I-Vote: Un système de vote électronique hautement sécurisé

S. Benmeziane[1] & L. Khelladi[2]

1: Laboratoire des Logiciels de Base, CERIST,
3 Rue des Frères Aissou Ben Aknoun, Alger
sbenmeziane@mail.cerist.dz
2: Laboratoire des Logiciels de Base, CERIST,
3 Rue des Frères Aissou Ben Aknoun, Alger
lkhelladi@mail.cerist.dz

Résumé

Nous présentons dans cet article la conception et l'implémentation de i-vote, un prototype de système de vote électronique sur Internet. Le prototype implémenté encapsule un protocole de vote reposant sur l'utilisation d'outils de cryptographie avancées pour assurer l'intégrité et la confidentialité du vote d'une part, l'authentification et l'anonymat des électeurs d'autre part.

Basé sur les travaux de Fujioka, Okamoto et Ohta et du protocole Sensus, i-vote applique la technique de signature en aveugle au bulletin du votant. Ainsi, il est impossible de tracer le bulletin de vote pour savoir le votant associé, par conséquent le système garantit l'anonymat du votant.

Mots clés : vote, anonymat, vérifiabilité, signature en aveugle.

1. Introduction

L'interconnexion des réseaux et l'expansion rapide du Web ont permis le développement d'un grand nombre d'applications que l'utilisateur peut exécuter à distance sans se déplacer physiquement. L'une des applications qui devrait profiter actuellement de ces avancées technologiques est le vote. En effet, les élections et les référendums traditionnels nécessitent le déplacement de tous les participants au vote or, il est difficile de convaincre tout le monde de faire le déplacement alors qu'il serait si facile de voter de chez soi, de façon électronique. Les avantages seraient multiples : un plus grand nombre de participants grâce à l'aisance de cette opération impliquée par le non-déplacement et la simplicité du processus, le dépouillement automatisé et donc plus rapide, le coût d'organisation réduit à cause de l'élimination des dépenses associées à l'établissement des bureaux de vote et le personnel qu'ils requièrent, etc. Néanmoins, la réalisation d'un système de vote électronique n'est pas une tâche facile, car le vote électronique pose un double problème qui est celui de l'anonymat et la confidentialité [1].

En effet, une telle procédure nécessite la satisfaction d'au moins deux propriétés essentielles :

La vérifiabilité : chacun doit être en mesure de vérifier la validité du scrutin, et

L'anonymat : ou chacun veut conserver le secret de son vote.

Ces deux propriétés semblent contradictoires, car pour vérifier le résultat du scrutin, il faut voir toutes les étapes de calcul. Dans cet article, nous allons présenter une solution à ce problème qui consiste à utiliser la cryptographie et notamment la technique de signature en aveugle pour garantir l'anonymat du votant. Le but de ce travail [9] consiste donc, à concevoir et réaliser un système de vote électronique qui nécessite la définition d'un protocole de vote satisfaisant les deux propriétés précitées d'une part, et permettant un scrutin à candidats multiples d'autre part (la plus part des protocoles se limitent à la situation de référendum avec seulement une alternative oui/non). Le système mis en oeuvre, qui ne sera pas destiné aux élections à grande échelle de participation, est implémenté dans un environnement Internet via une interface Web en utilisant le langage Java.

Dans cet article, nous présentons la conception et l'implémentation du prototype i-vote. Pour cela, nous décrirons, dans la section 2, les propriétés du vote électronique en insistant sur les exigences de sécurité. Dans la section 3, nous présenterons une synthèse des protocoles de vote existants. Puis, nous consacrerons la section 4 à la description du protocole de vote adopté. Dans la section 5, nous étudierons la mise en oeuvre du système de vote. Enfin, nous finirons par une conclusion où nous évaluerons notre prototype et proposerons les éventuelles extensions.

2. Le vote électronique : définition et propriétés

Le vote électronique est un exemple d'application distribuée qui permet aux élections d'avoir lieu sur des réseaux informatiques ouverts [4]. Dans cette application un ensemble de votants envoie leurs bulletins à travers le réseau à un centre de dépouillement virtuel responsable de la réception, validation, et classification des bulletins.

D'une manière générale, les participants impliqués dans une élection électronique sont un collectif d'électeurs et un ensemble d'autorités de vote. Le nombre et l'utilité de ces autorités sont variables, ils dépendent du schéma de vote considéré [4].

Le scénario d'une élection électronique peut être divisé en trois phases :

Phase d'enregistrement : Durant cette première étape, l'autorité de vote crée la liste électorale de toutes les personnes éligibles qui sont enregistrées pour cette opération de vote et la publie à travers le réseau.

Phase de vote : Cette phase permet aux votants d'envoyer leurs bulletins de vote en utilisant les facilités de communication offertes par le réseau.

Phase de décompte : A la fin de la phase de vote, l'autorité arrête la réception des bulletins, et le processus de décompte des résultats est déclenché. Finalement, les résultats sont publiés et mis à la disposition des votants à travers le réseau.

L'application du vote étant destinée à être exécutée sur le réseau, un bon système de vote électronique doit assurer quelques propriétés qui définissent des exigences concernant sa sécurité et son implémentation [2, 3]. Dans ce qui suit, nous allons définir les exigences de sécurité dont nous tiendrons compte lors de la conception du système.

Précision : Une élection est précise si elle vérifie les exigences suivantes :
- Un vote ne doit pas être altéré, par conséquent les résultats du vote ne doivent pas être modifiés en ajoutant des votes invalides ou en changeant le contenu des bulletins par exemple (intégrité).
- Un vote valide doit être compté.
- Un vote invalide ne doit pas être compté.

Démocratie : Cette propriété est assurée si :
- Seuls les votants éligibles peuvent voter.
- Chaque votant ne peut voter qu'une seule fois. La propriété de démocratie est généralement liée à l'intégrité de la liste électorale (liste des votants éligibles). Pour cela, quelques mécanismes supplémentaires doivent être ajoutés pour empêcher l'administrateur de cette liste de casser cette propriété.

Confidentialité : Nous qualifions de vote confidentiel, un vote dans lequel :
- ni l'autorité du vote ni personne d'autre ne doit pouvoir faire le lien entre un votant et son vote (anonymat) : l'anonymat constitue probablement la pierre angulaire de tout système de vote électronique [11].
- aucun votant ne peut prouver qu'il a voté dans un chemin particulier : ce dernier facteur de confidentialité est aussi important pour la prévention contre l'achat du vote, en effet les électeurs

ne peuvent vendre leurs votes que s'ils sont capables de prouver à l'acheteur qu'ils ont réellement voté d'après leurs vœux.

Vérifiabilité : Il existe deux définitions de cette propriété, la vérifiabilité universelle et la vérifiabilité individuelle. Un système de vote est universellement vérifiable si toute personne peut indépendamment vérifier que tous les bulletins ont été comptés correctement. Un système de vote est individuellement vérifiable (définition plus faible) si chaque votant peut indépendamment vérifier que son propre bulletin a été correctement compté [12].

Avant d'expliquer le schéma de vote proposé et comment celui-ci va essayer de remplir les exigences de sécurité citées auparavant, nous allons brièvement présenter les principaux types de protocoles de vote décrits dans la littérature.

3. Synthèse et critiques des protocoles de vote électroniques

Les premiers protocoles de vote électronique n'utilisent pas de techniques cryptographiques. Ces protocoles sont basés généralement sur deux autorités de vote : la première est utilisée pour l'authentification des votants enregistrés, et la deuxième chargée de la collection des bulletins et le décompte des résultats. Malgré leur simplicité, ces protocoles présentent des inconvénients majeurs. En effet, ils ne répondent pas à la majorité des propriétés citées précédemment [8].

Dès lors, des protocoles utilisant les mécanismes cryptographiques ont été proposés. Ces derniers introduisent le chiffrement pour assurer la confidentialité du vote, et la signature numérique pour assurer l'authentification des votants et garantir ainsi qu'ils ne peuvent voter plus d'une fois.

Pour garantir l'anonymat des votants, certains de ces protocoles se sont basés sur l'utilisation de deux autorités pour séparer les deux tâches d'authentification du votant et le décompte de son bulletin. Cependant le problème d'anonymat s'est toujours posé à cause du risque de collusion existant entre les deux autorités pouvant ainsi déterminer qui a voté pour qui [8].

Par conséquent, et afin de dissocier complètement le votant de son vote, la technique de signature en aveugle introduite par David Chaum en 1982 a été utilisée [7]. Cette technique permet à l'autorité chargée de l'authentification des votants de signer leurs bulletins sans avoir la moindre idée sur le contenu. De cette manière, le risque de collusion entre les deux autorités est éliminé : la première n'ayant aucune information sur les bulletins qu'elle a validé. Ceci est similaire au fait de placer un document avec une feuille de papier Carbonne dans une enveloppe. Si quelqu'un signe cette dernière, le document sera signé aussi, la signature reste alors attachée au document même s'il est retiré de l'enveloppe. Parmi les protocoles de vote basés sur la signature en aveugle, nous distinguons les travaux de Fujioka, Okamoto et Ohta qui ont défini un protocole de vote utilisant deux autorités centrales et est à la base du protocole Sensus décrit dans [8].

4. Proposition d'un protocole de vote électronique

Afin de mettre en oeuvre notre système, nous avons choisi d'adopter le protocole Sensus. Notre choix est dû essentiellement au fait que ce protocole assure le maximum de propriétés désirées, et particulièrement les deux propriétés exigées préalablement : l'anonymat et la vérifiabilité. De plus, par rapport au protocole de Fujioka, Okamoto et Ohta, Sensus permet de réaliser une opération de vote en une seule session [8].

4.1. Scénario du protocole Sensus :

Notons que Sensus est un protocole qui utilise deux autorités centrales :

– Une autorité centrale de légitimation (ACL) qui est responsable de l'authentification des votants et la validation de leurs bulletins.

– Une autorité centrale de décompte (ACD) qui prend en charge la collection des bulletins et le dépouillement des votes.

Le protocole suit les étapes suivantes :

1. Le votant prépare le bulletin qui contiendra son vote.
2. Le votant chiffre son bulletin avec une clef secrète.
3. Le votant utilise une fonction de hachage pour avoir un condensat de son bulletin crypté.
4. Il camoufle le condensat en utilisant un facteur de camouflage aléatoire pour permettre la signature en aveugle à l'ACL [7].
5. Le votant signe le condensat camouflé avec sa clef de signature privée.
6. Il envoie le message résultant à l'ACL.
7. L'ACL vérifie la signature du votant avec la clef publique de ce dernier.
8. L'ACL vérifie que le votant n'a pas encore soumis un bulletin pour validation.
9. Si le votant est légitime et n'a pas validé un bulletin de vote précédemment, l'ACL lui valide son bulletin en le signant en aveugle avec sa clef privé.
10. L'ACL mentionne que le votant a déjà validé son bulletin de vote, et retourne par la suite ce bulletin au votant.
11. Le votant enlève le facteur de camouflage retrouvant ainsi son bulletin original crypté, haché et signé par l'ACL.
12. Le votant envoie à l'ACD le bulletin résultant de l'étape précédente, ainsi qu'une copie du vote chiffré produit lors de la deuxième étape.
13. L'ACD vérifie la signature sur le bulletin signé par l'ACL.
14. L'ACD utilise la même fonction de hachage employé au début par le votant pour calculer un condensat du vote chiffré reçu à l'étape n°12 et le comparer par la suite avec le message résultant de l'étape n°11.
15. Si l'ACD constate que la signature de l'ACL est valide et le bulletin n'a pas été modifié durant les étapes précédentes, elle le place dans la liste des bulletins valides pour les publier à la fin du vote.
16. L'ACD signe le bulletin avec sa clef privée, et elle le retourne au votant comme accusé de réception.
17. Apres avoir reçu l'accusé de réception, le votant envoie la clef secrète de déchiffrement à l'ACD.
18. A ce moment, l'ACD utilise cette clef privée pour déchiffrer le bulletin et ajoute le vote au décompte.

Dans ce protocole, et pour assurer la confidentialité du vote, le votant utilise le chiffrement symétrique [4] avec une clef secrète. Par conséquent, aucune entité ne peut savoir le contenu du bulletin de vote sauf le votant et l'ACD après avoir reçu la clef secrète de déchiffrement du votant.

La signature numérique est utilisée à plusieurs reprises afin de permettre l'authentification des différentes entités participant au vote (votant, ACL,ACD,...). De ce fait, aucun intrus ne peut se manifester comme étant l'une des ces entités.

Ce protocole utilise également la technique de signature en aveugle pour s'assurer que le validateur (ACL) n'ait aucune information sur les bulletins qu'il signe, et éviter le risque de collusion entre l'ACL et l'ACD et la corrélation de leurs bases de données, garantissant ainsi l'anonymat du vote. L'introduction de la notion d'accusé de réception constitue la différence principale remarquée entre le protocole de Fujioka, Okamoto et Ohta et celui de Sensus. Ce dernier n'exige pas au votant d'attendre jusqu'à la fin de la phase d'envoi des bulletins de vote pour donner sa clef de déchiffrement à l'ACD, mais il utilise l'accusé de réception pour permettre au votant de vérifier que son bulletin a été reçu correctement par l'ACD et d'envoyer juste après la clef de déchiffrement, ce qui termine l'opération du vote en une seule session et la rend plus rapide.

5. Schéma du processus de vote

Le protocole de vote que nous avons adopté dans la section précédente constitue la plate-forme sur laquelle est bâtie l'architecture de i-vote. Nous allons — dans ce qui suit — expliquer le schéma de vote en détaillant les échanges de messages entre les différentes autorités impliquées dans les différentes phases du processus de vote.

5.1. Phase d'inscription des votants

Cette phase précède l'opération de vote proprement dite, et consiste en l'établissement et la publication de la liste des votants éligibles qui désirent participer à l'opération de vote organisée. Pour cela, l'autorité chargée de cette opération doit disposer auparavant d'une liste des personnes autorisées à s'inscrire (liste de population).

L'introduction de cette phase dans notre système de vote s'est imposée à cause de deux facteurs :

1. Pour renforcer la propriété de mobilité dans notre système, aucun contact au préalable n'est exigé entre le votant et l'organisme de vote (dans le cadre de l'opération d'élection). Par conséquent, cette phase doit assurer l'authentification des votants à l'aide des informations disponibles chez le votant tel qu'un numéro d'identification et un mot de passe, ces informations peuvent être délivrés au votant dès son appartenance a l'institution qui organise le vote, par exemple, les membres d'une société peuvent les recevoir par courrier après qu'ils se joignent à la société.
2. L'étape d'inscription permet également de connaître le nombre de votants abstenant et donc de diminuer la possibilité qu'a l'autorité chargée de l'inscription d'envoyer des votes frauduleux à leur place.

La difficulté principale qui s'impose lors de la mise en œuvre de cette phase est la manière d'authentifier les personnes autorisées à s'inscrire et qui figurent dans la liste de population. Afin d'assurer ce service important, nous avons choisi d'utiliser le mécanisme d'authentification *challenge-response* [5] pour les raisons suivantes :

– *challenge-response* est un mécanisme d'authentification basé sur l'utilisation d'un mécanisme de mots de passe renforcé. Les mécanismes de signatures basés sur les clefs ne pouvant pas être utilisé car ces clefs n'étant pas disponibles avant l'organisation de l'opération de vote.
– *challenge-response* fait face aux importantes attaques qui peuvent survenir lors d'une session d'authentification, notamment l'attaque de rejeu [5], et ceci avec un nombre minimum de contraintes (de synchronisation par exemple), et un degré de complexité acceptable et possible à implémenter.

Pour accomplir l'étape d'inscription, chaque votant authentifié à l'aide de son mot de passe et de son numéro d'identification génère une paire de clef privée/clef publique, et envoie la clef publique à l'autorité d'inscription pour être utilisée dans la vérification de sa signature au moment des phases ultérieures du vote.

5.2. Phase de vote

Cette phase comprend deux étapes essentielles :

L'étape de validation du bulletin de vote qui comporte le chiffrement symétrique, le hachage, le camouflage et la signature du vote pour son envoi à l'autorité chargée de sa validation (signature en aveugle). Cette dernière retourne le vote validé au votant. Les messages échangés sont illustrées dans la figure 1.

L'étape de collection durant cette étape le votant commence par enlever le facteur de camouflage au bulletin validé. Ce bulletin doit être envoyé à l'autorité de collection qui doit vérifier sa validité et son intégrité avant de le déchiffrer avec la clef secrète du votant reçue via un canal sécurisé (figure 2).

5.3. Phase de décompte

C'est la dernière phase du processus de vote et comporte le déchiffrement du vote et son stockage avec la clef de déchiffrement correspondante dans la base de donnée consacrée à cette fin. Dans cette phase (figure 3),

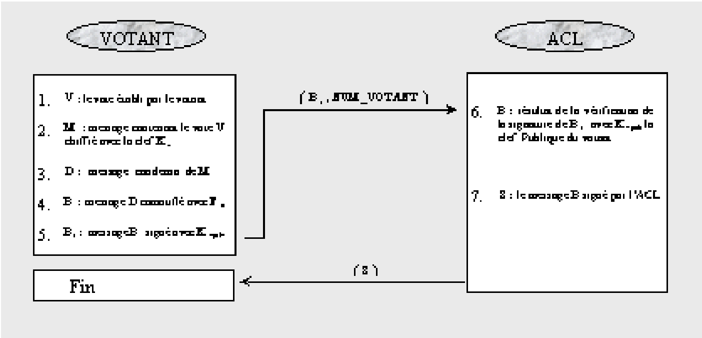

FIG. 1 – étape de validation

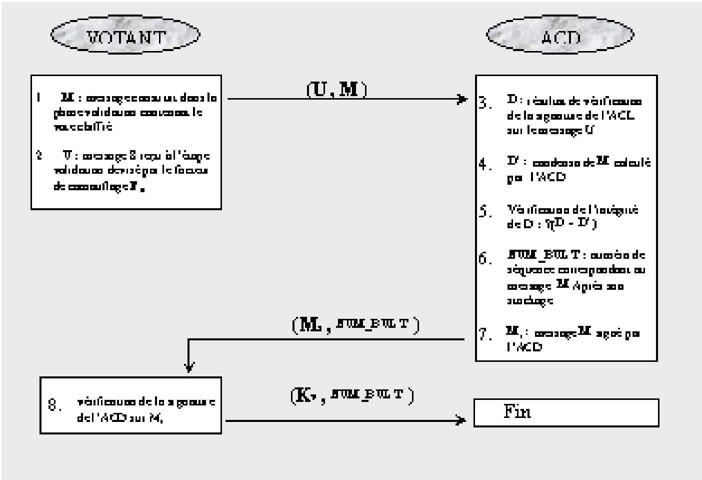

FIG. 2 – étape de collection

la même autorité qui a effectué la phase de collection compte le vote en clair et rend publique après la fin de l'élection une liste contenant tous les votes chiffrés reçus, leurs clefs de déchiffrement, et les votes déchiffrées correspondants, ainsi qu'une liste qui donne le résumé de résultats en montrant le nombre de voix qui ont voté pour chaque option (alternative) de vote.

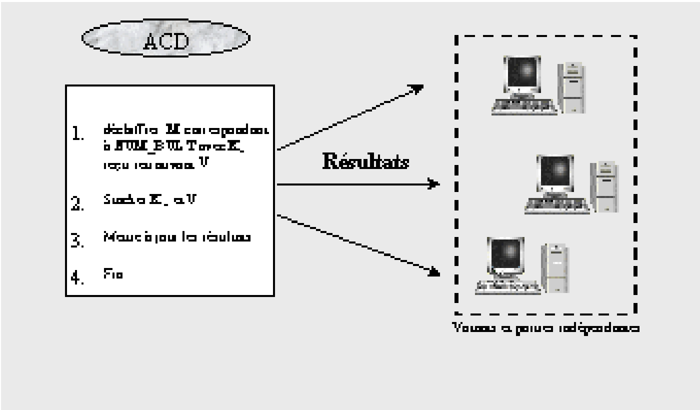

FIG. 3 – phase de décmopte

6. Implémentation

Afin d'implémenter le schéma décrit précédemment, nous avons utilisé l'environnement de développement *Java*, car il offre une solution qui permet l'intégration de programmes exécutables dans les pages Web. Ces programmes appelés *applets* sont utilisés dans notre système pour assurer l'inscription des votants, l'envoi des bulletins et la consultation des résultats, et peuvent s'exécuter sans compromettre la sécurité des système client [9]. De plus les *applets* peuvent communiquer avec des serveurs et exécuter des appels de procédures a distance (*RPC*) dans le contexte d'un mécanisme puissant purement Java appelé *RMI*(*Remote Methode Invocation*) [9].

Un autre facteur important qui argumente le choix de l'environnement Java est que ce langage inclut des librairies permettant la réalisation de toutes les fonctions cryptographiques de base nécessaires pour l'implémentation des deux protocoles d'inscription et de vote.

En effet, le paquetage `java.security` disponible dans le *JDK SUN* permet une multitude d'opérations dans ce domaine. Il contient des classes pour les algorithmes de signature numérique, tel que *DSA*, la génération des paires de clef publique/clef privée, les algorithmes de hachage comme *MD5* et un ensemble d'abstractions pour gérer les entités, leurs clefs et leurs certificats.

Nous avons également utilisé l'API `logi.crypto` [12] qui contient un ensemble de classes permettant des différentes fonctionnalités, entre autre l'utilisation simple et directe du mécanisme de signature en aveugle.

6.1. Les modules de système de vote

Pour mener une opération de vote, i-vote utilise quatre modules représentant respectivement le votant, l'ACL, l'ACD, en plus du module qui représente l'organisateur de l'élection et qui est chargé d'automatiser la phase d'inscription et la construction dynamique du bulletin de vote.

6.1.1. Le module Organisateur

Le module Organisateur est invoqué par l'administrateur de l'opération de vote. Ce dernier doit introduire un mot de passe afin de pouvoir l'exécuter.

En plus de la phase d'inscription des votants, le module Organisateur est responsable des préparations nécessaires au vote. Son rôle se résume essentiellement en :

- la construction du bulletin de vote : en utilisant *HMTL* comme langage de construction, l'administrateur du vote définit le modèle du bulletin de vote qui sera employé durant l'élection. Ce modèle dépend des spécificités que présente chaque opération de vote tel que son genre (élection, referendum, ...), le nombre de choix suggéré pour le vote, etc.
- le module Organisateur est également utilisé pour préparer la liste de population, déclencher et arrêter les différentes phases de l'élection organisée.

6.1.2. Le module ACL

Le module ACL est chargé de l'accomplissement de la phase de validation tout en garantissant qu'un seul bulletin sera validé pour chaque votant enregistré.

6.1.3. Le module ACD

Le module ACD est responsable de l'étape de collection des bulletins de vote et le décompte des résultats ainsi que leur publication.

6.1.4. Le module Votant

Ce module fonctionne comme étant un agent du votant. Il doit pouvoir :

- Présenter un bulletin de vote lisible au votant (utilisation d'une interface graphique ou textuelle).
- Prendre en charge les votes des électeurs.
- Exécuter toutes les opérations cryptographiques qui doivent être effectuées par le votant.
- Obtenir et recevoir les validations nécessaires et les accusés de réception.
- Délivrer le bulletin de vote aux différentes autorités (ACL, ACD).
- Vérifier les résultats du scrutin et éventuellement protester en cas d'erreur.

7. Évaluation et Conclusion

Dans cet article, nous avons présenté i-vote : un prototype de système de vote électronique sécurisé. Ce prototype encapsule un protocole de vote basé sur celui de Sensus. Tout au long de la conception et la mise en oeuvre du système, nous avons tenu à assurer les propriétés essentielles d'un bon système de vote électronique. Dans ce qui suit, nous pouvons évaluer notre système relativement à chaque propriété et proposer les extensions possibles :

Précision : Notre système de vote satisfait bien cette propriété. En effet, tout comportement de type modification, suppression ou ajout de votes est détectable en examinant la liste publiée par l'ACD à la fin des élections.

Démocratie : Cette propriété est complètement satisfaite si tous les électeurs inscrits soumettent leurs votes. Cependant, si les votants s'abstenant ne le font pas, il devient possible pour l'ACL de valider et soumettre des bulletins à leur place. L'introduction d'une autre autorité chargée de la vérification de la signature des votants pour toutes les demandes de validation peut résoudre ce genre de problème, mais le compte final ne peut être corrigé.

Confidentialité : En utilisant la technique de signature en aveugle, nous garantissons la propriété d'anonymat mais pas de manière complète. En effet, il faut assurer qu'un vote ne peut pas être lié à un votant particulier en traçant les paquets dans lesquels les messages sont transmis du votant à l'ACD, en plus, il faut garantir que les messages d'électeurs n'arriveront pas à l'ACL et l'ACD dans le même ordre des votants, sinon cela permettra aux deux autorités — après collusion — de pouvoir lier entre les électeurs et leurs votes. Pour atteindre l'anonymat complet, nous proposons l'utilisation des serveurs mixtes conçus par David Chaum [7]. Cependant, la prévention contre l'achat du vote n'est pas garantie.

Vérifiabilité : La propriété de vérifiabilité est également satisfaite. En effet, chaque électeur peut facilement, grâce à liste publiée par l'ACD, vérifier que son vote correspondant au numéro `NUM_BULT` qu'il a reçu dans la phase de vote a été compté correctement (vérifiabilité individuelle). La liste publiée par l'ACD contient également la clef de déchiffrement relative à chaque bulletin, cela permet à toute partie indépendante de vérifier la validité du résultat global de l'opération de vote, et de corriger les erreurs éventuelles, sans sacrifier la confidentialité des votes (vérifiabilité universelle).

En plus des propriétés discutées auparavant, i-vote garantit d'autres propriétés liées à son implémentation :

Commodité : i-vote permet aux électeurs d'envoyer leurs votes rapidement, en une seule session et avec le minimum d'équipement ou de compétences spéciales.

Flexibilité : notre système permet également une variété de formats de bulletins de vote ce qui donne la possibilité d'organiser plusieurs types de vote.

Mobilité : i-vote peut être utilisé de n'importe quel ordinateur connecté au réseau (Internet/intranet), et ses serveurs (autorités de vote) peuvent être lancés sur n'importe quelle plate-forme.

Références

[1] A. Riera-Jorba. An introduction to electronic voting schemes. Rapport interne PIRDI n.9-98, U.A.B. Computer Science Department, septembre 1998.

[2] A. Riera-Jorba. *Design of Implementable Solutions for Large Scale Electronic Voting Schemes*. PhD Thesis, Universitat Autònoma de Barcelona, décembre 1999.

[3] A.D. Rubin. Security considerations for remote electronic voting over the Internet. *29th Research Conference on Communication, Information and Internet Policy (TPRC 2001)*, octobre 2001. `http://www.arxiv.org/abs/cs.CY/0108017`.

[4] B. Schneier. *Cryptographie appliquée*. International Thomson Publishing Company, Paris 1997.

[5] S. Benmeziane. Mécanismes d'authentification. Rapport interne, CERIST, 2001.

[6] C. Bidan et V. Issarny. Un aperçu des problèmes de sécurité dans les systèmes informatiques. IRISA, publication interne no. 959, octobre 1995.

[7] D. Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM*, vol. 24, no. 2, pages 84–88, 1981.

[8] L.F.Cranor et R.K. Cytron. Sensus : A security conscious electronic polling system for the Internet. *Proceedings of the Hawaii International Conference on System Sciences*, janvier 1997, Wailea, Hawaii, USA.

[9] L. Khelladi et K. Bouguessa. Conception et réalisation d'un système de vote électronique en Java. Mémoire de fin d'étude, novembre 2001.

[10] M.A. Herschberg. Secure Electronic Voting Over the World Wide Web. Master's thesis, Massachusetts Institute of Technology, mai 1997.

[11] M.J. Radwin. An untraceable, universally verifiable voting scheme. Seminar in Cryptology, December 12, 1995. `http://www.radwin.org/michael/projects/voting.pdf`.

[12] *The* `logi.crypto` *Java Package*, version 1.1.1. `http://www.logi.org/logi.crypto/index.html`.