Coercion-resistance with cast-as-intended verification

Quentin Yang

May 2021

Introduction

Voting requires two major properties.

Privacy

No one should know how you voted.

Verifiability

The result is guaranteed to be correct.

Introduction

Voting requires two major properties.

Privacy

No one should know how you voted.

Verifiability

The result is guaranteed to be correct.

Those properties come with refinements.

Coercion-resistance:
You should not be able to prove that you voted in a certain way.

Cast-as-intended:
You should be convinced that your vote has been cast correctly.

Why coercion-resistance?

Le Monde | ACTUALITÉS | ÉCONOMIE | VIDÉOS | OPINIONS | CULTURE | M LE MAG | SERVICES

INTERNATIONAL • LETTRES DE

Favoris | Partage

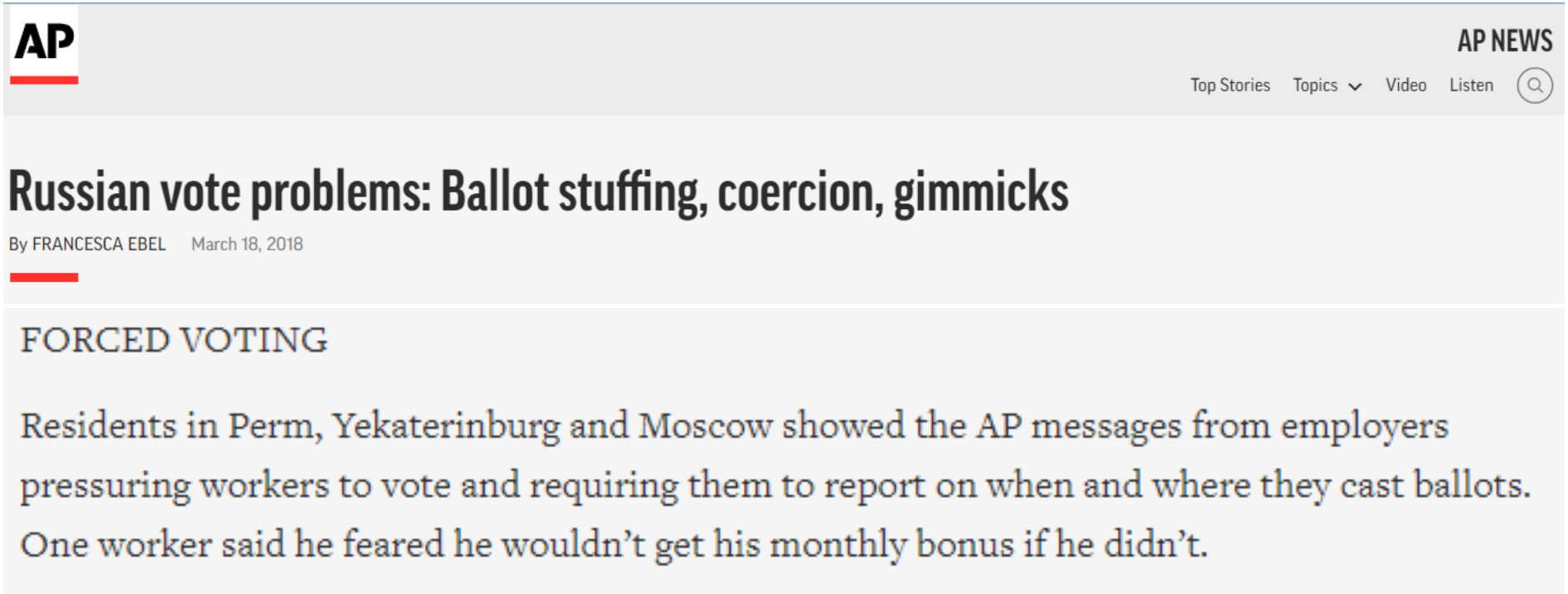
« Beaucoup d'électeurs sont prêts à vendre leur voix » : l'achat de votes, un fléau bulgare

A la veille des élections législatives en Bulgarie du 4 avril, une étude confirme une pratique endémique et partagée par tous les partis du pays : payer les électeurs pour s'assurer leur voix.

Par Jean-Baptiste Chastand (Vienne, correspondant régional)

Publié le 02 avril 2021 à 00h14 - Mis à jour le 02 avril 2021 à 12h18 • Lecture 4 min.

Why coercion-resistance?



AP

AP NEWS

Top Stories Topics Video Listen

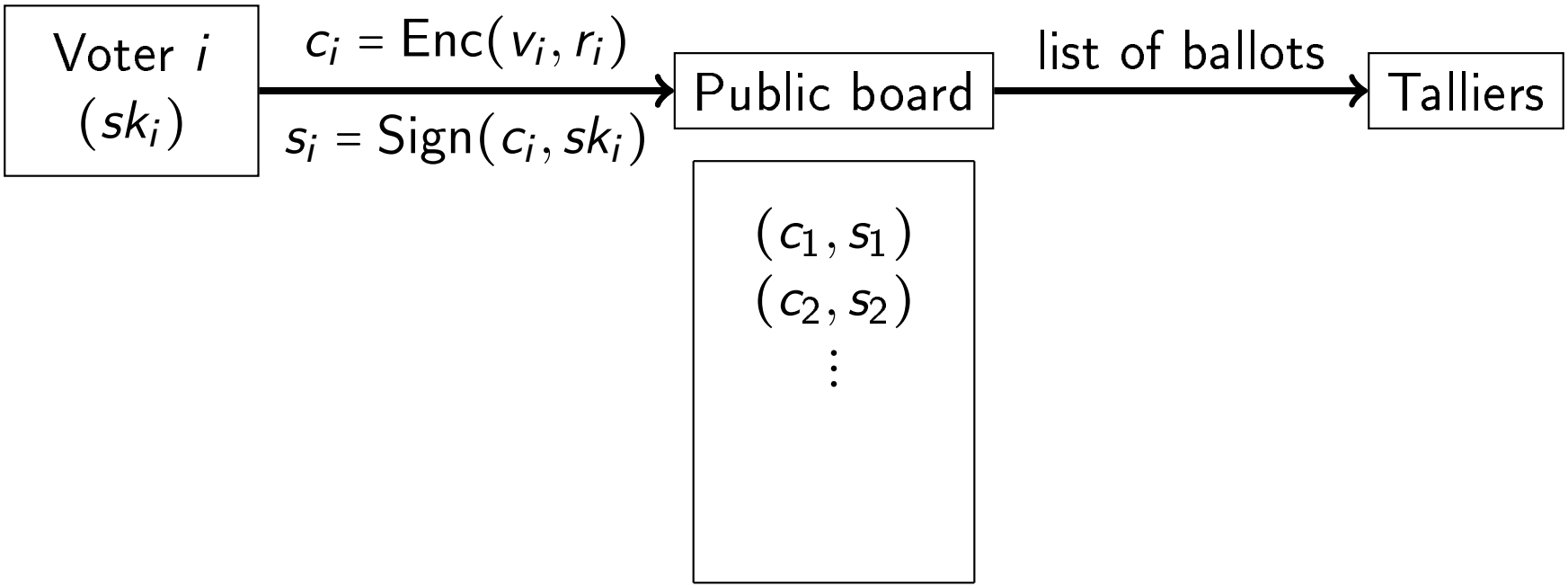
Russian vote problems: Ballot stuffing, coercion, gimmicks

By FRANCESCA EBEL March 18, 2018

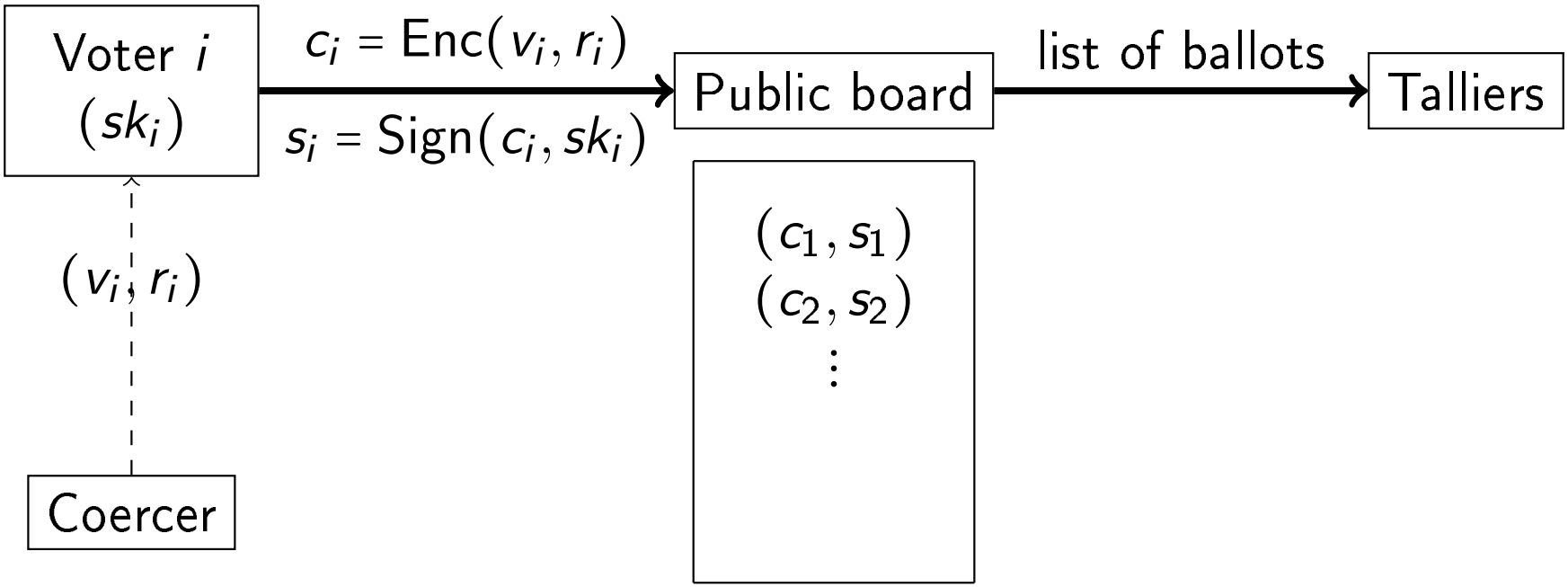
FORCED VOTING

Residents in Perm, Yekaterinburg and Moscow showed the AP messages from employers pressuring workers to vote and requiring them to report on when and where they cast ballots. One worker said he feared he wouldn't get his monthly bonus if he didn't.

Why is electronic voting not coercion-resistant?

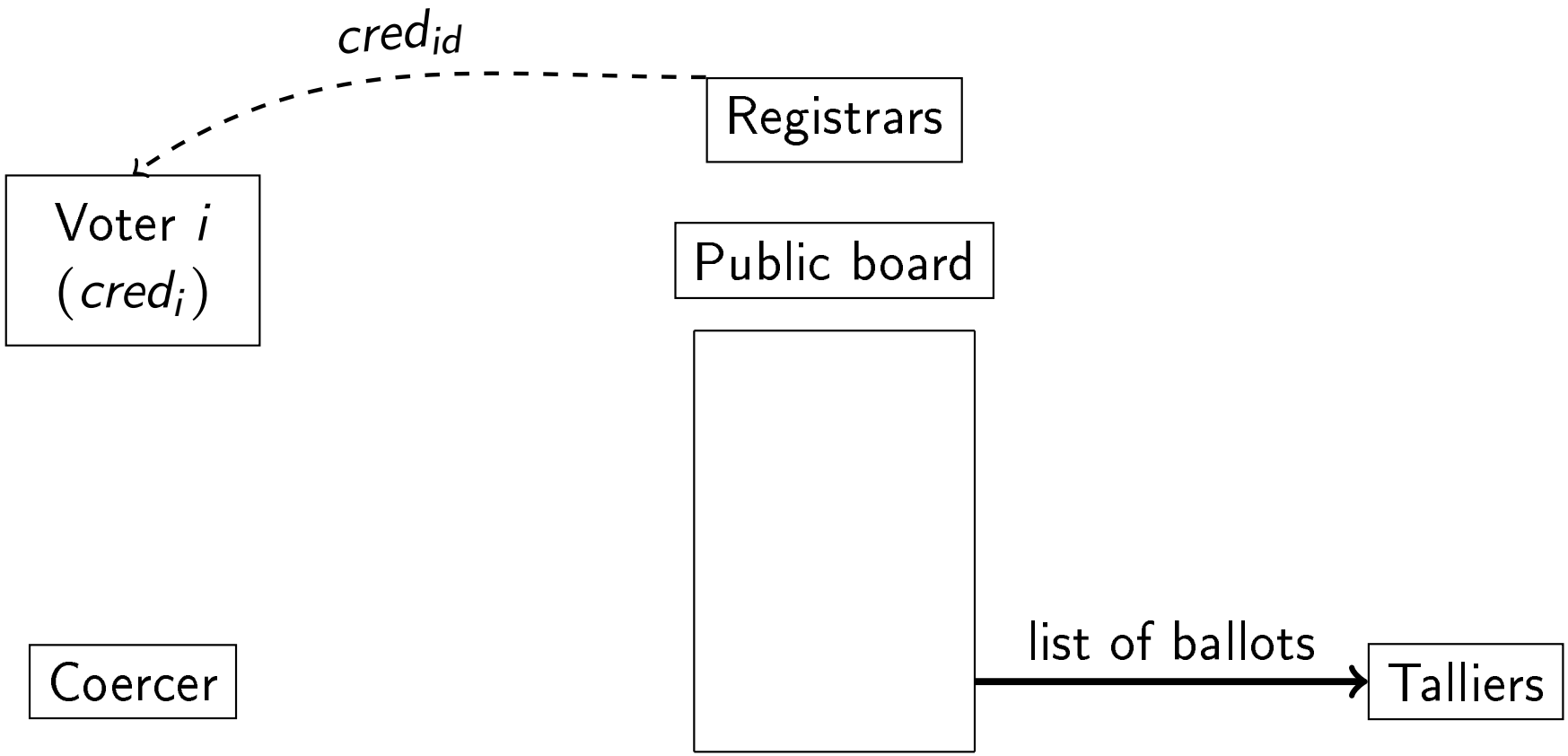


Why is electronic voting not coercion-resistant?



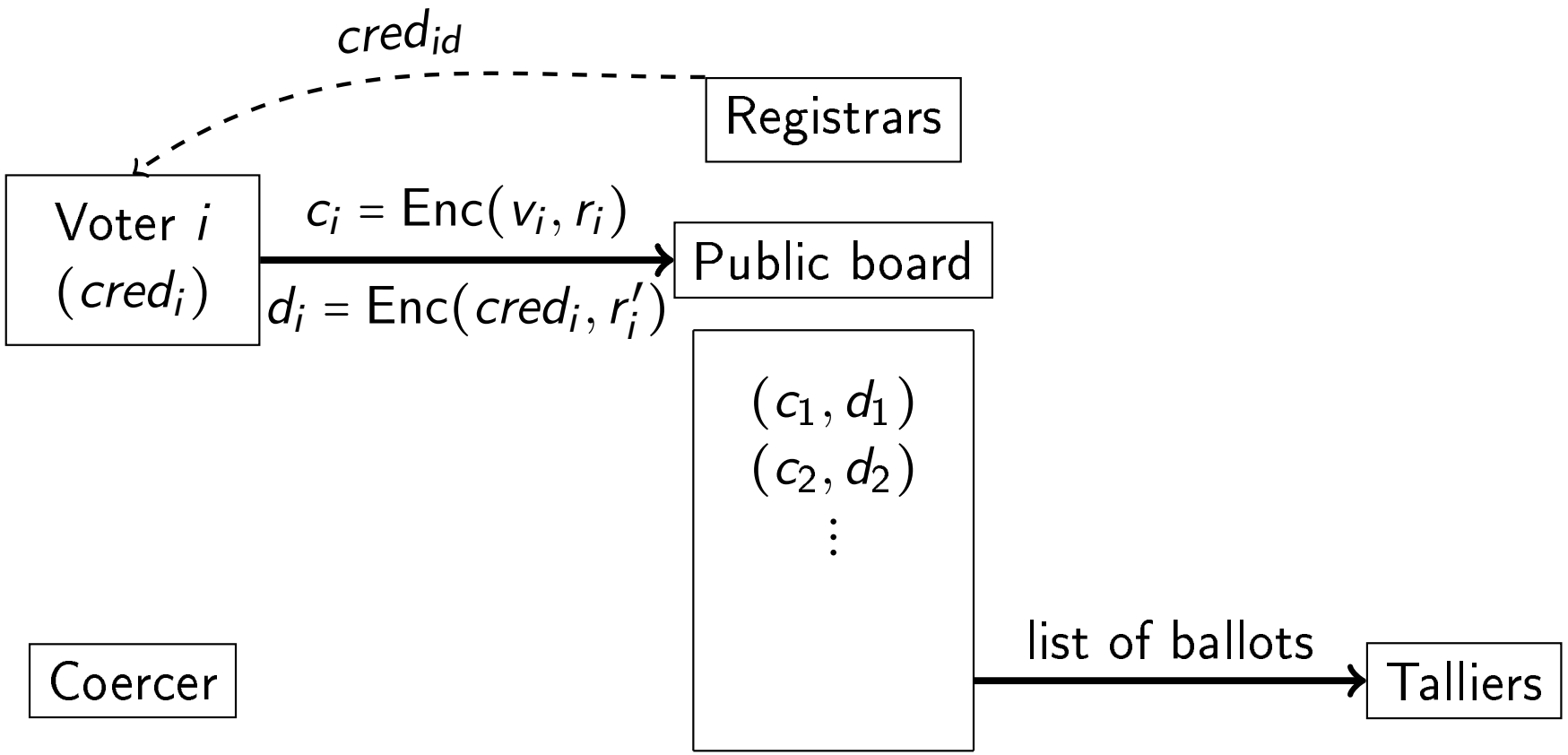
How to achieve coercion-resistance?

The example of the JCJ / Civitas protocol.



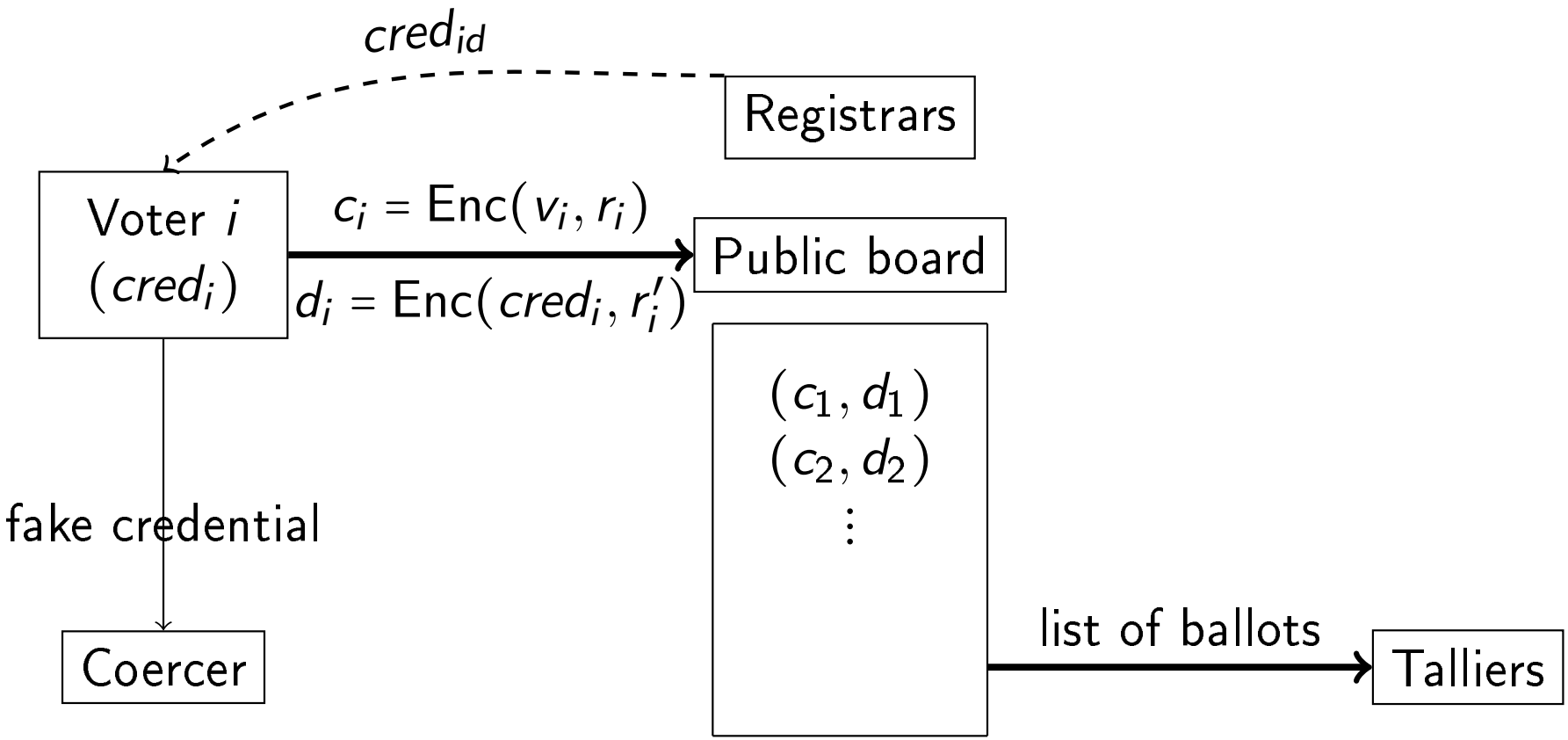
How to achieve coercion-resistance?

The example of the JCJ / Civitas protocol.



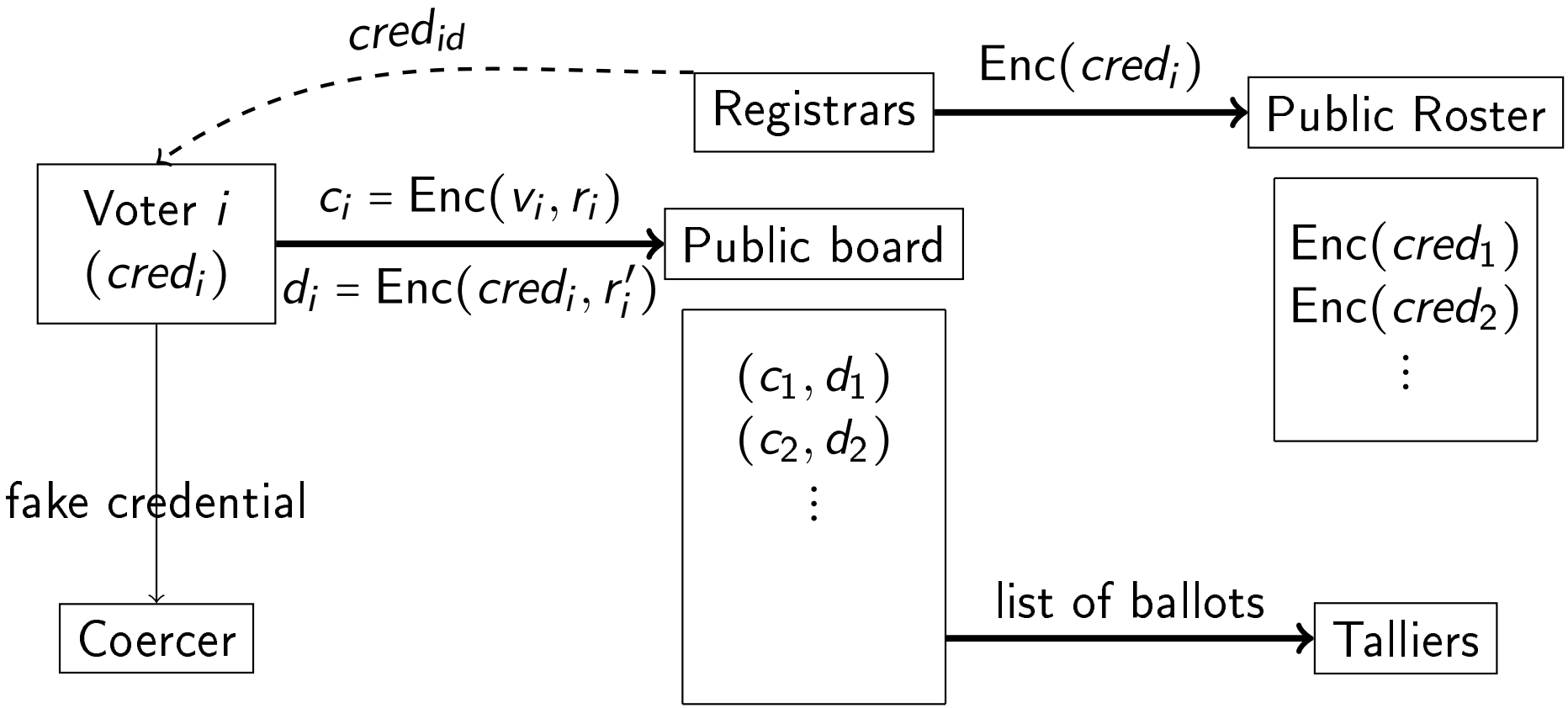
How to achieve coercion-resistance?

The example of the JCJ / Civitas protocol.



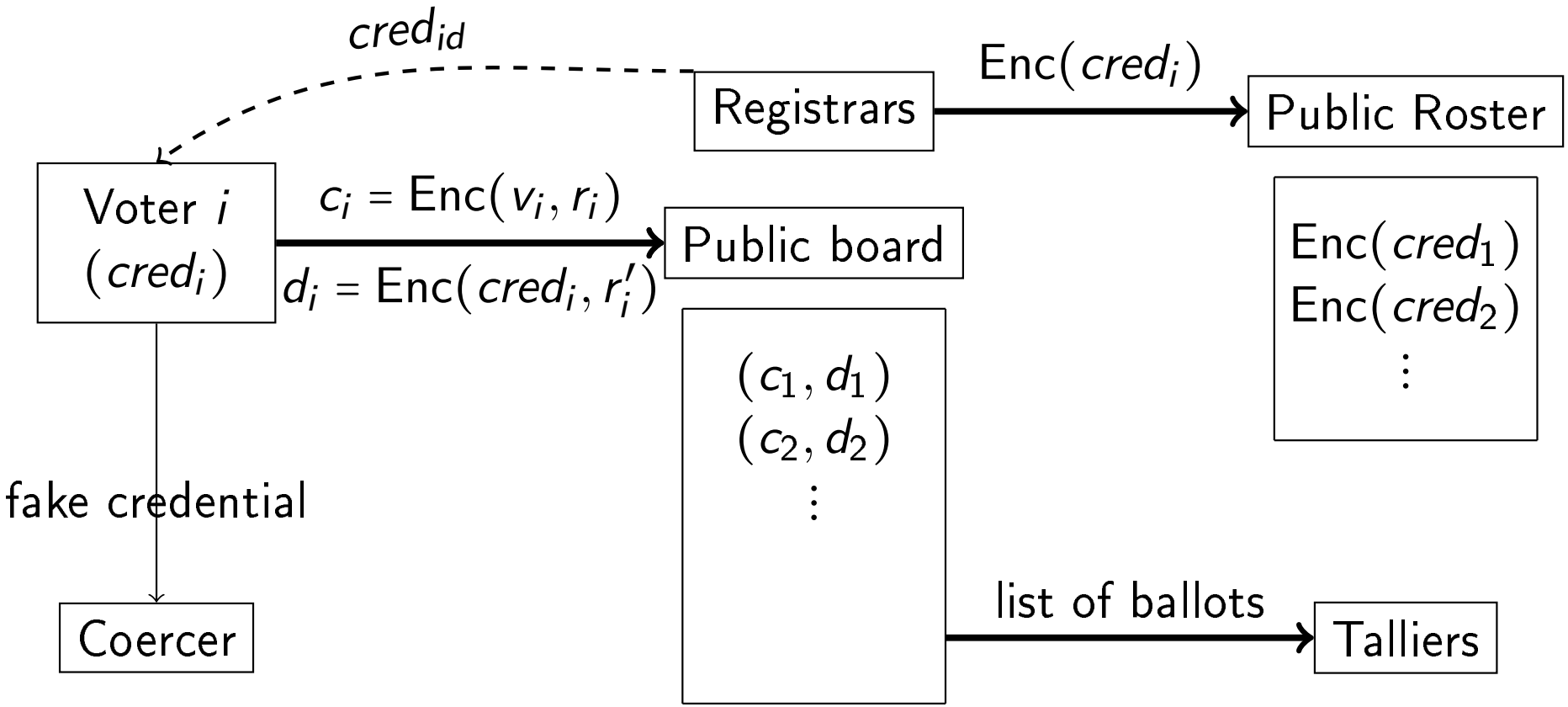
How to achieve coercion-resistance?

The example of the JCJ / Civitas protocol.



How to achieve coercion-resistance?

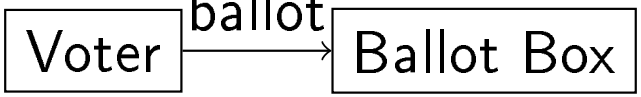
The example of the JCJ / Civitas protocol.



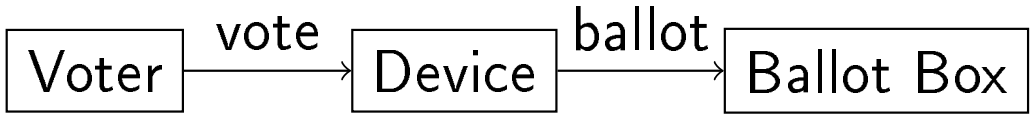
A classical way to obtain coercion-resistance uses two tools: **Plaintexts Equivalence Tests** and **Mixnets**.

Why cast-as-intended verification?

Real World Election

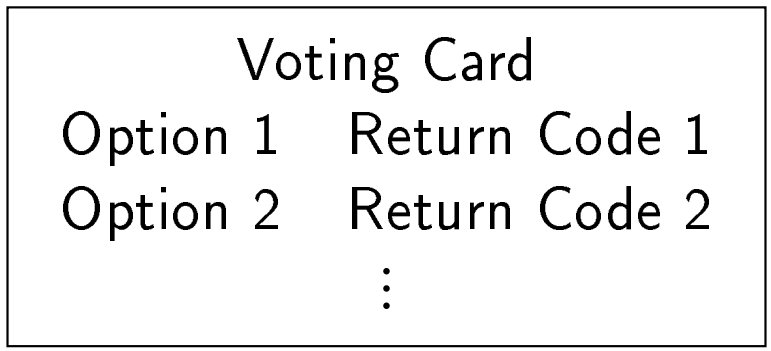


Electronic Election

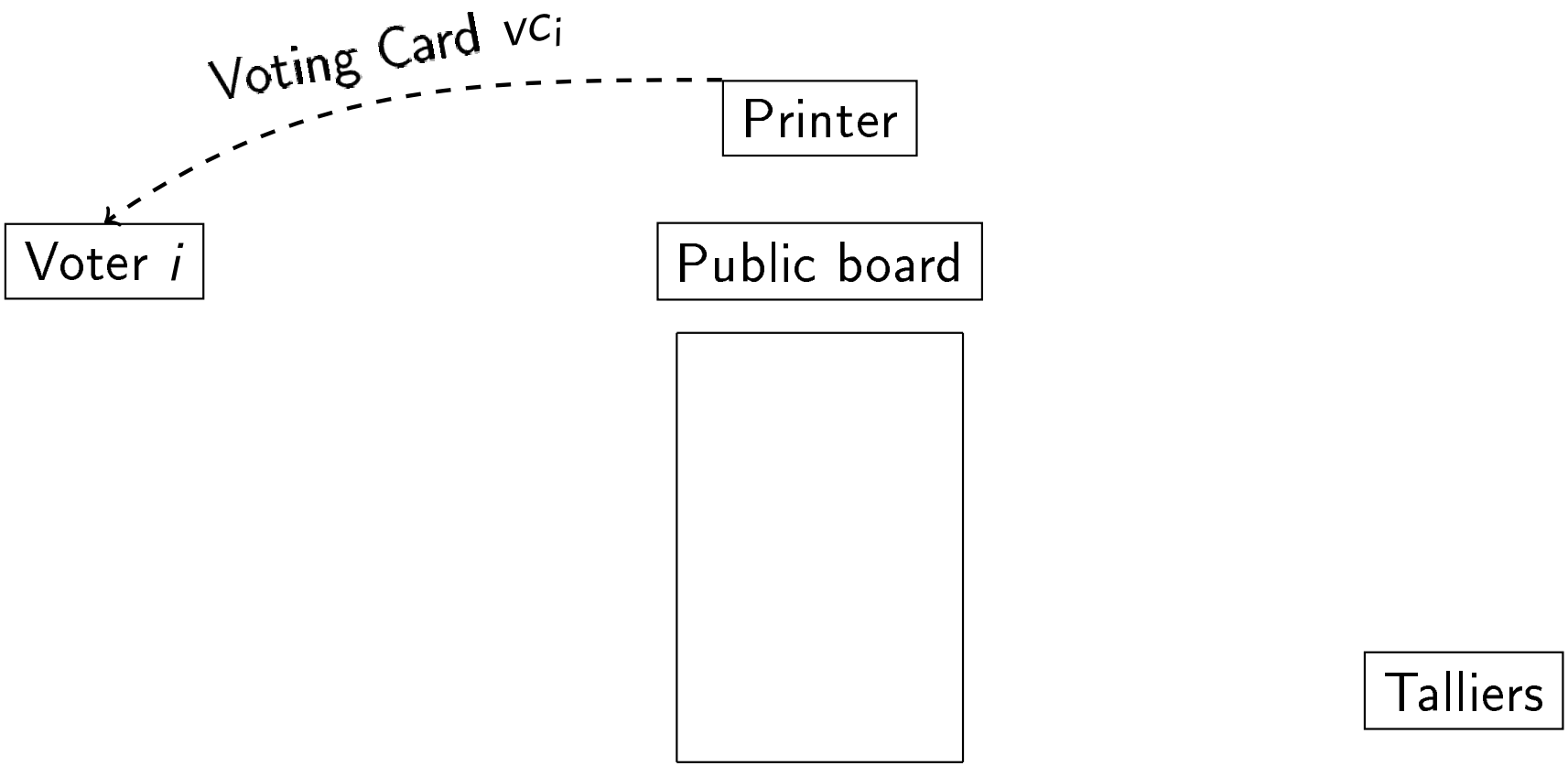


How to achieve cast-as-intended verification?

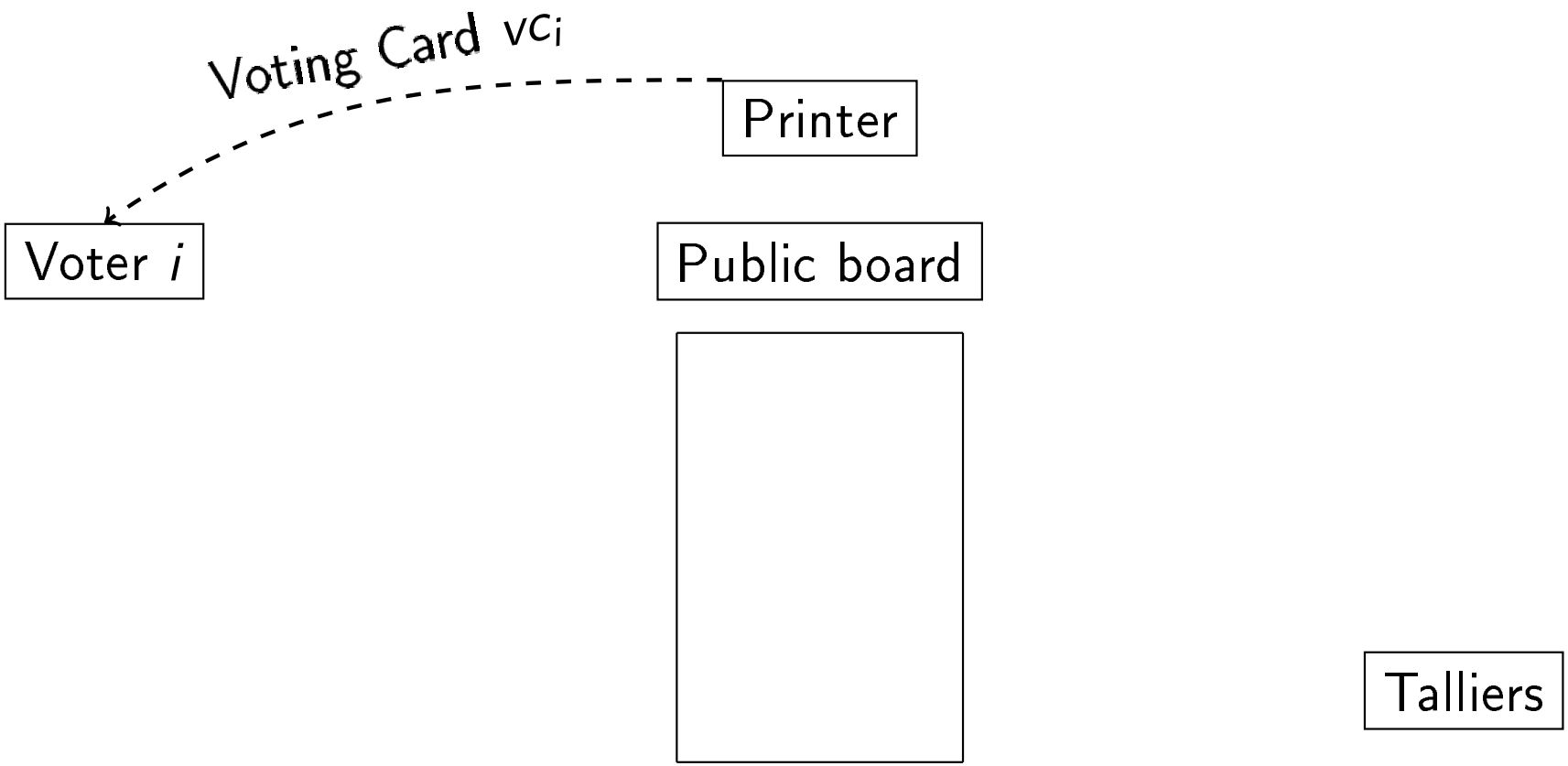
Example of the Swiss voting system: cast-as-intended verification achieved with **return codes**.



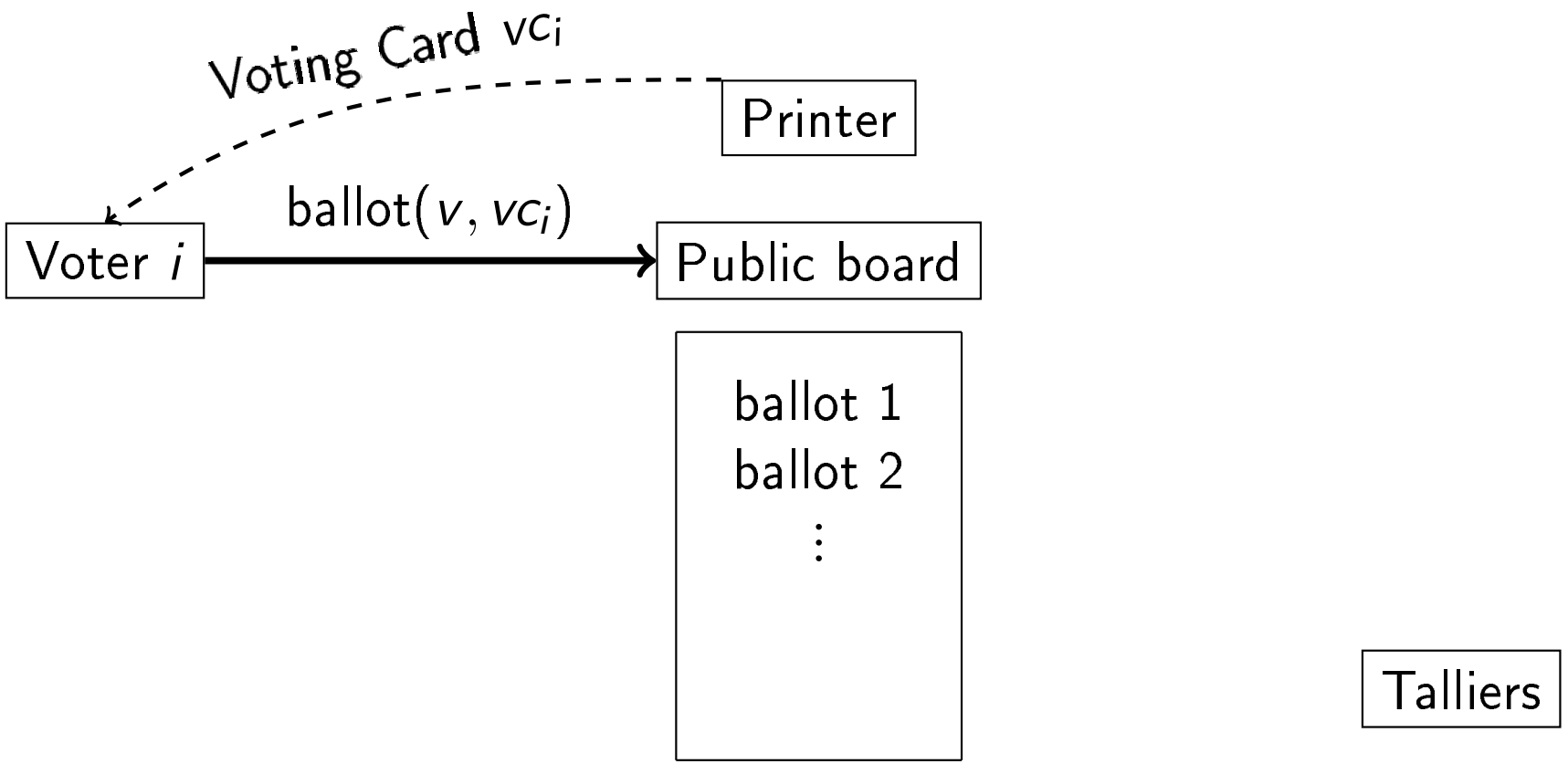
How to achieve cast-as-intended verification?



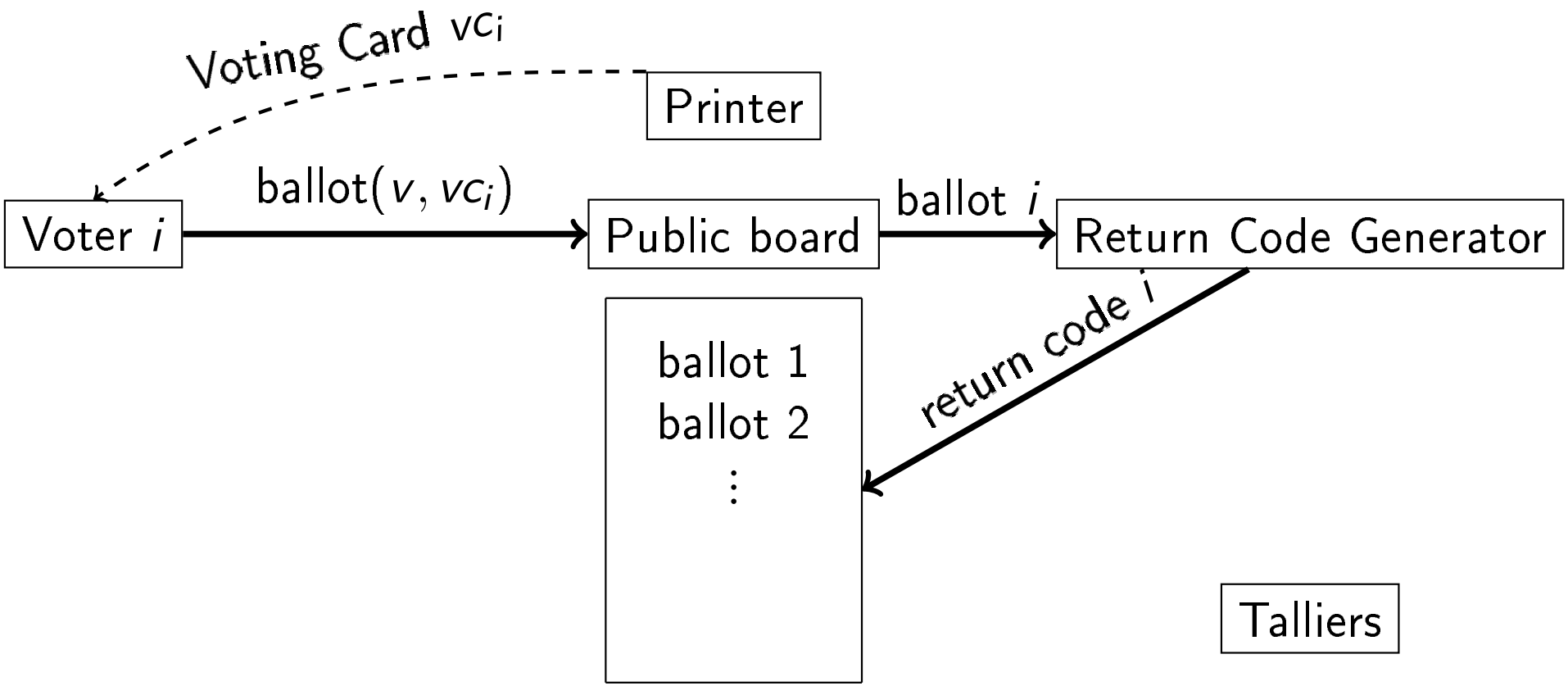
How to achieve cast-as-intended verification?



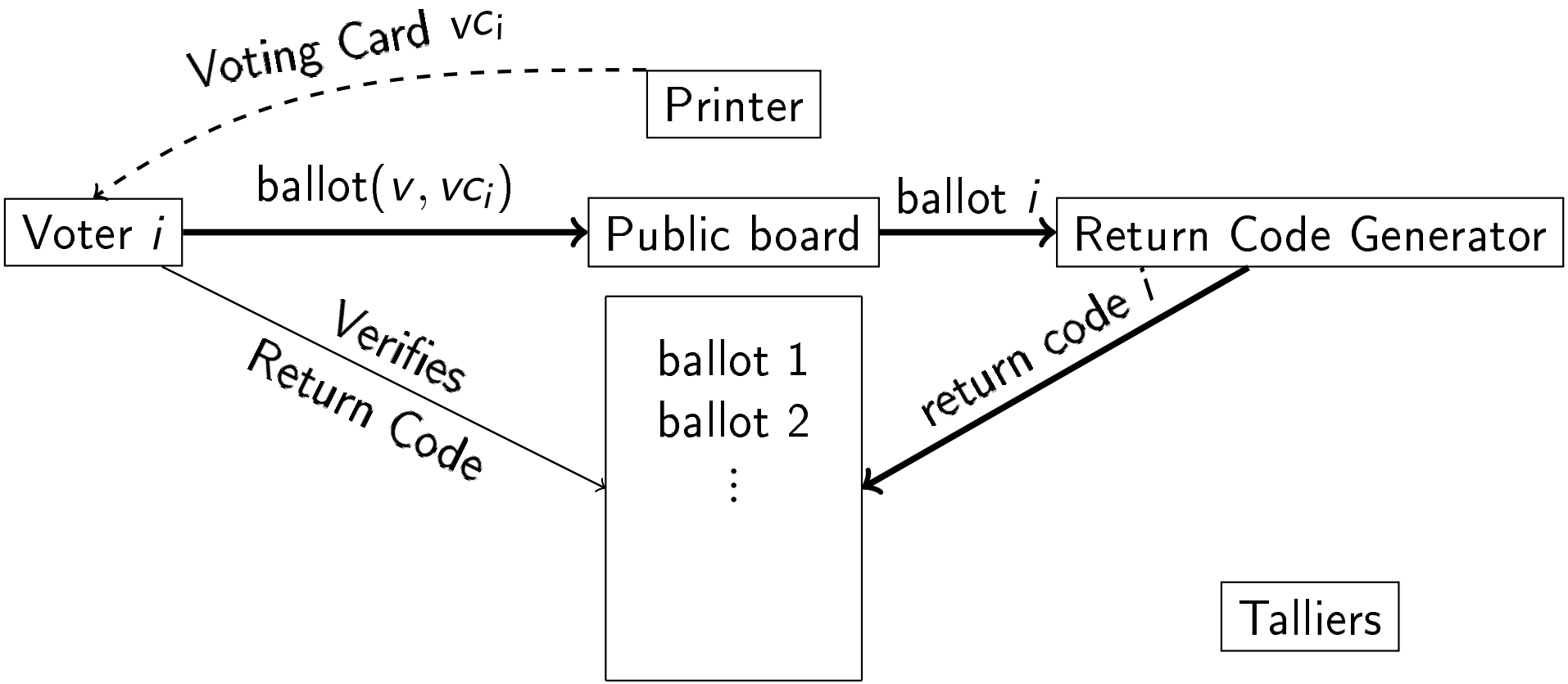
How to achieve cast-as-intended verification?



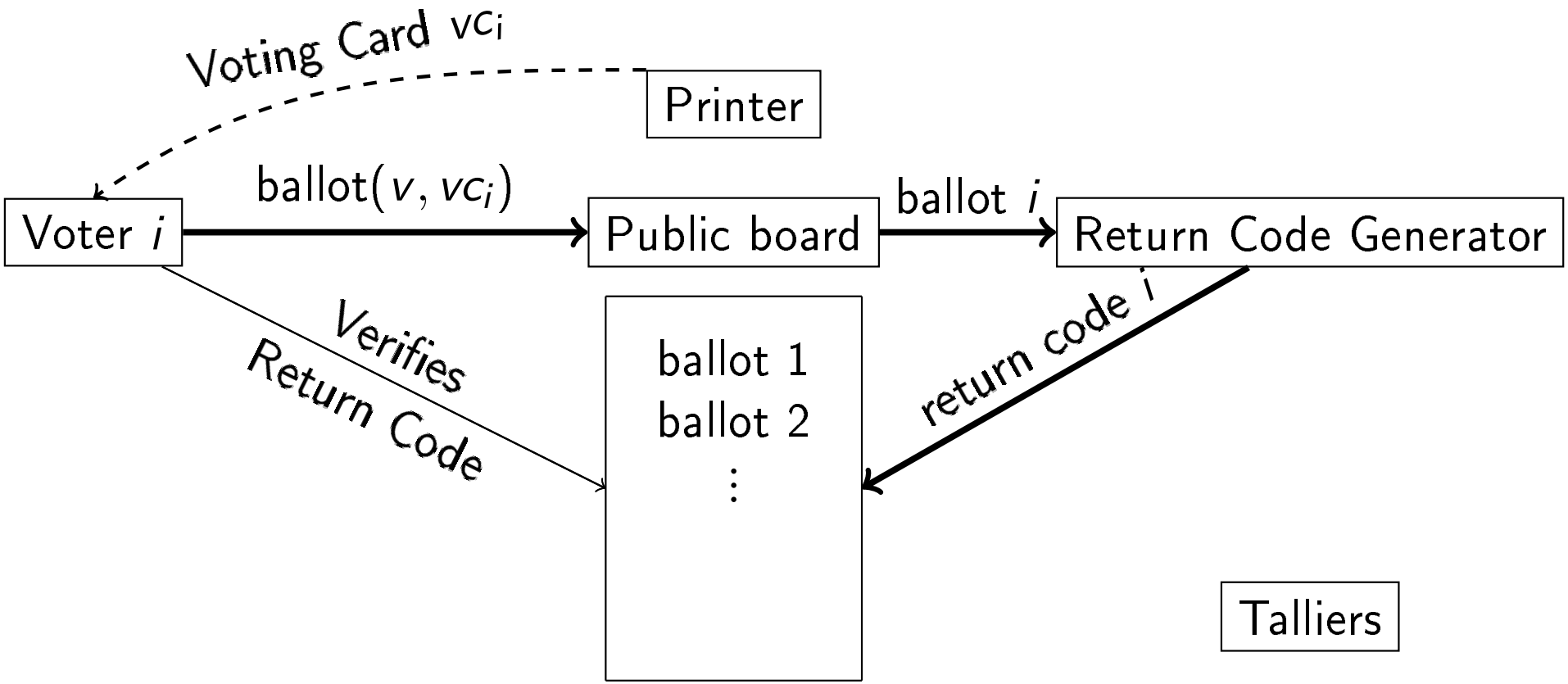
How to achieve cast-as-intended verification?



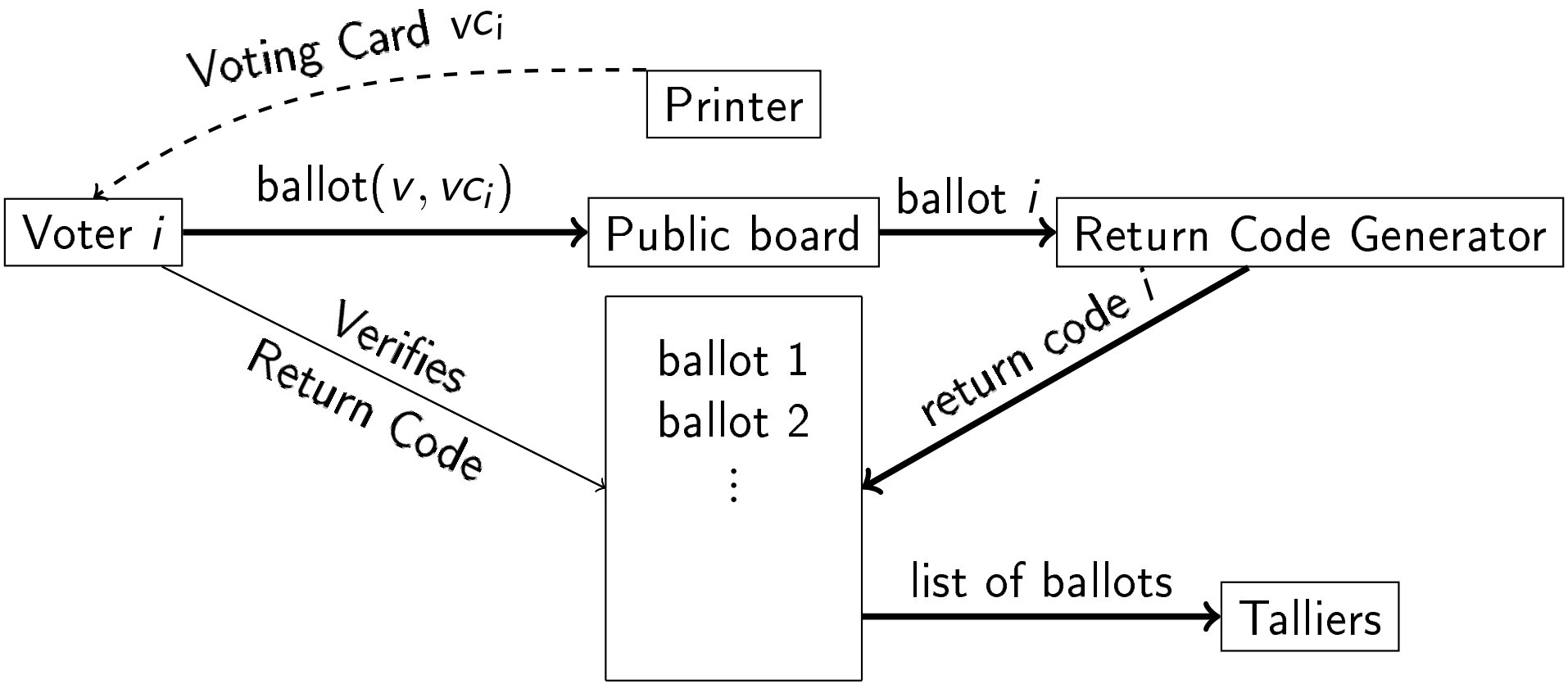
How to achieve cast-as-intended verification?



How to achieve cast-as-intended verification?



How to achieve cast-as-intended verification?



What are we working on?

Design a voting protocol that has both properties.

- Coercion resistance.
- Cast-as-intended verification.

What are we working on?

Design a voting protocol that has both properties.

- Coercion resistance.
- Cast-as-intended verification.

PROVE that it does have both properties.

Provide the relevant definitions.

What are we working on?

Design a voting protocol that has both properties.

- Coercion resistance.
- Cast-as-intended verification.

PROVE that it does have both properties.

Provide the relevant definitions.

By the way, address some annoying issues...

- The complexity of the cast-as-intended verification (number of actors, communications...).
- The registration process and the quadratic tally in coercion-resistant protocols.

Thank you !