Rapport vote électronique

Gaston PLOT - 5A SAGI Polytech Angers - 2025-2026

Note : Ce rapport a été réalisée à l'aide d'une intelligence artificielle générative, qui a compilé et structuré des informations factuelles disponibles publiquement.

Question 1

La Suisse, souvent citée comme un modèle de démocratie directe, a connu un coup d'arrêt majeur en 2019 concernant son système de vote par internet. Le système développé par La Poste suisse, censé être totalement "vérifiable", a été soumis à un audit public. Des chercheurs en cryptographie ont alors mis en évidence une faille critique dans le code source, spécifiquement au niveau du processus de mélange cryptographique des bulletins. Cette vulnérabilité aurait théoriquement permis à un administrateur malveillant de modifier des votes valides sans que le système de vérification ne détecte l'anomalie. Face à ce risque avéré, les autorités fédérales ont pris la décision de geler le déploiement du vote électronique pour les élections fédérales de cette année-là.

En Russie, c’est lors des élections législatives de septembre 2021 que le vote en ligne a suscité de vives controverses, notamment à Moscou. Alors que le dépouillement des bulletins papier montrait une avance pour les candidats de l'opposition dans plusieurs circonscriptions, la publication des résultats électroniques a été retardée de plusieurs heures sans explication officielle. À leur publication, ces résultats ont inversé la tendance au profit du parti au pouvoir, "Russie Unie". Des analystes indépendants ont par la suite relevé des anomalies statistiques massives dans les données numériques, souvent qualifiées de "kystes de Shpilkin", qui ne correspondaient pas à une distribution naturelle des voix, suggérant une manipulation artificielle des résultats numériques.

Sur le plan juridique, l'Allemagne a établi un précédent fondamental en Europe dès 2009. La Cour constitutionnelle fédérale a jugé l'utilisation des machines à voter inconstitutionnelle, en s'appuyant sur le principe de publicité de l'élection. Les juges ont estimé que le processus électoral doit pouvoir être surveillé et compris par n'importe quel citoyen, sans qu'il soit nécessaire de posséder des connaissances techniques spécialisées en informatique. Le vote électronique étant par nature une "boîte noire" pour l'électeur moyen, il ne permet pas ce contrôle démocratique citoyen, ce qui a conduit à son interdiction.

Enfin, la vulnérabilité intrinsèque des machines est régulièrement mise en lumière lors des conférences de cybersécurité, comme le DEF CON à Las Vegas. Chaque année, le "Voting Village" rassemble des hackers éthiques qui parviennent systématiquement à pénétrer les défenses de machines à voter réelles en quelques heures. Que ce soit par des ports d'accès physiques mal protégés ou des failles logicielles élémentaires, ces exercices démontrent de

manière récurrente que les standards de sécurité de ces équipements sont souvent inférieurs à ceux exigés dans d'autres secteurs sensibles.

Question 2

L'Organisation pour la sécurité et la coopération en Europe (OSCE), par l'intermédiaire de son Bureau des institutions démocratiques (BIDDH), maintient une vigilance critique sur ces technologies. Dans son manuel d'observation du vote électronique, l'organisme insiste sur le fait que la rapidité du décompte ne doit jamais primer sur la transparence. L'OSCE souligne régulièrement dans ses rapports post-électoraux que la complexité technique des systèmes entrave la capacité des observateurs indépendants à certifier la sincérité du scrutin, créant un fossé de confiance avec les citoyens.

Le Conseil de l'Europe a adopté une position réglementaire stricte avec sa recommandation de 2017, qui fait office de standard pour les pays membres. Si l'institution n'interdit pas le vote électronique, elle exige que tout système respecte le principe de "vérifiabilité de bout en bout". Selon cet avis, un système n'est acceptable que si l'électeur peut prouver que son bulletin a été correctement enregistré et comptabilisé, sans pour autant briser le secret du vote, une équation technique que le Conseil reconnaît comme extrêmement difficile à résoudre parfaitement.

Bruce Schneier, cryptographe de renommée mondiale et expert en sécurité informatique, est l'un des opposants les plus vocaux au vote par internet. Il soutient la thèse selon laquelle il est impossible de sécuriser totalement une élection en ligne avec la technologie actuelle. Son argument principal repose sur la distinction entre la sécurité bancaire et électorale : contrairement à une fraude bancaire qui peut être compensée financièrement par l'établissement, une fraude électorale est irréversible et peut déstabiliser une nation entière. Il résume souvent sa pensée par l'idée qu'on ne peut pas avoir à la fois le secret absolu du vote et la vérifiabilité totale en ligne.

Ron Rivest, professeur au MIT et co-inventeur de l'algorithme de chiffrement RSA (le "R" de RSA), partage cette méfiance technique. Il a cosigné plusieurs rapports, notamment pour les académies nationales américaines des sciences, recommandant l'usage exclusif de bulletins papier marqués à la main pour les élections fédérales. Selon lui, le papier reste la seule technologie indépendante du logiciel capable de fournir une piste d'audit fiable pour un recomptage manuel en cas de contestation ou de bug informatique.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a émis des avis qui ont conduit à restreindre l'usage du vote par internet. L'agence considère que le niveau de menace cybernétique actuel rend le vote électronique trop risqué pour les élections majeures sur le territoire national, comme l'élection présidentielle. C'est sur la base de ces expertises techniques que le Sénat français et le gouvernement ont maintenu l'usage du papier pour l'ensemble des citoyens résidant en France, limitant le vote électronique aux seules élections consulaires pour les expatriés.

Question 3

Question 4

1. Attaques par collusion (Entités internes)

La collusion représente le véritable talon d'Achille de la plupart des systèmes distribués : dès lors que les entités censées se surveiller mutuellement décident de collaborer, la sécurité du système s'effondre. Le scénario le plus critique pour la confidentialité réside dans l'association entre l'Anonymiseur et le Décompteur. Dans cette configuration, l'anonymiseur détient l'identité de l'électeur (via son code N1 ou son adresse IP) ainsi que le bulletin chiffré, tandis que le décompteur possède la clé privée nécessaire au déchiffrement. En échangeant secrètement ces informations, ils deviennent capables de relier chaque vote à son émetteur, provoquant une désanonymisation totale du scrutin, bien que l'intégrité du comptage puisse techniquement rester intacte.

En revanche, une tentative de bourrage d'urne orchestrée par l'Administrateur et le Commissaire est vouée à l'échec. Si l'administrateur peut générer de fausses signatures et le commissaire valider de faux codes N1, ils se heurtent à une barrière cryptographique lors de la création du bulletin. Pour qu'un vote soit valide, il doit inclure un code N2 dont l'empreinte figure dans la liste du commissaire. Or, le protocole stipule que les codes N2 clairs ont été détruits ; le commissaire ne possède que leurs hachages (N’2). Ne pouvant deviner la pré-image de ces hachages (détenue uniquement par les électeurs), ce duo malveillant se trouve dans l'incapacité de fabriquer des bulletins valides indétectables.

2. Administrateur malveillant

L'administrateur occupe une position pivot puisqu'il autorise le vote, mais ses pouvoirs de nuisance sur le contenu sont limités par la cryptographie. Il ne peut pas altérer le vote grâce au mécanisme de signature à l'aveugle. Mathématiquement, l'électeur envoie un message masqué (m’) que l'administrateur signe. Si ce dernier tentait de modifier m’, par exemple en changeant un bit, la signature résultante ne correspondrait plus au message original une fois le masque retiré par l'électeur. Le logiciel de vote détecterait cette anomalie immédiatement et l'électeur pourrait prouver la fraude en révélant son facteur aléatoire de masquage (k). Toutefois, l'administrateur conserve un pouvoir de nuisance sous la forme de censure : il peut effectuer une attaque par déni de service (DoS) ciblée en refusant simplement de signer le bulletin d'un électeur légitime, prétextant une invalidité ou une panne technique.

3. Décompteur corrompu

Le décompteur, ayant accès aux votes en clair à la fin du scrutin, pourrait être tenté de manipuler les résultats. S'il envisageait de supprimer des bulletins défavorables, il serait rapidement trahi par la comptabilité de l'anonymiseur. Si ce dernier a transmis 10 000 bulletins chiffrés et que le décompteur n'en présente que 9 950, la fraude est manifeste, d'autant que la liste des bulletins reçus peut être auditée publiquement. Par ailleurs, la modification d'un vote (transformer un "Vote A" en "Vote B") est rendue impossible par la

signature de l'administrateur présente sur le bulletin. Le décompteur ne possédant pas la clé privée de l'administrateur, il est incapable de générer une nouvelle signature valide pour le vote modifié. Tout bulletin altéré serait donc mathématiquement rejeté lors de la vérification publique.

4. Attaque externe sur l'Anonymiseur

Dans l'éventualité où un pirate parviendrait à prendre le contrôle du serveur de l'anonymiseur (l'urne) pendant le scrutin, les dégâts seraient contenus. Concernant le vol de données, l'attaquant pourrait récupérer les couples (N1, Bulletin Chiffré). Puisqu'il ne possède pas la clé privée du décompteur, le contenu du vote reste illisible ; le risque se limite donc à savoir qui a voté, sans savoir pour qui. L'attaquant pourrait également tenter de détruire l'urne numérique, ce qui annulerait l'élection à moins que des sauvegardes sécurisées en temps réel (type Blockchain ou disques WORM) ne soient en place. Enfin, une attaque par rejeu, consistant à renvoyer plusieurs fois le même bulletin intercepté pour gonfler un score, serait bloquée par le commissaire. Ce dernier "consomme" le code N1 lors de la première utilisation, rejetant systématiquement toute tentative ultérieure avec ce même identifiant.

Résumé de la sécurité

Entité menacée	Risque Principal	Contre-mesure du protocole
Confidentialité	Collusion Anonymiseur/Décompteur	Aucune technique (faiblesse structurelle). Solution : utiliser plusieurs anonymiseurs en chaîne (Mix-nets).
Intégrité (Modif)	Admin ou Décompteur modifie le vote	Signature RSA (Admin) + Hash (Intégrité)
Bourrage d'urne	Création de faux électeurs	Distribution séparée de et + Destruction des clairs.
Censure	Admin refuse de signer	Auditabilité des logs de l'Admin (difficile à empêcher techniquement).

Question 5

De l'isoloir physique à l'enveloppe cryptographique : une transposition imparfaite

La transition du vote papier vers le protocole numérique proposé ne constitue pas une simple numérisation des tâches, mais un changement de paradigme profond qui redéfinit les garanties démocratiques. Le vote papier traditionnel tire sa robustesse de sa simplicité tangible : l'isoloir garantit physiquement l'absence de contrainte, l'urne transparente assure que les bulletins ne sont pas pré-remplis, et le dépouillement public permet une surveillance citoyenne distribuée. Notre protocole tente de mimer ces étapes par des équivalents mathématiques : la signature à l'aveugle remplace l'enveloppe opaque et le chiffrement RSA remplace l'urne scellée.

Si ce système excelle dans l'exactitude du comptage et l'élimination des bulletins nuls ou ambigus — une amélioration notable par rapport au papier —, il affaiblit considérablement la résistance à la coercition. Dans l'isoloir physique, il est impossible de prouver à un tiers pour qui l'on a voté, ce qui neutralise l'achat de voix. Avec ce protocole numérique, un électeur peut voter depuis chez lui sous la menace ou contre rémunération, en montrant son écran à un tiers. La "liberté" du vote est mathématiquement préservée, mais socialement fragilisée. De plus, la notion d'unicité de l'électeur, garantie par la présence physique et la carte d'identité dans un bureau de vote, repose ici entièrement sur la confidentialité des codes N1 et N2. Le vol de ces codes équivaut au vol de l'identité électorale, une attaque beaucoup plus "scalable" (réalisable à grande échelle) que le bourrage d'urne physique.

Le paradoxe de la transparence : de la vision à la vérification

Ce système déplace le curseur de la confiance d'une manière qui peut sembler contre-intuitive. Le vote papier repose sur une transparence visuelle accessible à tous, quel que soit le niveau d'éducation : n'importe qui peut surveiller une urne. Le vote électronique proposé ici repose sur une transparence logique et mathématique. Bien que le code puisse être "open source" et les algorithmes publics, la vérification réelle du scrutin devient l'apanage d'une élite technique. Pour le citoyen lambda, le processus devient une "boîte noire". Il doit faire confiance aux administrateurs systèmes et aux auditeurs qui certifient que le code exécuté sur le serveur est bien celui qui a été publié.

Paradoxalement, ce système demande donc *plus* de confiance aveugle envers les infrastructures techniques que le système papier, tout en offrant théoriquement *plus* de transparence sur le résultat final grâce aux preuves cryptographiques. C'est une transparence "a posteriori" (on peut vérifier mathématiquement que le vote a été compté) qui s'oppose à la transparence "en temps réel" du vote papier (on voit le bulletin tomber dans l'urne). Cette opacité technique risque de nourrir la suspicion : une simple panne de serveur ou un bug d'affichage, même bénins, pourraient être interprétés comme une tentative de manipulation massive, là où une erreur humaine dans un bureau de vote reste locale et compréhensible.

Positionnement : Prudence pour la nation, audace pour l'organisation

Dans l'état actuel de la technologie et des mentalités, le déploiement de ce protocole pour une élection présidentielle ou législative majeure me semble prématuré et risqué. L'enjeu principal d'une élection nationale n'est pas seulement l'exactitude du résultat, mais l'acceptation de ce résultat par le peuple (le consentement). Si une fraction significative de la population ne comprend pas le mécanisme de la signature à l'aveugle ou doute de l'intégrité des serveurs — un doute que la cryptographie seule ne peut lever —, la légitimité du vainqueur pourrait être contestée, ouvrant la voie à une crise institutionnelle. La centralisation des données (même chiffrées) crée de plus un point de défaillance unique : une cyberattaque réussie pourrait invalider l'ensemble du scrutin, un scénario impossible avec des milliers de bureaux de vote déconnectés.

Cependant, ce système serait parfaitement acceptable et même souhaitable dans des contextes où les enjeux de coercition sont moindres et le besoin d'agilité supérieur. Pour des

référendums d'entreprise, des élections syndicales, des votes associatifs ou des consultations locales consultatives, ce protocole offre un équilibre coût-sécurité excellent. Il permettrait d'augmenter la participation en facilitant l'acte de vote, sans les lourdeurs logistiques du papier. Dans ces environnements contrôlés, la confiance entre les acteurs est souvent préexistante, et la rapidité du résultat prime sur la résistance absolue aux attaques étatiques.

Vers un horizon technologique plus robuste

Les limites identifiées, notamment la confiance requise envers les entités centrales (l'administrateur qui signe, le décompteur qui possède la clé privée), pourraient être dépassées par l'intégration de technologies émergentes. La Blockchain, par exemple, pourrait remplacer le serveur de l'anonymiseur en offrant un registre public immuable : chaque vote chiffré y serait inscrit de manière indélébile, empêchant toute censure ou suppression de bulletins a posteriori. Cela résoudrait le problème de la confiance dans le stockage des voix.

Plus prometteur encore, le chiffrement homomorphe permettrait de réaliser le décompte des voix *sans jamais les déchiffrer*. Le décompteur pourrait additionner les bulletins chiffrés pour obtenir un résultat lui-même chiffré, qui ne serait révélé qu'à la fin. Ainsi, aucune entité, même corrompue, ne verrait jamais un bulletin individuel en clair. Enfin, l'usage des preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs - ZKP) permettrait à un électeur de prouver qu'il possède un droit de vote valide sans révéler son identité ni ses codes N1/N2, renforçant drastiquement l'anonymat et rendant la collusion entre entités inefficace. Ces technologies, bien que gourmandes en ressources de calcul, dessinent l'avenir d'un vote électronique où la confiance dans l'humain ou l'institution deviendrait superflue, remplacée par la certitude mathématique.