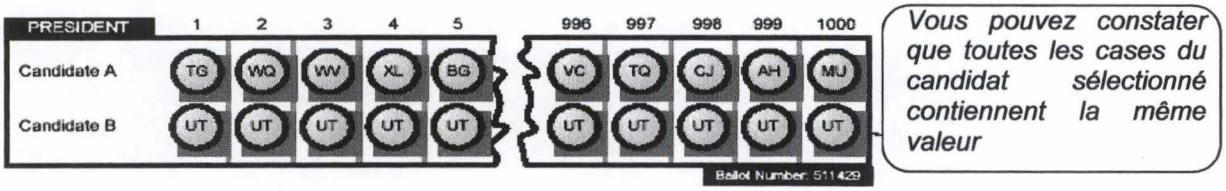


Fig 8 *Transmission du vote (étape 2)*

3. La machine crée un « ticket à gratter » sur base du bulletin de vote en occultant chaque case.

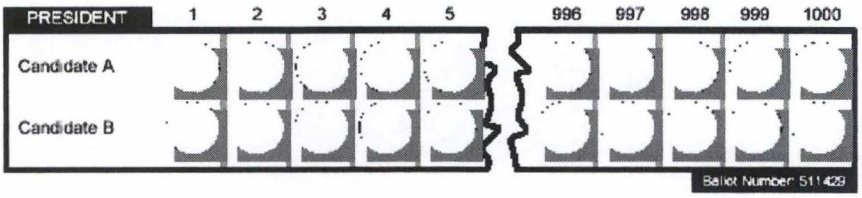


Fig 9 *Transmission du vote (étape 3)*

4. La machine informe l'électeur que, quel que soit la case du candidat B que vous choisissiez, vous trouverez le code « UT » si vous la découvrez.
5. Pour le candidat que vous avez choisi, vous sélectionnez une case quelconque (dans cet exemple, la case 997) et vous la découvrez. Vous vous attendez, bien sûr, à trouver le code « UT » sous celle-ci. Si tel n'était pas le cas, vous auriez pris la machine en flagrant délit de tricherie.

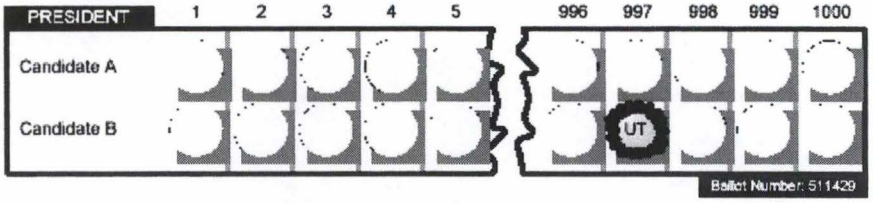


Fig 10 *Transmission du vote (étape 5)*

6. Pour protéger le secret de votre vote, vous découvrez une case de l'autre candidat, pour lequel vous n'avez pas voté (dans cet exemple, l 'électeur choisit de découvrir la case 3)

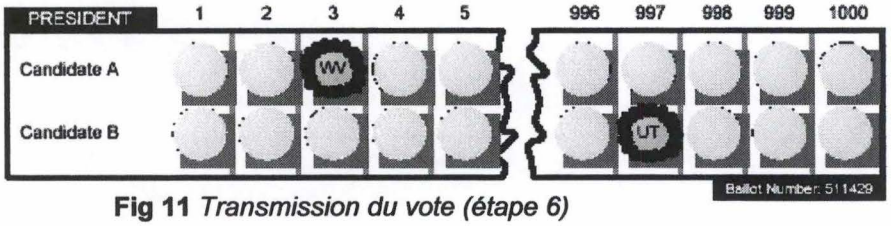


Fig 11 *Transmission du vote (étape 6)*

7. Maintenant que le système a prouvé à l'électeur que c'est bien son vote que se trouve caché derrière ce « ticket à gratter », le vote peut être transmis à l'urne électronique.

   Pendant toute la période précédent le comptage (y compris avant que le scrutin soit clôturé), l'électeur a la possibilité de vérifier que son bulletin est bien dans l'urne, grâce au numéro unique de chaque bulletin. L'électeur peut constater qu'il s'agit bien de son bulletin, avec les même cases dévoilées et contenant les mêmes valeurs.

8. Avant le décompte des voix, le numéro est effacé du bulletin et les bulletins sont mélangés.

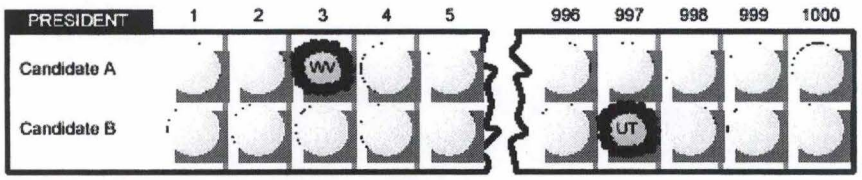
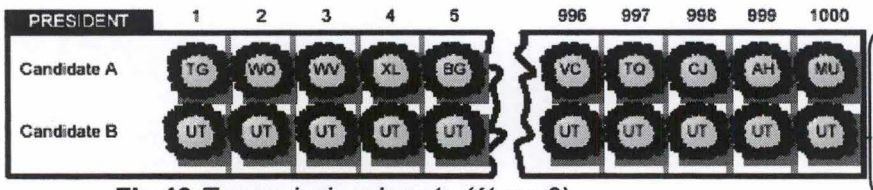


Fig 12 *Transmission du vote (étape 8)*

9. Une fois les bulletins mélangés, toutes les cases de tous les bulletins sont dévoilées, et, pour chaque bulletin, seule la ligne du candidat dont les cases contiennent **toutes la même valeur** sont prises en compte. Dans notre exemple, toutes les cases de la ligne du candidat B contiennent la même valeur « UT » ; une voix sera donc comptabilisée pour lui.



Une voix est ajoutée au candidat B puisque toutes les cases contiennent la même valeur.

Fig 13 *Transmission du vote (étape 9)*

2. *Remarques*

L'avantage de ce « ticket à gratter » est que l'électeur possède un accusé de réception sur lequel figure son vote, mais sous une forme cachée, si bien que nul, si ce n'est l'électeur lui-même, n'est capable de savoir pour qui l'électeur a voté. Si cette procédure permet de certifier que le vote d'un électeur est bien acheminé à bon port jusque dans l'urne électronique, celle-ci manque de rigueur au niveau du comptage ; en effet, si l'on est certain que le vote qui va être comptabilisé est bien celui de l'électeur, il n'y a aucune preuve que ce vote soit réellement comptabilisé : le numéro du bulletin est effacé, les bulletins sont mélangés de sorte que plus personne ne puisse retrouver la trace d'aucun bulletin, et, au terme du comptage, aucun électeur n'a plus aucune trace de son vote ; il ne peut donc pas être certain que son vote soit comptabilisé.

C. SafeVote.com

[*SafeVote.com*]

1. *Présentation*

Autre société commerciale, SafeVote, fut, après deux ans d'activité dans le milieu du vote électronique, lancée sur orbite après la débâcle lors du décompte des élections présidentielles de 2000 en Floride, où les systèmes de vote américains classiques qui étaient utilisés (bulletins de vote classiques, bulletins à cocher, bulletins à remplir, vote sur micro avec un écran à touches .) ont montré leurs limites. Ce fiasco involontairement donné un énorme coup de pouce aux moyens électroniques, qui, du moins dans les esprits des gens pourraient être **LA** solution qui permettrait d'empêcher la fraude et les mises en doute des résultats.

Fig 14 *Logo The Bell*

Membre de l' « IVTA » (Internet Voting Technology Alliance) depuis sa création le 28 février 2000 (les participants à cette réunion comprenaient initialement : Safevote de San Rafael, Californie ; VoteHere, de Kirkland, Washington ; Modulo Security Solutions, de Rio de Janeiro ; l'International Foundation for Election Systems, de Washington, D.C. ; et e-Elections, d'Oakland, Californie.), la société est aussi connue aussi pour son bi-mensuel « The Bell », entièrement consacré au vote électronique.[*The Bell*]

Le 7 novembre 2000, elle organisait - sous contrat avec l'Etat de Californie - un essai d'élections électroniques parallèles au véritable processus électoral. Les électeurs des comtés de Sacramento, San Diego, Contra Costa et San Mateo avaient la possibilité de voter « à blanc » sur l'Internet, Des terminaux étaient mis à disposition dans les bureaux de vote et les électeurs invités à exprimer leur suffrage une deuxième fois par ce biais. Cette expérience, première du genre à cette échelle, devait permettre d'évaluer les logiciels et de les certifier en vue d'opérations réelles. Safevote avait invité les hackers à essayer de pénétrer dans le site et leur avait fourni toutes les informations nécessaires pour y parvenir. Apparemment, personne n'y est arrivé.

En 2001, Safevote a signé un contrat avec la Suède en vue de la fourniture de la technologie nécessaire à l'organisation d'une élection. Celle-ci devait permettre à 12.500 étudiants de l'université d'Umea, située dans le nord de la Suède, de voter pour l'union des étudiants. Cette élection permettait trois types de votes :

- ☑ Par courrier
- ☑ Par Internet
- ☑ Dans un bureau de vote

Contrairement à une élection classique, tout électeur pouvait voter un nombre illimité de fois, seul le dernier vote étant retenu. Pour éviter tout malentendu, chaque option de vote se voit attribuer un poids différent : le vote par Internet prime sur le vote-courrier, et le vote dans un bureau de vote a plus de poids que le vote par Internet.

Peu importe sa façon de voter, chaque électeur devait établir son identité d'électeur au moyen de ce que SafeVote appelle un DVC (Digital Vote Certificate). Ces signatures électroniques, anonymes et chiffrées, doivent permettre aux officiels de vérifier chaque vote off-line. Au moyen des 6 caractères de ce DVC, les électeurs pouvaient consulter un site Web qui leur permettait de vérifier que leur vote était arrivé à bon port et qu'il avait été validé pour le comptage.

2. Remarques

Madame Rebecca Mercuri, professeur de science informatique, spécialiste du vote électronique (sa thèse doctorale concernait l'e-Voting) soutient que le système présenté par SafeVote fait fi de certains dangers qui guettent toute élection par Internet [*Mercuri*].

Selon ses dires, ces dangers ont moins de rapport avec la technologie qu'avec les problèmes sociaux : vente de votes, contraintes, sans parler des fraudes.

La vente de votes était déjà active en 2000 (le site VoteAuction.com vendait des voix aux plus offrant ; lorsque New York a tenté de bloquer ses activités, le site a utilisé une adresse offshore) et la mise des élections sur la toile ne fera qu'augmenter ce type d'activité.

Elle ajoute aussi que le système SafeVote n'est pas robuste vis à vis des possibles pannes de courant, refus de service, qui pourraient toutes deux entraver le bon fonctionnement d'un vote par Internet.

Si, au niveau du transport du vote jusqu'à l'urne électronique, le transport du vote est garanti, la garantie ne va pas jusqu'à prouver son contenu ; selon Ed Gerck, qui dirige la société SafeVote.com, « personne ne doit être en mesure de prouver pour qui quelqu'un a voté ou n'a pas voté ; si tel était le cas, il pourrait être le proie d'un maître-chanteur ou pourrait être tenté de monnayer son vote ».

Pour ce qui est du décompte final, il faut faire une confiance aveugle, car vu l'opacité des bulletins dans l'urne et l'absence de bulletin papier, il n'existe aucune possibilité de recomptage des votes par un second canal.

D. E-Poll

[*E-Poll*]

1. Présentation

E-Poll n'est pas à proprement parler un société active dans le milieu de l'I-Vote, mais plutôt un projet de dimension européenne visant à analyser les différentes options disponibles sur le marché afin de sélectionner celles qui soient le plus à même de convenir à toute 'Union Européenne.

La Commission développe le projet E-Poll qui a pour but d'expérimenter le vote électronique sur des réseaux privés virtuels. Les technologies utilisées sont la biométrie pour la signature, les cartes à puce afin d'identifier les cartes électorales et les écrans tactiles (urnes) pour voter. Il s'agit à terme d'uniformiser ce type de scrutin dans tous les pays de l'Union afin de permettre aux électeurs de s'exprimer depuis n'importe quel bureau de vote.

Allemagne : Lors des prochaines élections en 2006, des bornes connectées à un réseau Internet sécurisé seront installées dans plusieurs points du pays. Aucune date n'a été fixée quant à la généralisation du vote en ligne aux PC des particuliers.

Autriche : L'Université d'Economie de Vienne a développé un prototype de vote électronique qui s'inspire du vote par correspondance. L'électeur s'inscrit sur Internet. Il reçoit ensuite des autorités une 'carte d'électeur électronique' comportant une signature électronique et qui lui permet de rester anonyme au moment du vote". La signature comprend une clé publique et une clé privée. L'électeur crypte son vote avec la clé publique du destinataire. Ce dernier déchiffre le message reçu avec sa propre clé privée." [*Revue Web*]

E. Scytl.com

[*Scytl.com*]

1. Présentation

Le nom de cette société trouve ses origines dans la Grèce antique : en effet, le premier dispositif de cryptographie militaire connu, la **scytale spartiate**, remonte au Ve siècle avant J.-C. La scytale consiste en un bâton de bois autour duquel est entourée une bande de cuir ou de parchemin, comme le montre la figure ci-dessous. L'expéditeur écrit son message sur toute la longueur de la scytale et déroule ensuite la bande qui apparaît alors couverte d'une suite de lettres sans signification. Le messager emportera la bande de cuir, l'utilisant comme ceinture, les lettres tournées vers l'intérieur. Le destinataire enroulera alors cette bande sur son bâton (de même diamètre) pour lire le message en clair.

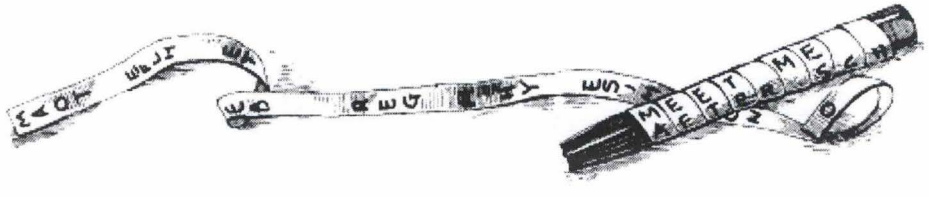


Fig 15 *Scytale spartiate*

La société espagnole Scytl.com a développé un module software qui implémente des protocoles cryptographiques spécialement conçus pour résoudre les problèmes de sécurité et de anonymat dans le vote électronique ; ce produit se nomme Pnyx.core : encore une allusion à l'histoire , puisqu'à Athènes, l'assemblée, l'ecclésia, qui était ouverte à tous les citoyens, se réunissait sur la colline de la Pnyx, au sud-ouest de l'Agora, spécialement aménagée à cet effet.

Pnyx.core a été implémenté avec succès dans différentes plate-formes de vote électronique en Europe, entre autre dans le canton suisse de Neuchâtel, dans lequel une plate-forme permanente de vote par Internet a été installée pour les élections et les référendums. Le software a aussi été récemment utilisé lors de la seconde édition de Madrid-Participa, le projet pilote le plus avancé jamais entrepris en Europe dans le domaine de la démocratie électronique en ce qui a trait à la variété des moyens employés, aux technologies de sécurité utilisées pour protéger la confidentialité et l'intégrité du vote ainsi qu'au nombre prévu de participants. Environ 120.000 résidants du centre de Madrid auront la possibilité de participer, au moyen d'Internet ou d'un téléphone cellulaire ; les citoyens qui votent par téléphone cellulaire ont le choix de voter au moyen du service d'envoi de messages courts (sms) ou d'une application java téléchargeable compatible avec certains types de téléphones cellulaires. Avant de passer au vote, les citoyens doivent faire une demande de certificat numérique en direct ou en se présentant à l'un des bureaux d'enregistrement désignés.

Le module Pnyx.core peut, selon les informations dispensées sur le site de Sctyl.com, être intégré à toute plate-forme de vote électronique afin de garantir le même degré de confiance, de sécurité et d'anonymat que celui qui existe dans un système de vote traditionnel, sans avoir à faire confiance ni aux administrateurs du système ni aux systèmes électroniques complexes utilisés. La société fait d'ailleurs partie, grâce à ce produit, des 20 sociétés gagnantes du « European IST Prize », prix récompensant les produits qui représentent la plus grande innovation dans le domaine de la technologie de l'information [*IST*]

Fig 16 *Logo prix IST*

De la même manière que, lors d'une élection classique, le vote papier est placé dans l'urne, le vote électronique est placé dans une enveloppe digitale. Selon les dires de Mr Pere Vallés, Managing Director de Scytl.com : « Nous avons essentiellement recréé le monde physique dans un environnement en ligne ». [*eGovernment News – 20 décembre 2004*]

Cette enveloppe digitale est basée sur un système breveté de cryptographie au niveau de l'application ; les électeurs chiffrent leur vote au moyen d'une clé publique et celui-ci est déchiffré au moment du décompte final grâce à la clé privée, exactement comme si l'on ouvrait des bulletins classiques. « Il n'y a pas moyen de manipuler les bulletins et les électeurs reçoivent un accusé de réception leur confirmant que leur vote a correctement été pris en compte, ce qui renforce la confiance dans le vote électronique. » ajoute Mr Vallés.

2. *Remarques*

Il y a, par définition, un nombre fini de manière de voter, donc aussi un nombre fini de bulletins de vote différents. Le fait d'utiliser une clé pour chiffrer un bulletin va certes le rendre illisible, mais, puisque la clé de chiffrement est publique, une personne pourrait chiffrer toutes les possibilités de votes, et ensuite comparer.

Imaginons un vote simpliste : il est possible de voter soit pour le candidat A, soit pour le candidat B. Pour protéger le secret du vote, nous allons placer chaque vote dans une enveloppe ; afin de préserver le secret du vote. Mais, si vous savez que les votes pour le candidat A sont placés dans des enveloppes rouges, tandis que les votes pour le candidat B sont, eux, placés dans des enveloppes bleues, peut-on encore considérer qu'il y a un secret du vote ?

Pour éviter ce type d'inconvénient, il faut que deux votes identiques soient différents après chiffrement, ce qui signifie que d'autres informations vont devoir être jointes au vote lui-même. C'est effectivement le cas chez scytl.com, comme l'a confirmé Ivan Font, Marketing Manager :

« dans une enveloppe digitale, une méthode à clé publique et une méthode symétrique sont combinées comme suit :

- ☑ Une clé aléatoire est générée (clé de session)
- ☑ Le vote est chiffré au moyen d'un algorithme symétrique, grâce à la clé créée
- ☑ Un petit message contenant la clé est chiffré au moyen de la clé publique
- ☑ Ce petit message est envoyé conjointement avec le vote chiffré.

Veuillez noter que, comme la clé de session est aléatoire, il est impossible de connaître le contenu du vote chiffré. » [*Ivan Font*]

Les clés de session étant différentes d'une personne à l'autre, celle-ci peuvent être assimilées à un identifiant. D'autre part, puisqu'il y a accusé de réception pour confirmer le bon traitement du vote, il faut que le vote ait été transmis de manière non-anonyme. Nous nous trouvons donc en face d'un message qui contient un identifiant et qui est nominatif ; dans ce cas, l'anonymat du vote est-il bien respecté ?

F. TrueBallot.com

[*TrueBallot.com*]

1. *Présentation*

Forts d'une longue expérience dans les élections syndicales et associatives, TrueBallot a conçu un produit pour les élections par Internet nommé WebVote®. Celui-ci s'ajoute aux autres produits de la gamme et a été conçu pour pouvoir fonctionner en parallèle avec eux.

La société met en avant les points forts de son produit :

- ☑ Compatibilité complète avec tous les autres produits de la gamme (ScanVote®,TouchVOTE®, TeleVote®)

- ☑ Système à niveaux de sécurité multiples permettant de certifier que seuls les électeurs autorisés votent, et qu'ils ne votent qu'une fois
- ☑ Comptage des voix pratiquement instantané, multiples possibilités de rapports
- ☑ Collecte d'informations gravées sur CD-Rom en fin d'élection, pour des analyses ultérieures.

2. Remarques

Les produits de TrueBallot n'étant pas actuellement utilisés à des fins d'élections publiques, et se cantonnant plutôt à des élections privées, associatives ou syndicales de petite envergure, le secret du vote et l'assurance de la prise en compte du vote de l'électeur ne font pas partie des points cruciaux de leurs applications. John Seibel, Président de TrueBallot nous l'a d'ailleurs confirmé : à la question « quand l'électeur et son vote sont-ils découplés », il nous a répondu textuellement ceci : « dans notre système, ils ne sont jamais liés ». Il n'y a donc aucune possibilité de prouver à un électeur que son vote a été correctement traité.[*John Seibel*]

G. Choose

[*Choose*]

1. Présentation

Le projet CHOOSE a été développé par un groupe d'étudiants de l'Université Technique de Delft, sous la supervision de Pieter G. MacLaine Pont, membre de TNO-TPD. L'un des buts principaux de ce projet était de développer un système de vote électronique d'un usage possible en réseau ouvert, tel ,qu'Internet. Il a été testé lors des élections étudiantes de la TU Delft en mai 2000.

Le système est basé sur la thèse de Maîtrise de Herman Robers, un étudiant de cette même université. Cette thèse avait pour titre : « Electronic elections employing DES smart cards » et a été terminée en décembre 1998. Il avait été décidé de n'utiliser que de la cryptographie symétrique, afin de pouvoir se servir de smart cards (équipées de l'algorithme DES). Ce système limitait évidemment le niveau de sécurité, ne permettant pas, par exemple, d'utiliser les signatures digitales.

Le processus électoral se déroulait en deux étapes distinctes :

Dans un premier temps, l 'électeur se connecte avec sa smart card, et dans un second temps, le vote est envoyé. Comme dans beaucoup d'autres systèmes, le vote aurait dû voyager dans un canal préservant son anonymat, mais cela n'avait pas été implémenté.

Il est à noter que les parties possédant les clés privées doivent être considérées comme personnes de confiance, qui ne se serviront pas de celle-ci pour violer le secret et la sécurité du système.

2. *Remarques*

Le serveur utilisé dans ce système est séparé en deux parties : le comité électoral gère une partie, tandis que l'autre s'occupe de la gestion des votes pendant l'élection. La description de la partie du serveur s'occupant de la gestion des votes spécifie que c'est cette partie qui est chargée d'éliminer toute référence à l'électeur ainsi que l'heure du vote, mais une procédure telle que celle-ci demande une confiance totale dans le serveur et ses applications. Il est à noter que, même si cette partie du serveur suit les consignes à la lettre, il n'y a aucune garantie que d'autres processus du serveur ne gardent trace des opérations effectuées et donc aussi le lien entre l'électeur et son vote.

H. iSOCO

[*iSOCO*]

1. *Présentation*

La société iSOCO est une spin-off du CSIC (Spanish Scientific Research Council). Cette compagnie est spécialisée dans le design et le développement d'applications d'e-commerce et d'e-business, utilisant des techniques d'intelligence artificielle.

En ce qui concerne le vote électronique sur Internet, elle a développé un schéma qui permet le déroulement d'élections sécurisées utilisant des réseaux de communication.

iSOCO attache une très grande importance à l'aspect sécuritaire du vote en ligne. Actuellement, à son avis, la majorité des applications de vote par Internet ne considèrent pas la sécurité comme un point essentiel à prendre en compte dans le design. Seules quelques petites précautions sécuritaires sont prises, et la plupart des solutions proposées sont basées sur l'usage de mots de passe ou moyens désuets, comme le courrier postal.

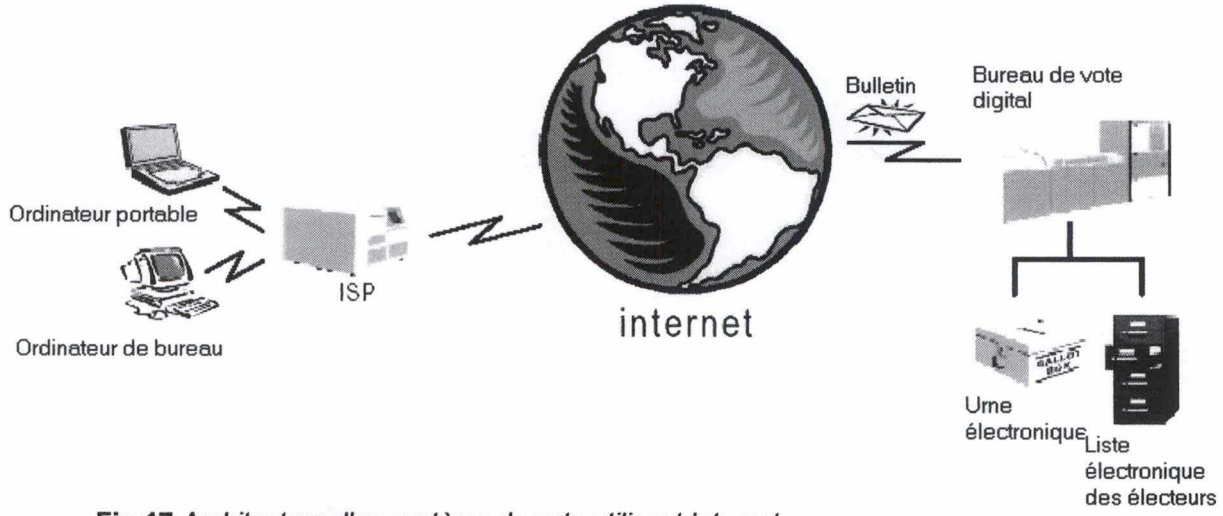


Fig 17 *Architecture d'un système de vote utilisant Internet*

Selon iSOCO, avant qu'une élection puisse avoir lieu sur Internet, une étape préalable doit avoir lieu : l'enregistrement des électeurs. Le but de cette opération est la construction d'une liste digitale des électeurs, avec pour chacun d'eux son certificat électronique ainsi que clé privée. Ceci va permettre au votant d'envoyer son vote avec un maximum de sécurité. Cette phase d'enregistrement nécessite un contact direct en face à face avec chaque électeur, en utilisant les bonnes vieilles méthodes que sont les formulaires et les systèmes d'identification habituels tels que la carte d'identité. Ce n'est qu'après cette opération préliminaire qu'une élection en ligne pourra avoir lieu.

La figure 17 présente l'architecture proposée par iSOCO pour une élection sur l'Internet qui accepte de réceptionner des votes provenant de tout terminal connecté à l'Internet (ordinateur de bureau, portable, GSM avec option WAP ...). La collecte des votes est effectuée par un serveur connecté au réseau qui agit comme une version électronique d'un collège électoral conventionnel.

Ce n'est que dans le cas d'un nombre de votants limités qu'un seul collège digital peut suffire ; si le nombre de votants augmente, un seul bureau de vote digital deviendrait vite un goulot d'étranglement. Dans de tels cas, la liste électronique des électeurs doit être distribuée sur plusieurs collèges électoraux digitaux fonctionnant en parallèle. Chacun d'eux traitera alors avec un nombre limité de votants. Quelques mécanismes (principalement implémentés dans le format de la liste électronique des électeurs) doivent être implémentés pour permettre de reconnaître aisément le bureau de vote digital auquel un électeur est assigné.

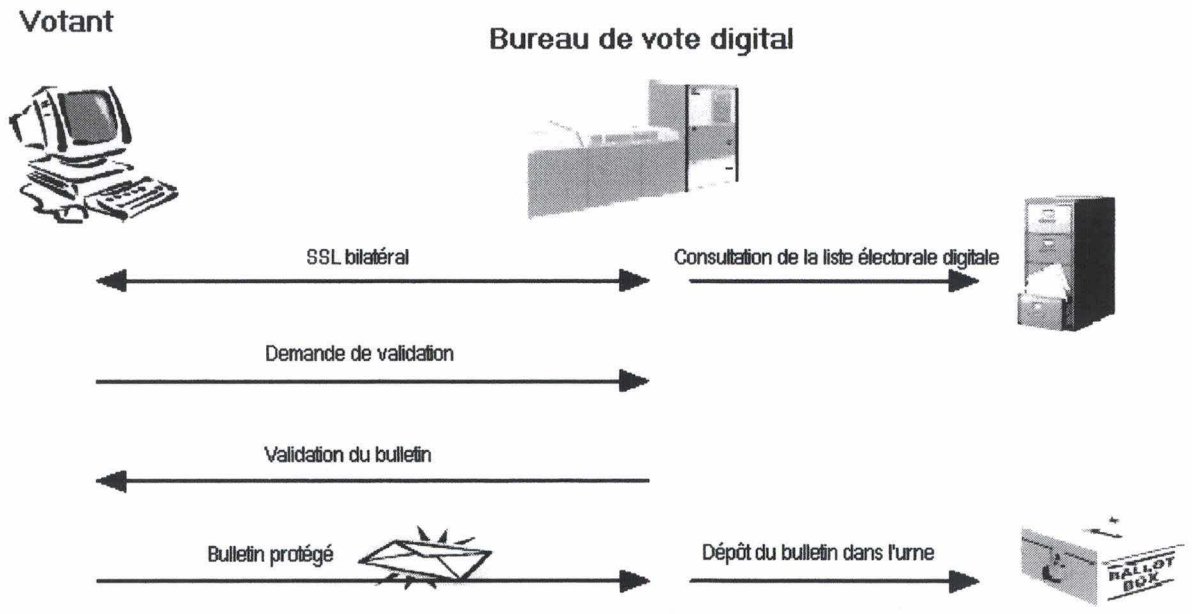


Fig 18 *Protocole d'enregistrement d'un vote*

Afin d'enregistrer son vote, chaque votant contacte son bureau de vote digital au moyen de l'Internet à partir de n'importe quel terminal (ordinateur à la maison, au bureau, ordinateur portable connecté au réseau Internet, GSM, ...). Le protocole employé pour l'enregistrement des votes est schématisé sur la figure 18. La première étape consiste à établir une connexion https (http incorporant SSL au niveau de la couche transport) au site web du bureau de vote digital. Le protocole initial de

« handshaking » de SSL permet une authentication mutuelle et l'établissement d'un contexte sécurisé :

1. Le votant est certain d'avoir contacté le bon bureau de vote digital, et non un imposteur.
2. Le bureau de vote digital est certain de l'identité de l'électeur qui le contacte (une infrastructure de type PKI (Public Key Infrastructure) a été utilisée lors de la phase d'enregistrement, afin de créer et de certifier les clés des électeurs).
3. Les deux protagonistes établissent un canal de communication sécurisé, garantissant la confidentialité, l'intégrité et l'authenticité de tout échange ultérieur.

Lorsque le votant a été identifié, le bureau de vote digital consulte la liste électronique des électeurs, afin de vérifier si celui-ci fait partie du corps électoral, s'il s'adresse à son bureau de vote digital et s'il a déjà voté.

Il est important de garder le système de vote le plus simple possible. Pour des raisons de facilité, le votant ne devrait idéalement pas avoir à installer de logiciel sur son terminal. La seule obligation est d'avoir un navigateur web qui permette la connexion avec le bureau de vote. Pour cette raison, la page web que le site envoie au votant lors de sa connexion contient un groupe d'applets Java qui vont créer les fonctionnalités nécessaires permettant l'acheminement des bulletins de vote en assurant toute la sécurité nécessaire. Tous les applets Java envoyés sont signés par l'autorité électorale, afin de prouver leur authenticité et leur intégrité.

La première opération effectuée par les applets du protocole est de préparer une requête de validation du bulletin de vote, afin d'obtenir un bulletin validé qui ne permettra plus aucune modification ultérieure (même par le bureau de vote). La requête de validation utilise un mécanisme cryptographique qui empêchera le bureau de vote de connaître les choix du votant.

Après validation, le bulletin, toujours au moyen des applets, place le bulletin dans une enveloppe digitale qui le protègera, comme dans un processus d'élections basées sur bulletins de vote en papier. Dans la pratique, ces enveloppes digitales sont construites à partir d'une combinaison d'une cryptographie symétrique et d'une cryptographie à clé publique (pour le détail, voir les remarques concernant le produit Pnyx.core de la société Scytl.com, p 18)

L'électeur signe (de manière digitale) l'enveloppe qui contient son vote. L'objectif de cette opération est de pouvoir prouver qu'un électeur a voté ou non. Il est important de remarquer que c'est l 'enveloppe qui est signée, et non le vote qu'elle contient (ceci n'influe donc en rien sur le secret du vote).

Le bulletin, ainsi protégé dans son enveloppe signée, est placé dans une urne électronique au bureau de vote électronique. Le stockage s'effectue sur une machine sûre et sécurisée, n'ayant aucun lien direct avec Internet, et est donc de ce fait une cible impossible à atteindre pour toute personne étrangère au bureau de vote électronique. En fait, l'urne électronique ne sert que comme protection contre la destruction des votes qu'elle contient ; l'enveloppe digitale est elle-même suffisamment sûre pour pouvoir préserver les votes (impossibilité de lire ou d'altérer).

Quand l'élection est arrivée à son terme, l'urne digitale peut être manipulée par les autorités électorales ; le comptage des votes et la publication des résultats du scrutin peut avoir lieu. L'opération consistant en l'ouverture des enveloppes et celle de la séparation enter bulletins et enveloppes est effectuée en une seule passe, en

mélangeant les bulletins, pour garantir l'anonymat. L'objectif de cette oprération est d'empêcher les organisateurs de l'élection de relier un vote à un votant en utilisant l'ordre de contact des votants avec le bureau de vote électronique. Après avoir decouplé les votes des votants, le décompte des voix peut être publié, directement sur le web.

2. Remarques

Dans l'urne électronique se trouvent des enveloppes signées par les votants. Ces enveloppes contiennent non seulement les votes des votants, mais aussi une « clé de session » utilisée pour chiffrer le vote en vue de le rendre illisible pendant son acheminement vers l'urne électronique.

Pour que ce type d'élection soit complètement anonyme, il faudrait être certain que, lors de la comptabilisation des votes, la séparation efface complètement toutes les traces des votants, c'est-à-dire l'enveloppe signée ainsi que la clé de session. Il faudrait aussi que les votes originaux de l'urne, dans leur enveloppe, soient détruits sans aucune possibilité de récupération, et qu'aucune copie de ceux-ci n'existe ; si tel était le cas, il faudrait les détruire. Il faut donc placer toute sa confiance dans le bureau de vote électronique, et espérer qu'aucun problème ne survienne, car, si tout est effacé, il sera impossible de répéter l'opération.

Un autre problème découle du problème précité : s'il n'y a plus aucune trace des votes originaux, il n'y a plus, non plus, aucune possibilité de vérification, de recomptage.

S'il est un fait que, jusqu'au moment du décompte des voix, tout votant peut être certain que son vote est dans l'urne électronique, et qu'il n'a pas été altéré, dès que la procédure démarre, tous les liens sont coupés ; le votant ne peut plus avoir d'information sur son vote et ne peut pas être certain que son vote a été pris en compte et qu'il n'a pas été altéré lors de la procédure de décompte.

Chapitre III. Vote sur Internet : critères de validité d'un vote sécurisé

A. Sécurisation d'un vote sur Internet

Au vu des différentes applications et différents projets qui existent autour de ce vote électronique sur Internet, il apparaît que, pour avoir la certitude que l'élection s'est déroulée correctement, certaines vérifications doivent être impérativement réalisées ; la liste qui suit est un minimum que toute élection qui se dit correcte et sécurisée devrait être en état de respecter :

- ☑ Seuls les électeurs autorisés peuvent voter
- ☑ Personne ne peut voter plus d'une fois
- ☑ Le vote d'un électeur doit être secret
- ☑ Toute modification d'un vote doit être décelée
- ☑ Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final
- ☑ Pour certaines élections, il est possible de savoir qui a et qui n'a pas voté.

B. Commentaires sur ces critères

1. Seuls les électeurs autorisés peuvent voter

Afin de pouvoir vérifier la validité d'un électeur, il faut que celui-ci soit identifié avant l'élection. Une liste d'électeurs, accessible à tous avant l'élection, pourrait être une solution acceptable, vu que chacun pourrait ainsi vérifier si chaque personne de la liste existe réellement et est réellement un électeur potentiel. Pour pouvoir voter, un électeur doit être inscrit dans cette liste.

2. Personne ne peut voter plus d'une fois

Lorsqu'un électeur vote, l'information de son acte doit être notée, afin qu'il ne puisse pas le reproduire. En d'autres termes, une base de données des votants devra être mise à jour en temps réel lors de l'élection.

3. Le vote d'un électeur doit être secret

Pendant le déroulement de l'élection, il ne devra pas exister de lien direct qui puisse connecter l'électeur et son vote. Il n'est pas possible d'obtenir, par quelque moyen que ce soit, une information où le votant et son vote apparaissent simultanément.

4. Toute modification d'un vote doit être décelée

A partir du moment où un électeur envoie son vote sur Internet, il doit être impossible à un tiers de modifier, de remplacer d'ajouter ou de soustraire des votes au scrutin.

5. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

Au terme de l'élection doivent subsister des traces permettant à chaque électeur de vérifier que son vote a été traité correctement.

6. Pour certaines élections, il est possible de savoir qui a et qui n'a pas voté

Dans le cas de telles élections, il devra être possible, au terme du scrutin, d'établir une liste complète des électeurs et de leur participation à celui-ci.

Chapitre IV. Abréviations

A : Electeur

Demande : Demande d'autorisation de voter, créée pas A et envoyée à T_1

D_X*(message chiffré)* : Déchiffrement par *X*, au moyen de sa clé privée, d'un message chiffré à son attention

E_X*(message)* : Chiffrement d'un message au moyen de la clé publique de X

$Ident_A$, $Ident_T$, $Ident_1$, $Ident_2$, $Ident_3$: Identifiants. Pour être identifiant, un champ doit permettre d'effectuer un lien entre deux informations ; dans le cas qui nous intéressent, entre le votant et des informations le concernant, en ce y compris dans une cascade ($Ident_2$ permet de retrouver $Ident_1$ qui permet de retrouver *A*)

Liste : Liste des électeurs, créée par *S*

Not_OK : Message informant d'un problème lors d'une opération.

OK : Message pour informer qu'une opération s'est déroulée correctement

S : Organisation pour laquelle l'élection est organisée

S_X : Signature d'un message par *X*

T : Tiers de confiance unique

T_1 : Premier tiers de confiance

T_2 : Second tiers de confiance

X : Electeur quelconque

Var : Champ variable, utiliser pour masquer un vote

VoteA : Vote de l'électeur *A*, qui doit être transféré à *S*

V_X : Vérification de la signature d'un message par X

Chapitre V. Analyse de différents protocoles

A. Vote simple

Nous allons dans un premier temps tenter, à partir d'un protocole, simpliste, de construire un protocole qui respecte les 6 critères cités précédemment. Tout d'abord, nous analyserons le cas d'un vote où le votant entre en contact directement avec l'organisateur de l'élection, et tenterons d'y apporter des améliorations en vue de le sécuriser.

1. A envoie son vote à S

a) Protocole

A envoie son vote à *S*.

A → S : *VoteA*

S enregistre le vote de *A* dans la liste des votes.

VoteA → {*Votes*}

b) Respect des critères

a. Seuls les électeurs autorisés peuvent voter

→ Non respecté

N'importe qui peut voter : il n'y a aucun contrôle sur l'émetteur du vote.

b. Personne ne peut voter plus d'une fois

→ Non respecté

Il n'y a aucune vérification : il est possible de voter plusieurs fois.

c. Le vote d'un électeur doit être secret

→ Non respecté

S'il est vrai que l'organisateur de l'élection reçoit le vote de façon anonyme, le vote est envoyé non chiffré sur le réseau, toute personne qui intercepte ce vote alors qu'il quitte la machine du votant peut le consulter.

d. Toute modification d'un vote doit être décelée

→ Non respecté

Toute personne interceptant le vote d'un électeur, tout comme l'organisateur, peut remplacer le contenu par celui qu'il souhaite ; ceci n'a que peu d'intérêt puisqu'il est plus aisé, pour modifier le résultat de l'élection, de placer autant de votes que nécessaire afin de faire basculer l'élection dans le sens où l'on veut.

e. *Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final*

→ Non respecté

Le vote envoyé est complètement anonyme ; il pourrait être envoyé par n'importe qui ; il n'y a donc aucune traçabilité possible.

f. *Il est possible de savoir qui a voté ou non*

→ Non respecté

Pour cette même raison d'anonymat du vote, il est impossible pour l'organisateur de l'élection de savoir qui a voté ou non, tout comme il lui est impossible de savoir qu'un électeur a voté plusieurs fois.

c) Conclusion

Il apparaît, de manière évidente, que ce vote est d'une grande insécurité, tant au niveau du secret du vote que du sérieux des résultats. Une première amélioration va permettre de protéger l'intégrité du vote pendant son transport sur Internet ; si l'électeur chiffre son vote, il faudra le déchiffrer afin de pouvoir le lire ; pour ce faire, il faut posséder la clé qui permettra le déchiffrement.

Plusieurs méthodes de chiffrement peuvent être utilisées ; pour la clarté du travail, nous nous contenterons d'utiliser les raccourcis suivants lorsqu'une personne *X* voudra chiffrer un message :

E_X(message) : Chiffrement d'un message au moyen de la clé publique de *X*

D_X(message chiffré) : Déchiffrement par *X*, au moyen de sa clé privée, d'un message chiffré à son attention

Pour pouvoir envoyer un message chiffré à l 'attention de quelqu'un, il faut que celui-ci ait fait parvenir sa clé.

Nous allons considérer comme acquis le fait que la clé de l'organisateur de l'élection a été publiée et que tout électeur connaît celle-ci. La clé de l'organisateur de l'élection est bien sûr certifiée par un tiers de confiance (**KCA** : **K**ey **C**ertification **A**uthority, ou **KDC** : **K**ey **D**istribution **C**enter) ; il n'y a donc pas possibilité pour une personne de se faire passer pour l'organisateur de l'élection afin d'intercepter les votes.

2. *A chiffre son vote au moyen de la clé publique de S*

a) Protocole

Par ce chiffrement, le vote de A est secret et illisible pour toute personne hormis *S*.

$A \rightarrow S : : E_S(VoteA)$

Lorsqu'il reçoit le vote, *S* doit le déchiffrer avant de pouvoir le lire. Il enregistre le vote de *A* dans la liste des votes.

$S : D_S(E_S(VoteA)) = VoteA$

$VoteA \rightarrow \{Votes\}$

b) Critères

a. Seuls les électeurs autorisés peuvent voter

→ Non respecté

N'importe qui peut voter : il n'y a aucun contrôle sur l'émetteur du vote.

b. Personne ne peut voter plus d'une fois

→ Non respecté

Il n'y a aucune vérification : il est possible de voter plusieurs fois.

c. Le vote d'un électeur doit être secret

→ Non respecté

En effet, bien que le vote soit chiffré, il n'est pas à l'abri. La clé publique est accessible à tous ; si une personne intercepte un vote chiffré, il lui suffit de chiffrer lui-même toutes les combinaisons possibles de vote et de comparer ; il pourra ainsi, par comparaison, déterminer le vote qui se trouve dans le message chiffré.

d. Toute modification d'un vote doit être décelée

→ Non respecté

Toute personne interceptant le vote d'un électeur, tout comme l'organisateur, peut remplacer le contenu par celui qu'il souhaite ; ceci n'a que peu d'intérêt puisqu'il est plus aisé, pour modifier le résultat de l'élection, de placer autant de votes que nécessaire afin de faire basculer l'élection dans le sens où l'on veut.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Non respecté

Le vote envoyé est complètement anonyme ; il pourrait être envoyé par n'importe qui ; il n'y a donc aucune traçabilité possible.

f. Il est possible de savoir qui a voté ou non

→ Non respecté

Pour cette même raison d'anonymat du vote, il est impossible pour l'organisateur de l'élection de savoir qui a voté ou non, tout comme il lui est impossible de savoir qu'un électeur a voté plusieurs fois.

c) Conclusion

Pour éviter qu'une personne non autorisée vote, il faut que le vote soit identifiable comme émanant d'un électeur autorisé. Pour ce faire, l'électeur pourrait, par exemple marquer son vote de sa signature.

S'il y a signature, nous sommes amenés à supposer que chaque électeur est en possession d'une signature électronique. La carte d'identité électronique que nous sommes tous amenés à posséder dans un délai relativement court pourrait être un support pour cette signature électronique. La paire de clés permettant la signature ainsi que le chiffrement est d'un type similaire à celui employé pour le clé de l'organisateur de l'élection. Il va de soi que l'organisateur de l'élection possède la clé publique de tous les électeurs ($Liste=\{Electeur,Clé\}$) et que toutes ces clés sont certifiées.

3. *A signe son vote au moyen de sa clé privée*

a) Protocole

A envoie son vote signé ainsi que son identité à *S*.

$A \rightarrow S : : E_S(S_A(VoteA)A)$

S vérifie si *A* est un électeur.

$A \in \{Electeur\}$

S déchiffre le message reçu.

$S : D_S(E_S(S_A(VoteA)A)) = S_A(VoteA)A$

S vérifie que le vote est bien par *A*, et enregistre le vote de *A* dans la liste des votes et sa participation au scrutin dans la liste des votants.

$S : V_A(S_A(VoteA)) = VoteA$

$A \rightarrow \{A\_Voté\}$

$VoteA \rightarrow \{Votes\}$

b) Critères

a. *Seuls les électeurs autorisés peuvent voter*

→ Respecté (à condition que l'organisateur ne triche pas)

Puisque l'électeur doit s'identifier, l'organisateur peut vérifier que l'électeur est sur la liste. Il faut pour cela faire une confiance aveugle à la bonne foi de l'organisateur de l'élection, qui pourrait manipuler ces informations (en ajoutant des voix pour un candidat à la place d'électeurs de la liste qui ne se seraient pas manifestés, par exemple ; l'affichage en fin de scrutin de la liste des électeurs ayant voté éviterait ce problème, car le nombre de voix devra correspondre au nombre de votants).

b. *Personne ne peut voter plus d'une fois*

→ Respecté

Le vote de l'électeur étant signé, l'organisateur de l'élection peut vérifier qu'un électeur a déjà voté et ainsi empêcher celui-ci de soumettre un vote ultérieur ; une liste des votants à l'issue du scrutin permet de vérifier que l'opération a été correctement réalisée (en ce qui concerne les votants uniquement).

c. *Le vote d'un électeur doit être secret*

→ Non respecté

Comme l'électeur signe son vote, l'organisateur, lorsqu'il déchiffre le vote, est au courant du contenu du vote de chacun.

d. Toute modification d'un vote doit être décelée

→ Non respecté

Tant que le vote de l'électeur est chiffré, il n'est pas possible de le modifier ; seul l'organisateur du vote est capable de le déchiffrer, et donc aussi de le modifier. Comme déjà dit précédemment, pour que ce protocole fonctionne correctement, il faut faire une confiance aveugle en la bonne foi de l'organisateur de l'élection. Par contre, comme la réception d'un vote ne demande pas l'envoi d'un accusé de réception, il est toujours possible de bloquer le vote afin qu'il ne parvienne jamais à destination.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Non respecté

A moins de publier la liste des votes à laquelle serait jointe l'identité de l'électeur (ce qui, il faut bien l'avouer, va à l'encontre du secret du vote), il n'est pas possible pour un électeur d'être certain que son vote a été pris en compte.

f. Il est possible de savoir qui a voté ou non

→ Respecté

L'organisateur peut tenir à jour une liste des électeurs ayant voté ; il doit d'ailleurs utiliser une telle liste pour vérifier qu'un électeur ne vote pas une seconde fois. Il suffit de rendre cette liste publique et ainsi tout le monde peut savoir qui a participé ou non à l'élection.

c) Conclusions

Bien que l'électeur s'identifie lors de son vote (en le signant), il ne lui est pas possible de vérifier que le vote a été pris en compte sans que l'organisateur de l'élection ne publie le vote de l'électeur accompagné de son identité ; ceci laisse à désirer au niveau du secret du vote... Pour cacher l'identité de l'électeur, il faut faire appel à un identifiant ; celui-ci doit permettre à l'électeur de retrouver son vote parmi tous les autres sans que son identité y soit liée. Ceci permettra à l'électeur de vérifier que son vote a bien été comptabilisé et qu'il n'a pas subi de modification.

L'identifiant est un nombre choisi de manière aléatoire. Il convient de donner à cet identifiant une longueur telle que la probabilité de doublons soit extrêmement faible ; si tel était quand même le cas, il faudraitr pouvoir en changer.

Une autre information primordiale est aussi apparue ci-dessus : la liste des électeurs, liste contenant les noms de toutes les personnes autorisées à voter, doit être accessible avant le vote, afin que des personnes extérieures à l'organisation puissent vérifier la validité de celle-ci.

4. *A se sert d'un identifiant lui permettant de retrouver son vote*

a) Protocole

A envoie son vote signé, ainsi qu'un identifiant.

$A \rightarrow S : E_S(S_A(VoteA),A,Ident_A)$

S vérifie si *A* est un électeur.

$A \in \{Electeur\}$

S déchiffre le message reçu.

$S : D_S(E_S(S_A(VoteA),A,Ident_A)) = S_A(VoteA),A,Ident_A$

S vérifie que l'identifiant utilisé par *A* n'est pas déjà utilisé ; si tel est le cas, *S* demande à *A* de lui renvoyer un nouvel identifiant.

$S \rightarrow A : E_A(Ident_A,Not\_OK)$

Lorsqu'il reçoit ce message, *A* recommence le protocole depuis le début en utilisant un nouvel identifiant.

Sinon, *S* accepte le vote et l'identifiant.

S vérifie la signature ; il enregistre le vote de *A* et son identifiant dans la liste des votes et sa participation au scrutin dans la liste des votants.

$S : V_A(S_A(VoteA)) = VoteA$

$A \rightarrow \{A\_Voté\}$

$VoteA,Ident_A \rightarrow \{Votes\}$

A la fin du scrutin, une liste des votes et des identifiants est publiée, permettant à chacun de vérifier si son vote a été pris en compte et qu'il n'a pas été modifié ; la liste des votants est elle aussi publiée.

b) Critères

a. *Seuls les électeurs autorisés peuvent voter*

→ Respecté

L'électeur s'identifie, et son vote est publié à la fin du scrutin, accompagné de l'identifiant ; seul un électeur présent sur la liste peut voter. La liste des votants étant aussi publiée, il est possible de connaître le nombre de votants ainsi que leur nom ; il n'est donc pas possible d'ajouter des électeurs fantômes sans risque d'être découvert.

b. *Personne ne peut voter plus d'une fois*

→ Respecté

Pour la même raison que ci-dessus, un électeur votant deux fois devrait apparaître à deux reprises dans les listes, ce qui est impossible.

c. Le vote d'un électeur doit être secret

→ Non respecté

Comme l'électeur signe son vote, l'organisateur est au courant du contenu du vote de chacun.

d. Toute modification d'un vote doit être décelée

→ Respecté

A l'issue du scrutin, le votant a la possibilité de retrouver son vote dans la liste des votes au moyen de son identifiant; il peut donc vérifier que son vote n'a pas été modifié.

L'organisateur ne sait pas quel votant viendra consulter la liste ; il ne peut donc pas, sans risque, effacer un vote et son identifiant.

Un nombre de votants coïncidant avec le nombre de votes indique qu'aucun ajout n'a été effectué.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Respecté

La liste des votes étant publiée, l'électeur, grâce à l'identifiant qu'il a envoyé, peut retrouver son vote parmi tous ceux qui ont été comptabilisés. Il est donc certain que son vote a été pris en compte.

f. Il est possible de savoir qui a voté ou non

→ Respecté

L'organisateur tient à jour une liste des votants ; il doit d'ailleurs utiliser une telle liste pour vérifier qu'un électeur ne vote pas une seconde fois. Il suffit de rendre cette liste publique et ainsi tout le monde peut savoir qui a participé ou non à l'élection.

c) Conclusions

Si l'identifiant permet de cacher le lien entre l'électeur et son vote pour le public, il ne cache pas son identité aux yeux de l'organisateur ; en effet, il peut faire le lien entre identité et identifiant du votant, éliminant de ce fait tout secret du vote pour lui. Un autre problème, celui des identifiants doublons, peut être réglé si l'identifiant est créé par l'organisateur de l'élection plutôt que par l'électeur lui-même.

5. *S renvoie un identifiant qui permettra à A de retrouver son vote*

a) Protocole

A envoie son vote à *S*.

$A \rightarrow S : E_S(S_A(VoteA)A,)$

S vérifie si *A* est un électeur.

$A \in \{Electeur\}$

S déchiffre le message reçu.

$S : D_S(E_S(S_A(VoteA)A)) = S_A(VoteA)A$

S vérifie la signature.

$S : V_A(S_A(VoteA)) = VoteA$

S crée un identifiant unique qui sera associé à *A*, et il le lui envoie comme accusé de réception de son vote ; il enregistre le vote de *A* et son identifiant dans la liste des votes et sa participation au scrutin dans la liste des votants..

$S \rightarrow A : E_A(Ident_A)$

$A \rightarrow \{A\_Voté\}$

$VoteA, Ident_A \rightarrow \{Votes\}$

A la fin du scrutin, une liste des votes et des identifiants est publiée, ainsi que la liste des votants (Cfr protocole 4)

b) Critères

Que l'identifiant soit émis par l'électeur ou par l'organisateur ne change que peu de choses : cette solution évitera les doublons dans les identifiants, puisque tous les identifiants émaneront de la même entité. Pour le reste, les résultats pour les 6 critères sont exactement pareils à ceux du protocole précédent.

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

L'électeur s'identifie, et son vote est publié à la fin du scrutin, accompagné de l'identifiant ; seul un électeur étant présent sur la liste peut voter. La liste des électeurs ayant voté étant aussi publiée, il est possible de connaître le nombre de votants ainsi que leur nom ; il n'est donc pas possible d'ajouter des électeurs fantômes sans risque d'être découvert.

b. Personne ne peut voter plus d'une fois

→ Respecté

Pour la même raison que ci-dessus, un électeur votant deux fois devrait apparaître à deux reprises dans les listes, ce qui est impossible.

c. Le vote d'un électeur doit être secret

→ Non respecté

Comme l'électeur signe son vote, l'organisateur est au courant du contenu du vote de chacun.

d. Toute modification d'un vote doit être décelée

→ Respecté

A l'issue du scrutin, le votant a la possibilité de retrouver son vote dans la liste des votes au moyen de son identifiant; il peut donc vérifier que son vote n'a pas été modifié.

L'organisateur ne sait pas quel votant viendra consulter la liste ; il ne peut donc pas, sans risque, effacer un vote et son identifiant.

Un nombre de votants coïncidant avec le nombre de votes indique qu'aucun ajout n'a été effectué.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Respecté

La liste des votes étant publiée, l'électeur, grâce à l'identifiant qui lui a été envoyé, peut retrouver son vote parmi tous ceux qui ont été comptabilisés. Il est donc certain que son vote a été pris en compte.

f. Il est possible de savoir qui a voté ou non

→ Respecté

L'organisateur peut tenir à jour une liste des électeurs ayant voté ; il doit d'ailleurs utiliser une telle liste pour vérifier qu'un électeur ne vote pas une seconde fois. Il suffit de rendre cette liste publique et ainsi tout le monde peut savoir qui a participé ou non à l'élection.

c) Conclusions

L'identifiant permet de cacher le lien entre l'électeur et son vote pour le public, mais il ne cache pas son identité aux yeux de l'organisateur. Ceci va à l'encontre de ce que l'on attend d'une élection.

6. *Signature aveugle*

a) Protocole

Avant toute chose, une petite explication à propos de la signature aveugle ; ce système se sert de la propriété suivante : signature et aveuglement sont commutatifs, ce qui signifie qu'il est possible d'aveugler, de signer à l'aveugle et ensuite de désaveugler pour obtenir un message en clair et signé par une personne qui ne l'a pas vu .

Soit un message aveuglé par X et signé par Y ; comme

$S_Y(B_X(Message))=B_X(S_Y(Message))$,

nous obtenons, lorsque X désaveugle le message signé

$U_X(S_Y(B_X(Message)))=U_X(B_X(S_Y(Message)))=S_Y(Message)$

Ce vote se déroule en deux temps :

1 Dans un premier temps,

1.1 A génère un ensemble de messages, couvrant toutes les possibilités de vote.

Chaque message contient aussi un numéro de série généré de manière aléatoire ($Ident_A$), grand assez pour éviter tout doublon avec d'autres électeurs. A aveugle ses messages et les envoie à S. A précise aussi son identité et signe son envoi.

$A \rightarrow S : \forall i: S_A(E_S(B_A(VoteA_i, Ident_A)))A$

1.2 S déchiffre l'ensemble des messages envoyés par A ; que A est l'auteur du message en vérifiant sa signature ; il vérifie que A est un électeur et qu'il n'a pas déjà soumis d'autres messages aveuglés.

$S : \forall i: V_A(S_A(E_S(B_A(VoteA_i, Ident_A))))=E_S(B_A(VoteA_i, Ident_A))$

$S : \forall i: D_S(E_S(B_A(VoteA_i, Ident_A)))=B_A(VoteA_i, Ident_A)$

$A \in \{Electeurs\}$

$A \notin \{Votants\}$

1.3 Si ce n'est pas le premier envoi de A, S le lui fait savoir en lui envoyant un message d'information.

$S \rightarrow A : Déjà\_reçu, \forall i: B_A(VoteA_i, Ident_A)$

Si cet envoi est le premier de A, S lui renvoie l'ensemble des votes signés.

$S \rightarrow A : \forall i: E_A(S_S(B_A(VoteA_i, Ident_A)))$

1.4 *S* introduit l'électeur dans sa liste des votants.

$S : A \rightarrow \{Votants\}$

2 La seconde partie de l'opération est le vote proprement dit.

2.1 *A* déchiffre le message envoyé par *S*

$A : \forall i: D_A(E_A(S_S(B_A(VoteA_i, Ident_A)))) = S_S(B_A(VoteA_i, Ident_A))$

2.2 *A* « désaveugle » l'ensemble des messages (les fonctions d'aveuglement et de signature sont commutatives). *A* possède ainsi la gamme complète de tous les votes possibles, tous signés par *S*.

$A : \forall i: U_A(S_S(B_A(VoteA_i, Ident_A))) = U_A(B_A(S_S(VoteA_i, Ident_A))) = S_S(VoteA_i, Ident_A)$

2.3 *A* va pouvoir choisir le vote qu'il va renvoyer à *S*. Il renvoie donc le vote choisi ainsi que son identifiant, signés par *S*.

$A \rightarrow S : E_S(S_S(VoteA, Ident_A))$

2.4 *S* déchiffre le message, vérifie la signature

$S : D_S(E_S(S_S(VoteA, Ident_A))) = S_S(VoteA, Ident_A)$

$S : V_S(S_S(VoteA, Ident_A)) = VoteA, Ident_A$

2.5 *S* vérifie dans sa liste des votes qu'aucun vote n'a déjà été placé pour cet identifiant (pour qu'un votant ne puisse pas voter plusieurs fois), accepte le vote s'il est acceptable, enregistre le vote ainsi que son identifiant dans la liste des votes. L'ensemble des votes est publié à l'issue du scrutin.

$S : Ident_A \notin \{Votes\}$

$S : VoteA, Ident_A \rightarrow \{Votes\}$

b) Critères

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

L'électeur s'identifie, et son vote est publié à la fin du scrutin, accompagné de l'identifiant ; seul un électeur présent sur la liste peut voter. La liste des électeurs ayant voté étant aussi publiée, il est possible de connaître le nombre de votants ainsi que leur nom ; l'organisateur n'a donc pas la possibilité d'ajouter des électeurs fantômes sans risque d'être découvert.

b. Personne ne peut voter plus d'une fois

→ Respecté

Pour la même raison que ci-dessus, un votant qui soumettrait deux fois devrait apparaître à deux reprises dans la liste, ce qui est impossible.

c. Le vote d'un électeur doit être secret

→ Non respecté

Puisque, grâce au principe de la signature aveugle, l'organisateur n'a pas pu voir l'identifiant associé au vote que lui soumettait le votant, celui-ci n'a pas la possibilité de connaître, à l'issue du scrutin, à quel votant l'identifiant est associé.

Par contre, il est possible à l'électeur de prouver à n'importe qui quel a été son choix. Une telle possibilité est un danger pour le bon déroulement d'une élection : le fait qu'un électeur puisse prouver à autrui la manière dont il a voté peut être utilisé de manière nuisible à la démocratie : vente de votes aux plus offrants, menaces et contraintes, preuve de fidélité, copie de l'identifiant ...

Comme l'électeur possède un moyen direct de vérifier son vote dans une liste, son vote n'est plus secret, puisque d'autres peuvent effectuer la même démarche.

d. Toute modification d'un vote doit être décelée

→ Non respecté

A l'issue du scrutin, le votant a la possibilité de retrouver son vote dans la liste des votes au moyen de son identifiant; il peut donc vérifier que son vote n'a pas été modifié.

L'organisateur ne sait pas quel votant viendra consulter la liste ; il ne peut donc pas, sans risque, effacer un vote et son identifiant.

Il est toujours envisageable, dans un protocole tel que celui-ci, que l'organisateur de l'élection profite de l'abstentionnisme pour ajouter des votes et ainsi fausser les résultats.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Respecté

La liste des votes étant publiée, l'électeur, grâce à l'identifiant qui lui a été envoyé, peut retrouver son vote parmi tous ceux qui ont été comptabilisés. Il est donc certain que son vote a été pris en compte.

f. Il est possible de savoir qui a voté ou non

→ Respecté

L'organisateur tient à jour une liste des électeurs ayant voté ; il l'utilise pour vérifier qu'un électeur ne vote pas une seconde fois. Cette liste publiée permet à tout le monde de savoir qui a participé ou non à l'élection.

c) Conclusions

Dans ce protocole, l'identifiant ne permet pas à l'organisateur de connaître l'identité du votant, mais cet identifiant pose un problème, car il permet a posteriori de rétablir un lien entre un électeur et son vote : si une personne parvient à connaître l'identifiant qu'un votant a utilisé, cette personne est aussi à même de connaître le choix de celui-ci.

7. *S utilise un protocole ANDOS pour distribuer un identifiant de manière anonyme.*

a) Protocole

Tout d'abord, une petite explication à propos de cette méthode *ANDOS* (All-or-Nothing Disclosure of Secrets) : celle-ci permet de distribuer des données à *n* personnes, chaque personne recevant une et une seule donnée et deux personnes ne recevant jamais la même donnée, tout en assurant que le distributeur ne puisse pas savoir qui a reçu quelle donnée. La méthode *ANDOS* est assez compliquée et ce n'est pas l'endroit pour la décrire ici. Cette méthode est décrite en détails dans de nombreux ouvrages concernant la cryptographie.[*ANDOS*]

Ce système permet donc à l'électeur de posséder un identifiant qui lui est propre et qui est inconnu de l'organisateur. Pour la simplicité de l'explication du protocole, nous symboliserons l'obtention de l'identifiant au moyen d'un protocole *ANDOS* au moyen de l'expression « $ANDOS_A(X)$ ».

1. *S* publie une liste des électeurs.

   $S : \{Electeur\}$

2. Tout électeur *A* doit, à une date donnée, manifester son intention de voter.

   $A \rightarrow S : A,Demande$

3. *S* vérifie que la demande de *A* est fondée, c'est-à-dire que *A* appartient à la liste des électeurs.

   $S : A \in \{Electeur\}$

4. *S* publie la liste des personnes désirant voter.

   $S : \{DésireVoter\}$

5. *S* crée et publie une liste d'identifiants ; elle contient le même nombre d'éléments que la liste des personnes désirant voter.

   $S : \{Identifiant\}$

6. Au moyen du protocole *ANDOS*, chaque électeur désirant voter obtient un identifiant, sans que *S* ne sache qui reçoit lequel.

   $\forall A \in \{DésireVoter\} : S \rightarrow A : ANDOS_A(X)$

   Ce système évitera à *S* de reconnaître *A* lorsque celui-ci placera son vote.

7. Dès lors, *A* est en possession d'un identifiant connu de *S*, sans que *S* ne puisse relier *A* à l'identifiant qui lui a été octroyé.

   $A : ANDOS_A(X) = Ident_A$

8. *A* vote et chiffre son vote avec la clé publique de *S*, il y joint l'identifiant que *S* lui avait envoyé.

   $A \rightarrow S : E_S(Ident_A, VoteA)$

9. *S* déchiffre le vote ; il vérifie que l'identifiant est valide.

   S : $D_S(E_S(Ident_A, VoteA)) = Ident_A, VoteA$

   S : $Ident_A \in \{Identifiants\}$

   S : $Ident_A \notin \{A\_Voté\}$

10. *S* reçoit donc un vote, d'origine anonyme, mais valide. Il peut comptabiliser le vote. Il enregistre aussi que l'identifiant « $Ident_A$ » a été utilisé ; aucun électeur ne pourra donc plus l'utiliser.

    S : $VoteA \rightarrow \{Votes\}$

    S : $Ident_A \rightarrow \{A\_Voté\}$

b) Critères

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Pour pouvoir effectuer une demande d'identifiant, *A* doit être reconnu comme un électeur valable.

b. Personne ne peut voter plus d'une fois

→ Respecté

Seul un électeur préalablement enregistré (et reconnu en tant qu'électeur valable) recevra un et un seul identifiant ; il aura donc au plus une seule possibilité de vote.

c. Le vote d'un électeur doit être secret

→ Non respecté

Puisque, grâce au principe de la distribution des identifiants par la méthode ANDOS, l'organisateur n'a pas pu voir l'identifiant que le votant a reçu et associe à son vote, celui-ci n'a pas la possibilité de connaître, à l'issue du scrutin, à quel votant l'identifiant est associé.

Par contre, il est possible à l'électeur de prouver à n'importe qui quel a été son choix. Une telle possibilité est un danger pour le bon déroulement d'une élection : le fait qu'un électeur puisse prouver à autrui la manière dont il a voté peut être utilisé de manière nuisible à la démocratie : vente de votes aux plus offrants, menaces et contraintes, preuve de fidélité, copie de l'identifiant, ...

Comme l'électeur possède un moyen direct de vérifier son vote dans une liste, son vote n'est plus secret, puisque d'autres peuvent effectuer la même démarche.

d. Toute modification d'un vote doit être décelée

→ Respecté

A l'issue du scrutin, le votant a la possibilité de retrouver son vote dans la liste des votes au moyen de son identifiant; il peut donc vérifier que son vote n'a pas été modifié.

L'organisateur ne sait pas quel votant viendra consulter la liste ; il ne peut donc pas, sans risque, effacer un vote et son identifiant.

Un électeur ayant effectué une demande d'identifiant peut lui aussi consulter la liste des votes ; il ne peut pas trouver son identifiant dans cette liste. Ce fait exclut la possibilité pour l'organisateur d'ajouter des votes sans risque.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Respecté

La liste des votes étant publiée, l'électeur, grâce à l'identifiant qui lui a été envoyé, peut retrouver son vote parmi tous ceux qui ont été comptabilisés. Il est donc certain que son vote a été pris en compte.

f. Il est possible de savoir qui a voté ou non

→ Non respecté

S ne peut pas vérifier si un électeur a bien voté ; tout ce qu'il peut dire, c'est que cet électeur a effectué ou non une demande.

c) Conclusions

La méthode *ANDOS* garantit que tous les électeurs ayant confirmé leur intention de participer à l'élection reçoivent un et un seul identifiant, sans que l'organisateur sache lequel. La liste des électeurs désirant voter et la liste des identifiants sont toutes deux publiées et possèdent le même nombre d'éléments, et chaque électeur ayant manifesté son intention de voter peut retrouver son nom dans la première, et son identifiant dans la seconde.

Toutes les élections ne le demandent pas, mais certaines exigent de savoir qui a voté ou non ; ce protocole ne permet pas à l'organisateur d'obtenir cette information.

Dans ce protocole, l'identifiant ne permet pas à l'organisateur de connaître l'identité du votant, mais cet identifiant pose un problème, car il permet a posteriori de rétablir un lien entre un électeur et son vote : si une personne parvient à connaître l'identifiant qu'un votant a utilisé, cette personne est aussi à même de connaître le choix de celui-ci.

8. *Protocole de Hannu Nurmi, Arto Solomaa et Lila Santean*

(Extrait de l'ouvrage « Applied cryptography »)

a) Protocole

Cette variante de la méthode précédente permet d'obtenir un résultat similaire sans devoir utiliser une paire de clés certifiées pour chaque électeur ainsi que pour l'organisateur.

L'électeur reçoit, tout comme dans le protocole précédent, un identifiant qui sera inconnu de l'organisateur, en utilisant un protocole ANDOS.

Ce protocole satisfait la plupart des exigences d'une élection, et possède deux propriétés additionnelles :

- Les électeurs peuvent changer d'avis et modifier leur vote (endéans un certain délai)
- Si un électeur s'aperçoit que son vote n'a pas été correctement traité, il peut protester tout en conservant son anonymat.

1. *S* publie une liste des électeurs

   $S : \{Electeur\}$

2. Tout électeur *A* doit, à une date donnée, manifester son intention de voter.

   $A \rightarrow S : A, Demande$

3. *S* vérifie que la demande de *A* est fondée, c'est-à-dire que *A* appartient à la liste des électeurs.

   $S : A \in \{Electeur\}$

4. *S* publie la liste des personnes désirant voter.

   $S : \{DésireVoter\}$

5. *S* crée une liste d'identifiants et la publie.

   $S : \{Identifiant\}$

6. Au moyen du protocole *ANDOS*, chaque votant *A* obtient un identifiant de celle liste, sans que *S* ne sache qui reçoit lequel.

   $S \rightarrow A : ANDOS_A(X)$

Ce système évitera à *S* de reconnaître *A* lorsque celui-ci votera.

7. Dès lors, *A* est en possession d'un identifiant connu de *S*, sans que *S* ne puisse relier *A* à son identifiant.

   $A : ANDOS_A(X) = Ident_A$

8. *A* génère un jeu clé publique / clé privée puis envoie son vote chiffré avec la clé publique dans un message.

   $A : Cl\acute{e}A_S$ & $Cl\acute{e}A_P$

   $A \rightarrow S : E_S(Ident_A, E_{Cl\acute{e}A}(Ident_A, VoteA))$

9. *S* déchiffre le message, vérifie que l'identifiant est dans la liste des identifiants ;il vérifie aussi que celui-ci n 'a pas déjà été utilisé. Si l'identifiant est valide, il publie le vote chiffré dans une liste contenant tous les votes chiffrés des électeurs ayant déjà procédé à l'opération.

   $S : D_S(E_S(Ident_A, E_{Cl\acute{e}A}(Ident_A, VoteA))) = Ident_A, E_{Cl\acute{e}A}(Ident_A, VoteA)$

   $S : Ident_A \in \{Identifiant\}$

   $S : Ident_A \notin \{VotesChiffrés\}$

   $S : E_{Cl\acute{e}A}(Ident_A, VoteA), Ident_A \rightarrow \{VotesChiffrés\}$

10. *A* vérifie dans la liste que le vote qu'il a envoyé a été correctement reçu.

    $A : Ident_A\, E_{Cl\acute{e}A}(Ident_A, VoteA) \in \{VotesChiffrés\}$

11. *A* envoie à *S* la partie privée de la clé accompagnée de son identifiant.

    $A \rightarrow S : E_S(Ident_A, Cl\acute{e}A_S)$

12. *S* déchiffre le message ; il vérifie que l'identifiant a déjà été utilisé pour envoyer un vote chiffré ; si tel est le cas, la clé reçue va permettre de déchiffrer le vote. Après déchiffrement, il peut constater que l'identifiant est celui qui avait été annoncé. Il peut dès lors comptabiliser le vote. Il sait aussi que l'électeur ayant l'identifiant « $Ident_A$ » a voté ; plus personne ne pourra donc voter en utilisant cet identifiant.

    $S : D_S(E_S(Ident_A, Cl\acute{e}A_S)) = Ident_A, Cl\acute{e}A_S$

    $S : Ident_A \in \{VotesChiffrés\} \Rightarrow E_{Cl\acute{e}A}(Ident_A, VoteA)$

    $S : D_{Cl\acute{e}A}(E_{Cl\acute{e}A}(Ident_A, VoteA)) = Ident_A, VoteA$

    $S : VoteA,\ E_{Cl\acute{e}A}(Ident_A, VoteA) \rightarrow \{Votes\}$

    $S : Ident_A \rightarrow \{A\_Voté\}$

13. En fin de scrutin, *S* publie une liste des votes qu'il a reçus, sous les deux formes : en format chiffré, et en format déchiffré.

14. Si *A* constate que son vote n'a pas été correctement comptabilisé, il peut protester en envoyant un message à *S*.

    $A \rightarrow S : Ident_A, E_{Cl\acute{e}A}(Ident_A, VoteA) Cl\acute{e}A_S$

15. Si *A* veut modifier son vote (ce qui est possible dans certaines élections), il envoie le message suivant à *S*.

    $A \rightarrow S : Ident_A, E_{Cl\acute{e}A}(Ident_A, VoteA) VoteAbis$

b) Critères

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Pour pouvoir effectuer une demande d'identifiant, *A* doit être reconnu comme un électeur valable.

b. Personne ne peut voter plus d'une fois

→ Respecté

Seul un électeur préalablement enregistré (et reconnu en tant qu'électeur valable) recevra un et un seul identifiant ; il aura donc au plus une seule possiblité de vote.

c. Le vote d'un électeur doit être secret

→ Non respecté

Puisque, grâce au principe de la distribution des identifiants par la méthode ANDOS, l'organisateur n'a pas pu voir l'identifiant que le votant a reçu et associe à son vote, celui-ci n'a pas la possibilité de connaître, à l'issue du scrutin, à quel votant l'identifiant est associé.

Par contre, il est possible à l'électeur de prouver à n'importe qui quel a été son choix. Une telle possibilité est un danger pour le bon déroulement d'une élection : le fait qu'un électeur puisse prouver à autrui la manière dont il a voté peut être utilisé de manière nuisible à la démocratie : vente de votes aux plus offrants, menaces et contraintes, preuve de fidélité, copie de l'identifiant, ...

Comme l'électeur possède un moyen direct de vérifier son vote dans une liste, son vote n'est plus secret, puisque d'autres peuvent effectuer la même démarche.

d. Toute modification d'un vote doit être décelée

→ Non respecté

Grâce à son vote chiffré qui lui sert d'identifiant, l'électeur a la possibilité, à l'issue du scrutin, de retrouver son vote dans la liste des votes au moyen de celui-ci; il peut donc vérifier que son vote n'a pas été modifié. Il a même la possibilité de demander à modifier son vote, au cas où il changerait d'avis (cette manière d'agir n'est toutefois pas toujours autorisée).

L'organisateur ne sait pas quel votant viendra consulter la liste ; il ne peut donc pas, sans risque, effacer un vote et son identifiant.

L'organisateur connaît le nombre de personnes ayant manifesté leur intention de voter ; il connaît aussi le nombre de votes qui lui ont été transmis. La différence correspond au nombre d'électeurs qui se sont inscrits, mais n'ont pas voté. Il est envisageable que l'organisateur se substitue à ceux-ci pour enregistrer des votes supplémentaires.

e. *Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final*

→ Respecté

La liste des votes étant publiée, l'électeur, grâce au message chiffré contenant son vote et son identifiant qu'il a envoyé, peut retrouver son vote parmi tous ceux qui ont été comptabilisés. Il est donc certain que son vote a été pris en compte.

f. *Il est possible de savoir qui a voté ou non*

→ Non respecté

S ne peut pas vérifier si un électeur a bien voté ; tout ce qu'il peut dire, c'est que cet électeur a effectué ou non une demande.

c) Conclusions

La méthode *ANDOS* garantit que tous les électeurs ayant confirmé leur intention de participer à l'élection reçoivent un et un seul identifiant, sans que l'organisateur sache lequel. La liste des électeurs désirant voter et la liste des identifiants sont toutes deux publiées et possèdent le même nombre d'éléments, et chaque électeur ayant manifesté son intention de voter peut retrouver son nom dans la première, et son identifiant dans la seconde.

Toutes les élections ne le demandent pas, mais certaines exigent de savoir qui a voté ou non ; ce protocole ne permet pas à l'organisateur d'obtenir cette information.

Dans ce protocole, contrairement au protocole précédent, un électeur qui a manifesté son intention de voter, et qui a donc reçu un identifiant, ne peut pas vérifier que son identifiant n'a pas été utilisé, puisqu'il n'apparaît dans la liste des votes que sous une forme chiffrée. Il serait donc possible à l'organisateur de fausser le scrutin en rajoutant des votes. Un affichage de la liste des identifiants ayant été utilisés pour voter pourrait solutionner le problème ; le nombre de vote et le nombre de votants devrait être le même. Si un électeur possédant un identifiant et n'ayant pas voté trouve son identifiant dans la liste, c'est qu'il y a eu fraude.

Dans ce protocole, l'identifiant ne permet pas à l'organisateur de connaître l'identité du votant, mais cet identifiant pose un problème, car il permet a posteriori de rétablir un lien entre un électeur et son vote : si une personne parvient à connaître l'identifiant qu'un votant a utilisé, cette personne est aussi à même de connaître le choix de celui-ci.

Il est à noter que ce protocole original n'utilise pas la clé publique de l'organisateur pour chiffrer les messages que le votant envoie à celui-ci. Nous avons ajouté cette fonctionnalité afin d'augmenter la sécurité de ce protocole.

B. Théorème

Comme constaté après différentes tentatives, il ne semble pas possible de respecter tous les critères.

Essayons d'aller plus loin dans le raisonnement, et tentons de démontrer que toute élection où l'électeur traite en direct avec l'organisateur n'est pas une élection sécurisée.

Tout protocole de vote par Internet où l'électeur traite directement avec l'organisateur ne pourra jamais respecter les 6 critères de validité suivants :

1. Seuls les électeurs autorisés peuvent voter
2. Personne ne peut voter plus d'une fois
3. Le vote d'un électeur doit être secret
4. Toute modification d'un vote doit être décelée
5. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final
6. Pour certaines élections, il est possible de savoir qui a et qui n'a pas voté.

Dans le cas où l'électeur communique directement avec l'organisateur, il est impossible de connaître la liste des votants sans savoir pour qui ils ont voté (ce qui semble mettre dos à dos les critères 3 et 6).

Ce critère n'étant pas d'application à toute élection, nous allons plutôt nous attarder sur le fait que le vote doit être secret, c'est-à-dire qu'il ne peut pas exister de lien direct qui puisse relier l'électeur à son vote, sans pour cela laisser le champ libre à l'organisateur.

- Pour que l'organisateur n'ait pas la possibilité de changer les votes, il faut que les votes soient identifiables, donc que soit adjoint à chaque vote un champ d'identification et que celui-ci soit publié en regard du vote concerné à l'issue du scrutin.

  $ListeVotes=\{voteA,Ident_A\}$

- Par essence, un champ d'identification doit être connu à deux endroits différents ; il permet de relier des informations entre elles.
- Les protocoles qui précèdent ont tous un point en commun : l'électeur traite directement avec l'organisateur.
- Le champ d'identification doit servir à l'électeur afin de vérifier que son vote est pris en compte et n'a pas été changé ; l'électeur doit donc aussi le connaître.
- Ce champ d'identification est donc un lien qui relie directement un électeur avec son vote, ce qui est à l'encontre du secret de l'élection.

  X connaît $Ident_A \Rightarrow X$ connaît $voteA$

C.Q.F.D.

C. Vote en utilisant un tiers de confiance

Puisque l'électeur ne peut pas traiter directement avec l'organisateur, il faut un intermédiaire, un tiers de confiance entre l'organisateur et l'électeur. La confiance envers ce tiers porte sur la fiabilité des services qu'il doit proposer, la fiabilité de son matériel ; durant l'élection, il faut pouvoir être certain que le tiers pourra effectuer les opérations qui lui auront été assignées. Puisque le cas a été débattu auparavant, je ne vais pas, dans les protocoles qui suivent, envisager ceux où le résultat de l'élection n'est pas vérifiable, c'est-à-dire ceux pour lesquels, en fin de parcours, nous trouvons des votes qui ne sont pas d'une manière ou d'une autre identifiables. Cette impossibilité de contrôle enlèverait toute crédibilité à un tel scrutin.

1. Protocole simple utilisant un tiers de confiance

a) Protocole

Le principe de ce protocole est d'utiliser un intermédiaire qui permettra de masquer des informations à l'organisateur sans nuire à la sécurité et à la fiabilité de l'élection. Tout comme l'organisateur, le tiers de confiance devra posséder une clé de chiffrement qui aura été rendue publique et sera dès lors connue de tous les électeurs. Tout comme la clé de l'organisateur, la clé du tiers de confiance est bien sûr certifiée par une autorité de certification reconnue (**KCA** : **K**ey **C**ertification **A**uthority, ou **KDC** : **K**ey **D**istribution **C**enter) ; il n'y a donc pas possibilité pour une personne de se faire passer pour le tiers de confiance afin d'intercepter les votes.

Le tiers de confiance, placé en intermédiaire entre l'électeur et l'organisateur permettra, entre autres, de pouvoir prouver qu'un électeur a voté, sans que l'organisateur n'ait d'informations à ce propos durant l'élection.

Puisque le but de l'identifiant est de relier des informations communes, nous n'allons pas ici discuter de la manière dont l'identifiant est créé (par l'émetteur, par le récepteur au moyen d'un générateur aléatoire, ou en en utilisant un protocole de type ANDOS). Pour la clarté du protocole, quand différentes options peuvent être utilisées, sans changer la sécurité du protocole, nous n'utiliserons que l'identifiant créé par l'émetteur.

1. *S* publie la liste des électeurs et la communique à *T*.

   $S \rightarrow T : \{Electeur\}$

2. *A* envoie son vote à *T*.

   $A \rightarrow T : E_T(A,VoteA)$

3. *T* vérifie que la demande de *A* est fondée, c'est-à-dire que *A* appartient à la liste des électeurs et qu'il n'a pas encore voté.

   $T : D_T(E_T(A,VoteA)) = A,VoteA$

   $T : A \in \{Electeur\}$ et $A \notin \{A\_Voté\}$

4. *T* place l'électeur ainsi qu'un identifiant (généré de manière aléatoire) dans la liste des votants.

   T : $A,Ident_A \rightarrow \{A\_Voté\}$

5. *T* envoie le vote de *A* et l'identifiant crée à *S*.

   $T \rightarrow S$: $E_S(VoteA,Ident_A)$

6. *S* déchiffre le message et stocke le vote ainsi que son identifiant.

   S : $D_S(E_S(VoteA,Ident_A)) = VoteA,Ident_A$

   S : $VoteA,Ident_A \rightarrow \{Résultat\_Election\}$

7. A l'issue du scrutin, *T* envoie la liste des votants à *S*, après l'avoir mélangée.

   $T \rightarrow S$: $\{A\_Voté\}$

8. *S* publie la liste des votes et la liste des votants.

b) Critères

Ce protocole simpliste présente bien des défauts, mais l'on peut déjà remarquer qu'une dissociation est effectuée entre l'électeur et son vote, mais que la traçabilité, du fait des identifiants, est possible. Une autre remarque d'importance ; il saute aux yeux que le 6ème critère (Il est possible de savoir qui a voté) est, grâce à l'intermédiaire, d'une gestion aisée : la dissociation entre le vote et l'électeur est effectuée par le tiers de confiance.

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Un vote n'est accepté que si l'électeur est présent dans la liste des électeurs, qui est publiée.

b. Personne ne peut voter plus d'une fois

→ Respecté

Chaque fois qu'un électeur envoie son vote, une vérification est effectuée pour savoir si celui-ci est en droit de placer son vote .

c. Le vote d'un électeur doit être secret

→ Non respecté

L'électeur chiffre son vote au moyen de la clé du tiers de confiance ; le tiers de confiance transmet le vote à l'organisateur en le chiffrant avec la clé de ce dernier. A l'issue du scrutin, seuls l'électeur, le tiers de confiance et l'organisateur connaissent le vote.

S'il est logique que l'électeur soit au courant de son vote (aucune démonstration n'est nécessaire afin de prouver ceci), que l'organisateur soit au courant du vote (afin de pouvoir les comptabiliser), le tiers de confiance, quant à lui, n'est pas dans l'obligation de le connaître.

De plus, contrairement à l'organisateur, le tiers de confiance connaît l'électeur et son vote, il possède le lien direct et a donc à lui seul toutes les informations de l'élection, ce qui est contraire à notre définition du secret du vote.

d. Toute modification d'un vote doit être décelée

→ Non respecté

Dans ce protocole simpliste, l'électeur s'identifie auprès du tiers de confiance en lui présentant son identité. Aucun contrôle sur la validité de celle-ci n'est effectué ; il est donc possible pour tout un chacun de prendre l'identité de quelqu'un d'autre sans être inquiété ; si l'électeur ne vote pas, personne ne s'apercevra du manège.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Non respecté

Bien qu'il n'existe plus de lien direct entre l'électeur et son vote, il est possible, moyennant l'aide du tiers de confiance, de retrouver le vote de chacun. Il y a donc moyen, au prix d'une démarche dont il faudrait définir les critères de faisabilité, de retracer le chemin complet d'un vote précis.

Il est néanmoins possible que le tiers de confiance dupe les électeurs ; si deux électeurs, *A* et *B*, qui ont tous deux voté pour le même candidat, demandent une preuve que leur vote a été pris en compte, le tiers de confiance pourrait aisément tromper *B* en lui montrant le vote de *A*. (Voir Conclusions et si le tiers de confiance se mettait à tricher ?)

f. Il est possible de savoir qui a voté ou non

→ Respecté

Chaque vote reçu par le tiers de confiance est noté dans une liste, accompagnée d'un identifiant, et est publié.

c) Conclusions

Pour satisfaire aux critères de sécurité de vote, il faut que le vote soit caché au tiers de confiance afin que celui-ci ne puisse pas en connaître la teneur. Il convient donc de chiffrer celui-ci.

Il convient aussi de pouvoir prouver que l'auteur du vote est l'électeur que l'on dit être dans le message. Une paire de clés pour chaque électeur pourrait être une solution à ce problème. La paire de clés permettant la signature ainsi que le chiffrement est d'un type similaire à celui employé pour la clé de l'organisateur de l'élection. Il va de soi que l'organisateur de l'élection possède les clés publiques de tous les électeurs ($Liste=\{Electeur,Clé\}$) et que celles-ci sont certifiées.

Et si le tiers de confiance se mettait à tricher ?

Comment pourrait-il tricher ? D'une manière bien simple : puisque le vote est transmis en clair au tiers de confiance, il connaît le vote de tous les électeurs ; il sait

donc pour qui chacun a voté. Il lui est donc loisible d'établir les liens qu'il souhaite entre un électeur et un vote. Un exemple permettra aisément de comprendre :

Soient 2 électeurs, *A* et *B*, qui ont tous deux émis le même vote. Lorsque *T*, le tiers de confiance, reçoit ces deux votes, il stocke les votes accompagnés de leur identifiant respectif.

Pour l'électeur *A*, *T* ne triche pas et envoie le vote correct, accompagné d'un identifiant ($Ident_A$).

$T \rightarrow S : E_S(VoteA, Ident_A)$

Pour l'électeur *B*, *T* triche et envoie un vote qui n'est pas celui initialement envoyé par *B*, accompagné d'un identifiant ($Ident_B$).

$T \rightarrow S : E_S(VoteB\text{modifié}, Ident_B)$

Par contre, dans sa liste, il introduit des informations fausses et associe l'identifiant de *A* à l'électeur *B*.

$T : A, Ident_A \rightarrow \{A\_Voté\}$

$T : B, Ident_A \rightarrow \{A\_Voté\}$

Si, lors du contrôle, l'on demande à *T* de fournir la preuve que le vote de *B* a été pris en compte, *T* peut fournir comme identifiant $Ident_A$, et il aura ainsi donné l'impression que le vote de *B* a bien été pris en compte, alors que celui-ci a été remplacé par un vote frauduleux.

2. *Protocole utilisant un tiers de confiance ; amélioration*

a) Protocole

1. *S* publie la liste des électeurs et de leurs clés publiques et communique celle-ci à *T*.

   $S \rightarrow T : \{Electeur,Clé\}$

2. A envoie son vote chiffré à *T*; il le signe.

   $A \rightarrow T : E_T(A,S_A(E_S(VoteA)))$

3. *T* vérifie que la demande de *A* est fondée, c'est-à-dire que *A* appartient à la liste des électeurs et qu'il n'a pas encore voté ; il contrôle que le message provient de *A* en vérifiant la signature.

   $T : D_T(E_T(A,S_A(E_S(VoteA)))) = A,S_A(E_S(VoteA))$

   $T : A \in \{Electeur\}$ et $A \notin \{A\_Voté\}$

   $T : V_A(S_A(E_S(VoteA))) = E_S(VoteA)$

4. *T* place l'électeur, son vote chiffré et signé ainsi qu'un identifiant (généré de manière aléatoire) dans la liste des votants.

   $T : A,S_A(E_S(VoteA))Ident_A \rightarrow \{A\_Voté\}$

5. *T* envoie le vote chiffré de *A* ainsi que l'identifiant à *S*.

   $T \rightarrow S : E_S(E_S(VoteA)Ident_A)$

6. *S* déchiffre le message, déchiffre le vote, stocke celui-ci ainsi que son identifiant dans la liste des résultats.

   $S : D_S(E_S(E_S(VoteA)Ident_A)) = E_S(VoteA)Ident_A$

   $S : D_S(E_S(VoteA)) = VoteA$

   $S : VoteA,Ident_A \rightarrow \{Résultat\_Election\}$

7. A l'issue du scrutin, *T* envoie la liste des votants à *S*, après l'avoir mélangée.

   $T \rightarrow S : \{A\_Voté\}$

8. *S* publie la liste des votes et la liste des votants.

b) Critères

Les changements de ce protocole par rapport au précédent sont le chiffrement des données afin de les cacher. L'on s'aperçoit directement que, puisque la liste des votes est publiée, le tiers de confiance, qui y a accès, peut grâce à elle, connaître le vote de chaque votant ; en effet, il connaît le lien qui rattache le votant à son identifiant, et, par transitivité, il obtient facilement l'information. Nous nous retrouvons donc exactement dans la même situation que dans le cas précédent.

Même si la liste de résultats n'est pas publiée, il reste au tiers de confiance un autre système qui lui permet de connaître les votes sans pour cela connaître la clé de chiffrement : le nombre de possibilités de votes différents est limité, est un nombre fini ; T, comme tout le monde, a accès à la clé publique de S . S'il établit une liste $\{Vote_i, E_S(Vote_i)\}$, reprenant toutes les différentes possibilités de voter, il lui suffit de comparer chaque vote chiffré avec ceux de sa liste, et il pourra, pour chaque électeur, connaître le choix de chacun et établir une liste complète du scrutin. Ce chiffrement ne permet donc pas le secret.

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Un vote n'est accepté que si l'électeur est présent dans la liste des électeurs, qui est publiée.

b. Personne ne peut voter plus d'une fois

→ Respecté

Chaque fois qu'un électeur envoie son vote, une vérification est effectuée pour savoir si celui-ci est en droit de placer son vote .

c. Le vote d'un électeur doit être secret

→ Non respecté

L'électeur chiffre son vote au moyen de la clé du tiers de confiance ; le tiers de confiance transmet le vote à l'organisateur en le chiffrant avec la clé de ce dernier. A l'issue du scrutin, seuls l'électeur, le tiers de confiance et l'organisateur connaissent le vote.

S'il est logique que l'électeur soit au courant de son vote (je pense qu'aucune démonstration n'est nécessaire afin de prouver ceci), que l'organisateur soit au courant du vote (afin de pouvoir les comptabiliser), le tiers de confiance, quant à lui, n'est pas dans l'obligation de le connaître. Les explications ci-dessus montrent que, même s'il n'a pas accès directement au vote non chiffré, il n'a aucune difficulté à accéder a cette information.

De plus, contrairement à l'organisateur, le tiers de confiance connaît l'électeur et peut faire le lien avec son vote ; il possède le lien direct et a donc à lui seul toutes les informations de l'élection, ce qui est contraire à notre définition du secret du vote.

d. Toute modification d'un vote doit être décelée

→ Non respecté

Dans ce protocole, l'électeur s'identifie auprès du tiers de confiance en lui présentant son identité. Son message est signé et le tiers de confiance peut donc être certain que le message émane bien de la personne qui prétend en être. Il n'y a donc pas possibilité pour un tricheur d'endosser l'identité d'un électeur sans être en possession de sa clé privée.

Comme expliqué dans les conclusions du protocole précédent, il y a possibilité pour le tiers de confiance de fausser les élections. Il est capable, sans risque de se faire prendre, de modifier complètement le résultat d'une élection en substituant son vote au vote de certains électeurs.

e. *Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final*

→ Respecté

Bien qu'il n'existe plus de lien direct entre l'électeur et son vote, il est possible, moyennant l'aide du tiers de confiance, de retrouver le vote de chacun. Il y a donc moyen, au prix d'une démarche dont il faudrait définir les critères de faisabilité, de retracer le chemin complet d'un vote précis.

Il est néanmoins possible que le tiers de confiance dupe les électeurs ; si deux électeurs, *A* et *B*, qui ont tous deux votés pour le même candidat, demandent une preuve que leur vote a été pris en compte, le tiers de confiance pourrait aisément tromper *B* en lui montrant le vote de *A*. (Voir conclusions du protocole précédent : et si le tiers de confiance se mettait à tricher ?)

f. *Il est possible de savoir qui a voté ou non*

→ Respecté

Chaque vote reçu par le tiers de confiance est noté dans une liste, accompagnée d'un identifiant, et est publié.

c) Conclusions

Pas de changement par rapport au protocole précédent. L'essai de cacher le vote au tiers de confiance est un échec. Le fait que le vote soit chiffré de manière anonyme le rend aussi transparent que s'il n'avait pas été chiffré.

Pour éviter cet écueil, il faut donc que le vote soit chiffré de manière différente pour chaque électeur ; il faut donc adjoindre au vote un champ supplémentaire qui sera chiffré en même temps que lui.

3. *Protocole utilisant un tiers de confiance ; séparer pour régner*

a) Protocole

Ce protocole est décrit dans le livre « Applied Cryptography » et est présenté comme un protocole relativement sécurisé, puisque chacun des protagonistes n'a pas assez d'éléments pour pouvoir tricher seul. Ce protocole se décompose en deux parties :

I. Dans la première partie, les électeurs vont informer le tiers de confiance de leur intention de voter ; celui-ci octroie à chacun d'eux un numéro d'identification.

1. *S* publie une liste des électeurs et de leurs clés publiques et communique celle-ci à *T*.

   $S \rightarrow T : \{Electeur,Clé\}$

2. *A* envoie un message à *T* lui indiquant son intention de voter ; il lui demande un numéro d'identification.

   $A \rightarrow T : E_T(A,S_A(Demande))$

3. *T* vérifie que la demande de *A* est fondée, c'est-à-dire que *A* appartient à la liste des électeurs et qu'il n'a pas encore effectué de demande ; il contrôle que le message provient de *A* en vérifiant la signature.

   $T : D_T(E_T(A,S_A(Demande))) = A,S_A(Demande)$

   $T : A \in \{Electeur\}$ et $A \notin \{Demandeurs\}$

   $T : V_A(S_A(Demande)) = Demande$

4. *T* génère un « code d'électeur » ($Ident_T$) de manière aléatoire ; il l'attribue à *A* et place cette information dans deux listes ; l'une pour son propre usage, afin de vérifier que l'électeur n'effectue qu'une seule demande, l'autre afin de passer à *S* la liste des identifiants distribués; il envoie cet identifiant à *A*

   $T : Ident_T$

   $T : A \rightarrow \{Demandeurs\}$

   $T : Ident_T \rightarrow \{CodesElecteurs\}$

   $T \rightarrow A : E_A(Ident_T)$

II. Lorsque la période prévue pour cette première opération est échue, l'élection proprement dite peut commencer .

5. A cette fin, *T* envoie à *S* la liste des identifiants qu'il a distribués.

   $T \rightarrow S : \{CodesElecteurs\}$

6. *A* envoie son vote à *S*, accompagné de l'identifiant octroyé par *T* et d'un autre identifiant, qu'il génère lui-même ; il le chiffre.

   $A \rightarrow S : E_S(VoteA,Ident_T,Ident_A)$

7. *S* vérifie que le vote est acceptable, c'est-à-dire que le l'identifiant $Ident_T$ appartient à la liste des codes d'électeurs transmise par *T* et qu'il n'a pas encore voté ; *S* note que l'identifiant $Ident_T$ a été utilisé pour voter, consigne le vote en enregistrant la paire *VoteA* / $ident_A$ dans une liste

   $S : D_S(E_S(VoteA,Ident_T,Ident_A))=VoteA,Ident_T,Ident_A$

   $S : Ident_T \in \{CodesElecteurs\}$ et $Ident_T \notin \{A\_Voté\}$

   $S : VoteA,Ident_A \rightarrow \{RésutatsElection\}$

b) Critères

Dans ce protocole, il est clair que, contrairement aux précédents, le tiers de confiance, qui n'a qu'un rôle de distributeur d'identifiants, ne connaît rien des votes des électeurs. Comme il ne possède pas d'informations, le tiers de confiance n'est pas à même de pouvoir tricher.

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Un vote n'est accepté que si l'électeur a reçu son « code d'électeur » ; il n'a pu recevoir celui-ci que parce qu'il était un électeur reconnu et que c'était sa première demande.

b. Personne ne peut voter plus d'une fois

→ Respecté

Comme précisé ci-dessus, l'électeur ne peut recevoir qu'un seul « code d'électeur » ; lors du vote proprement dit, l'organisateur de l'élection vérifie la validité du code ; un code ne permet qu'un vote.

c. Le vote d'un électeur doit être secret

→ Non respecté

L'organisateur reçoit le vote de façon anonyme ; il connaît juste le lien qui lie le vote à l'identifiant que le votant y a joint. Il ne peut pas, sans l'aide du tiers de confiance, remonter jusqu'à l'électeur. Pour que l'organisateur connaisse ce lien, il faudrait qu'il y ait collusion entre l'organisateur et le tiers de confiance.

L'identifiant créé par l'électeur se retrouve publié en regard de son vote, en clair. L'organisateur et l'électeur sont tous deux en possession d'un élément qui permet de relier directement un électeur à son vote, ce qui contredit la définition que nous avons donnée secret du vote.

d. Toute modification d'un vote doit être décelée

→ Respecté

L'identifiant que l'électeur a placé en regard de son vote lui permet de retrouver celui-ci parmi tous les autres ; si le vote a été modifié, l'électeur peut s'en rendre compte de visu, en consultant la liste des votes publiée à l'issue de l'élection.

e. *Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final*

→ Respecté

Pour la même raison que ci-dessus, puisque chaque électeur a la possibilité de consulter son vote, il est donc certain que son vote est pris en compte. Comme tous les électeurs sont dans ce cas, la liste complète est donc valide et le résultat de l'élection peut être facilement contrôlé.

f. *Il est possible de savoir qui a voté ou non*

→ Non respecté

Le tiers de confiance est cantonné dans un rôle de distributeur d'identifiants ; il ne possède donc pas les éléments suffisants pour permettre d'informer l'organisateur des électeurs ayant participé ou non ; il peut seulement fournir une liste d'électeurs ayant manifesté leur intention de participer ; ceux qui ont réellement participé font partie de cette liste, mais c'est la seule information disponible.

c) Conclusions

Limiter les informations transmises au tiers de confiance, c'est aussi limiter les informations qu'il est capable de fournir. Ainsi, le fait de ne pas faire transiter le vote par son intermédiaire augmente le secret, mais il empêche par ailleurs tout contrôle permettant d'accéder au 6ème critère. Pour arriver à ce résultat, il faut donc que le vote transite par le tiers de confiance, mais sous une forme illisible pour celui-ci.

4. *Amélioration : le vote transite par le tiers de confiance*

a) Protocole

Afin de pouvoir être informé des participants à l'élection, le protocole précédent est modifié afin de faire transiter, sans pour autant le divulguer, le vote de l'électeur.

La demande préalable, vu que l'électeur fait transiter son vote par *T*, n'est plus nécessaire ; la vérification de la validité de l'électeur peut s'effectuer en temps réel.

1. *S* publie une liste des électeurs et de leurs clés publiques et communique celle-ci à *T*.

   $S \rightarrow T : \{Electeur,Clé\}$

2. *A* envoie un message à *T*, contenant son vote accompagné d'un identifiant ; celui-ci est chiffré afin de le rendre illisible pour *S* ; il est aussi signé afin que *T* ne puisse avoir aucun doute sur l'identité de *A*.

   $A \rightarrow T : E_T(A,S_A(E_S(VoteA,Ident_A)))$

3. *T* vérifie que la demande de *A* est fondée, c'est-à-dire que *A* appartient à la liste des électeurs et qu'il n'a pas encore effectué de demande ; il contrôle que le message provient de *A* en vérifiant la signature.

   $T : D_T(E_T(A,S_A(E_S(VoteA,Ident_A)))) = A,S_A(E_S(VoteA,Ident_A))$

   $T : A \in \{Electeur\}$ et $A \notin \{A\_Voté\}$

   $T : V_A(S_A(E_S(VoteA,Ident_A))) = E_S(VoteA,Ident_A)$

4. *T* place le nom de l'électeur dans la liste des électeurs ayant voté. Ceci permet d'éviter qu'un électeur vote à plusieurs reprises, et permet aussi, à l'issue du scrutin, de savoir quels sont les électeurs ayant réellement participé au scrutin. En parallèle, il transmet le vote de l'électeur à l'organisateur ; il le signe par sécurité. Comme celui-ci est chiffré en même temps qu'un identifiant, il est impossible à *T* de connaître le contenu du vote.

   $T : A \rightarrow \{A\_Voté\}$

   $T \rightarrow S : S_T(E_S(VoteA,Ident_A))$

5. *S* sait que le vote est acceptable, puisque la validité de l'électeur a été vérifiée par *T* ; *S* vérifie tout d'abord que l'envoi provient bien de *T*, en vérifiant la signature, ensuite, il déchiffre puis consigne le vote, et enregistre la paire vote / identifiant dans une liste.

   $S : V_T(S_T(E_S(VoteA,Ident_A))) = E_S(VoteA,Ident_A)$

   $S : D_S(E_S(VoteA,Ident_A)) = VoteA,Ident_A$

   $S : VoteA,Ident_A \rightarrow \{RésutatsElection\}$

b) Critères

Dans ce protocole, le tiers de confiance voit transiter les votes sans en connaître le contenu ; ceci lui permet, de noter les électeurs qui ont participé réellement, sans pour autant influer sur le secret de l'élection.

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Un vote n'est accepté que si l'électeur se trouve dans la liste des électeurs, publiée préalablement à l'élection ; le tiers de confiance, lors de l'élection, vérifie que le vote provient de la personne qui prétend voter et que cette personne est un électeur de la liste.

b. Personne ne peut voter plus d'une fois

→ Respecté

Comme précisé ci-dessus, la validité de l'électeur est contrôlée par le tiers de confiance au moment du vote ; un des contrôles est l'assurance que l'électeur n'a pas déjà voté.

c. Le vote d'un électeur doit être secret

→ Non respecté

L'organisateur reçoit le vote de façon anonyme ; il connaît juste le lien qui lie le vote à l'identifiant que le votant y a joint. Il ne peut pas, sans l'aide du tiers de confiance, remonter jusqu'à l'électeur. Pour que l'organisateur connaisse ce lien, il faudrait qu'il y ait collusion entre l'organisateur et le tiers de confiance.

Par ailleurs, l'identifiant créé par l'électeur se retrouve publié en regard de son vote, en clair. L'organisateur et l'électeur sont tous deux en possession d'un élément qui permet de relier directement un électeur à son vote, ce qui contredit la définition que nous avons donnée du secret du vote.

d. Toute modification d'un vote doit être décelée

→ Respecté

L'identifiant que l'électeur a placé en regard de son vote lui permet de retrouver celui-ci parmi tous les autres ; si le vote a été modifié, l'électeur peut s'en rendre compte de visu, en consultant la liste des votes publiée à l'issue de l'élection.

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Respecté

Pour la même raison que ci-dessus, puisque chaque électeur a la possibilité de consulter son vote, il est donc certain que son vote est pris en compte. Comme tous les électeurs sont dans ce cas, la liste complète est donc valide et le résultat de l'élection peut être facilement contrôlé.

f. Il est possible de savoir qui a voté ou non

→ Respecté

Lors du transit du vote, le tiers de confiance prend note de l'électeur qui vient de voter. A l'issue du scrutin, il est donc possible de déterminer dans la liste des électeurs ceux qui ont voté et ceux qui ne l'auront pas fait. Ceci permet une vérification croisée supplémentaire : le nombre d'électeurs et le nombre de votes devraient être exactement les mêmes.

c) Conclusions

Ce protocole semble ne pas être très loin du résultat escompté ; 5 des 6 points sont correctement respectés ; un seul est encore problématique : le secret du vote ; celui-ci pourtant est primordial pour l'obtention d'élections sécurisées. Le problème réside dans le fait que nous voulions une élection dont les votes soient traçables, et qui doivent dès lors être « marqués », « identifiés ».

D. Théorème

Tout protocole de vote par Internet où l'électeur et l'organisateur utilisent un seul tiers de confiance ne pourra jamais respecter les 6 critères de validité suivants :

1. Seuls les électeurs autorisés peuvent voter
2. Personne ne peut voter plus d'une fois
3. Le vote d'un électeur doit être secret
4. Toute modification d'un vote doit être décelée
5. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final
6. Pour certaines élections, il est possible de savoir qui a et qui n'a pas voté.

Pour pouvoir prouver à un électeur que son vote a été pris en compte, il faut qu'un vote soit traçable. Cette traçabilité impose que chaque vote enregistré soit différentiable des autres, ce qui nécessite l'existence d'un identifiant permettant, dans la liste des votes de l'organisateur de retrouver un vote parmi tous les autres.

Pour cette même raison, il faut que l'électeur possède un élément qui permette la traçabilité aussi ; nous appellerons cet élément « identifiant » aussi, puisqu'il sert à identifier, bien qu'il puisse prendre plusieurs formes (cela pourrait être simplement l'identité de l'électeur, mais cela nuirait quelque peu au secret...)

Pour qu'un identifiant soit utile, il faut qu'au moins deux parties le connaissent ; considérons l'identifiant se trouvant dans la liste des votes de l'organisateur ; celui-ci est évidemment connu de l'organisateur et d'une autre partie ; il y a donc deux cas de figure :

- Soit l'identifiant est partagé entre l'organisateur et l'électeur ①
- Soit l'identifiant est partagé entre l'organisateur et le tiers de confiance ②

Analysons ces deux cas séparément

① Identifiant partagé entre l'organisateur et l'électeur

L'électeur et l'organisateur possèdent un identificateur commun ; il existe donc un lien direct qui permet de relier un électeur à son vote, ce qui va à l'encontre du secret de l'élection (critère 3).

② Identifiant partagé entre l'organisateur et le tiers de confiance, donc pas d'identifiant partagé entre l'électeur et l'organisateur

Puisque l'organisateur et l'électeur ne possèdent pas d'identifiant commun, c'est que l'identifiant de l'électeur n'a pas accompagné son vote jusqu'à l'organisateur (sinon, nous nous retrouverions dans le cas ①).

L'identifiant de l'électeur est lui aussi partagé avec le tiers de confiance (sinon, nous nous retrouverions aussi dans le cas ①).

Le tiers de confiance possède donc en mains

- un identifiant commun avec l'électeur, et le lien qui relie l'électeur à son identifiant.
- un identifiant commun avec l'organisateur, ainsi que le lien qui le relie au vote (l'on a vu précédemment qu'un vote chiffré, s'il est anonyme, ne peut pas être considéré comme secret)

En résumé, le tiers de confiance possède toutes les informations nécessaires pour, à lui seul, recomposer l'élection complète, attribuant son vote à chaque électeur. Une seule organisation possède, à elle seule, toutes les informations concernant l'élection ; ceci est contraire au 3ème critère (Le vote d'un électeur doit être secret)

Quel que soit le cas, le résultat est le même ; au moins un des 6 critères n'est pas respecté. Puisque les cas ① et ② sont complémentaires, nous avons couvert toutes les possibilités ; il est donc impossible, avec un seul tiers de confiance, de respecter les 6 critères simultanément.

C.Q.F.D.

E. Vote utilisant deux tiers de confiance

Puisqu'il est établi qu'un seul tiers de confiance est une condition nécessaire mais pas suffisante pour pouvoir respecter les 6 critères de sécurité d'une élection, nous allons travailler en utilisant deux tiers de confiance, que nous nommerons T_1 et T_2

La technique du « diviser pour régner » va permettre de dissocier l'électeur et son vote : en effet, l'un des tiers connaît l'électeur, sans connaître son vote, tandis que l'autre connaît le vote sans connaître l'électeur. Il va de soi que l'organisateur connaît le vote sans connaître l'électeur, et, de plus, ne possède pas d'information permettant d'identifier directement celui-ci.

En résumé, en fin d'opération, chacun connaît une partie du secret :

- ☑ *A* connaît *A*, *VoteA*, $Ident_{A1}$
- ☑ T_1 connaît : *A*, $Ident_{A1}$
- ☑ T_2 connaît : *VoteA*, $Ident_{A2}$
- ☑ *S* connaît : *VoteA*, $Ident_{A2}$

Pour atteindre T_2 sans que T_1 soit au courant du vote, et que T_2 ne connaisse pas *A*, il faut que le vote de *A* transite par T_1, mais de manière à ce que T_1 ne puisse pas le lire ; il faut donc que *A* le chiffre.

Nous avons vu précédemment que, si l'on chiffre un message qui possède un nombre fini de variantes, il suffisait de chiffrer soi-même toutes les variantes et de comparer afin de pouvoir connaître la valeur du message avant chiffrement ; il faut donc accompagner le chiffrement d'une variable aléatoire.

Pour envoyer le message à T_2, illisible par T_1, le message devra être d'une forme semblable à la suivante : $E_{T_2}(Var, VoteA)$. Ce champ variable ne peut en aucun cas être l'identifiant commun à *A* et à T_1, sous peine de se retrouver dans la même problématique, T_1 étant capable de reproduire toutes les variantes du vote. Il faut donc que le champ variable soit généré par *A* tout en étant inconnu de T_1.

Le champ variable étant généré par l'électeur au moment de son vote, il n'est pas exclu (bien que la probabilité soit très faible) que deux électeurs aient sélectionné le même vote et la même variable. Il n'est donc pas possible de considérer le message chiffré $E_{T_2}(Var, VoteA)$ comme un identifiant, puisqu'il existe une possibilité (très faible, mais présente) de doublon. Pour qu'il existe une traçabilité qui ne permette aucun doute, il faudra donc éliminer cette possibilité de doublon. Pour ce faire, deux options s'offrent à nous :

- ☑ S'arranger pour que le champ variable soit identifiant
- ☑ Placer un identifiant qui fasse le lien entre T_1 et T_2.

L'utilisation de deux tiers de confiance rendant la procédure plus longue, il pourrait arriver qu'un électeur vote une seconde fois alors que son premier vote est toujours en cours de traitement. Pour éviter ce problème, une nouvelle liste, la liste des votants en cours de procédure, permettra de détecter et d'empêcher cet état de fait.

1. *L'électeur génère ses identifiants*

a) Protocole

Passons en revue toutes les listes qui seront nécessaires dans ce Protocole

- ☑ La liste des électeurs, contenant les informations suivantes :
  - *A*
  - Clé publique de *A*
- ☑ La liste des votants en cours, contenant les informations suivantes :
  - *A*
  - $Ident_1$
  - le message que T_1 est chargé de transmettre à T_2
  - le message que *A* a transmis à T_1 signé.
- ☑ La liste des votants, contenant les mêmes informations que la précédente ; en fait, en fin de procédure de vote, les informations d'un vote contenues dans la liste des votants en cours sont retirées de celle-ci et transférées dans la liste des votants.
- ☑ La liste des participants, qui est la liste des votants simplifiée, que T_1 envoie à *S* à l'issue du scrutin ; cette liste sera publiée et contient les informations suivantes :
  - *A*
  - $Ident_1$
- ☑ La liste des votes, qui reprend l'ensemble des votes qui ont été envoyés par T_1 à T_2, auxquels T_2 adjoint un identifiant avant de transférer à *S*.
  - *VoteA*
  - $Ident_3$
- ☑ La liste des résultats, qui reprend l'ensemble des votes qui ont été envoyés par T_2 à *S* ; si le vote est correct, la liste des votes en possession de T_2 et celle-ci devraient être semblables.
  - *VoteA*
  - $Ident_3$
- ☑ La liste des identifants, utilisée par T_2 afin d'éviter que deux votant aient généré (risque fort improbable, mais pas nul) le même identifiant. Si tel est le cas, il faut prévenir le votant qu'il doit recommencer sa procédure de vote.
  - $Ident_3$

2. L'organisation (S) établit la liste des électeurs (registre employés, population, inscription volontaire,...). Notez que cette tâche pourrait être exécutée par T_1, et ensuite envoyée à S ; l'important est que S et T_1 possèdent la même liste des électeurs. La publication de cette liste des électeurs permet de vérifier que personne n'a été oublié et qu'il n'y a pas d'électeurs-fantômes qui pourraient mettre à mal l'élection.

   $S : A, cléA \rightarrow \{Electeurs\}$

3. S envoie la liste des électeurs potentiels à T_1.

   $S \rightarrow T_1 : E_{T_1}(\{Electeurs\})$

4. A vote et envoie son vote à T_1 ; il le chiffre à l'intention de T_2 en y ajoutant un identifiant ; il signe le tout après y avoir adjoint un identifiant à l'intention de T_1. Il s'identifie.

   $A \rightarrow T_1 : E_{T_1}(A, S_A(Ident_1, E_{T_2}(Ident_2, VoteA)))$

5. T_1 déchiffre le message et vérifie que A est un électeur valide (c'est-à-dire qu'il est présent sur la liste des électeurs et qu'il ne l'est pas encore ni sur la liste des votants ni sur celle des votants en cours de procédure) et que A est l'auteur du message, en contrôlant sa signature.

   $T_1 : D_{T_1}(E_{T_1}(A, S_A(Ident_1, E_{T_2}(Ident_2, VoteA)))) = A, S_A(Ident_1, E_{T_2}(Ident_2, VoteA))$

   $T_1 : A \in \{Electeur\}$ et $A \notin \{En\_Cours\}$ et $A \notin \{A\_Voté\}$

   $T_1 : V_A(S_A(Ident_1, E_{T_2}(Ident_2, VoteA))) = Ident_1, E_{T_2}(Ident_2, VoteA)$

6. Si $A \notin \{Electeur\}$ ou $A \in \{En\_Cours\}$ ou $A \in \{A\_Voté\}$, l'électeur A n'est pas (ou plus) autorisé à voter. T_1 en informe A ; il serait envisageable d'envoyer un message différent pour chaque type de problème.

   $T_1 \rightarrow A : E_A(Not\_OK, A)$

7. Si $Ident_1 \in \{En\_Cours\}$ ou $Ident_1 \in \{A\_Voté\}$, l'identifiant $Ident_1$ est un doublon. Si $E_{T_2}(Ident_2, VoteA) \in \{En\_Cours\}$, l'identifiant $Ident_2$ est un doublon. T_1 en informe A .

   $T_1 \rightarrow A : E_A(Not\_OK, Ident_1, E_{T_2}(Ident_2, VoteA))$

8. A déchiffre le message ; apprenant qu'un identifiant n'est pas accepté, A relance la procédure à partir du point 3. en utilisant un nouvel identifiant.

   $A : D_A(E_A(Not\_OK, Ident_1, E_{T_2}(Ident_2, VoteA))) = Not\_OK, Ident_1, E_{T_2}(Ident_2, VoteA)$

   GOTO étape 4.

7'. T_1 envoie le vote chiffré à T_2 et place temporairement l'électeur A ainsi que son vote dans la liste des votants en cours, afin d'éviter les votes doubles.

   $T_1 \rightarrow T_2 : E_{T_2}(Ident_2, VoteA)$

   $T_1 : A, Ident_1, E_{T_2}(Ident_2, VoteA), S_A(Ident_1, E_{T_2}(Ident_2, VoteA)) \rightarrow \{En\_Cours\}$

8'. T_2 déchiffre le message.

$T_2 : D_{T_2}(E_{T_2}(Ident_2,VoteA))=Ident_2,VoteA$

9'. T_2 vérifie que l'identifiant n'a pas encore été utilisé. Si $Ident_2 \in \{Identifiants\}$, l'identifiant est un doublon. T_2 en informe T_1 .

$T_2 \rightarrow T_1 : E_{T_1}(Not\_OK,E_{T_2}(Ident_2,VoteA))$

$T_1 : D_{T_1}(E_{T_1}(Not\_OK,E_{T_2}(Ident_2,VoteA)))=Not\_OK,E_{T_2}(Ident_2,VoteA)$

10'. T_1 retrouve A grâce à son vote chiffré conservé dans la liste des votes en cours. Il est à noter que $E_{T_2}(Ident_2,VoteA)$ est unique ; cet état de fait a été testé au point 6.

$T_1 : E_{T_2}(Ident_2,VoteA) \in \{En\_Cours\} \Rightarrow A,Ident_1 , S_A(Ident_1,E_{T_2}(Ident_2,VoteA))$

11'. T_1 informe A que son identifiant a posé problème ; il retire A et les informations concernant son vote de celui-ci de la liste des votants en cours.

$T_1 \rightarrow A : E_A(Not\_OK,Ident_1,E_{T_2}(Ident_2,VoteA))$

$T_1 : A,Ident_1,E_{T_2}(Ident_2,VoteA), S_A(Ident_1,E_{T_2}(Ident_2,VoteA)) \leftarrow \{En\_Cours\}$

12'. A déchiffre le message ; apprenant que son identifiant n'est pas accepté, A recommence la procédure à partir du point 4, en générant de nouveaux identifiants.

$A : A : D_A(E_A(Not\_OK,Ident_1,E_{T_2}(Ident_2,VoteA)))=Not\_OK,Ident_1,E_{T_2}(Ident_2,VoteA)$

GOTO étape 4.

9". Si $Ident_2 \notin \{Identifiants\}$, l'identifiant n'a pas encore été utilisé et est donc correct. T_2 envoie donc à T_1 un message l'informant de la validité du vote.

$T_2 \rightarrow T_1 : E_{T_1}(OK,E_{T_2}(Ident_2,VoteA))$

$T_1 : D_{T_1}(E_{T_1}(OK,E_{T_2}(Ident_2,VoteA)))=OK,E_{T_2}(Ident_2,VoteA)$

10". T_1 retrouve A grâce à son vote chiffré conservé dans la liste des votes en cours.

$T_1 : E_{T_2}(Ident_2,VoteA) \in \{En\_Cours\} \Rightarrow A,Ident_1 , S_A(Ident_1,E_{T_2}(Ident_2,VoteA))$

11". T_1 informe A que son vote a été correctement traité ; T_1 retire A et le vote de celui-ci de la liste des votants en cours et l'ajoute dans la liste des votants. L'électeur ainsi que son identifiant sont ajoutés à la liste des participants à l'élection qui est publiée.

$T_1 \rightarrow A : E_A(OK,E_{T_2}(Ident_2,VoteA))$

$T_1 : A,Ident_1,E_{T_2}(Ident_2,VoteA), S_A(Ident_1,E_{T_2}(Ident_2,VoteA)) \leftarrow \{En\_Cours\}$

$T_1 : A,Ident_1,E_{T_2}(Ident_2,VoteA), S_A(Ident_1,E_{T_2}(Ident_2,VoteA)) \rightarrow \{A\_Voté\}$

T_1 : $A,Ident_1 \rightarrow \{Participants\}$

12". T_2 envoie le vote qu'il a accepté à S ; il y joint un identifiant. Il place le vote et l'identifiant dans la liste des votes.

$T_2 \rightarrow S$: $E_S(VoteA,Ident_3)$

T_2 : $VoteA,Ident_3 \rightarrow \{Votes\}$

13". S déchiffre le message et enregistre le vote ainsi que l'identifiant qui lui est associé.

S : $D_S(E_S(VoteA,Ident_3)) = VoteA,Ident_3$

S : $VoteA,Ident_3 \rightarrow \{Résultat\}$

14". A l'issue du scrutin, la liste des résultats est publiée ainsi que la liste des participants. Ces deux listes doivent contenir le même nombre d'enregistrements.

En fin d'opération :

- ☑ A connaît : A, $VoteA$, $Ident_1$, $Ident_2$, $E_{T_2}(Ident_2,VoteA)$
- ☑ T_1 connaît : A, $Ident_1$, $E_{T_2}(Ident_2,VoteA)$,
- ☑ T_2 connaît : $VoteA$, $Ident_2$, $E_{T_2}(Ident_2,VoteA)$, $Ident_3$
- ☑ S connaît : $VoteA$, $Ident_3$

Listes publiques :

- ☑ Electeurs : cette liste existe et est fixée avant le début de l'élection
- ☑ Participants : liste contenant 2 champs : A et $Ident_1$
- ☑ Résultat : liste contenant 2 champs : $VoteA$ et $Ident_3$

b) Critères

Dans ce protocole, le premier tiers de confiance (T_1), voit transiter les votes sans en connaître le contenu ; ceci lui permet de noter les électeurs qui ont participé à l'élection, sans pour autant influer sur le secret de l'élection. T_2 reçoit le vote de manière anonyme : il connaît le contenu, mais pas l'électeur. A et S ne partagent aucune information, si ce n'est le vote lui-même.

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Un vote n'est accepté que si l'électeur se trouve dans la liste des électeurs publiée préalablement à l'élection ; le premier tiers de confiance, lors de l'élection, vérifie que le vote provient de la personne qui prétend voter et que cette personne est un électeur de la liste.

b. Personne ne peut voter plus d'une fois

→ Respecté

Comme précisé ci-dessus, la validité de l'électeur est contrôlée par le premier tiers de confiance au moment du vote ; un des contrôles est l'assurance que l'électeur n'a pas déjà voté.

c. Le vote d'un électeur doit être secret

→ Respecté

L'organisateur reçoit le vote de façon anonyme ; il connaît juste le lien qui lie le vote à l'identifiant donné par le second tiers de confiance. Le second tiers de confiance ne connaît pas l'identité de l'électeur, puisque le premier tiers lui a transmis le vote sans indiquer quel était l'électeur ; il connaît seulement un identifiant qui lui a été transmis (de manière chiffrée) par le premier tiers ; cet identifiant est le lien qui lui permet le relier à l'électeur. Il y a aussi une donnée qui est partagée par les deux tiers de confiance et qui pourrait servir à réunir l'électeur et son vote : c'est le vote chiffré que l'électeur fait transiter par le premier tiers de confiance. Au moyen de celui-ci, s'il y a collusion entre les deux tiers de confiance, nous nous ramenons au cas précédent (un seul tiers de confiance) et le secret du vote peut être mis à jour.

d. Toute modification d'un vote doit être décelée

→ Respecté

Les identifiants placés par l'électeur et par les tiers de confiance peuvent permettre de retracer le cheminement complet du vote. Pour cela, il faut que les différents protagonistes donnent chacun un morceau du puzzle. Puisqu'il est possible de recréer le chemin d'un vote au départ d'un électeur, il peut être possible de créer une procédure qui permettrait à tout électeur de vérifier la validité de son vote (une procédure doit être mise en place afin de permettre, a posteriori, à un électeur de consulter son vote ; les modalités de cette consultation doivent permettre de conserver le secret du vote), il n'est donc pas possible de le modifier sans avoir le risque d'être découvert. De plus, le nombre de personnes comptabilisées par le premier tiers comme ayant voté ($\{Participants\}$) doit correspondre au nombre de votes comptabilisés par le second tiers ($\{Votes\}$) ainsi qu'à ceux comptabilisés par l'organisateur ($\{Résultat\}$).

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Respecté

Pour la même raison que ci-dessus, puisque chaque électeur a la possibilité de consulter son vote, il peut donc être certain que son vote est pris en compte. Comme tous les électeurs sont dans ce cas, la liste complète est donc valide et le résultat de l'élection peut être facilement contrôlé.

f. Il est possible de savoir qui a voté ou non

→ Respecté

Lors du transit du vote, le premier tiers de confiance prend note de l'électeur qui vient de voter. A l'issue du scrutin, il est donc possible de consulter la liste des électeurs qui ont voté et donc, par élimination à partir de la liste des électeurs, ceux qui ne l'ont pas fait. Ceci permet une vérification croisée supplémentaire : le nombre de votants et le nombre de votes doit être exactement le même.

c) Conclusions

Le fait d'avoir placé deux tiers de confiance comme intermédiaires entre l'organisateur et l'électeur cache donc complètement le lien direct qui relie l'électeur à son vote, sans pour autant le briser. Il est toujours possible de reconstruire complètement l'élection à partir des données que se partagent les différents protagonistes, alors qu'aucun d'eux n'est capable à lui seul d'effectuer cette opération. L'électeur est aussi mis au courant de la prise en compte de son vote. Ce protocole respecte les 6 critères de sécurité du vote sur Internet.

Il est toutefois à remarquer que les deux tiers de confiance possèdent une information commune, en provenance de l'électeur, et qui pourrait jouer le rôle d'identifiant : $E_{T_2}(Ident_2, VoteA)$. La seule différence est que le premier tiers ne la connaît que sous forme chiffrée, alors que le second a la possibilité de le déchiffrer. Il apparaît donc qu'une certaine redondance d'information existe entre l'électeur et les tiers de confiance ; chacun d'entre eux possède un identifiant lui permettant de retrouver un vote chez les deux autres ; il serait dès lors plus aisé qu'un seul identifiant soit commun aux trois.

D'autre part, pour éviter les problèmes de doublons, l'identifiant pour tous les électeurs devrait être généré par une seule et même personne ; de cette manière, chacun des électeurs recevra un identifiant unique.

Pour améliorer le protocole précédent, nous allons le transformer de la manière suivante :

- ☑ Un seul identifiant sera commun entre l'électeur et les deux tiers de confiance.
- ☑ Le premier tiers de confiance sera chargé de générer les identifiants et de les distribuer aux électeurs.

2. *L'identifiant est distribué par le tiers de confiance*

a) Protocole

Comme pour le protocole précédent, passons en revue toutes les listes qui seront nécessaires :

- ☑ La liste des électeurs, contenant les informations suivantes :
  - *A*
  - Clé publique de *A*
- ☑ La liste des votants en cours, contenant les informations suivantes :
  - *A*
  - $Ident_1$
  - $Ident_2$
  - le message
  - le message signé que *A* a transmis à T_1, T_1 étant chargé de le transmettre à anonymement à T_2.
- ☑ La liste des votants, contenant les mêmes informations que la précédente ; en fait, en fin de procédure de vote, les informations d'un vote contenues dans la liste des votants en cours sont retirées de celle-ci et transférées dans la liste des votants.
- ☑ La liste des participants, qui est la liste des votants simplifiée, que T_1 envoie à *S* à l'issue du scrutin ; cette liste sera publiée et contient les informations suivantes :
  - *A*
  - $Ident_1$
- ☑ La liste des votes, qui reprend l'ensemble des votes qui ont été envoyés par T_1 à T_2, auxquels T_2 adjoint un identifiant avant de transférer à *S*.
  - *VoteA*
  - $Ident_3$
- ☑ La liste des résultats, qui reprend l'ensemble des votes qui ont été envoyés par T_2 à *S* ; si le vote est correct, la liste des votes en possession de T_2 et celle-ci devraient être semblables.
  - *VoteA*
  - $Ident_3$

1. *S* établit la liste des électeurs (registre employés, population, inscription volontaire ...) Cette liste comporte, pour chaque électeur, son identification ainsi que sa clé publique. Comme dans le protocole précédent, T_1 pourrait se

charger de cette tâche, l'important étant en fin de compte que S et T_1 utilisent une même liste d'électeurs, liste pouvant être rendue publique.

$S : A, cléA \rightarrow \{Electeurs\}$

2. S envoie la liste des électeurs potentiels à T_1.

   $S \rightarrow T_1 : E_{T_1}(\{Electeurs\})$

3. A vote et envoie celui-ci à T_1 ; il le chiffre à l'intention de T_2 ; il y ajoute une variable servant à masquer le vote pour T_1 ; il signe le tout. Il s'identifie.

   $A \rightarrow T_1 : E_{T_1}(A, S_A(E_{T_2}(Var, VoteA)))$

4. T_1 déchiffre le message et vérifie que A est un électeur valide (c'est-à-dire qu'il est présent sur la liste des électeurs et qu'il ne l'est pas encore ni sur la liste des votants ni sur celle des votants en cours de procédure) et que A est l'auteur du message, en contrôlant sa signature.

   $T_1 : D_{T_1}(E_{T_1}(A, S_A(E_{T_2}(Var, VoteA)))) = A, S_A(E_{T_2}(Var, VoteA))$

   $T_1 : A \in \{Electeur\}$ et $A \notin \{En\_Cours\}$ et $A \notin \{A\_Voté\}$

   $T_1 : V_A(S_A(E_{T_2}(Var, VoteA))) = E_{T_2}(Var, VoteA)$

5. T_1 génère un identifiant, pour A et un autre pour T_2 ; il envoie le vote chiffré à T_2, accompagné du second identifiant. Il envoie un message à A, accompagné du premier identifiant, en guise d'accusé de réception et place temporairement l'électeur A, son vote signé et les identifiants dans la liste des votes en cours de traitement, afin d'éviter les votes doubles.

   $T_1 \rightarrow A : E_A(Ident_1, E_{T_2}(Var, VoteA))$

   $T_1 \rightarrow T_2 : E_{T_2}(Ident_2, E_{T_2}(Var, VoteA))$

   $T_1 : A, Ident_1, Ident_2, S_A(E_{T_2}(Var, VoteA)) \rightarrow \{En\_Cours\}$

6. A déchiffre le message et prend note de l'identifiant qui lui est assigné.

   $A : D_{T_2}(E_{T_2}(Ident_1, E_{T_2}(Var, VoteA))) = Ident_1, E_{T_2}(Var, VoteA)$

7. T_2 déchiffre le message et prend note de l'identifiant.

   $T_2 : D_{T_2}(E_{T_2}(Ident_2, E_{T_2}(Var, VoteA))) = Ident_2, E_{T_2}(Var, VoteA)$

   $T_2 : D_{T_2}(E_{T_2}(Var, VoteA)) = Var, VoteA$

8. T_2 envoie le vote qu'il a accepté à S ; il y joint un identifiant qu'il génère. Il place le vote, l'identifiant reçu et l'identifiant généré dans la liste des votes.

   $T_2 \rightarrow S : E_S(VoteA, Ident_3)$

   $T_2 : VoteA, Ident_2, Ident_3 \rightarrow \{Votes\}$

9. *S* déchiffre le message et enregistre le vote ainsi que l'identifiant qui lui est associé ; il envoie à T_2 un accuse réception du vote.

   $S : D_S(E_S(VoteA,Ident_3)) \models VoteA,Ident_3$

   $S : VoteA,Ident_3 \rightarrow \{Résultat\}$

   $S \rightarrow T_2 : E_{T_2}(OK,Ident_3)$

10. T_2 déchiffre le message reçu de S. Grâce à l'identifiant de ce message, il retrouve le vote dans la liste des votes. Il envoie à T_1 un accusé de réception signifiant que son vote a été envoyé à *S* qui l'a enregistré.

    $T_2 : D_{T_2}(E_{T_2}(OK,Ident_3)) \models OK,Ident_3$

    $T_2 : Ident_3 \in \{Votes\} \Rightarrow VoteA,Ident_2$

    $T_2 \rightarrow T_1 : E_{T_1}(OK,Ident_2)$

11. T_1 déchiffre le message ; il retire *A* ainsi que les informations au sujet de son vote de la liste des votants en cours et le place dans la liste des votants. L'électeur ainsi que son identifiant sont ajoutés à la liste des participants à l'élection qui est publiée.

    $T_1 : D_{T_1}(E_{T_1}(OK,Ident_2)) \models OK,Ident_2$

    $T_1 : Ident_2 \in \{En\_Cours\} \Rightarrow A,Ident_1,S_A(E_{T_2}(Var,VoteA))$

    $T_1 : A,\ Ident_1,Ident_2,S_A(E_{T_2}(Var,VoteA)) \leftarrow \{En\_Cours\}$

    $T_1 : A,Ident_1,Ident_2,S_A(E_{T_2}(Var,VoteA)) \rightarrow \{A\_Voté\}$

    $T_1 : A,Ident_1 \rightarrow \{Participants\}$

12. T_1 informe *A* que son vote est accepté.

    $T_1 \rightarrow A : E_A(OK,Ident_1)$

13. A la fin de l'élection, T_1 publie la liste des participants. *S* publie la liste des votes et leur identifiant.

    En fin d'opération :

    - ☑ *A* connaît : *A*, *VoteA*, $Ident_1$, $E_{T_2}(Var,VoteA)$
    - ☑ T_1 connaît : *A*, $Ident_1$, $Ident_2$, $E_{T_2}(Var,VoteA)$
    - ☑ T_2 connaît : *VoteA*, $Ident_2$, $Ident_3$, $E_{T_2}(Var,VoteA)$
    - ☑ *S* connaît : *VoteA*, $Ident_3$

    Listes publiques :

    - ☑ Electeurs : cette liste existe et est fixée avant le début de l'élection
    - ☑ Participants : liste contenant 2 champs : *A* et $Ident_1$
    - ☑ Résultat : liste contenant 2 champs : *VoteA* et $Ident_3$

b) Critères

Dans ce protocole, l'on pourrait croire que les identifiants $Ident_1$, commun à A et à T_1, et $Ident_2$, commun à T_1 et à T_2, ne sont pas nécessaire du fait de l'existence d'une autre variable, $E_{T_2}(Var;VoteA)$, mais il n'en n'est rien : cette variable, bien qu'il y ait de fortes chances pour qu'elle soit unique, n'est pas déclarée comme l'étant ; il se pourrait, à une probabilité minime, que deux électeurs ayant voté de la même manière génèrent le même champ variable. Les identifiant $Ident_1$ et $Ident_2$, par contre, sont générés par T_1, ce qui permet d'avoir la certitude que les identifiants sont uniques pour chaque électeur. En fin d'opération, A et S ne partagent aucune information, si ce n'est le vote lui-même.

Un seul identifiant aurait pu être utilisé en lieu et place des deux identifiants du protocole ci-dessus semble-t-il, mais il devenait alors impossible de rendre publique la liste des électeurs ayant voté accompagnée de l'identifiant ; en effet, cette liste étant publique, le second tiers de confiance, T_2, aurait pu l'employer pour reconstituer l'élection complète, vu qu'il recevait, par le biais de cette liste publique, le lien entre l'identifiant et l'électeur, alors qu'il possédait déjà le lien entre l'identifiant et le vote.

a. Seuls les électeurs autorisés peuvent voter

→ Respecté

Un vote n'est accepté que si l'électeur se trouve dans la liste des électeurs, publiée préalablement à l'élection ; le premier tiers de confiance, lors de l'élection, vérifie que le vote provient de la personne qui prétend voter et que cette personne est un électeur de la liste.

b. Personne ne peut voter plus d'une fois

→ Respecté

Comme précisé ci-dessus , la validité de l'électeur est contrôlée par le premier tiers de confiance au moment du vote ; un des contrôles est l'assurance que l'électeur n'a pas déjà voté.

c. Le vote d'un électeur doit être secret

→ Respecté

L'organisateur reçoit le vote de façon anonyme ; il connaît juste le lien qui lie le vote à l'identifiant donné par le second tiers de confiance. Le second tiers de confiance ne connaît pas l'identité de l'électeur, puisque le premier tiers lui a transmis le vote de manière anonyme ; il connaît seulement un identifiant qui lui a été transmis par le premier tiers ; cet identifiant est le lien qui lui permet le relier à l'électeur. Il faut toutefois supposer qu'il n'y a pas collusion entre les deux tiers de confiance, sans quoi il n'y a plus aucun secret.

d. Toute modification d'un vote doit être décelée

→ Respecté

Les identifiants placés par l'électeur et par les tiers de confiance peuvent permettre de retracer le cheminement complet du vote. Pour cela, il faut que les différents protagonistes donnent chacun un morceau du puzzle. Puisqu'il est possible de recréer le chemin d'un vote au départ d'un électeur, il peut être possible de créer une procédure qui permettrait à tout électeur de vérifier la validité de son vote (une procédure doit être mise en place afin de permettre, a posteriori, à un électeur de consulter son vote ; les modalités de cette consultation doivent permettre de conserver le secret du vote), il n'est donc pas possible de le modifier sans avoir le risque d'être découvert. De plus, le nombre de personnes comptabilisées par le premier tiers comme ayant voté ($\{Participants\}$) doit correspondre au nombre de votes comptabilisés par le second tiers ($\{Votes\}$) ainsi qu'à ceux comptabilisés par l'organisateur ($\{Résultat\}$).

e. Tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final

→ Respecté

Pour la même raison que ci-dessus, puisque chaque électeur a la possibilité de consulter son vote, il peut donc être certain que son vote est pris en compte. Comme tous les électeurs sont dans ce cas, la liste complète est donc valide et le résultat de l'élection peut être facilement contrôlé.

f. Il est possible de savoir qui a voté ou non

→ Respecté

Lors du transit du vote, le premier tiers de confiance prend note de l'électeur qui vient de voter. A l'issue du scrutin, il est donc possible de déterminer dans la liste des électeurs ceux qui ont voté et ceux qui ne l'auront pas fait. Ceci permet une vérification croisée supplémentaire : le nombre d'électeurs et le nombre de votes devra être exactement le même.

c) Conclusions

Le fait d'avoir placé deux tiers de confiance comme intermédiaires entre l'organisateur et le votant cache donc complètement le lien qui relie le votant à son vote, sans pour autant le briser. Il n'y a donc plus de lient direct, mais il subsiste un lien indirect. Il est toujours possible de reconstruire complètement l'élection à partir des données que se partagent les différents protagonistes, alors qu'aucun d'eux n'est capable à lui seul d'effectuer cette opération. Le votant est aussi mis au courant de la prise en compte de son vote au moyen d'accusés de réception en cascade à partir de l'organisateur. Ce protocole respecte les 6 critères de sécurité du vote sur Internet, et la distribution des identifiants par le premier tiers de confiance l'a rendu plus simple, sans pour cela nuire à la sécurité.

Le contrôle de la validité d'un vote, grâce aux identifiants qui ont été créés, est possible dans les deux sens : au départ de l'organisateur, l'identifiant $Ident_3$, s'il est présenté à T_2, permettra d'obtenir $Ident_2$, ainsi que le vote chiffré tel que T_2 l'a reçu

de T_1 ; si $Ident_2$ est présenté à T_1, celui-ci est capable de fournir le nom du votant, ainsi que son vote chiffré **et signé**, ce qui est la preuve que le vote est bien celui du votant, car lui seul est capable d'apposer sa signature électronique. Donc, au départ du vote, il est possible, grâce aux informations que possèdent T_1 et T_2, de trouver de manière indiscutable qui est le votant qui a placé ce vote.

De la même manière, tout votant peut retrouver le cheminement de son vote au travers du protocole. Si un votant soumet à T_1 l'identifiant qui lui a été envoyé, T_1 est capable de fournir l'identité du votant à qui il a été octroyé, ainsi que le vote chiffré et signé qu'il lui a envoyé ; il prouve par ce fait que l'identifiant n'a été distribué qu'à une seule personne, et que cette personne est le votant qui effectue la demande ; il peut aussi fournir l'identifiant qu'il a transmis à T_2, lequel permettra d'interroger celui-ci. T_2, grâce à cet identifiant, peut retrouver le vote de A, ainsi que l'identifiant qu'il a transmis en même temps à l'organisateur. Ces informations doivent concorder avec les informations qui ont été publiées par l'organisateur à l'issue de l'élection.

Conclusion

Après un long chemin, protocole après protocole, nous sommes parvenus à obtenir un protocole qui respecte ce que nous nous étions fixés comme critères minimaux pour une élection sécurisée sur Internet.

Le dernier des protocoles a même des atouts supplémentaires : grâce aux accusés de réception en cascade, le vote est devenu interactif, et, lorsque l'électeur reçoit son accusé de réception, il est certain que son vote est arrivé à bon port.

Un point plus délicat serait celui de la preuve ; comment prouver à un électeur que son vote est comptabilisé, sans pour cela lever le secret du vote, donc sans permettre à une personne que le votant lui-même de vérifier que son vote est comptabilisé ?

Un système pourrait être un « isoloir électronique », dans lequel un votant pourrait pénétrer, afin d'effectuer une demande de preuve. Quelles demandes du votant peuvent-elles être satisfaites ?

- A partir de son identifiant ($Ident_1$) ou de son identité (A), le premier tiers de confiance pourrait donner à l'électeur un second identifiant ($Ident_2$) lui permettant d'effectuer des demandes auprès du second tiers de confiance.
- A partir de l'identifiant ainsi obtenu ($Ident_2$), le second tiers de confiance pourrait prouver à l'électeur que son vote est correctement arrivé (en lui renvoyant son vote en clair).
- A partir de ce même identifiant ($Ident_2$), le second tiers de confiance peut fournir au votant l'identifiant avec lequel son vote a été enregistré dans la liste des résultats ($Ident_3$).
- Grâce à ce troisième identifiant ($Ident_3$), le votant est à même de retrouver son vote dans la liste des résultats.

Ces différentes demandes pourraient faire l'objet d'une procédure en cascade, donnant toutes les informations et effectuant toutes les démarches en une seule étape.

Le fait que cette demande se fasse sur une machine protégée dans un milieu fermé où le votant est seul garantit le secret ; en effet, lorsqu'il sort de cet « isoloir électronique », il n'a rien de plus qu'avant, hormis la certitude que son vote a été pris en compte.

Tout serait pour le mieux dans le meilleur des mondes, s'il n'y avait un petit hic : s'il est vrai que, sur papier, le protocole défini semble sans gros défaut, il n'en n'est plus de même lorsque l'on envisage une implémentation de celui-ci dans le monde réel. En effet, pour que le protocole puisse fonctionner, il faut la participation de deux tiers de confiance.

C'est justement à ce niveau que le bât blesse :

- ces deux tiers de confiance ne peuvent pas se connaître (il y aurait, s'ils se connaissaient, un risque évident de collusion)
- ces deux tiers de confiance ne peuvent pas travailler l'un sans l'autre ; de plus, il doivent travailler simultanément.

Nous nous trouvons donc ici devant une situation assez cornélienne ; où sera-t-il possible de trouver des sociétés qui, en aucune manière, ne peuvent avoir la mainmise sur le service qu'elles exploitent, et qui, en plus, sont dépendantes d'une autre société, dans la même situation qu'elle, et avec laquelle elle n'est pas en relation.

Une ébauche de solution à ce problème serait peut-être d'obliger toute société voulant s'impliquer dans une telle entreprise, d'être en mesure d'offrir les deux types de service. L'organisateur d'une élection sélectionnerait deux entreprises pour l'exécution de l'opération, et choisirait aussi le rôle que chacune d'elles y jouerait.

L'arrivée d'Internet dans nos procédures électorales n'est, à notre avis, qu'une question de temps. Les années qui suivent ont encore leur part de mystère qui ne se découvrira qu'en allant de l'avant. Quel type de protocole sera utilisé ? Peut-être légèrement similaire à celui que nous proposons ? Sait-on jamais.

Références

[*ANDOS*]

Applied cryptography by Bruce schneier

[*Arizona 2000*]

Rapports et études : Dossier e-vote : Expérience en Amérique du Nord : les Etats-Unis : http://www.democratie-electronique.org/rens_voteel/ue_gen/an/am.htm

[*Choose*]

Cybervote chapter 3 Online voting systems : http://www.eucybervote.org/Reports/KUL-WP2-D4V1-v1.0-02.htm

[*eGovernment News – 20 December 2004*]

EUROPA - IDABC - E-voting security solution wins European IST Prize : http://europa.eu.int/idabc/en/document/3688/5718

[Election.com]

Accenture eDemocracy Services : http://www.accenture.com/xd/xd.asp?it=enweb&xd=industries\government\gove_democ.xml

[*E-Poll*]

E-Poll Electronic polling system for remote voting operations : http://www.e-poll-project.net/

[*EU-StudentVote*]

World student
http://www.eu-studentvote.org
http://www.worldstudent.com/mag/temoignages/studentvote.shtml

[*Forum Mondial lDémocratie*]

Bienvenue sur le site d'Issy-les-Moulineaux - Forum Mondial eDemocratie
http://www.issy.com/Rub.cfm?Esp=1&Rub=42

[*Irlande*]

Commission on Electronic Voting – Reports : http://www.cev.ie/htm/report/index.htm

Les machines à voter Nedap Powervote mises à l'index en Irlande : http://padawan.info/fr/politique/les_machines_a_voter_nedap_powervote_mises_a_lindex_en_irlande.html

[*iSOCO*]

Providing Security to Electronic Elections : http://e-voto.di.fc.ul.pt/docs/e-voting.pdf

[*IST*]

The European IST Prize : http://www.ist-prize.org/

[*Ivan Font*]

voir mail en annexe

[*John Seibel*]

Voir mail en annexe

[*Mercuri*]

Electronic voting : http://www.notablesoftware.com/evote.html

TechTV | Can the Swedes Swing the Net Vote?
http://www.notablesoftware.com/Press/TechTV.html

Testimony by Rebecca Mercuri, Ph.D.
Presented to the U.S. House of Representatives Committee on Science
http://www.house.gov/science/full/may22/mercuri.htm

[*NEDAP*]

NEDAP Specials/Voting systems :
http://www.nedapspecials.com/ms/website.nsf/46f5b44c63a393f8c12564960027438 9/a004506355e920d4c12565b4002aa855

[PourEVA]

Pour une Ethique du Vote Automatisé (Vote Electronique) : http://www.poureva.be

[*Revue Web*]

Revue de Web sur le vote électronique :
www.minefi.gouv.fr/minefi/ministere/documentation/revuesdeweb/vote.htm

[*Scytl.com*]

Scytl : Secure electronic voting : http://www.scytl.com

[*SafeVote.com*]

SafeVote – Products : http://www.safevote.com/products.htm

[*The Bell*]

The Bell -- Newsletter on Internet Voting : http://www.thebell.net

[*TrueBallot*]

TrueBallot WebVote® : http://www.trueballot.com/WebVOTE.htm

[*VoteHere.net*]

VoteHere, Inc. : http://www.votehere.net/vhti.php

Table des figures

Annexes

----- Original Message -----

From: Ivan Font

To: 'Francis Jeanmoye'

Sent: Wednesday, May 18, 2005 9:20 AM

Subject: RE: Electronic voting information.

Dear Francis,

In a digital envelope, symmetric and public key methods can be combined as follows:

- A random key (called a /session/ key) is generated.

– The message is encrypted using a symmetric algorithm, with this key.

– A small message containing the key is created, and encrypted this using a public key algorithm, with your public key.

– This small message is sent along with the longer encrypted message.

Note that because of the randomness of the session key, there is no possibility of knowing the contents of the encrypted ballot.

Hope this helps

Best regards,

Ivan Font
Marketing Dept.
email: ivan.font@scytl.com
phone: +34 934 230 324
fax: +34 933 251 028

Scytl Secure Electronic Voting
Entença, 95, 4-1
08015 Barcelona, Spain
http://www.scytl.com

NOTICE: The information in this e-mail and in any of its attachments is confidential and intended solely for the attention and use of the named addressee(s). If you are not the intended recipient, any disclosure, copying, distribution or retaining of this message or any part of it, without the prior written consent of Scytl Secure Electronic Voting is prohibited and may be unlawful. If you have received this in error, please contact the sender and delete the material from any computer.

From: Francis Jeanmoye [mailto:francis.jeanmoye@swing.be]
Sent: martes, 17 de mayo de 2005 17:07

To: Ivan Font
Subject: Re: Electronic voting information.

Dear Ivan,

I already read the information on your web site, but there is still a question I could not find an answer to :

It is said on your site that the ballots are "placed into a digital envelope", in other words, encrypted using the public part of a key pair.

Am I right or not if I tell the following :

- Two voters, A and B, select the same candidate on their Ballot.
- This means that the ballot from voter A is the same as the ballot from voter B
- this means that the encrypted ballot from voter A is the same as the encrypted ballot from voter B, as they are encrypted using the same public key.
- If user C creates one encrypted ballot for each voting possibility, it will be the possible for him, by comparing an encrypted ballot with the ones he has, to exactly know the contents of this encrypted ballot.

If this is not so, could you please tell me where I am wrong.

Thanks beforehand for your answer.

Francis Jeanmoye

----- Original Message -----

From: Ivan Font

To: 'Francis Jeanmoye'

Sent: Tuesday, May 17, 2005 4:49 PM

Subject: RE: Electronic voting information.

Dear Francis,

Most information regarding how our systems works is published in our web. Under the section Science or under our News.

However, if you require a more specific information I will be happy to answer you again.

Kind regards,

Ivan Font
Marketing Dept.
email: ivan.font@scytl.com
phone: +34 934 230 324
fax: +34 933 251 028

Scytl Secure Electronic Voting
Entença, 95, 4-1
08015 Barcelona, Spain
http://www.scytl.com

NOTICE: The information in this e-mail and in any of its attachments is confidential and intended solely for the attention and use of the named addressee(s). If you are not the intended recipient, any disclosure, copying, distribution or retaining of this message or any part of it, without the prior written consent of Scytl Secure Electronic Voting is prohibited and may be unlawful. If you have received this in error, please contact the sender and delete the material from any computer.

From: Francis Jeanmoye [mailto:francis.jeanmoye@swing.be]
Sent: lunes, 16 de mayo de 2005 17:08
To: info@scytl.com
Subject: Electronic voting information.

Dear sir,

For the end of my univerity studies, I am writing an essay which title is "Security and internet voting". I read some articles about your Pnyx products and would be very interrested about more info concerning the cryptographic system used in it.

All the info I could receive should be very apreciated.

Thanks beforehand.

Francis Jeanmoye

Student at FUNDP in Namur, Belgium.

De: Ivan Font <ivan.font@scytl.com>
À: Francis Jeanmoye <francis.jeanmoye@swing.be>
Objet: RE: Electronic voting information.
Date: mercredi 18 mai 2005 9:19

Dear Francis,

In a digital envelope, symmetric and public key methods can be combined as follows:

- A random key (called a /session/ key) is generated.

– The message is encrypted using a symmetric algorithm, with this key.

– A small message containing the key is created, and encrypted this using a public key algorithm, with your public key.

– This small message is sent along with the longer encrypted message.

Note that because of the randomness of the session key, there is no possibility of knowing the contents of the encrypted ballot.

Hope this helps

Best regards,

Ivan Font
Marketing Dept.
email: <mailto:ivan.font@scytl.com> ivan.font@scytl.com
phone: +34 934 230 324
fax: +34 933 251 028

Scytl Secure Electronic Voting
Entença, 95, 4-1
08015 Barcelona, Spain
<http://www.scytl.com/> http://www.scytl.com

NOTICE: The information in this e-mail and in any of its attachments is confidential and intended solely for the attention and use of the named addressee(s). If you are not the intended recipient, any disclosure, copying, distribution or retaining of this message or any part of it, without the prior written consent of Scytl Secure Electronic Voting is prohibited and may be unlawful. If you have received this in error, please contact the sender and delete the material from any computer.

From: Francis Jeanmoye [mailto:francis.jeanmoye@swing.be]
Sent: martes, 17 de mayo de 2005 17:07
To: Ivan Font
Subject: Re: Electronic voting information.

Dear Ivan,

I already read the information on your web site, but there is still a question I could not find an answer to :

It is said on your site that the ballots are "placed into a digital envelope", in other words, encrypted using the public part of a key pair.

Am I right or not if I tell the following :
- Two voters, A and B, select the same candidate on their Ballot.
- This means that the ballot from voter A is the same as the ballot from voter B
- this means that the encrypted ballot from voter A is the same as the encrypted ballot from voter B, as they are encrypted using the same public

key.
- If user C creates one encrypted ballot for each voting possibility, it will be the possible for him, by comparing an encrypted ballot with the ones he has, to exactly know the contents of this encrypted ballot.

If this is not so, could you please tell me where I am wrong.

Thanks beforehand for your answer.

Francis Jeanmoye

----- Original Message -----

From: John Seibel

To: Francis Jeanmoye

Sent: Monday, May 16, 2005 9:09 PM

Subject: RE: Electronic voting information

It depends on what configuration we are running.

He/she is registered against the voter list as having voted. Sometimes we send a confirmation, but not with the vote on it.

You are discovering the limitations of any fully electronic system.

TrueBallot, Inc
John Seibel, President
http://www.trueballot.com
Tel. 301 656-9500

-----Original Message-----
From: Francis Jeanmoye [mailto:francis.jeanmoye@swing.be]
Sent: Monday, May 16, 2005 2:56 PM
To: john@trueballot.com
Subject: Re: Electronic voting information

- How is it possible then to prove to a voter that his vote was taken in account ?

- Does the voter receive a receipt ?

----- Original Message -----

From: John Seibel

To: Francis Jeanmoye

Sent: Monday, May 16, 2005 8:51 PM

Subject: RE: Electronic voting information

In our system, they are never bound.

TrueBallot, Inc
John Seibel, President
http://www.trueballot.com
Tel. 301 656-9500

-----Original Message-----
From: Francis Jeanmoye [mailto:francis.jeanmoye@swing.be]
Sent: Monday, May 16, 2005 2:28 PM
To: john@trueballot.com
Subject: Re: Electronic voting information

Hi John,

My focus point is the protocol itself; the information I would like to receive is the way used to unbind the voter and his vote, and who the vote is protected against external attacks while travelling on the Internet (DES or other cryptographic system?)

Thanks for your quick answer.

Francis

----- Original Message -----

From: John Seibel

To: Francis Jeanmoye

Sent: Monday, May 16, 2005 7:51 PM

Subject: RE: Electronic voting information

Francis:

Thanks for your inquiry. I'm not sure how to answer your inquiry. Security in Internet voting comes from different places.

There is the session security (SSL encryption)

there is voter authentication (how you know the voter is entitled to vote)

there is the vote and voter data security (how and where they are stored, and what method is used to access it)

The kind of cryptographic system to which you may be referring is a system where the vote and the identity of the voter are stored together but are separated by a cryptographic key. We don't, for a number of policy reasons, use that system. We find that it is so complicated that we can't adequately explain it to less sophisticated people, and because it does not fit our model of how elections /voting works.

TrueBallot, Inc
John Seibel, President

http://www.trueballot.com
Tel. 301 656-9500

-----Original Message-----
From: Francis Jeanmoye [mailto:francis.jeanmoye@swing.be]
Sent: Monday, May 16, 2005 12:01 PM
To: john@trueballot.com
Subject: Electronic voting information

Dear sir,

For the end of my univerity studies, I am writing an essay which title is "Security and internet voting". I read some articles about WebVote and would be very interrested about more info concerning the cryptographic system and the security used in it.

All the info I could receive should be very apreciated.

Thanks beforehand.

Francis Jeanmoye

Student at FUNDP in Namur, Belgium.