Pushing JCJ Towards Reality

Reto E. Koenig, Rolf Haenni

Univeristy of Fribourg
&
University of Applied Science Berne

03.09.2010

Outline

1. Introduction
2. Restricting JCJ to a fixed amount of acceptable votes
3. Dummy credentials τ
4. Issues On τ
5. Features of τ

Field of Research

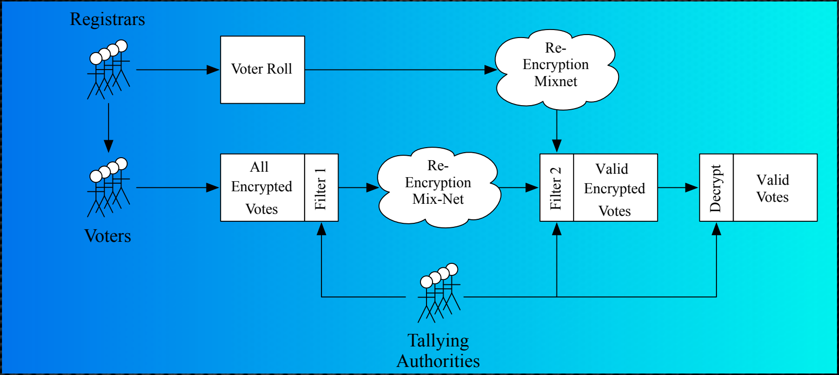
Improving the practicability of JCJ-05

- Restricting JCJ-05 to a fixed amount of acceptable votes

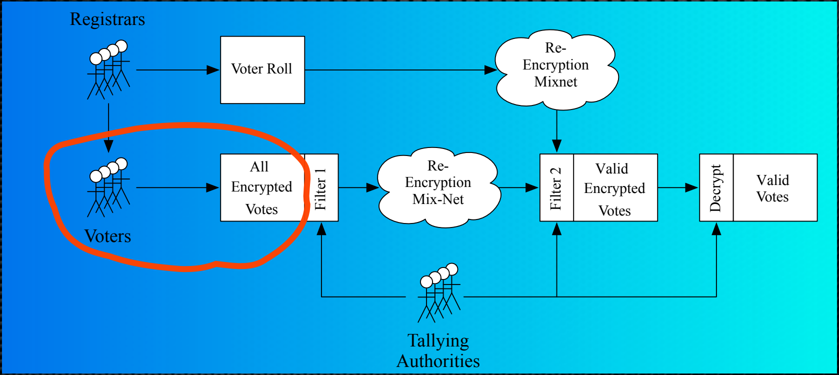
Outline

1. Introduction
2. Restricting JCJ to a fixed amount of acceptable votes
3. Dummy credentials τ
4. Issues On τ
5. Features of τ

Original JCJ Protocol

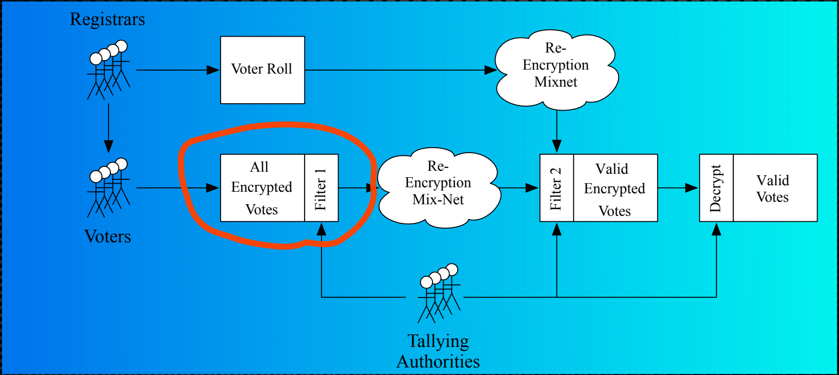


Original JCJ Protocol



Any Internet-User can send data to the public board.

Original JCJ Protocol



After vote cast period: The first filter eliminates votes with invalid proofs and duplicate votes from the public board

Original JCJ Protocol

Duplicate elimination Complexity of JCJ

Time $O(n^2 + s^2)$

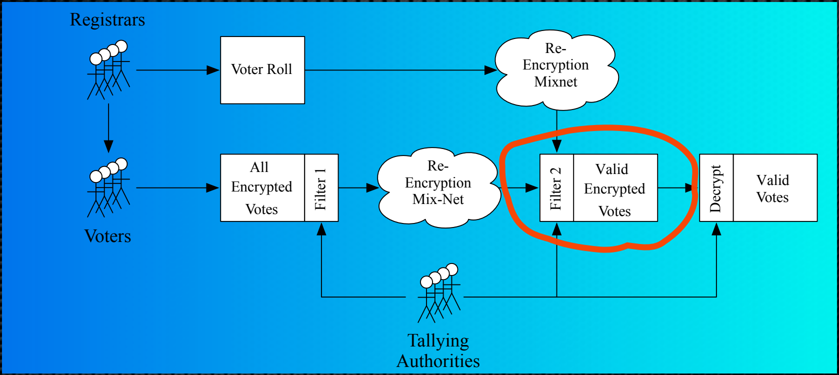
Space $O(n + s)$

Where...

$n =$ amount of eligible voters

$s =$ amount of double or fake votes... An unpredictable high value

Original JCJ Protocol



The second filter checks the votes cast against the voter roll (and thus eliminates votes created from fake credentials)

Original JCJ Protocol

Fake vote elimination Complexity of JCJ

Time $O(n^2 + s^2)$

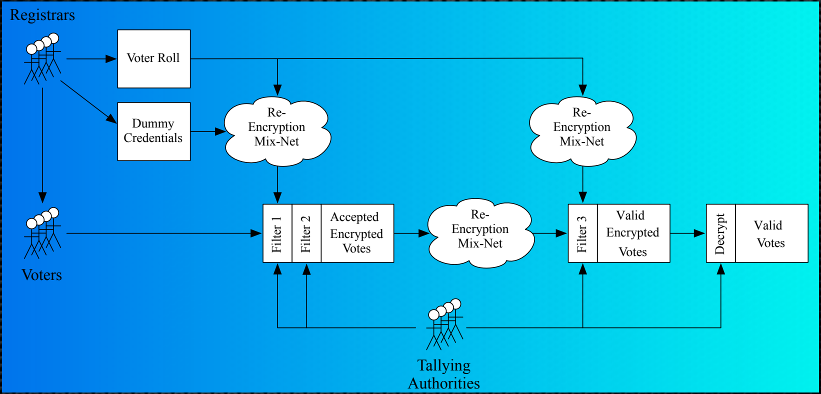
Space $O(n + s)$

Where...

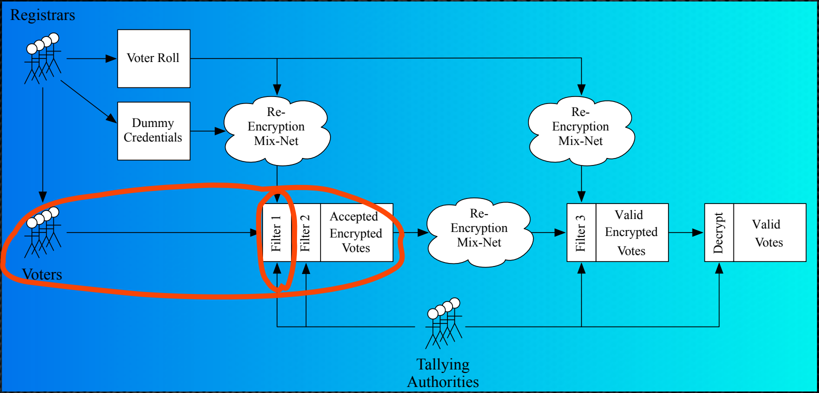
n = amount of eligible voters

s = amount of fake votes... An unpredictable high value

Modified JCJ Protocol

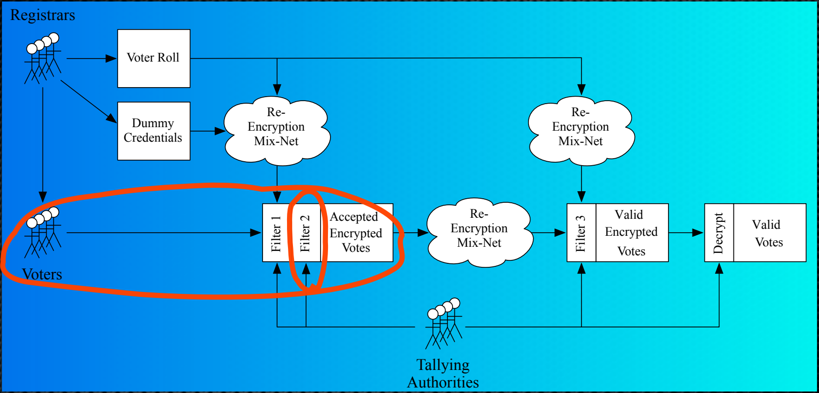


Modified JCJ Protocol



During vote cast period: The first filter discards votes created from unauthorized credentials ⇒ Accepts only eligible voters votes

Modified JCJ Protocol



During vote cast period: The second filter rejects duplicate votes

Modified JCJ Protocol

Duplicate / unauthorized vote elimination Complexity of mod.JCJ

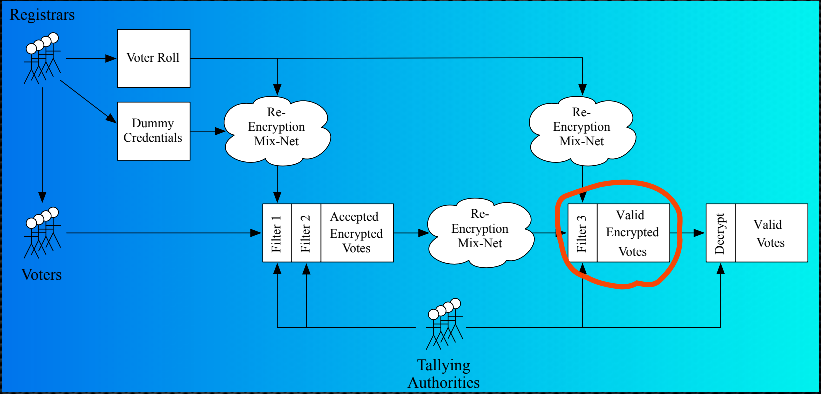
Time $O(m)$

Space $O(m)$

Where...

$m =$ amount of issued credentials... A fix number

Modified JCJ Protocol



The third filter checks the votes against the credentials stored on the voter roll. ⇒ Only accepts 'real'-votes

Modified JCJ Protocol

Dummy vote elimination Complexity of mod.JCJ

Time $O(m)$

Space $O(m)$

Where...
$m =$ amount of issued credentials

Direct Comparison

Complexity analysis

JCJ $O(n^2 + s^2)$ (where s can grow uncontrollably)

Mod. JCJ $O(m)$ (where m is a fixed known number)

Outline

1. Introduction
2. Restricting JCJ to a fixed amount of acceptable votes
3. Dummy credentials τ
4. Issues On τ
5. Features of τ

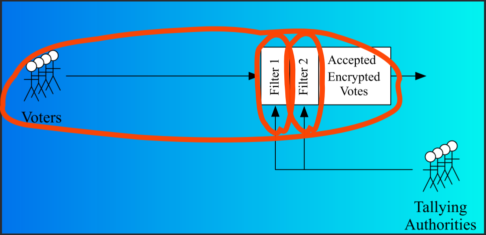
Change to JCJ

Introduction of Dummy credentials τ

- In addition to the credential σ each voter gets some τ-s
- The voter can either:
  - declare a dummy-vote by applying a τ to the ballot.
  - declare the real vote by applying the σ to the ballot.

Change to JCJ

Filtering during vote cast period...



The system

... accepts only

- valid σ
- valid τ

... rejects any

- duplicate σ
- duplicate τ

Outline

1. Introduction
2. Restricting JCJ to a fixed amount of acceptable votes
3. Dummy credentials τ
4. Issues On τ
5. Features of τ

How many τ-s per voter?

A constant amount for every voter

- The voter gets coercible
- The voter can sell the right to vote

A random amount per voter with upper limit

- The voter is not coercible
- The voter can sell the the right to vote

A random amount per voter without upper limit

- The voter is not coercible
- The voter can not sell the the right to vote
- The system can be 'flooded' by τ-s

How many τ-s per voter?

A constant amount for every voter

- The voter gets coercible
- The voter can sell the right to vote

A random amount per voter with upper limit

- The voter is not coercible
- The voter can sell the the right to vote

A random amount per voter without upper limit

- The voter is not coercible
- The voter can not sell the the right to vote
- The system can be 'flooded' by τ-s

How many τ-s per voter?

A constant amount for every voter

- The voter gets coercible
- The voter can sell the right to vote

A random amount per voter with upper limit

- The voter is not coercible
- The voter can sell the the right to vote

A random amount per voter without upper limit

- The voter is not coercible
- The voter can not sell the the right to vote
- The system can be 'flooded' by τ-s

How to store the set of τ of a voter

The amount of τ per voter has to stay 'secret'

In contrast to σ every τ has to be stored anonymously.

List carrying all τ-s of all voters

The system has to provide an anonymized list (in contrast to the electoral-roll carrying the σ-credentials) where all τ-s are listed publicly.

How to store the set of τ of a voter

The amount of τ per voter has to stay 'secret'

In contrast to σ every τ has to be stored anonymously.

List carrying all τ-s of all voters

The system has to provide an anonymized list (in contrast to the electoral-roll carrying the σ-credentials) where all τ-s are listed publicly.

How to generate a random set of τ per voter

Blinding the system about the amount of τ-s in voters possession

It is absolutely crucial that no one (except the voter) knows the amount of τ-s a single voter can operate on.

Paper in progress...

Donation of τ-s amongst voters

Voters can donate (trade) τ-s

How to generate a random set of τ per voter

Blinding the system about the amount of τ-s in voters possession

It is absolutely crucial that no one (except the voter) knows the amount of τ-s a single voter can operate on.

Paper in progress...

Donation of τ-s amongst voters

Voters can donate (trade) τ-s

Outline

1. Introduction
2. Restricting JCJ to a fixed amount of acceptable votes
3. Dummy credentials τ
4. Issues On τ
5. Features of τ

Delegate Online PETs to the Voter-Side

Could the voter prove the 'equivalence' of two credentials

Distribute the work of filter 1 to the voter (Getting rid of the online PET)

Work in progress...

The voter proves the usage of a certain credential

If the voter knows the randomness of the anonymized-mixed list $(\sigma + \tau)$, the voter can send a *zkp* of the chosen credential.

Time complexity during voting process $O(1)$

Workload can be distributed

Delegate Online PETs to the Voter-Side

Could the voter prove the 'equivalence' of two credentials

Distribute the work of filter 1 to the voter (Getting rid of the online PET)

Work in progress...

The voter proves the usage of a certain credential

If the voter knows the randomness of the anonymized-mixed list $(\sigma + \tau)$, the voter can send a *zkp* of the chosen credential.

Time complexity during voting process $O(1)$

Workload can be distributed

Summary

Benefit of τ introduction to JCJ...

Application-Level Flooding resistance

Time complexity $O(1)$ during voting-process

Summary

Benefit of τ introduction to JCJ...

Application-Level Flooding resistance

Time complexity $O(1)$ during voting-process