Being a doctor…
what's next (for me)?

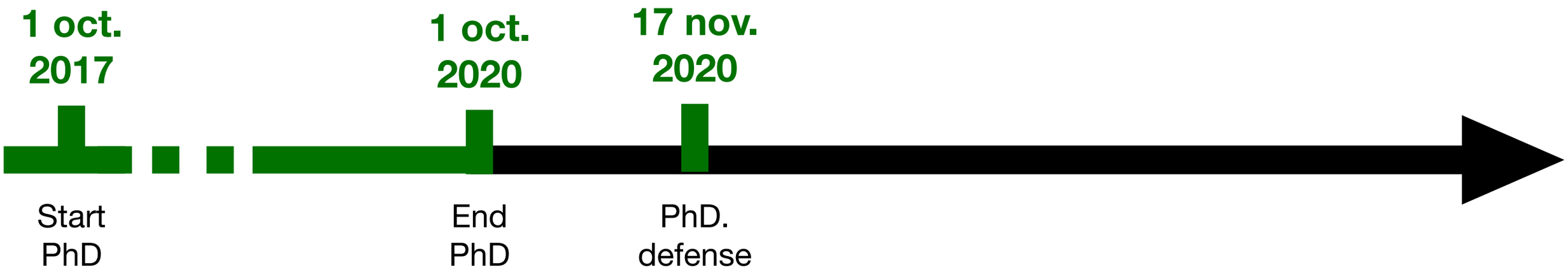
Alexandre Debant

CORGI seminar

Rennes, France

July 12th 2021

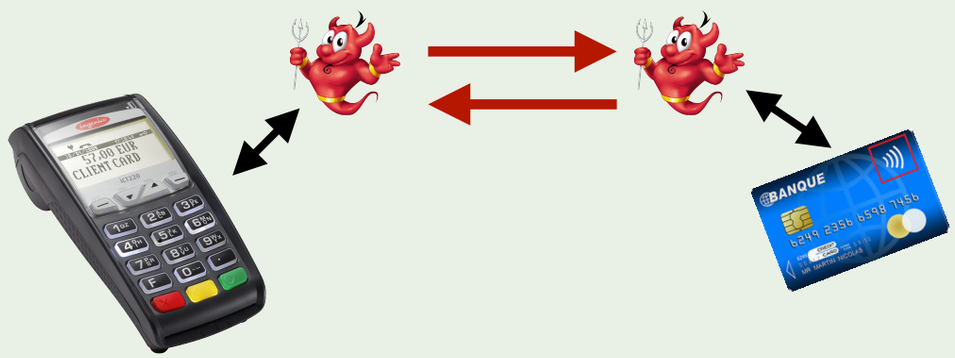
Who am I?



PhD. Thesis

Title: Symbolic verification of distance-bounding protocols - application to contactless paiement protocols

Supervision: Stéphanie Delaune



Who am I?

Post-doc

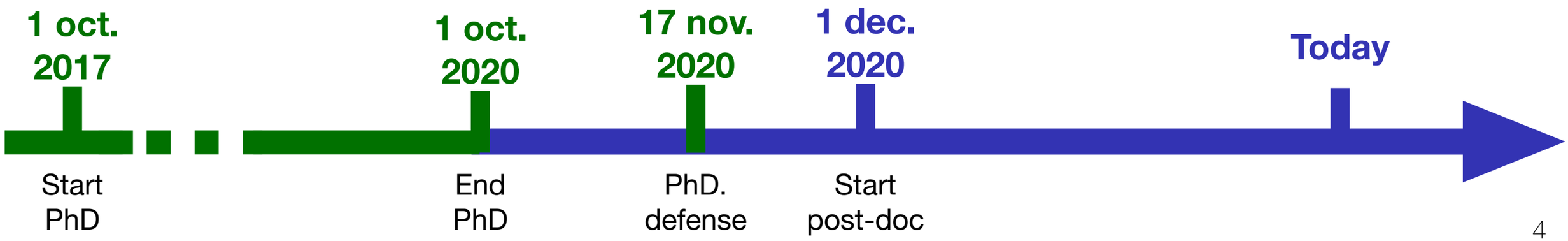
Title: Designing and proving the security of electronic-voting protocols

Supervision: Véronique Cortier

Location: Inria Nancy - Grand Est

Outline

What was the main steps of my first year of post-doc?

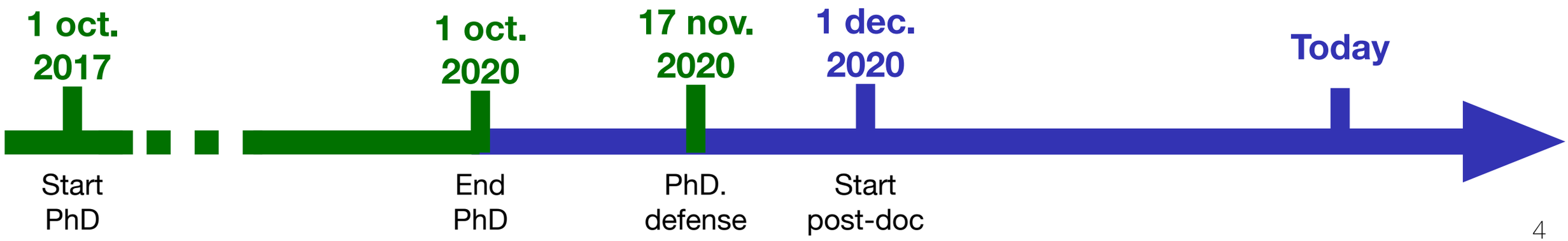


Outline

What was the main steps of my first year of post-doc?

From an administrative point-of-view

- Looking for a post-doc
- Qualification
- Applications to CR/MCF positions
- ...



Outline

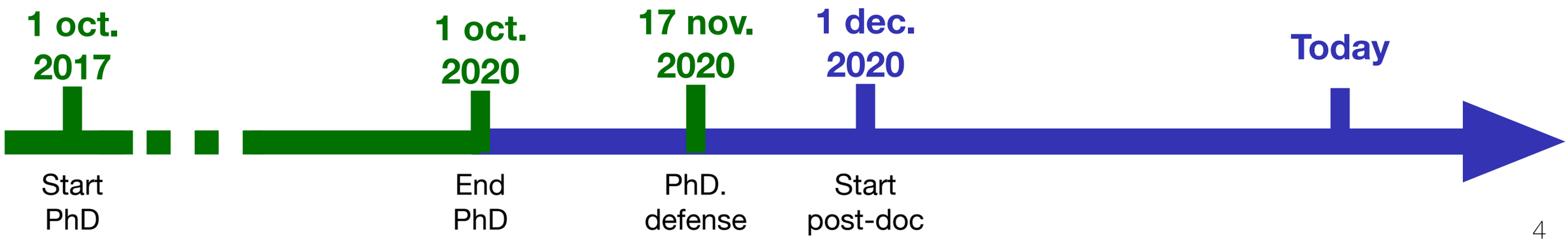
What was the main steps of my first year of post-doc?

From an administrative point-of-view

- Looking for a post-doc
- Qualification
- Applications to CR/MCF positions
- …

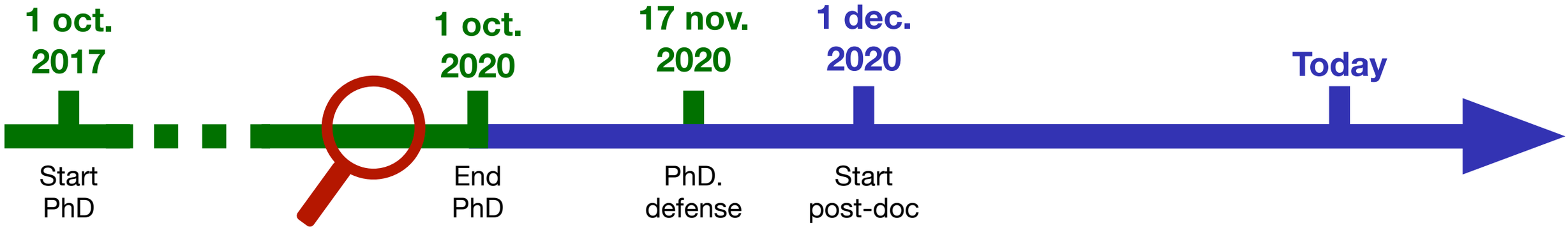
From a scientific point-of-view

- Studying a new topic
- Having more freedom
- A new organisation
- …



My post-doc from an administrative point-of-view

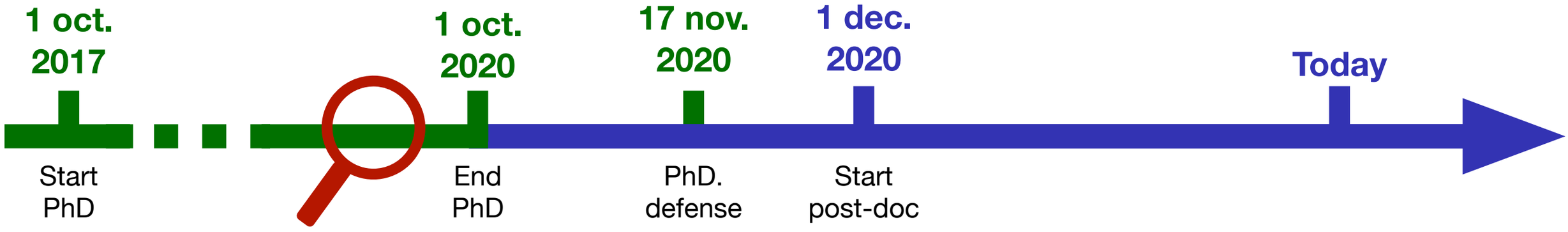
Look for a « good » post-doc



When: when you start writing the manuscript

What: what do I want to do after the phd?

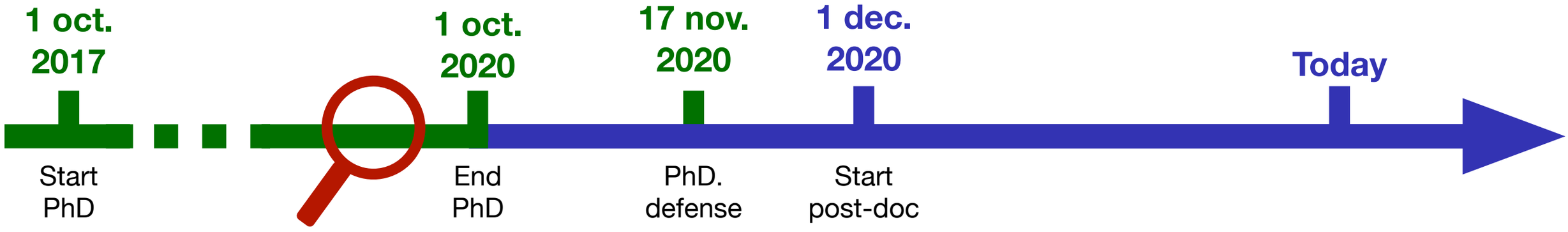
Look for a « good » post-doc



When: when you start writing the manuscript

What: what do I want to do after the phd? Academia

Look for a « good » post-doc



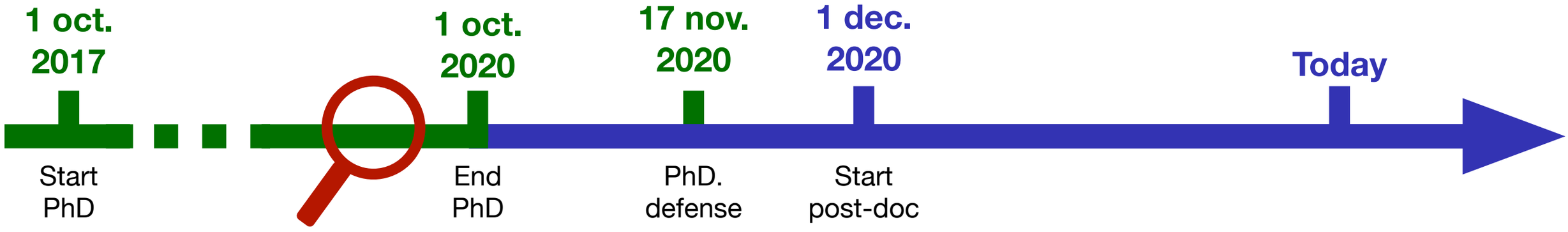
When: when you start writing the manuscript

What: what do I want to do after the phd? Academia

A « good » post-doc?

- Find a location you want to visit (better if abroad)
- Find a topic you want to investigate
- Find a « good » supervisor:
  - ➡ with whom you can work (e.g. not a ghost)
  - ➡ who is not too busy
  - ➡ who publishes

Look for a « good » post-doc



When: when you start writing the manuscript

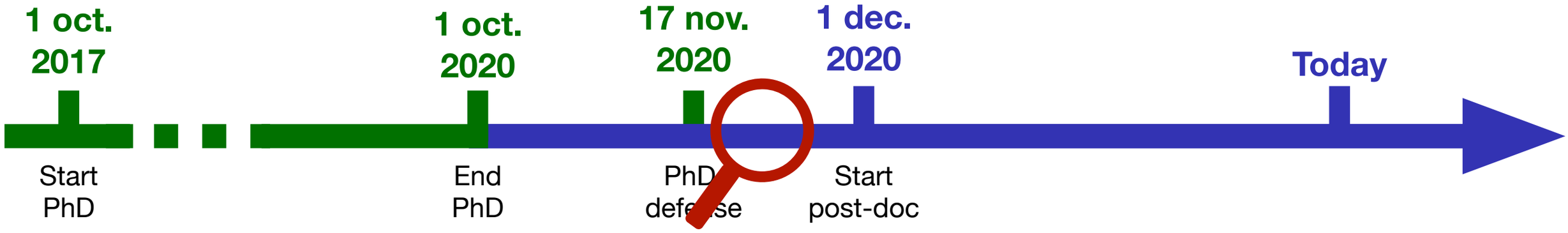
What: what do I want to do after the phd? Academia

A « good » post-doc?

- Find a location you want to visit (better if abroad)
- Find a topic you want to investigate
- Find a « good » supervisor:
  - ➡ with whom you can work (e.g. not a ghost)
  - ➡ who is not too busy
  - ➡ who publishes

Your phd advisor is probably able to give you names!

Apply for the « qualification »



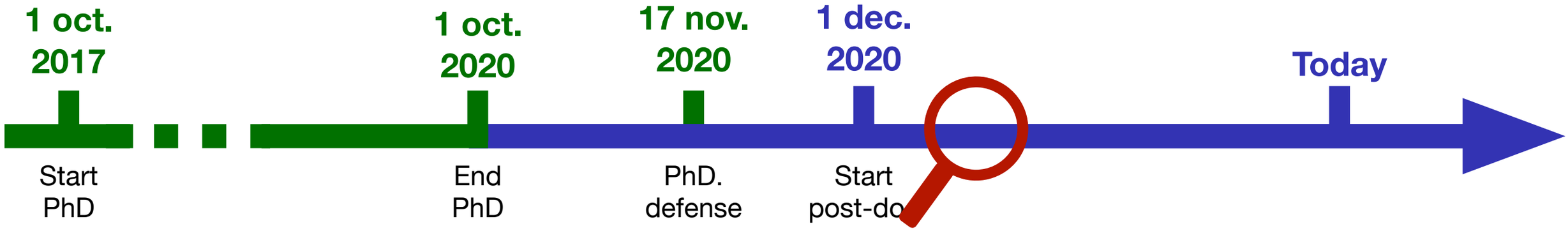
When: November/December (reg.: November 9th, app. form: December 15th)

What: gather all the supporting documents

- a detailled CV
- administrative documents about the phd defense (reviews, PV…)
- a summary of past/current research
- a summary of the teachings

https://cnu27.univ-lille.fr/qualification-note.html

Apply for a CR/MCF position

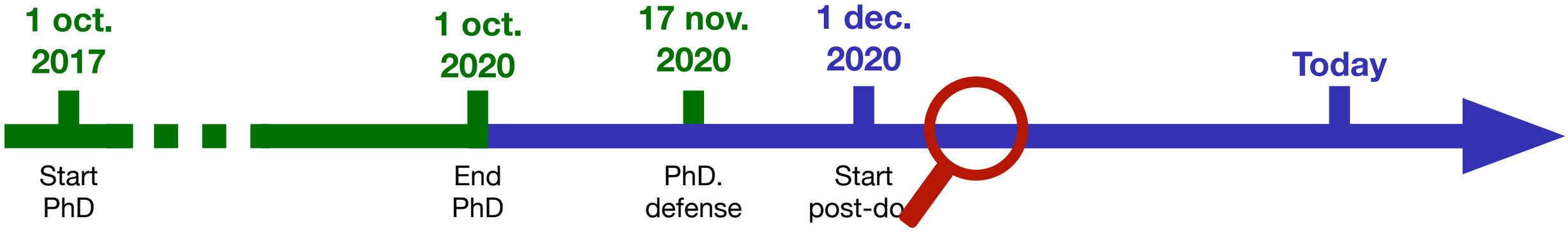


When: January-March (eligibility) and April/May (admission interview)

Main steps:

- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible

Apply for a CR/MCF position

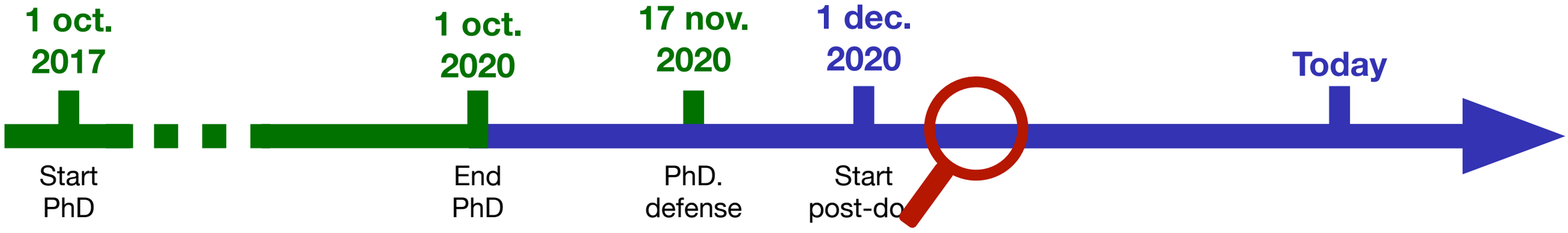


When: January-March (eligibility) and April/May (admission interview)

Main steps:

- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible
- Develop a research project
  - ➡ which problem(s) I'd like to solve in the next years?
  - ➡ why this problem(s) is interesting? Why now? Why me?

Apply for a CR/MCF position

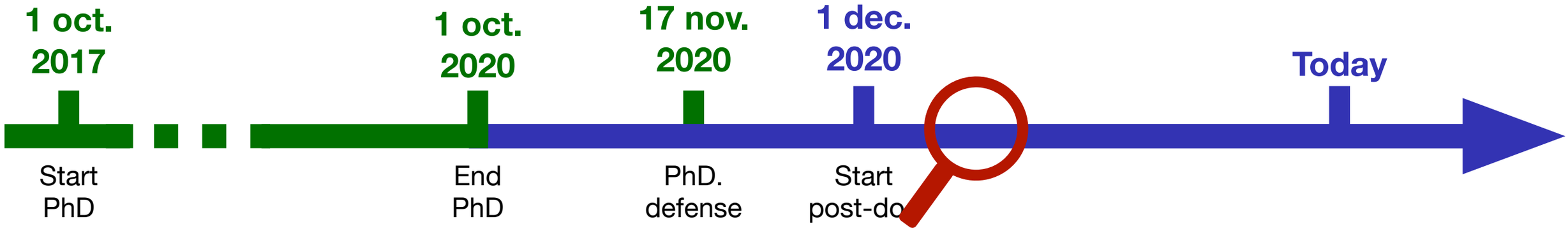


When: January-March (eligibility) and April/May (admission interview)

Main steps:

- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible
- Develop a research project
  - ➡ which problem(s) I'd like to solve in the next years?
  - ➡ why this problem(s) is interesting? Why now? Why me?
- Develop a teaching project
  - ➡ how I'd like to teach (project, MOOC, flipped classroom…)?
  - ➡ how can I meet the department expectations?

Apply for a CR/MCF position

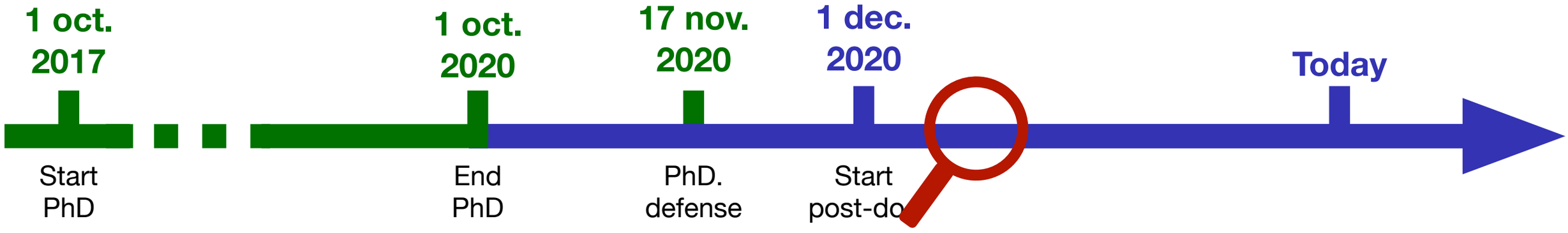


When: January-March (eligibility) and April/May (admission interview)

Main steps:

- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible
- Develop a research project
  - ➡ which problem(s) I'd like to solve in the next years?
  - ➡ why this problem(s) is interesting? Why now? Why me?
- Develop a teaching project
  - ➡ how I'd like to teach (project, MOOC, flipped classroom…)?
  - ➡ how can I meet the department expectations?
- Do a presentation
  - ➡ a short presentation (15min) but a lot of things to mention!
  - ➡ no documentation to explain the expectations…

Apply for a CR/MCF position



When: January-March (eligibility) and April/May (admission interview)

Main steps:

- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible
- Develop a research project
  - ➡ which problem(s) I'd like to solve in the next years?
  - ➡ why this problem(s) is interesting? Why now? Why me?
- Develop a teaching project
  - ➡ how I'd like to teach (project, MOOC, flipped classroom…)?
  - ➡ how can I meet the department expectations?
- Do a presentation
  - ➡ a short presentation (15min) but a lot of things to mention!
  - ➡ no documentation to explain the expectations…

Seek advice
from permanent members, post-docs…

My post-doc from a scientific point-of-view

A trendy application of security protocols

Recherche

Les Echos

CONNEXION S'ABONNER

À la une Idées Économie Politique Élections Monde Entreprises Tech-Médias Start-up Bourse Finance - Marchés Ré

Hauts-de-Seine : Neuilly-sur-Seine met en place un système de vote électronique

La mairie de Neuilly-sur-Seine va tester un système de vote électronique pour permettre aux habitants d'arbitrer des décisions local
imaginée par l'association fran

LE TEMPS

SE CONNECTER SEF

RUBRIQUES EN CONTINU BLOGS VIDÉOS CHAPPATTE MULTIMÉDIA EPAPER/PDF

Accueil › Suisse › Le vote électronique fera son retour en 2022

DROITS POPULAIRES ABONNÉ

Le vote électronique fera son retour en 2022

Après la découverte de failles en 2019, tous les projets de
pendus. La Poste a cependant
éveloppe à Neuchâtel un système
nettra à des hackers

Consulter le journal

Le Monde

Se connecter S'abonner

ACTUALITÉS ÉCONOMIE VIDÉOS OPINIONS CULTURE M LE MAG SERVICES

LES DÉCODEURS · RÉGIONALES & DÉPARTEMENTALES

Partage

Elections régionales 2021 : le vote électronique, remède à l'abstention ?

Après un premier tour marqué par une abstention historique, des membres de la majorité ont appelé à moderniser les scrutins, pour voter plus facilement, et donc de mobiliser davantage les électeurs.

Par Assma Maad et Clément Perruche

Publié le 25 juin 2021 à 18h40 - Mis à jour le 26 juin 2021 à 16h42 · Lecture 7 min.

A trendy application of security protocols but with a complex development

Recherche — Les Echos — CONNEXION — S'ABONNER

À la une | Idées | Économie | Politique | Élections | Monde | Entreprises | Tech-Médias | Start-up | Bourse | Finance - Marchés | Ré

Une faille dans le système de vote internet en Suisse

Communiqué de presse

En bref :

- Le **Crypto Group de l'UCLouvain** a effectué des **coups de sonde dans le code du système sVote** utilisé en Suisse pour le vote par internet, à la demande du gouvernement suisse.
- **Résultat ?** Il existe une **trappe dans le système**.
- **Conséquence ?** Cette faille pourrait permettre de **modifier des votes** et **produire un résultat non conforme** aux bulletins transmis par les électeurs.

Contact presse :
Pr **Olivier Pereira**, responsable du CRYPTO Group de l'UCLouvain, GSM sur demande

LE TEMPS — SE CONNECTER — SEF

RUBRIQUES | EN CONTINU | BLOGS | VIDÉOS | CHAPPATTE | MULTIMÉDIA | EPAPER/PDF

Accueil › Suisse › Le vote électronique fera son retour en 2022

OPINIONS

…e vote
…abstention ?

Après un premier tour marqué par …stention historique, des membres de la majorité ont appelé à moderniser les scrutins, pou… …us facilement, et donc de mobiliser davantage les électeurs.

Par Assma Maad et Clément Perruche

Publié le 25 juin 2021 à 18h40 - Mis à jour le 26 juin 2021 à 16h42 · Lecture 7 min.

NEWS

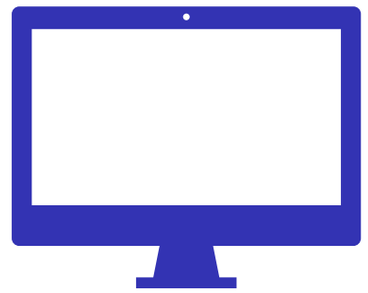
Flaw in NSW's iVote platform confirmed by researcher

By Rohan Pearce
Editor, Computerworld | NOV 14, 2019 6:08 AM PST

A security researcher has confirmed that the version of New South Wales' online voting platform, iVote, employed during the 2019 election contained a vulnerability that potentially allowed the creation of false decryption proofs for ballots.

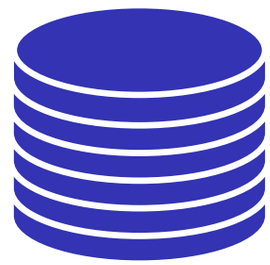
E-voting protocols

Bulletin board

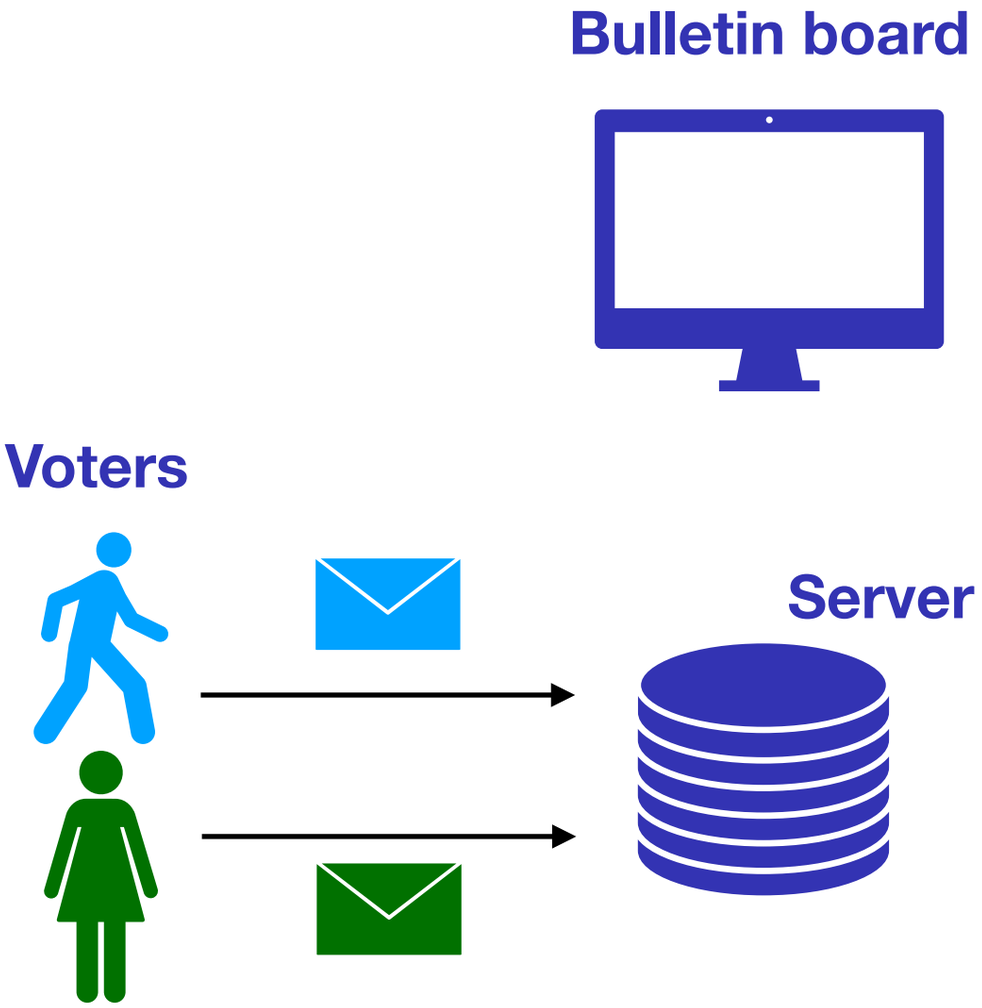


Voters

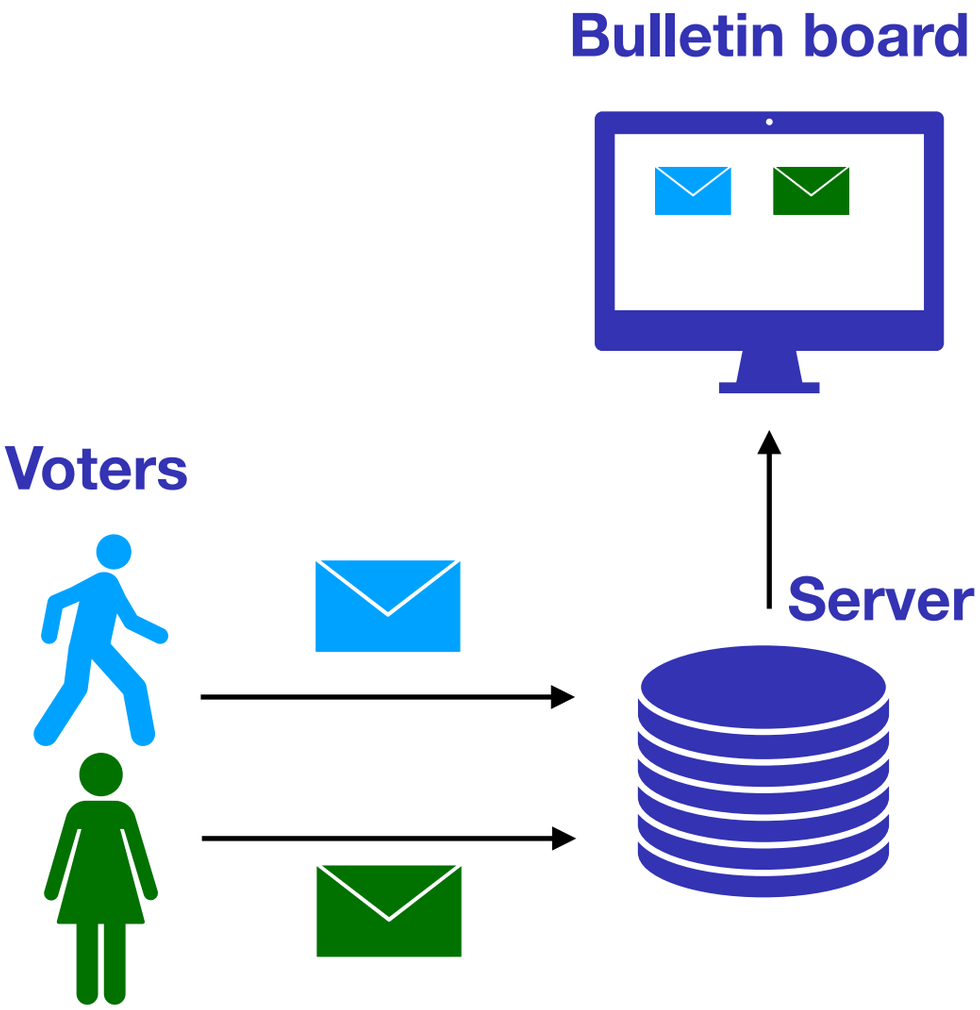
Server



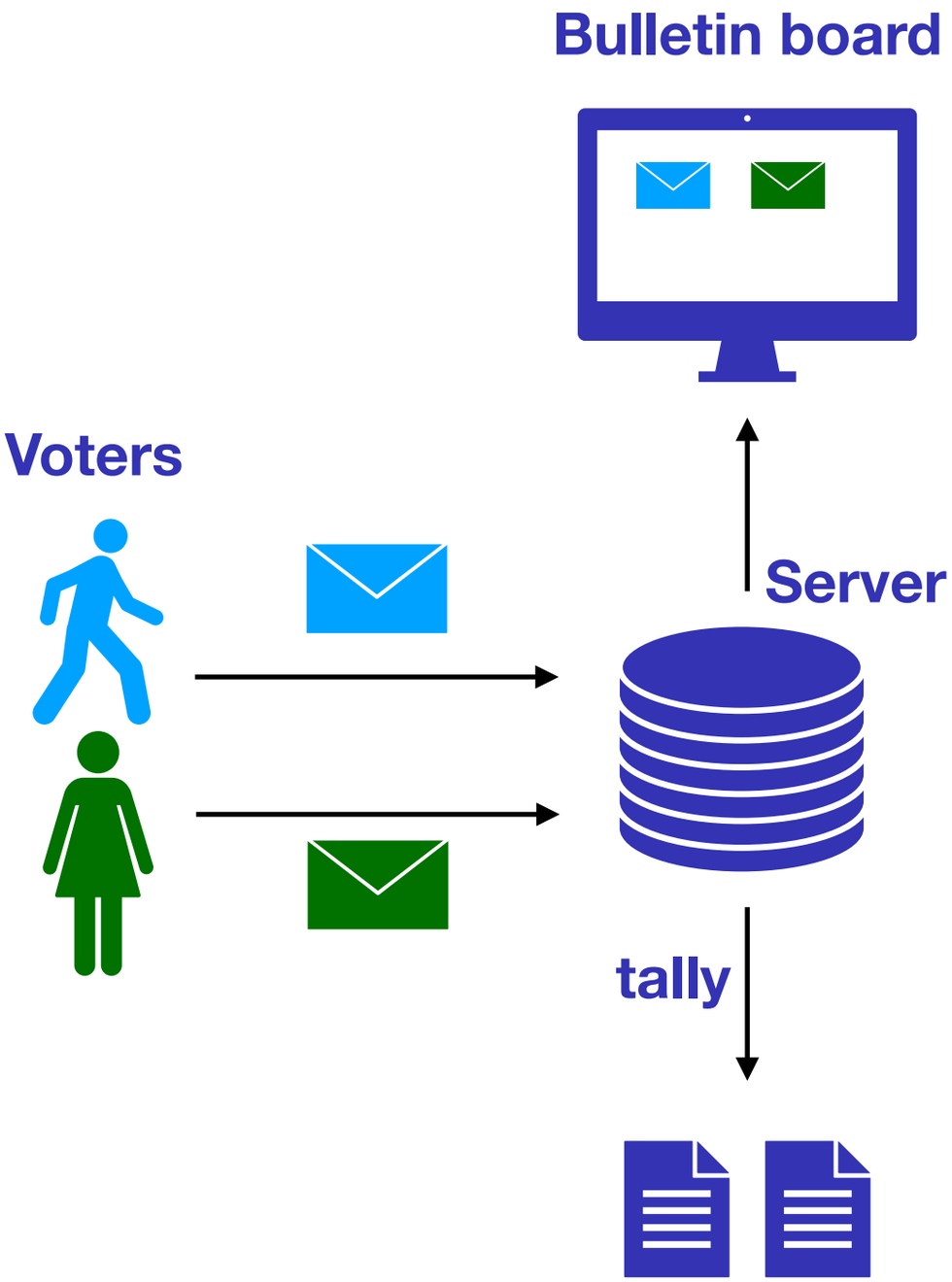
E-voting protocols



E-voting protocols



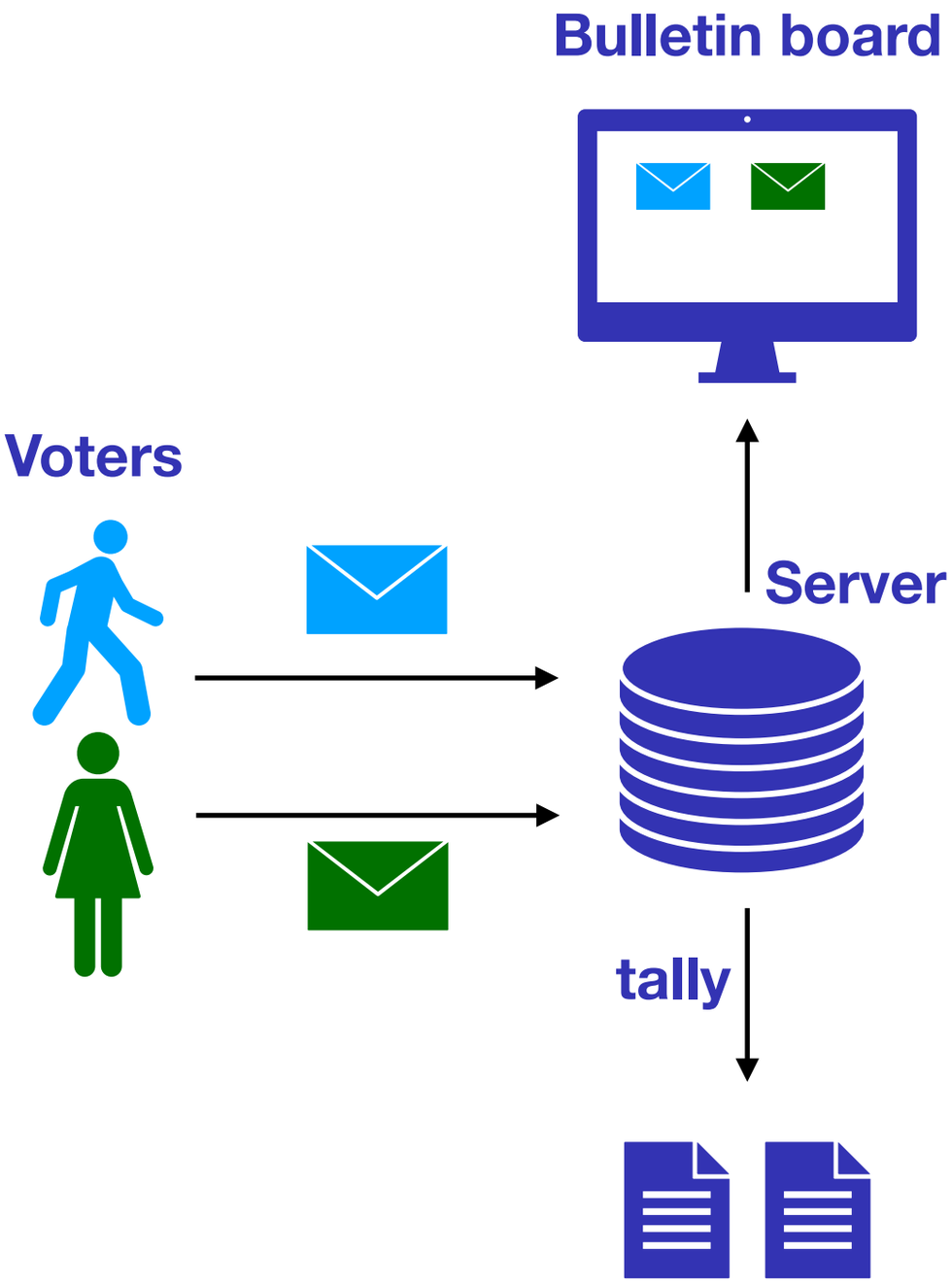
E-voting protocols



E-voting protocols

What are the expected security guarantees?

➡ Vote privacy
- no-one should know Alice/Bob votes for

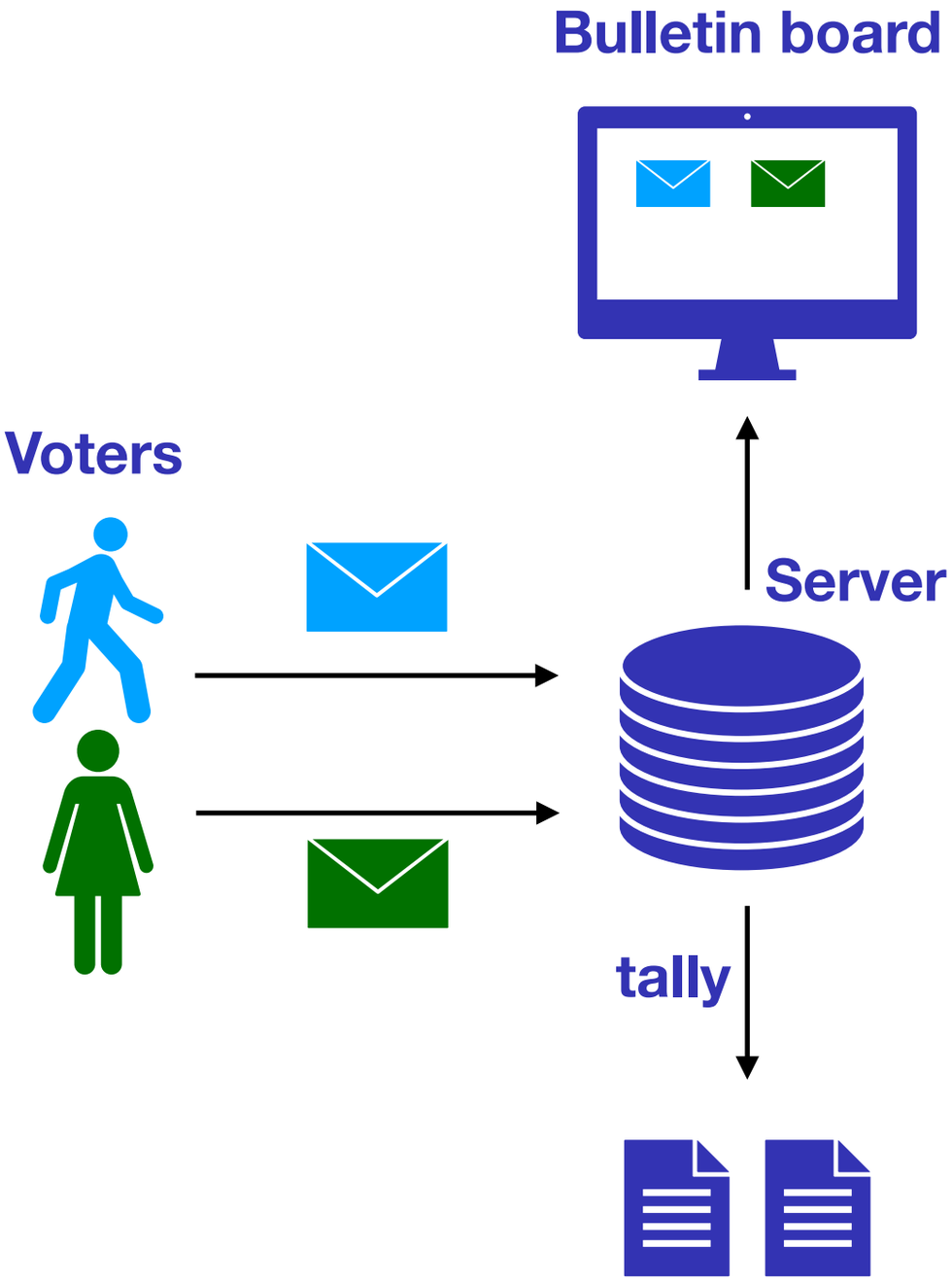


E-voting protocols

What are the expected security guarantees?

- ➡ Vote privacy
  - no-one should know Alice/Bob votes for

- ➡ Individual verifiability
  - Alice/Bob can convince themselves that his/her votes are correctly published on the bulletin board



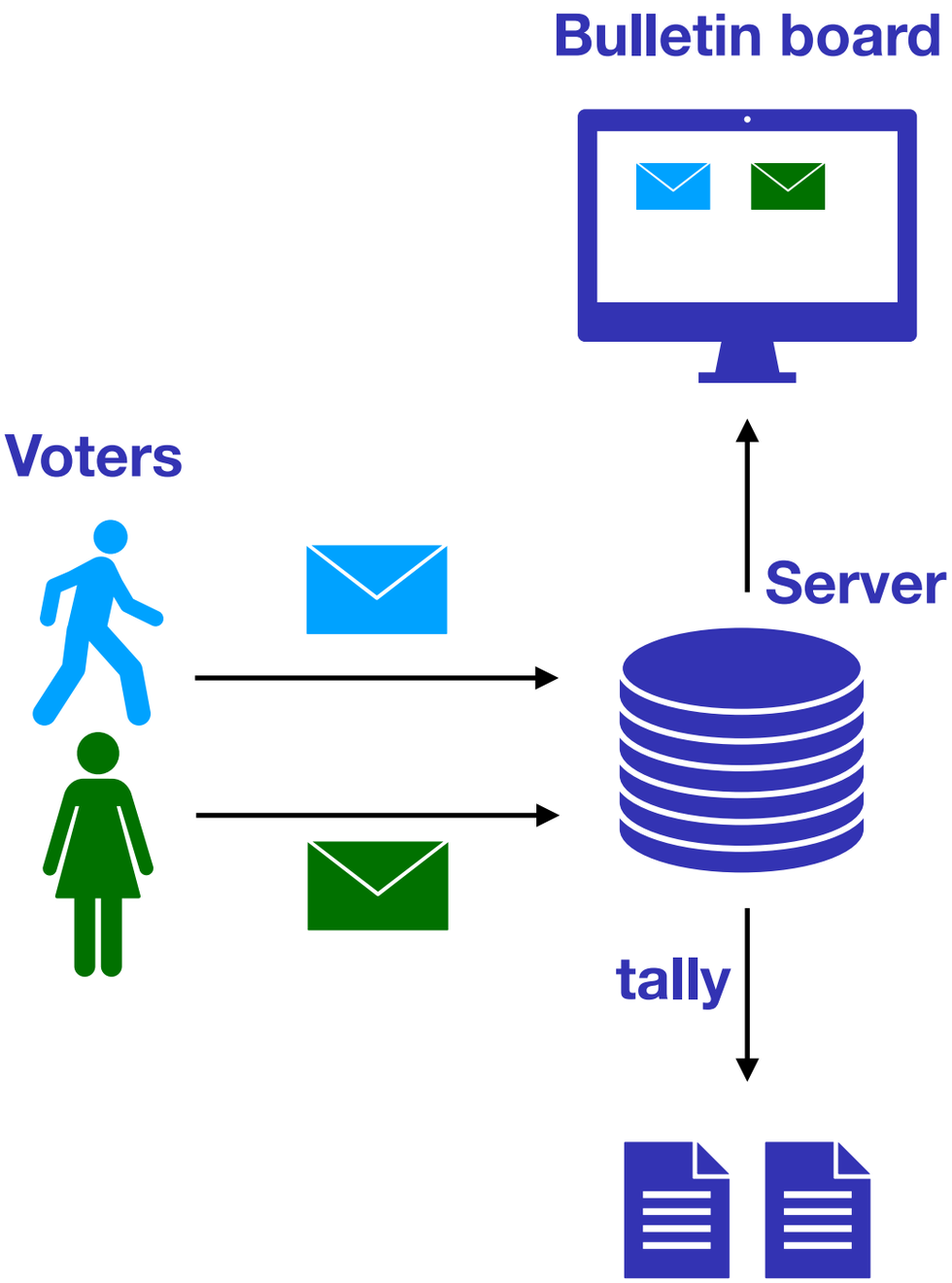
E-voting protocols

What are the expected security guarantees?

- ➡ Vote privacy
  - no-one should know Alice/Bob votes for

- ➡ Individual verifiability
  - Alice/Bob can convince themselves that his/her votes are correctly published on the bulletin board

- ➡ Universal verifiability
  - everyone can check that the result of the election corresponds to the content of the public bulletin-board



E-voting protocols

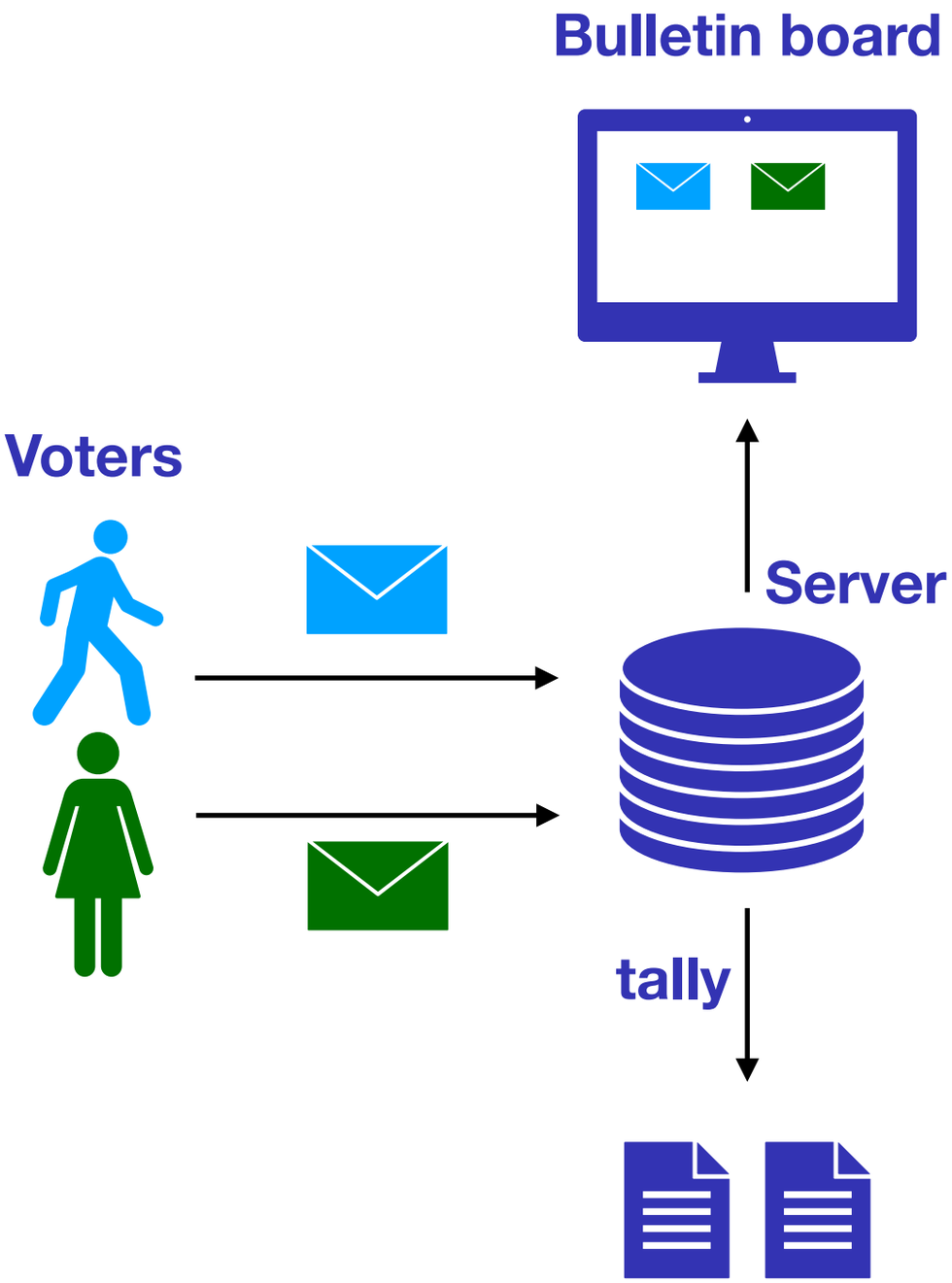
What are the expected security guarantees?

- ➡ Vote privacy
  - no-one should know Alice/Bob votes for

- ➡ Individual verifiability
  - Alice/Bob can convince themselves that his/her votes are correctly published on the bulletin board

- ➡ Universal verifiability
  - everyone can check that the result of the election corresponds to the content of the public bulletin-board

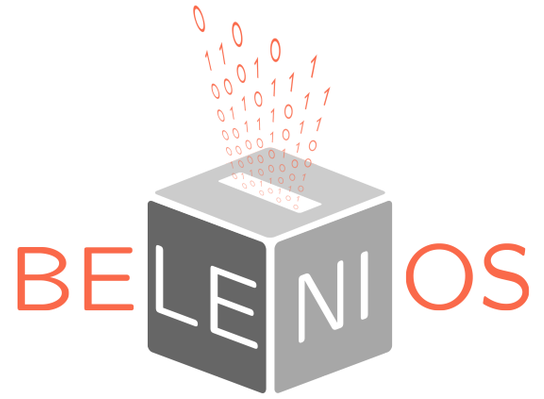
- ➡ Accountability
  - if a participant misbehaves then it can be detected and prosecuted
  - however, he can also defend himself and prove his honesty in case of false-accusation



Current work

Belenios protocol

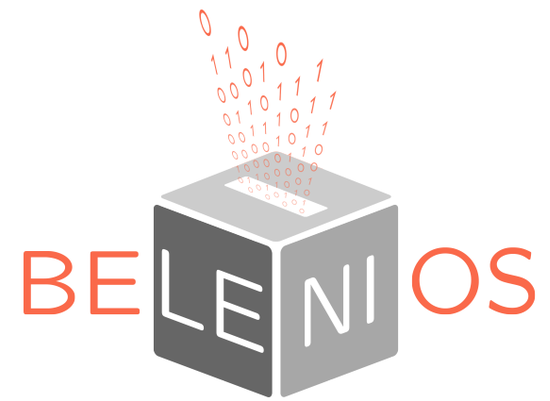
- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

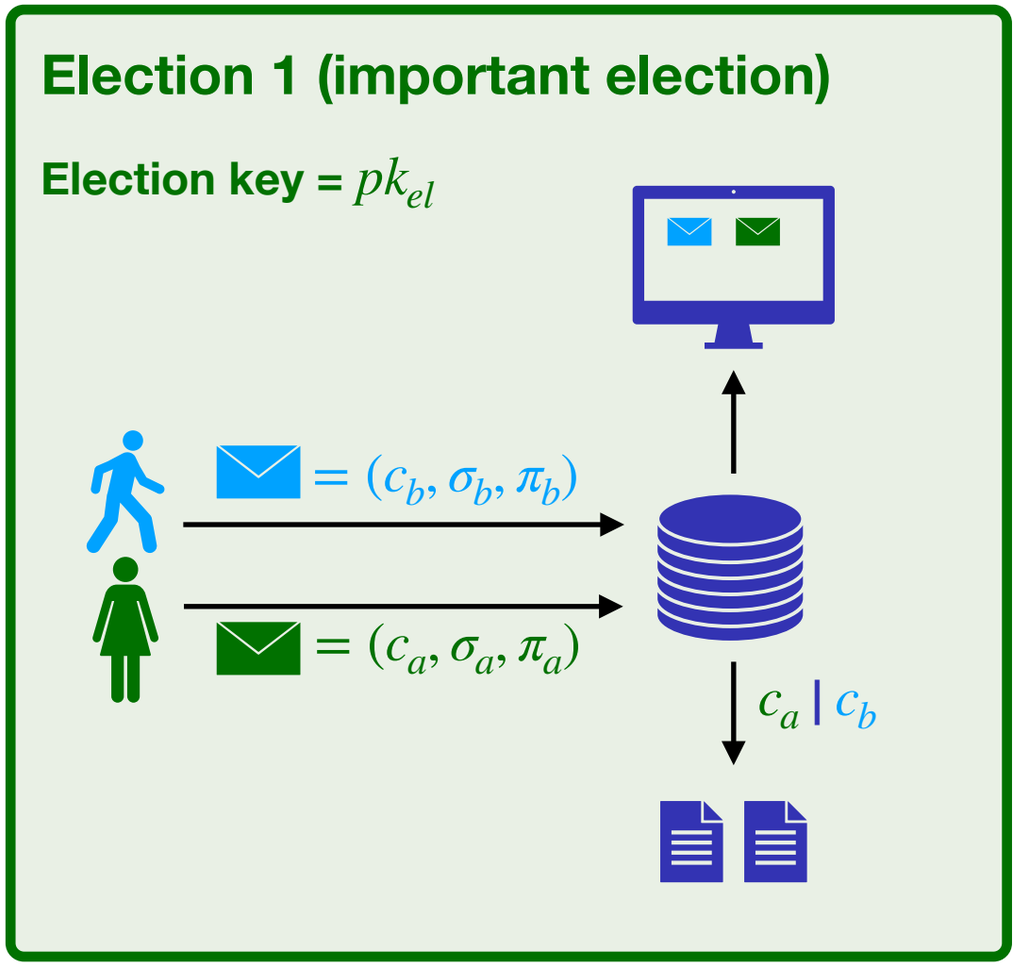


Current work

Belenios protocol

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

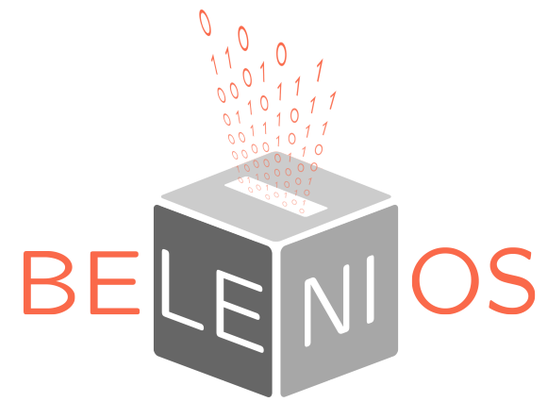


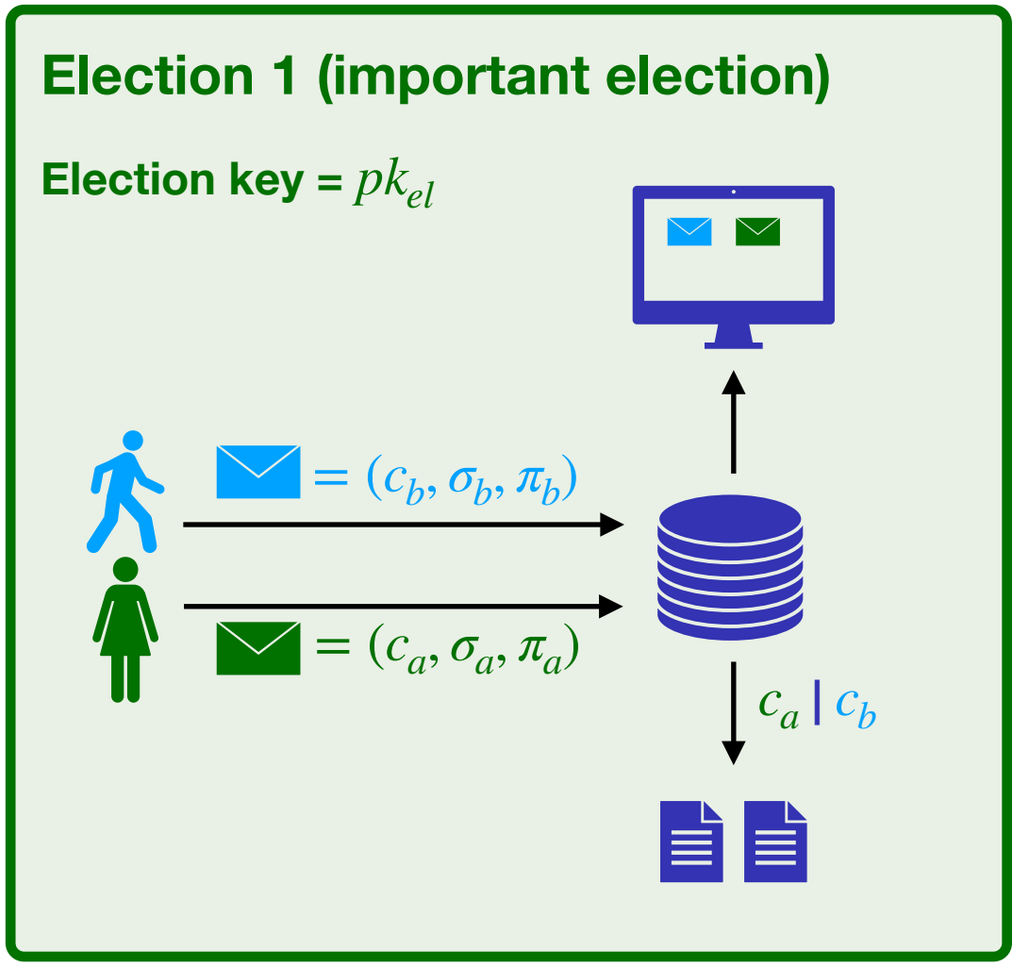


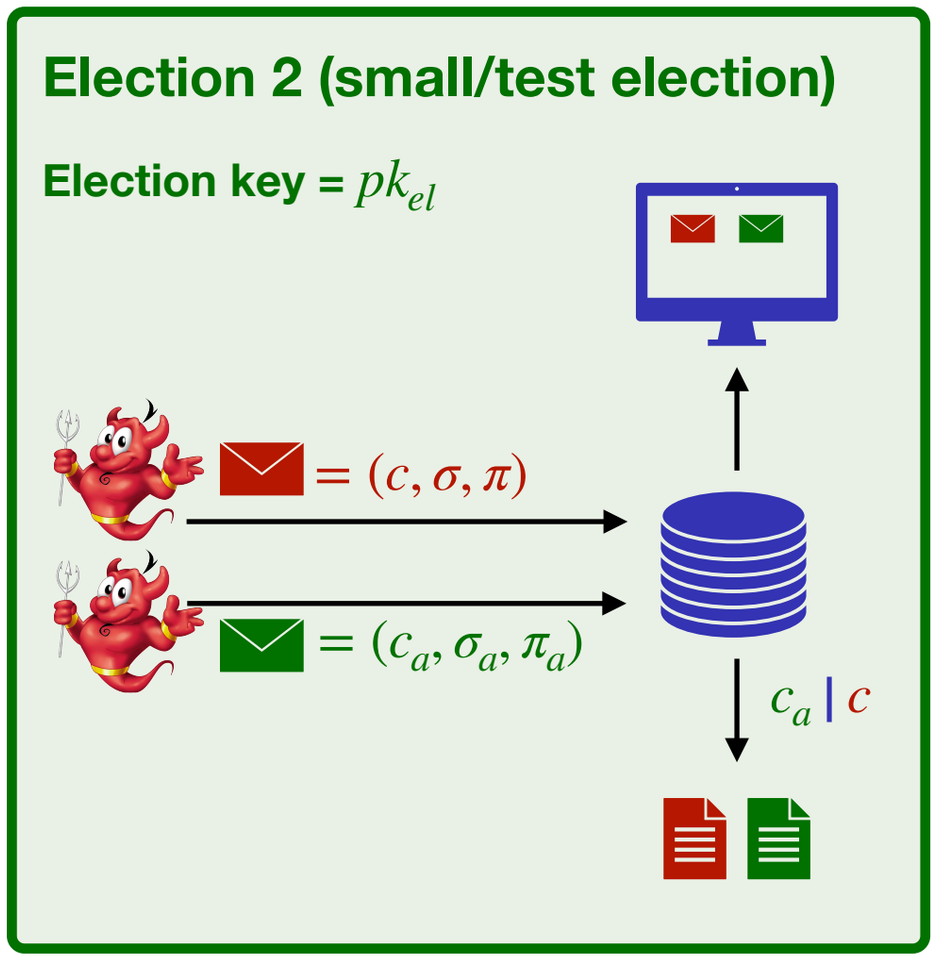
Current work

Belenios protocol

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability



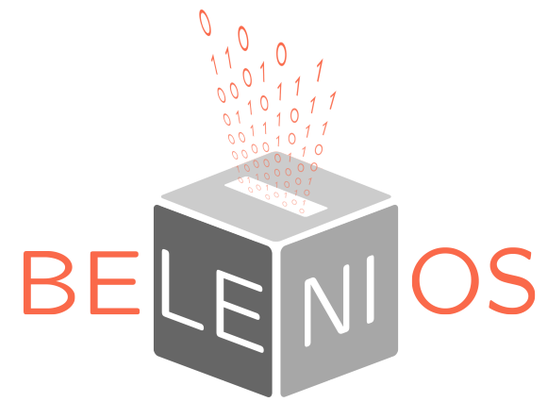


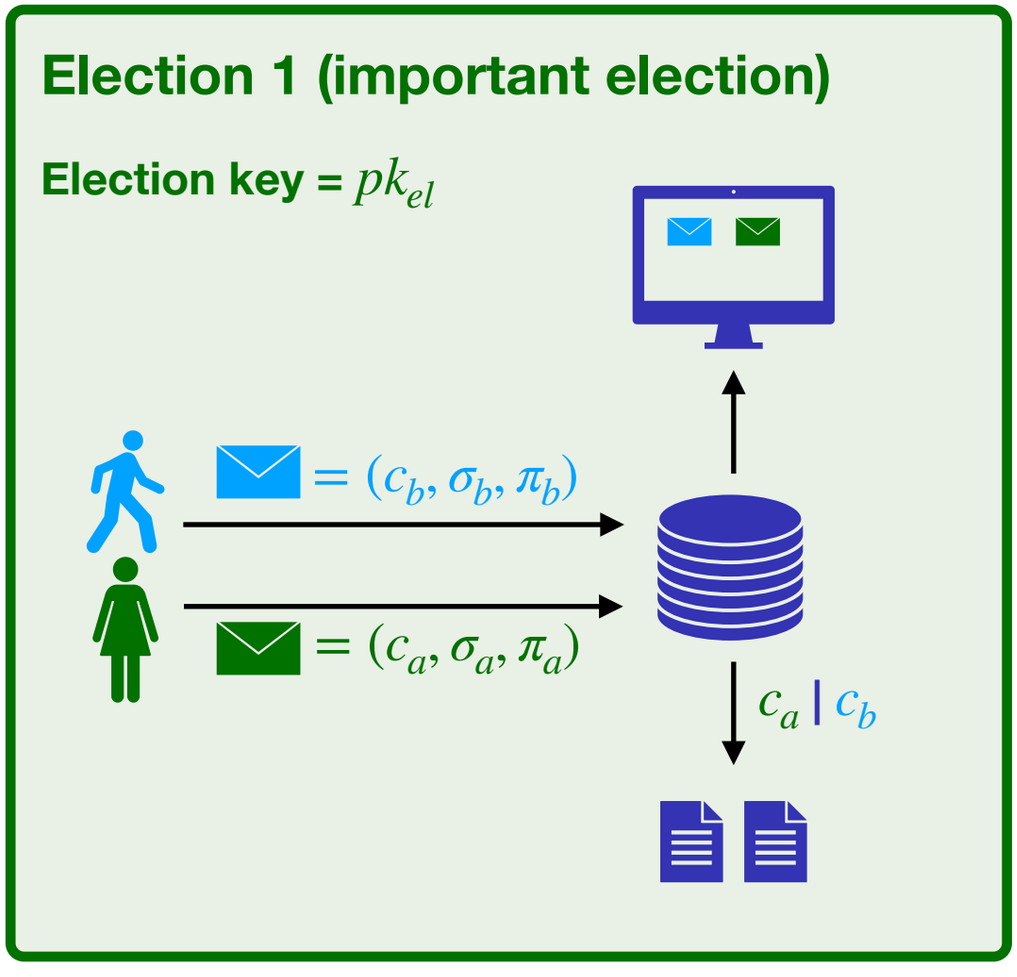


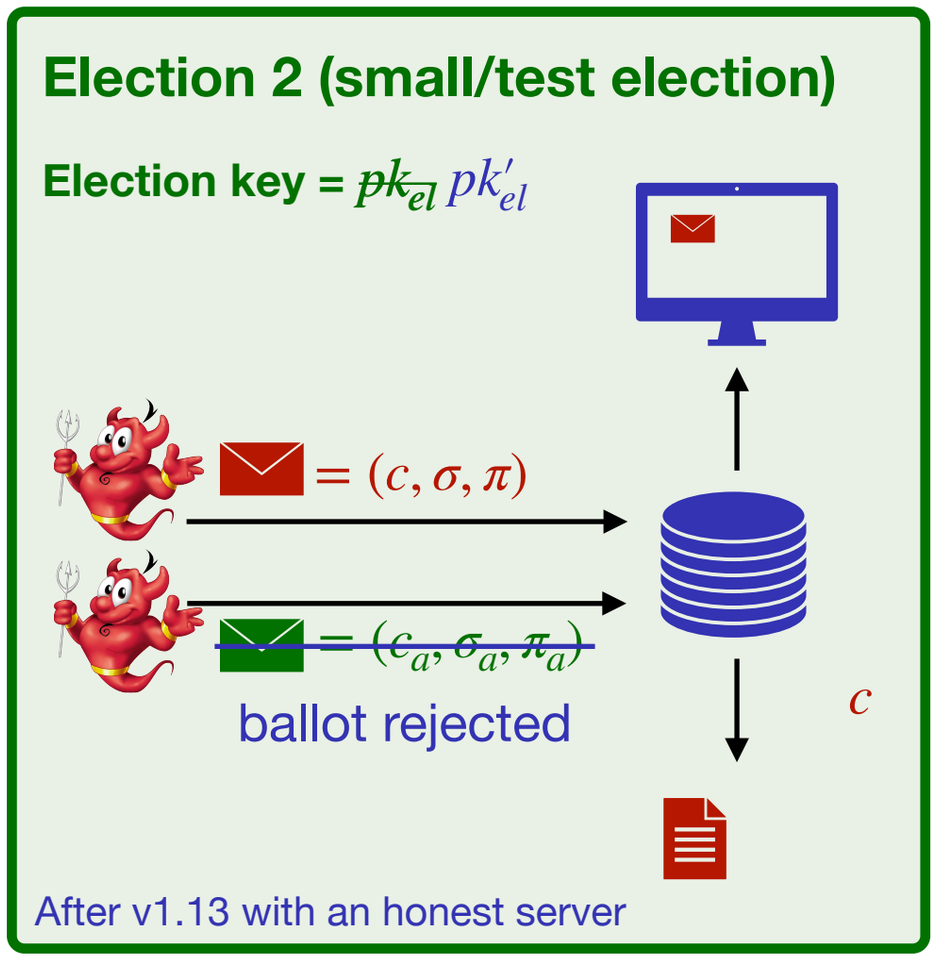
Current work

Belenios protocol

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability



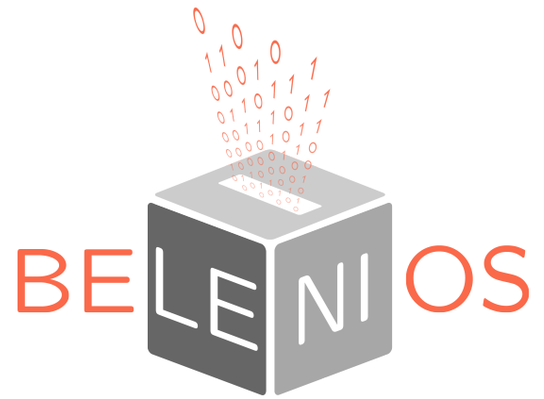




Current work

Belenios protocol

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability



IDEMIA

Themis project

- Industrial project between Idemia and Loria
- Results/contributions:
  - Design a voting machine protocol (with industrial constraints)
  - Symbolic proofs of vote secrecy, verifiability, and accountability

Current work

Belenios protocol

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

Themis project

- Industrial project between Idemia and Loria
- Results/contributions:
  - Design a voting machine protocol (with industrial constraints)
  - Symbolic proofs of vote secrecy, verifiability, and accountability

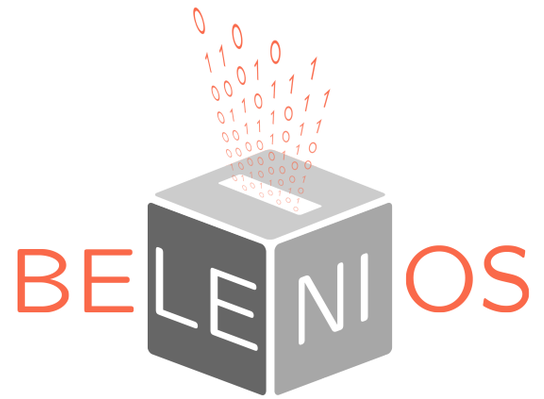
Swiss Post's e-voting solution

- Industrial protocol developed by Scytl and now Swiss Post (expected to be deployed in 2022)
- Results/contributions:
  - Adapt the symbolic proofs to the new version of the specification

Current work

Belenios protocol

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability



IDEMIA

Themis project

- Industrial project between Idemia and Loria
- Results/contributions:
  - Design a voting machine protocol (with industrial constraints)
  - Symbolic proofs of vote secrecy, verifiability, and accountability

Swiss Post's e-voting solution

- Industrial protocol developed by Scytl and now Swiss Post (expected to be deployed in 2022)
- Results/contributions:
  - Adapt the symbolic proofs to the new version of the specification
  - We discovered a (critical?) vote privacy flaw…

SWISS POST

Conclusion

From an administrative point-of-view

- Do not hesitate to contact the teams
- Do not hesitate to discuss with researchers you trust to get advices
- Do not underestimate the work/time that an application requires!

Conclusion

From an administrative point-of-view

- Do not hesitate to contact the teams
- Do not hesitate to discuss with researchers you trust to get advices
- Do not underestimate the work/time that an application requires!

From a scientific point-of-view

- Designing a secure e-voting protocol is complex
- Considering multiple elections is necessary!

➡ Much work is still needed to obtain a (reasonably) secure e-voting protocol…

Conclusion

From an administrative point-of-view

- Do not hesitate to contact the teams
- Do not hesitate to discuss with researchers you trust to get advices
- Do not underestimate the work/time that an application requires!

From a scientific point-of-view

- Designing a secure e-voting protocol is complex
- Considering multiple elections is necessary!

➡ Much work is still needed to obtain a (reasonably) secure e-voting protocol…

Thank you!