La sécurité des systèmes de vote

Frédéric Connes
frederic.connes(@)hsc.fr

Hervé Schauer Consultants
4bis, rue de la Gare
92300 Levallois-Perret

Résumé La sécurité des systèmes de vote consiste à garantir l'intégrité des suffrages, le secret du vote, ainsi que la disponibilité et l'auditabilité des instruments électoraux. Nous présentons d'abord la sécurité des systèmes traditionnels, en montrant que le secret est, dans les démocraties, un acquis récent dont le respect n'est pas imposé de façon stricte, tandis que l'intégrité, la disponibilité et l'auditabilité sont des impératifs anciens et majeurs que la loi et le juge de l'élection s'attachent à faire respecter. Nous abordons ensuite le délicat problème de l'automatisation des systèmes de vote, qui soulève de graves problèmes en termes de sécurité. Pour y remédier, des solutions à base de trace papier et d'émission d'un reçu ont été proposées, mais elles ne résolvent pas totalement les problèmes soulevés. Nous proposons un protocole de vote se voulant simple à comprendre et relativement facile à mettre en œuvre. Son principe consiste à donner aux électeurs un reçu associant une marque anonyme à leur vote, cette association étant reprise sur un site web. Ainsi, les électeurs peuvent vérifier que leur suffrage a bien été pris en compte et toute personne peut refaire le calcul des résultats à partir du site. Le secret est quant à lui protégé en plaçant sur le reçu non seulement l'association entre la marque et le vote de l'électeur, mais aussi, pour chaque autre choix possible offert au vote, l'association de ce choix avec une marque ayant déjà été liée à ce choix lors du vote d'un électeur précédent.

1 Introduction

Le récent développement des systèmes de vote électronique pose la question de la sécurité des machines à voter et des serveurs de vote par Internet. De nombreuses études ont été consacrées à ce problème depuis une dizaine d'années (voir notamment : [1,10,11,13,14,16,17,18,26,27]), mais elles ont en général une approche exclusivement technique. Nous avons voulu dans notre thèse en droit [6] soutenue le 4 février 2009 à l'Université Paris-II Panthéon-Assas avoir une approche plus globale des difficultés soulevées, en abordant la question sous l'angle à la fois juridique et technique de la « sécurité des systèmes de

vote ». Il nous semble en effet possible de distinguer, comme cela est traditionnellement fait dans le domaine de la sécurité de l'information, des impératifs de confidentialité, d'intégrité, de disponibilité et d'auditabilité dans les systèmes de vote, définis comme les systèmes recueillant en entrée des suffrages et les agrégeant pour fournir en sortie des résultats bruts pouvant être interprétés par les modes de scrutin. La confidentialité correspond ici au secret du vote, l'intégrité à l'absence d'erreur ou de fraude, la disponibilité à la possibilité effective pour les électeurs de s'exprimer le jour du scrutin, et enfin l'auditabilité à la faculté, pour toute personne le désirant, de suivre le déroulement des opérations et de s'assurer de leur conformité à la procédure électorale.

Partant de ces impératifs, nous avons d'abord cherché à savoir comment ils étaient assurés dans le cadre du vote traditionnel, afin de pouvoir établir des comparaisons avec les systèmes de vote automatisés. Ensuite, nous avons étudié en détail les problèmes de sécurité soulevés par l'automatisation, qui demeurent importants et sont donc une source d'inquiétude pour la population. Ces difficultés font que l'acceptation du vote électronique passe aujourd'hui par des solutions permettant de restaurer la confiance des électeurs, et donc par la mise en œuvre de protocoles de vote prenant en compte les impératifs de sécurité. Après avoir présenté les propositions de plusieurs experts, qui reposent sur une trace papier ou font usage de procédés souvent difficiles à appréhender par des non spécialistes, nous avons proposé un protocole de vote se voulant simple à comprendre et relativement facile à mettre en œuvre. Il permet aux votants de vérifier, grâce à la fourniture d'un reçu et à la publication des votes sur Internet, que leur suffrage a correctement été pris en compte et que le résultat d'ensemble est correct, sans pour autant porter atteinte au secret. Cette possibilité de vérifier à tout instant l'intégrité des résultats constitue un avantage indéniable par rapport au vote traditionnel.

2 La sécurité des systèmes de vote traditionnels

2.1 L'adoption progressive du vote secret

L'étude de la sécurité des systèmes de vote dans le cadre traditionnel montre d'abord que le secret du vote, considéré aujourd'hui

comme indispensable à l'expression libre des choix des électeurs, est en réalité un acquis relativement récent dans les démocraties modernes. Certes, il existait dans l'Antiquité dans les civilisations grecque et romaine, mais il occupait à Athènes une place très limitée et il fut institué à Rome pour des raisons qui n'étaient en rien liées à une volonté de démocratisation, bien au contraire [2].

Ainsi, c'est avec la Révolution française de 1789 que le « scrutin », terme désignant à l'époque le vote secret, s'est développé. Après une période d'hésitations, le secret fut adopté durablement en France par une loi du 29 juin 1820, qui ne fut pas remise en cause par la suite. Toutefois, les conditions pratiques de mise en œuvre du secret ne permettaient alors pas de garantir une véritable confidentialité, et il fallut attendre une loi du 29 juillet 1913, adoptée après plusieurs décennies d'efforts de la part de nombreux parlementaires, pour que soient instaurés les enveloppes uniformes et les isoloirs [12], encore utilisés aujourd'hui.

Au Royaume-Uni, le vote public est resté en usage pendant très longtemps et de nombreuses tentatives de réforme échouèrent dans les années 1830. Ce n'est qu'avec l'adoption du vote secret dans les colonies d'Australie à partir de 1856, qui fut à l'origine, dans les pays anglo-saxons, de l'expression « *Australian ballot* » pour désigner le recours à un bulletin unique regroupant tous les choix possibles, rempli dans un isoloir et plié par les électeurs, que les idées commencèrent à évoluer. Finalement, la confidentialité des suffrages fut adoptée au Royaume-Uni en 1872 [15]. Il s'agissait non pas d'une volonté de démocratisation mais du résultat de tractations politiques. Pour autant, la confidentialité fut confirmée par des lois ultérieures et finit par s'imposer comme une condition de l'expression libre des choix politiques.

Enfin, aux États-Unis, où chaque État est responsable de ses techniques électorales, il fallut attendre la fin de la guerre de Sécession pour que le secret du vote s'impose comme un moyen de préserver la paix, car il permettait, à une époque où se développaient les groupes extrémistes, d'éviter les représailles contre des citoyens en raison de leurs opinions politiques. La confidentialité fut adoptée rapidement par les États fédérés, principalement entre 1888 et 1929 [9]. Toutefois, dans les États du Sud, le secret était d'abord vu comme un moyen d'empêcher les Noirs, majoritairement analphabètes, de

s'exprimer. Mais, comme au Royaume-Uni, la confidentialité s'est ensuite imposée progressivement comme un outil indispensable à la démocratie, et peu nombreux sont aujourd'hui ceux qui remettent en cause son utilité.

2.2 La force du principe de sécurité aujourd'hui

Nous avons ensuite cherché à évaluer la force du principe de sécurité des systèmes de vote aujourd'hui, à partir principalement d'une étude du droit positif et de la jurisprudence électorale en France.

Nous avons commencé par nous intéresser à la protection de la confidentialité, d'abord par l'électeur lui-même (notamment dans le contexte d'un scrutin), puis au moment de l'émission du vote (par l'isolement du votant et la dissimulation du bulletin). Nous avons ensuite étudié l'anonymat du vote lors de la comptabilisation des suffrages (absence d'éléments distinctifs), sans oublier la délicate phase d'anonymisation des votes à l'interface entre l'émission et la comptabilisation. Cette étude nous a permis de constater que, bien que correctement garanti, le principe de secret n'en connaissait pas moins certaines limites, liées avant tout à des contraintes pratiques et à la volonté du législateur de ne pas ouvrir la voie à de trop nombreuses invalidations liées au non-respect de règles certes protectrices de la confidentialité et de l'anonymat mais en pratique impossibles à appliquer strictement. Ainsi, le secret du vote apparaît comme un principe fort, souffrant toutefois de certaines limites qui sont considérées comme acceptables.

Tel n'est pas le cas des impératifs de disponibilité, d'intégrité et d'auditabilité, dont le strict respect est imposé.

Le législateur et le juge de l'élection encadrent ainsi la disponibilité des instruments de vote et la lutte contre les empêchements de voter, afin que le scrutin puisse se dérouler le jour prévu et que tous les électeurs puissent y participer.

Concernant l'intégrité, il importe d'abord que seuls les citoyens autorisés puissent participer au vote, ce qui implique notamment l'exactitude de la liste électorale, le contrôle d'identité des participants et l'enregistrement des votes, ce dernier étant destiné à empêcher qu'une même personne ne s'exprime plusieurs fois. Ensuite, l'intention des électeurs doit être transmise exactement, sans quoi le

choix reçu par le système de vote sera inexact. Il s'agit ici de mettre à disposition des bulletins sincères et clairs et de limiter les risques d'interprétation erronée des bulletins par les scrutateurs. Enfin, les résultats doivent correspondre aux choix émis, et il importe alors de lutter contre les erreurs et les fraudes, notamment par l'effet dissuasif des sanctions pénales, un contrôle des opérations, une gestion stricte des bulletins et des enveloppes, des contrôles de cohérence et un recomptage des bulletins si nécessaire. Ces mesures permettent d'obtenir les résultats les plus fiables possible et font l'objet d'une application très stricte par le juge de l'élection.

Pour ce qui est de l'auditabilité, la loi permet à toute personne le désirant d'assister à l'ensemble des opérations électorales, de l'ouverture à la fermeture du bureau. Le fait que l'urne soit désormais transparente est également un élément important de contrôle.

Ainsi, les systèmes de vote traditionnels apparaissent régis par le principe de sécurité, qui s'applique strictement pour ses composantes disponibilité, intégrité et auditabilité, et de façon plus souple pour la confidentialité.

3 La sécurité problématique des systèmes de vote automatisés

3.1 Les problèmes de sécurité des systèmes automatisés

L'étude des systèmes traditionnels permet de faire une comparaison avec les systèmes automatisés. Ceux-ci regroupent les machines à levier, les cartes perforées, les bulletins à lecture optique, les machines électroniques à enregistrement direct des votes et le vote au travers d'un réseau de communication comme Internet, dans l'ordre de leur apparition. Toutes ces techniques ont été utilisées lors de scrutins officiels, notamment aux États-Unis, depuis les premières machines à levier employées en 1892 à Lockport dans l'État de New York. Il faut reconnaître que ces techniques présentent d'indéniables avantages, tant lors de l'émission des suffrages (notamment pour les personnes handicapées) que lors du dépouillement (en termes de rapidité). Cependant, force est également de constater qu'elles souffrent de défauts majeurs en termes de sécurité, comme l'ont montré

de nombreuses études réalisées par des experts (voir les références données en introduction).

Tout d'abord, l'indisponibilité du système de vote peut provenir de l'absence d'alimentation électrique, de défaillances matérielles ou d'un déni de service, et les solutions existantes pour se protéger contre ces menaces ne sont pas pleinement satisfaisantes [10,24].

Ensuite, l'intégrité peut être compromise par un dysfonctionnement des mécanismes d'autorisation [18,26], un problème d'interface avec le votant comme cela a notamment été le cas en Floride lors des élections présidentielles américaines de novembre 2000 [20], ou encore des altérations involontaires ou volontaires des résultats. Sur ce dernier point, il existe de nombreux exemples de résultats aberrants fournis par des machines (voir notamment les chiffres tenus à jour par l'Election Incident Reporting System et la Verified Voting Foundation aux États-Unis), sans que l'on sache généralement quelle en est la cause, mais il est certain que ces altérations, largement commentées dans la presse, nuisent considérablement à l'image des nouvelles techniques de vote dans la population.

L'auditabilité est également remise en cause, puisque les machines apparaissent le plus souvent comme des « boîtes noires », dont il est impossible de connaître le fonctionnement de façon précise et exhaustive. A cet égard, la publication du code source, si elle est un point positif souvent réclamé, ne constitue pas une protection véritablement efficace, car il faudrait pour cela s'assurer de l'intégrité du compilateur [25] et de l'ensemble des composants exécutant le binaire, et également garantir que le code exécuté correspond exactement au code audité, ce qui demeure extrêmement difficile en pratique.

Enfin, il apparaît que le secret du vote disparaît totalement avec les systèmes automatisés. En effet, dans les bureaux de vote, il est d'abord possible pour une personne malveillante de capter à l'extérieur des signaux parasites compromettants [8] émis par les machines. Il est également possible que les machines stockent l'ordre dans lequel elles ont reçu les votes, et qu'une personne complice note l'ordre dans lequel les électeurs ont utilisé les machines [18]. Il devient alors possible de relier une personne à un vote. De son côté, le vote par Internet soulève de nombreux et graves problèmes de secret. Tout d'abord, les suffrages peuvent être captés sur les ordinateurs d'émis-

sion, par exemple à l'aide d'un logiciel espion. Ils peuvent également être interceptés lorsqu'ils transitent sur le réseau, le chiffrement ne constituant pas une protection parfaite, puisque rien ne garantit que l'algorithme utilisé ne sera pas cassé plusieurs années après le scrutin, ni que la clé utilisée a correctement été détruite, ce qui pourrait permettre la reconstitution *a posteriori* du lien unissant un électeur à son choix. Par ailleurs, l'ordinateur d'émission d'un suffrage est identifié par son adresse IP, ce qui peut éventuellement permettre d'identifier la personne auteur du vote. Il faut également mentionner le risque de *phishing* et de *pharming*, les électeurs entrant leur choix sur un faux site qui révèlerait ensuite leurs opinions. Enfin, les systèmes actuels de vote par Internet n'offrent pas une protection suffisante contre le rapprochement d'informations entre le serveur d'autorisation et le serveur de réception des choix, les deux pouvant s'échanger des données permettant d'établir le lien entre une personne autorisée et le vote qu'elle a émis.

L'ensemble de ces éléments montre que la sécurité des systèmes de vote, qui est correctement assurée dans le cadre traditionnel, est remise en cause dans tous ses aspects lorsque les systèmes sont automatisés. Dès lors, il est absolument indispensable de trouver des solutions de sécurisation avant que le vote automatisé ne soit utilisé à grande échelle.

3.2 La recherche de protocoles de vote sécurisés

Aujourd'hui, les recherches des experts en vote électronique se concentrent sur les protocoles de vote sécurisés, devant permettre de garantir l'intégrité des suffrages tout en préservant le secret, sans remettre en cause la disponibilité et l'auditabilité. Ces recherches ne signifient pas que leurs auteurs veulent à tout prix développer l'automatisation, mais simplement que les avantages du vote électronique sont tels qu'il n'est pas inutile de rechercher des nouveaux protocoles de vote si ceux-ci peuvent permettre d'aboutir à un vote automatisé aussi sûr que le vote traditionnel.

L'objectif est ici de parvenir à détecter et corriger les problèmes d'intégrité tout en préservant le caractère secret du vote, qui empêche précisément de détecter facilement les problèmes. En effet, dans la plupart des autres systèmes critiques, une défaillance est

visible et peut donner lieu à des actions correctives. Par exemple, une transaction bancaire erronée sera détectée par les parties et les banques pourront la rectifier ; l'accident d'un moyen de transport ne passera pas inaperçu et provoquera des modifications techniques ; de même une machine à sous se mettant à produire des gains à une fréquence anormalement élevée sera identifiée et réparée. Mais, dans le cas du vote, le secret empêche de savoir si les résultats produits sont corrects ou non, dès lors que le nombre de suffrages recueillis correspond au nombre de votants comptabilisés. Les protocoles de vote proposés tentent donc, pour garantir l'exactitude des résultats, de s'appuyer sur une référence indépendante, ne devant pas porter atteinte au secret.

La trace papier. La première possibilité consiste à recourir à une trace papier des suffrages, qui permet de comparer les résultats électroniques avec les votes enregistrés sur papier. Dans sa forme la plus simple, l'électeur place lui-même un bulletin papier imprimé par la machine dans une urne, mais cette solution soulève de nombreuses difficultés puisque, en particulier, rien ne garantit que tous les électeurs placeront effectivement un bulletin dans l'urne après avoir voté sur la machine. Rebecca Mercuri a proposé une amélioration consistant à faire inscrire le vote, par la machine, sur un rouleau présenté derrière une vitre [19], l'électeur pouvant valider ou non le choix inscrit. Cependant, cette solution n'est pas exempte de défauts (le rouleau stocke les votes dans l'ordre d'émission, la machine peut ajouter des votes lorsque personne n'est dans l'isoloir, etc.) et Aviel Rubin a proposé que la machine se contente d'imprimer un bulletin à lecture optique remis à l'électeur, à charge pour ce dernier de le passer dans une seconde machine comptabilisant les résultats [24]. Cette solution est intéressante en ce qu'elle permet de faciliter le recomptage manuel des bulletins, mais, comme les autres propositions, elle repose encore sur une comptabilisation électronique par défaut. Il existe donc un doute sur les résultats tant qu'un décompte manuel n'a pas été réalisé, ce qui limite l'intérêt de ce type de solution puisque le décompte manuel ne peut pas être organisé à chaque fois, sauf à rendre l'automatisation superflue. Il est certes possible de procéder à des recomptages de façon aléatoire, mais il faudrait alors pour donner confiance aux électeurs que les comptabilisations

manuelles confirment systématiquement les résultats électroniques. Or, eu égard aux problèmes rencontrés par certaines machines et au fait que le décompte manuel peut donner lieu à des erreurs, une telle hypothèse semble peu probable. De fait, les recomptages organisés dans certains États ont souvent montré des disparités dans les résultats. La trace papier telle qu'elle est envisagée aujourd'hui ne constitue donc pas une véritable solution de sécurisation du vote électronique.

Le reçu papier. Étant donné les limites de la trace papier, certains experts se sont tournés vers une autre solution, qui consiste à donner à l'électeur un reçu de son vote, qui est une référence non plus globale mais individuelle, permettant au citoyen de faire valoir son suffrage dans l'hypothèse où ce dernier n'aurait pas été correctement pris en compte. Les votes sont également, le plus souvent, publiés sur un site web de manière anonyme, de sorte que toute personne intéressée puisse recompter les résultats. Il s'agit là de propriétés que l'on ne retrouve pas dans le vote traditionnel, et qui constituent un avantage majeur de ce type de solution. Toutefois, il importe ici de faire très attention à la préservation du secret du vote, ce qui s'avère délicat. Une première proposition a été formulée par David Chaum en 2004 [3], qui se fonde sur un algorithme cryptographique très complexe, difficile à comprendre par les citoyens et présentant malgré tout certains défauts en termes de sécurité. En 2006, Ronald Rivest a proposé le protocole « ThreeBallot », qui présente l'avantage de ne pas recourir à la cryptographie [22] [7]. Néanmoins, il ne garantit pas l'intégrité des résultats si la machine de vote est corrompue et il rend possible une atteinte au secret du vote dans certaines hypothèses. Il a été perfectionné sous la forme du protocole « VAV », mais ce dernier présente encore des risques d'incohérence rendant sa mise en œuvre délicate. Le protocole « Twin », proposé par Ronald Rivest et Warren Smith en même temps que VAV, consiste quant à lui à donner à chaque électeur un reçu constitué de la copie du vote d'un électeur précédent, sans que ce dernier ne soit identifié [23]. Toutefois, il ne s'agit alors pas d'un véritable reçu, puisque le votant ne peut pas vérifier l'intégrité du bulletin qui lui est remis. Enfin, en 2008, un autre protocole, baptisé « Scantegrity », a été proposé par un groupe d'experts [4]. Cependant, le secret des votes repose ici sur le secret

d'une base de permutations, ce qui signifie que si le contenu de cette base était dévoilé, tous les votes seraient de fait rendus publics. La mise en œuvre de ce protocole s'avère donc délicate.

4 Proposition de protocole de vote

4.1 Présentation

Nos recherches nous ont conduit à imaginer un protocole de vote se voulant simple à comprendre et relativement facile à mettre en œuvre, tout en offrant des garanties en termes d'intégrité et de secret. Ce protocole a été présenté dans un article publié sur le site ArXiv le 18 août 2008 et a été commenté par Ronald Rivest et d'autres experts en vote électronique sur la liste de discussion « Scantegrity ». Nous en présentons ici une nouvelle version, tenant compte des remarques formulées par les spécialistes et intégrant des améliorations et simplifications auxquelles nous avons pu penser depuis la soutenance de notre thèse.

Le but de ce protocole étant d'être compréhensible par les citoyens, cette présentation n'est volontairement pas écrite à destination d'un public d'informaticiens et tente d'être compréhensible par le public le plus large possible. Toutefois, il s'agit bien ici de proposer un protocole ayant pour but d'offrir de réelles garanties en termes de sécurité, et non de se contenter de rassurer les citoyens.

Le protocole décrit ci-après se rapporte à un vote sur machine dans un bureau. Il peut néanmoins être transposé à un vote par Internet, même si cette dernière modalité soulève certains problèmes de sécurité supplémentaires non négligeables, qui n'ont pas trouvé de solution à ce jour, comme par exemple l'absence de garanties relatives à la protection du secret du vote de l'utilisateur d'un ordinateur personnel.

4.2 Principe

Nous estimons que la seule solution permettant de garantir l'exactitude des résultats indépendamment du bon fonctionnement de la machine (ce que Ronald Rivest nomme « l'indépendance logicielle » [21]) consiste à publier en clair, de façon anonyme, les choix des

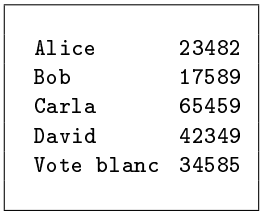
citoyens sur un site web, de façon que toute personne le désirant puisse procéder au recomptage des résultats, et que tout électeur puisse également retrouver et contrôler aisément son vote. Un autre élément de confiance consiste à donner à chaque votant un reçu lui permettant de faire valoir son choix en justice dans l'hypothèse d'une erreur, sans pour autant que le juge puisse connaître le choix du demandeur.

Pour parvenir à ces objectifs, nous proposons d'assigner à chaque électeur une marque, correspondant à un nombre aléatoire, et de rendre public le lien entre cette marque et le choix de l'électeur. Le secret du vote repose ici sur le secret du lien entre l'identité du votant et la marque qui lui a été attribuée. Il est impératif que ce lien ne survive pas en dehors de l'isoloir, de sorte que l'électeur lui-même soit incapable de prouver à un tiers qu'une marque particulière lui a été allouée. Pour autant, il importe que l'électeur puisse, seul, après être sorti de l'isoloir, se souvenir de sa marque, afin de pouvoir vérifier son vote sur le site web.

La solution que nous proposons pour réunir ces propriétés consiste à remettre à l'électeur, à l'issue de son vote, un reçu comportant non seulement l'association entre la marque qui lui a été attribuée et son vote, mais aussi, pour chaque autre choix possible offert au vote, l'association de ce choix avec une marque ayant déjà été liée à ce choix lors du vote d'un électeur précédent.

Afin d'illustrer notre propos, imaginons une élection opposant quatre candidats, que nous appellerons Alice, Bob, Carla et David. Imaginons également un électeur, qui entre dans l'isoloir et se voit proposer, sur la machine, le choix entre nos candidats, sans oublier la possibilité de voter blanc. Notre électeur choisit de voter pour Bob, et se voit remettre par la machine, avant de sortir de l'isoloir, un reçu. Ce reçu associe à Alice la marque 23482, à Bob la marque 17589, à Carla la marque 65459, à David la marque 42349, et au vote blanc la marque 34585. L'important ici est que le seul élément différenciant le vote de notre électeur pour Bob est que la marque associée à Bob est une marque nouvelle, qui n'a jamais été utilisée lors de ce scrutin, alors que toutes les autres marques sont en fait réutilisées : elles ont été créées à l'occasion d'un vote précédent, et ont été associées au choix de l'électeur s'exprimant lors de ce précédent vote. Par exemple, il existe un électeur ayant voté pour Alice, avant

le passage de notre électeur, dont le vote s'est vu associé à la marque 23482, qui était alors une nouvelle marque. De même, il existe un électeur précédent ayant voté pour Carla, dont le vote a été associé à la marque 65459, et ainsi de suite pour David et le vote blanc.



Alice	23482
Bob	17589
Carla	65459
David	42349
Vote blanc	34585

Figure 1. Reçu donné à l'électeur

Ainsi, en apparence, tous les appariements inscrits sur le reçu sont placés sur un pied d'égalité et rien ne les distingue les uns des autres. Un tiers qui entrerait en possession du reçu de notre électeur serait donc incapable de déterminer quelle marque nouvelle a été attribuée à notre électeur, et partant le sens de son vote. En revanche, notre électeur peut se souvenir très facilement que la marque qui a été associée à son vote est 17589, puisque celle-ci est inscrite sur son reçu en face de Bob.

A l'issue du scrutin, tous les appariements sont publiés sur un site web public, et l'on y retrouve notamment l'association entre Alice et la marque 23482, Bob et 17589, Carla et 65459, etc. Aucune information ne permet ici de lier une marque à un électeur. Malgré tout, notre électeur peut aller vérifier que tous les appariements présents sur son reçu se retrouvent bien sur le site web, et en particulier l'appariement entre Bob et 17589. Il s'agit là de son vote, mais lui-seul le sait, et il ne peut pas le prouver à un tiers. S'il constate une erreur, il pourra aller devant le juge de l'élection pour demander une rectification, le magistrat n'ayant alors aucun moyen de savoir, à partir du reçu présenté, si l'électeur se plaint de la mauvaise prise en compte de son véritable vote ou du vote d'une personne ayant voté avant lui.

On peut faire un parallèle en remarquant que, dans le vote traditionnel tel qu'il est pratiqué notamment en France, les électeurs

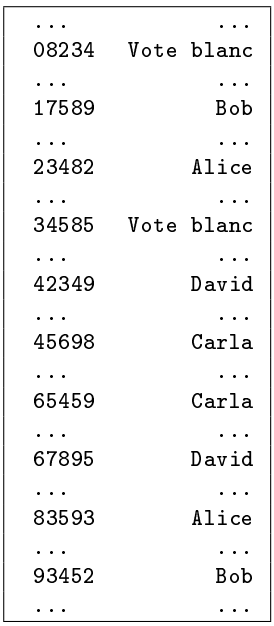


Figure 2. Site web public

prennent, avant d'entrer dans l'isoloir, autant de bulletins qu'il y a de choix possibles, afin de préserver le secret de leur vote. Ici, les électeurs se voient en quelque sorte remettre autant de bulletins qu'il y a de choix possibles, non pas avant d'entrer dans l'isoloir, mais juste avant d'en sortir.

Le principe que nous venons d'exposer propose une solution pour garantir l'intégrité des résultats tout en préservant le secret du vote, en apportant également des éléments d'auditabilité. Il ne fournit en revanche aucune solution pour renforcer la disponibilité des instruments de vote.

Il est finalement à noter que le protocole présenté part du principe que les électeurs doivent voter pour un seul choix parmi les possibilités qui leur sont offertes. Rien n'interdit cependant de leur permettre de s'exprimer en faveur de plusieurs possibilités, une nouvelle marque étant alors générée pour chaque choix sélectionné. En revanche, ce protocole, en lui-même, ne permet pas, comme cela est possible dans certains États comme les États-Unis, de voter en faveur d'un

candidat ne s'étant pas officiellement présenté. Cette hypothèse est traitée par l'émission d'un bulletin séparé.

4.3 Problèmes de mise en œuvre et solutions proposées

La mise en œuvre du principe que nous venons d'exposer soulève un certain nombre de problèmes. Nous les présentons ici avec les solutions que nous proposons pour y remédier.

Génération de la marque attribuée au votant. Le premier problème soulevé par le protocole a trait à la génération de la marque attribuée au votant. En effet, celle-ci pourrait dissimuler une information qui pourrait permettre à un tiers de la reconnaître parmi l'ensemble des marques figurant sur le reçu. Par exemple, un calcul utilisant certains chiffres de la marque pourrait donner un résultat spécifique, qui aurait très peu de chances d'être obtenu à partir des autres marques. Dès lors, il est impératif que la marque de l'électeur ne soit pas déterminée par la machine seule ou par le votant seul.

Pour parvenir à ce que la machine et l'électeur se mettent d'accord sur une marque aléatoire, nous proposons deux solutions.

La première solution consiste à présenter à l'électeur, avant qu'il n'entre dans l'isoloir, une corbeille remplie de papiers cachetés comportant une marque imprimée à l'intérieur sous la forme d'un code barre lisible par un humain. Le citoyen choisirait un papier au hasard et l'emporterait dans l'isoloir. Ainsi, ni lui ni la machine n'aurait de contrôle sur la marque choisie. Il reviendrait alors à la machine d'ouvrir le papier devant l'électeur et de lire automatiquement la marque inscrite, le citoyen pouvant vérifier que le nombre retenu est bien celui qui figure sur le papier. Cette solution, présentée dans notre thèse, a l'avantage d'être simple à comprendre, mais elle n'est pas adaptée au vote par Internet.

Nous proposons ici une seconde solution, qui est plus générale mais nécessite l'emploi d'un dispositif électronique par le votant. Pour commencer, la machine à voter génère un nombre binaire aléatoire, le chiffre avec une clé secrète et envoie le cryptogramme au dispositif électronique du citoyen. Ce dispositif génère à son tour un nombre binaire aléatoire de même taille que le nombre généré par la machine à voter, le chiffre avec une clé secrète et l'envoie à la

machine. Celle-ci envoie alors sa clé secrète au dispositif électronique, qui fait de même en sens inverse. Le dispositif et la machine déchiffrent alors le message envoyé par l'autre partie, réalisent un « ou exclusif » entre leur nombre et celui qu'ils viennent de déchiffrer, et considèrent le résultat comme la marque à utiliser. Ainsi, aucune des deux parties n'a pu décider du nombre final, tout en ayant pu l'influencer de manière non décisive. Le dispositif électronique utilisé par l'électeur peut être un matériel dédié ou un logiciel installé par exemple sur le téléphone mobile du citoyen, ou, dans le cadre du vote par Internet, sur son ordinateur. L'élément important ici est que l'électeur ait confiance dans le dispositif utilisé, et donc qu'il ait le choix de son fournisseur et qu'il puisse même, s'il le souhaite et en a la compétence, écrire lui-même le logiciel qu'il utilisera.

Génération des autres marques. S'il importe que la marque attribuée au votant ne renferme pas en elle-même d'élément distinctif et soit donc générée aléatoirement, il est également impératif que cette marque ne puisse pas être distinguée en la comparant avec les autres marques correspondant à des votes antérieurs. Par exemple, la marque du votant pourrait être celle dont le chiffre des milliers est le plus petit, les autres marques étant choisies par la machine pour respecter cette propriété. Il faut donc empêcher la machine de choisir les autres marques en fonction de celle qui a été attribuée au votant. Pour cela, nous proposons de lui faire générer ces autres marques avant que ne soit déterminée la marque du votant.

Pour autant, il n'est pas possible de faire générer les marques correspondant à des votes antérieurs lorsque le citoyen n'a pas encore fait son choix. En effet, si les marques étaient générées dès le début, une marque serait générée pour le futur choix du votant. Au final, celui-ci connaîtrait donc pour son choix deux marques valables, à savoir une marque correspondant à un votant précédent et la marque qui lui a été attribuée. La connaissance de deux marques valables pour un choix donné, contre une seule marque pour les autres choix, lui permettrait alors de prouver le sens de son vote. Il importe donc que les marques correspondant à des votes antérieurs ne soient générées qu'une fois le choix du citoyen définitivement validé.

Ainsi, les autres marques doivent être générées après le choix du votant et avant la génération de sa propre marque.

Premier votant. Le protocole que nous proposons repose sur l'intégration dans le reçu de l'électeur de marques correspondant à des votes antérieurs. Or, lorsque le premier citoyen se présente, il n'existe aucun vote antérieur et cette situation doit trouver une solution. Nous proposons ici que, lors du premier vote, la machine génère une marque aléatoire pour chaque choix autre que celui du citoyen, ce qui revient à créer des votes antérieurs fictifs.

Ainsi, aucun élément de la procédure n'indiquera au premier électeur qu'il est le premier à s'exprimer. Dans l'éventualité où ce citoyen saurait grâce à d'autres éléments qu'il est le premier à voter, il pourrait déterminer que les marques ne correspondant pas à son choix sont fictives. Cependant, une fois sorti de l'isoloir, il ne pourrait pas prouver ce fait à un tiers, rien ne distinguant sur son reçu les votes fictifs de son véritable choix.

Il faut indiquer ici qu'il n'est pas possible de générer préalablement au scrutin un vote fictif pour l'ensemble des choix offerts, car, outre le fait qu'il faudrait garantir le secret de ces votes fictifs puisque sinon le vote du premier électeur serait dévoilé, la machine n'attribuerait pas dans cette hypothèse toutes les marques fictives au premier votant : il lui resterait la marque fictive correspondant au vote de ce dernier. Or, rien ne permettrait alors de garantir que la machine attribue effectivement par la suite cette marque fictive au choix du premier votant, et non à un autre choix qu'elle souhaiterait favoriser. Ainsi, en ne générant pas de votes fictifs préalablement au scrutin, la solution proposée évite la gestion complexe de la bonne répartition des votes fictifs.

La génération de marques fictives lors du premier vote induit trois propriétés qui doivent être précisées. Tout d'abord, contrairement aux systèmes de vote traditionnels, si une seule personne vote, son choix restera secret, chaque possibilité recueillant officiellement une voix. Il s'agit là d'une propriété qui peut être intéressante dans les petits bureaux, puisqu'il est déjà arrivé, notamment en France, qu'un seul bulletin soit dépouillé, ce dont il est résulté une atteinte au secret du vote de la seule personne de la liste électorale ayant accompli son devoir civique. Ensuite, tous les choix recueillant officiellement au moins une voix, il sera impossible d'affirmer que personne n'a voté dans un sens déterminé. En particulier, cela supprime la possibilité qu'une décision soit prise à l'unanimité, ce qui renforce

le secret du vote et évite qu'un candidat ou un choix n'obtienne officiellement aucun suffrage. Enfin, il existe une incertitude d'une voix sur le résultat final, puisqu'une voix a été ajoutée fictivement à tous les choix sauf à celui effectué par le premier votant, sans que l'on puisse déterminer ce choix. Dès lors, aucune décision ne peut être prise en cas d'égalité ou d'écart d'une seule voix. Il s'agit là d'une propriété que l'on peut regretter, mais on peut aussi considérer qu'une décision collective ne saurait être prise, en définitive, par une seule personne, même si celle-ci est indéterminée. Cette propriété affirme donc le caractère collectif de la décision.

Attaque par comparaison de reçus. Du fait de la génération de reçus comportant des marques correspondant à des votes antérieurs, le protocole proposé est vulnérable à une attaque visant à comparer des reçus afin d'en déduire des informations pouvant permettre de porter atteinte au secret du vote. Ainsi, si une personne entre en possession de deux reçus et sait dans quel ordre ces reçus ont été générés, elle peut déterminer, si le second reçu comporte une marque qui apparaît aussi sur le premier reçu, que la personne a qui le second reçu a été remis n'a pas voté dans le sens associé à la marque déjà apparue. En effet, une marque présente sur un bulletin précédent ne peut correspondre à un nouveau vote.

Pour faire échec à une telle attaque, nous proposons de ne plus rendre systématique le fait qu'un nouveau vote soit associé à une nouvelle marque. En rendant simplement possible le fait qu'un nouveau vote soit associé à une marque déjà utilisée auparavant, une incertitude est créée qui ne permet plus d'affirmer qu'une personne n'a pas voté dans un sens déterminé du simple fait que la marque associée au choix correspondant est déjà apparue sur un reçu précédent.

Concrètement, nous proposons que la machine, au moment de déterminer la marque qui sera associée à l'électeur, demande à ce dernier s'il souhaite disposer d'un reçu « de contrôle » ou « absolument secret ». Le premier est un reçu qui comporte devant le choix effectué une marque nouvelle, qui permettra au citoyen de contrôler efficacement que son vote a bien été pris en compte. Le second est un reçu qui associe au choix effectué une marque déjà utilisée et liée à ce choix à l'occasion d'un vote précédent. Ce reçu ne permet pas

un contrôle du nouveau vote sur le site web, mais il protège le secret de manière absolue. Bien entendu, le nouveau vote est comptabilisé par ailleurs, dans un registre des votes « absolument secrets », à la manière des machines à voter traditionnelles.

On voit ici que, grâce à la simple possibilité qu'un reçu « absolument secret » ait été généré, un attaquant qui comparerait deux bulletins et constaterait que le second comporte une marque déjà présente sur le premier ne pourrait pas en déduire que le second électeur n'a pas voté pour le choix lié à la marque redondante, puisqu'il ne pourrait pas avoir la preuve que le second reçu n'est pas un reçu « absolument secret », comportant exclusivement des marques correspondant à des votes antérieurs. Le point important ici est qu'il n'est pas nécessaire que le second reçu soit effectivement un reçu « absolument secret », la seule possibilité qu'il le soit suffisant à créer le doute chez un attaquant.

Toutefois, il est important qu'à l'issue du vote au moins un reçu « absolument secret » ait été généré, sinon un attaquant saurait que les reçus dont il dispose sont tous « de contrôle », et que donc ils comportent tous une marque nouvelle devant un nouveau vote, ce qui supprime l'incertitude et rend l'attaque efficace. Nous proposons donc que la machine impose, de manière aléatoire, à certains électeurs que leur reçu soit « absolument secret ».

Authenticité et intégrité du reçu. Le reçu remis à l'électeur pouvant permettre à ce dernier de faire valoir son vote en justice s'il s'aperçoit que son choix n'a pas été correctement pris en compte sur le site web, il est important que le citoyen et le juge aient la preuve que le reçu est authentique et intègre. Il est possible d'imaginer que la machine appose un sceau physique sur un reçu papier, mais cette solution ne s'applique qu'au vote dans un bureau et reste vulnérable à l'altération des mentions du reçu sans toucher au sceau. Dès lors, il nous semble préférable que la machine signe numériquement un reçu électronique. Cette solution présente l'avantage de pouvoir être mise en œuvre dans un bureau et lors d'un vote par Internet, et permet un contrôle immédiat par l'électeur de l'authenticité du reçu, tout en interdisant la modification de son contenu *a posteriori*. En pratique, le citoyen votant dans un bureau recevrait le reçu électronique signé sur un dispositif de contrôle, qui pourrait par exemple être intégré

à son téléphone mobile, et il pourrait vérifier immédiatement son authenticité et son intégrité. Par Internet, le logiciel client utilisé par l'électeur réaliserait les mêmes opérations. Dans les deux cas, le citoyen ne signerait la liste d'émargement qu'après avoir contrôlé son reçu. Le juge pourrait quant à lui réaliser les mêmes opérations sur les reçus électroniques qui lui seraient soumis.

4.4 Déroulement de la procédure de vote.

Les solutions proposées aux différents problèmes de mise en œuvre du principe ayant été exposées, il faut maintenant les synthétiser en faisant une présentation chronologique de la procédure de vote, toujours dans le cadre d'un scrutin organisé dans un bureau sur des machines.

Lorsqu'un électeur se rend dans l'isoloir, la machine affiche les différentes possibilités comme cela se pratique habituellement, sans oublier le vote blanc. L'électeur fait son choix et le valide définitivement sur une page de confirmation.

La machine choisit alors au hasard, pour chaque choix autre que celui sélectionné, une marque antérieure associée à ce choix. Si le votant est le premier à se présenter, et qu'il n'existe donc pas de votes antérieurs, la machine génère aléatoirement un vote antérieur fictif pour chaque choix non sélectionné. A l'issue de cette étape, la machine affiche toutes les possibilités offertes au vote, qui sont toutes associées à une marque, sauf le choix du votant, qui n'a aucune marque associée.

Vient ensuite la phase de détermination de la marque qui sera associée au choix de l'électeur. La machine demande ici à ce dernier s'il souhaite disposer d'un reçu « de contrôle » ou « absolument secret ». Parfois, elle impose au votant la génération d'un reçu « absolument secret ». Si le reçu est de type « absolument secret », la machine associe au choix de l'électeur une marque antérieurement associée à ce choix, comme pour les marques liées aux autres choix possibles. Si le reçu est en revanche « de contrôle », la machine et l'électeur doivent se mettre d'accord sur une nouvelle marque aléatoire. Pour commencer, la machine génère un nombre binaire aléatoire, le chiffre avec une clé secrète et envoie le cryptogramme à un dispositif possédé par l'électeur, comme un téléphone mobile. Ce dispositif génère

également un nombre binaire aléatoire de même taille que le nombre généré par la machine à voter, le chiffre avec une clé secrète et l'envoie à la machine. Ensuite, la machine à voter envoie sa clé secrète au dispositif de l'électeur, qui fait de même en sens inverse. Le dispositif et la machine déchiffrent alors le message envoyé par l'autre partie, réalisent un « ou exclusif » entre leur nombre et celui qu'ils viennent de déchiffrer, et considèrent le résultat comme la marque à utiliser. Il appartient alors à l'électeur de s'assurer que la machine utilise la marque correcte. La machine doit quant à elle vérifier que la marque choisie n'a pas déjà été utilisée, et provoquer une nouvelle séquence de génération si tel est le cas. La longueur de la marque peut ici être choisie de manière à limiter considérablement la probabilité d'occurrence de cet événement. Une fois la marque déterminée, elle est associée au vote de l'électeur.

La machine génère alors un reçu électronique, qu'elle signe numériquement. Elle le transmet alors au dispositif électronique de l'électeur, qui vérifie son authenticité et son intégrité. Si le reçu est validé, l'électeur quitte l'isoloir et signe la liste d'émargement.

Dès le scrutin clos, les correspondances entre les votes et les marques sont publiées sur un site web, ainsi que le décompte des votes correspondant à des reçus « absolument secrets », qui sont simplement additionnés. Toute personne intéressée peut alors recompter manuellement les résultats, et les électeurs peuvent vérifier que l'ensemble des appariements présents sur leur reçu, et notamment celui correspondant à leur vote, se retrouvent bien sur le site web. La liste des personnes ayant émargé peut également être publiée sur un site web, afin que toute personne puisse la contrôler et vérifier que le nombre de suffrages publiés correspond au nombre de votants.

4.5 Problèmes restant à résoudre

Malgré les solutions proposées précédemment, le protocole exposé soulève encore certains problèmes.

Tout d'abord, le protocole n'est d'aucun secours face à certaines attaques classiques comme la captation de signaux parasites compromettants, l'usage d'une caméra à l'intérieur de l'isoloir ou encore la sauvegarde de l'ordre de passage des électeurs par la machine à

voter, mais ces problèmes ne peuvent sans doute pas être résolus par un protocole comme celui que nous avons présenté.

Ensuite, rien ne garantit à l'électeur que les marques associées aux choix autres que le sien correspondent bien à des votes antérieurs, et qu'elles n'ont pas été purement et simplement « inventées » par la machine. Ce problème est important car si plusieurs personnes font valoir devant le juge de l'élection des bulletins comportant de fausses marques, la solution à adopter pour résoudre les incohérences n'est pas évidente et peut conduire à l'annulation du scrutin. Cette question devra donc faire l'objet de recherches complémentaires.

Par ailleurs, la génération de marques fictives lors du passage du premier électeur peut paraître poser un problème, puisque le choix en faveur duquel ce premier électeur s'exprime semble perdre une voix par rapport aux autres choix en présence, même si en réalité les règles de majorité évoquées plus haut garantissent dans toutes les hypothèses l'exactitude de la décision. Il n'est donc pas impossible que certaines personnes ne veuillent pas voter en premier, de peur de défavoriser le choix qu'elles soutiennent, et il semble ici souhaitable que des dispositions soient prises pour ne pas indiquer aux électeurs qu'ils sont les premiers à utiliser la machine. Ceci est sans doute plus facile à réaliser dans le cadre du vote par Internet qu'avec des machines installées dans des bureaux de vote.

Enfin, il faut indiquer qu'il existe une attaque contre le secret du vote si une personne dispose de l'ensemble des reçus ayant été générés depuis l'ouverture du scrutin, dans l'ordre de leur émission. En effet, une telle personne saurait alors qu'une marque nouvelle correspond à un nouveau vote. Toutefois, cette attaque ne concerne que les premiers reçus, puisqu'il suffit qu'un électeur ne fournisse pas son reçu à l'attaquant pour qu'il devienne impossible à ce dernier de déterminer le sens des votes ultérieurs. En effet, dans une telle hypothèse, l'attaquant constatant qu'une marque n'est pas apparue sur un reçu antérieur dont il dispose ne pourra pas déterminer avec certitude que cette marque n'est pas en réalité déjà apparue sur un reçu antérieur dont il ne dispose pas. Cette attaque ne peut donc fonctionner que si des électeurs non corrompus ne votent pas parmi les premiers, ce qui en pratique peut être considéré comme très peu probable. En effet, un scrutin oppose généralement des citoyens aux opinions

divergentes, et certains électeurs non corrompus s'exprimeront très vraisemblablement parmi les premiers, surtout s'ils savent qu'une attaque de ce type est possible. En outre, il suffit en réalité que l'attaquant n'ait pas la preuve qu'il dispose de tous les reçus émis depuis l'ouverture du scrutin pour que l'attaque soit inopérante, ce qui est notamment très difficile à déterminer dans l'hypothèse d'un vote par Internet. Il faut également souligner que cette attaque ne fonctionne qu'à la condition que les électeurs corrompus soient coopératifs, puisqu'il leur est toujours possible, s'ils souhaitent voter dans un sens différent de celui qui leur a été demandé, soit de « perdre » volontairement leur reçu, soit de demander à la machine de leur donner un reçu « absolument secret », en prétendant que c'est la machine qui a imposé la génération d'un tel reçu, même si tel n'est pas le cas. Une telle attaque par rassemblement exhaustif de reçus depuis l'origine, bien que possible en théorie, a donc en pratique une portée très limitée.

5 Conclusion

Nous avons vu que la sécurité des systèmes de vote était correctement assurée dans le cadre traditionnel, mais qu'elle était loin d'être garantie avec les nouveaux systèmes automatisés. Or, il est indispensable pour le développement de ces derniers, qui est considéré comme souhaitable par certaines personnes en raison des avantages qui y sont liés en termes de convivialité et de rapidité du dépouillement, que leur sécurité soit au moins équivalente à celle des systèmes traditionnels, tant en termes de confidentialité que d'intégrité, de disponibilité et d'auditabilité. Les recherches se concentrent aujourd'hui sur les nouveaux protocoles de vote, et notamment sur ceux qui permettent de donner un reçu aux électeurs.

Nous avons proposé un protocole de ce type se voulant à la fois compréhensible par les citoyens et relativement facile à mettre en œuvre. Nous estimons qu'il pourrait permettre de donner aux citoyens confiance dans les résultats, en leur donnant la possibilité de s'assurer que leur choix a bien été pris en compte et de recompter eux-mêmes les votes. Il s'agit là d'un avantage indéniable par rapport au vote traditionnel, qui peut se révéler capital dans les États où les scrutins sont souvent douteux et contestés, ce qui peut donner

lieu à des tensions ou à des troubles. Ce protocole n'est pas exempt de défauts, mais, comme nous l'avons vu, le secret ne fait pas non plus l'objet dans le cadre traditionnel d'une protection absolue, et peut parfois être compromis à la marge. Finalement, ce protocole a maintenant besoin d'être examiné par les experts afin de dire s'il pourrait utilement être mis en œuvre lors de scrutins réels.

Références

1. Blaze, M. *et al.* : Source Code Review of the Sequoia Voting System. California Secretary of State (2007) 95 pages http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf
2. Buchstein, H. : Öffentliche und geheime Stimmabgabe. Eine Wahlrechthistorische und ideengeschichtliche Studie. Nomos Verlagsgesellschaft, Baden-Baden (2000) 747 pages
3. Chaum, D. : Secret-Ballot Receipts : True Voter-Verifiable Elections. IEEE Security & Privacy, vol. 2, n° 1 (2004) 38
4. Chaum, D. *et al.* : Scantegrity : End-to-End Voter-Verifiable Optical-Scan Voting. IEEE Security & Privacy, vol. 6, n° 3 (2008) 40
5. Connes, F. : A Simple E-Voting Protocol. ArXiv cs.CY/0808.2431v1 (2008) 8 pages http://arxiv.org/PS_cache/arxiv/pdf/0808/0808.2431v1.pdf
6. Connes, F. : La sécurité des systèmes de vote. Thèse, Université Paris-II Panthéon-Assas (2009) 512 pages http://www.fconnes.org/docs/secsysvote.pdf
7. Costa, R., Santin, A., Maziero, C. : A Three-Ballot-Based Secure Electronic Voting System. IEEE Security & Privacy, vol. 6, n° 3 (2008) 14
8. Eck, V. van : Electromagnetic Radiation from Video Display Units : An Eavesdropping Risk ? Computer & Society, vol. 4 (1985) 269-286
9. Evans, E. : A History of the Australian Ballot System in the United State. University of Chicago Press, Chicago (1917)
10. Feldman, A., Halderman, J., Felten, E. : Security Analysis of the Diebold AccuVote-TS Voting Machine (2006) 24 pages http://citp.princeton.edu/pub/ts06full.pdf
11. Fischer, E. (dir.) : Election Reform and Electronic Voting Systems (DREs) : Analysis of Security Issues. C.R.S. Report for Congress (2003) 37 pages http://epic.org/privacy/voting/crsreport.pdf
12. Garrigou, A. : Le secret de l'isoloir. Actes de la recherche en sciences sociales, n° 71/72 (1988) 22-45
13. Gonggrijp, R. *et al.* : Nedap/Groenendaal ES3B voting computer. A security analysis (2006) 22 pages http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf
14. Inguva, S. *et al.* : Source Code Review of the Hart InterCivic Voting System. California Secretary of State (2007) 93 pages http://www.sos.ca.gov/elections/voting_systems/ttbr/Hart-source-public.pdf
15. Jaffrelot, C. : L'invention du vote secret en Angleterre. Politix, n° 22 (1993) 43-68
16. Jefferson, D. *et al.* : A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). (2004) 34 pages http://www.servesecurityreport.org/
17. Keller, A. *et al.* : Privacy Issues in an Electronic Voting Machine. (2004) 19 pages http://gnosis.cx/publish/voting/privacy-electronic-voting.pdf
18. Kohno, T., Stubblefield, A., Rubin, A., Wallach, D. : Analysis of an Electronic Voting System. In : Proceedings of the 2004 IEEE Symposium on Security and Privacy, IEEE Computer Society Press (2004) 27-42 http://avirubin.com/vote.pdf

19. Mercuri, R. : Physical Verifiability of Computer Systems. In : Proceedings of the Fifth International Computer Virus and Security Conference (1992)

20. Pleasants, J. : Hanging Chads. The Inside Story of the 2000 Presiential Recount in Florida. Palgrave Macmillan, New York (2004) 304 pages

21. Rivest, R., Wack, J. : On the notion of "software independence" in voting systems (2006) 11 pages http://vote.nist.gov/SI-in-voting.pdf

22. Rivest, R. : The ThreeBallot Voting System (2006) 15 pages http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf

23. Rivest, R., Smith, W. : Three Voting Protocols : ThreeBallot, VAV, and Twin (2007) 14 pages http://www.usenix.org/event/evt07/tech/full_papers/rivest/rivest_html/

24. Rubin, A. : Brave New Ballot. Morgan Road Books, New York (2006) 280 pages

25. Thompson, K. : Reflections on trusting trust. Communications of the ACM, vol. 27, n° 28 (1984) 761-763

26. Wertheimer, M. (dir.) : Trusted Agent Report. Diebold AccuVote-TS Voting System. RABA Innovative Solution Cell (2004) 25 pages http://euro.ecom.cmu.edu/program/courses/tcr17-803/TA_Report_AccuVote.pdf

27. Yasinsac, A. *et al.* : Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware. Florida Department of State (2007) 66 pages http://nob.cs.ucdavis.edu/bishop/notes/2007-fsusait-1/2007-es+s.pdf