How to analyse real-world e-voting protocols?

Alexandre Debant

Université de Lorraine, CNRS, Inria, LORIA,
Nancy, France

Clermont-Ferrand, February 10th 2022

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Inria

A trendy sort 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 sort 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.

Outline

1. **Belenios: a real-world protocol**
   - description of the protocol
   - expected security properties

2. **Existing attacks and new fixes**

3. **Multi-elections… a real threat…**
   - a new attack against Belenios
   - the Swiss-Post protocol: another victim

4. **Studying new security properties**
   - cast-as-intended
   - accountability

Outline

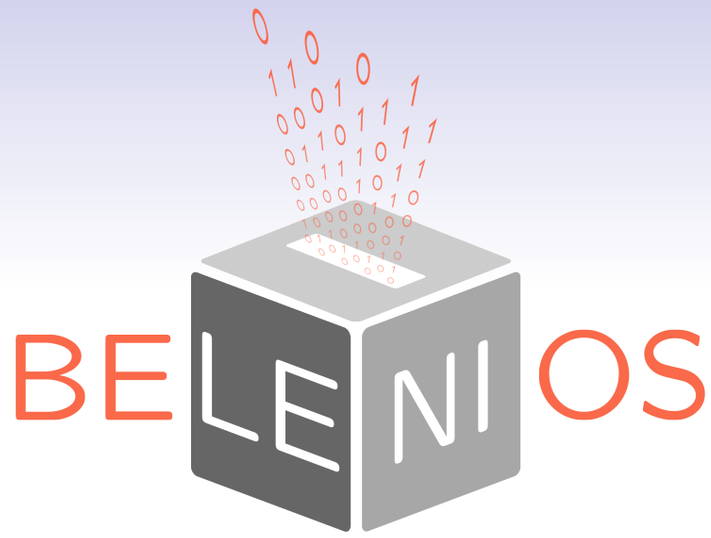
1. **Belenios: a real-world protocol**
   - description of the protocol
   - expected security properties

2. **Existing attacks and new fixes**

3. **Multi-elections… a real threat…**
   - a new attack against Belenios
   - the Swiss-Post protocol: another victim

4. **Studying new security properties**
   - cast-as-intended
   - accountability

Belenios



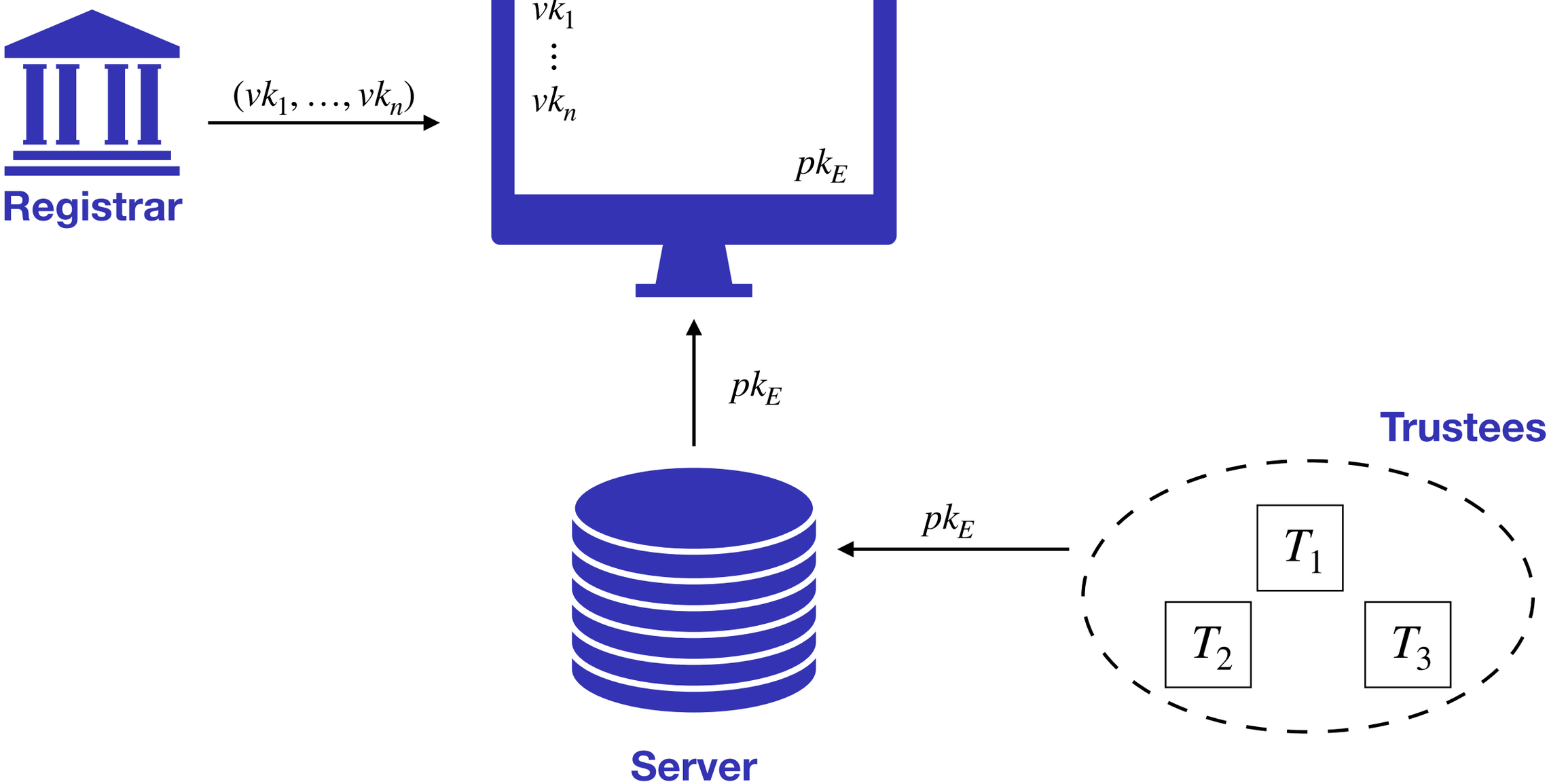
General information

- developers: Véronique Cortier, Pierrick Gaudry, Stéphane Glondu
- context: developed for associative or professional elections
- +1400 elections in 2020, +100 000 ballots
- multi-languages platform: French, English, Spanish…

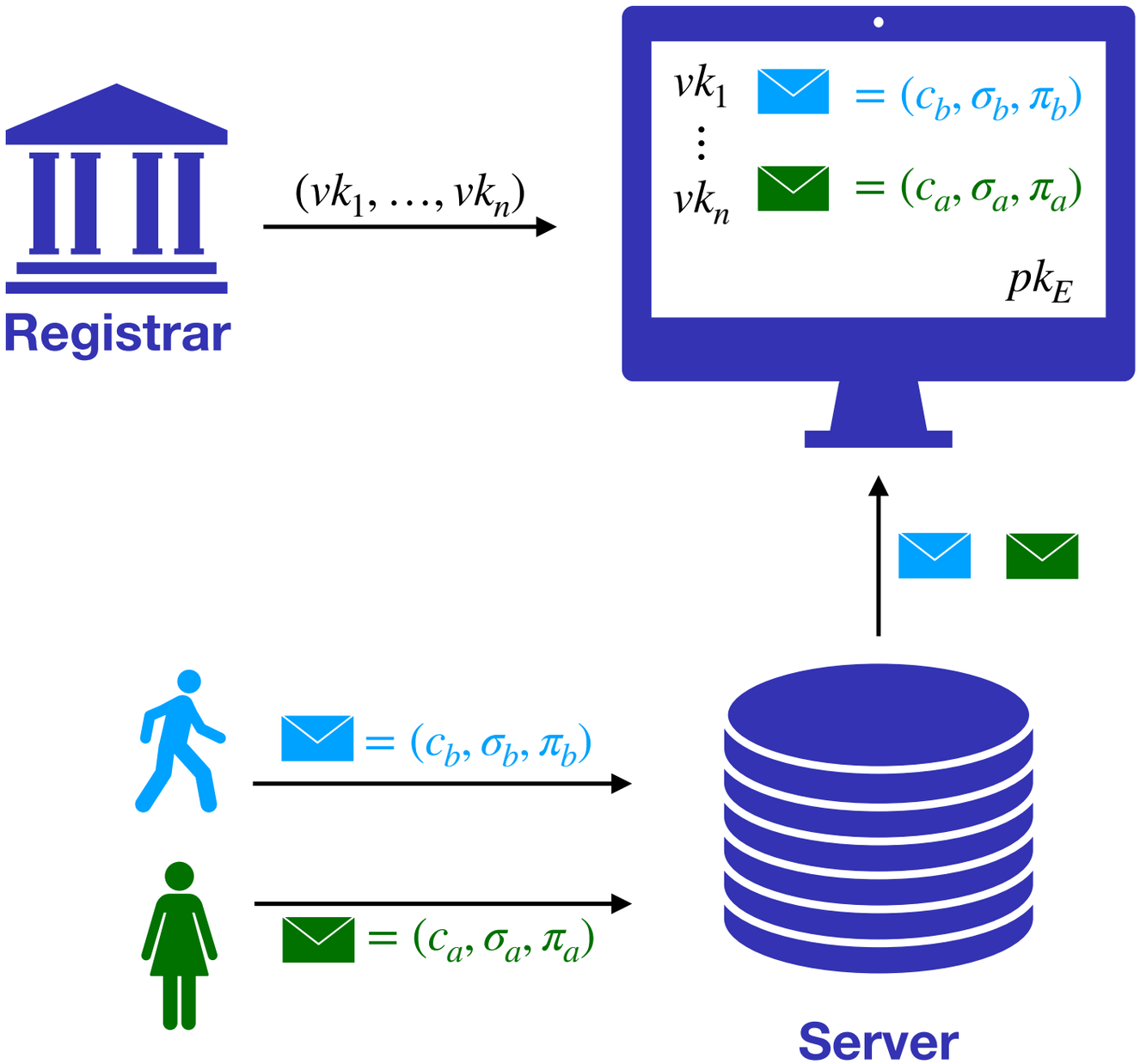
Technical details

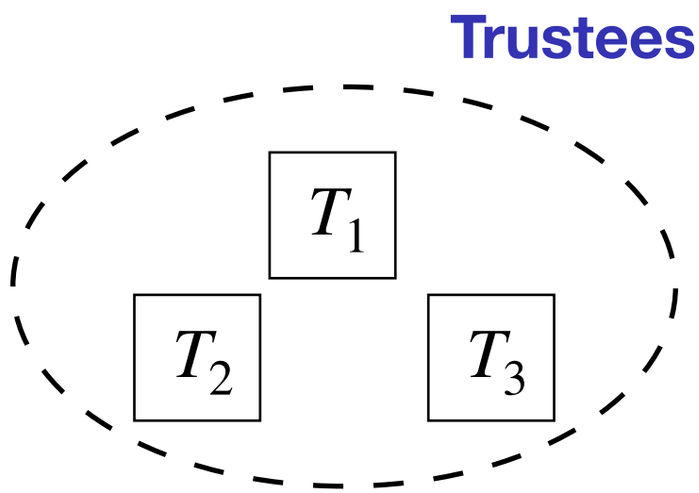
- re-vote
- homomorphic tally and/or mixnets
- threshold decryption
- vote secrecy as soon as **k out of n** decryption trustees are honest
- verifiability as soon as the registrar **or** the voting server is honest

How it works? (setup phase)

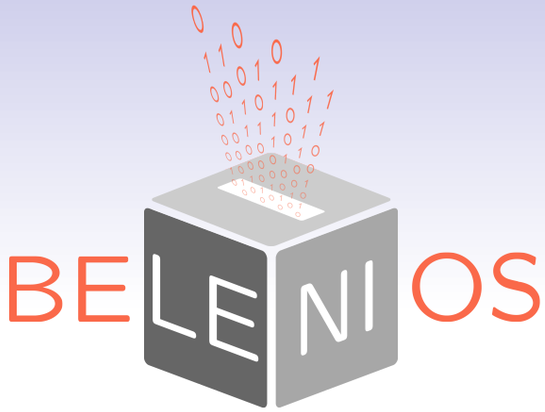


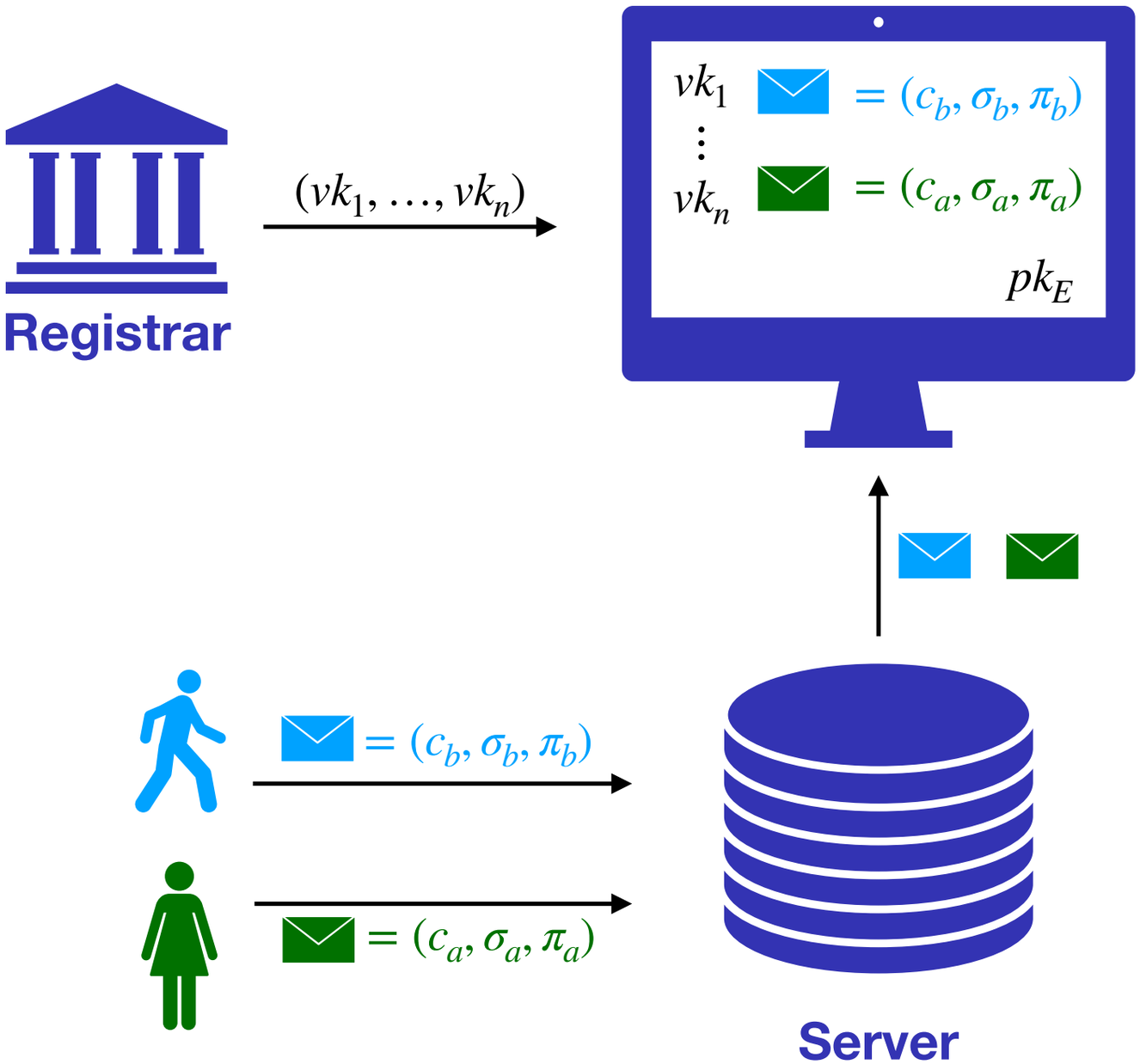
How it works? (voting phase)



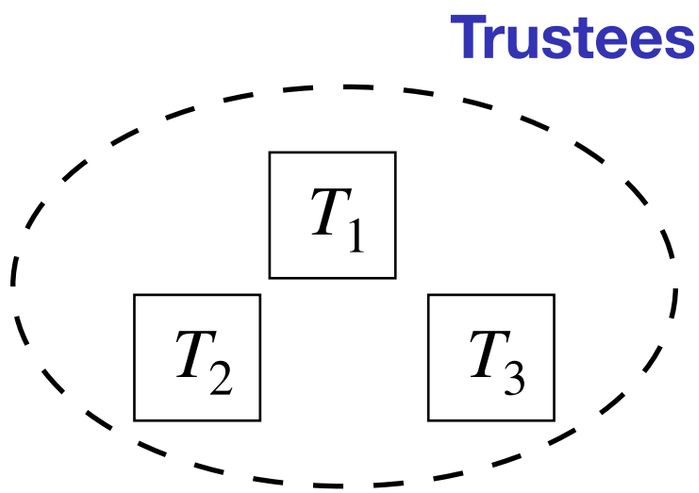


How it works? (voting phase)

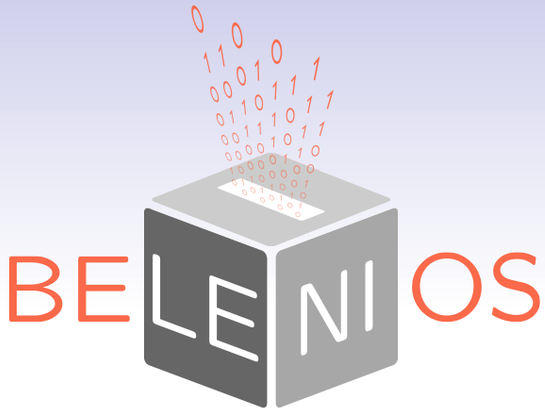


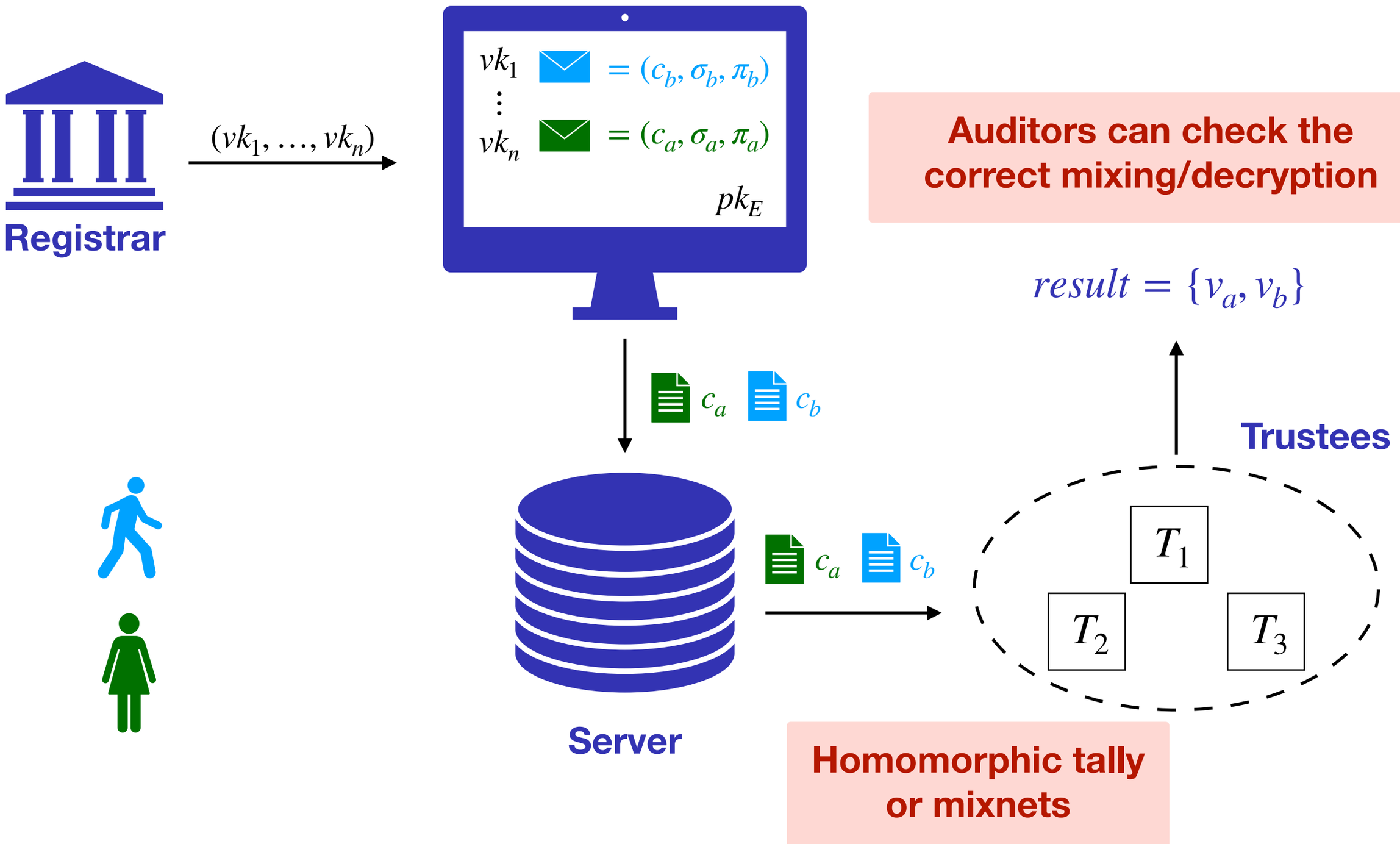


Auditors can check the validity of the ballots



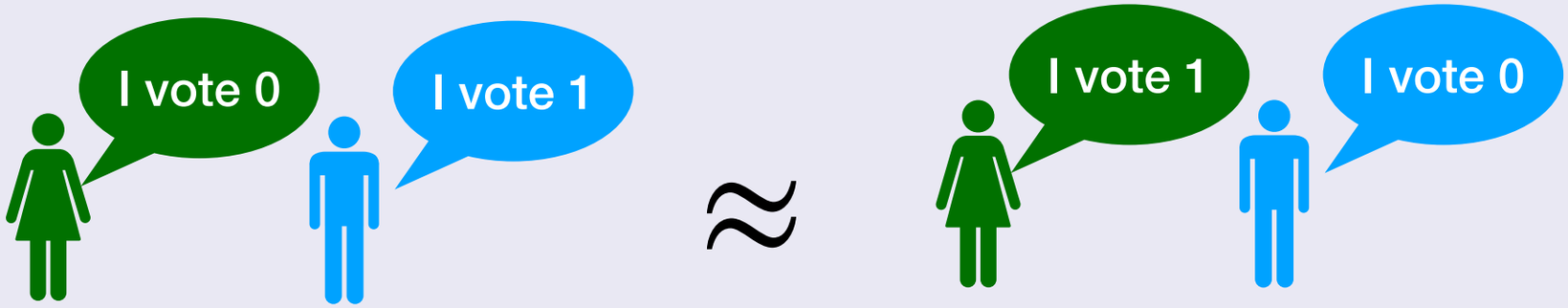
How it works? (tally phase)





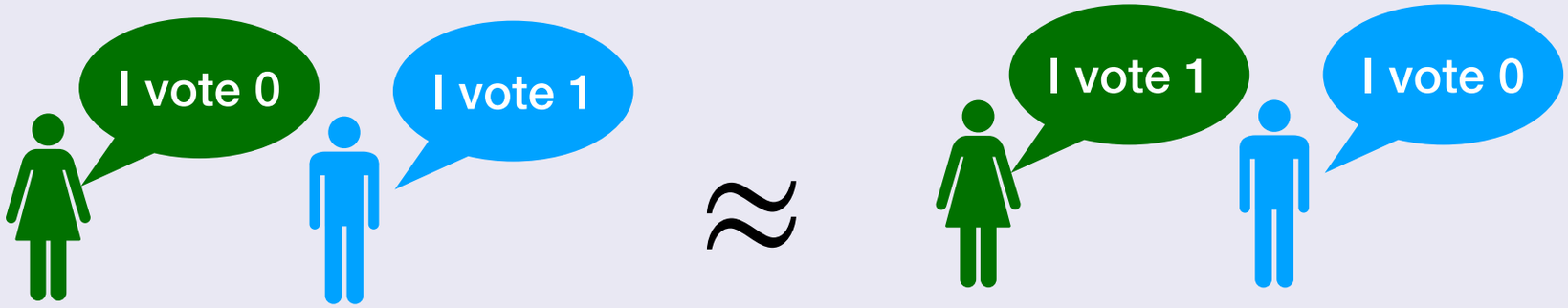
Security properties

Vote secrecy - no one is able to learn who I voted for!



Security properties

Vote secrecy - no one is able to learn who I voted for!

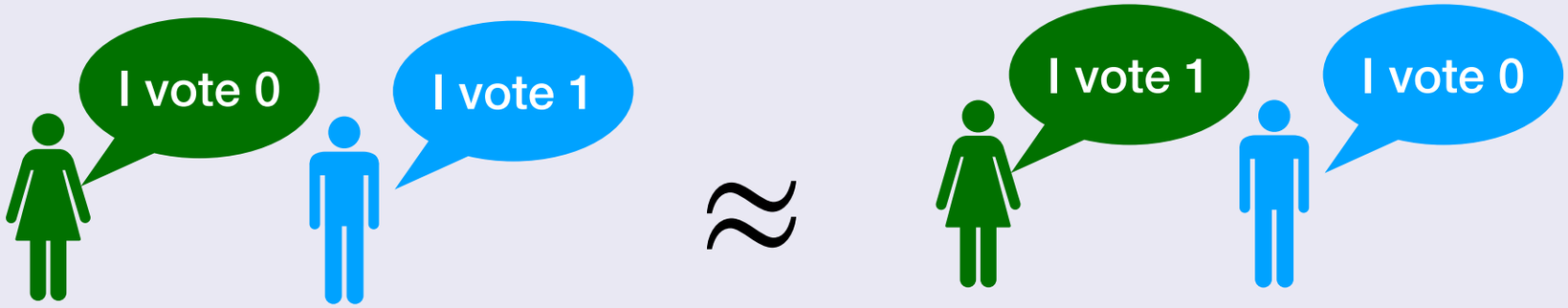


Verifiability - no one is able to modify the result of an election!

- Eligibility: all the counted ballots belong to legitimate voters
- Individual verifiability: if I see my last ballot on the bulletin board, it will be counted
- Universal verifiability: the result corresponds to the content of the ballot box

Security properties

Vote secrecy - no one is able to learn who I voted for!



Verifiability - no one is able to modify the result of an election!

- Eligibility: all the counted ballots belong to legitimate voters
- Individual verifiability: if I see my last ballot on the bulletin board, it will be counted
- Universal verifiability: the result corresponds to the content of the ballot box

Many others… cast-as-intended, coercion-resistance, accountability…

What about Belenios?

Technical details

- vote secrecy as soon as **k out of n** decryption trustees are honest
- verifiability as soon as the registrar **or** the voting server is honest

What about Belenios?

Technical details

- vote secrecy as soon as **k out of n** trustees are honest
- verifiability as soon as the re… voting server is honest

Such claims require proofs!

5.1.1	Examination criteria: The protocol must meet the security objective according to the trust assumptions in the abstract model in accordance with Section 4. In addition, a cryptographic and a symbolic proof must be provided. The proofs relating to cryptographic basic components may be provided according to generally accepted security assumptions (for example, the "random oracle model", "decisional Diffie-Hellman assumption", "Fiat-Shamir heuristic"). The protocol should be based if possible on existing and proven protocols.

Swiss Federal Chancellery

Two major families of models…

… with some advantages and some drawbacks.

Computational models

\+ messages are bitstrings, a general and powerful attacker

– tedious proofs, sometimes mechanized, but often hand-written

Symbolic models

– Some abstractions (messages, attacker…)

\+ procedures and automated tools

Some results make a link between these two models
[Abadi & Rogaway - 2000]

Two major families of models…

… with some advantages and some drawbacks.

Computational models

\+ messages are bitstrings, a general and powerful attacker

– tedious proofs, sometimes mechanized, but often hand-written

Symbolic models

– Some abstractions (messages, attacker…)

\+ procedures and automated tools

Some results make a link between these two models
[Abadi & Rogaway - 2000]

Outline

1. **Belenios: a real-world protocol**
   - description of the protocol
   - expected security properties

2. **Existing attacks and new fixes**

3. **Multi-elections… a real threat…**
   - a new attack against Belenios
   - the Swiss-Post protocol: another victim

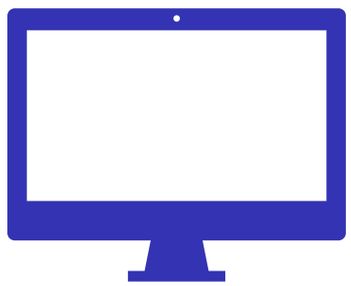
4. **Studying new security properties**
   - cast-as-intended
   - accountability

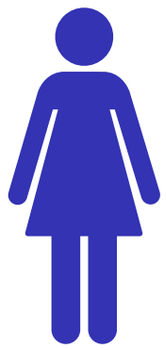
Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Honest scenario



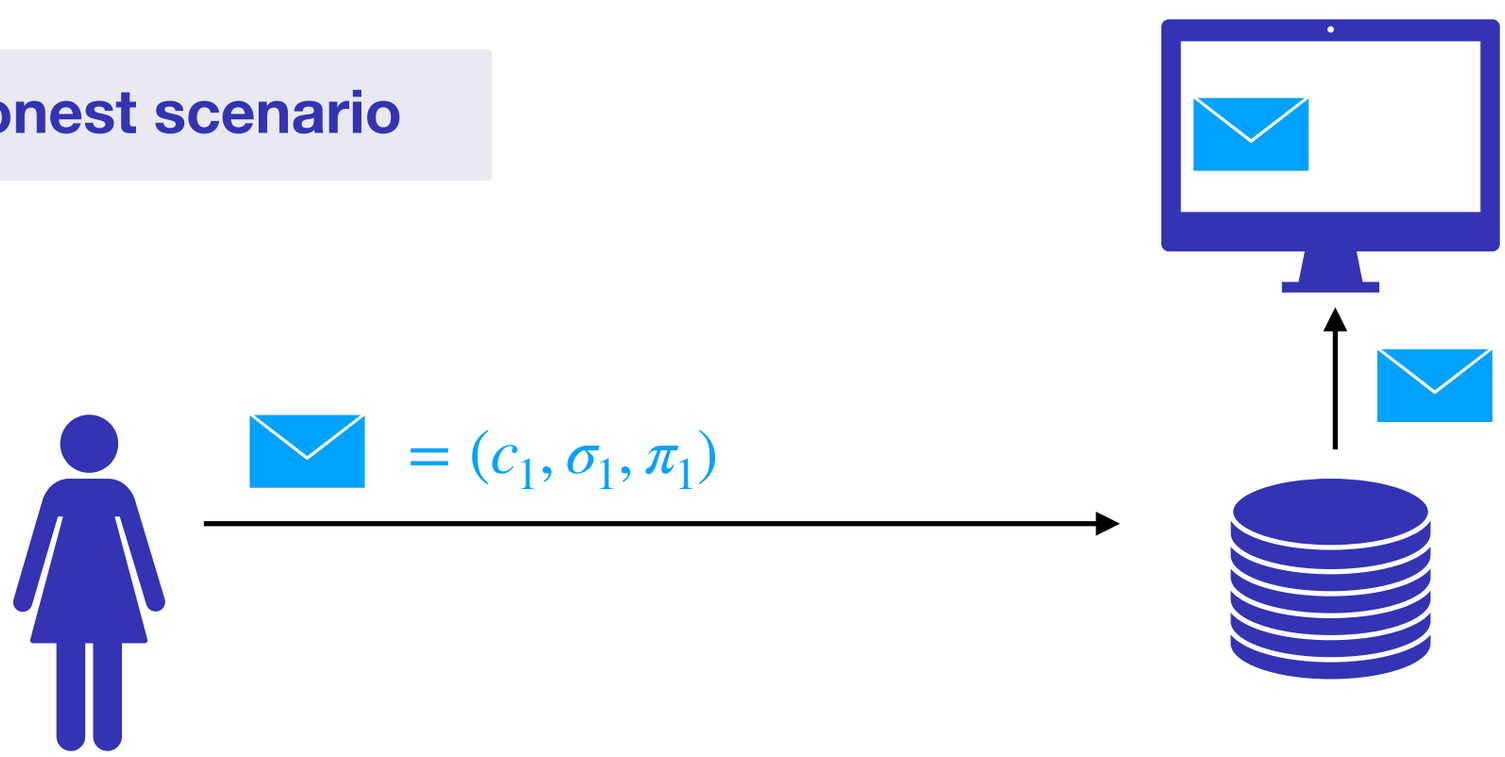


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Honest scenario

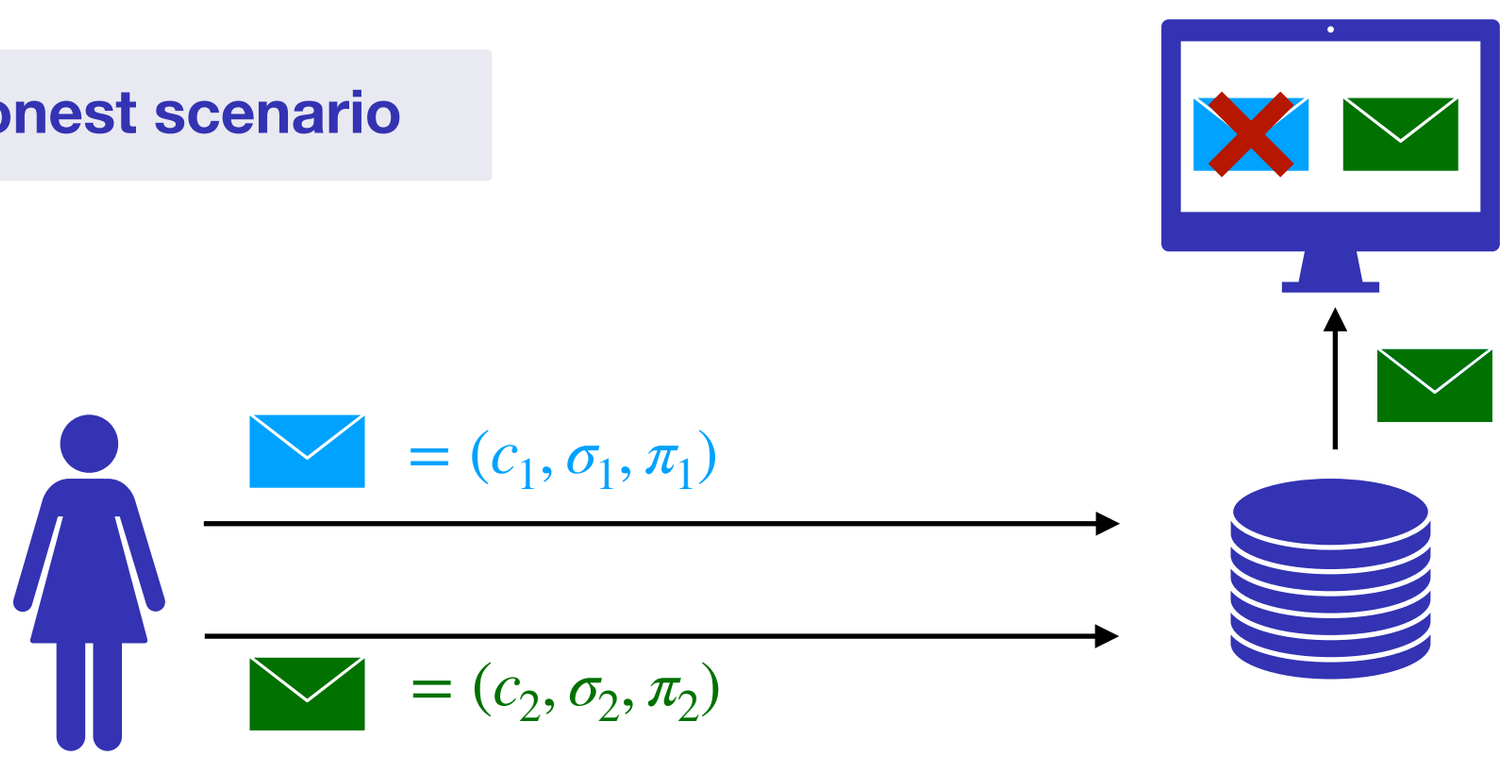


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Honest scenario

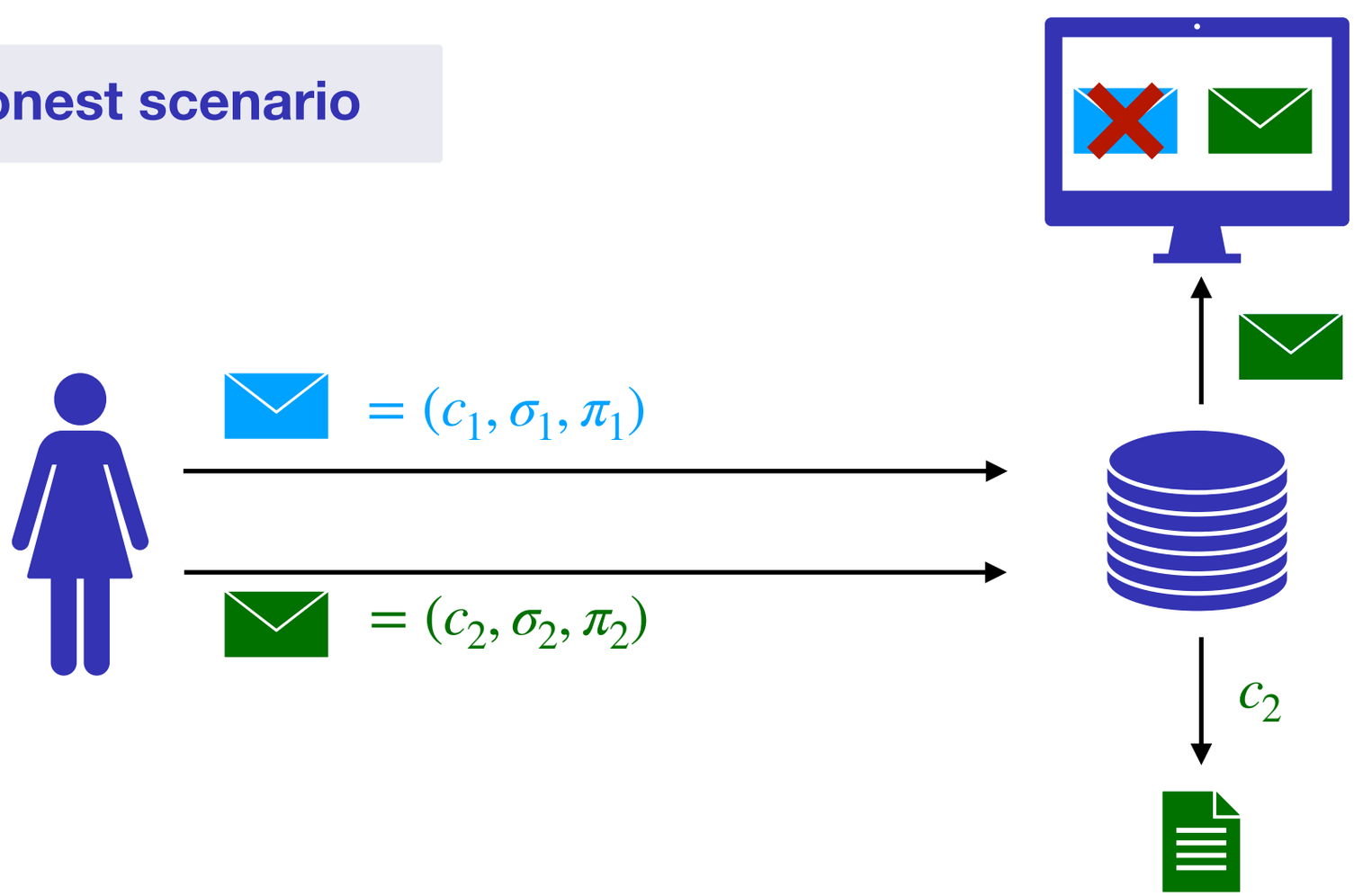


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Honest scenario

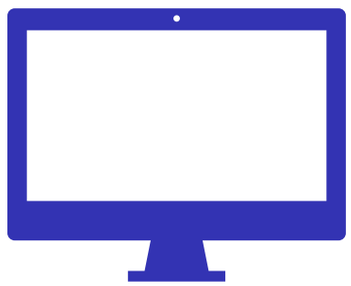


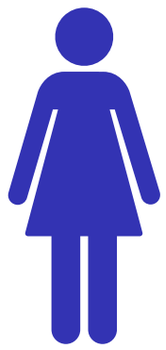
Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Attack scenario



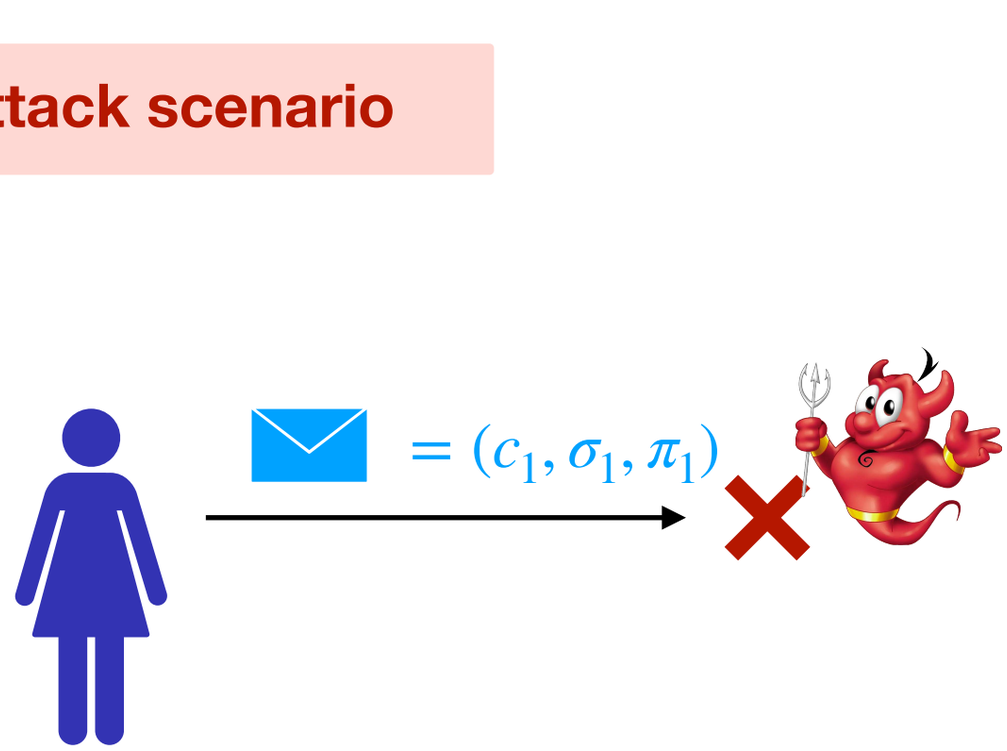


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Attack scenario

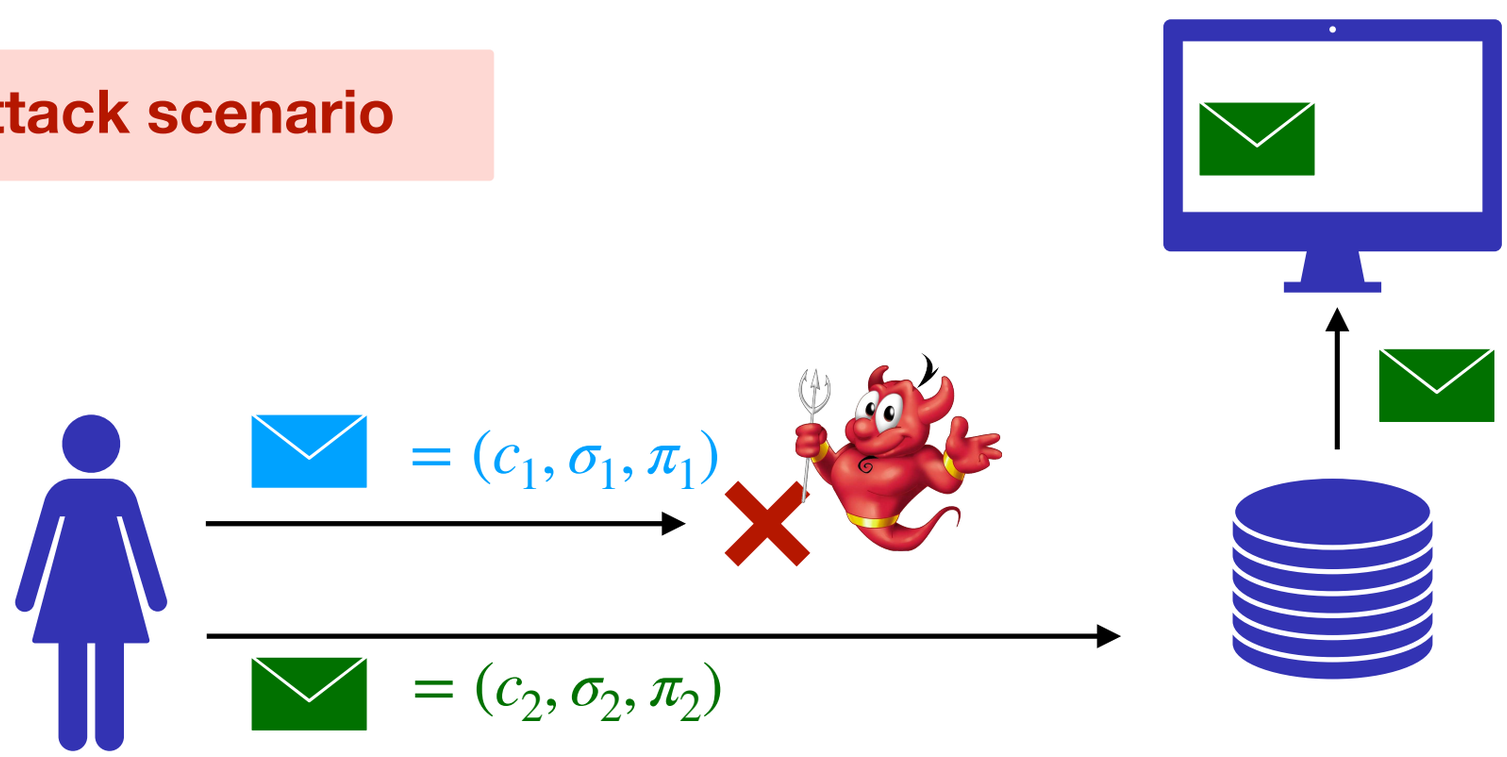


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Attack scenario

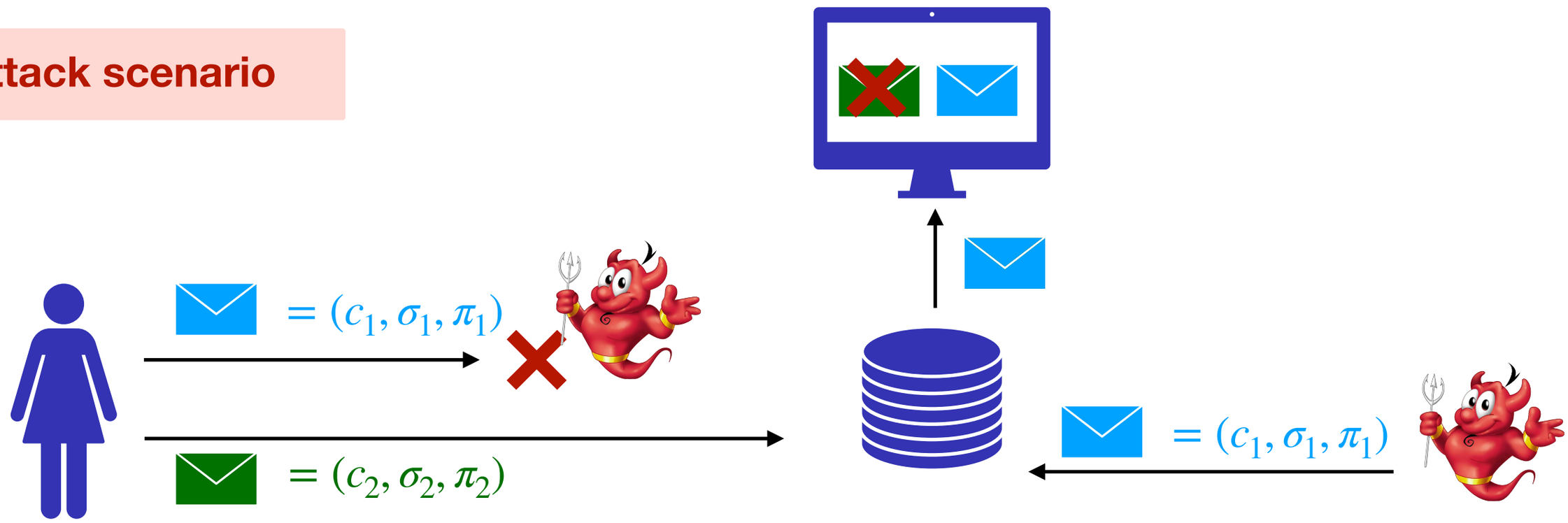


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Attack scenario

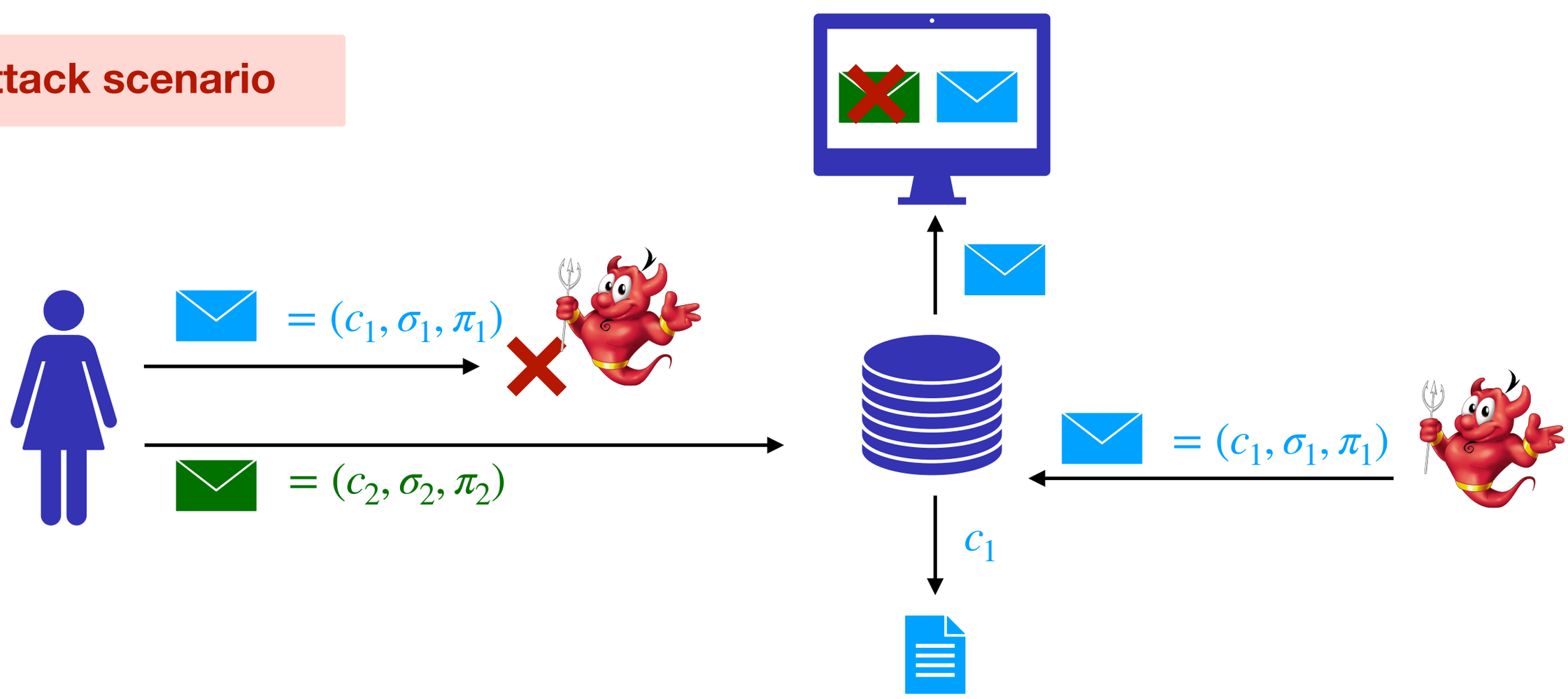


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

Attack scenario

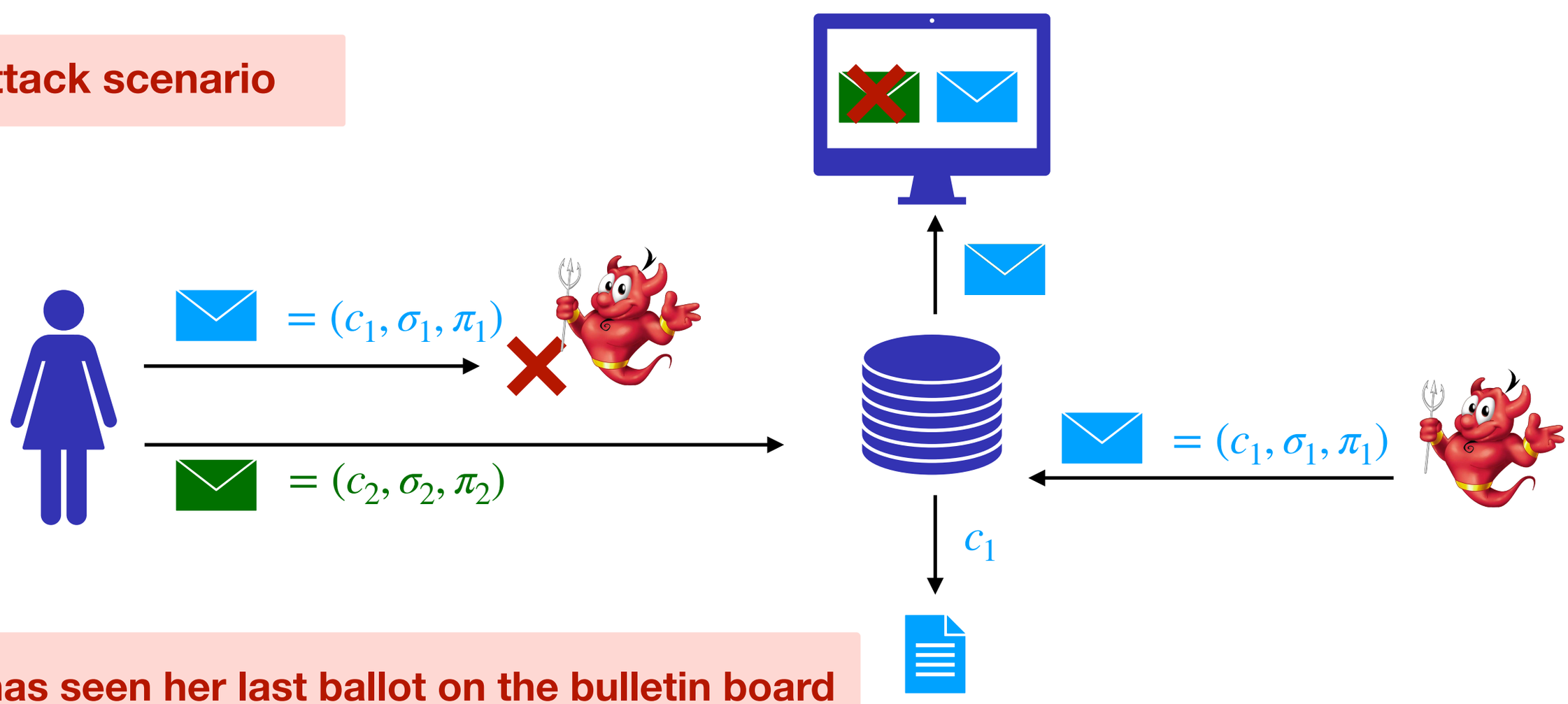


Ballot re-ordering attack

[Baloglu *et. al.*- CSF'21]

Individual verifiability - if I see my last ballot on the bulletin board, it will be counted

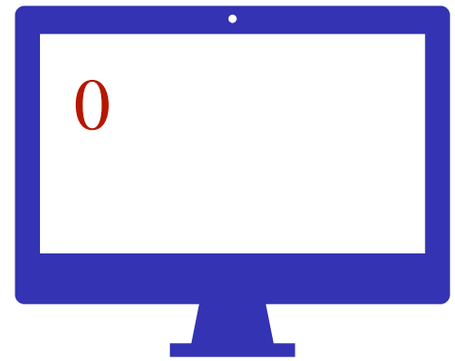
Attack scenario



Alice has seen her last ballot on the bulletin board but this is not the one that will be counted…

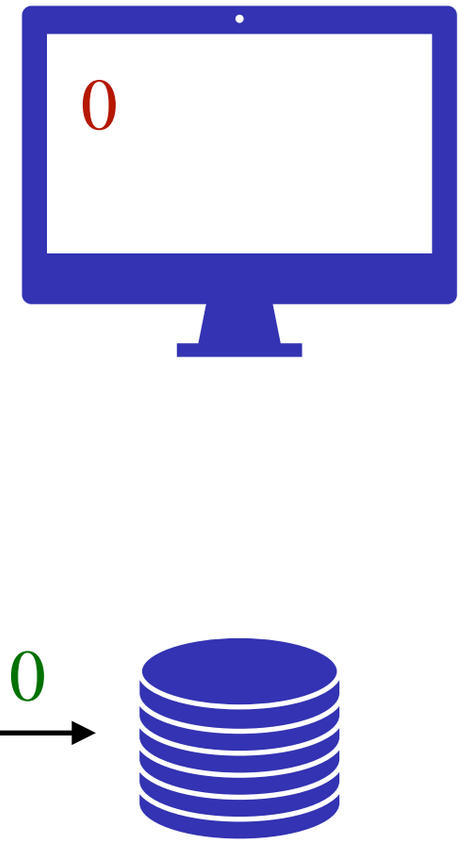
Fixing the attack with counters

1. The bulletin board is initialized with a counter set to 0



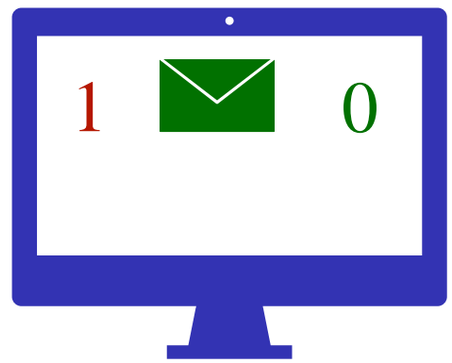
Fixing the attack with counters

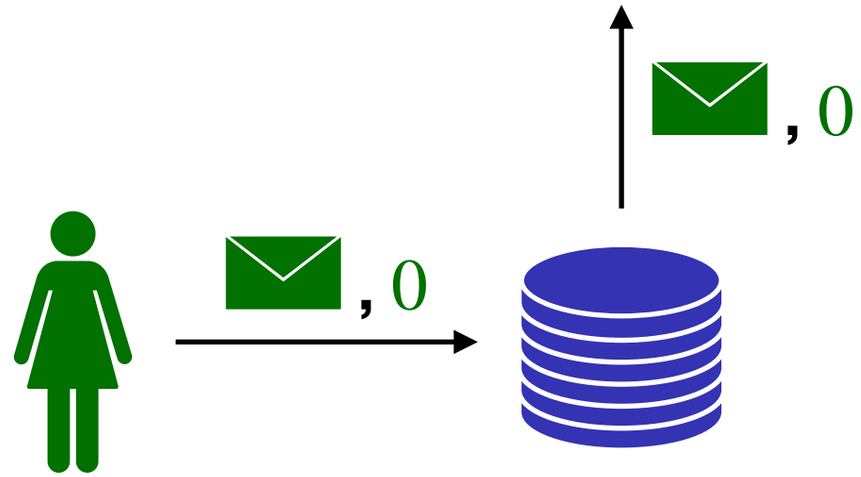
1. The bulletin board is initialized with a counter set to 0
2. Create a ballot:
   - get the current counter onto the bulletin board
   - add it to the signature σ



Fixing the attack with counters

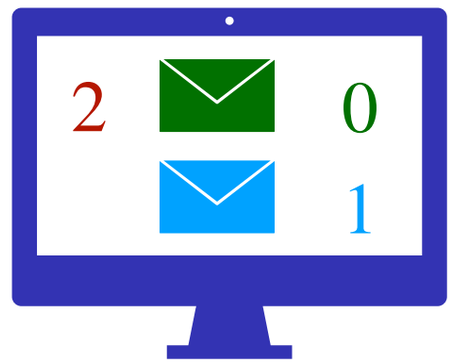
1. The bulletin board is initialized with a counter set to 0
2. Create a ballot:
   - get the current counter onto the bulletin board
   - add it to the signature σ
3. Accept a ballot with counter i_{new}:
   - get the last Alice's ballot onto the bulletin board
   - extract its counter i_{old}
   - accept the new ballot if $i_{new} > i_{old}$
   - increment the global counter

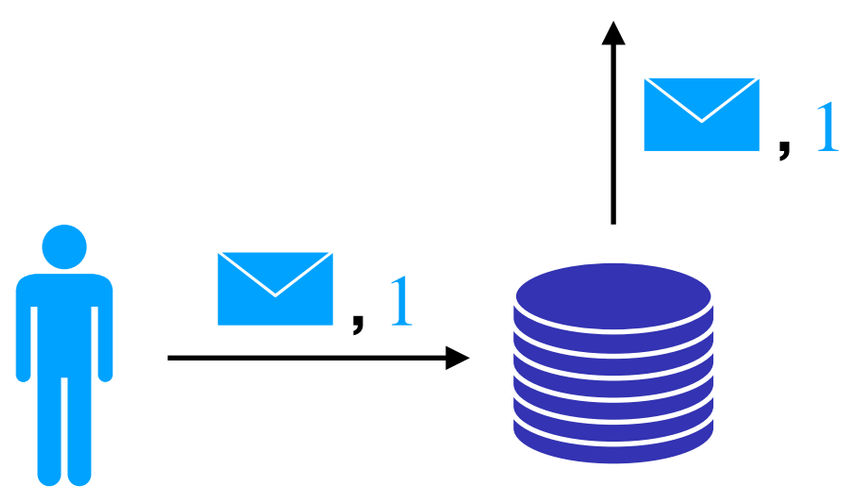




Fixing the attack with counters

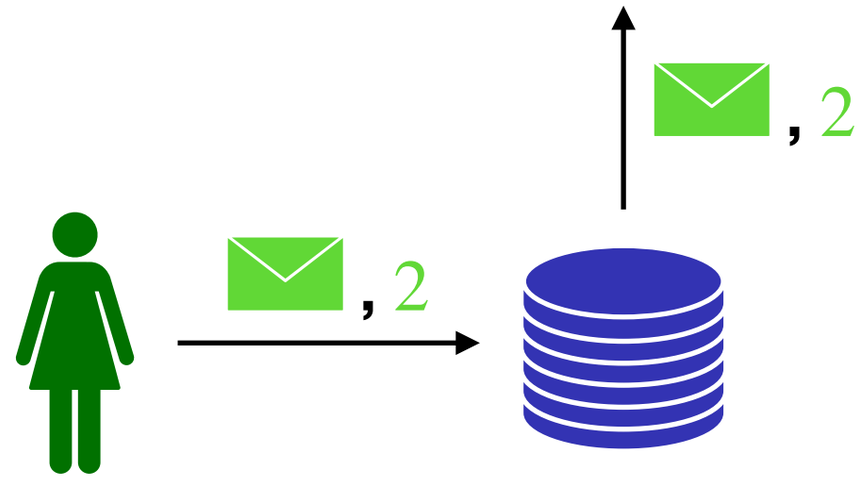
1. The bulletin board is initialized with a counter set to 0
2. Create a ballot:
   - get the current counter onto the bulletin board
   - add it to the signature σ
3. Accept a ballot with counter i_{new}:
   - get the last Alice's ballot onto the bulletin board
   - extract its counter i_{old}
   - accept the new ballot if $i_{new} > i_{old}$
   - increment the global counter





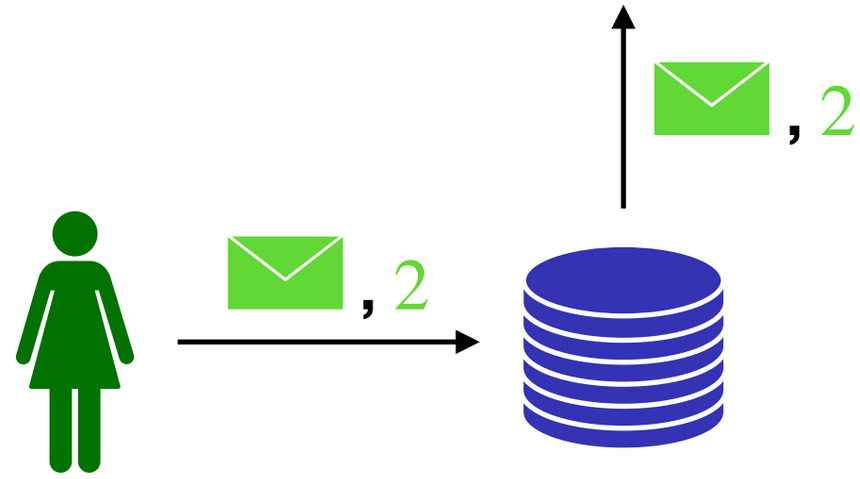
Fixing the attack with counters

1. The bulletin board is initialized with a counter set to 0
2. Create a ballot:
   - get the current counter onto the bulletin board
   - add it to the signature σ
3. Accept a ballot with counter i_{new}:
   - get the last Alice's ballot onto the bulletin board
   - extract its counter i_{old}
   - accept the new ballot if $i_{new} > i_{old}$
   - increment the global counter



Fixing the attack with counters

1. The bulletin board is initialized with a counter set to 0
2. Create a ballot:
   - get the current counter onto the bulletin board
   - add it to the signature σ
3. Accept a ballot with counter i_{new}:
   - get the last Alice's ballot onto the bulletin board
   - extract its counter i_{old}
   - accept the new ballot if $i_{new} > i_{old}$
   - increment the global counter



Technical issues

- Automatic tools does not support counters very well…
- Need to model a slightly different protocol and bridge the gap with a paper proof

Belenios - summary

[submission at ESORICS'22 in preparation]

Contributions :

- Two fixes: counters for replay attacks and pok or commitment for authentication
- A comprehensive model of Belenios including multi-elections
- A model including counters
- Paper proofs justifying the approximations about counters, e.g.

Belenios - summary

[submission at ESORICS'22 in preparation]

Contributions :

- Two fixes: counters for replay attacks and pok or commitment for authentication
- A comprehensive model of Belenios including multi-elections
- A model including counters
- Paper proofs justifying the approximations about counters, e.g.

Theorem: Belenios ensures verifiability when relying on a counter for each voter

$\Rightarrow$ Belenios is secure with a global counter

Belenios - summary

[submission at ESORICS'22 in preparation]

Contributions :

- Two fixes: counters for replay attacks and pok or commitment for authentication
- A comprehensive model of Belenios including multi-elections
- A model including counters
- Paper proofs justifying the approximations about counters, e.g.

Theorem: Belenios ensures verifiability when relying on a counter for each voter

⇒ Belenios is secure with a global counter

	Registrar	Server	Belenios <v1.13	Belenios + counters	Belenios + counters + pok+commit
Verifiability	Hon	Dis	❌	✅	✅
	Dis	Hon	❌	❌	✅

Outline

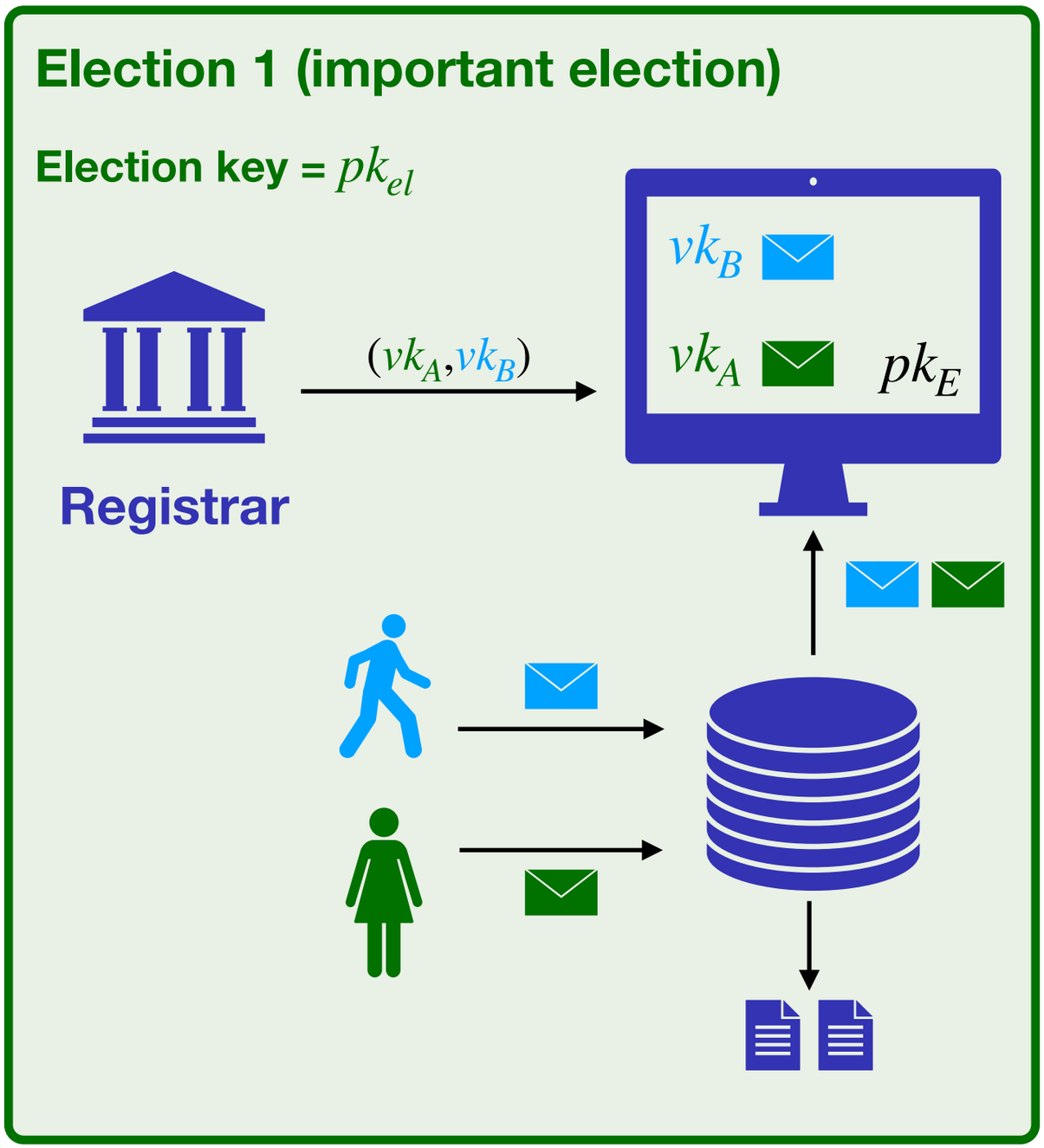
1. **Belenios: a real-world protocol**
   - description of the protocol
   - expected security properties

2. **Existing attacks and new fixes**

3. **Multi-elections… a real threat…**
   - a new attack against Belenios
   - the Swiss-Post protocol: another victim

4. **Studying new security properties**
   - cast-as-intended
   - accountability

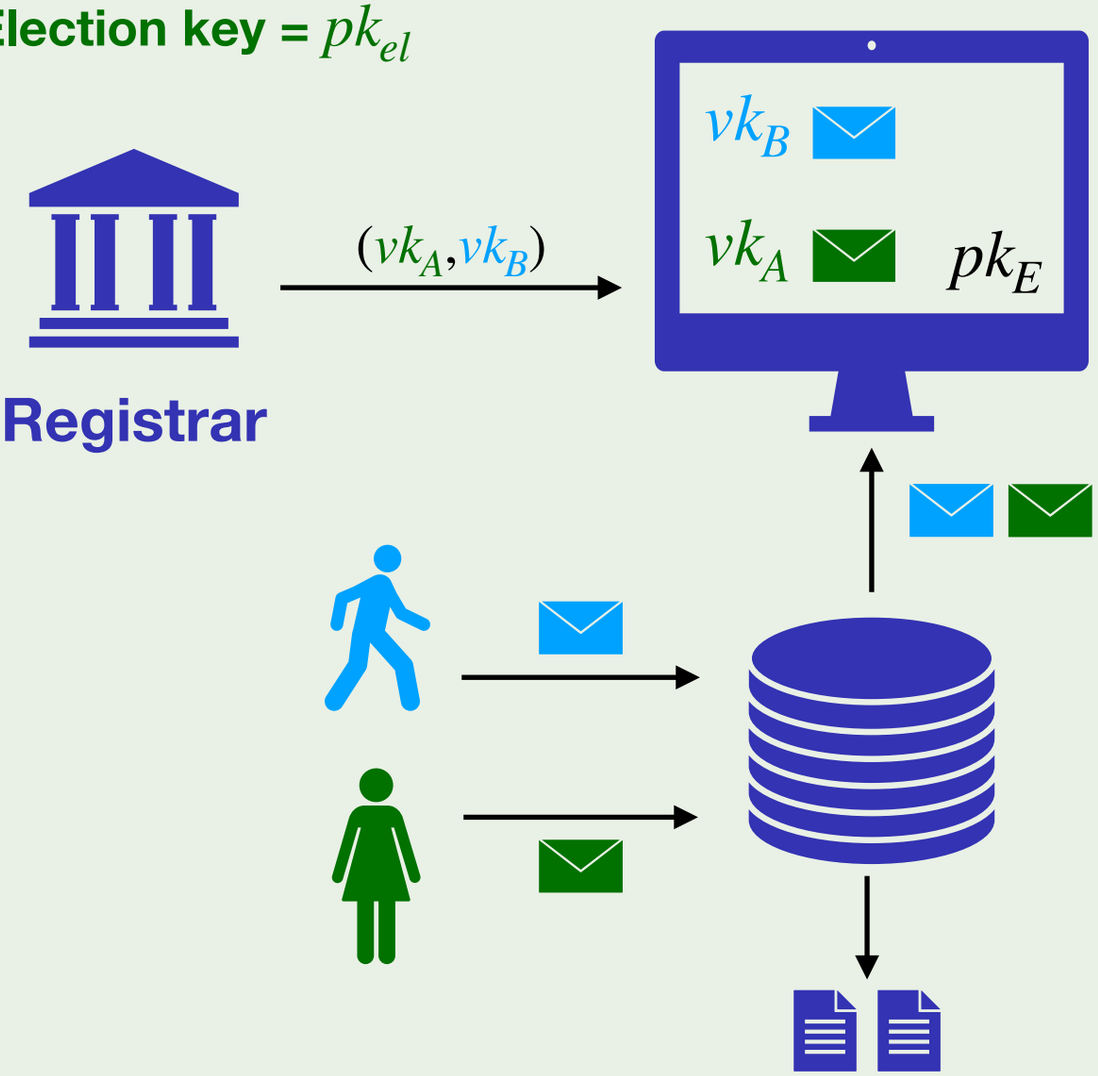
A privacy attack against Belenios



A privacy attack against Belenios

Election 1 (important election)

Election key = pk_{el}



Election 2 (small/test election)

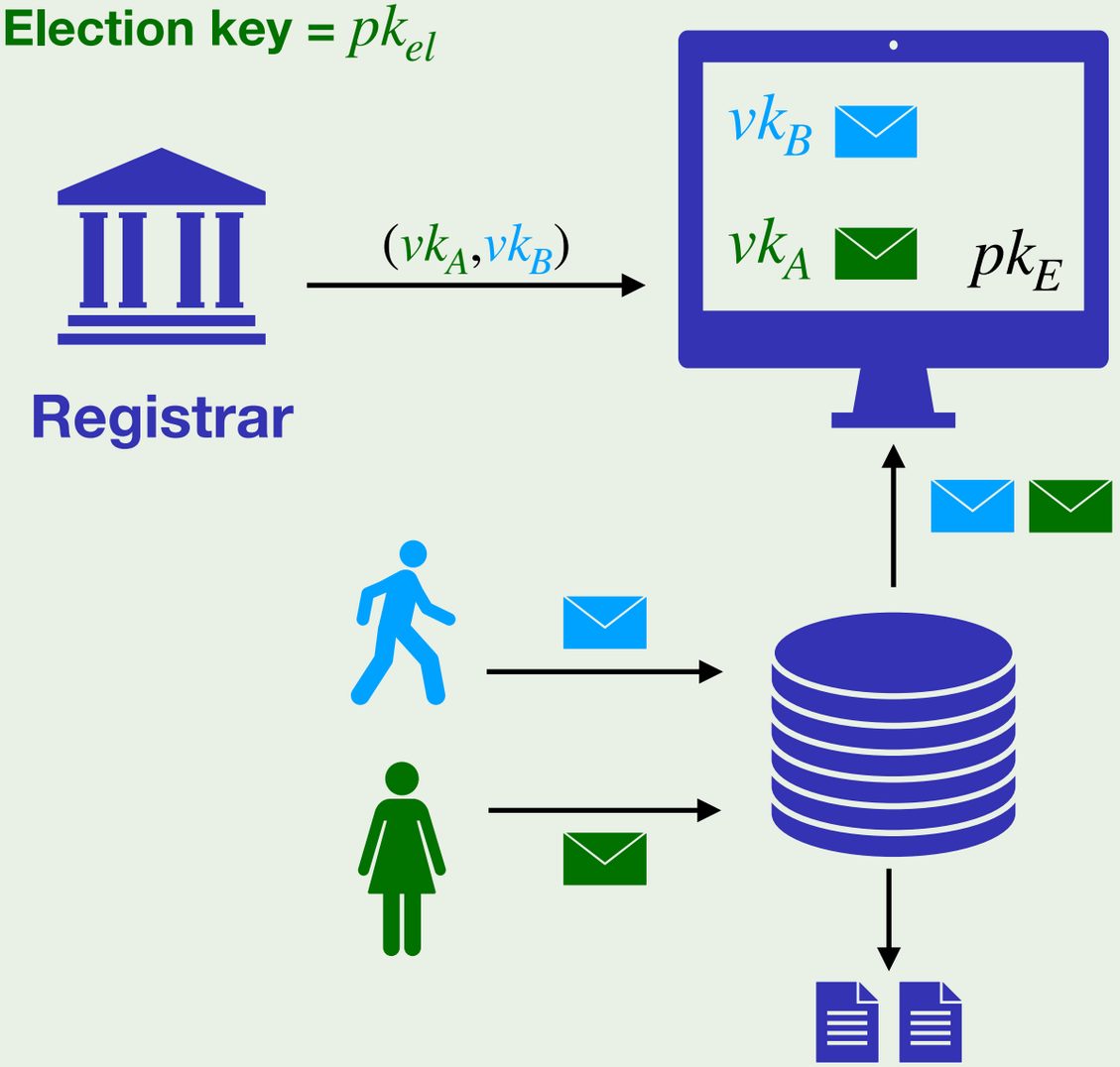
Election key = pk_{el}

The trustees can use the same keys

A privacy attack against Belenios

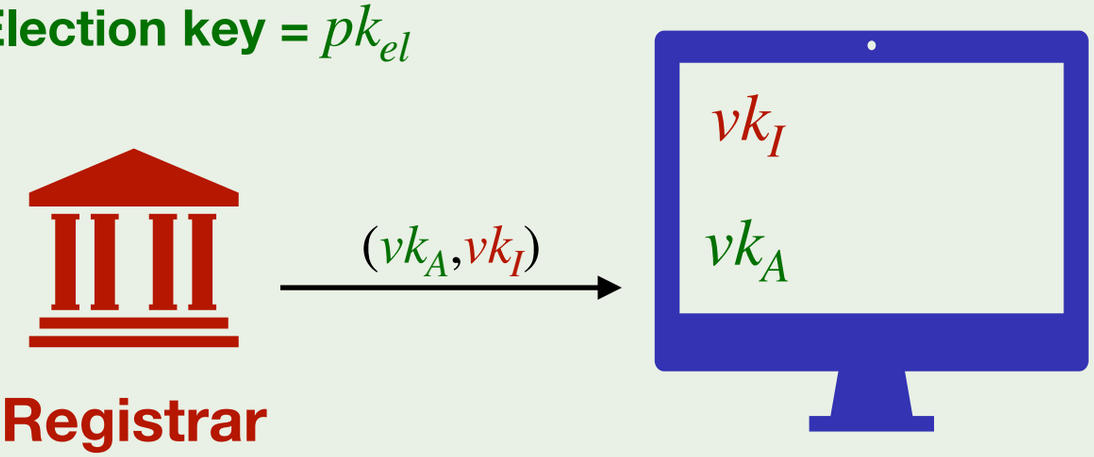
Election 1 (important election)

Election key = pk_{el}



Election 2 (small/test election)

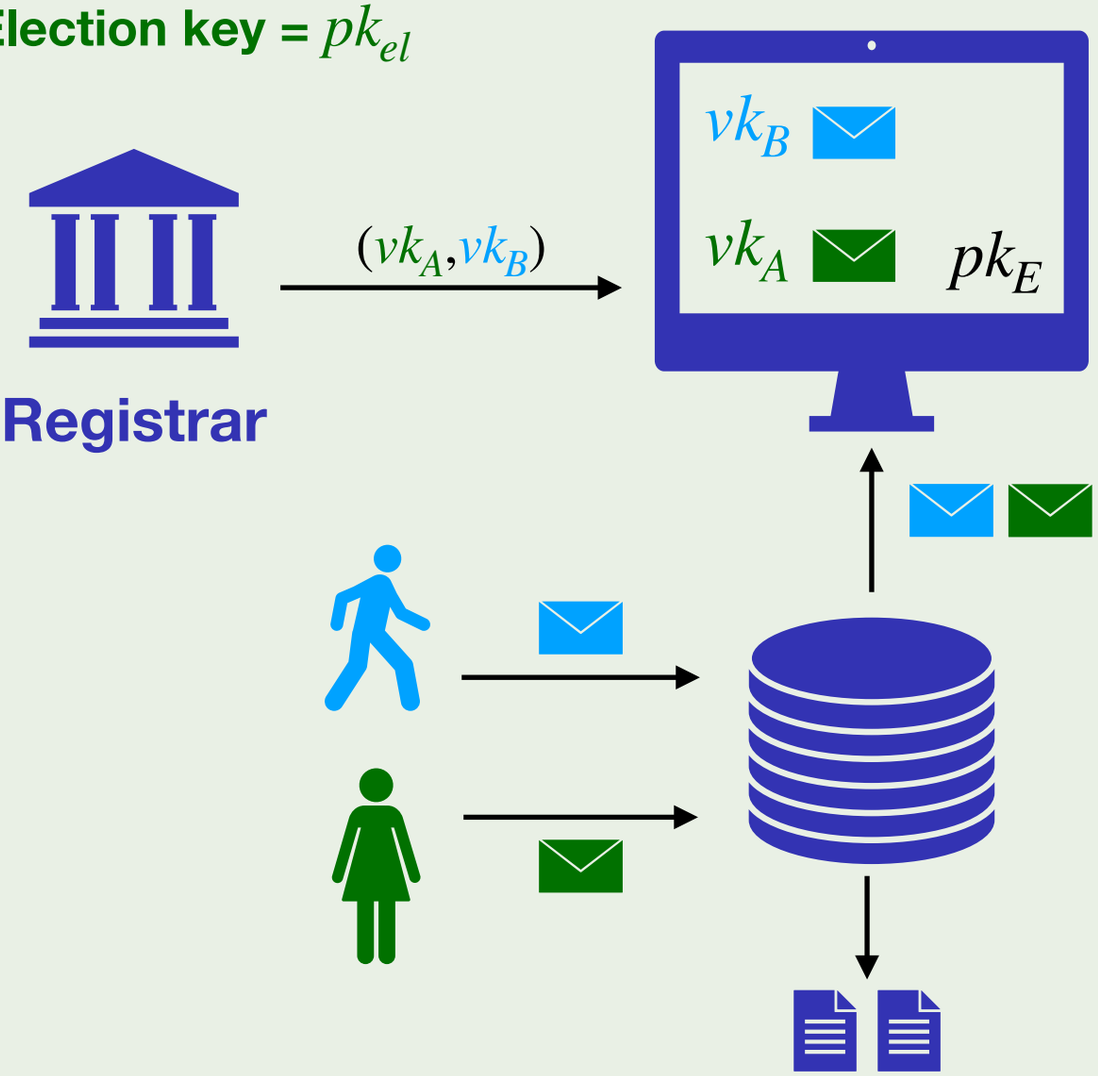
Election key = pk_{el}



A privacy attack against Belenios

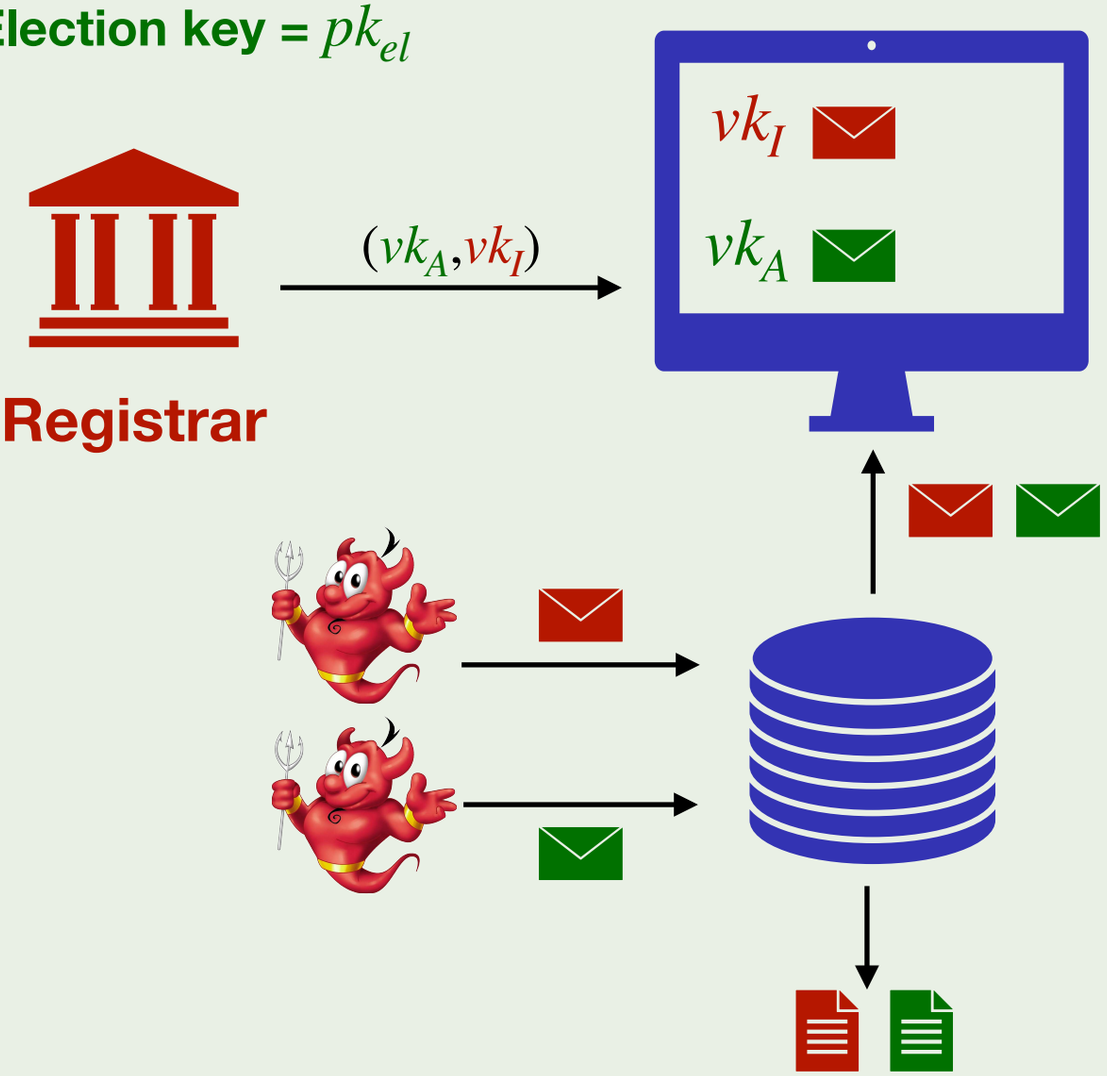
Election 1 (important election)

Election key = pk_{el}



Election 2 (small/test election)

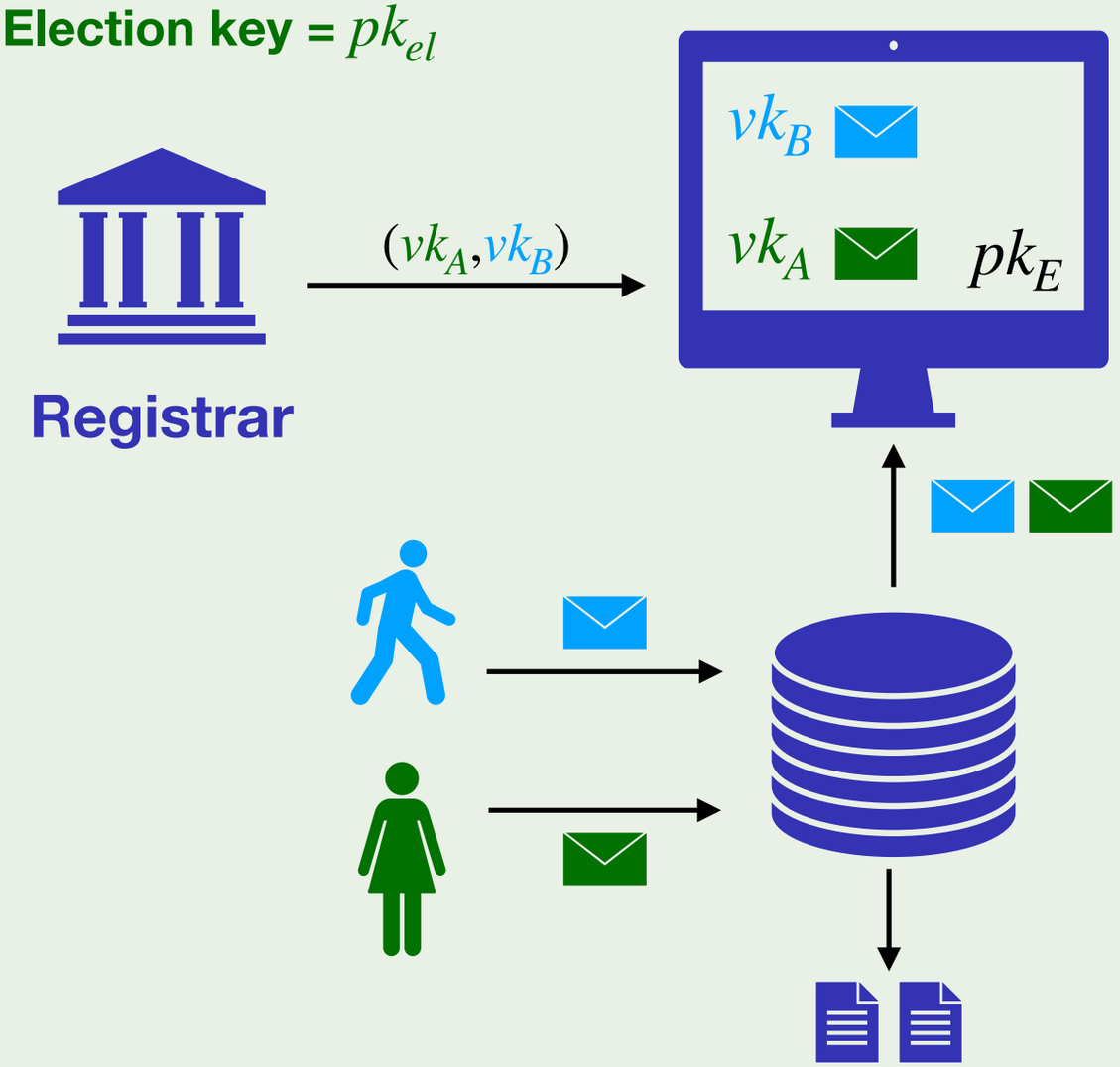
Election key = pk_{el}



A privacy attack against Belenios

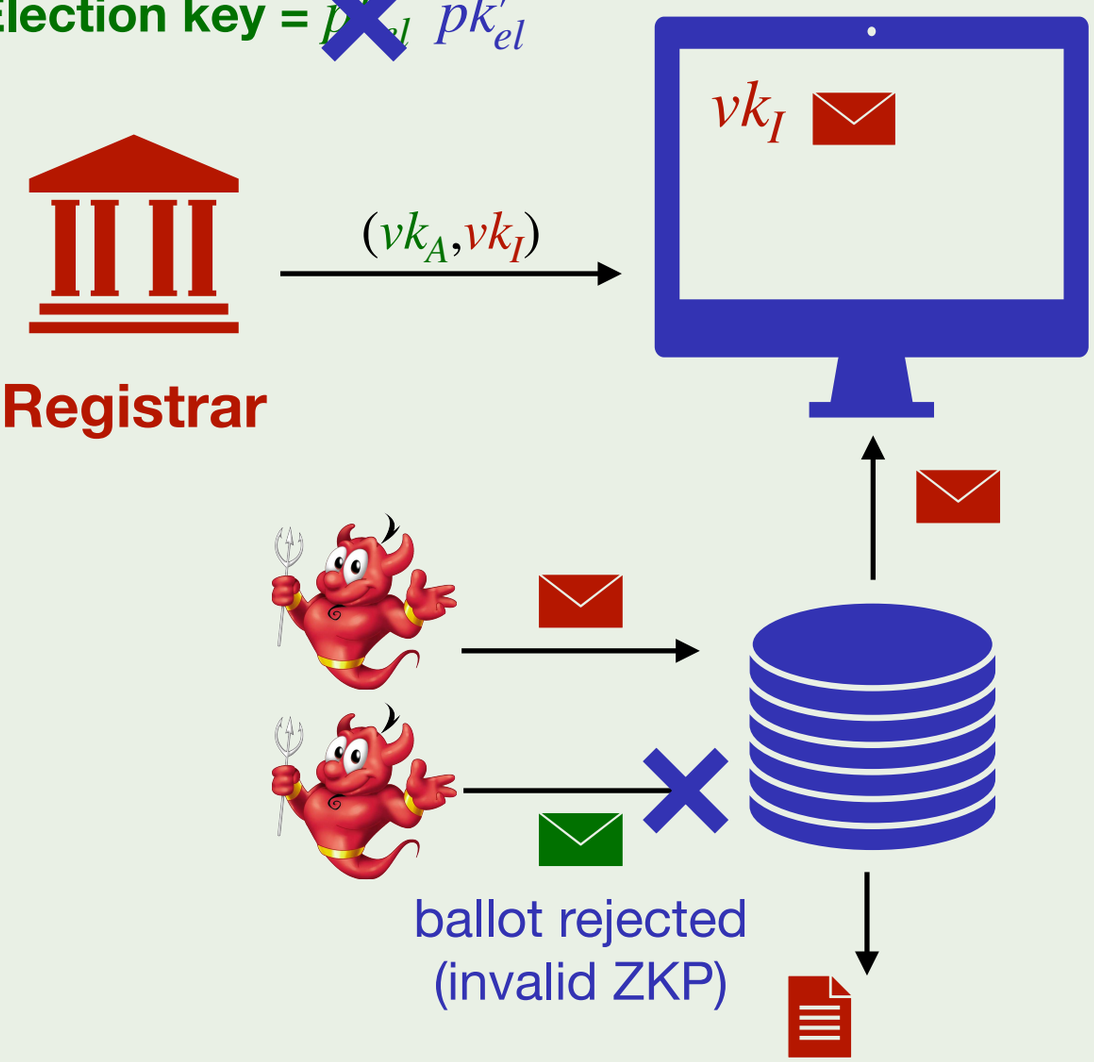
Election 1 (important election)

Election key = pk_{el}



Election 2 (small/test election)

Election key = ~~pk_{el}~~ pk'_{el}

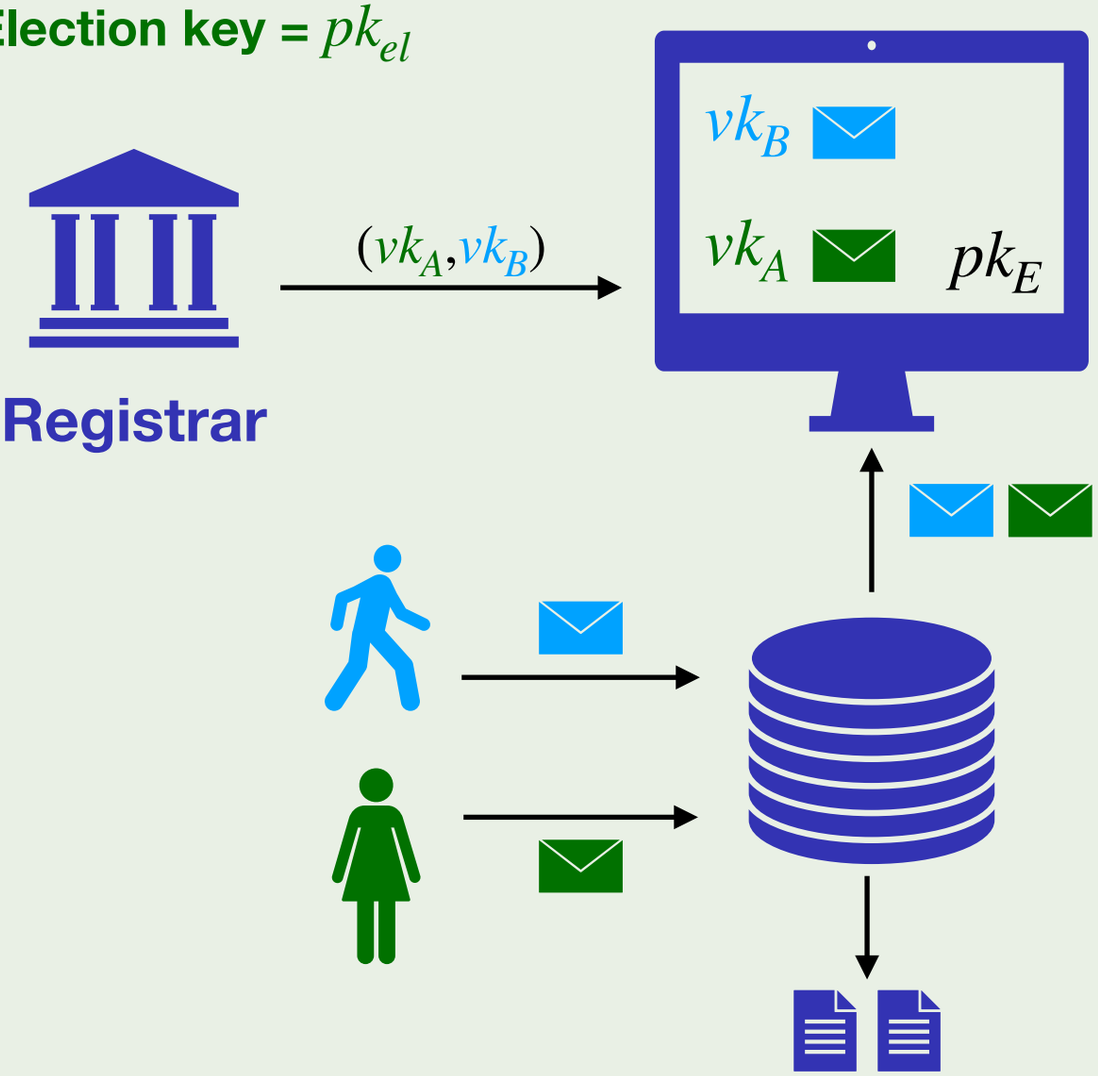


After v1.13 with an honest server

A privacy attack against Belenios

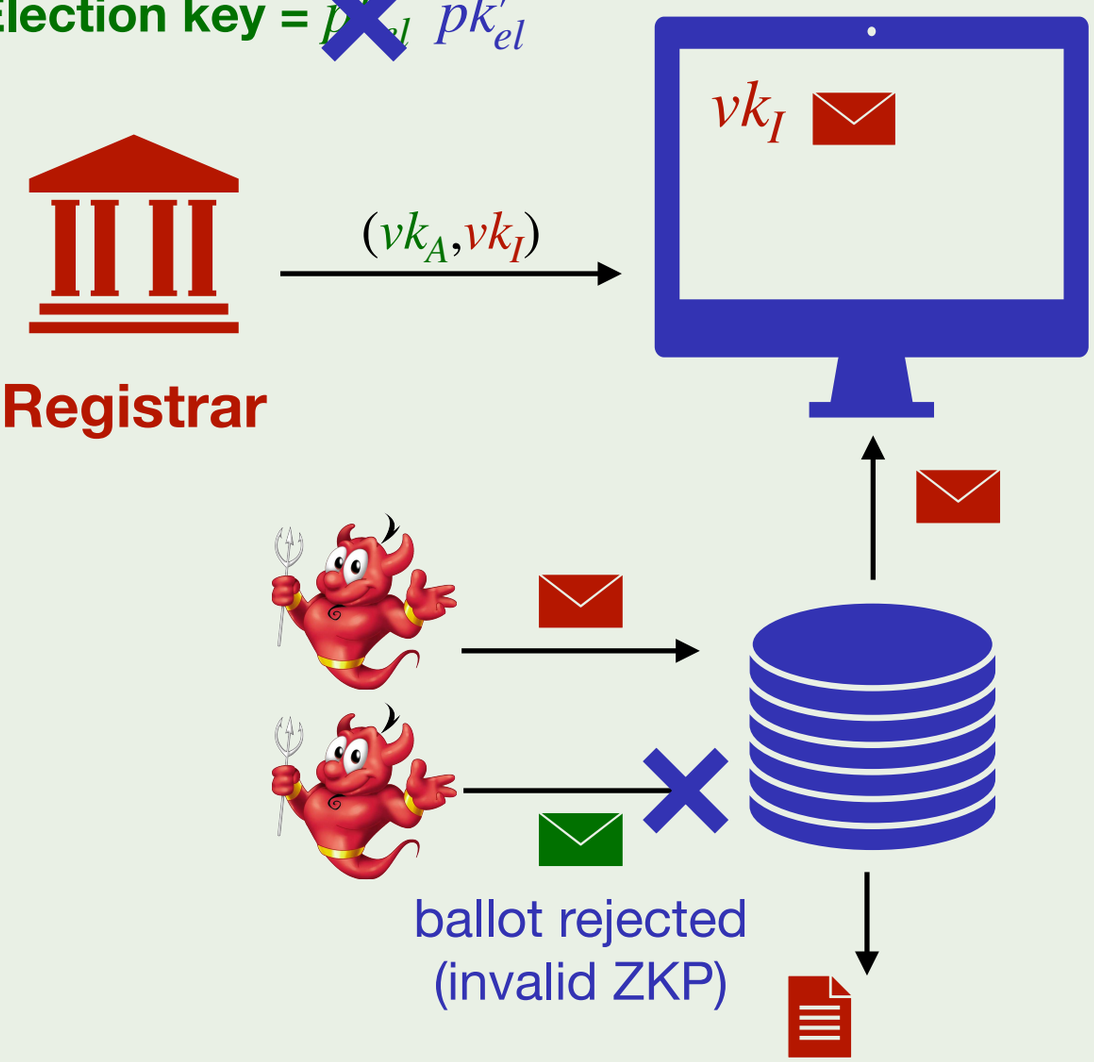
Election 1 (important election)

Election key = pk_{el}



Election 2 (small/test election)

Election key = ~~pk_{el}~~ pk'_{el}



After v1.13 with an honest server

Fix - the server acts as a decryption trustee and must refresh its key for each election

Belenios - summary

[submission at ESORICS'22 in preparation]

Contributions :

- A (partial) fix: the Voting Server acts as a Trustee for decryption!
- A comprehensive model of Belenios including multi-elections
- Security proofs in ProVerif
- Paper proofs justifying the approximations about counters

Belenios - summary

[submission at ESORICS'22 in preparation]

Contributions :

- A (partial) fix: the Voting Server acts as a Trustee for decryption!
- A comprehensive model of Belenios including multi-elections
- Security proofs in ProVerif
- Paper proofs justifying the approximations about counters

	Registrar	Server	Belenios <v1.13	Belenios + Server Trustee	Belenios + Server Trustee + counters/pok/commit
Verifiability	Hon	Dis	❌	❌	✅
	Dis	Hon	❌	❌	✅
Privacy	Hon	Dis	❌	❌	❌
	Dis	Hon	❌	✅	✅

Outline

1. **Belenios: a real-world protocol**
   - description of the protocol
   - expected security properties

2. **Existing attacks and new fixes**

3. **Multi-elections… a real threat…**
   - a new attack against Belenios
   - the Swiss-Post protocol: another victim

4. **Studying new security properties**
   - cast-as-intended
   - accountability

Swiss-Post protocol

Context :

- Switzerland is going to restart e-voting in 2022
- The Federal Chancellerie asks for cryptographic and symbolic proofs

➡ collaboration to update the symbolic proofs w.r.t. the Chancellery's requirements

Swiss-Post protocol

Context :

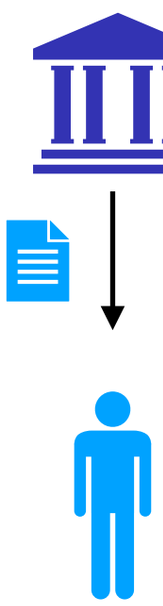
- Switzerland is going to restart e-voting in 2022
- The Federal Chancellerie asks for cryptographic and symbolic proofs

➡ collaboration to update the symbolic proofs w.r.t. the Chancellery's requirements

Vote secrecy attack: an attacker can learn the vote of everyone!

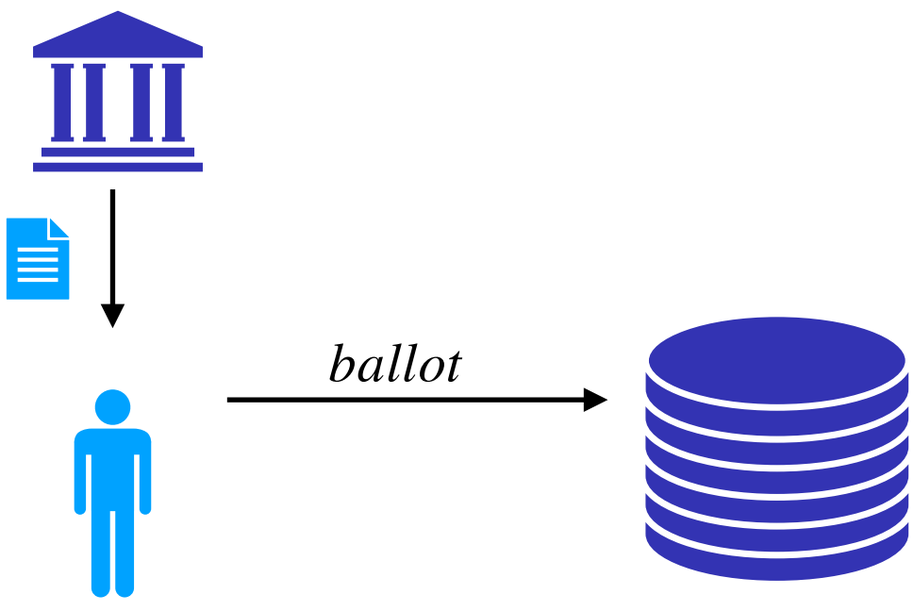
A privacy attack against Swiss-Post protocol

Overview of the protocol :



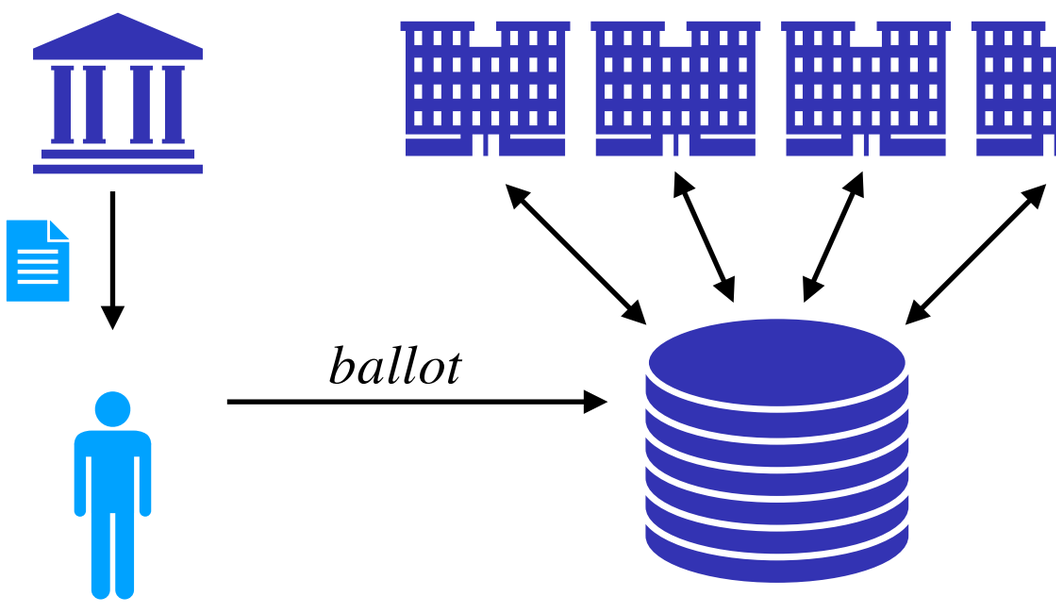
A privacy attack against Swiss-Post protocol

Overview of the protocol :



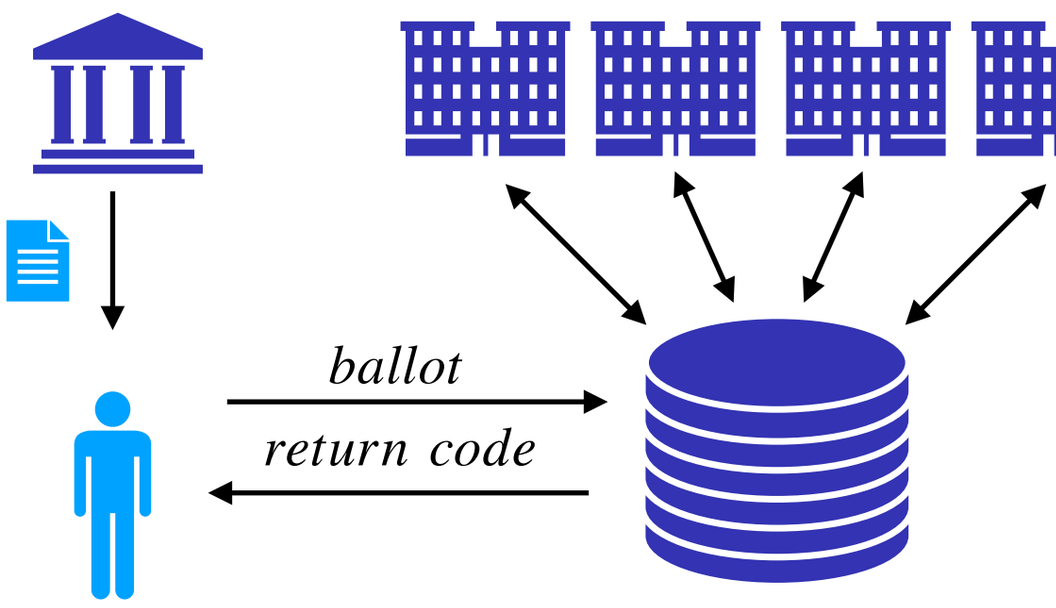
A privacy attack against Swiss-Post protocol

Overview of the protocol :



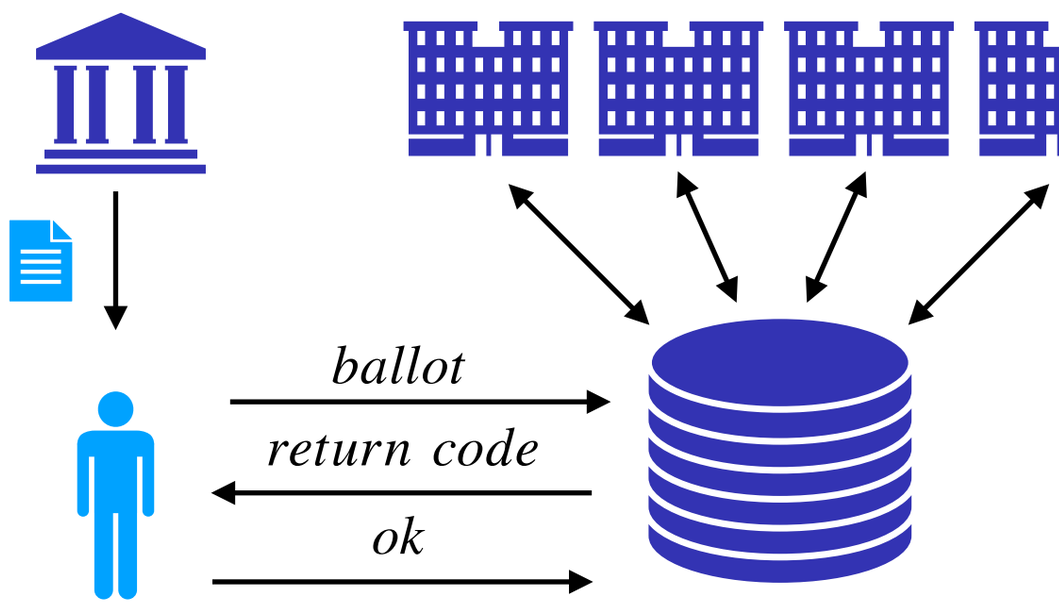
A privacy attack against Swiss-Post protocol

Overview of the protocol :



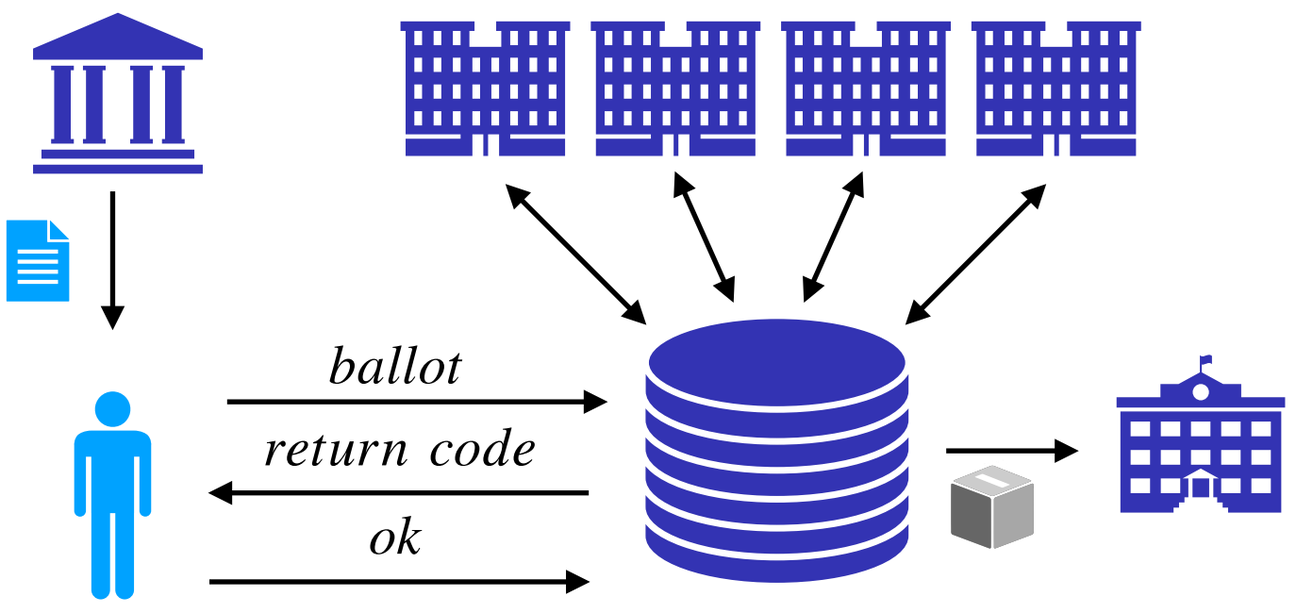
A privacy attack against Swiss-Post protocol

Overview of the protocol :



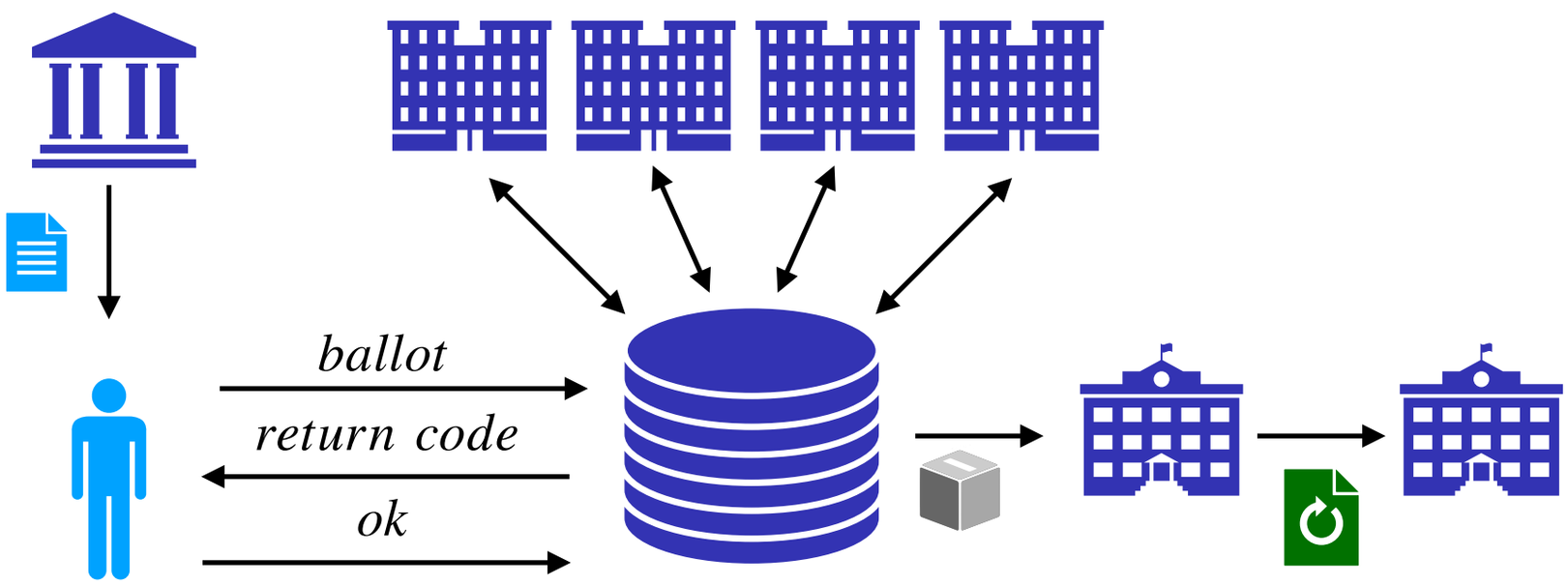
A privacy attack against Swiss-Post protocol

Overview of the protocol :



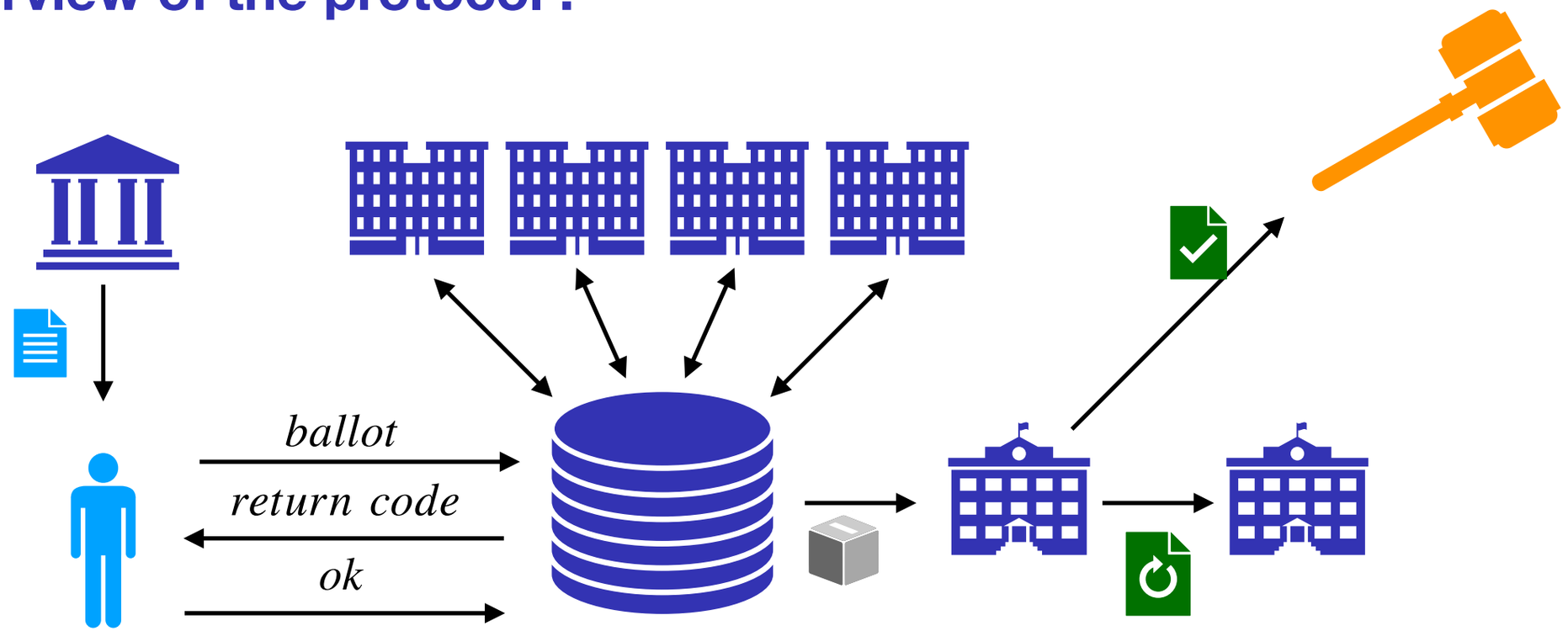
A privacy attack against Swiss-Post protocol

Overview of the protocol :



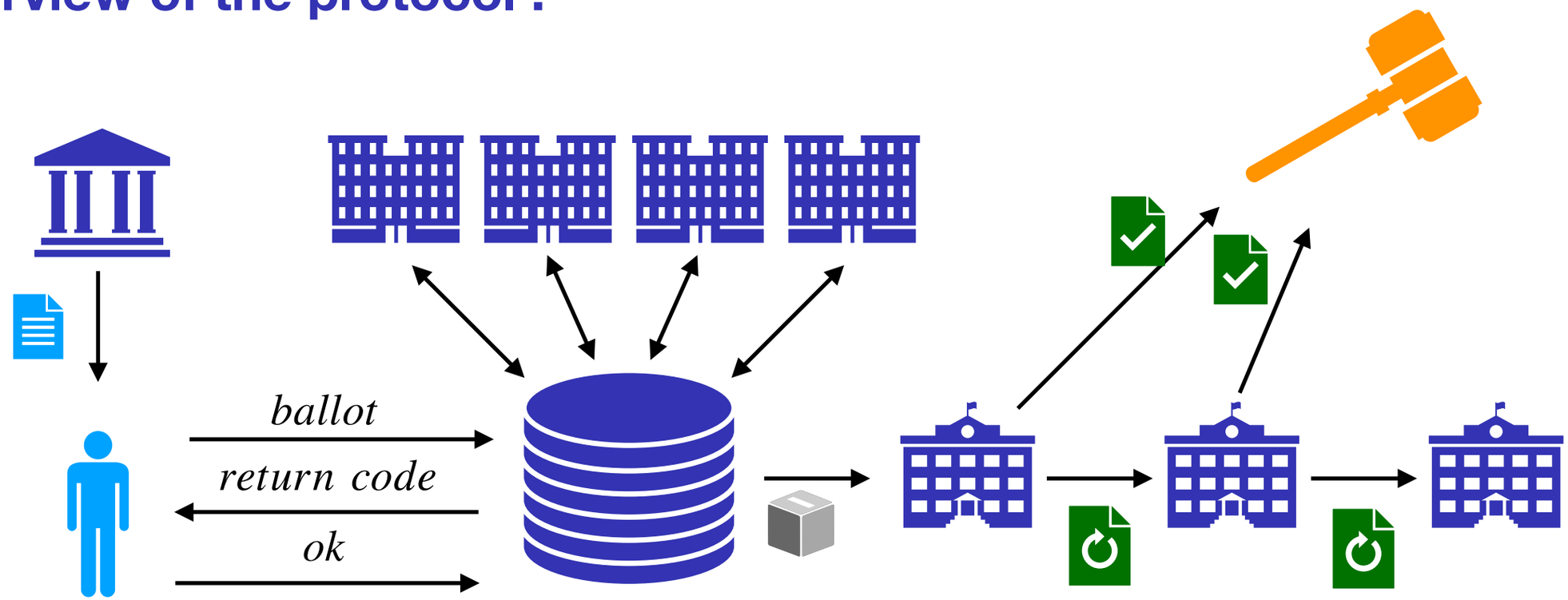
A privacy attack against Swiss-Post protocol

Overview of the protocol :



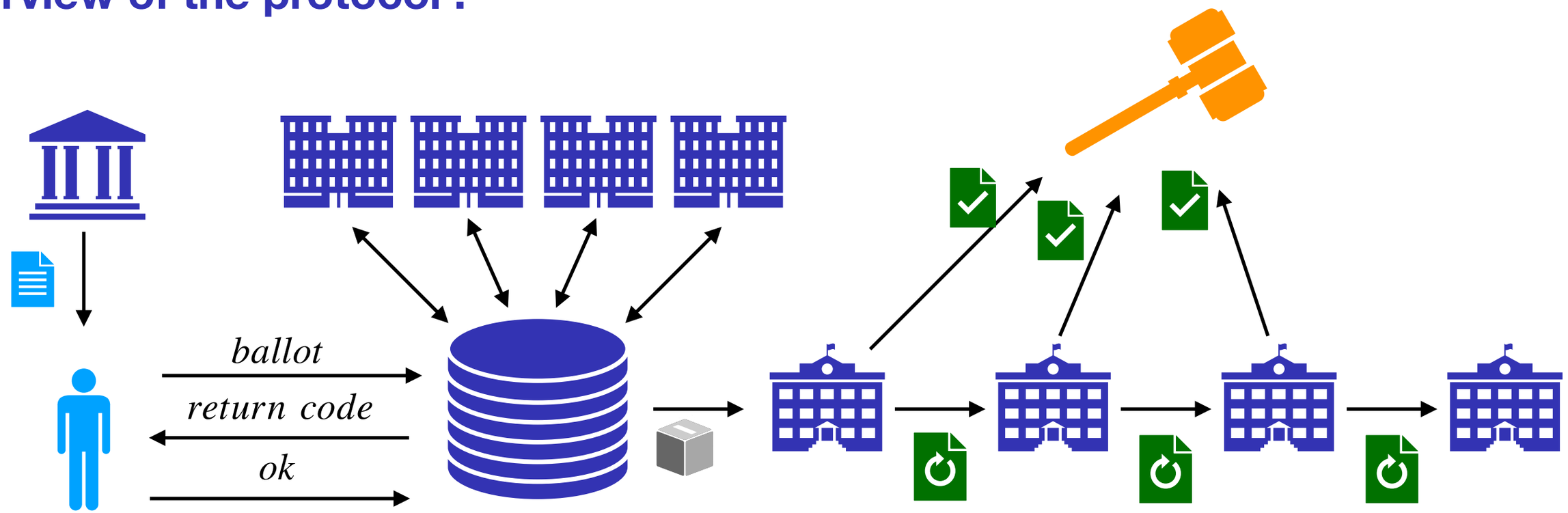
A privacy attack against Swiss-Post protocol

Overview of the protocol :



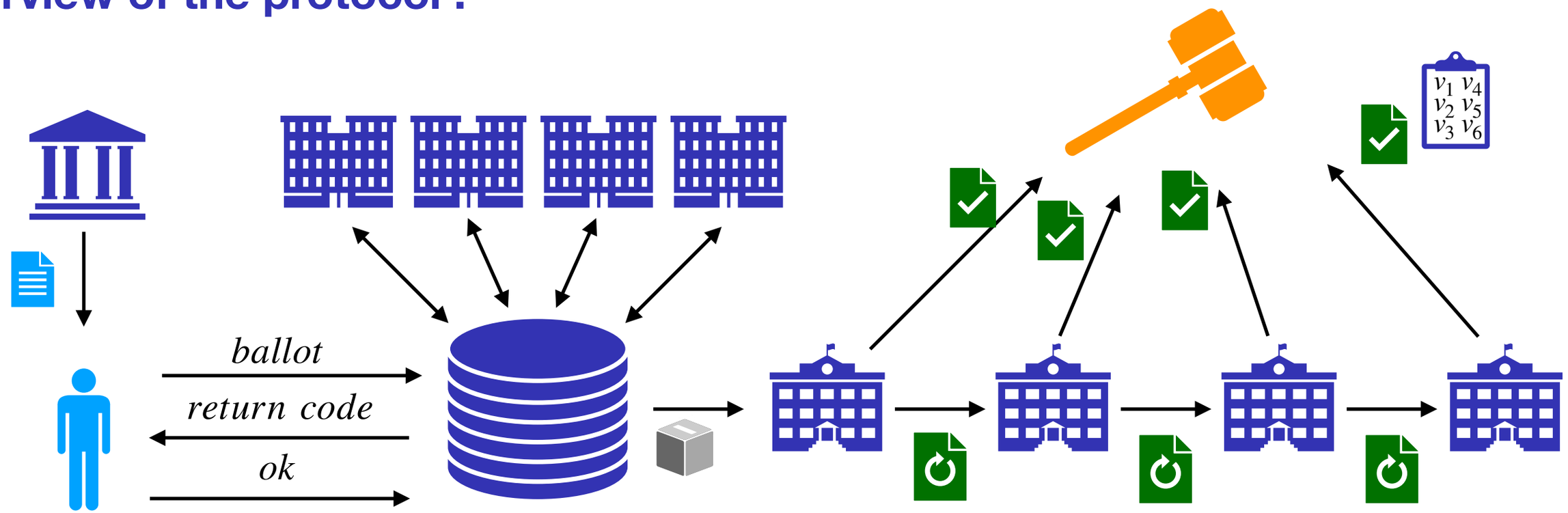
A privacy attack against Swiss-Post protocol

Overview of the protocol :



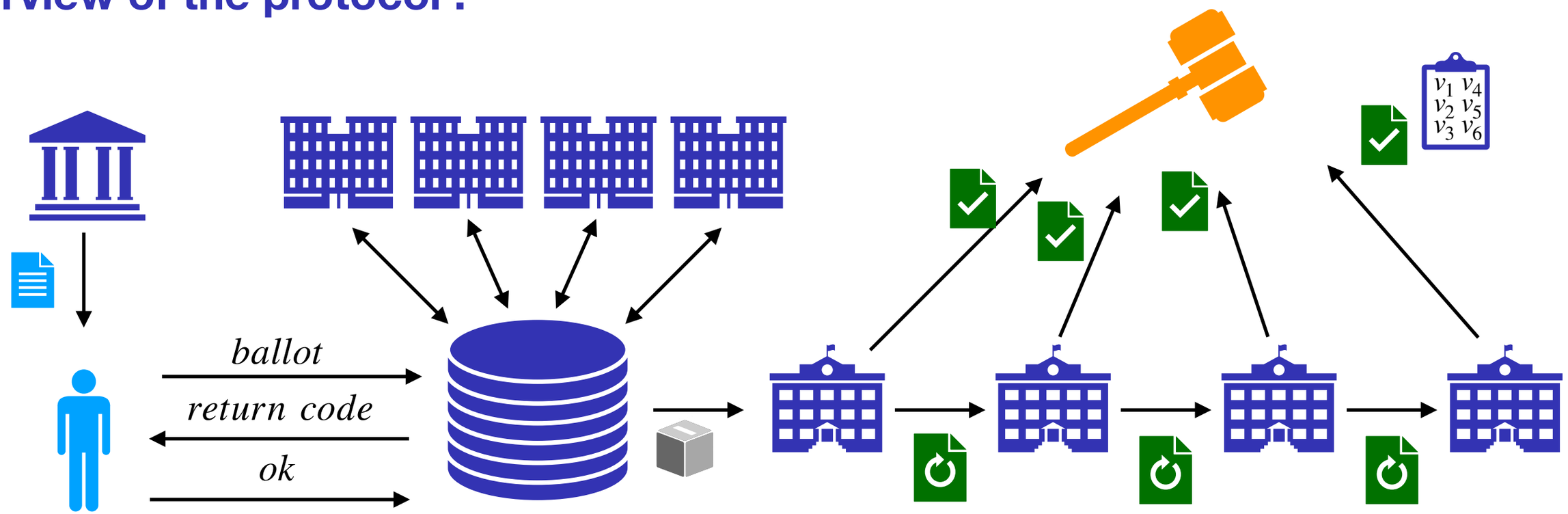
A privacy attack against Swiss-Post protocol

Overview of the protocol :



A privacy attack against Swiss-Post protocol

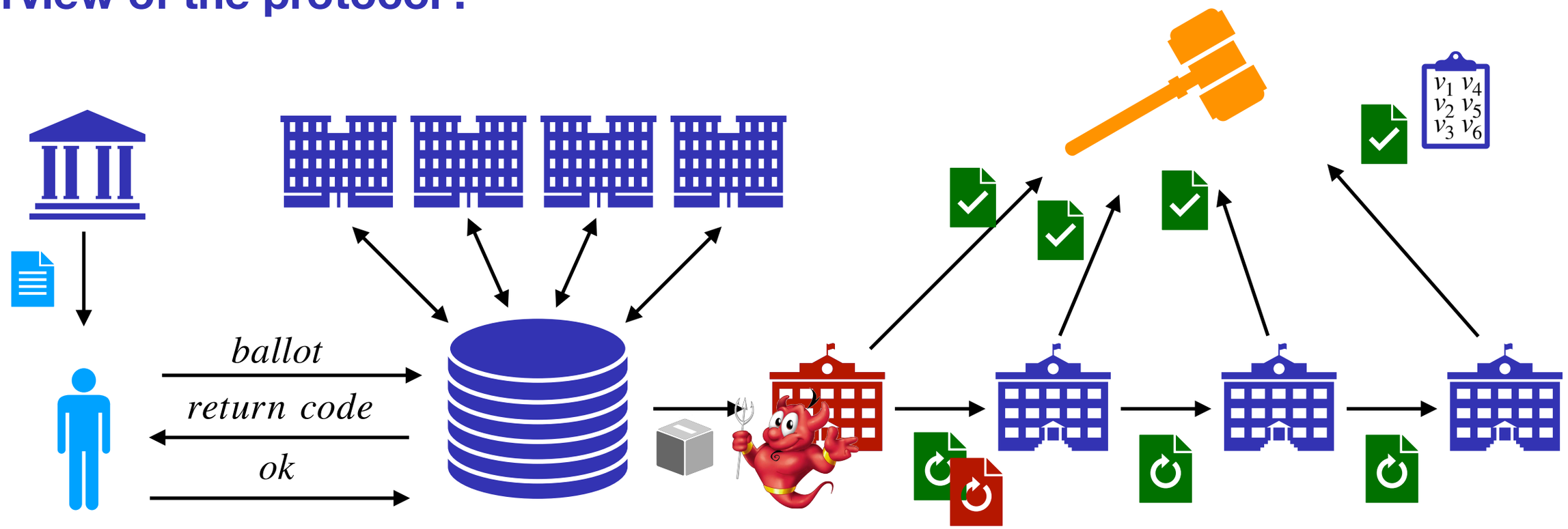
Overview of the protocol :



Attack :
- A control component must decrypt many ballot-boxes in a raw…
- An attacker can create **fake ballot-boxes** to break Alice's privacy!

A privacy attack against Swiss-Post protocol

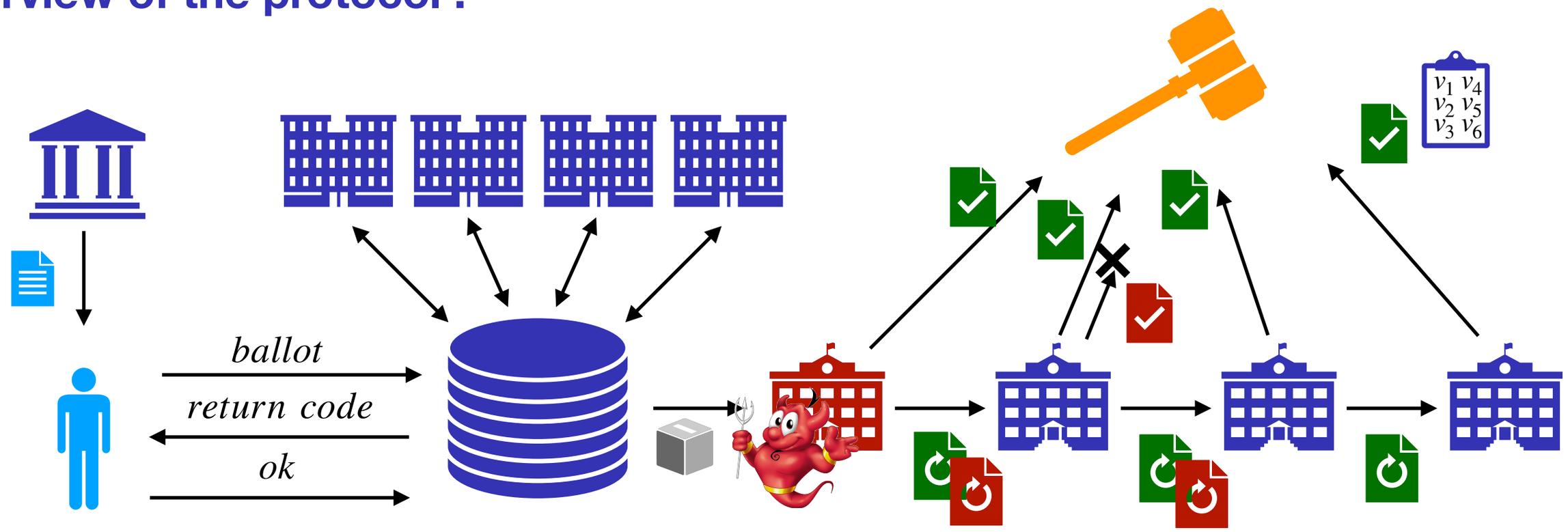
Overview of the protocol :



Attack :
- A control component must decrypt many ballot-boxes in a raw…
- An attacker can create **fake ballot-boxes** to break Alice's privacy!

A privacy attack against Swiss-Post protocol

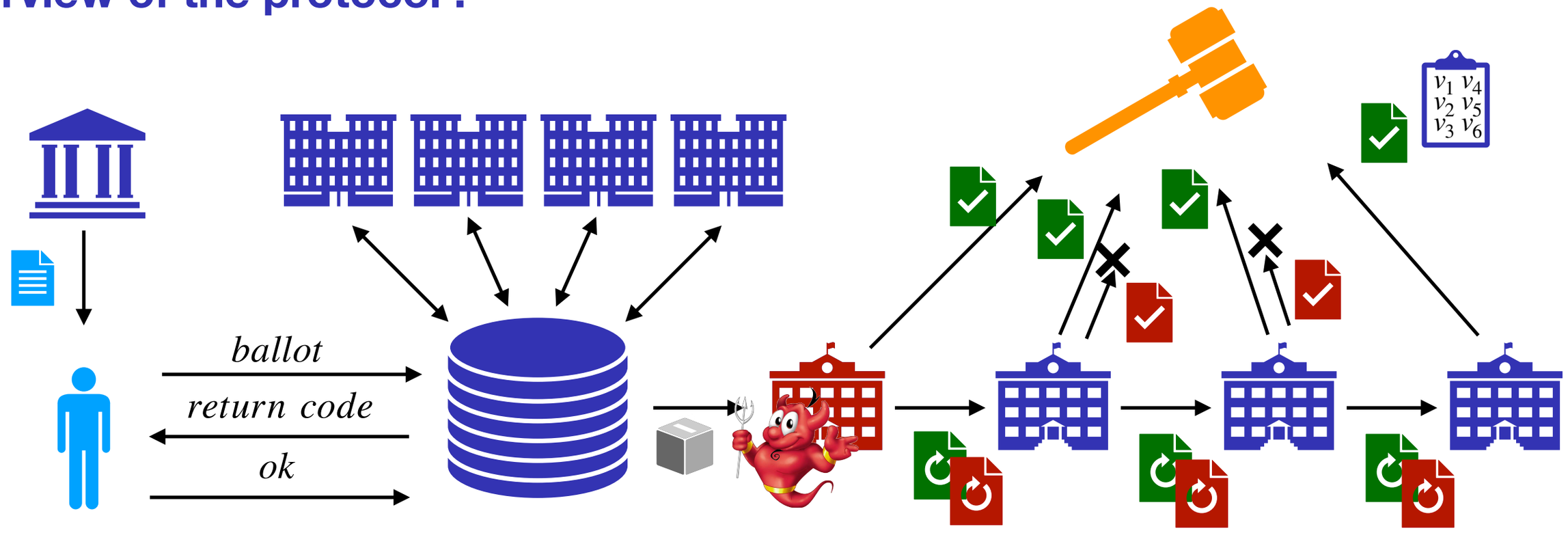
Overview of the protocol :



Attack :
- A control component must decrypt many ballot-boxes in a raw…
- An attacker can create **fake ballot-boxes** to break Alice's privacy!

A privacy attack against Swiss-Post protocol

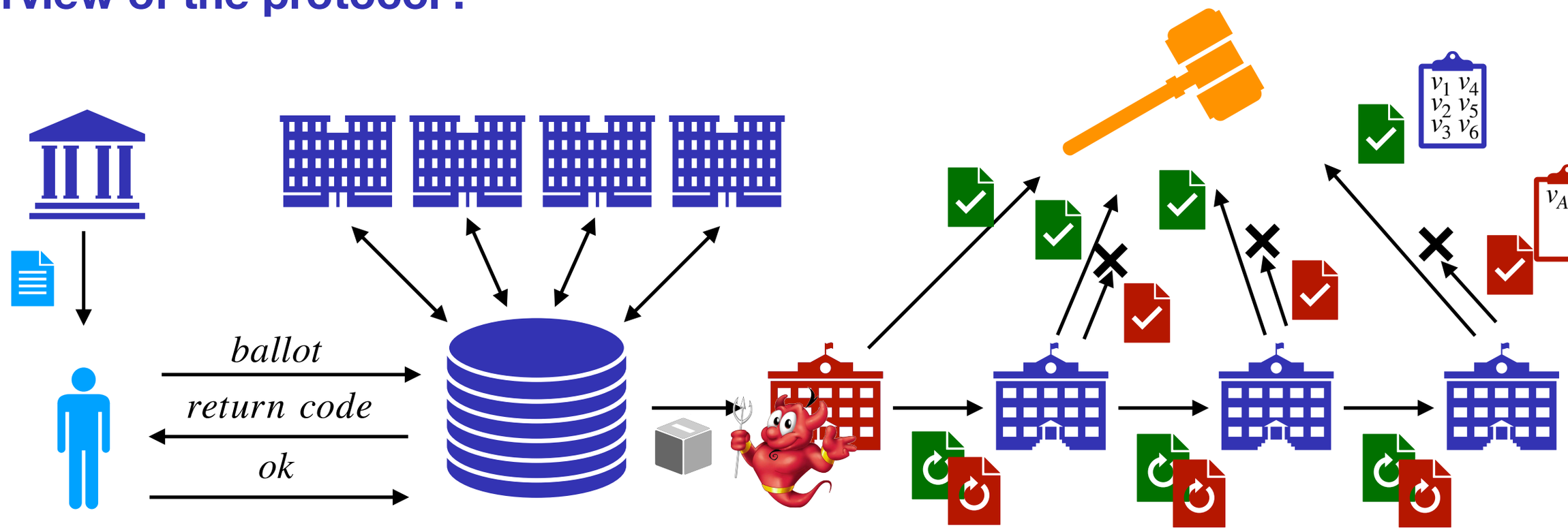
Overview of the protocol :



Attack :
- A control component must decrypt many ballot-boxes in a raw…
- An attacker can create **fake ballot-boxes** to break Alice's privacy!

A privacy attack against Swiss-Post protocol

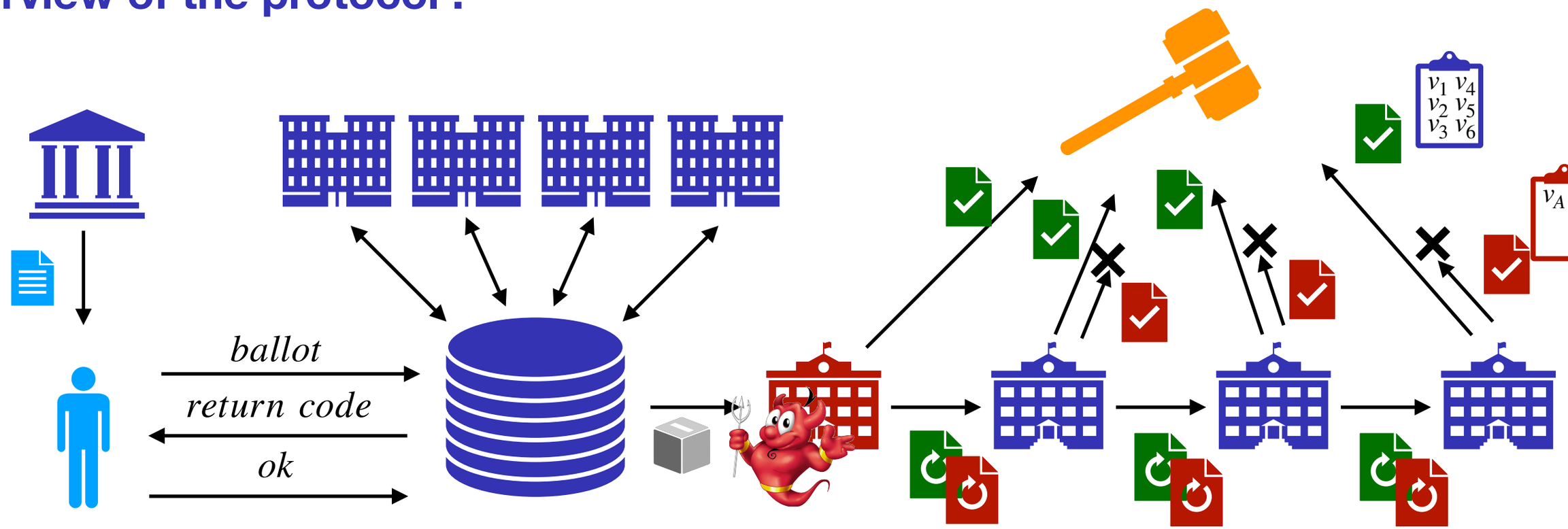
Overview of the protocol :



Attack :
- A control component must decrypt many ballot-boxes in a raw…
- An attacker can create **fake ballot-boxes** to break Alice's privacy!

A privacy attack against Swiss-Post protocol

Overview of the protocol :



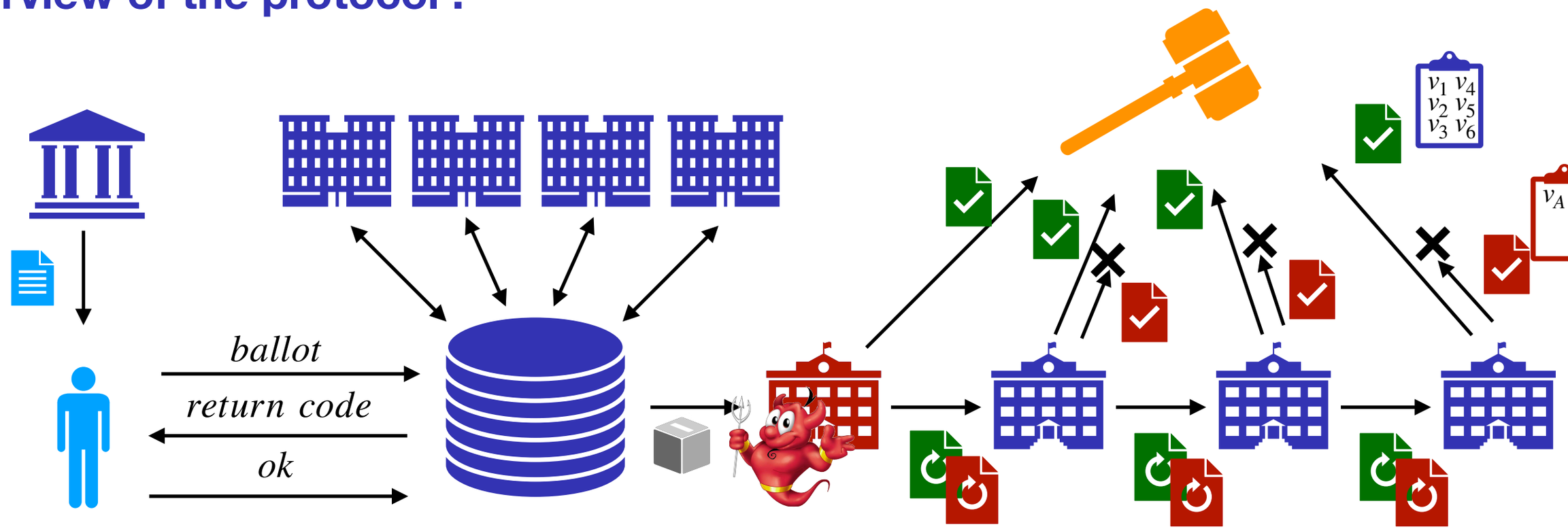
Attack reported to Swiss Post and we got a bounty 😇

Attack : A control component must decrypt many ballot-boxes in a raw…

- An attacker can create **fake ballot-boxes** to break Alice's privacy!

A privacy attack against Swiss-Post protocol

Overview of the protocol :



Attack reported to Swiss Post and we got a bounty 😇

Paper accepted at RWC'22

- An attacker can create **fake ballot-boxes** to break Alice's privacy!

Lessons learned…

1. Both computational and symbolic proofs are not accurate enough to analyse the security of real-world e-voting protocols

- ➡ Considering scenarios with a unique election and a unique ballot-box is too limited…
- ➡ Attacks are missed ✗

2. Considering multiple elections is of worth interest but complexifies the proofs…

- ➡ (probably) true for computational analysis
- ➡ less clear for symbolic analysis due to internal optimizations in tools (e.g. ProVerif) ✓

Lessons learned…

1. Both computational and symbolic proofs are not accurate enough to analyse the security of real-world e-voting protocols

- ➡ Considering scenarios with a unique election and a unique ballot-box is too limited…
- ➡ Attacks are missed ✗

2. Considering multiple elections is of worth interest but complexifies the proofs…

- ➡ (probably) true for computational analysis
- ➡ less clear for symbolic analysis due to internal optimizations in tools (e.g. ProVerif) ✓

Open questions

What is the « good » definition of privacy when considering multiple elections ?

Can we capture correlations between voter's votes across elections?

Outline

1. **Belenios: a real-world protocol**
   - description of the protocol
   - expected security properties

2. **Existing attacks and new fixes**

3. **Multi-elections… a true threat…**
   - a new attack against Belenios
   - the Swiss-Post protocol: another victim

4. **Studying new security properties**
   - cast-as-intended
   - accountability

Themis projet

[submission at CCS'22 in preparation]

Context :

- Collaboration with the company IDEMIA started in 2019
- Goal: design a secure e-voting protocol
- Difficulties:
  - vote on electronic devices
  - no printer or the Internet during the voting phase
  - must ensure cast-as-intended
  - must protect the company against false accusation of fraud

My contributions :

- provide a view from an outside perspective
- help to formalise the security properties (e.g., accountability)
- bring my expertise in terms of modeling and symbolic analysis

Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

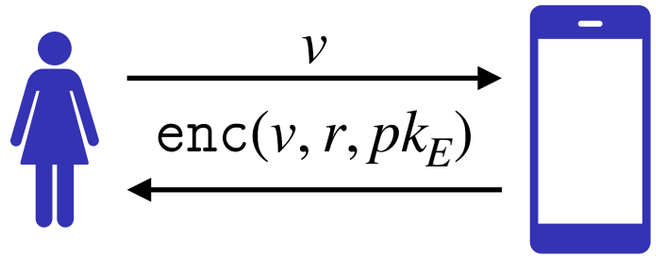
Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)

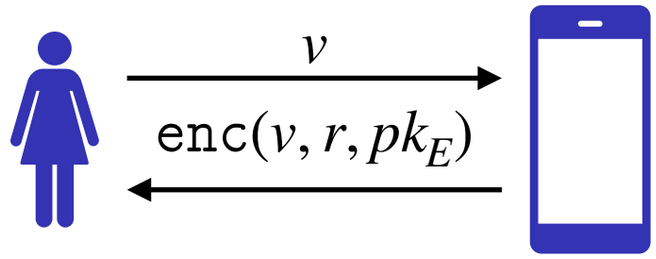


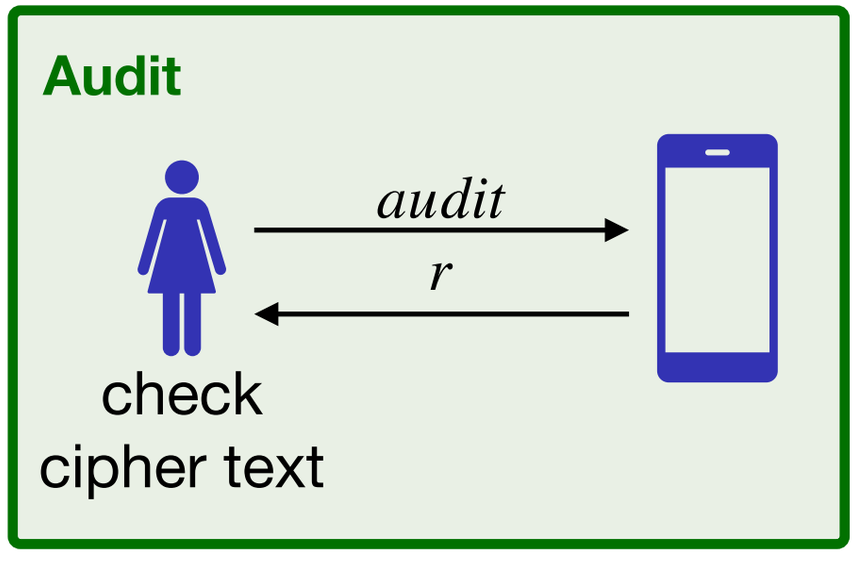
Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)



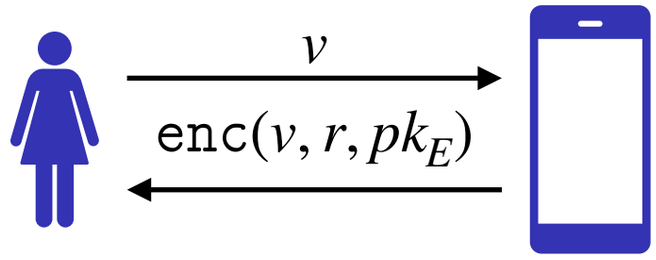


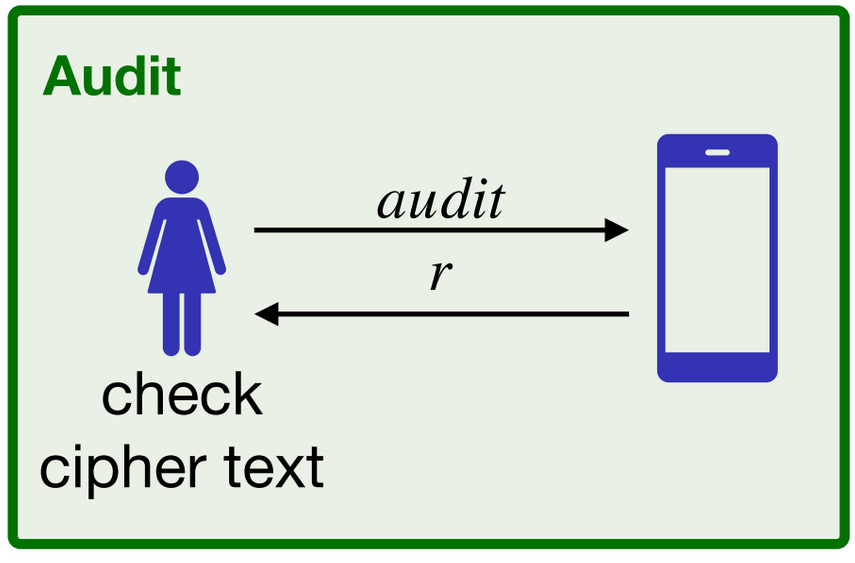
Cast-as-intended

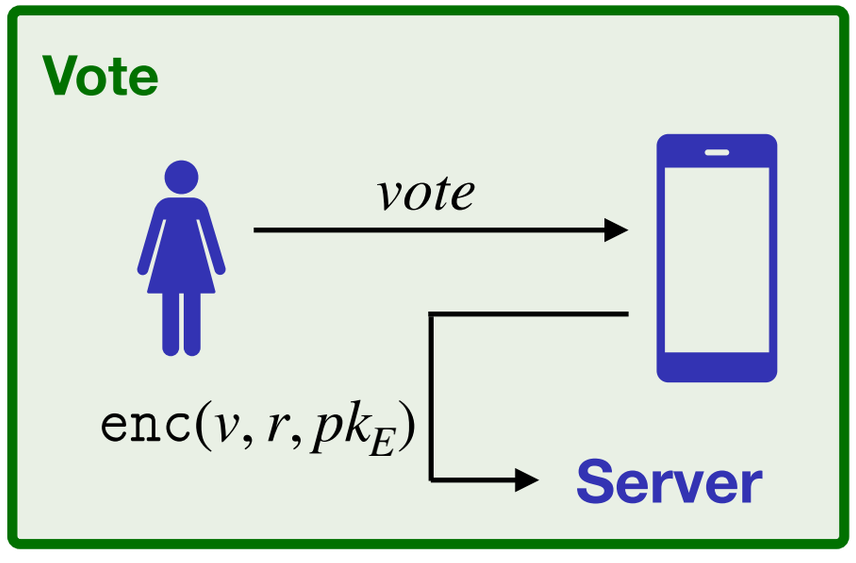
Cast-as-intended - a voter can check her voting device correctly encrypted her vote

Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)





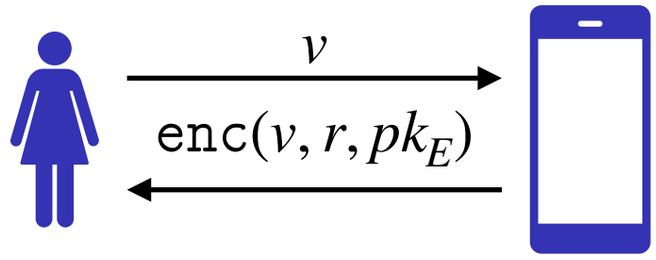


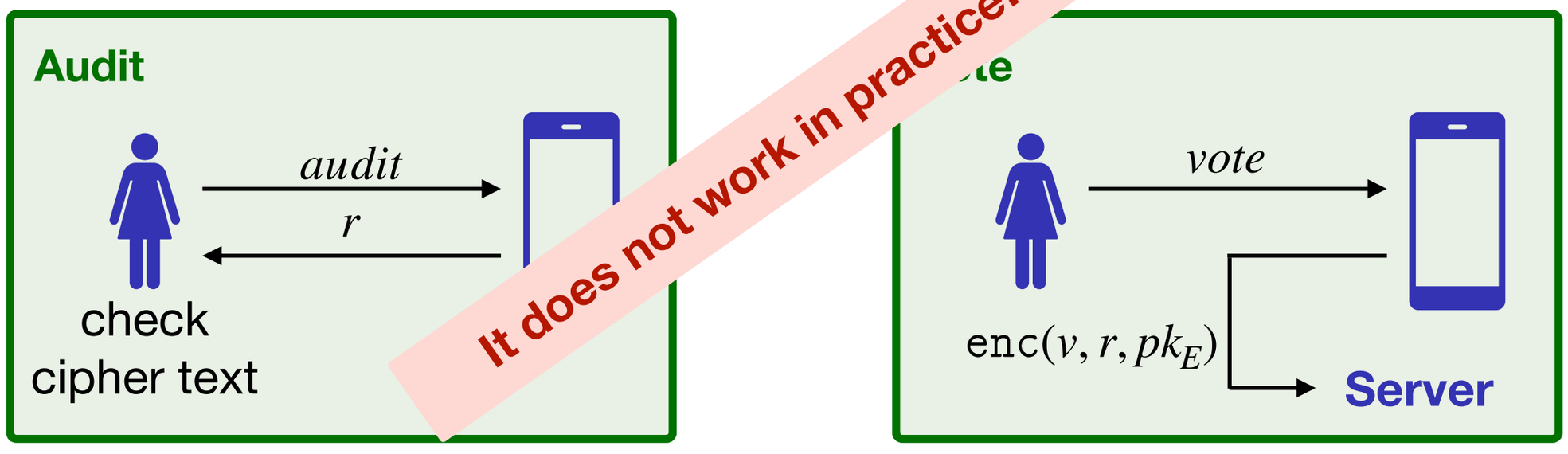
Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)



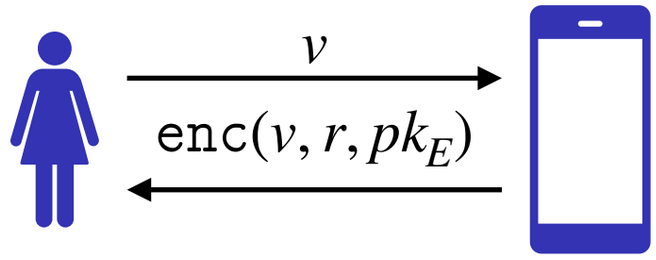


Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

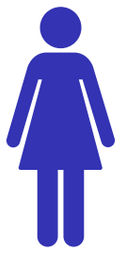
Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

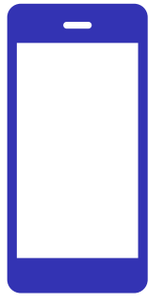
Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)



It does not work in practice…

Solution 3 : Make sure that Alice always audits



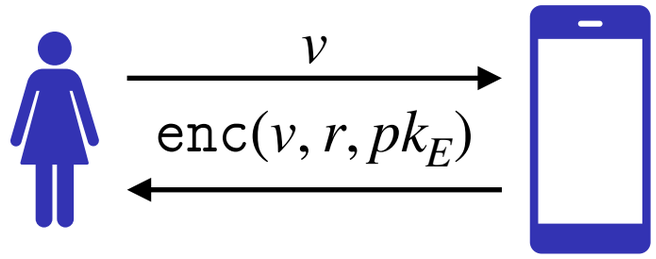


Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

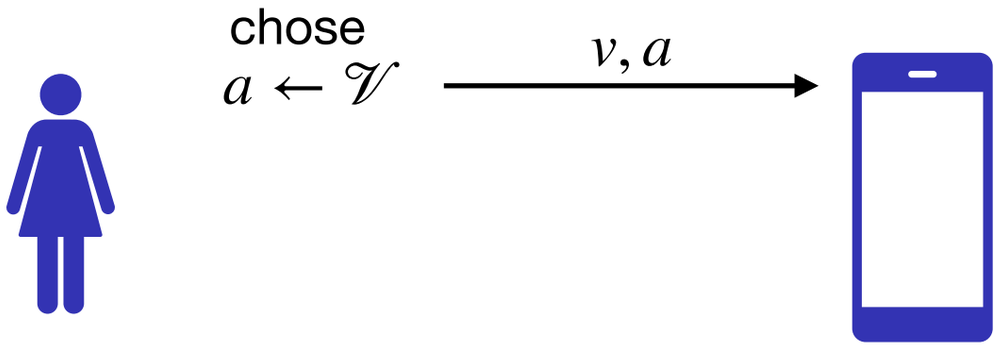
Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)



It does not work in practice…

Solution 3 : Make sure that Alice always audits

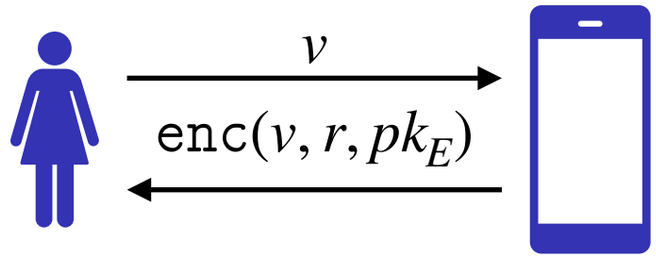


Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

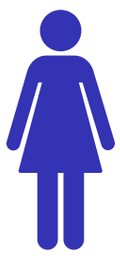
Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)

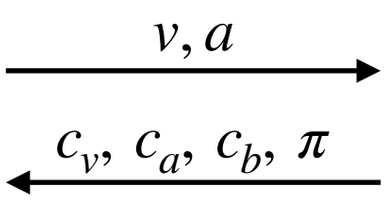


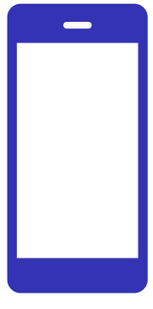
It does not work in practice…

Solution 3 : Make sure that Alice always audits



chose
$a \leftarrow \mathscr{V}$





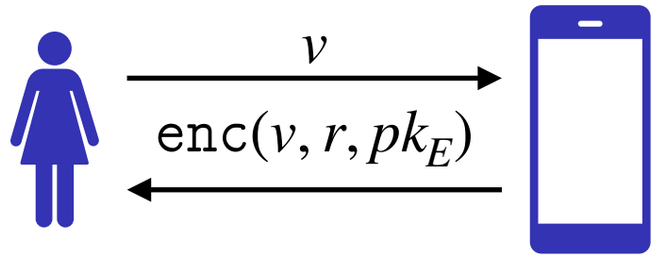
$c_v = \texttt{enc}(v, r_v, pk_E)$
$c_a = \texttt{enc}(a, r_a, pk_E)$
$c_b = \texttt{enc}(v + a, r_b, pk_E)$
π a proof that $ptxt(c_b) = ptxt(c_v) + ptxt(c_a)$

Cast-as-intended

Cast-as-intended - a voter can check her voting device correctly encrypted her vote

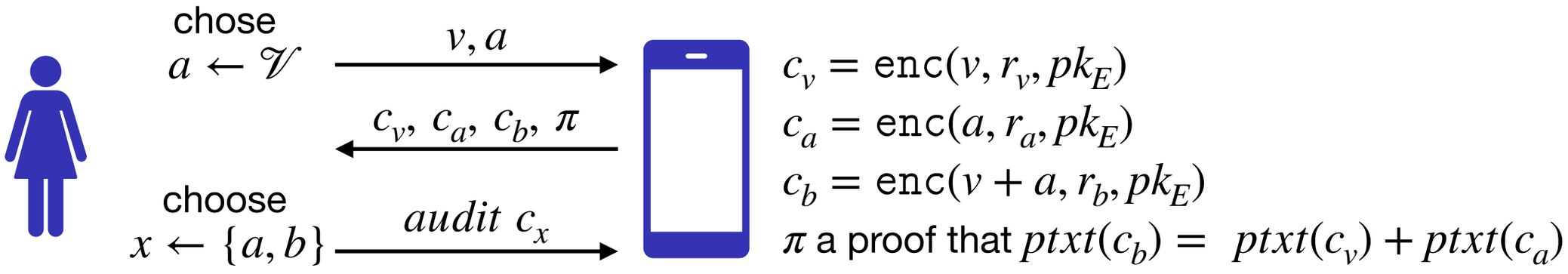
Solution 1 : Alice uses a paper ballot and trust the Print Office
(e.g. the Swiss Post protocol)

Solution 2 : Alice randomly audits electronic ballots
(e.g. Benaloh protocol)



It does not work in practice…

Solution 3 : Make sure that Alice always audits



Proving cast-as-intended

Difficulty 1 - automatic tools does not handle arithmetics

Proving cast-as-intended

Difficulty 1 - automatic tools does not handle arithmetics

- For reachability properties: extract the main properties of the arithmetics that make it works, e.g.,

« For all $x, a \in \mathbb{N}$, there exists $b \in \mathbb{N}$ such that $x = a + b$ »

Proving cast-as-intended

Difficulty 1 - automatic tools does not handle arithmetics

- For reachability properties: extract the main properties of the arithmetics that make it works, e.g.,

  « For all $x, a \in \mathbb{N}$, there exists $b \in \mathbb{N}$ such that $x = a + b$ »

- For equivalence properties: prove that the relation $x = a + b$ is preserved on both sides of the equivalence, i.e.

  « For all $x, a, b \in \mathcal{N}$, if $\texttt{isSum}(x, a, b)$ on the left, then $\texttt{isSum}(x, a, b)$ on the right »

Proving cast-as-intended

Difficulty 1 - automatic tools does not handle arithmetics

- For reachability properties: extract the main properties of the arithmetics that make it works, e.g.,

  « For all $x, a \in \mathbb{N}$, there exists $b \in \mathbb{N}$ such that $x = a + b$ »

- For equivalence properties: prove that the relation $x = a + b$ is preserved on both sides of the equivalence, i.e.

  « For all $x, a, b \in \mathcal{N}$, if $\texttt{isSum}(x, a, b)$ on the left, then $\texttt{isSum}(x, a, b)$ on the right »

Open questions - automatic tools does not handle probabilities

Proving cast-as-intended

Difficulty 1 - automatic tools does not handle arithmetics

- For reachability properties: extract the main properties of the arithmetics that make it works, e.g.,

  « For all $x, a \in \mathbb{N}$, there exists $b \in \mathbb{N}$ such that $x = a + b$ »

- For equivalence properties: prove that the relation $x = a + b$ is preserved on both sides of the equivalence, i.e.

« For all $x, a, b \in \mathcal{N}$, if $\texttt{isSum}(x, a, b)$ on the left, then $\texttt{isSum}(x, a, b)$ on the right »

Open questions - automatic tools does not handle probabilities

- Extend models with probabilities: not so easy…
  but some works exist or are in progress
- Adapt tools or find simplification results to encode it in the existing frameworks

Accountability

“ The integrity of an election is guaranteed if all the checks performed by auditors succeed. ”

Accountability

> “ The integrity of an election is guaranteed if all the checks performed by auditors succeed. ”

What happens if a check fails?

Accountability

> “ The integrity of an election is guaranteed if all the checks performed by auditors succeed. ”

What happens if a check fails?

In the models: the protocol stops and restarts from the beginning!

Accountability

> “ The integrity of an election is guaranteed if all the checks performed by auditors succeed. ”

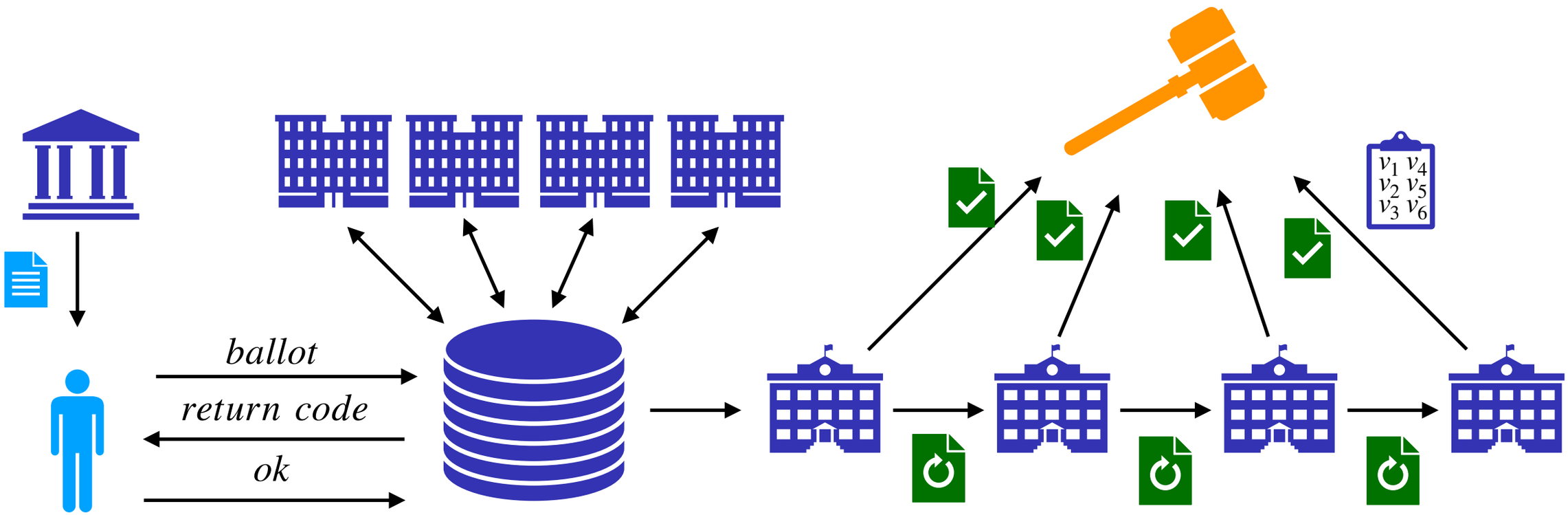
What happens if a check fails?

Not acceptable in practice!

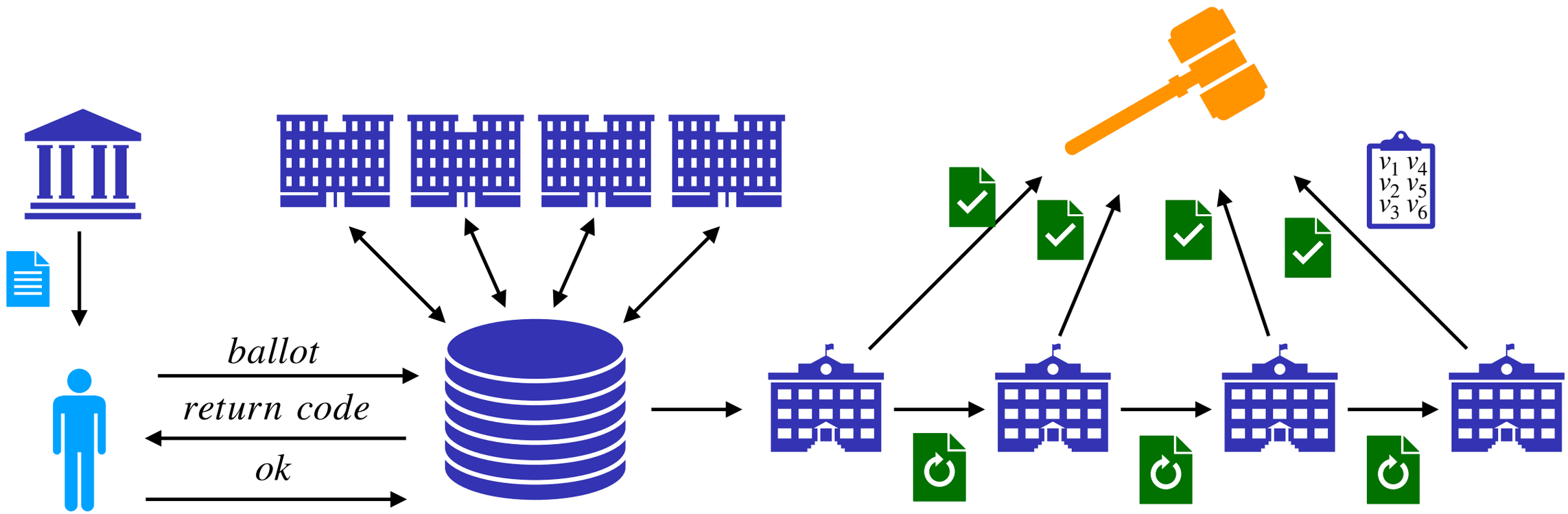
~~**In the models:** the protocol stops and restarts from the beginning!~~

In practice… the protocol continues et all the security is lost…

Accountability

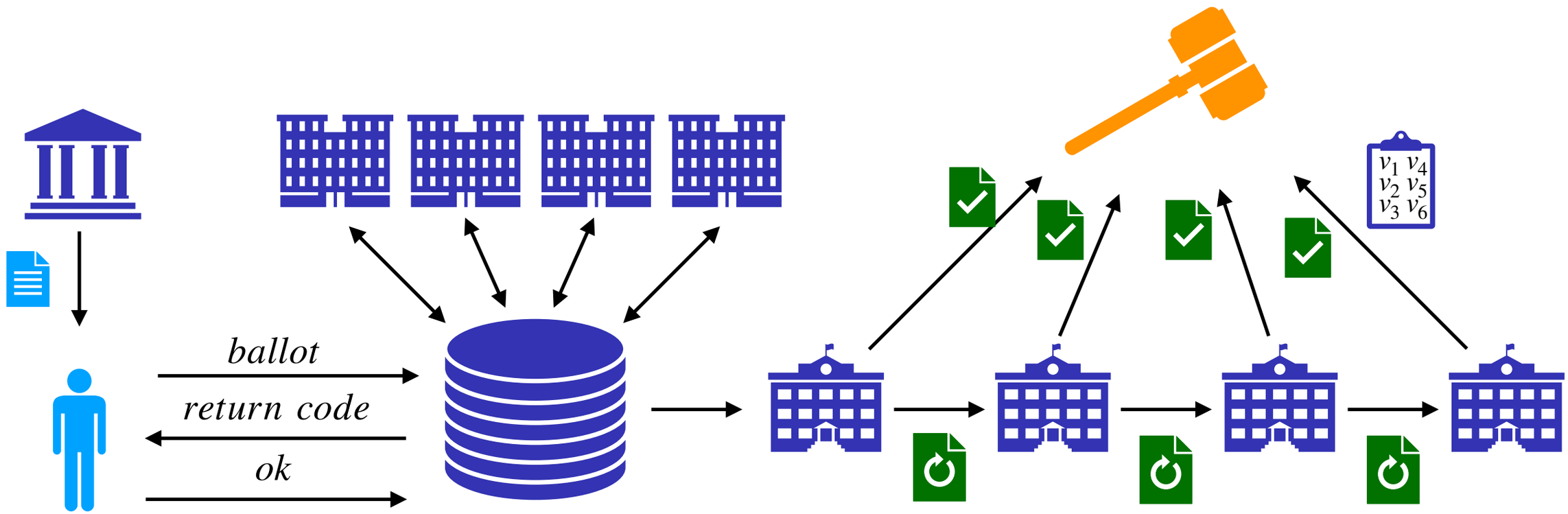


Accountability



Questions : ▸ what happens if something went wrong? we cannot stop and restart…

Accountability



Questions :
- what happens if something went wrong? we cannot stop and restart…
- can we blame/prosecute someone?

Accountability

Accountability - each time an error occurs, a participant can be prosecuted

⚠️ nobody should be wrongly blamed

Accountability

Accountability - each time an error occurs, a participant can be prosecuted

⚠️ nobody should be wrongly blamed

Our approach on a specific e-voting protocol

- assume an honest trusted party, i.e., a judge with whom all the participants can securely communicate
- design a dispute resolution procedure to identify culprits
- use signatures to authenticates the messages

Accountability

Accountability - each time an error occurs, a participant can be prosecuted

⚠ nobody should be wrongly blamed

Our approach on a specific e-voting protocol

- assume an honest trusted party, i.e., a judge with whom all the participants can securely communicate
- design a dispute resolution procedure to identify culprits
- use signatures to authenticates the messages

Open questions

- can we define a framework to formalise our approach?
- can we develop a generic approach that applies to other e-voting protocols?
  - for now, the dispute resolution is quite intrusive…
  - sign all the messages is expensive… and not enough in most cases…
- can it be adapted to other applications, e.g. payment, IoT…?

Conclusion

Conclusion

Design and prove the security of an e-voting protocol is difficult… even for experts!

(e.g., attacks against Belenios or Swiss-Post protocol)

Conclusion

Design and prove the security of an e-voting protocol is difficult… even for experts!

(e.g., attacks against Belenios or Swiss-Post protocol)

« A protocol that is not formally proved secure is probably flawed! »

Conclusion

Design and prove the security of an e-voting protocol is difficult… even for experts!

(e.g., attacks against Belenios or Swiss-Post protocol)

« A protocol that is not formally proved secure is probably flawed! »

⚠️ inverse implication is false!

Conclusion

Design and prove the security of an e-voting protocol is difficult… even for experts!

(e.g., attacks against Belenios or Swiss-Post protocol)

« A protocol that is not formally proved secure is probably flawed! »

⚠️ inverse implication is false!

Open questions to improve the inverse implication:

- improve the expressivity of the verification tools (e.g. probabilities)
- improve the accuracy of the scenarios under study (e.g. multi-elections)
- keep on working on the definitions of the security properties (e.g. accountability)