A privacy attack on the Swiss Post e-voting system

Véronique Cortier, Alexandre Debant, and Pierrick Gaudry

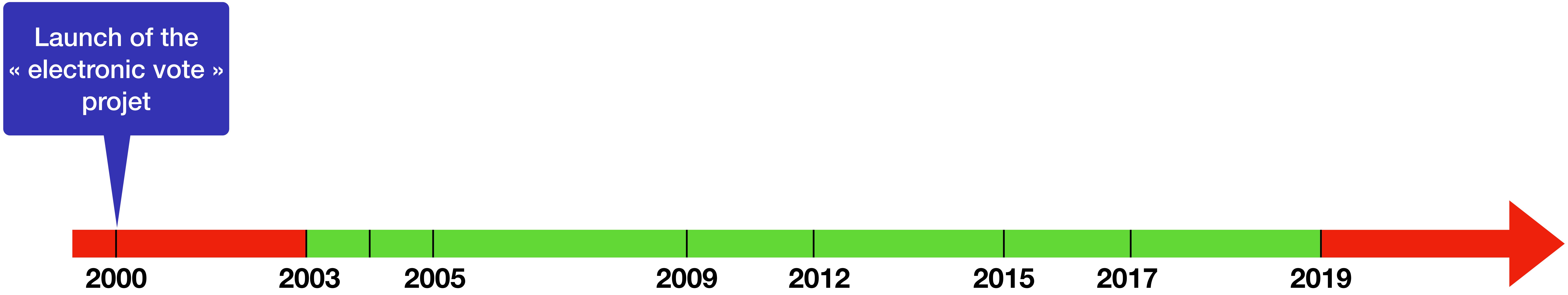
*Université de Lorraine, CNRS, Inria, LORIA,
Nancy, France*

RWC'22

Amsterdam, April 13th 2022

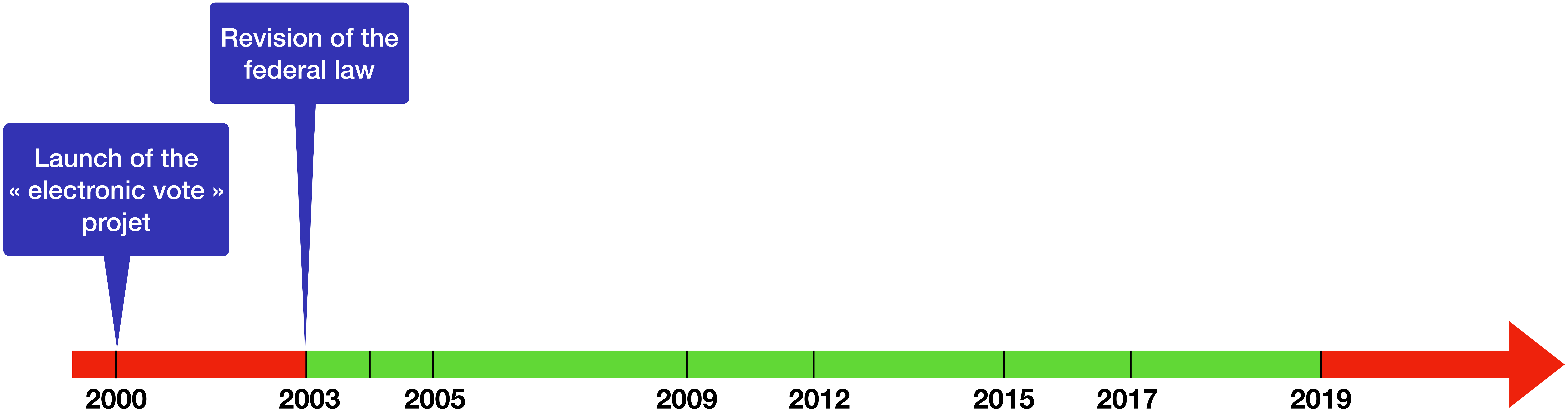
Laboratoire lorrain de recherche en informatique et ses applications

A brief history



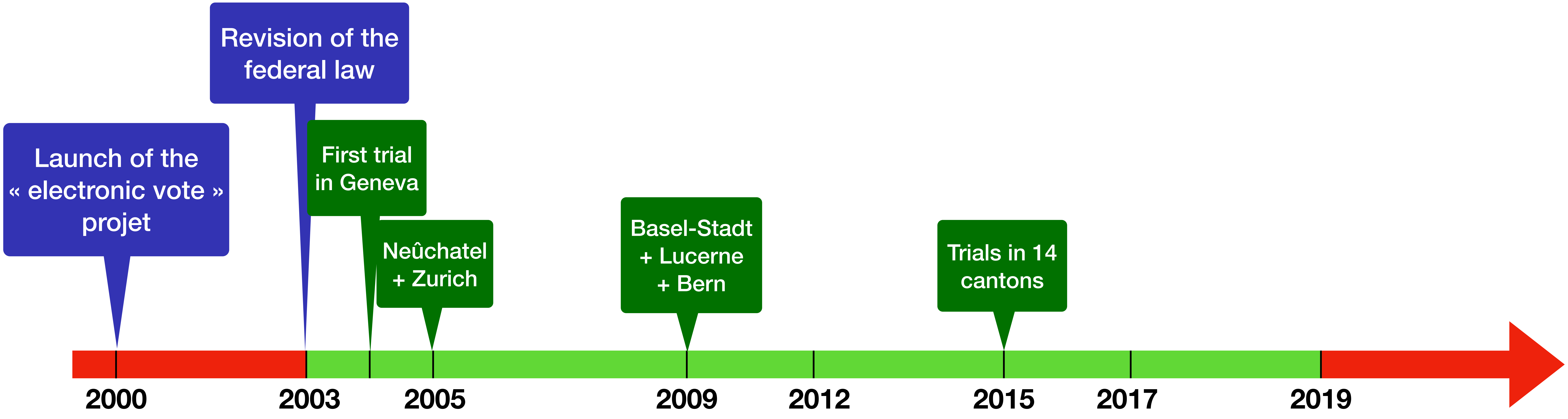
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/chronik.html

A brief history



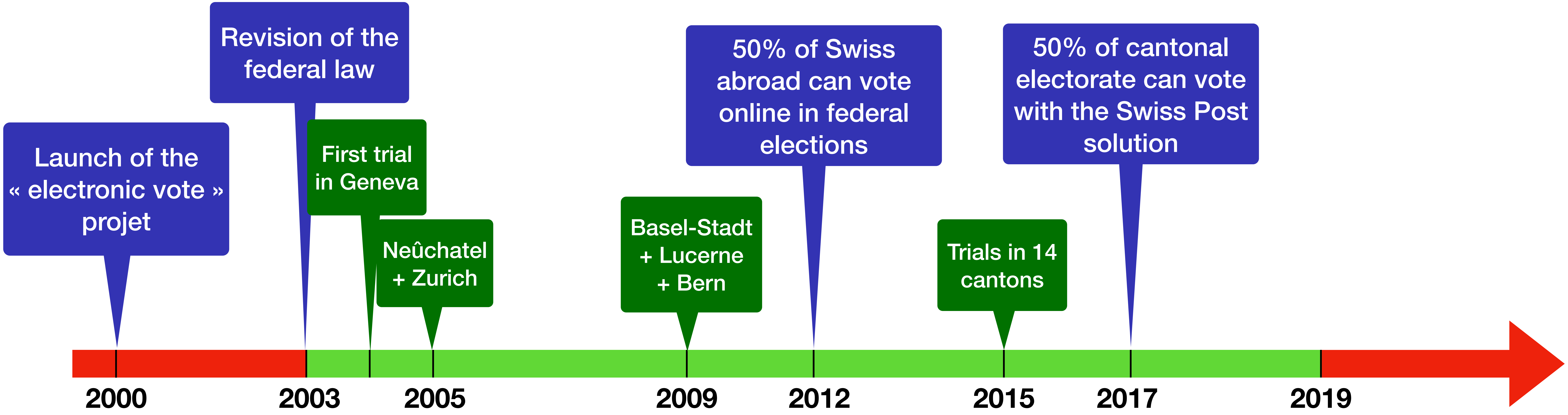
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/chronik.html

A brief history



https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/chronik.html

A brief history



https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/chronik.html

A brief history

https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/chronik.html

Strategy of the Chancellerie

1. discuss with experts to:
   - define a very precise threat model
   - obtain audits the system
   - obtain formal proofs (symbolic and computational)

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.

2. push for public scrutiny: (especially since 2019)
   - public release of the specification and the code
   - organise public intrusion tests
   - prod companies to organise a bug bounty program

Art. 7a[4] Publication of the source code

[1] The source code for the system software must be made public.

https://www.fedlex.admin.ch/eli/cc/2013/859/en
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsbedingungen.html

Strategy of the Chancellerie

1.discuss with experts to:

- define a very precise threat model
- obtain audits the system
- obtain formal proofs (symbolic and computational)

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.

2. push for public scrutiny: (especially since 2019)

- public release of the specification and the code
- organise public intrusion tests
- prod companies to organise a bug bounty program

Art. 7a[4] Publication of the source code

[1] The source code for the system software must be made public.

Target: re-introduce e-voting in September 2022

https://www.fedlex.admin.ch/eli/cc/2013/859/en
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsbedingungen.html

Swiss-Post system

Context :

- Swiss Post bought Scytl's solution in 2020
- Fixed vulnerabilities
- Improved the code and the specification

Swiss-Post system

Context :

- Swiss Post bought Scytl's solution in 2020
- Fixed vulnerabilities
- Improved the code and the specification

We have been contacted to update the symbolic proofs of the systems.

Swiss-Post system

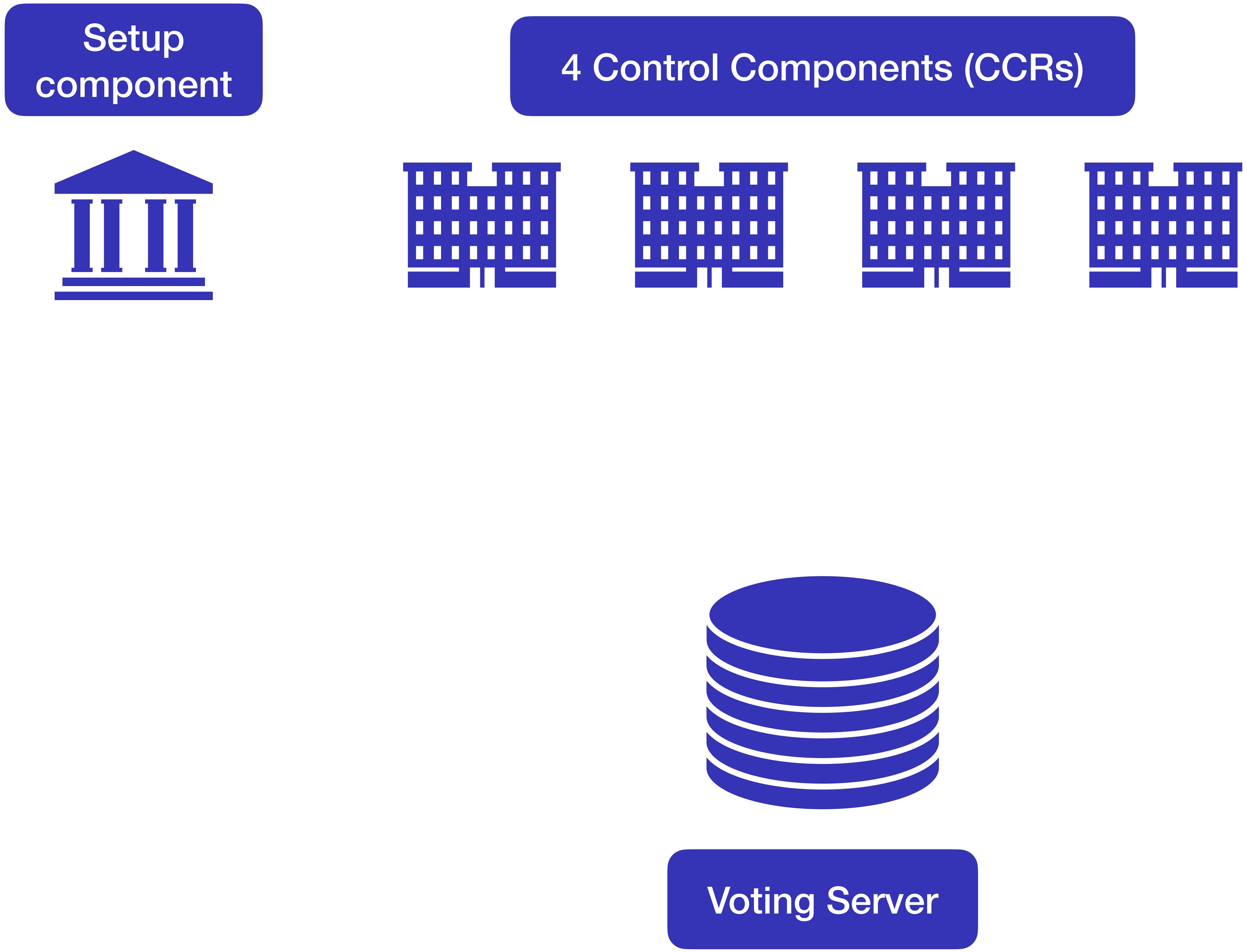
Context :

- Swiss Post bought Scytl's solution in 2020
- Fixed vulnerabilities
- Improved the code and the specification

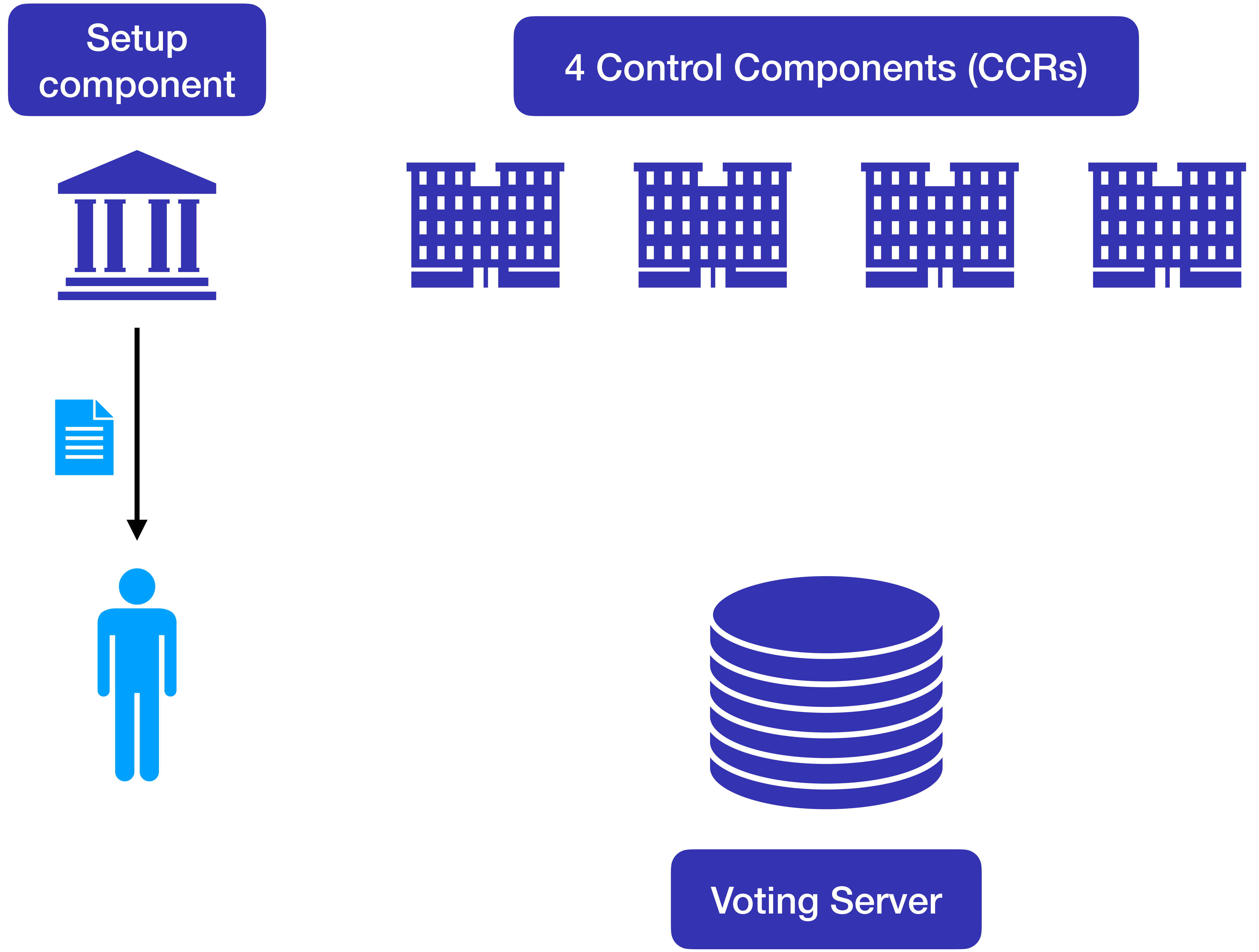
We have been contacted to update the symbolic proofs of the systems.

There is a vote secrecy attack: an attacker can learn the vote of everyone!

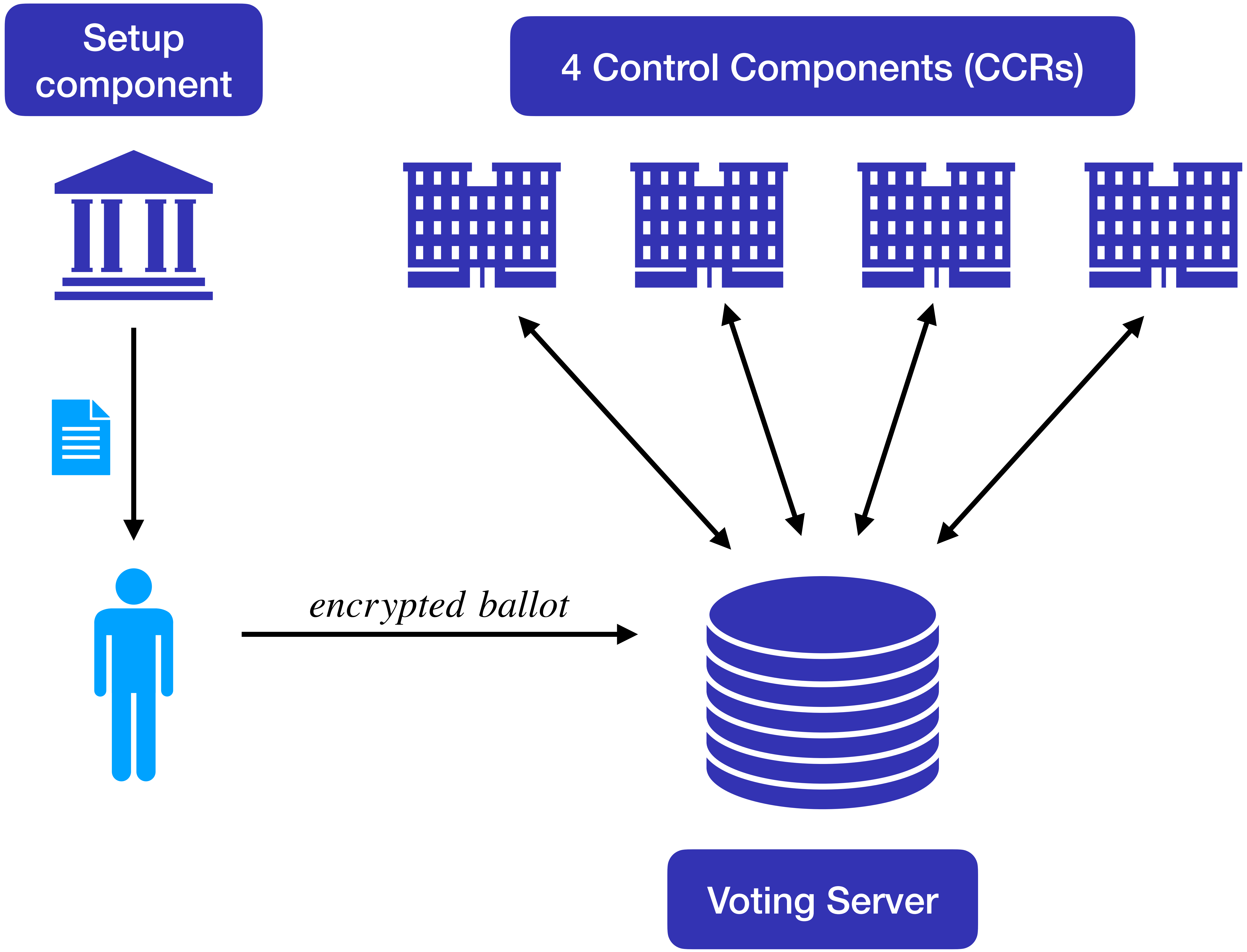
Overview of the system



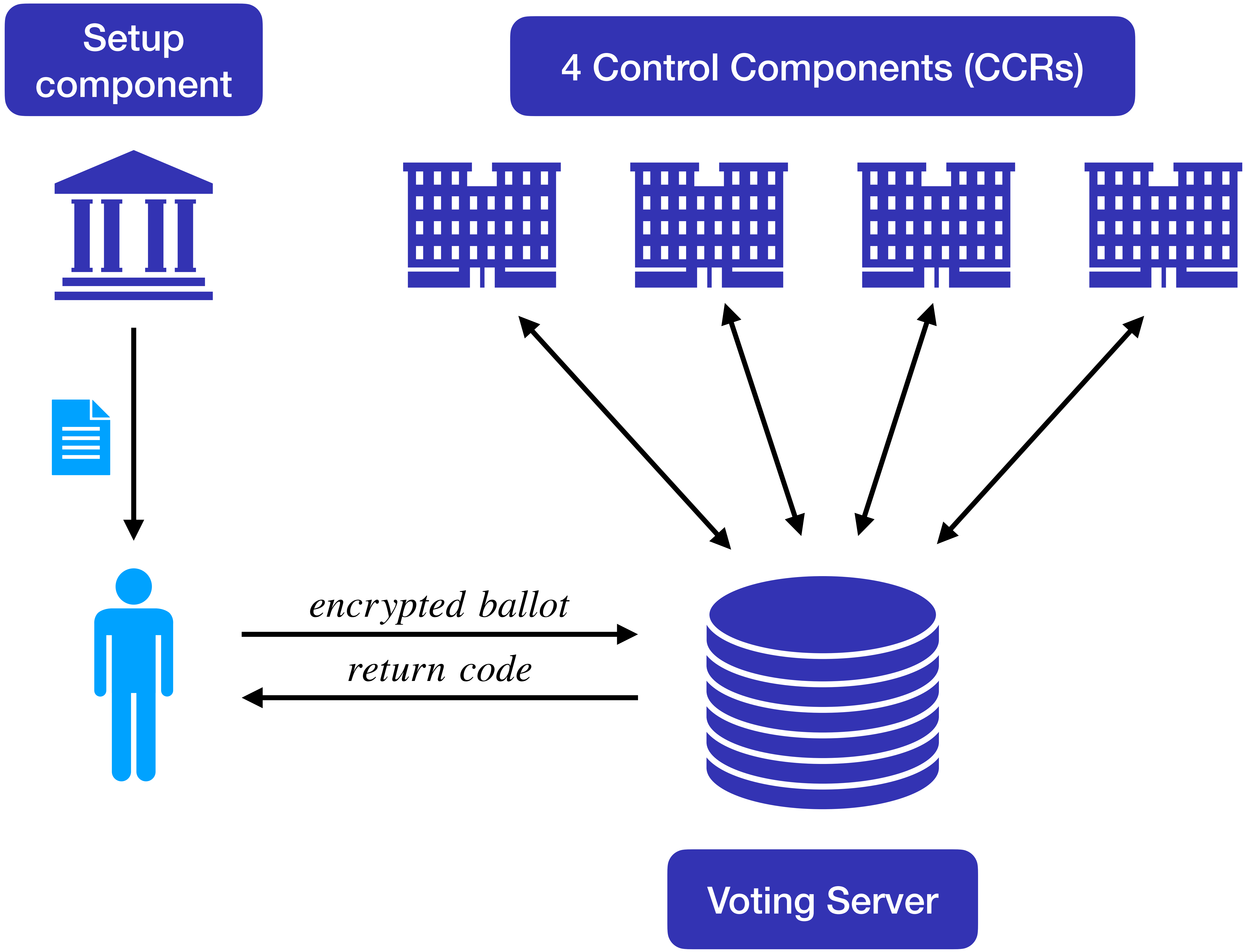
Overview of the system



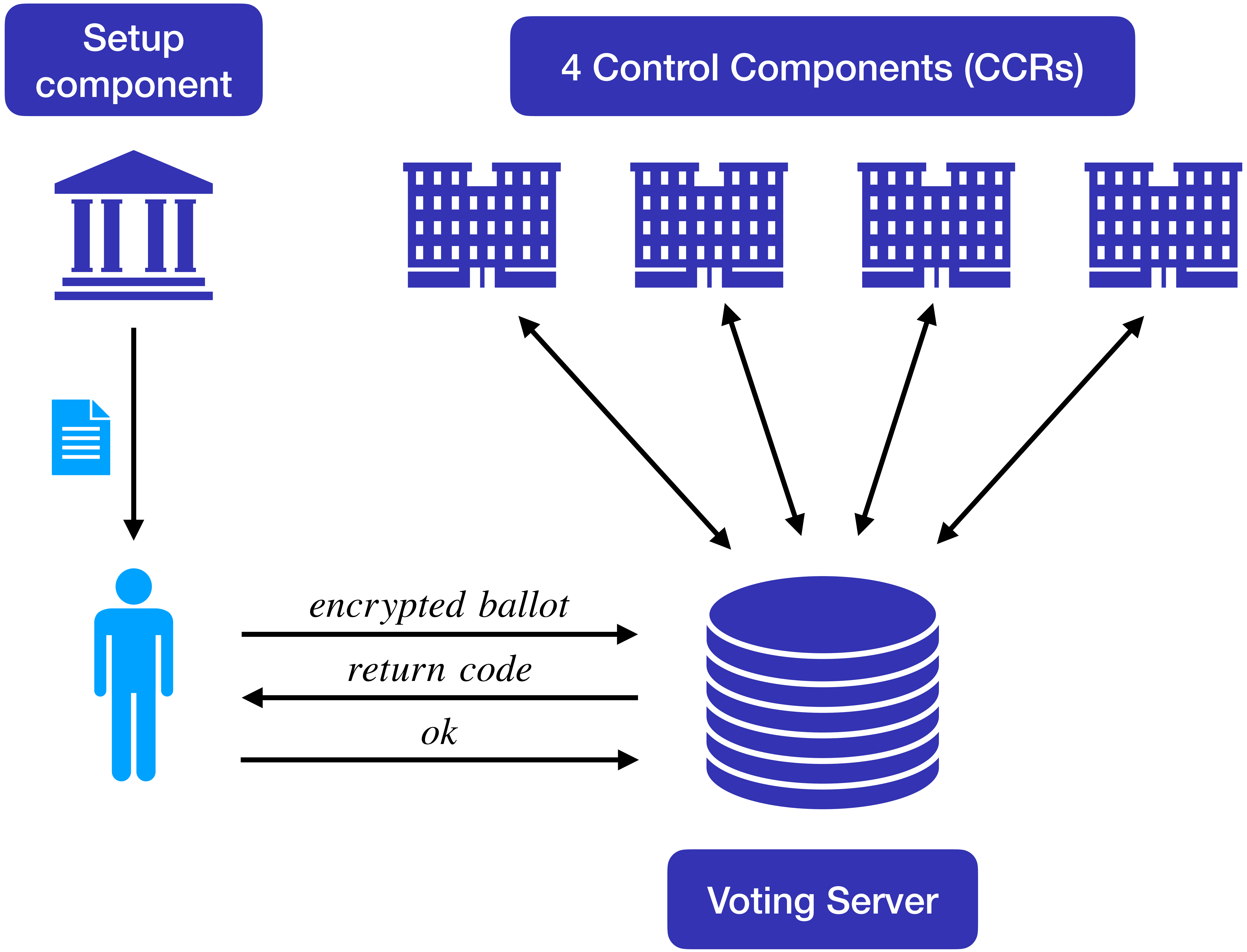
Overview of the system



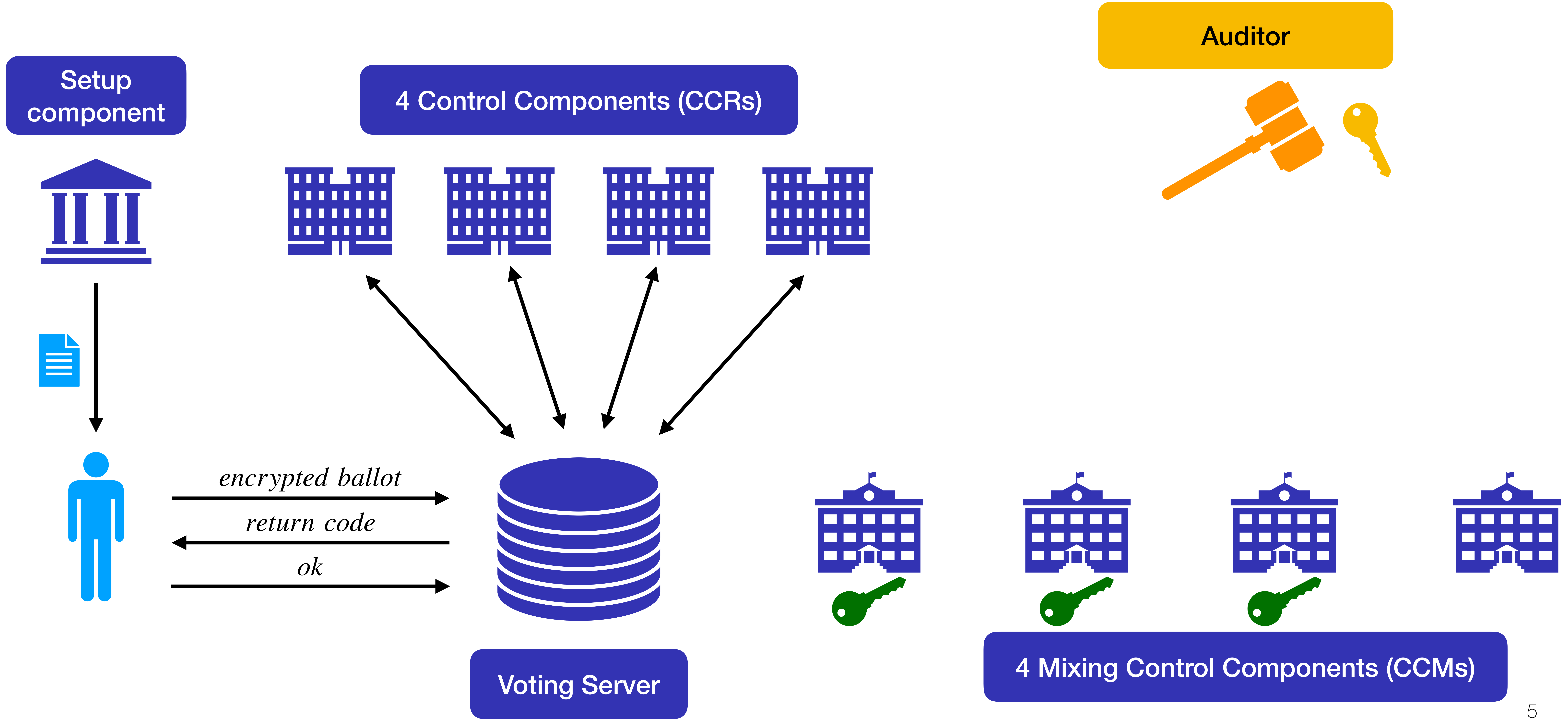
Overview of the system



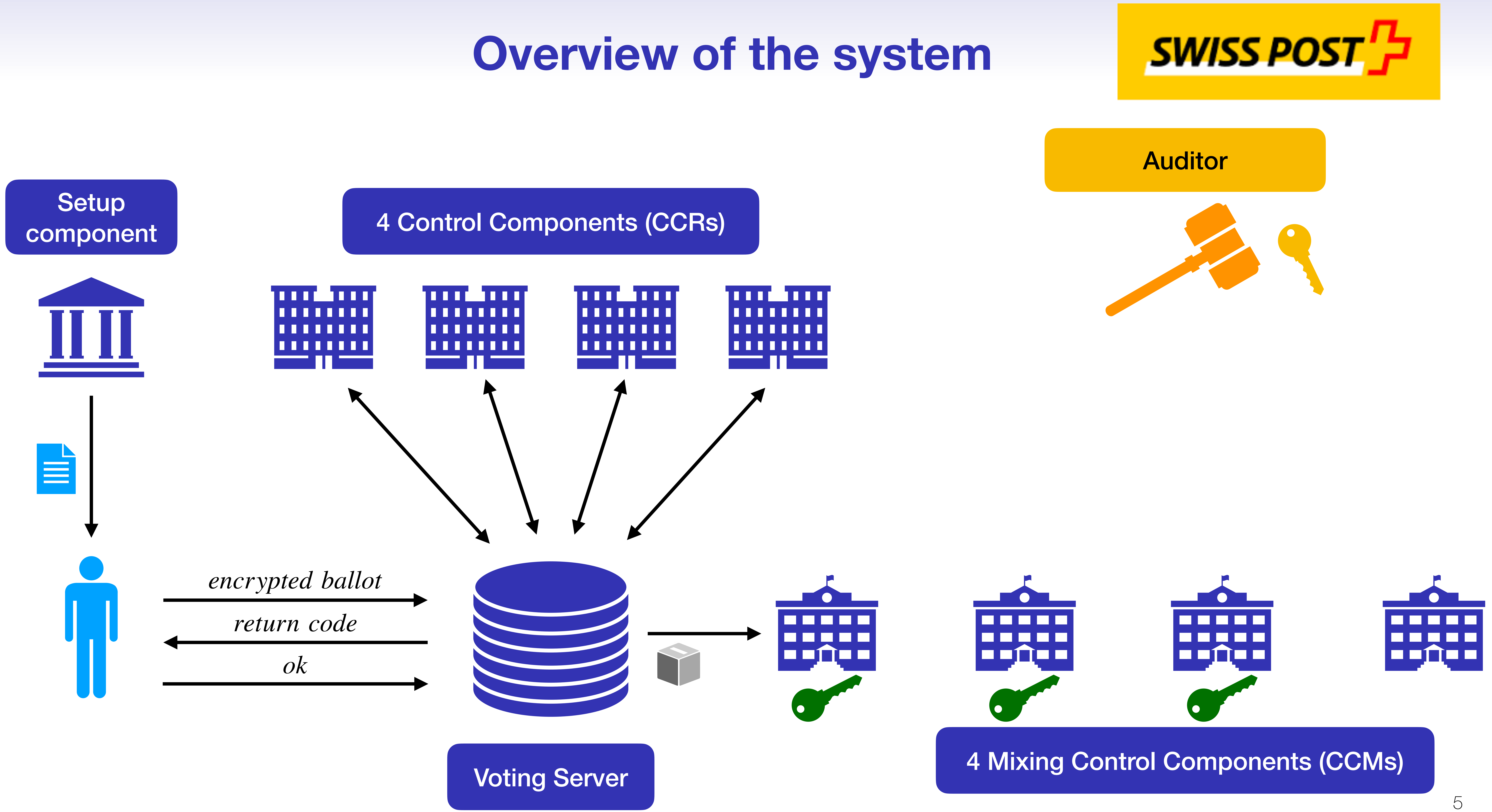
Overview of the system



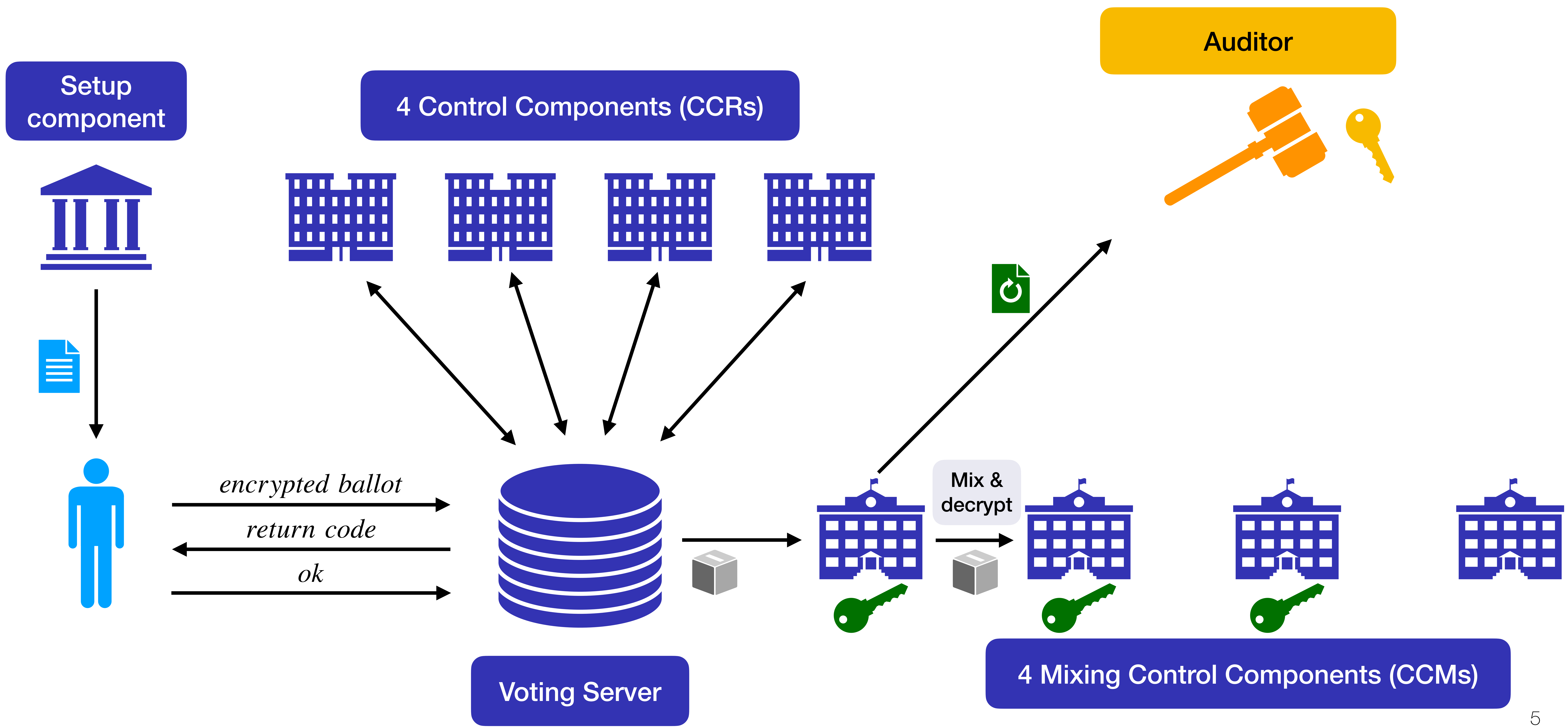
Overview of the system



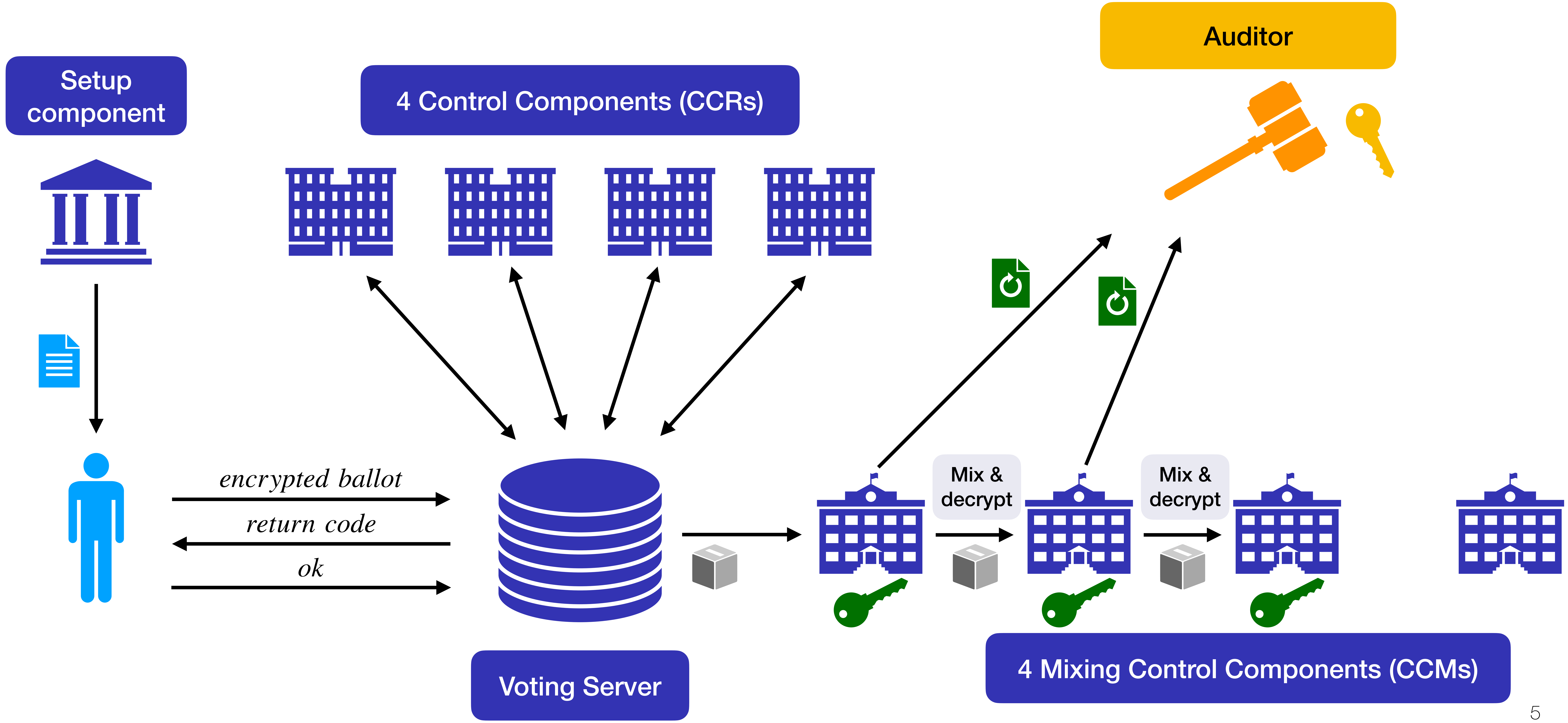
Overview of the system



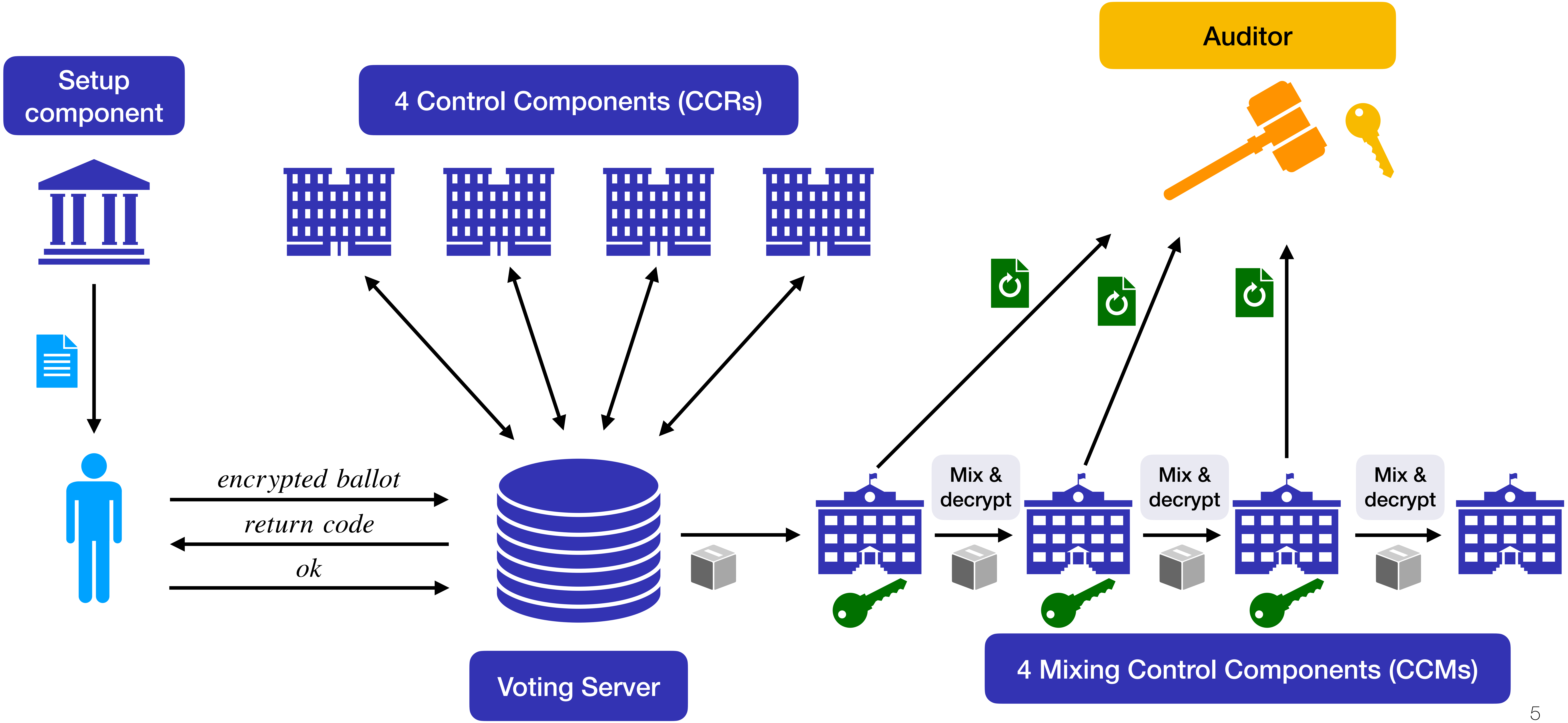
Overview of the system



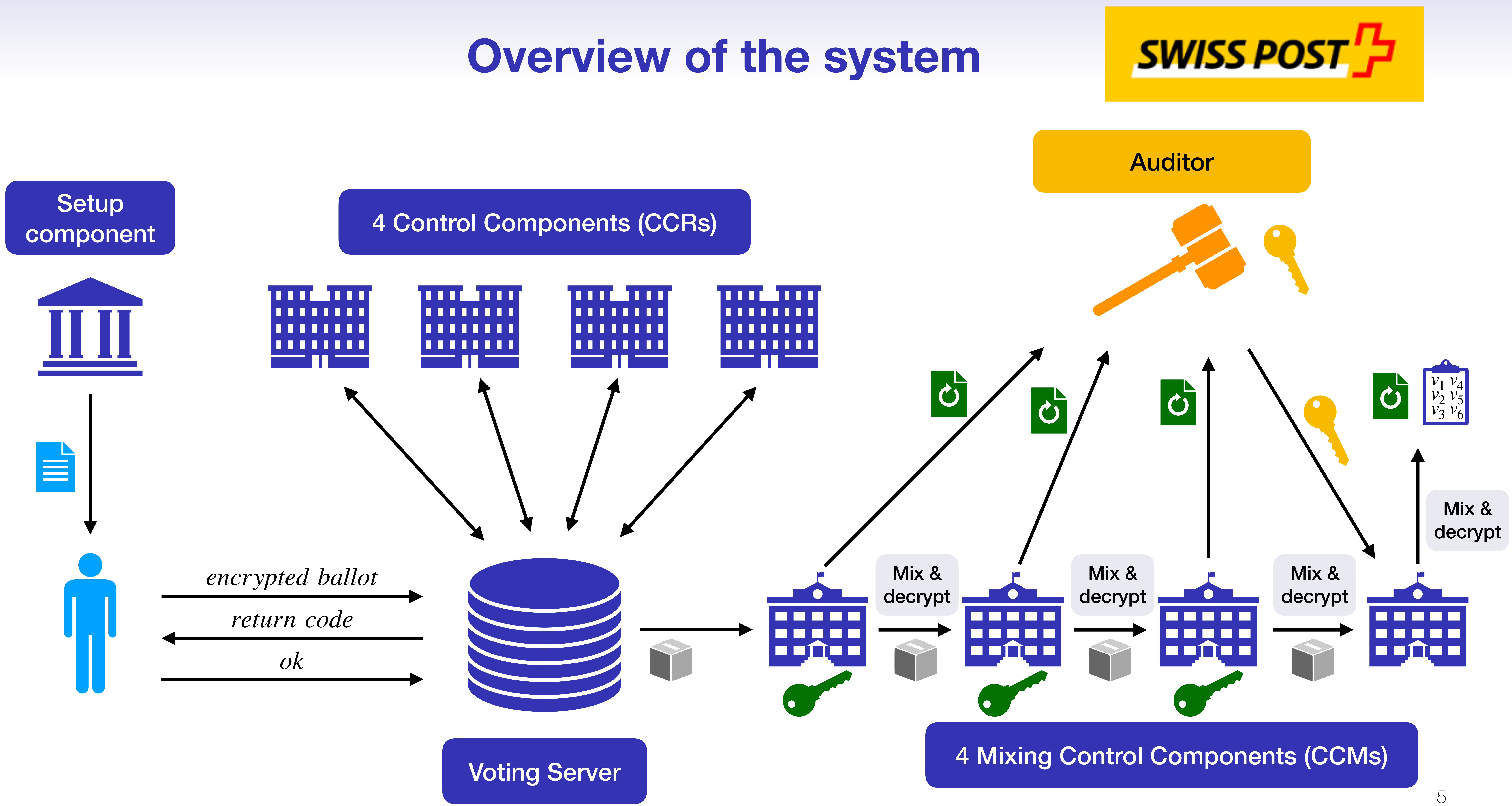
Overview of the system



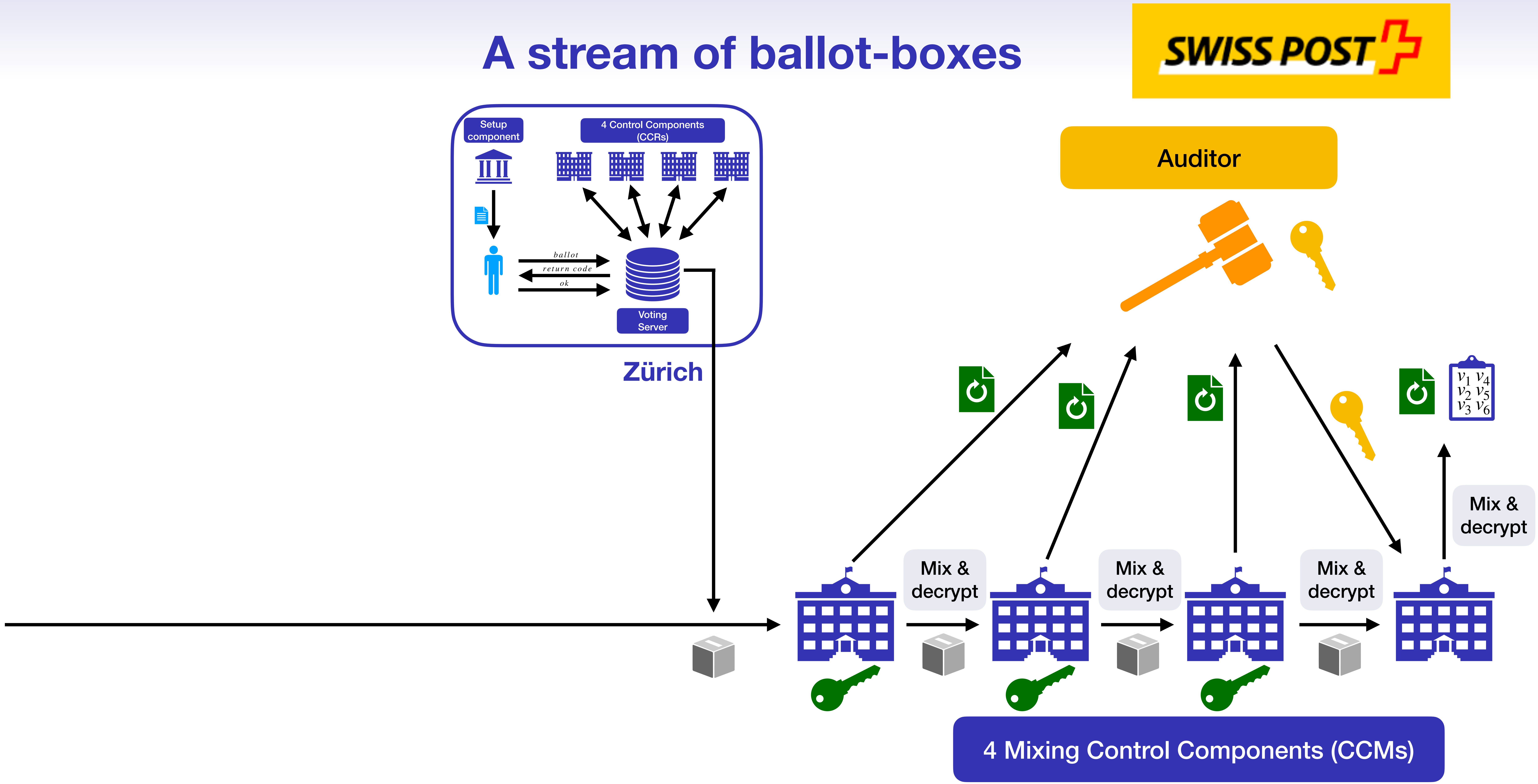
Overview of the system



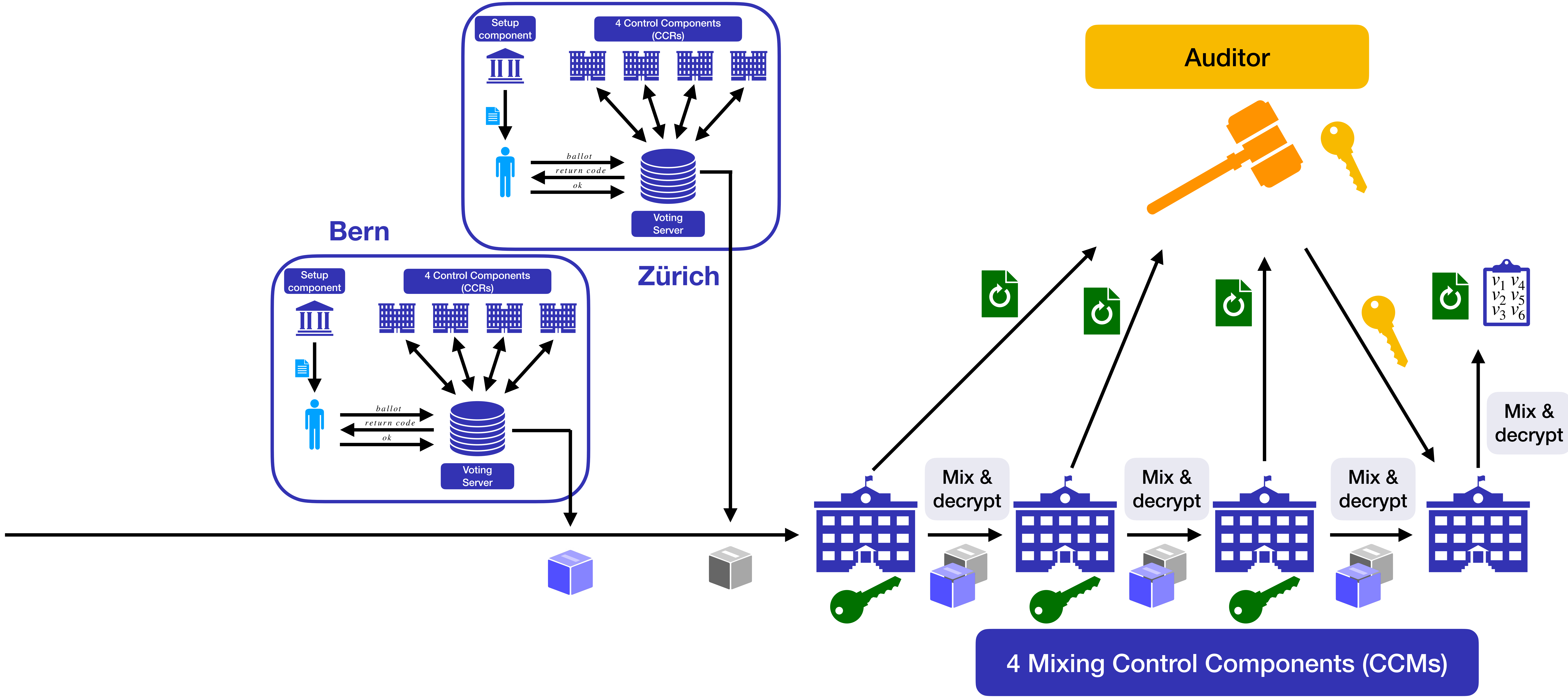
Overview of the system



A stream of ballot-boxes



A stream of ballot-boxes



A stream of ballot-boxes

Vote secrecy

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

https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

Vote secrecy

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

Federal chancellerie requirements:

2.9.3.1 The following system participants are regarded as untrustworthy:

- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters

2.9.3.2 The following system participants may be considered trustworthy:

- set-up component
- print component
- user device
- one of four control components per group, leaving open which one it is
- one auditor in any group, leaving open which auditor it is; Number 2.7.2 takes precedence

https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

Vote secrecy

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

Federal chancellerie requirements:

2.9.3.1 The following system participants are regarded as untrustworthy:

- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters

2.9.3.2 The following system participants may be considered trustworthy:

- set-up component
- print component
- user device
- one of four control components per group, leaving open which one it is
- one auditor in any group, leaving open which auditor it is; Number 2.7.2 takes precedence

The judge/auditor is trusted

https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

Vote secrecy

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

Federal chancellerie requirements:

Only 1 CCM is trusted

The judge/auditor is trusted

2.9.3.1 The following system participants are regarded as untrustworthy:

- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters

2.9.3.2 The following system participants may be considered trustworthy:

- set-up component
- print component
- user device
- one of four control components per group, leaving open which one it is
- one auditor in any group, leaving open which auditor it is; Number 2.7.2 takes precedence

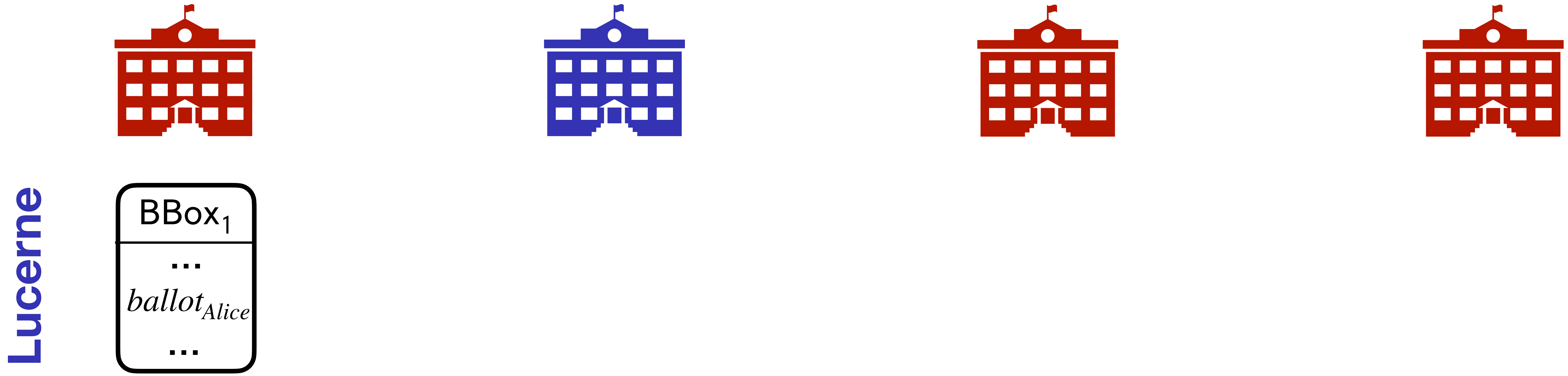
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

A stream of ballot-boxes

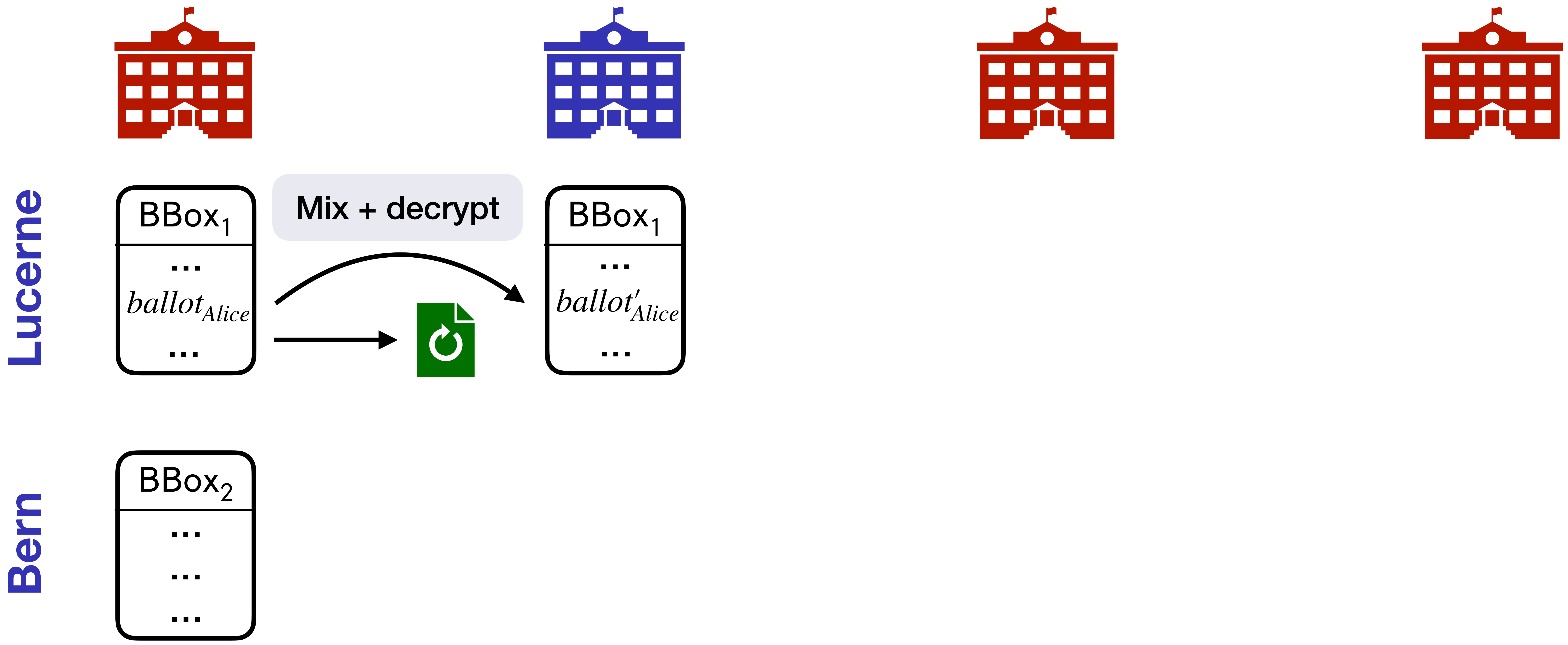
A stream of ballot-boxes

A vote secrecy attack

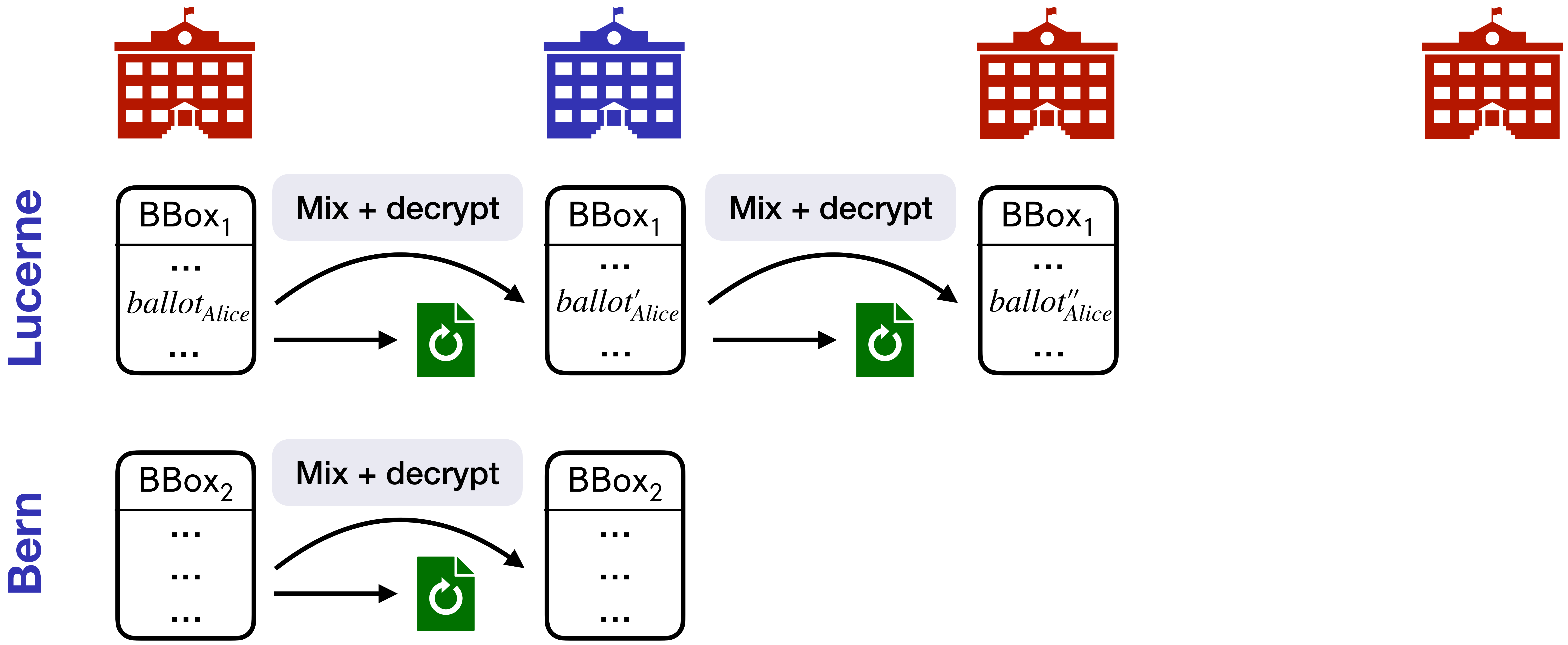
A vote secrecy attack



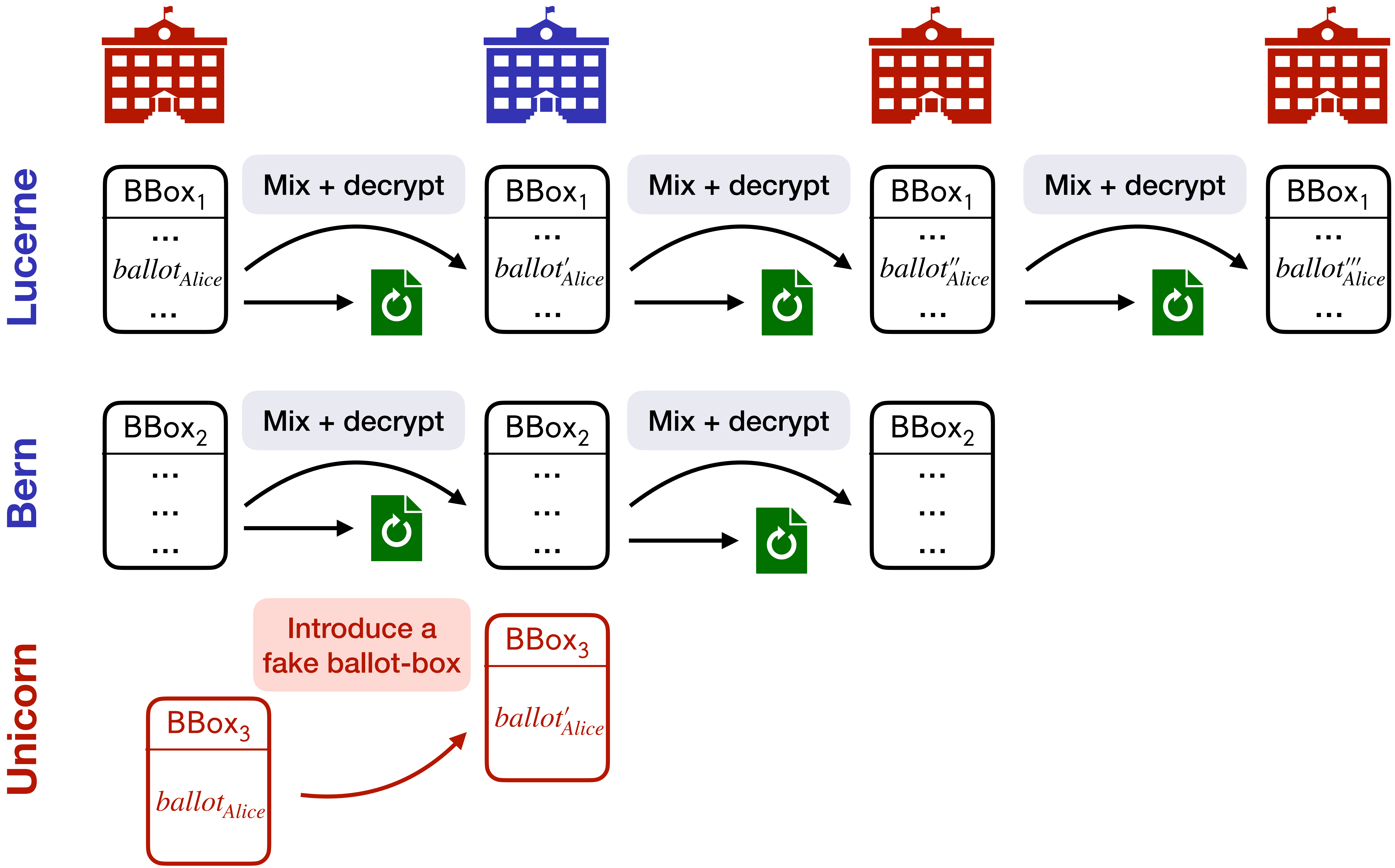
A vote secrecy attack



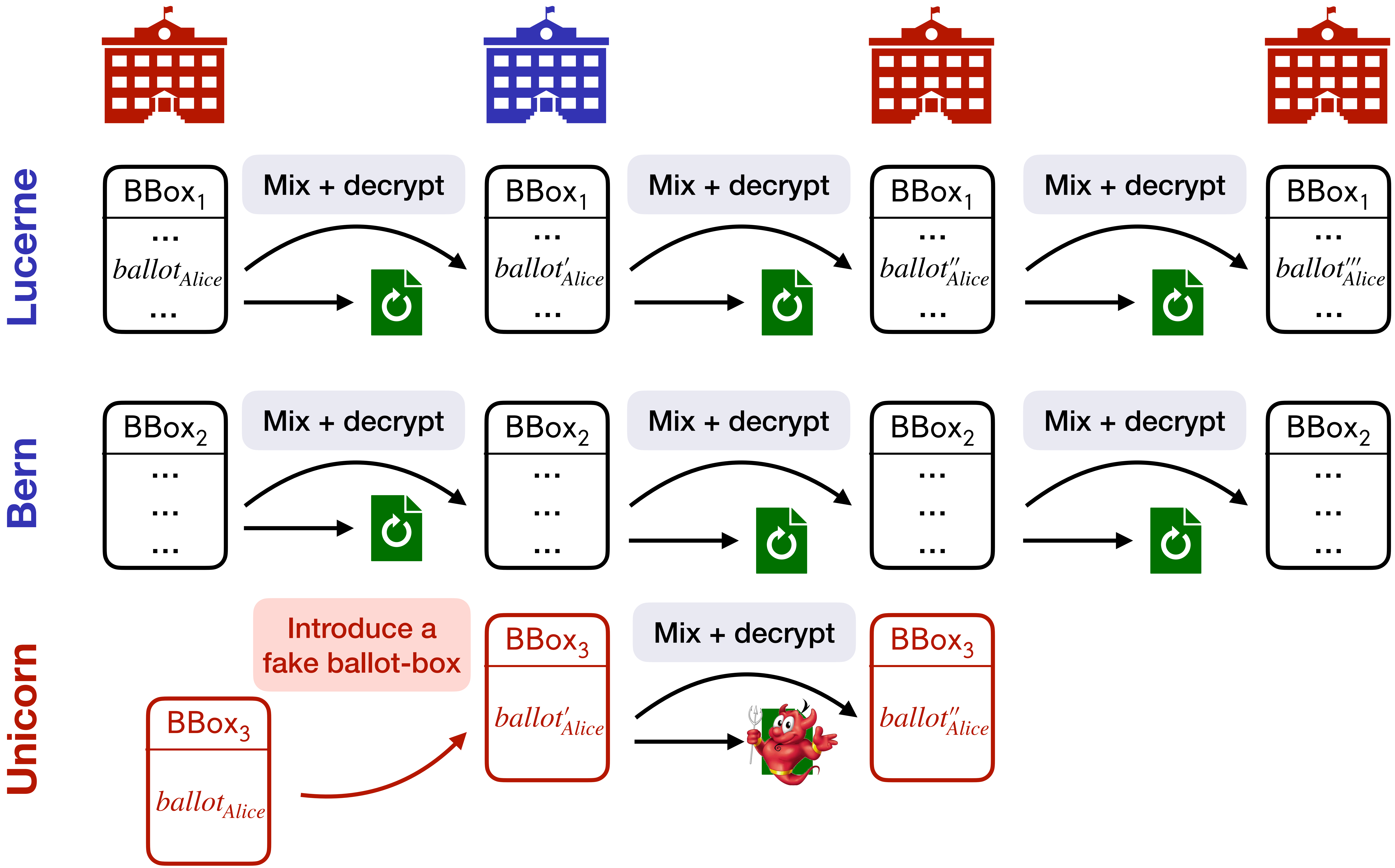
A vote secrecy attack



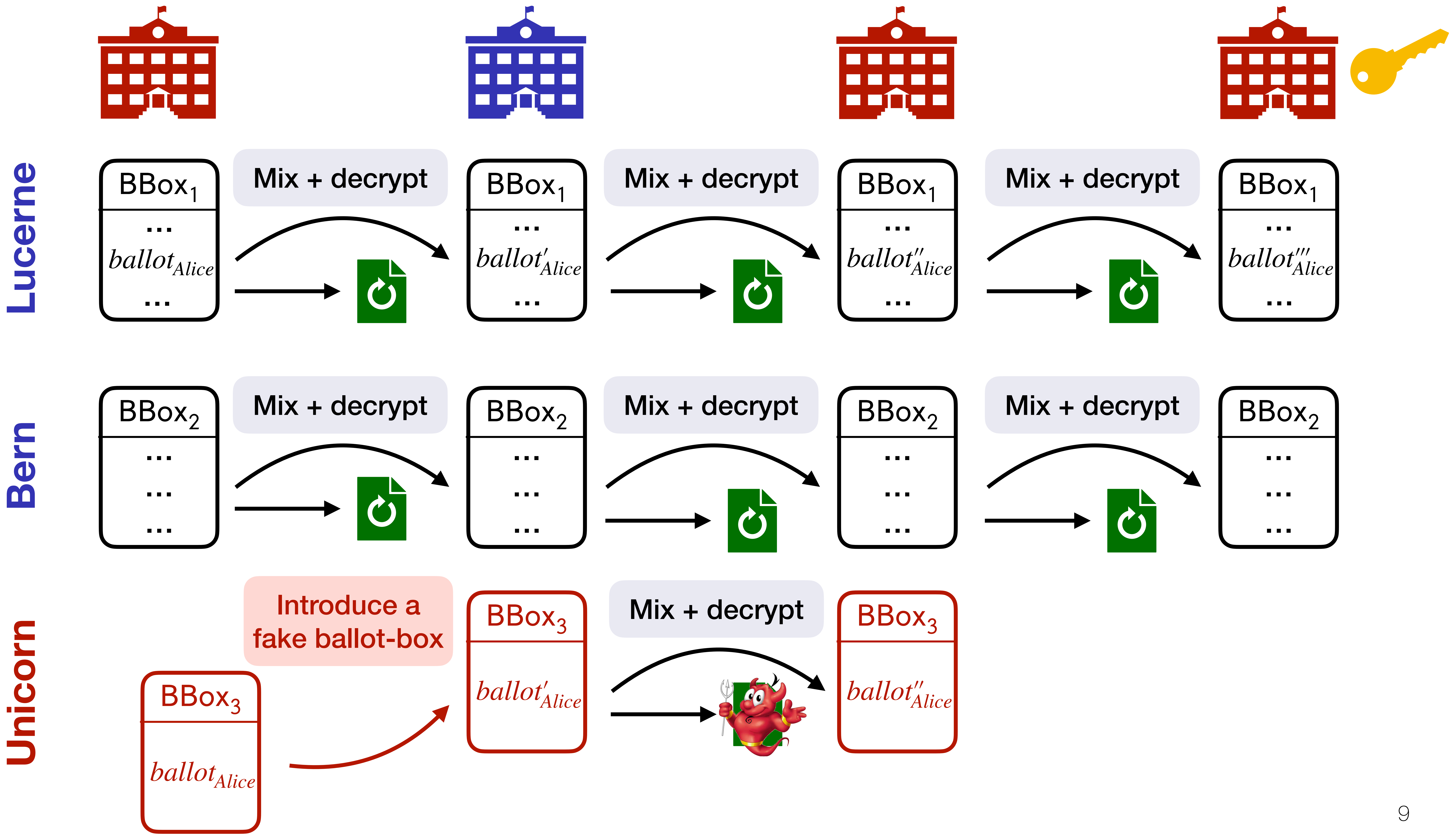
A vote secrecy attack



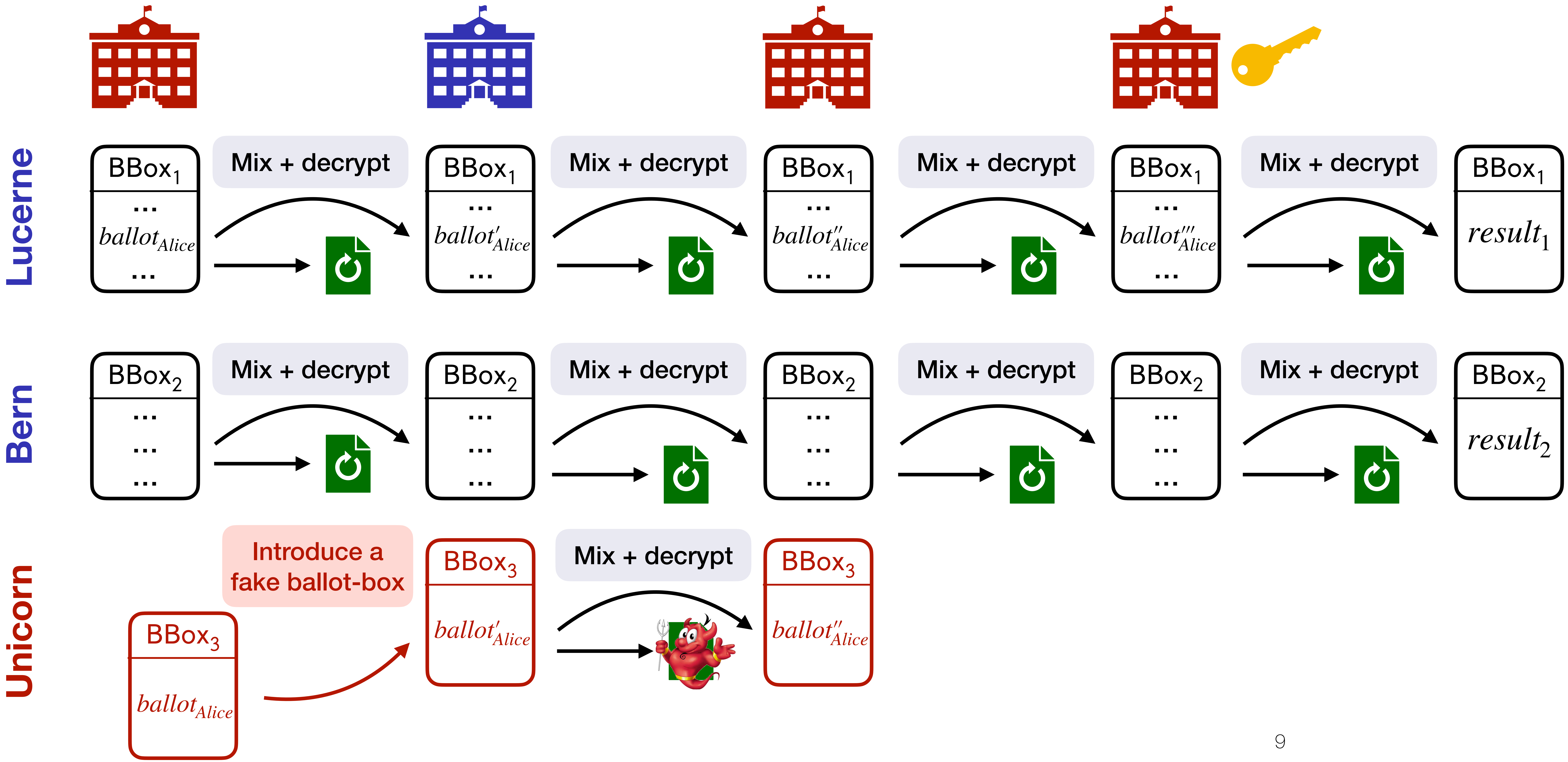
A vote secrecy attack



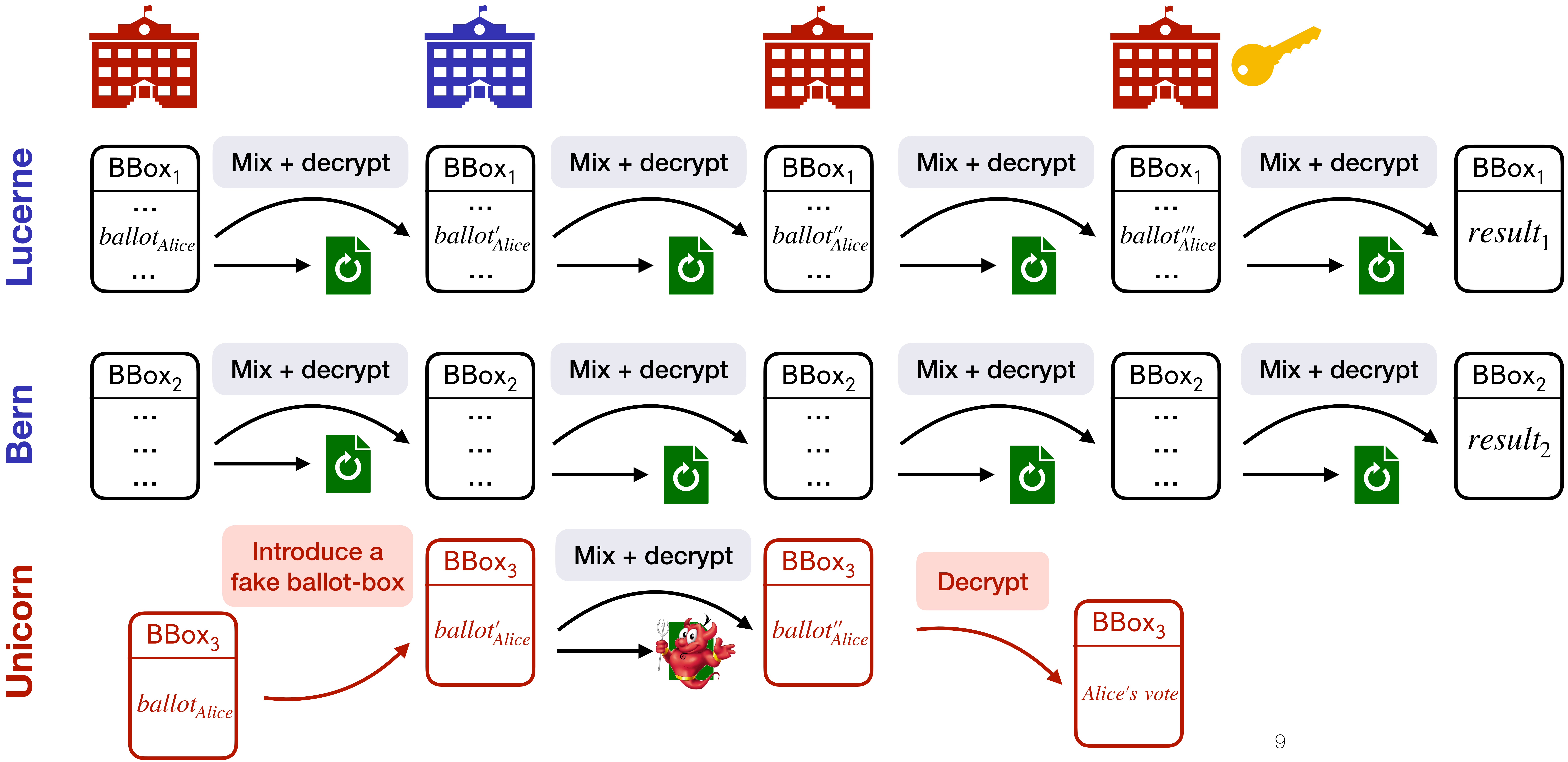
A vote secrecy attack



A vote secrecy attack



A vote secrecy attack



Impact of the attack

In theory: the attacker can learn the vote of all the voters

Impact of the attack

In theory: the attacker can learn the vote of all the voters

In practice:

- he cannot add too many fake ballot-boxes
- can learn the vote of at most k voters
  (k might be relatively large because fake ballot-boxes are very small, only one ballot)
- many variants of the attack exist

it would introduce a detectable overhead in the computation time

Impact of the attack

In theory: the attacker can learn the vote of all the voters

it would introduce a detectable overhead in the computation time

In practice:

- he cannot add too many fake ballot-boxes
- can learn the vote of at most k voters
  (k might be relatively large because fake ballot-boxes are very small, only one ballot)
- many variants of the attack exist

According to Swiss Post and the Chancellerie: it is a critical flaw that must be fixed!

Impact of the attack

In theory: the attacker can learn the vote of all the voters

it would introduce a detectable overhead in the computation time

In practice:

- he cannot add too many fake ballot-boxes
- can learn the vote of at most k voters
  (k might be relatively large because fake ballot-boxes are very small, only one ballot)
- many variants of the attack exist

We got a generous bounty

According to Swiss Post and the Chancellerie: it is a critical flaw that must be fixed!

How to fix the attack?

1. **A weak counter-measure to** detect attacks

- set the number n_B of ballot-boxes
- the CCMs decrypt exactly n_B ballot-boxes
- the auditor verifies exactly n_B proofs

How to fix the attack?

1. **A weak counter-measure to detect attacks**

- set the number n_B of ballot-boxes
- the CCMs decrypt exactly n_B ballot-boxes
- the auditor verifies exactly n_B proofs

2. **Better safe than sorry:**

- implement 1.
- require that each CCM recomputes the initial payloads (i.e. the content of the initial ballot-box)
- require that each CCM verifies all the previous proofs of correct mixing/decryption

How to fix the attack?

1. **A weak counter-measure to detect attacks**

- set the number n_B of ballot-boxes
- the CCMs decrypt exactly n_B ballot-boxes
- the auditor verifies exactly n_B proofs

2. **Better safe than sorry:**

- implement 1.
- require that each CCM recomputes the initial payloads (i.e. the content of the initial ballot-box)
- require that each CCM verifies all the previous proofs of correct mixing/decryption

➡ modify the infrastructure to let the CCMs compute the initial payloads

➡ these two requirements are quite expensive…

➡ add a delay before publishing the results

Conclusion

This attack will be fixed in a future release of the specification/implementation

Switzerland provides a solution with a high level of transparency and many audits by experts
(compared to other systems/countries)

Lesson learned

It is important to model all the specificities of the system when we do formal proofs (symbolic or computational ones)
e.g. multi ballot-boxes or elections scenarios

What about other e-voting protocols?

See you next year?

Since June 2021: a new requirement for vote secrecy!

> 2.9.3.3 If an entire group of control components is used by a private system operator, none of these control components is considered trustworthy.

In practice

Swiss Post operates the 4 Control Components, they mut be assumed untrustworthy

➡ it is difficult to externalize a component…

In theory

All the vote secrecy definitions (implicitly) assume verifiability

➡ the system is not verifiable with this requirement…

How can we make both meet? again…

a new definition, a (major) improvement of the system, a step in-between…?

https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsbedingungen.html