

When Cryptography Meets Reality: Insights from the Swiss Post E-Voting Protocol

Audhild Høgåsen, Chiara Spadafora



Swiss E-Voting Timeline: Past and Present

Informations générales

Ce texte est en vigueur

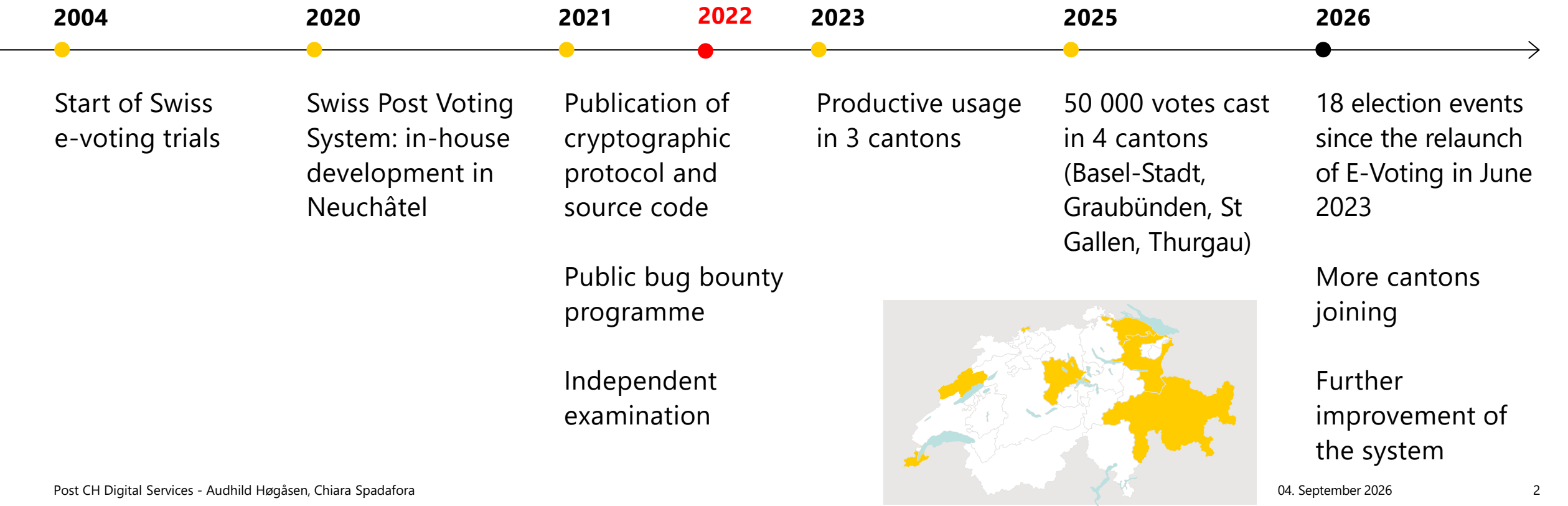
Abréviation	OVotE
Décision	25 mai 2022
Entrée en vigueur	1 juillet 2022
Source	RO 2022 336
Langue(s) de la publication	DE FR IT EN
Chronologie	Chronologie
Citations	Citations

161.116

Ordonnance de la ChF sur le vote électronique (OVotE)

du 25 mai 2022 (État le 1^{er} juillet 2022)

La Chancellerie fédérale suisse (ChF),
vu les art. 27e, al. 1^{bis}, 27g, al. 2, 27i, al. 3, et 27l, al. 3 et 4,
de l'ordonnance du 24 mai 1978 sur les droits politiques (ODP)¹,
arrête:



Ordinance on Electronic Voting – Security Requirements

Verifiability

Individual Verifiability:

- Cast-as-intended: voters can check that the ballot sent by their voting device contains their intended vote.
- Recorded-as-cast: voters can check that the system has registered the ballot they have cast.

Universal Verifiability (or tallied-as-recorded): the result corresponds to the registered ballots.

Eligibility Verifiability: registered ballots have been cast by eligible voters.

Privacy

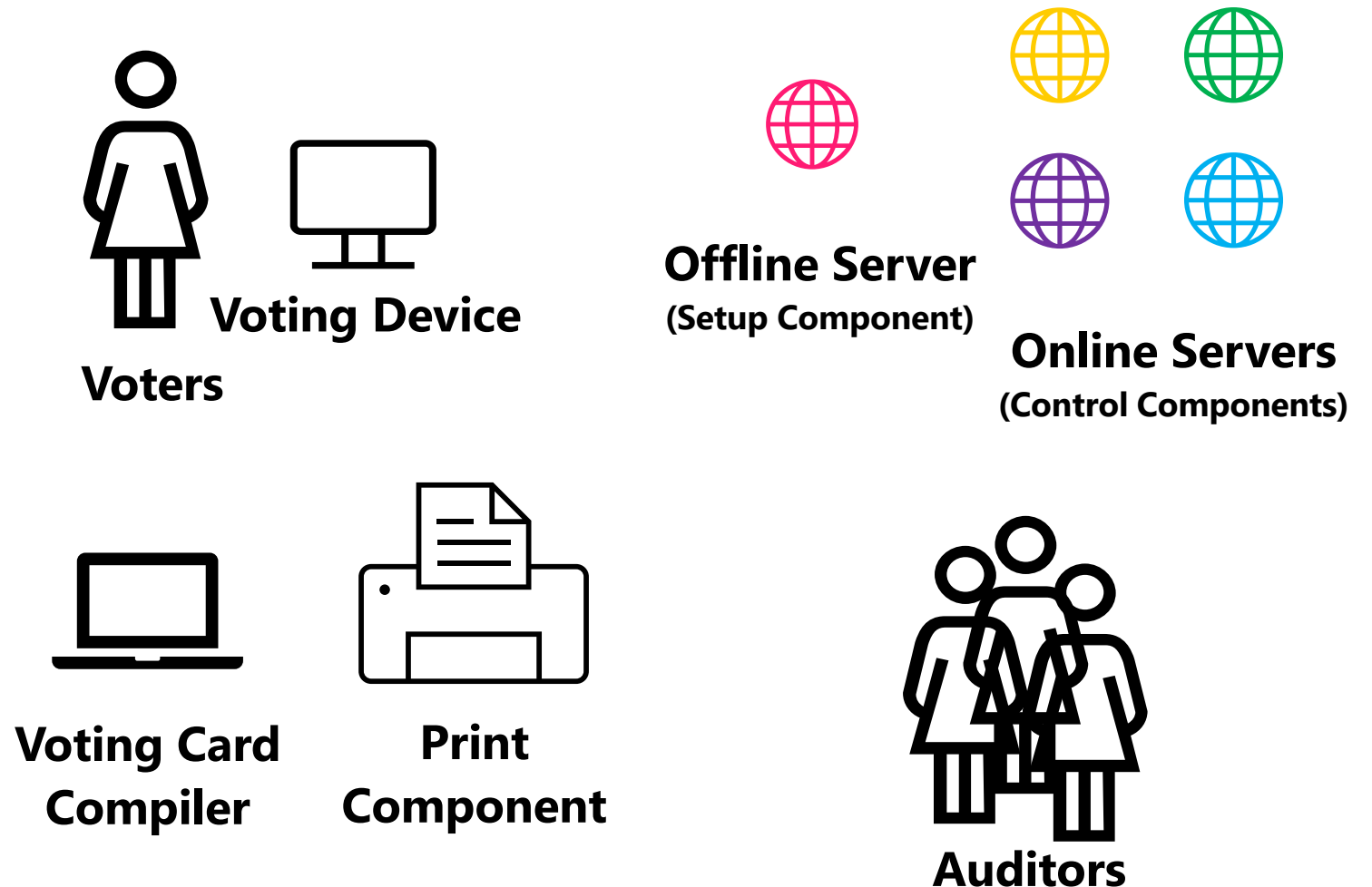
Vote secrecy: No one else should learn how a voter voted.

The Swiss Post Voting System

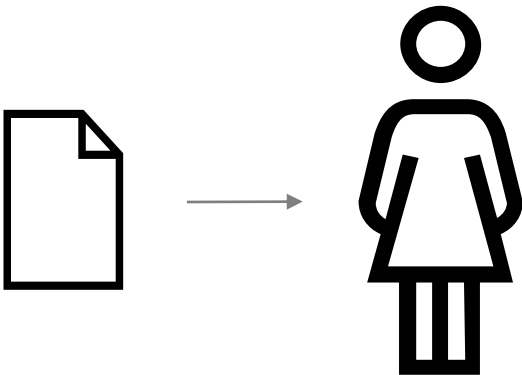
Swiss Post Voting System: Phases and Components

Election phases

- 1) Setup Phase
- 2) Voting Phase
- 3) Tally Phase



Swiss Post Voting System: The Voting Card





Code d'initialisation
5rqs tt2e r26a xp24 b266 vh7p



Codes de vérification

Démo Votation

1. Temps ensoleillé

Oui 6715 Non 7336 Blanc 9080

2. Temps pluvieux

Oui 7618 Non 1018 Blanc 7298

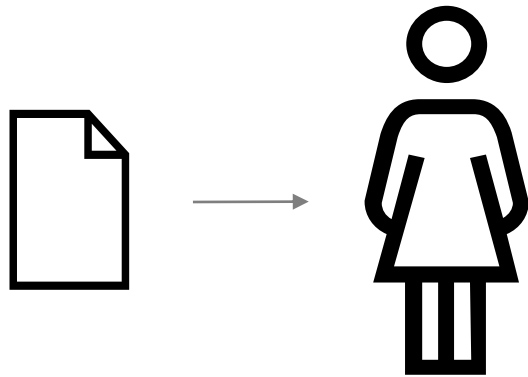


Code de confirmation
5043 8364 4



Code de finalisation
6403 0313

Swiss Post Voting System: Voting Phase



✓ Dispositions pénales

2 ▲ Démarrer le vote

3 Saisir votre vote

4 Contrôler votre vote

5 ♦ Vérifier les codes

6 ♣ Saisir votre code de confirmation

7 ★ Vérifier le code de finalisation

2 Démarrer le vote

Saisissez votre code d'initialisation

Le code figure sur votre carte de vote.

▲ Code d'initialisation

[? Qu'est-ce que le code d'initialisation?](#)

5 r q s t t 2 e r 2 6 a x p 2 4 b 2 6 6 v h 7 p

Vous pouvez écrire indifféremment en minuscules ou en majuscules.

Saisissez votre année de naissance

Cliquez ensuite sur Démarrer.

Année de naissance

1 9 7 1 |

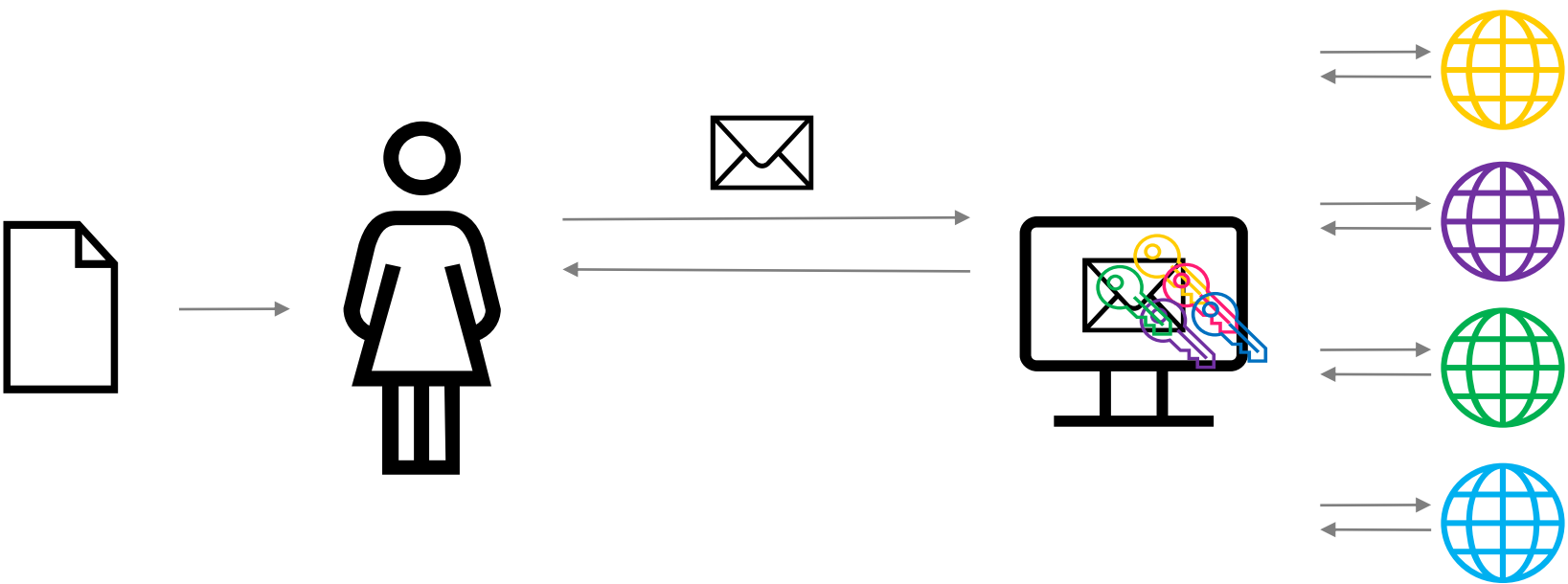
Démarrer →

Post CH Digital Services - Audhild Høgåsen, Chiara Spadafora

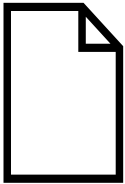
04. September 2026

7

Swiss Post Voting System: Voting Phase



Swiss Post Voting System: Voting Phase



Dispositions pénales

▲ Démarrer le vote

Saisir votre vote

Contrôler votre vote

◆ Vérifier les codes

6 Saisir votre code de confirmation

7 ★ Vérifier le code de finalisation

6 Saisir le code de confirmation

Saisissez votre code de confirmation pour transmettre votre vote électronique

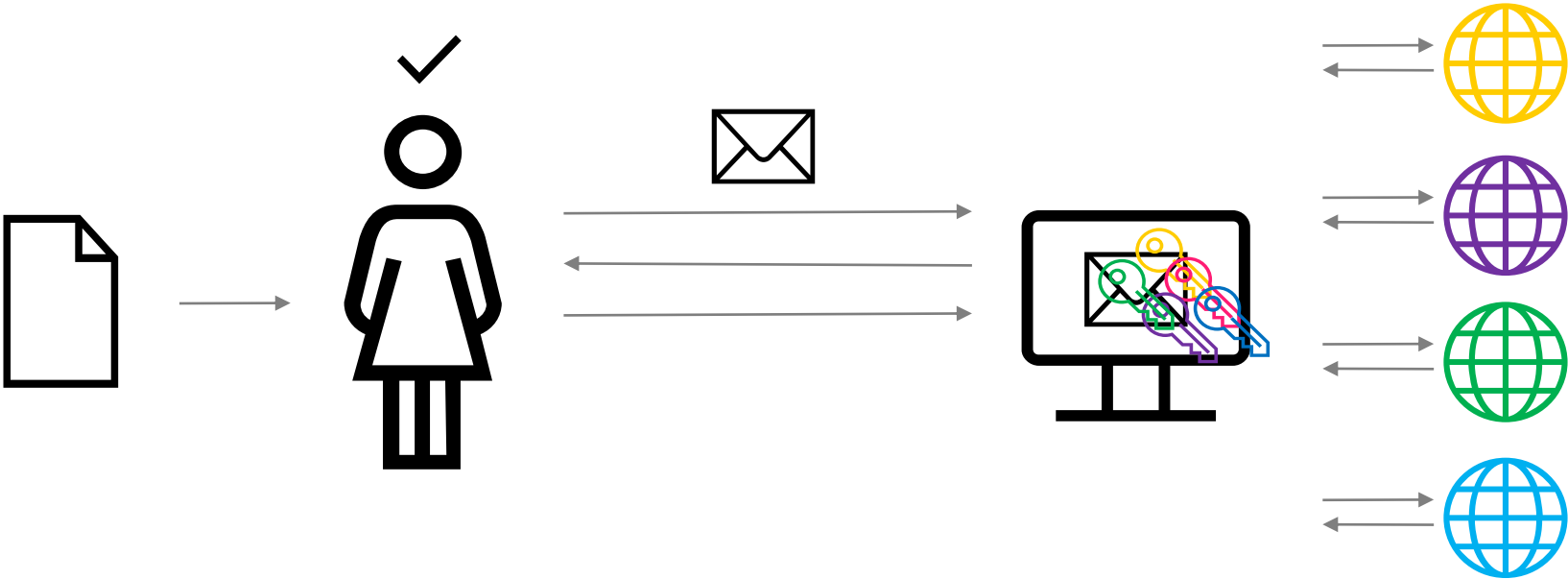
 **Code de confirmation** [? Qu'est-ce que le code de confirmation?](#)

5 0 4 3 8 3 6 4 4

 Une fois que vous l'avez confirmé, votre vote est enregistré et vous ne pouvez plus voter par correspondance ou à l'urne.

[Interrompre la procédure de vote](#) [Retour](#) **Confirmer le vote** 

Swiss Post Voting System: Voting Phase



Swiss Post Voting System: Voting Phase

- ✓ Dispositions pénales
- ✓ ▲ Démarrer le vote
- ✓ Saisir votre vote
- ✓ Contrôler votre vote
- ✓ ◆ Vérifier les codes
- ✓ ⬢ Saisir votre code de confirmation
- 7 ★ **Vérifier le code de finalisation**

7 Vérifier le code de finalisation

Veillez comparer le code de finalisation avec celui qui figure sur votre carte de vote



Code de finalisation

[? Qu'est-ce que le code de finalisation?](#)

6403 0313

⊖ Le code ne correspond pas

✓ Le code correspond

24 b266 vh7p



Codes de vérification
à partir de la page 2



Code de confirmation
5043 8364 4



Code de finalisation
6403 0313

Usability for the Voter

- Human-entered codes → User-friendly alphabet
 - Use letters and numbers easily found on any keyboard
 - Minimize chance of misspelling (exclude letters and/or numbers that look similar)

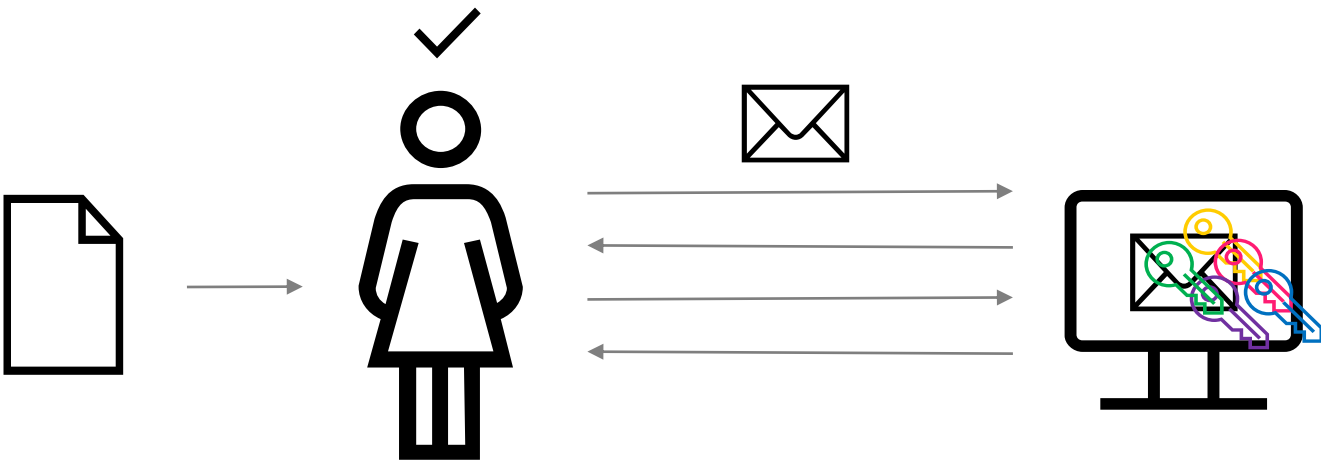
(a, b, c, d, e, f, g, h, i, j, k, m, n, p, q, r, s, t, u, v, w, x, y, z, 2, 3, 4, 5, 6, 7, 8, 9)

- Human-entered and human-verified codes → Code length trade-off between security and usability
 - Minimize chance of misspelling
 - If codes are too long, users may skip verification or make errors during the check

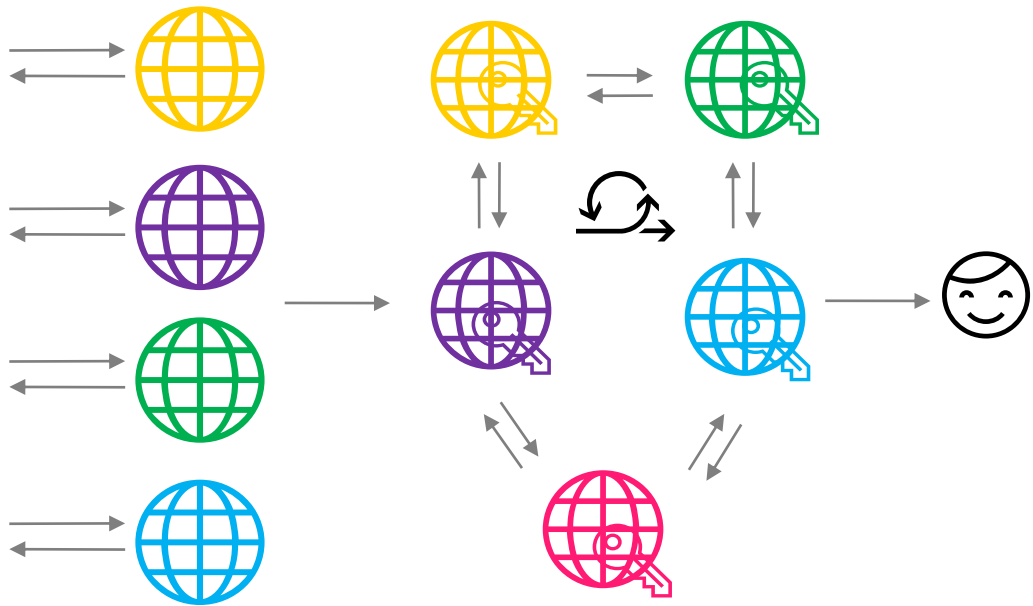
▲	Code d'initialisation	5rqs tt2e r26a xp24 b266 vh7p
◆	Codes de vérification à partir de la page 2	
▲	Code de confirmation	5043 8364 4
★	Code de finalisation	6403 0313

1x	2x
7689	
5914	3109
1769	3073
6451	
6311	9927
3998	1178
5316	
4214	
0289	
7058	
9849	

Swiss Post Voting System: Tally Phase

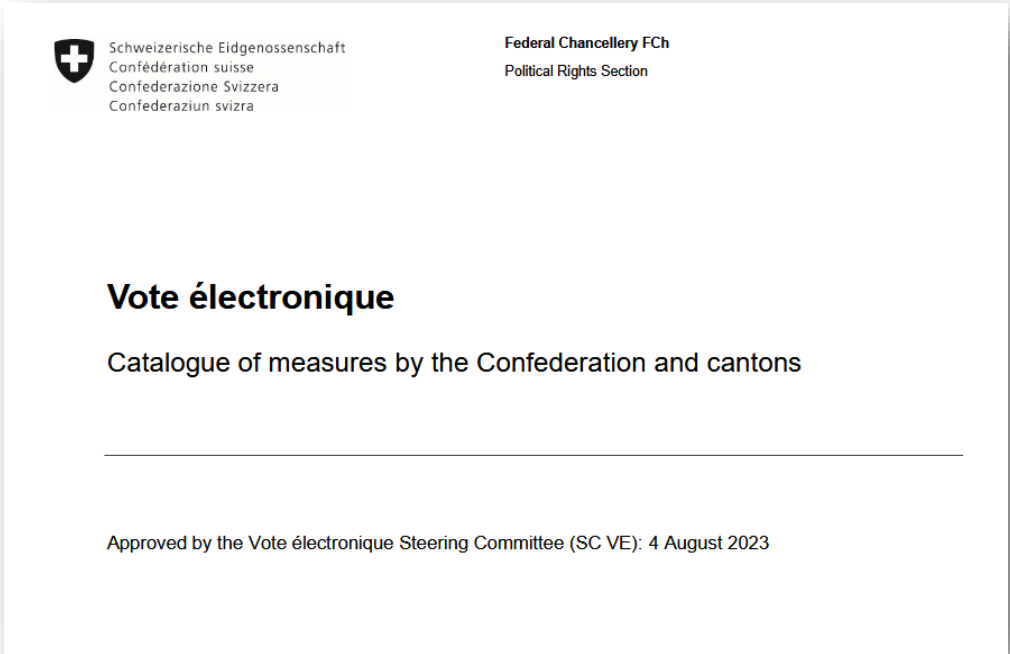
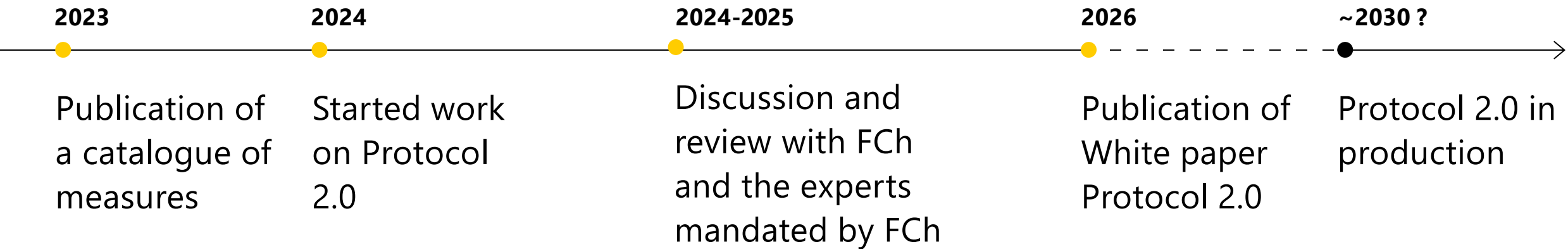


Eligibility Verifiability
Individual Verifiability
Universal Verifiability
Vote secrecy



Protocol 2.0

Roadmap towards Protocol 2.0



Protocol 2.0 Intuition

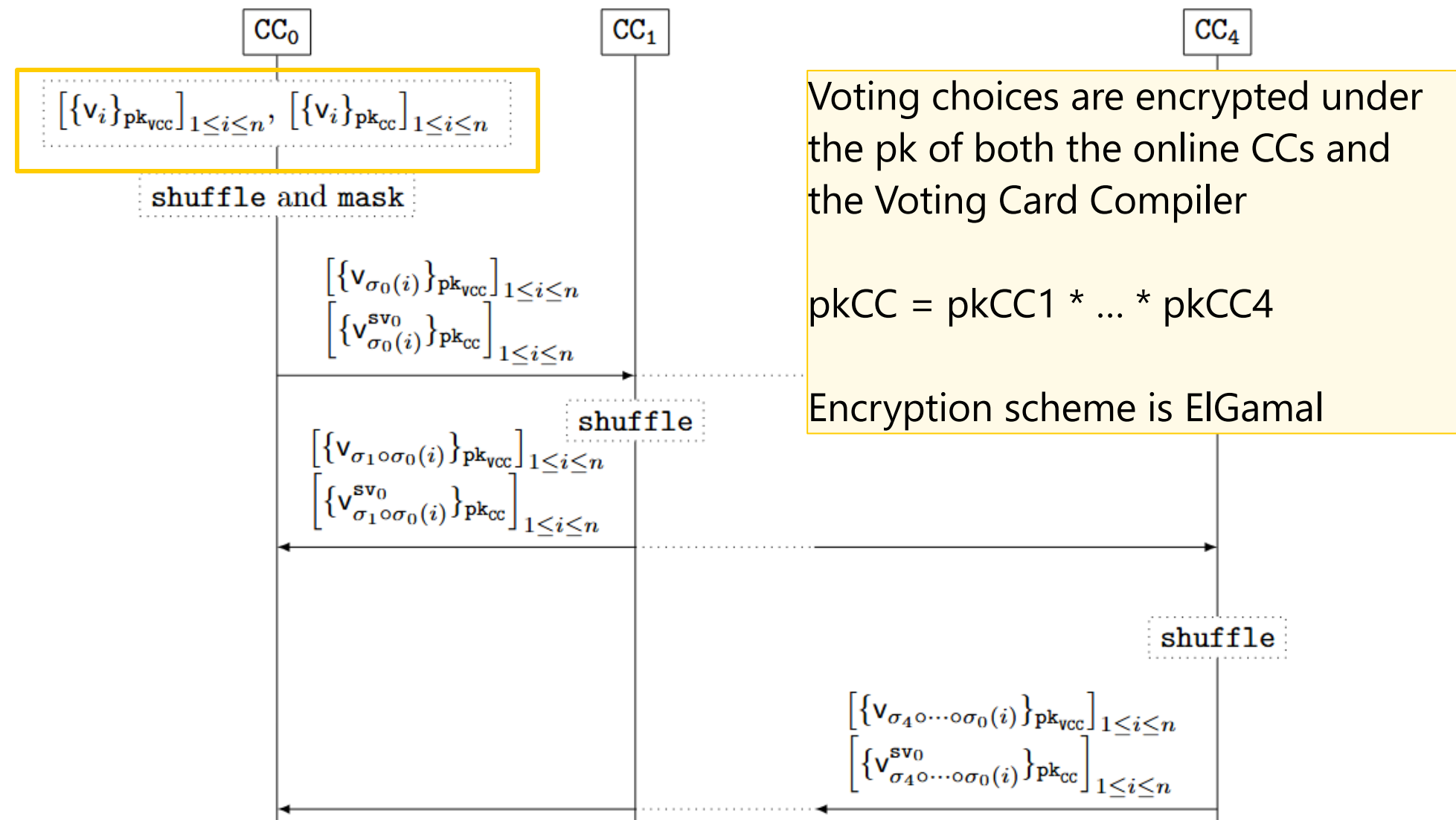
We consider the Setup Component as the zero Control Component CC0

We model the CC0 + 4 CCs as five entities jointly generating voting material in a distributed way

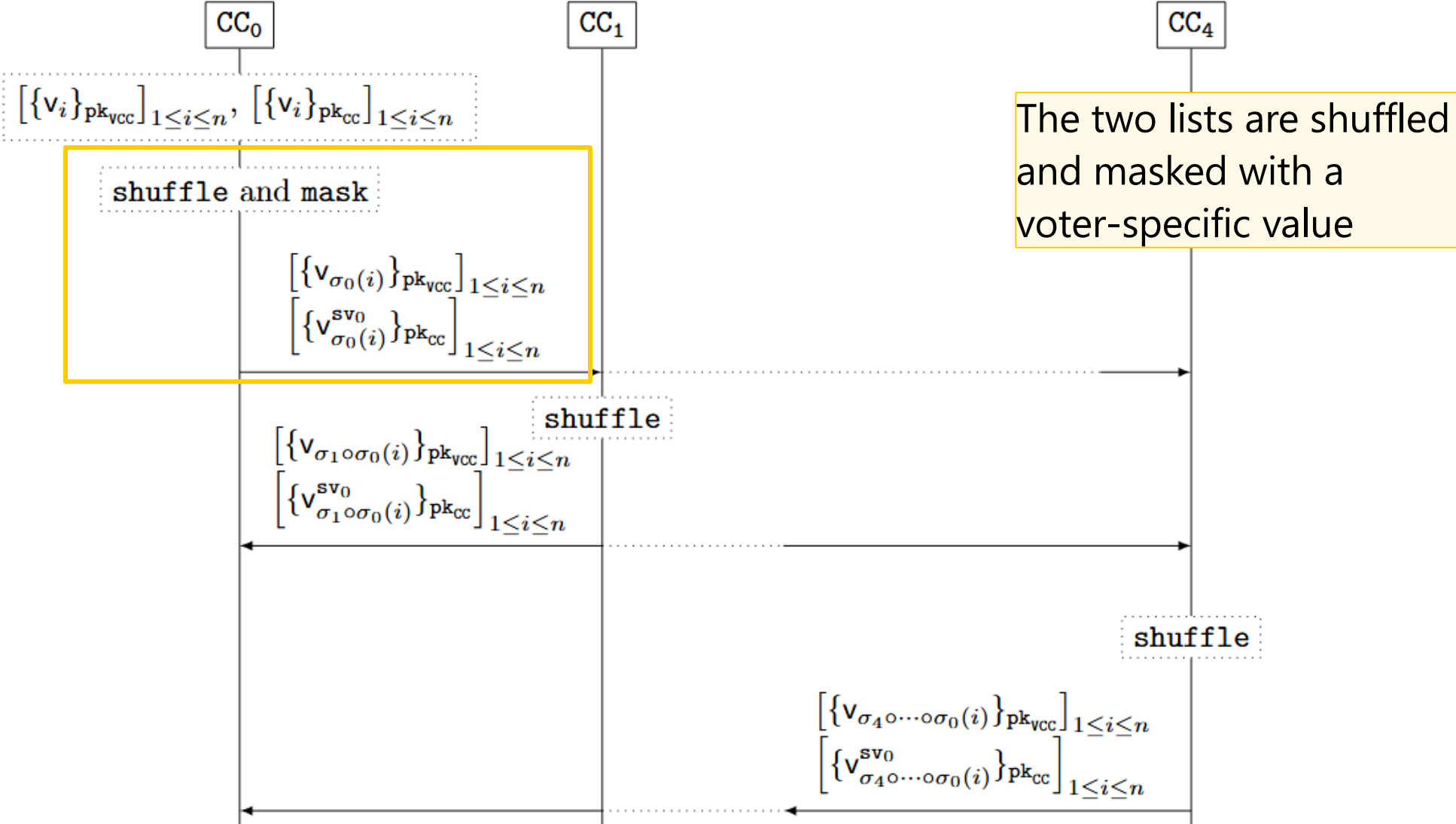
The five entities have asymmetric roles:

- return codes are generated during setup
- but sent to voters during voting, with one party offline
- vote privacy must be preserved throughout

Setup Phase – List of Voting Options

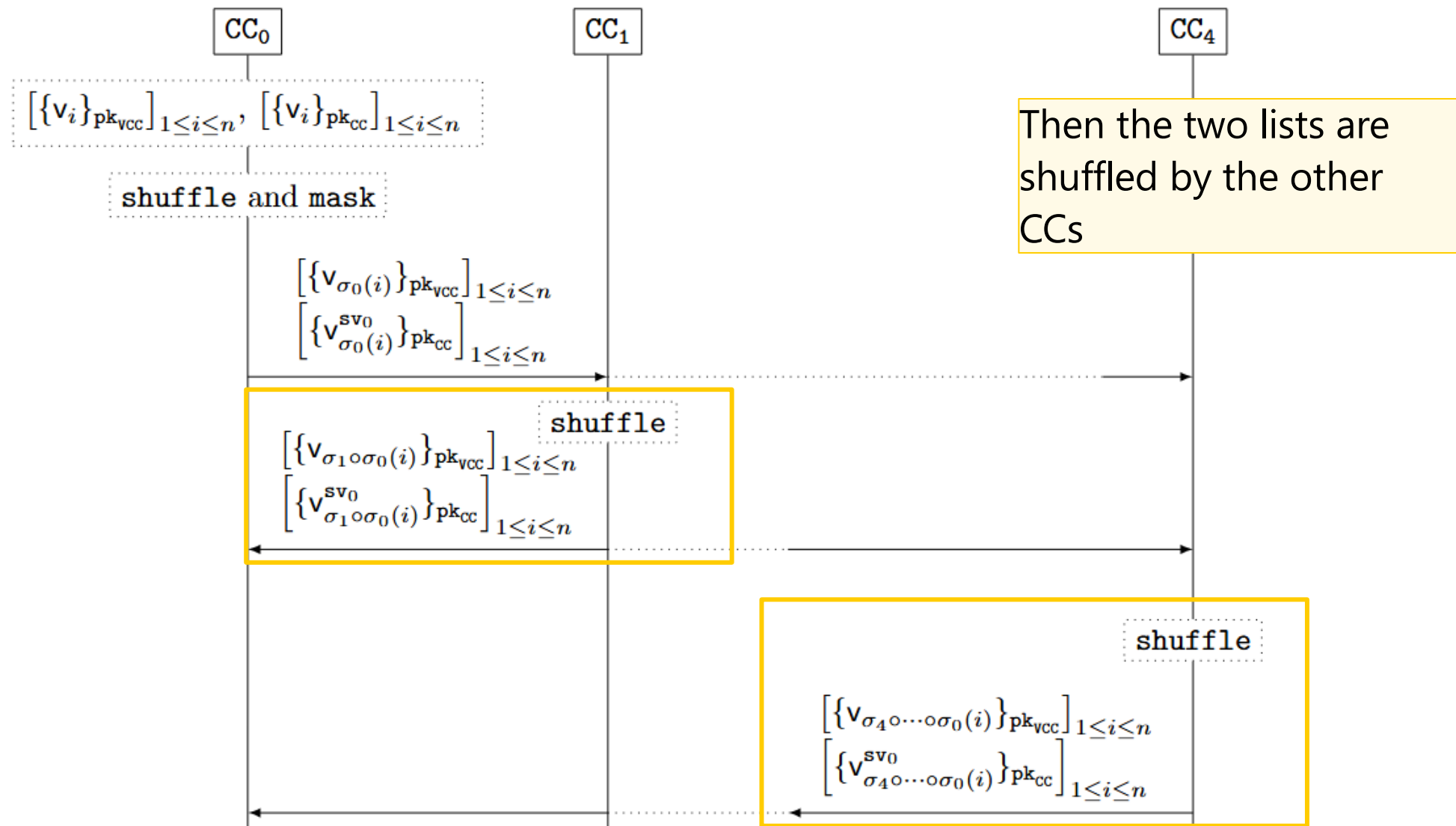


Setup Phase – List of Voting Options



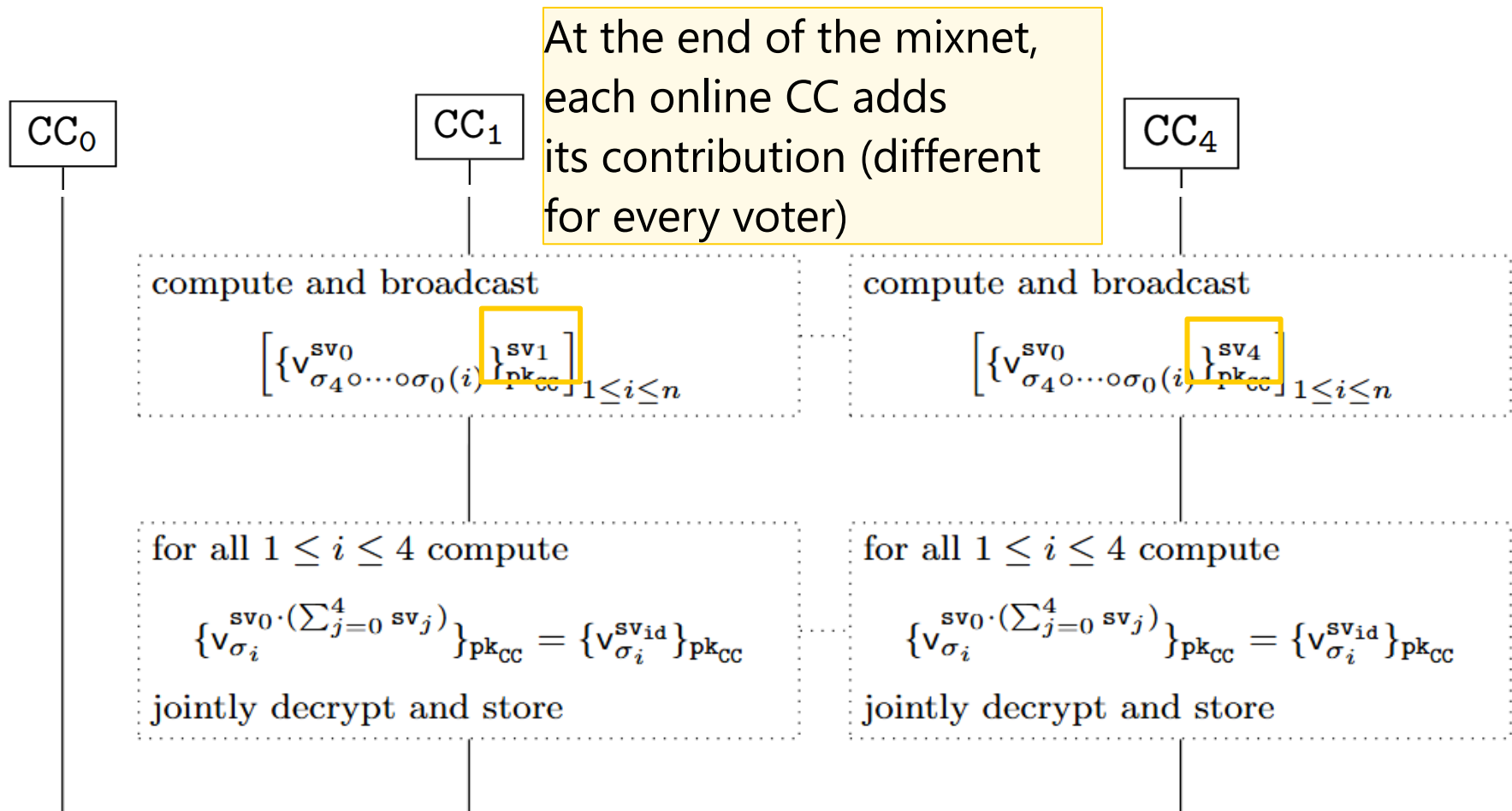
The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Setup Phase – List of Voting Options

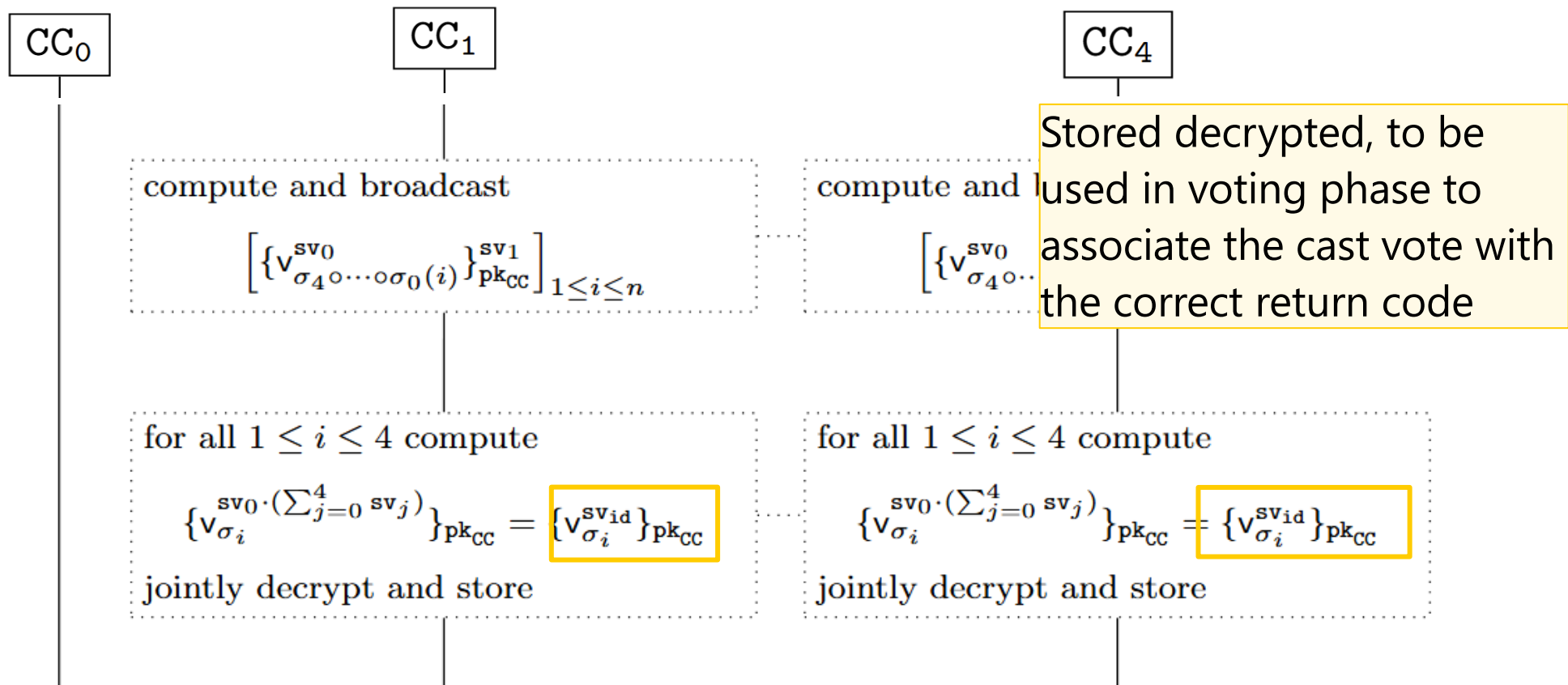


The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Setup Phase – List of Voting Options

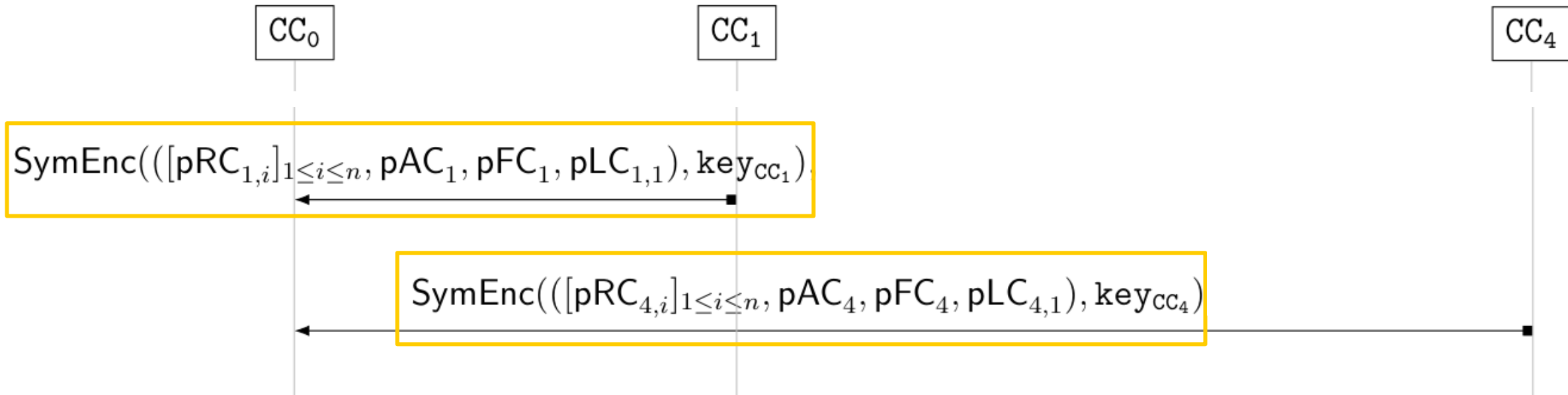


Setup Phase – List of Voting Options



Setup Phase – Codes Generation

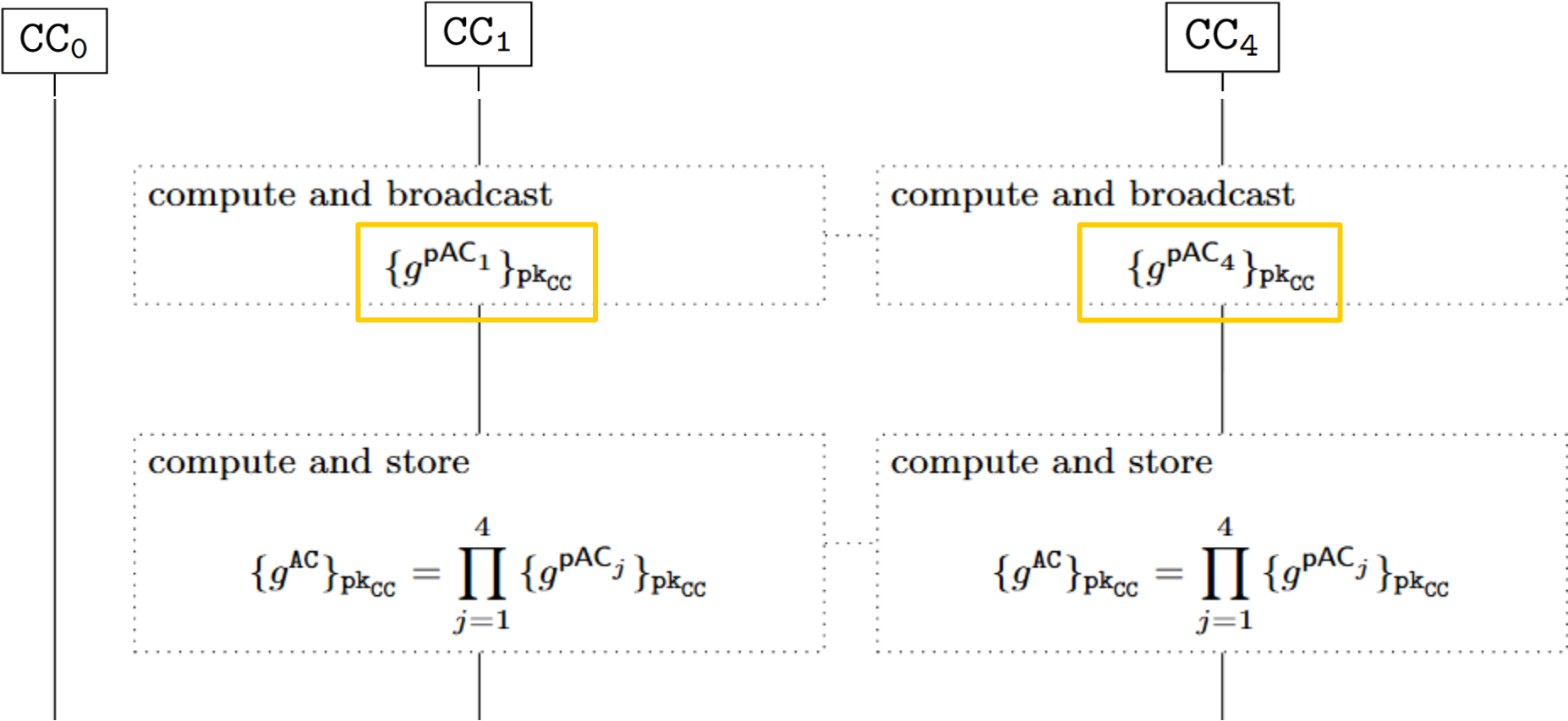
Each Online CC holds a share of each code



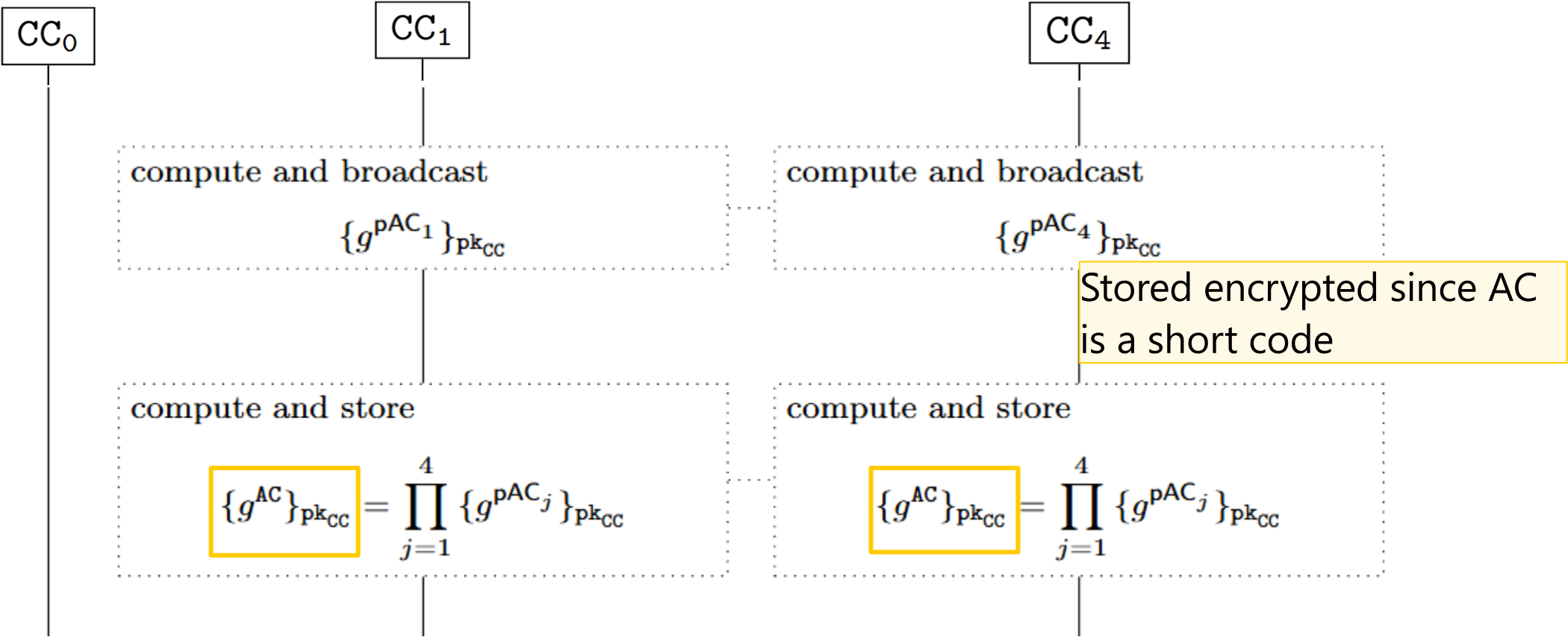
The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Setup Phase – Approve Code Subprotocol

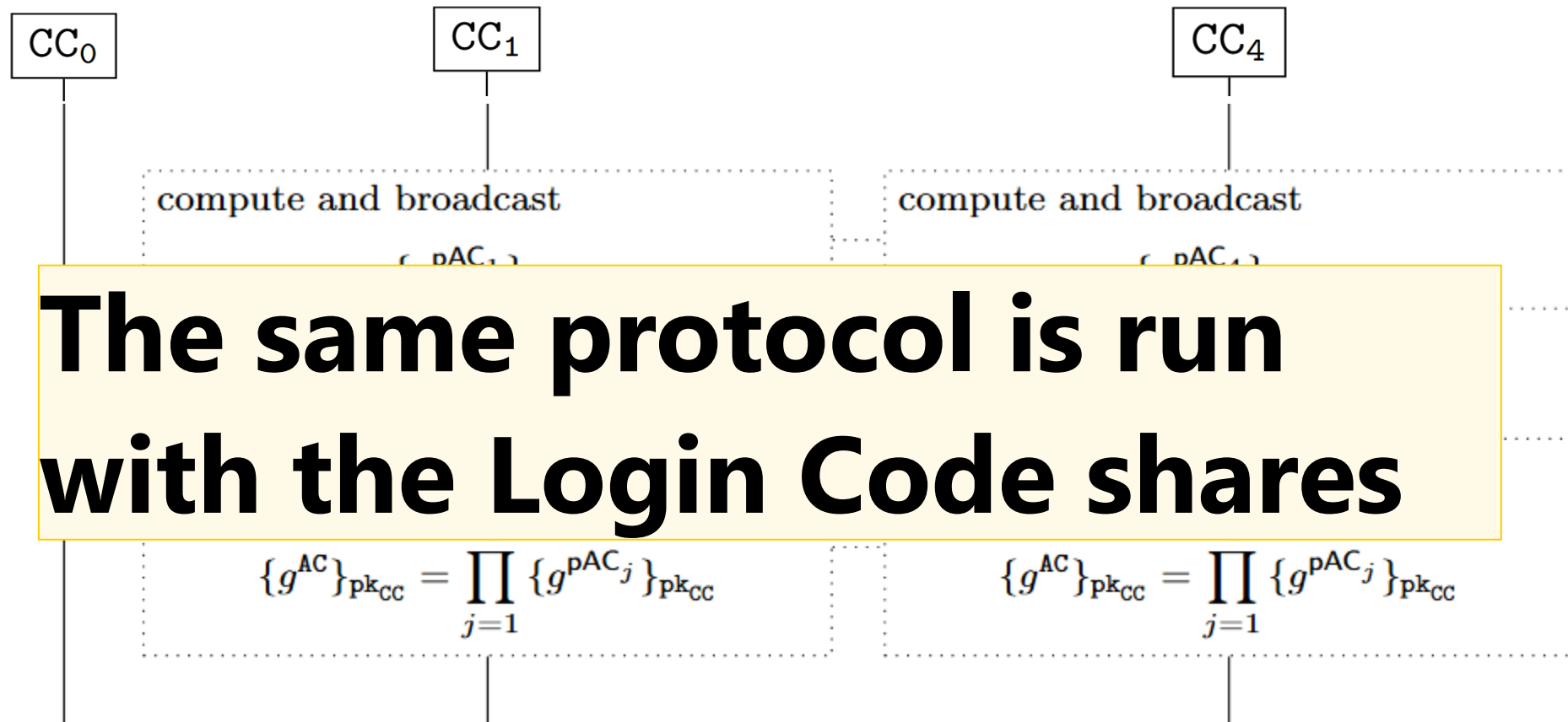
To retrieve AC, each CC computes



Setup Phase – Approve Code Subprotocol



Setup Phase – Approve Code Subprotocol



The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Setup Phase – PDF generation

Login code to access the voter portal

Generated by CC0 and CCjs:

- Prevent ballot stuffing from CCs
- Still CC0 is not able to cast votes

VCC

decrypt and generate PDFs:

$$LC = LC_0 || LC_1 \text{ with } LC_1 = \sum_{j=1}^4 pLC_{j,1}$$

$$(v_i, RC_{\sigma^{-1}(i)}) \text{ with } RC_i = \bigoplus_{j=1}^4 pRC_{j,i}$$

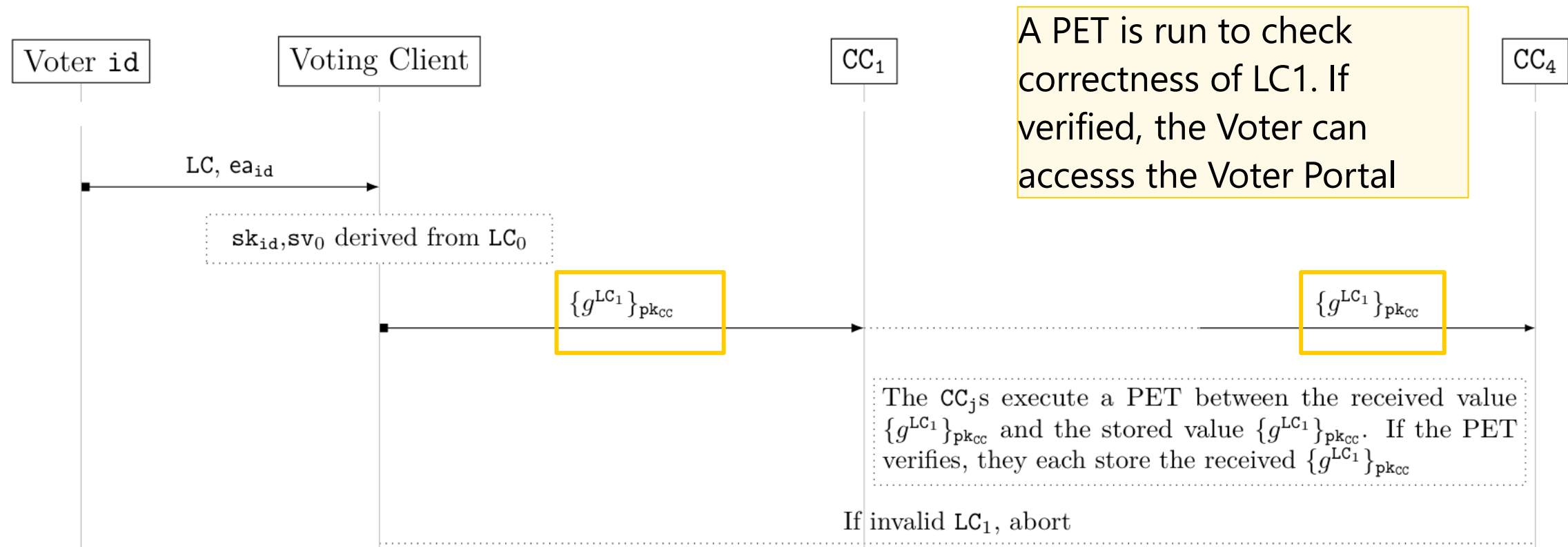
[The v_i 's are printed in the election prescribed order]

$$AC = \sum_{j=1}^4 pAC_j$$

$$FC = \bigoplus_{j=1}^4 pFC_j$$

The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

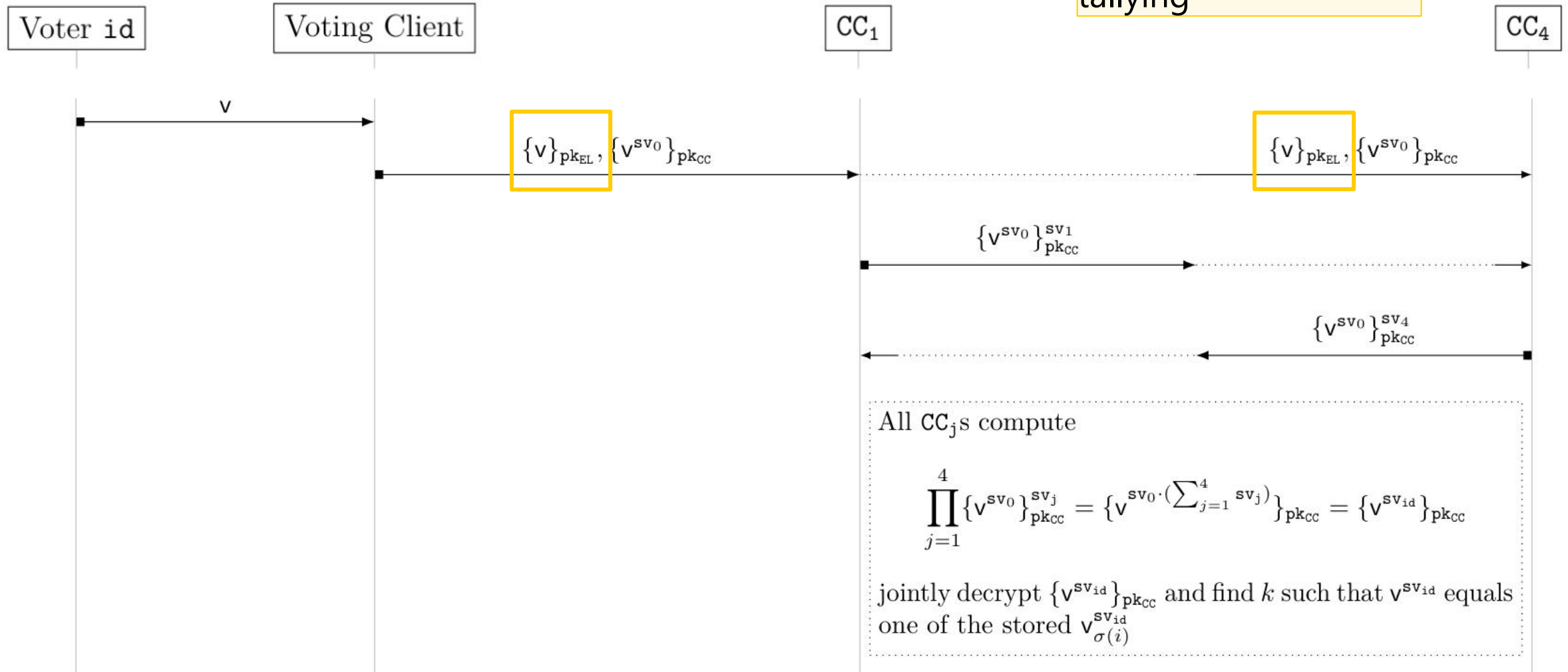
Voting Phase – Cast Vote



The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

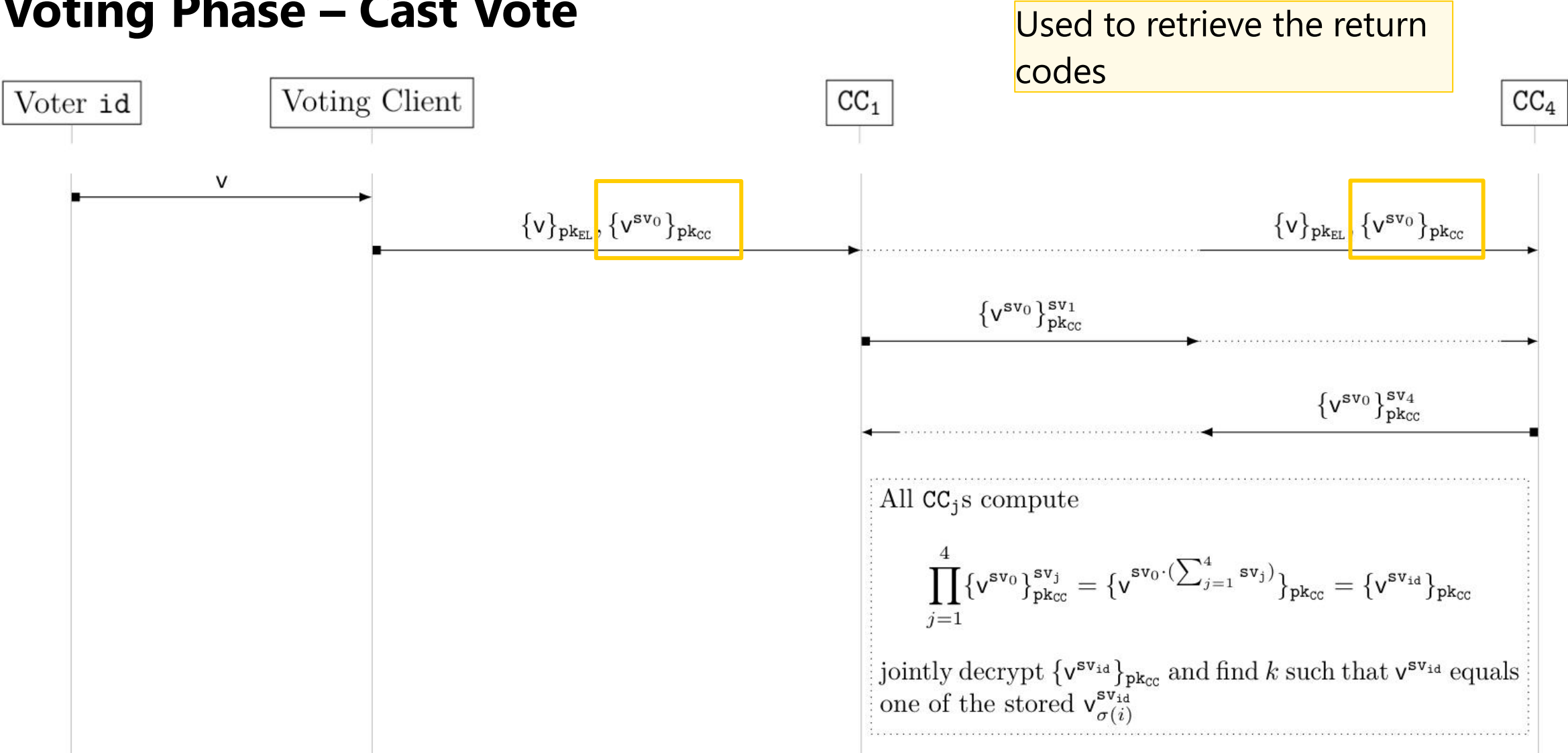
Voting Phase – Cast Vote

Will be used for
tallying

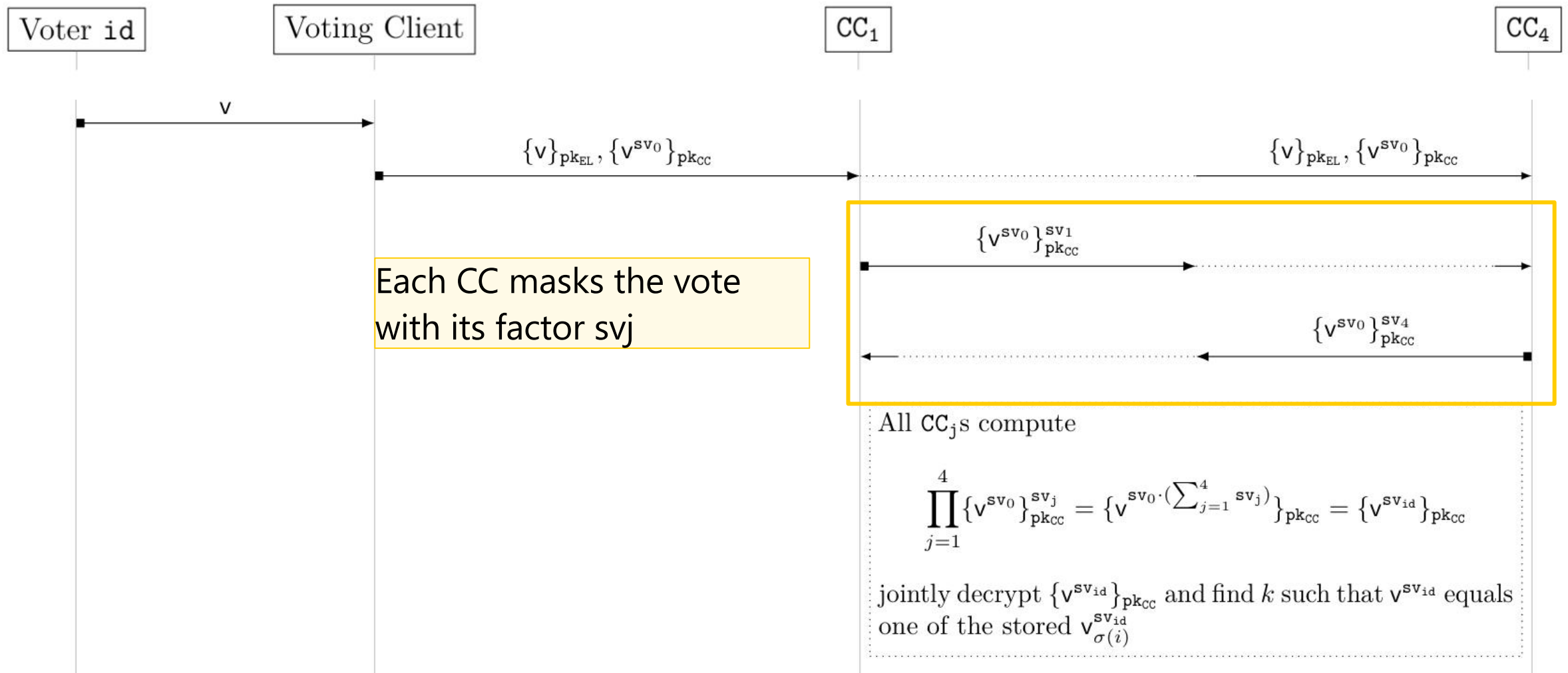


The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Voting Phase – Cast Vote

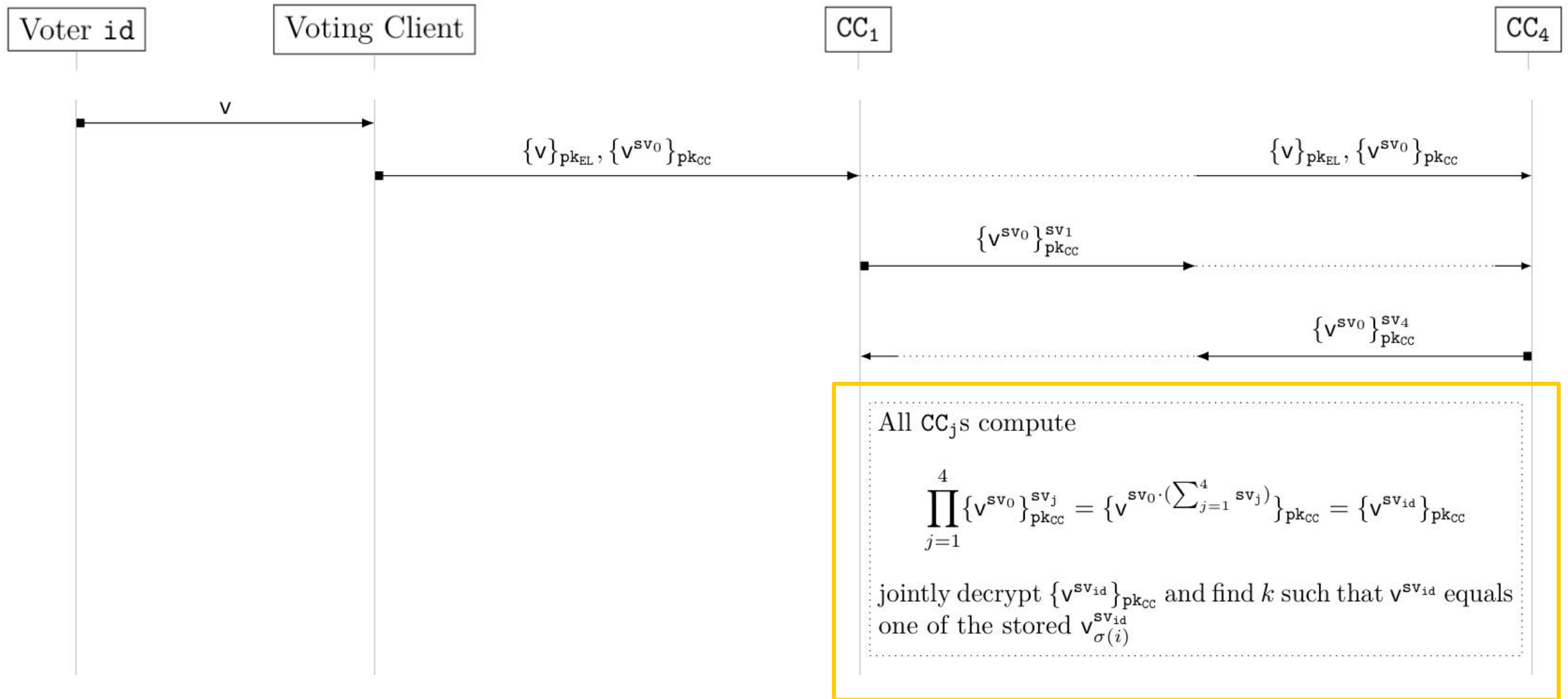


Voting Phase – Cast Vote



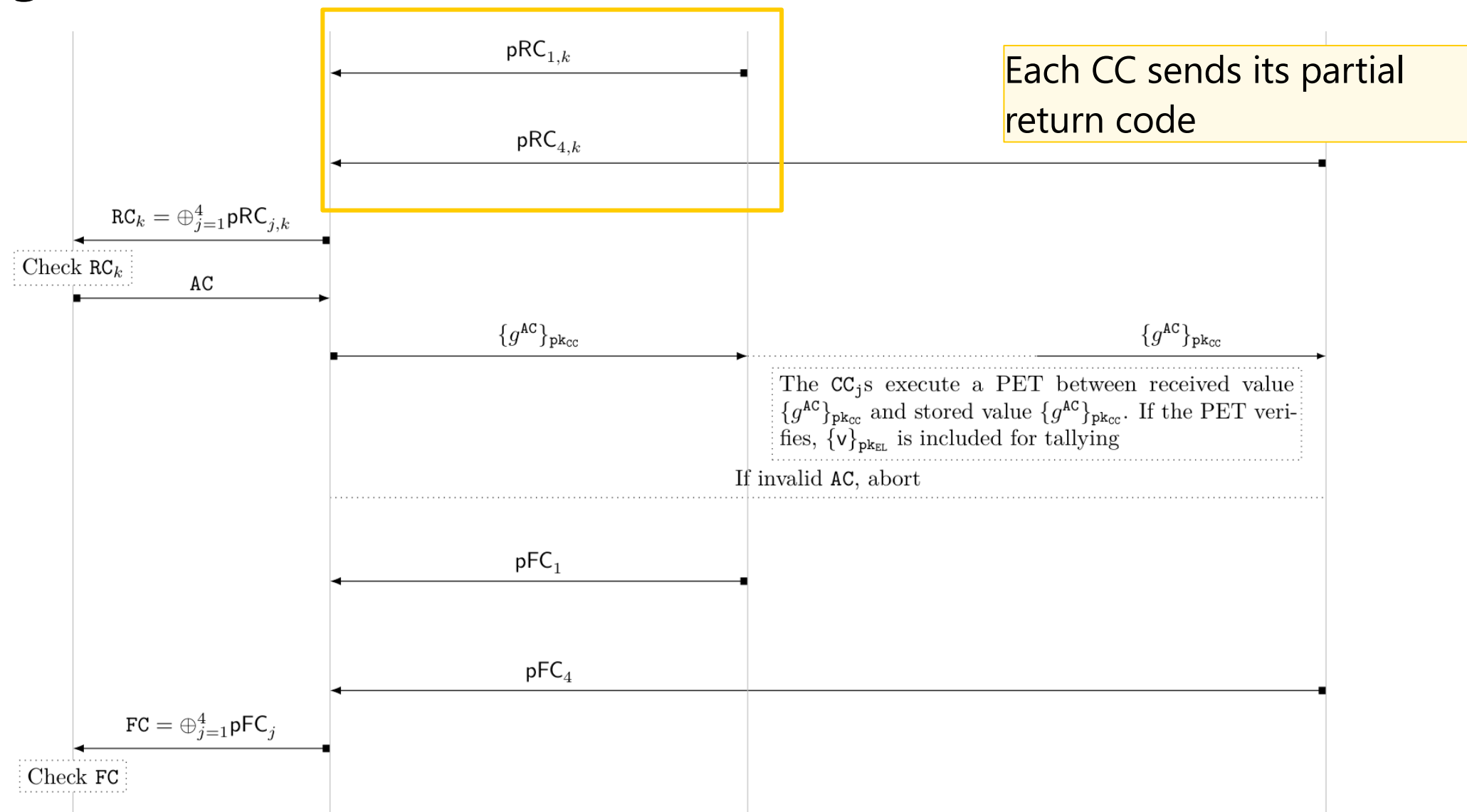
The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Voting Phase – Cast Vote

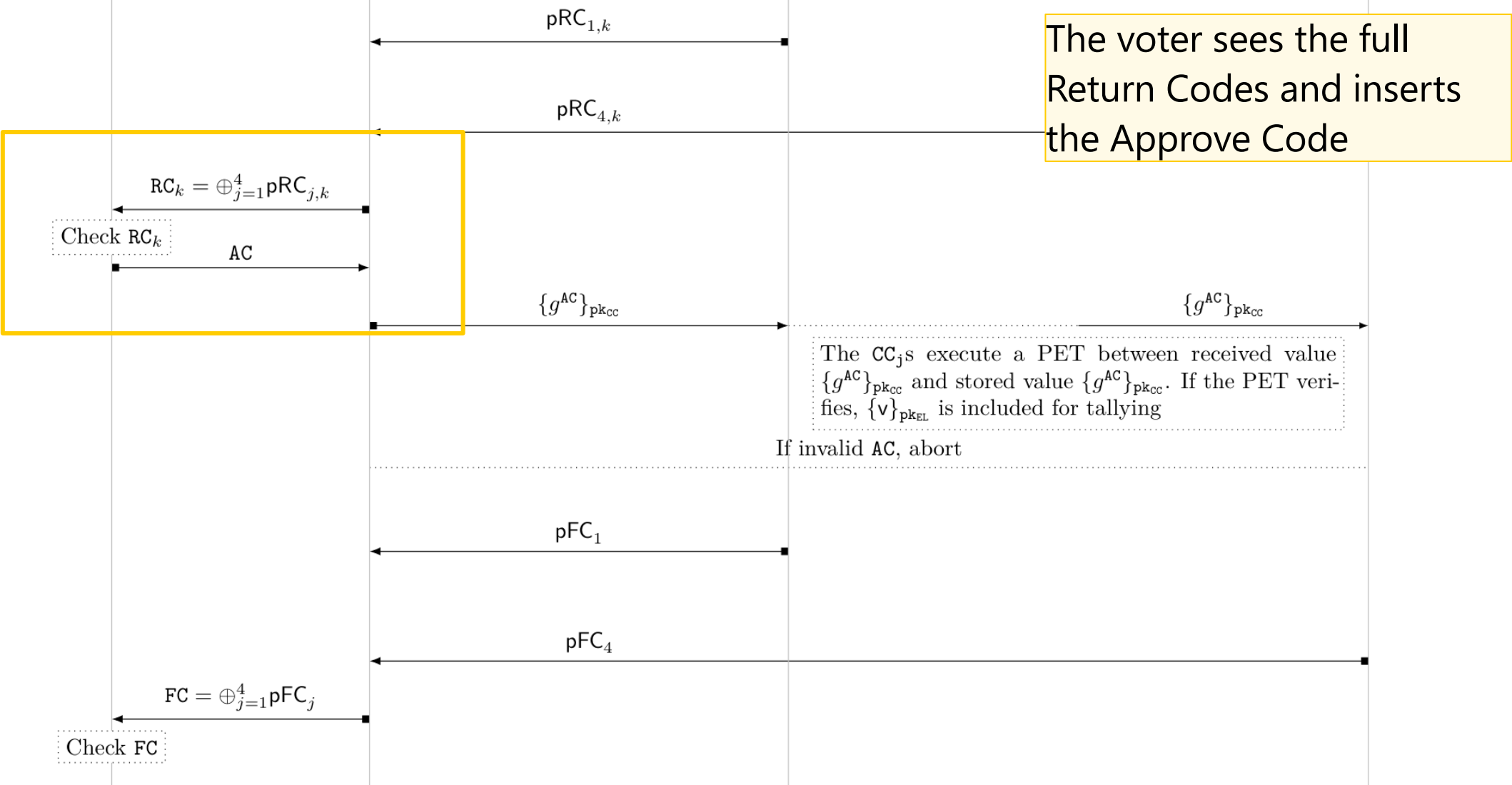


The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

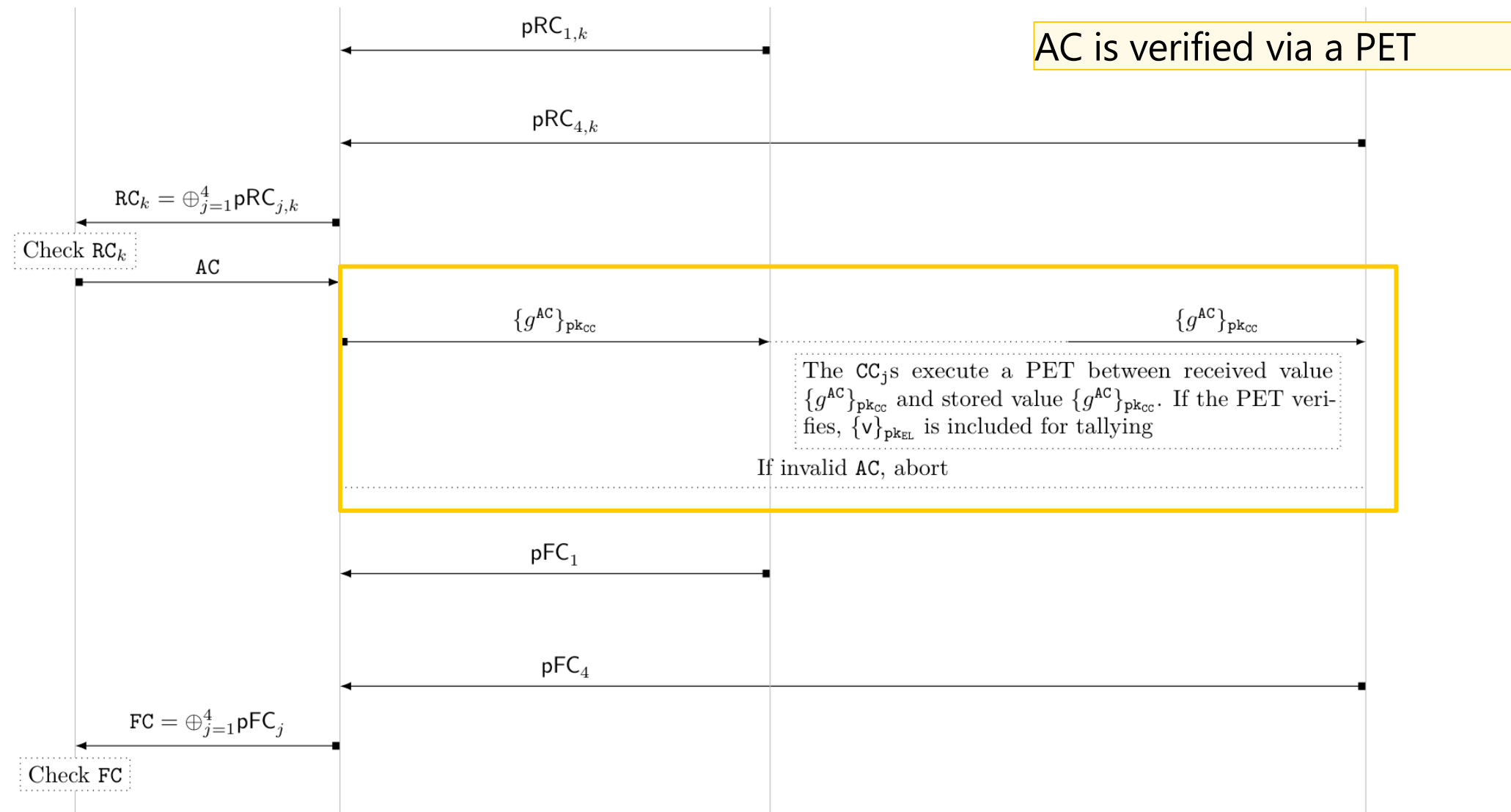
Voting Phase – Return Codes



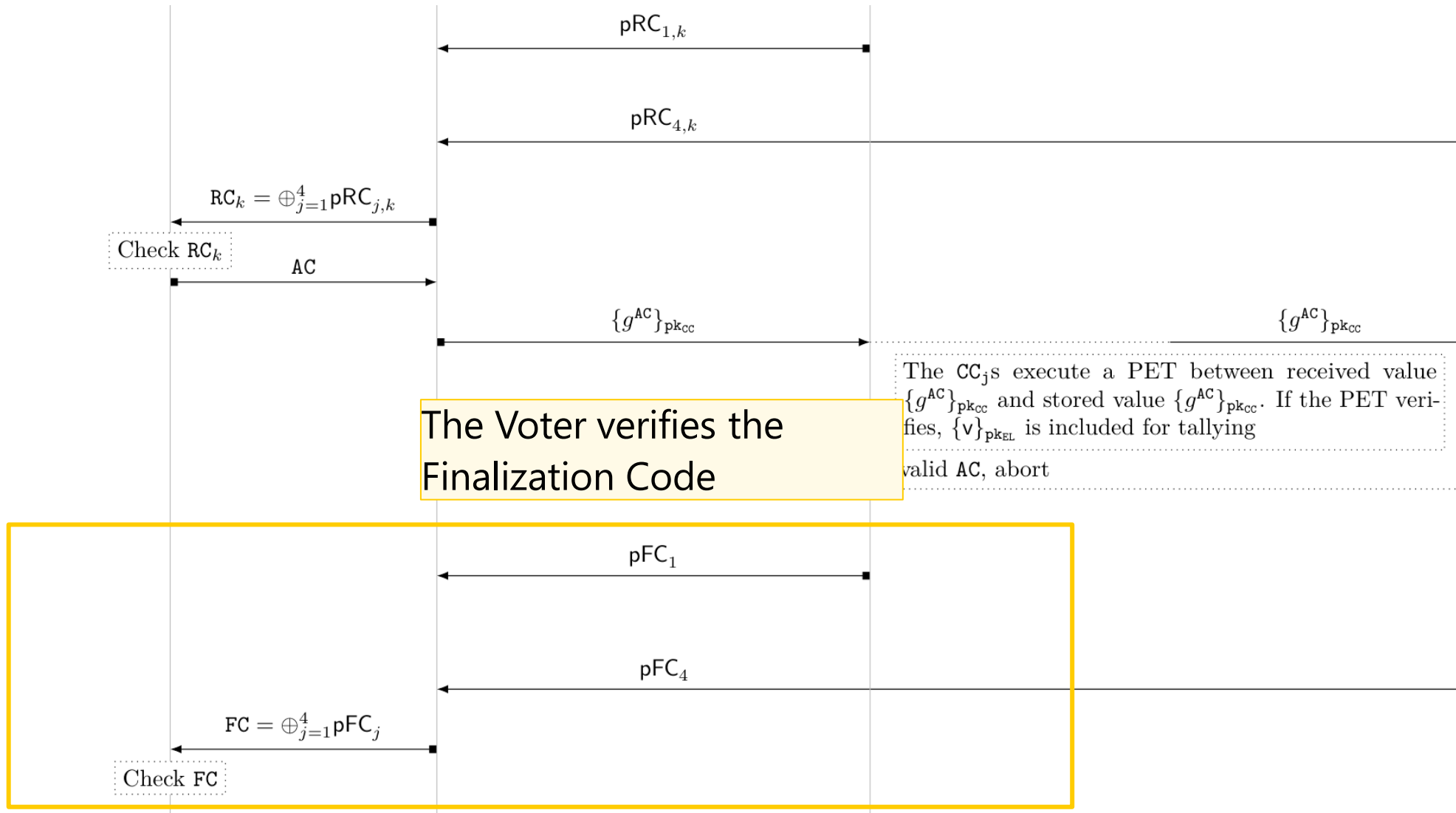
Voting Phase – Return Codes



Voting Phase – Return Codes



Voting Phase – Return Codes



The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Some more discussion on Protocol 2.0

Setup Phase – PDF generation

How can we guarantee unique return codes?

VCC

decrypt and generate PDFs:

$$\text{LC} = \text{LC}_0 \parallel \text{LC}_1 \text{ with } \text{LC}_1 = \sum_{j=1}^4 p\text{LC}_{j,1}$$

$$(v_i, \text{RC}_{\sigma^{-1}(i)}) \text{ with } \text{RC}_i = \bigoplus_{j=1}^4 p\text{RC}_{j,i}$$

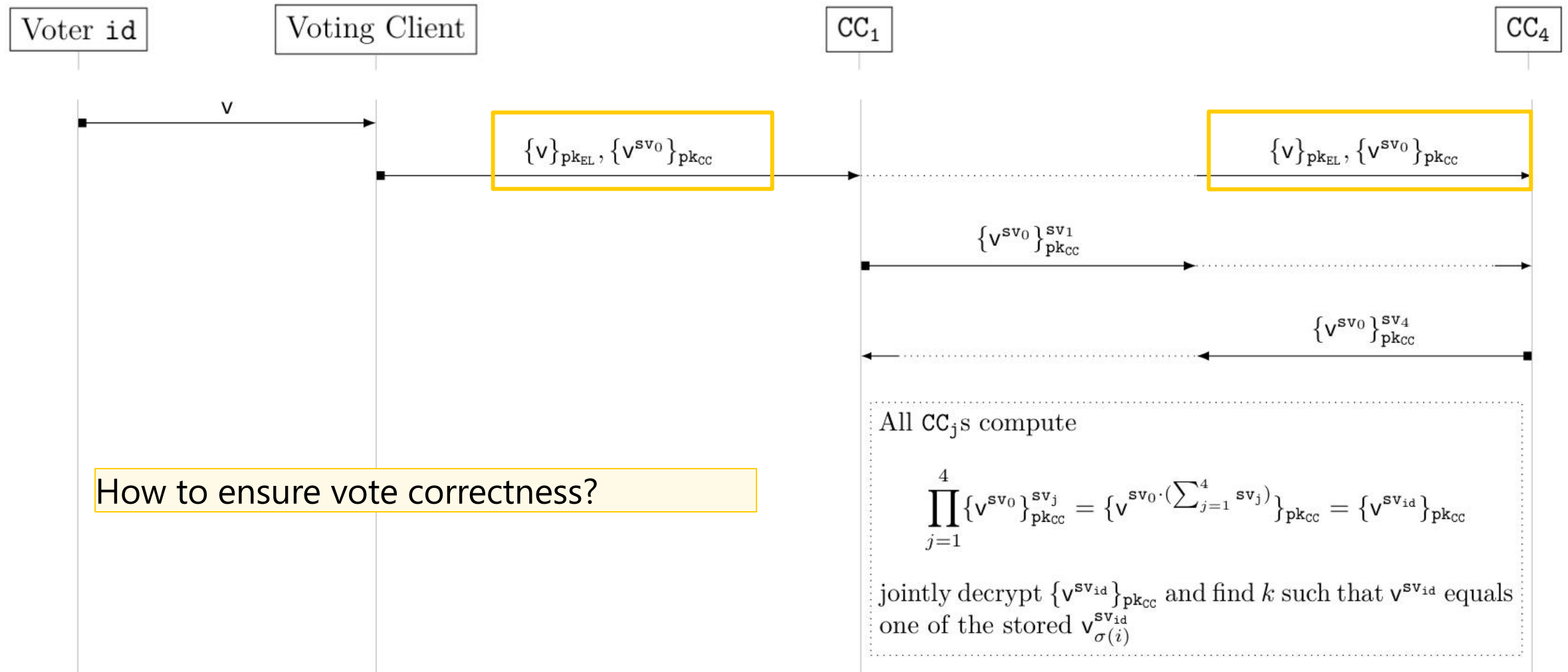
[The v_i 's are printed in the
election prescribed order]

$$\text{AC} = \sum_{j=1}^4 p\text{AC}_j$$

$$\text{FC} = \bigoplus_{j=1}^4 p\text{FC}_j$$

The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Voting Phase – Cast Vote



The diagrams are simplified for the presentation, all zero knowledge proofs and signatures are omitted

Thank you!

Audhild Høgåsen
audhild.hoegaasen@post.ch

Chiara Spadafora
chiara.spadafora.1@post.ch

<https://demo.evoting.ch/>



<https://gitlab.com/swisspost-evoting>



<https://swisspost-digital.ch/en/evoting-community/contributions>

