# Offre de stage : développement de protocoles cryptographiques pour un vote électronique (plus) sûrs dans la vraie vie

(1) un pastillage préservant le secret du vote
et
(2) une distribution des clés contraignante

**Localisation :** Nancy, France.

**Équipe et laboratoire**
PESTO au LORIA (Inria Nancy, CNRS, et Université de Lorraine).

**Encadrants**
Alexandre Debant, `alexandre.debant@inria.fr` & Lucca Hirschi, `lucca.hirschi@inria.fr`

**Nom et email du directeur de laboratoire**
Yannick Toussaint, `yannick.toussaint@loria.fr`

**Indémnisation**
Le stage est financé par le PEPR Sécurité (SVP).
**Durée :** à définir

**TL ;DR.** Le but de ce stage est de concevoir ou adapter des protocoles cryptographiques pour le vote électronique afin de garantir la sécurité des scrutins qui utilisent du pastillage ou des règles de quorums pour la distribution des clés de déchiffrement.

## Contexte

Le vote par internet apparait aujourd'hui comme la solution préférée lors des élections non-politiques en France, i.e., élections professionnelles, associatives, etc. À titre d'exemple, lors des élections professionnelles de la fonction publiques en 2022, ce n'était pas moins de 2,2 millions d'agents qui étaient appelés à se prononcer par internet, pour choisir leurs représentants pour près d'un million de bulletins électroniques soumis [8]. Le vote politique est strictement encadrée par la loi et ne peut aujourd'hui être réalisé par voie électronique, à l'exception des élections législatives pour les français non résidents en France. Ainsi, les électeurs français de l'étranger ont élu leur 11 députés lors des élections de 2022 puis 2024 en grande majorité par voie électronique, ce qui en a fait les plus grandes élections par vote électronique connue à ce jour dans le monde. Le vote électronique est aussi utilisé dans le monde, comme en Suisse, en Estonie, ou encore en Australie, pour des élections politiques.

Le vote par internet est rendu possible par l'utilisation de *protocoles cryptographiques* qui sont essentiellement des programmes concurrents qui utilisent des *primitives cryptographiques*, e.g., chiffrement, signature, preuves à divulgation nulle de connaissance, pour garantir des propriétés de sécurité, telles que la confidentialité des votes et l'intégrité du scrutin. Bien que les protocoles utilisés prétendent satisfaire aux plus hauts niveau de recommandations édictés par la CNIL [10] et ainsi fournir un haut niveau de sécurité, différentes études [2, 4, 5, 9] ont montré de sérieuses limitations et attaques sur ces protocoles pouvant affecter l'intégrité des résultats mais aussi la confidentialité des votes. Nous avons également trouvé des attaques sur le protocole de vote électronique utilisé lors des élections législatives en 2022 [6]. Si certaines sont dues à des erreurs d'implémentation ou des problèmes de conceptions qui ont été corrigés depuis, d'autres apparaissent comme des défis toujours ouverts.

Dans ce contexte, le stage s'intéressera à développer de nouveaux protocoles cryptographiques ou adapter des protocoles existants afin de permettre :

(1) un pastillage préservant la vie privée et le secret des votes ;
(2) une distribution de clés de déchiffrement respectant les règles qui définissent le quorum.

### 1 Distribution des clés

Nous avons démontré [6] que certaines exigences légales, qui définissent par exemple le quorum requis pour déchiffrer une urne électorale, ne sont pas garanties de manière cryptographique lors des élections législatives françaises. En conséquence, moins de personnes que ce que la loi prescrit peuvent collaborer afin de déchiffrer une urne électorale. Ce problème affecte également d'autres protocoles et élections à travers le monde. En effet, les solutions académiques actuelles, qui reposent sur du *chiffrement à seuil* et un schéma de génération de clé proposé par Pedersen en 1991 [11], ne peuvent pas être utilisées directement pour résoudre ce problème. L'objectif est d'adapter ces protocoles existants afin de transformer ces contraintes opérationnelles en contraintes cryptographiques.

### 2 Pastillage

Deuxièmement, le pastillage de votes est un mécanisme qui associe chaque bulletin de vote aux attributs de son électeur (par exemple, la tranche d'âge) [1]. Cela permet d'extraire des informations sur une élection, soit pour créer d'autres instances dans un cadre plus restreint (comme les électeurs éligibles de plus de cinquante ans), soit à des fins statistiques ou informatives. Ce mécanisme est largement utilisé en pratique, en particulier lors des élections professionnelles. Cependant, les solutions actuellement en usage (comme le chiffrement du choix de l'électeur et de ses attributs dans le même message) sont clairement sous-optimales et divulguent beaucoup plus d'informations que nécessaire, compromettant ainsi la confidentialité du vote. L'objectif est d'adapter le protocole de vote de l'état de l'art Belenios [3] pour assurer un pastillage préservant la confidentialité du vote.

## Objectifs

Le stagiaire pourra s'intéresser à un ou plusieurs objectifs selon ses préférences et dans l'ordre qu'il le souhaite. Il n'est pas attendu que l'ensemble des objectifs soient traités. Le cas d'étude proposé est le protocole de vote Belenios [3] qui est un protocole de vote électronique s'appuyant sur un schéma de *chiffrement homomorphe* (le chiffrement El Gamal). Les objectifs du stage seront d'adapter ce protocole (et possiblement d'en généraliser les extensions à d'autres protocoles de votes) pour permettre :

- pastillage : concevoir un mécanisme de pastillage limitant la fuite additionnelle d'information au minimum nécessaire pour obtenir les résultats/statistiques souhaités et définis en amont du scrutin.
- génération de la clé de déchiffrement : concevoir un processus de génération de clés de déchiffrement (idéalement distribué) encodant exactement un quorum dont les règles sont fixées en amont du scrutin. La principale difficulté réside dans la mise en œuvre d'un solution efficace pouvant être utilisée en pratique.
- analyse formelle d'un protocole de vote : le stagiaire utilisera un outils de preuve automatique [1] (e.g., ProVerif, Tamarin) pour prouver la sécurité d'un protocole de vote mettant en œuvre la/les contributions pré-citées (pastillage et distribution des clés). Cette modélisation nécessitera de prendre en main les outils et de proposer un modèle formel pour chacune des contributions.

## Pre-requis

Nous attendons une maturité mathématique et des connaissances de base en logique et en informatique théorique. Des connaissances en sécurité et en cryptographie ne sont pas obligatoires mais constituent un avantage certain. Si le candidat est intéressé, une poursuite en doctorat, pour lequel nous disposons déjà de financements, est possible.

1. Dans un rapport [7], l'Inspection générale de l'administration définit le *pastillage* comme : une solution permettant de *« rendre possibles des extractions d'informations sur un scrutin, soit pour constituer d'autres instances dans un périmètre qui lui est inférieur (comités locaux d'action sociale, notamment, en application, au ministère de l'intérieur, de l'arrêté du 17 octobre 2022 relatif aux commission locales d'action sociale), soit à des fins statistiques ou informatives de l'administration ou des organisations syndicales. »*.

# Références


[1] Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno. Sok : Computer-aided cryptography. In *2021 IEEE symposium on security and privacy (SP)*, pages 777–795. IEEE, 2021.

[2] Enka Blanchard, Antoine Gallais, Emmanuel Leblond, Djohar Sidhoum-Rahal, and Juliette Walter. An analysis of the security and privacy issues of the neovote online voting system. In *International Joint Conference on Electronic Voting*, pages 1–18. Springer International Publishing Cham, 2022.

[3] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. Belenios : a simple private and verifiable electronic voting system. *Foundations of Security, Protocols, and Equational Reasoning : Essays Dedicated to Catherine A. Meadows*, pages 214–238, 2019.

[4] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. How to fake zero-knowledge proofs, again. In *E-Vote-Id 2020-The International Conference for Electronic Voting*. Tal Tech Press, 2020.

[5] Véronique Cortier and Ben Smyth. Attacking and fixing helios : An analysis of ballot secrecy. *Journal of Computer Security*, 21(1):89–148, 2013.

[6] Alexandre Debant and Lucca Hirschi. Reversing, breaking, and fixing the french legislative election e-voting protocol. In *USENIX Security Symposium (SEC'23)*, 2023.

[7] Inspection générale de l'administration. Mission sur l'organisation des élections professionnelles 2022 au ministère de l'intérieur et des Outre-mer, N° 22117-R, avril 2023.

[8] Direction générale de ladministration et de la fonction publique. `https://www.fonction-publique.gouv.fr/files/files/ArchivePortailFP/www.fonction-publique.gouv.fr/files/files/statistiques/stats-rapides/resultats-electionsFP_2022.pdf`.

[9] Johannes Mueller. Breaking and fixing vote privacy of the estonian e-voting protocol ivxv. In *International Conference on Financial Cryptography and Data Security*, pages 325–334. Springer, 2022.

[10] Journal Officiel. Délibération nř 2019-053 du 25 avril 2019, 2019. Document téléchargé et accessible le 28 juin 2022 via le lien `https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239`.

[11] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Advances in CryptologyCRYPTO91 : Proceedings*, pages 129–140. Springer, 2001.