A formal analysis of the Norwegian e-voting protocol

Véronique Cortier, Cyrille Wiedling

A formal analysis of the Norwegian e-voting protocol

Véronique Cortier, Cyrille Wiedling

RESEARCH REPORT

N° 7781

November 2011

Project-Team Cassis

ISSN 0249-6399 ISRN INRIA/RR--7781--FR+ENG

A formal analysis of the Norwegian e-voting protocol[*]

Véronique Cortier[†], Cyrille Wiedling[†]

Project-Team Cassis

Research Report n° 7781 — November 2011 — 75 pages

Abstract: Norway has used e-voting in its last political election in September 2011, with more than 25 000 voters using the e-voting option. The underlying protocol is a new protocol designed by the ERGO group, involving several actors (a bulletin box but also a receipt generator, a decryption service, and an auditor). Of course, trusting the correctness and security of e-voting protocols is crucial in that context. Formal definitions of properties such as privacy, coercion-resistance or verifiability have been recently proposed, based on equivalence properties.
In this paper, we propose a formal analysis of the protocol used in Norway, w.r.t. privacy, considering several corruption scenarios. Part of this study has conducted using the ProVerif tool, on a simplified model.

Key-words: e-voting, privacy, formal methods

[*] The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Program (FP7/2007-2013) / ERC grant agreement no 258865, project ProSecure.

[†] LORIA, CNRS & INRIA project Cassis

RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Analyse formelle du protocole de vote électronique Norvégien

Résumé : En Septembre 2011, la Norvège a mis en place le vote électronique lors de ses élections politiques, avec plus de 25 000 votants qui ont effectivement utilisé cette option. Le protocole sous-jacent, créé par la compagnie ERGOgroup, met en jeu plusieurs acteurs (une urne mais également un générateur de reçu, un déchiffreur et un auditeur). Pouvoir faire confiance en l'exactitude et la sécurité des protocoles de votes électroniques est bien entendu crucial dans ce contexte. En se basant sur des propriétés d'équivalence, des définitions formelles de la confidentialité, de la résistance à la coercition ou de la vérifiabilité on été récemment proposées.

Dans ce rapport, nous proposons une analyse formelle du protocole utilisé en Norvège dans le but de démontrer la propriété de confidentialité en considérant plusieurs scénarios de corruption. Une partie de cette étude a été menée avec l'utilisation de l'outil ProVerif, sur un modèle simplifié.

Mots-clés : confidentialité, méthodes formelles, vote électronique

1 Introduction

Electronic voting protocols promise a convenient, efficient and reliable way for collecting and tallying the votes, avoiding for example usual human errors when counting. It is used or have been used for political elections in several countries like e.g. USA, Estonia, Swiss and recently Norway, at least in trials. However, the recent history has shown that these systems are highly vulnerable to attacks. For example, the Diebold machines as well as the electronic machines used in India have been attacked [12, 20]. Consequently, the use of electronic voting raises many ethical and political issues. For example, the German Federal Constitutional Court decided on 3 March 2009 that electronic voting used for the last 10 years was unconstitutional [1].

There is therefore a pressing need for a rigorous analysis of the security of e-voting protocols. A first step towards the security analysis of e-voting protocols consists in precisely defining security w.r.t. e-voting. Ryan *et al.* have proposed formal definitions for several key properties such as privacy, receipt-freeness, coercion resistance, or verifiability [11, 16] in terms of equivalence-based properties. It is however difficult to formally analyse e-voting protocols for two main reasons. First there are very few tools that can check equivalence properties: ProVerif [6, 7] is probably the only one but it does not really work in the context of e-voting (because it tries to show a stronger notion of equivalence, which is not fulfilled when checking for ballot secrecy). Moreover, the cryptographic primitives used in e-voting are rather complex and non standard and are typically not supported by existing tools.

In this paper, we study the protocol used in last September for political elections in Norway [2]. E-voting was proposed as trials in several municipalities and more than 25 000 voters did use e-voting to actually cast their vote. The protocol is publicly available [14] and can be seen as a variant of the Helios protocol [4] with additional components: a Receipt Generator and an Auditor which aim at watching the Bulletin Box recording the votes. The resulting protocol is therefore complex, e.g. using El Gamal encryption in a non standard way. In [14], Gjøsteen describes the protocol and discusses its security. To our knowledge, there does not exist any security proof, even for the crucial property of vote privacy.

Our contribution. We conduct a formal analysis of the Norwegian protocol w.r.t. privacy. Our first contribution is the proposition of a formal model of the protocol in applied-pi calculus [3]. One particularity of the protocol is to distribute public keys $\mathsf{pk}(a_1)$, $\mathsf{pk}(a_2)$, and $\mathsf{pk}(a_3)$ for the three authorities, such that the corresponding private keys a_1, a_2, and a_3 verify the relation $a_1 + a_2 = a_3$, allowing one component (here the Bulletin Box) to re-encrypt messages. The protocol also makes use of signature, of zero-knowledge proofs, of blinding functions and coding functions. We have therefore proposed a new equational theory reflecting the unusual behavior of the primitives.

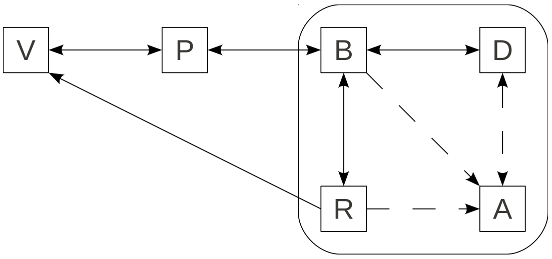
Our second contribution is a formal security proof of privacy, in the presence of arbitrarily many dishonest voters. Given the complexity of the equational theory (with e.g. four associative and commutative symbols), the resulting processes can clearly not be analyzed with existing tools, even ProVerif. We therefore proved privacy (expressed as an equivalence property) by hand. The proof happens to be quite technical. Its first step is rather standard and consists in guessing a relation such that the two initial processes and all their possible evolutions are in relation. The second step is more involved: it requires to prove equivalent an infinite number of frames, the frames representing all possible attacker knowledge. Indeed, unlike most previously analyzed protocols, the Norwegian protocol emits receipts for the voters, potentially providing extra information to the attacker. Proving static equivalence is also made difficult due to our equational theory (e.g. four associative and commutative symbols).

Our third contribution is an analysis of the protocol for further corruption scenarios, using the ProVerif tool in a simplified model (therefore possibly losing attacks). In conclusion, we did not find any attack, except when the bulletin box and the receipt generator or the decryption service alone are corrupted. These attacks are probably not surprising but they were never made explicit in the documentation we found.

Related Work. [14] provides a discussion on the security of the Norwegian protocol but no security proof. We do not know any other study related to this protocol. Several other e-voting protocols have been studying using formal methods. The FOO [13], Okamoto [19] and Lee *et al.* [17] voting protocols have been analysed in [11]. Similarly, Helios has been recently proved secure both in a formal [10] and a computational [5] model. However, all these protocols were significantly simpler to analyse. Indeed, the voters (and thus the dishonest voters) had very few interactions with the other components, sending only their ballots. In contrast, in the Norwegian protocol, both the Receipt Generator and the Bulletin Box send receipts to the voters, that depend in the casted ballot. Therefore, the knowledge of the attacker increases at each step.

We informally describe the protocol in Section 2. The applied-pi calculus is briefly defined in Section 3. We then provide a formal modeling of the protocol in Section 4 and formally state and prove the privacy properties satisfied by the protocol in Section 5. The results obtained with ProVerif are described in Section 6. Concluding remarks can be found in Section 7. All the proofs are provided in Appendix.

2 Norwegian E-Voting Protocol



Norwegian protocol features several players including four players representing the electronic poll's infrastructure : a ballot box (B), a receipt generator (R), a decryption service (D) and an auditor (A). Each voter (V) can log in using a computer (P) in order to submit his vote. Channels between computers (voters) and the ballot box are considered as authenticated channel, channels between infrastructure's player are untappable channels and channel between voters and receipt generator is a unidirectional out-of-band channel. (Example of SMS is given in [14].) The protocol can be divided in three phases : the

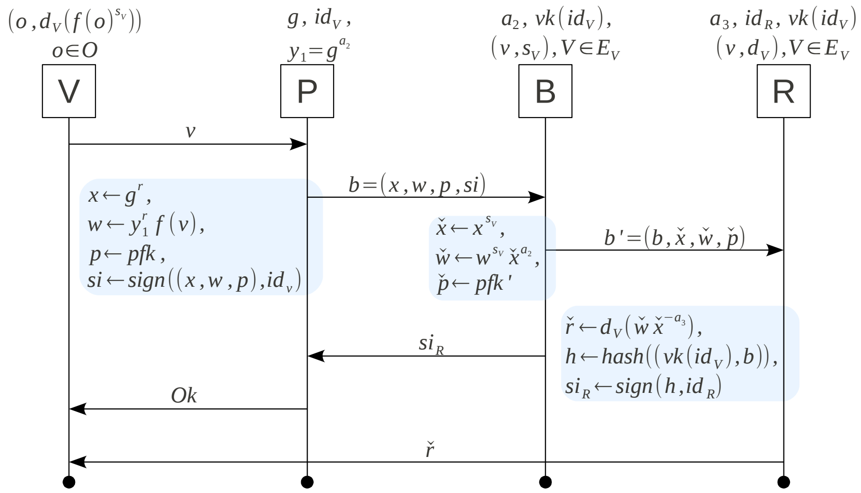

$(o, d_V(f(o)^{s_V}))$
$o \in O$
g, id_V,
$y_1 = g^{a_2}$
a_2, $vk(id_V)$,
$(v, s_V), V \in E_V$
a_3, id_R, $vk(id_V)$
$(v, d_V), V \in E_V$
V
P
B
R
v
$b = (x, w, p, si)$
$x \leftarrow g^r$,
$w \leftarrow y_1^r f(v)$,
$p \leftarrow pfk$,
$si \leftarrow sign((x, w, p), id_v)$
$\check{x} \leftarrow x^{s_V}$,
$\check{w} \leftarrow w^{s_V} \check{x}^{a_2}$,
$\check{p} \leftarrow pfk'$
$b' = (b, \check{x}, \check{w}, \check{p})$
$\check{r} \leftarrow d_V(\check{w} \check{x}^{-a_3})$,
$h \leftarrow hash((vk(id_V), b))$,
$si_R \leftarrow sign(h, id_R)$
si_R
Ok
$\check{r}$

Figure 1: Submission of one vote.

setting phase, the submission phase, where voters submit their votes, and the counting phase, where ballots are counted and auditor verifies the correctness of the election.

2.1 Setting phase

Before the election, private keys a_1, a_2, and a_3 (such that $a_1 + a_2 = a_3$) are distributed over, respectively D, B, and R, while the corresponding public keys are made publicly available. The receipt generator R is assumed to have a signing key id_R which corresponding verification key is distributed to P. The voters are also assume to each have a signing key id_V which corresponding verification key is distributed to B. The bulletin board B is provided with a table $V \mapsto s_V$ with a blinding factor s_V for each voter V. The receipt generator R is given a table $V \mapsto d_V$ with a permutation function d_V for each voter V. Finally, each voter V is assumed to received by post a table where, for each voting option o corresponds a precomputed receipt code $d_V(f(o)^{s_V})$.

2.2 Submission phase

The submission phase is depicted in Figure 1. We detail below the expected behavior of each participant.

Voter (V). Each voter tells his computer what voting option o to submit and allows it to sign the corresponding ballot on his behalf. Then, he has to wait for an acceptance message coming from the computer and a receipt $\check{r}$ sent by the receipt generator through the out-of-band channel. Using the receipt, he verifies that the correct vote was submitted, that is, he checks that $\check{r} = d_V(f(o)^{s_V})$ by verifying that the receipt code $\check{r}$ indeed appears in the line associated to o.

Computer (P). Voter's computer encrypts voter's ballot using the public key y_1 using standard El Gamal encryption. The resulting ballot is $(g^r, y^r f(o))$

where f is some encoding function for voting options. P also proves that the created ciphertext correspond to the correct vote, by computing a standard signature proof of knowledge *pfk*. How *pfk* is computed exactly can be found in [14]. P also signs the ballot with id_V and sends it to the ballot box. It then waits for a confirmation si_R coming from the latter, which is a hash of the initial encrypted ballot, signed by the receipt generator. After checking this signature, the computer notifies the voter that his vote has been taken into account.

Bulletin Box (B). Receiving an encrypted and signed ballot b from a computer, the ballot box checks first the correctness of signatures and proofs before re-encrypting with a_2 and blinding with s_V the original encrypted ballot, also generating a proof *pfk*$'$, showing that its computation is correct. B then sends the new modified ballot b' to the receipt generator. Once the ballot box receives a message si_R from the receipt generator, it simply checks that the receipt generator's signature is valid, and sends it to the computer.

Receipt generator (R). When receiving an encrypted ballot $b' = (b, \check{x}, \check{w}, \check{p})$ from the ballot box, the receipt generator first checks signature and proofs (from the computer and the ballot box). If the checks are successful, it generates:

- a receipt code $\check{r} = d_V(\check{w}\check{x}^{a_3})$ sent by out-of-band channel directly to the voter. Intuitively, the receipt generator decrypts the (blinded) ballot, applying the permutation function d_V associated to the voter. This gives assurance to the voter that the correct vote was submitted to the bulletin board.

- a signature on a hash of the original encrypted ballot for the ballot box. Once transmitted by the bulletin board, it allows the computer to inform the voter that his vote has been accepted.

2.3 Counting phase

Once the ballot box is closed, the counting phase begins (Figure 2). The ballot box selects the encrypted votes $x_1, \ldots, x_k$ which need to be decrypted (if a voter is re-voting, all the submitted ballots are in the memory of the ballot box and only the last ballot should be sent) and sends them to the decryption service. The whole content of the ballot box $b_1, \ldots, b_n$ $(n \geq k)$ is revealed to the auditor, including previous votes from re-voting voters. The receipt generator sends to the auditor the list of hashes of ballots it has seen during the submission phase. The decryption service decrypts the incoming ciphertexts $x_1, \ldots, x_k$ received from the ballot box and mix the results before outputting them $\mathsf{dec}(x_{\sigma(1)}, a_1), \ldots, \mathsf{dec}(x_{\sigma(k)}, a_1)$ where σ denotes the permutation obtained by shuffling the votes. It also provides the auditor with a proof *pfk* showing that the input ciphertexts and the outcoming decryption indeed match. Using the ballot box content and the list of hashes from the receipt generator, the auditor verifies that no ballots have been inserted or lost and computes his own list of encrypted ballots which should be counted. He compares this list with the one received from the decryption service and verifies the proof given by the latter.

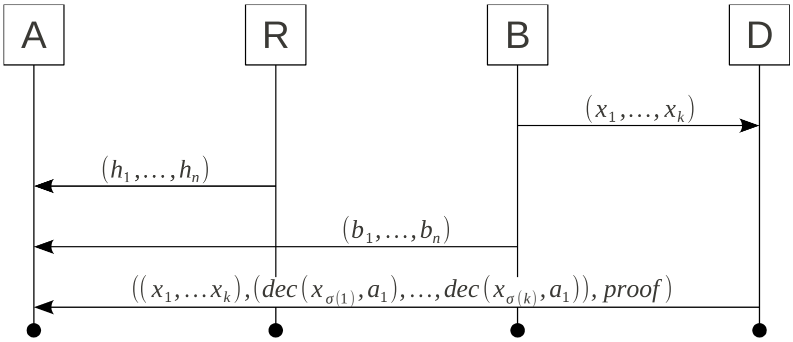

A
R
B
D
$(x_1,\ldots,x_k)$
$(h_1,\ldots,h_n)$
$(b_1,\ldots,b_n)$
$((x_1,\ldots x_k),(dec(x_{\sigma(1)},a_1),\ldots,dec(x_{\sigma(k)},a_1)), proof)$

Figure 2: Counting phase.

3 Applied Pi Calculus

We use the framework of the applied-pi calculus [3] for formally describing the Norwegian protocol. To help with readability, the definitions of the applied-pi calculus are briefly recalled here.

3.1 Terms

As usual, messages are represented by *terms* build upon an infinite set of *names* $\mathcal{N}$ (used to name communication channels or atomic data), a set of *variables* $\mathcal{X}$ and a *signature* Σ consisting of a finite set of *function symbols* which will be used to represent cryptographic primitives. A function symbol f is assumed to be given with its arity $ar(f)$. Then the set of terms $T(\Sigma, \mathcal{X}, \mathcal{N})$ is formally defined by the grammar

$$\begin{array}{ll}
t, t_1, t_2, \ldots ::= & \\
\quad x & x \in \mathcal{X} \\
\quad n & n \in \mathcal{N} \\
\quad f(t_1, \ldots, t_n) & f \in \Sigma, n = ar(f)
\end{array}$$

We write $\{^{M_1}/_{x_1}, \ldots, ^{M_n}/_{x_n}\}$ for the *substitution* that replaces the variables x_i with the terms M_i. $N\sigma$ refers to the result of applying substitution σ to the free variables of term N. A term is called *ground* when it does not contain variables.

In order to represent the properties of the primitives, the signature Σ is equipped with an *equational theory* E that is a set of equations which hold on terms built from the signature. We denote $=_E$ the smallest equivalence relation induced by E, closed under application of function symbols, substitution of terms for variables and bijective renaming of names. We write $M =_E N$ when the equation $M = N$ is in the theory E.

Example 3.1. *A standard signature for representing encryption is* $\Sigma = \{\mathsf{dec}, \mathsf{penc}\}$ *where* penc *represents encryption while* dec *is decryption. Then the property of decryption is modeled by the theory* E_{enc}*, defined by the equation* $\mathsf{dec}(\mathsf{penc}(x, r, \mathsf{pk}(k)), k) = x$.

$P, Q, R ::=$	(plain) processes
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu\, n.P$	name restriction
if ϕ then P else Q	conditional
$u(x).P$	message input
$\overline{u}\langle M\rangle.P$	message output
$A, B, C ::=$	extended processes
P	plain process
$A \mid B$	parallel composition
$\nu\, n.A$	name restriction
$\nu\, x.A$	variable restriction
$\{^{M}/_{x}\}$	active substitution

Figure 3: Syntax for processes

3.2 Processes

Processes and *extended processes* are defined in Figure 3. The process 0 represents the null process that does nothing. $P \mid Q$ denotes the parallel composition of P with Q while $!P$ denotes the unbounded replication of P (*i.e.* the unbounded parallel composition of P with itself). $\nu\, n.P$ creates a fresh name n and the behaves like P. if ϕ then P else Q behaves like P if ϕ holds and like Q otherwise. $u(x).P$ inputs some message in the variable x on channel u and then behaves like P while $\overline{u}\langle M\rangle.P$ outputs M on channel u and then behaves like P. We write $\nu\, \tilde{u}$ for the (possibly empty) series of pairwise-distinct binders $\nu\, u_1. \cdots .\nu\, u_n$. The active substitution $\{^{M}/_{x}\}$ can replace the variable x for the term M in every process it comes into contact with and this behaviour can be controlled by restriction, in particular, the process $\nu\, x\, (\{^{M}/_{x}\} \mid P)$ corresponds exactly to let $x = M$ in P. As in [10], we slightly extend the applied-pi calculus by letting conditional branches now depend on formulae $\phi, \psi ::= M = N \mid M \neq N \mid \phi \wedge \psi$. If M and N are ground, we define $[\![M = N]\!]$ to be true if $M =_E N$ and false otherwise. The semantics of $[\![\ ]\!]$ is then extended to formulae in the standard way.

The *scope* of names and variables are delimited by binders $u(x)$ and $\nu\,(u)$. Sets of bound names, bound variables, free names and free variables are respectively written $\mathrm{bn}(A)$, $\mathrm{bv}(A)$, $\mathrm{fn}(A)$ and $\mathrm{fv}(A)$. Occasionally, we write $\mathrm{fn}(M)$ (respectively $\mathrm{fv}(M)$) for the set of names (respectively variables) which appear in term M. An extended process is *closed* if all its variables are either bound or defined by an active substitution.

An *context* $C[\_]$ is an extended process with a hole instead of an extended process. We obtain $C[A]$ as the result of filling $C[\_]$'s hole with the extended process A. An *evaluation context* is a context whose hole is not in the scope of a replication, a conditional, an input or an output. A context $C[\_]$ closes A when $C[A]$ is closed.

A *frame* is an extended process built up from the null process 0 and active substitutions composed by parallel composition and restriction. The *domain* of a frame φ, denoted $\mathrm{dom}(\varphi)$ is the set of variables for which φ contains an active

$$\begin{array}{lrcl}
\textsc{Par-0} & A & \equiv & A \mid 0 \\
\textsc{Par-A} & A \mid (B \mid C) & \equiv & (A \mid B) \mid C \\
\textsc{Par-C} & A \mid B & \equiv & B \mid A \\
\textsc{Repl} & !P & \equiv & P \mid !P \\
\textsc{New-0} & \nu\, n.0 & \equiv & 0 \\
\textsc{New-C} & \nu\, u.\nu\, w.A & \equiv & \nu\, w.\nu\, u.A \\
\textsc{New-Par} & A \mid \nu\, u.B & \equiv & \nu\, u.(A \mid B) \\
 & & & \text{where } u \notin \mathrm{fv}(A) \cup \mathrm{fn}(A) \\
\textsc{Alias} & \nu\, x.\{^{M}/_{x}\} & \equiv & 0 \\
\textsc{Subst} & \{^{M}/_{x}\} \mid A & \equiv & \{^{M}/_{x}\} \mid A\{^{M}/_{x}\} \\
\textsc{Rewrite} & \{^{M}/_{x}\} & \equiv & \{^{N}/_{x}\} \\
 & & & \text{where } M =_E N
\end{array}$$

Figure 4: Structural equivalence.

substitution $\{^{M}/_{x}\}$ such that x is not under restriction. Every extended process A can be mapped to a frame $\varphi(A)$ by replacing every plain process in A with 0.

3.3 Operational semantics

The operational semantics of processes in the applied pi calculus is defined by three relations : *structural equivalence* ($\equiv$), *internal reduction* ($\rightarrow$) and *labelled reduction* ($\xrightarrow{\alpha}$). These relations are satisfying the rules in Figure 5 and are defined such that :

Structural equivalence is defined in Figure 4. It is closed by α-conversion of both bound names and bound variables, and closed under application of evaluation contexts. The *internal reductions* and *labelled reductions* are defined in Figure 5. They are closed under structural equivalence and application of evaluation contexts. Internal reductions represent evaluation of condition and internal communication between processes. Labelled reductions represent communications with the environment.

3.4 Equivalences

Privacy properties are often stated as equivalence relations [11]. Intuitively, if a protocol preserves ballot secrecy, an attacker should not be able to distinguish between a scenario where a voter votes 0 from a scenario where the voter votes 1. *Static equivalence* formally expresses indistinguishability of sequences of terms.

Definition 1 (Static equivalence)**.** *Two closed frames φ and ψ are statically equivalent, denoted $\varphi \approx_s \psi$, if dom(φ) = dom(ψ) and there exists a set of names $\tilde{n}$ and substitutions σ, τ such that $\varphi \equiv \nu\, \tilde{n}.\sigma$ and $\psi \equiv \nu\, \tilde{n}.\tau$ and for all terms M, N such that $\tilde{n} \cap (fn(M) \cup fn(N)) = \emptyset$, we have $M\sigma =_E N\sigma$ holds if and only if $M\tau =_E N\tau$ holds. Two closed extended processes A, B are statically equivalent, written $A \approx_s B$, if their frames are statically equivalent; that is, $\varphi(A) \approx_s \varphi(B)$.*

Example 3.2. *Consider the signature and equational theory E_{enc} defined in Example 3.1. Let $\varphi_1 = \nu\, k.\sigma_1$ and $\varphi_2 = \nu\, k.\sigma_2$ where $\sigma_1 = \{^{\mathsf{penc}(s_1, r_1, \mathsf{pk}(k))}/_{x_1},\ ^{\mathsf{pk}(k)}/_{x_2}\}$,*

$$\begin{array}{lll}
(\textsc{Comm}) & \overline{c}\langle x\rangle.P \mid c(x).Q \to P \mid Q & \\
(\textsc{Then}) & \text{if } \phi \text{ then } P \text{ else } Q \to P & \text{if } [\![\phi]\!] = \mathsf{true} \\
(\textsc{Else}) & \text{if } \phi \text{ then } P \text{ else } Q \to Q & \text{otherwise}
\end{array}$$

$$\begin{array}{lc}
(\textsc{In}) & c(x).P \xrightarrow{c(M)} P\{^{M}/_{x}\} \\[1em]
(\textsc{Out-Atom}) & \overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P \\[1em]
(\textsc{Open-Atom}) & \dfrac{A \xrightarrow{\overline{c}\langle u\rangle} A' \qquad u \neq c}{\nu\, u.A \xrightarrow{\nu\, u.\overline{c}\langle u\rangle} A'} \\[1em]
(\textsc{Scope}) & \dfrac{A \xrightarrow{\alpha} A' \qquad u \text{ does not occur in } \alpha}{\nu\, u.A \xrightarrow{\alpha} \nu\, u.A'} \\[1em]
(\textsc{Par}) & \dfrac{A \xrightarrow{\alpha} A' \qquad \mathrm{bv}(\alpha) \cap \mathrm{fv}(B) = \mathrm{bn}(\alpha) \cap \mathrm{fn}(B) = \emptyset}{A \mid B \xrightarrow{\alpha} A' \mid B} \\[1em]
(\textsc{Struct}) & \dfrac{A \equiv B \qquad B \xrightarrow{\alpha} B' \qquad B' \equiv A'}{A \xrightarrow{\alpha} A'}
\end{array}$$

where α is a *label* of the form $c(M)$, $\overline{c}\langle u\rangle$, or $\nu\, u.\overline{c}\langle u\rangle$ such that u is either a channel name or a variable of base type.

Figure 5: Semantics for processes

$\sigma_2 = \{^{\mathsf{penc}(s_2,r_2,\mathsf{pk}(k))}/_{x_1},\ ^{\mathsf{pk}(k)}/_{x_2}\}$ *and* s_1, s_2, k *are names. We have that* $\varphi_1 \not\approx_s \varphi_2$. *Indeed, we* $\mathsf{penc}(s_1, r_1, x_2)\sigma_1 =_E x_1\sigma_1$ *but* $\mathsf{penc}(s_1, r_1, x_2)\sigma_2 \neq_E x_1\sigma_2$ *However, we have that* $\nu\, k, r_1.\sigma_1 \approx_s \nu\, k, r_2.\sigma_2$.

Observational equivalence is the active counterpart of static equivalence, where the attacker can actively interact with the processes. The definition of observational equivalence requires to reason about all contexts (*i.e.* all adversaries), which renders the proofs difficult. Since observational equivalence has been shown to coincide [3, 18] with labelled bisimilarity, we adopt the later in this paper.

Definition 2 (Labelled bisimilarity)**.** *Labelled bisimilarity ($\approx_l$) is the largest symmetric relation $\mathcal{R}$ on closed extended processes such that $A\mathcal{R}B$ implies:*

1. $A \approx_s B$;
2. *if* $A \to A'$, *then* $B \to^* B'$ *and* $A'\mathcal{R}B'$ *for some* B';
3. *if* $A \xrightarrow{\alpha} A'$ *such that* $fv(\alpha) \subseteq dom(A)$ *and* $bn(\alpha) \cap fn(B) = \emptyset$, *then* $B \to^* \xrightarrow{\alpha} \to^* B'$ *and* $A'\mathcal{R}B'$ *for some* B'.

Examples of labelled bisimilar processes will be provided in Section 5.

4 Modelling the protocol in applied-pi calculus

We now provide a formal specification of the protocol, using the framework of the applied-pi calculus, defined in the previous section. The first step consists in modeling the cryptographic primitives used by the protocol.

4.1 Equational theory

We adopt the following signature to capture the cryptographic primitives used by the protocol.

$$\Sigma_{sign} = \{\mathsf{Ok}, \mathsf{fst}, \mathsf{hash}, \mathsf{p}, \mathsf{pk}, \mathsf{s}, \mathsf{snd}, \mathsf{vk}, \mathsf{blind}, \mathsf{d}, \mathsf{dec}, +, *, \circ, \diamond, \mathsf{pair}, \\ \mathsf{renc}, \mathsf{sign}, \mathsf{unblind}, \mathsf{checkpfk}_1, \mathsf{checkpfk}_2, \mathsf{checksign}, \mathsf{penc}, \mathsf{pfk}_1, \mathsf{pfk}_2\}$$

with function Ok is a constant ; fst, hash, p, pk, s, snd, vk are unary functions ; blind, d, dec, $+$, $*$, $\circ$, $\diamond$, pair, renc, sign, $\mathsf{unblind}$ are binary functions ; $\mathsf{checkpfk}_1$, $\mathsf{checkpfk}_2$, $\mathsf{checksign}$, penc are ternary functions and pfk_1, pfk_2 are quaternary functions.

The term $\mathsf{pk}(K)$ denotes the public key corresponding to the secret key K in asymmetric encryption. Terms $\mathsf{s}(I)$, $\mathsf{p}(I)$, and $\mathsf{vk}(I)$ are respectively the blinding factor, the parameter and the verification key associated to a secret id I. The specific coding function used by the receipt generator for a voter with secret id I, applied to a message M is represented by $\mathsf{d}(\mathsf{p}(I), M)$. It corresponds to the function $d_I(M)$ explained in Section 2.2. The term $\mathsf{blind}(M, N)$ the message M blinded by N. Unblinded such a blinded term P, using the same blinding factor N is denoted by $\mathsf{unblind}(P, N)$. The term $\mathsf{penc}(M, N, P)$ refers to the encryption of plaintext M using random nonce N and public key P. The term $M \circ N$ denotes the homomorphic combination of ciphertexts M and M' and the corresponding operation on plaintexts is written $P \diamond Q$ and $R * S$ on nonces. The decryption of ciphertext C using secret key K is denoted $\mathsf{dec}(C, K)$. The term $\mathsf{renc}(M, K)$ is the re-encryption of the ciphertext M using a secret key K and leads to another ciphertext of the same plaintext with the same nonce but a different public key. The operation between secret keys is denoted by $K + L$. The term $\mathsf{sign}(M, N)$ refers to the signature of the message M using secret id N. The term $\mathsf{pfk}_1(M, N, P, Q)$ represents a proof of knowledge that proves that Q is a ciphertext on the plaintext P using nonce N. The term $\mathsf{pfk}_2(M, N, P, Q)$ denotes another proof of knowledge proving that Q is either a re-encryption or a masking of a term P using a secret key or nonce N. We introduce tuples using pairings and, for convenience, $\mathsf{pair}(M_1, \mathsf{pair}(\ldots, \mathsf{pair}(M_{n-1}, M_n)))$ is abbreviated as $(M_1, \ldots, M_n)$ and $\mathsf{fst}(\mathsf{snd}^{i-1}(M))$ is denoted Π_i with $i \in \mathbb{N}$.

The properties of the primitives are then modelled by equipping the signature with an equational theory E that asserts functions $+$, $*$, $\circ$ and $\diamond$ are commutative and associative, and includes the equations defined in Figure 6. The three first equations are quite standard. Equation (4) allows to decrypt a blinded ciphertext in order to get the corresponding blinded plaintext. Equation (5) models the homomorphic combination of ciphertexts. Equation (6) represents the re-encryption of a ciphertext. The operation of unblinding is described through Equation (7). Equations (8), (9) and (10) allows respectively the verification of signatures and proofs of knowledge for pfk_1 and pfk_2 proofs.

$$
\begin{aligned}
\mathsf{fst}(\mathsf{pair}(x,y)) &= x \qquad (1)\\
\mathsf{snd}(\mathsf{pair}(x,y)) &= y \qquad (2)\\
\mathsf{dec}(\mathsf{penc}(x_{plain}, x_{rand}, \mathsf{pk}(x_{sk})), x_{sk}) &= x_{plain} \qquad (3)\\
\mathsf{dec}(\mathsf{blind}(\mathsf{penc}(x_{plain}, x_{rand}, \mathsf{pk}(x_{sk})), x_{blind}), x_{sk}) &= \mathsf{blind}(x_{plain}, x_{blind}) \qquad (4)\\
\mathsf{penc}(x_{pl}, x_{rand}, x_{pub}) \circ \mathsf{penc}(y_{pl}, y_{rand}, x_{pub}) &= \\
&\mathsf{penc}(x_{pl} \diamond y_{pl}, x_{rand} * y_{rand}, x_{pub}) \qquad (5)\\
\mathsf{renc}(\mathsf{penc}(x_{plain}, x_{rand}, \mathsf{pk}(x_{sk})), y_{sk}) &= \\
&\mathsf{penc}(x_{plain}, x_{rand}, \mathsf{pk}(x_{sk} + y_{sk})) \qquad (6)\\
\mathsf{unblind}(\mathsf{blind}(x_{plain}, x_{blind}), x_{blind}) &= x_{plain} \qquad (7)\\
\mathsf{checksign}(x_{plain}, \mathsf{vk}(x_{id}), \mathsf{sign}(x_{plain}, x_{id})) &= \mathsf{Ok} \qquad (8)\\
\mathsf{checkpfk}_1(\mathsf{vk}(x_{id}), \mathsf{ball}, \mathsf{pfk}_1(x_{id}, x_{rand}, x_{plain}, \mathsf{ball})) &= \mathsf{Ok}\\
\text{where } \mathsf{ball} = \mathsf{penc}(x_{plain}, x_{rand}, x_{pub})& \qquad (9)\\
\mathsf{checkpfk}_2(\mathsf{vk}(x_{id}), \mathsf{ball}, \mathsf{pfk}_2(x_{id}, x_{bk}, x_{plain}, \mathsf{ball})) &= \mathsf{Ok}\\
\text{where } \mathsf{ball} = \mathsf{renc}(x_{plain}, x_{bk}) \text{ or } \mathsf{ball} &= \mathsf{blind}(x_{plain}, x_{bk}) \qquad (10)
\end{aligned}
$$

Figure 6: Equations for encryption, blinding, signature amd proof of knowledge.

4.2 Norwegian protocol process specification

The description of the processes representing the actors of the protocol makes use of auxiliary checks that are defined in Figure 7. For simplicity, we did not model re-voting.

The voting process V represents both the voter and his computer. It is parametrized by a free variable x_{vote} representing voter's vote and free names c_{auth}, c_{RV} which denote the channel shared with the voter and, respectively, the ballot box and the receipt generator. g_1 is a variable representing the public key of the election, id is the secret id of the voter and idp_R is a variable representing the verification key of the receipt generator. Note that messages sent over c_{auth} and c_{RV} are also sent on the public channel c_{out} to the adversary, to simulate authenticated but not confidential channels.

$$
\begin{aligned}
\phi_{\mathsf{b}}(id_i, x) = [&(\Pi_1(x), \Pi_2(x), \Pi_3(x)) = x\\
&\wedge \mathsf{checksign}((\Pi_1(x), \Pi_2(x)), \mathsf{vk}(id_i), \Pi_3(x)) = \mathsf{Ok}\\
&\wedge\ \mathsf{checkpfk}_1(\mathsf{vk}(id_i), \Pi_1(x), \Pi_2(x)) = \mathsf{Ok}]
\end{aligned}
$$

$$\phi_{\mathsf{s}}(idp_R, x, y) = [\mathsf{checksign}(x, idp_R, y) = \mathsf{Ok}]$$

$$\phi_{\mathsf{v}}(idp_R, id_i, x, y, v, z) = [\mathsf{checksign}(x, idp_R, y) = \mathsf{Ok}\ \wedge\ \mathsf{d}(\mathsf{p}(id_i), \mathsf{blind}(v, \mathsf{s}(id_i))) = z]$$

$$
\begin{aligned}
&(\forall k = 1..3,\ \ x_i^k = \Pi_k(\Pi_1(x)),\ \forall k = 4..7,\ \ x_i^k = \Pi_{k-2}(x))\\
&\phi_{\mathsf{r}}(idp_i, x) = [(x_i^1, x_i^2, x_i^3) = \Pi_1(x) \wedge (\Pi_1(x), x_i^4, x_i^5, x_i^6, x_i^7) = x\\
&\qquad \wedge\ \mathsf{checksign}((x_i^1, x_i^2), idp_i, x_i^3) = \mathsf{Ok} \wedge \mathsf{checkpfk}_1(idp_i, x_i^1, x_i^2) = \mathsf{Ok}\\
&\qquad \wedge\ \mathsf{checkpfk}_2(idp_i, x_i^4, x_i^5) = \mathsf{Ok} \wedge \mathsf{checkpfk}_2(idp_i, x_i^6, x_i^7) = \mathsf{Ok}]
\end{aligned}
$$

Figure 7: Auxiliary checks performed by the participants to the protocol.

```
$V(c_{auth}, c_{out}, c_{RV}, g_1, id, idp_R, x_{vote}) = \nu\, t$ .
    let $e = \mathsf{penc}(x_{vote}, t, g_1)$ in
    let $p = \mathsf{pfk}_1(id, t, x_{vote}, e)$ in
    let $si = \mathsf{sign}((e, p), id)$ in
    $\overline{c_{out}}\langle (e, p, si) \rangle$ .
    $\overline{c_{auth}}\langle (e, p, si) \rangle$ .                    % encrypted ballot sent to B
    $c_{RV}(x)$ . $c_{auth}(y)$ .
    $\overline{c_{out}}\langle x \rangle$ . $\overline{c_{out}}\langle y \rangle$ .
    let $hv = \mathsf{hash}((\mathsf{vk}(id), e, p, si))$ in         % recomputes what should
                                                         be sent by R
    if $\phi_{\mathsf{v}}(idp_R, id, h, x, x_{vote}, y)$ then $\overline{c_{auth}}\langle \mathsf{Ok} \rangle$   % checks validity
```

Process B_n corresponds to the ballot box, ready to listen to n voters. The ballots are coming from authenticated channels $c_1, \ldots, c_n$ and the ballot box can send messages to the receipt generator, the decryption service and the auditor through secure channels c_{BR}, c_{BD} and c_{BA}. The parameters of the ballot box are keys : g_1, g_3 (public) and a_2 (secret); public ids of voters $idp_1, \ldots, idp_n$ (*i.e.* verification keys) and corresponding blinding factors $s_1, \ldots, s_n$. (Step $c(sy_1)$ is a technical synchronisation, it does not appear in the real specification.)

```
$B_n(c_{BR}, c_{BD}, g_1, a_2, g_3, idp_R, c_1, idp_1, s_1, \ldots, c_n, idp_n, s_n) =$
    ... . $c_i(x_i)$ .
    if $\phi_{\mathsf{b}}(idp_i, x_i)$ then                      % checks validity of ballot
    let $e_i = \mathsf{renc}(\Pi_1(x_i), a_2)$ in
    let $pfk_i^e = \mathsf{pfk}_2(idp_i, a_2, \Pi_1(x_i), e_i)$ in
    let $b_i = \mathsf{blind}(e_i, s_i)$ in
    let $pfk_i^b = \mathsf{pfk}_2(idp_i, s_i, e_i, b_i)$ in         % computes re-encrypted masked
                                                    ballot and corresponding proofs.
    $\overline{c_{BR}}\langle (x_i, e_i, pfk_i^e, b_i, pfk_i^b) \rangle . c_{BR}(y_i)$.   % message sent to R
    let $hb_i = \mathsf{hash}((\mathsf{vk}(id_i), \Pi_1(x_i), \Pi_2(x_i), \Pi_3(x_i)))$ in
    if $\phi_{\mathsf{s}}(idp_R, hb_i, y_i)$ then                % checks validity of confirmation
    $\overline{c_i}\langle y_i \rangle$ . $c_i(sy_i)$ ...                   % transmit confirmation to the voter
    $\overline{c_n}\langle y_n \rangle$ . $c_n(sy_n)$ .
    $\overline{c_{BD}}\langle \Pi_1(x_1) \rangle$ . ... . $\overline{c_{BD}}\langle \Pi_1(x_n) \rangle$ .   % output encrypted votes to the
                                                      Decryption Service
    $\overline{c_{BA}}\langle x_1 \rangle$ . ... . $\overline{c_{BA}}\langle x_n \rangle$           % output the content to the Auditor
```

Receipt generator's process is denoted by R_n. It deals with the ballot box and the auditor through secure channels c_{BR} and c_{RA} and directly with voters through out-of-band channels $c_{RV_1}, \ldots, c_{RV_n}$. It is parametrized with keys: g_1, g_2 (public) and a_3 (secret); the public ids of voters and corresponding receipt coding functions parametrized by $pr_1, \ldots, pr_n$.

```
$R_n(c_{BR}, g_1, g_2, a_3, id_R, c_{RV_1}, idp_1, pr_1, \ldots, c_{RV_n}, idp_n, pr_n) =$
    ... . $c_{BR}(x_i)$ .
    let $x_i^k = \Pi_k(\Pi_1(x_i)),\ k = 1..3$ in
    let $x_i^k = \Pi_{k-2}(x_i),\ k = 4...7$ in
    if $\phi_{\mathsf{r}}(idp_i, x_i)$ then                     % checks ballot box's computations
    let $hbr_i = \mathsf{hash}((idp_i, x_i^1, x_i^2, x_i^3))$ in
    let $hbpr_i = \mathsf{hash}((idp_i, x_i^1, x_i^2))$ in
```

$$\begin{array}{ll}
\quad \text{let } r_i = \mathsf{d}(pr_i, \mathsf{dec}(x_i^6, a_3)) \text{ in} & \text{\% computes the receipt code for V}\\
\quad \text{let } sig_i = \mathsf{sign}(hbr_i, id_R) \text{ in} & \text{\% computes confirmation for B}\\
\quad \overline{c_{RV_i}}\langle r_i\rangle \;.\; \overline{c_{BR}}\langle sig_i\rangle \;.\; \ldots & \\
\quad \overline{c_{RV_n}}\langle r_n\rangle \;.\; \overline{c_{BR}}\langle sig_n\rangle \;.\; \ldots & \\
\multicolumn{2}{l}{\quad \overline{c_{RA}}\langle(idp_1, hbpr_1, hbr_1)\rangle \;.\; \ldots \;.\; \overline{c_{RA}}\langle(idp_n, hbpr_n, hbr_n)\rangle}\\
 & \text{\% output content to the Auditor}
\end{array}$$

The decryption service is represented by process D_n. Communicating securely with the ballot box and the auditor through channels c_{BD} and c_{DA}, it also outputs results through public channel c_{out}. In order to decrypt ballots, it needs to know the secret key a_1. We model two processes, one including a swap between the two first votes, to model the shuffling which is necessary to ensure ballot secrecy.

$$\begin{array}{ll}
\multicolumn{2}{l}{D_n(c_{BD}, c_{DA}, c_{out}, a_1) =}\\
\quad c_{BD}(x_1) \;.\; \ldots \;.\; c_{BD}(x_n) \;. & \\
\quad \overline{c_{DA}}\langle \mathsf{hash}((x_1, \ldots, x_n))\rangle \;.\; c_{DA}(x) \;. & \text{\% creating hash of ciphertexts and}\\
 & \quad\text{waiting for auditor's approval}\\
\quad \text{let } dec_k = \mathsf{dec}(x_k, a_1),\; k = 1..n \text{ in} & \text{\% decryption of ciphertexts}\\
\quad \overline{c_{out}}\langle dec_1\rangle \;.\; \ldots \;.\; \overline{c_{out}}\langle dec_n\rangle & \text{\% publication of results}
\end{array}$$

$$\begin{array}{ll}
\multicolumn{2}{l}{\overline{D}_n(c_{BD}, c_{DA}, c_{out}, a_1) =}\\
\quad c_{BD}(x_1) \;.\; \ldots \;.\; c_{BD}(x_n) \;. & \\
\quad \overline{c_{DA}}\langle \mathsf{hash}((x_1, \ldots, x_n))\rangle \;.\; c_{DA}(x) \;. & \\
\quad \text{let } dec_1 = \mathsf{dec}(x_2, a_1) \text{ in} & \text{\% the swap between the two first}\\
\quad \text{let } dec_2 = \mathsf{dec}(x_1, a_1) \text{ in} & \quad\text{votes is modelled here}\\
\quad \text{let } dec_k = \mathsf{dec}(x_k, a_1),\; k = 3..n \text{ in} & \\
\quad \overline{c_{out}}\langle dec_1\rangle \;.\; \ldots \;.\; \overline{c_{out}}\langle dec_n\rangle &
\end{array}$$

Finally, the auditor process, AD_n, communicates with the other infrastructure players using secure channels c_{BA}, c_{RA} and c_{DA}. It knows public ids of voters.

$$\begin{array}{ll}
\multicolumn{2}{l}{AD_n(c_{BA}, c_{RA}, c_{DA}, idp_1, \ldots, idp_n) =}\\
\quad c_{DA}(h_d) \;. & \text{\% input of contents of B, R and D}\\
\multicolumn{2}{l}{\quad c_{BA}(x_1) \;.\; \ldots \;.\; c_{BA}(x_n) \;.\; c_{RA}(h_1) \;.\; \ldots \;.\; c_{RA}(h_1) \;.}\\
\multicolumn{2}{l}{\quad \text{let } hba_i = \mathsf{hash}((\Pi_1(x_i), \Pi_2(x_i), \Pi_3(x_i))) \text{ in}}\\
\multicolumn{2}{l}{\quad \text{let } hbpa_i = \mathsf{hash}((\Pi_1(x_i), \Pi_2(x_i))) \text{ in}}\\
\multicolumn{2}{l}{\quad \text{let } ha = \mathsf{hash}((\Pi_1(x_1), \ldots, \Pi_n(x_n))) \text{ in}}\\
\multicolumn{2}{l}{\quad \text{if } \phi_{\mathsf{a}}(x_1, h_1, idp_1, \ldots, x_n, h_n, idp_n, h, h_d) \text{ then } \overline{c_{DA}}\langle \mathsf{Ok}\rangle \text{ else } 0}\\
 & \text{\% checks and approval sent to D.}
\end{array}$$

where $\phi_{\mathsf{a}}(x_1, h_1, idp_1, \ldots, x_n, h_n, idp_n, h, h_d) = [(\Pi_1(x_i), \Pi_2(x_i), \Pi_3(x_i)) = x_i$
$\quad \wedge(\Pi_1(h_i), \Pi_2(h_i), \Pi_3(h_i)) = h_i \wedge\; \Pi_2(h_i) = hbp_i \wedge \Pi_3(h_i) = hb_i \wedge h_d = h$
$\quad \wedge\; \mathsf{checksign}((\Pi_1(x_i), \Pi_2(x_i)), idp_i, \Pi_3(x_i)) = \mathsf{Ok}]$

The interaction of all the players is simply modelled by considering all the processes in parallel, with the correct instantiation and restriction of the parameters. In what follows, the restricted name a_1, a_2, a_3 model secret keys used in the protocol and public keys $\mathsf{pk}(a_1)$, $\mathsf{pk}(a_2)$ and $\mathsf{pk}(a_3)$ are added in the process frame. The restricted name c_1, c_2 and c_{RV_1}, c_{RV_2} model authentic channels between honest voters and, respectively, the ballot box and the receipt generator. The restricted name id_1, id_2, id_R represent secret ids of honest voters and receipt generator, the corresponding public id's are added in the process's frame.

Then the setting of the authorities is modelled by $A_n\left[\_\right]$ where n is the number of voters and the hole is the voter place. $A_n\left[\_\right]$ is the analogue of $\overline{A}_n\left[\_\right]$ with the Decryption service swapping the two first votes (its use will be clearer in the next section, when defining vote privacy).

$$
\begin{aligned}
\tilde{n} &= (a_1, a_2, id_1, id_2, id_R, c_1, c_2, c_{RV_1}, c_{RV_2}, c_{BR}, c_{BD}, c_{BA}, c_{RA}, c_{DA}) \\
\Gamma &= \{^{\mathsf{pk}(a_1)}/_{g_1},\ ^{\mathsf{pk}(a_2)}/_{g_2},\ ^{\mathsf{pk}(a_3)}/_{g_3},\ ^{\mathsf{vk}(id_1)}/_{idp_1}, \ldots, ^{\mathsf{vk}(id_n)}/_{idp_n},\ ^{\mathsf{vk}(id_R)}/_{idp_R}\} \\
A_n\left[\_\right] &= \nu\,\tilde{n}\ .(\text{let } a_3 = a_1 + a_2 \text{ in } [\_|B_n\{^{\mathsf{s}(id_1)}/_{s_1}, \cdots, ^{\mathsf{s}(id_n)}/_{s_n}\} \\
&\qquad\qquad\qquad\qquad |R_n\{^{\mathsf{p}(id_1)}/_{pr_1}, \cdots, ^{\mathsf{p}(id_n)}/_{pr_n}\}|D_n|AD_n|\Gamma]) \\
\overline{A}_n\left[\_\right] &= \nu\,\tilde{n}\ .(\text{let } a_3 = a_1 + a_2 \text{ in } [\_|B_n\{^{\mathsf{s}(id_1)}/_{s_1}, \cdots, ^{\mathsf{s}(id_n)}/_{s_n}\} \\
&\qquad\qquad\qquad\qquad |R_n\{^{\mathsf{p}(id_1)}/_{pr_1}, \cdots, ^{\mathsf{p}(id_n)}/_{pr_n}\}|\overline{D}_n|AD_n|\Gamma])
\end{aligned}
$$

The frame Γ represents the initial knowledge of the attacker: it has access to the public keys of the authorities and the verification keys of the voters. Moreover, since only the two first voters are assumed to be honest, only their two secret ids are restricted (in $\tilde{n}$). The attacker has therefore access to the secret ids of all the other voters. Parameters of subprocesses are left implicit except for $s_1, \ldots, s_n$ for the ballot box and $pr_1, \ldots, pr_n$ for the receipt generator which are respectively replaced by $\mathsf{s}(id_1), \ldots, \mathsf{s}(id_n)$, the blinding factors, and $\mathsf{p}(id_1), \ldots, \mathsf{p}(id_n)$, used to distinguish the coding dunction associated to a voter.

5 Formal analysis of ballot secrecy

Our analysis shows that the Norwegian e-voting protocol preserves ballot secrecy, even when all but two voters are corrupted, provided that the other components are honest. We also identified several cases of corruption that are subject to attacks. Though not surprising, these cases were not previously mentioned in the literature.

5.1 Ballot secrecy with corrupted voters

Ballot secrecy has been formalized in terms of equivalence by Delaune, Kremer, and Ryan in [11]. A protocol with voting process $V(v, id)$ and authority process A preserves *ballot secrecy* if an attacker cannot distinguish when votes are swapped, *i.e.* it cannot distinguish when a voter a_1 votes v_1 and a_2 votes v_2 from the case where a_1 votes v_2 and a_2 votes v_1. This is formally specified by:

$$
\nu\tilde{n}.(A \mid V\{^{v_2}/_{x}, ^{a_1}/_{y}\} \mid V\{^{v_1}/_{x}, ^{a_2}/_{y}\}) \approx_l \nu\tilde{n}.(A \mid V\{^{v_1}/_{x}, ^{a_1}/_{y}\} \mid V\{^{v_2}/_{x}, ^{a_2}/_{y}\})
$$

We are able to show that the Norwegian protocol preserves ballot secrecy, even all but two voters are corrupted.

Theorem 3. *Let n be the number of voters. The Norwegian e-voting protocol process specification satisfies ballot secrecy with the auditing process, even with $n-2$ voters are corrupted, provided that the other components are honest.*

$$\begin{aligned} &A_n[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\sigma \mid V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\tau] \\ &\qquad\qquad \approx_l \overline{A}_n\,[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\tau | V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\sigma] \end{aligned}$$

where $\sigma = \{^{v_1}/_{x_{vote}}\}$ and $\tau = \{^{v_2}/_{x_{vote}}\}$.

We can also show ballot secrecy, without an auditor. This means that the auditor does not contribute to ballot secrecy in case the administrative components are honest (which was expected). Formally, we define $A'_n\,[\_]$ and $\overline{A}_n\,[\_]'$ to be the analog of $A_n\,[\_]$ and $\overline{A}_n\,[\_]$, removing the auditor.

Theorem 4. *Let n be the number of voters. The Norwegian e-voting protocol process specification satisfies ballot secrecy without the auditing process, even with $n-2$ voters are corrupted, provided that the other components are honest.*

$$\begin{aligned} &A'_n[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\sigma \mid V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\tau] \\ &\qquad\qquad \approx_l \overline{A'}_n\,[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\tau | V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\sigma] \end{aligned}$$

where $\sigma = \{^{v_1}/_{x_{vote}}\}$ and $\tau = \{^{v_2}/_{x_{vote}}\}$.

The proof of Theorems 3 and 4 works in two main steps. First we guess a relation $\mathcal{R}$ such that for any two processes P, Q in relation $(P\mathcal{R}Q)$ any move of P can be matched by a move of Q such that the resulting processes remain in relation. This amounts to characterize all possible successors of $A_n[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\sigma \mid V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\tau]$ and $\overline{A}_n[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\tau$ $|V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\sigma]$. We show in particular that whenever the attacker sends a term N that is accepted by the ballot box for a voter with secret id id, then N is necessarily an id - *valid ballot* for the following definition.

Definition 5. *Let $id \in \{id_1, \ldots, id_n\}$. A term N is said to be a* id - valid ballot *if $\phi_{\mathsf{b}}(id, N) = \mathsf{true}$, equivalently :*

$$\left\{ \begin{array}{rcl} N & = & (N_1, N_2, N_3) \\ \mathsf{checksign}((N_1, N_2), \mathsf{vk}(id), N_3) & =_E & \mathsf{Ok} \\ \mathsf{checkpfk}_1(\mathsf{vk}(id), N_1, N_2) & =_E & \mathsf{Ok} \end{array} \right. .$$

The second and most involved step of the proof consists in showing that the sequences of messages observed by the attacker remain in static equivalence. This requires to prove an infinite number of static equivalences. Let us introduce some notations.

$$\begin{aligned}
\theta_{sub} &= \{^{\mathsf{pk}(a_1)}/_{g_1}\}|\{^{\mathsf{pk}(a_2)}/_{g_2}\}|\{^{\mathsf{pk}(a_3)}/_{g_3}\}|\{^{\mathsf{vk}(id_R)}/_{idp_R}\}|\{^{ball_1}/_{b_1}\}|\{^{ballo_2}/_{b_2}\}| \\
&\quad \{\{^{\mathsf{vk}(id_i)}/_{idp_i}\}|\ i = 1..n\}|\{\{^{\mathsf{d}(\mathsf{p}(id_i),\mathsf{dec}(\mathsf{blind}(\mathsf{renc}(\Pi_1(x_i),a_2),\mathsf{s}(id_i)),a_3))}/_{y_i}\}| \\
&\quad \{^{\mathsf{sign}(\mathsf{hash}((\mathsf{vk}(id_i),x_i)),id_R)}/_{z_i}\}|\ i = 1..n\} \\
\Sigma_L &= \{^{v_1}/_{x^1_{vote}},^{v_2}/_{x^2_{vote}}\} \\
\Sigma_R &= \{^{v_2}/_{x^1_{vote}},^{v_1}/_{x^2_{vote}}\} \\
\theta_{ct} &= \{^{\mathsf{dec}(\Pi_1(x_1),a_1)}/_{result_1},^{\mathsf{dec}(\Pi_1(x_2),a_1)}/_{result_2},^{\mathsf{dec}(\Pi_1(x_i),a_1)}/_{result_i}|i = 3..n\} \\
\overline{\theta}_{ct} &= \{^{\mathsf{dec}(\Pi_1(x_2),a_1)}/_{result_1},^{\mathsf{dec}(\Pi_1(x_1),a_1)}/_{result_2},^{\mathsf{dec}(\Pi_1(x_i),a_1)}/_{result_i}|i = 3..n\}
\end{aligned}$$

where $ball_1$ and $ball_2$ are the terms sent by the two honest voters.

The frame θ_{sub} represents the messages sent over the (public) network during the submission phase. Σ_L represents the scenario where voter 1 votes v_1 and voter 2 votes v_2 while Σ_L represents the opposite scenario. $theta_{ct}$ and $\overline{\theta}_{ct}$ represent the results published by the decryption service.

All voters with secret id id_i with $i \geq 3$ are corrupted. Therefore, the attacker can submit any deducible term as a ballot, that is any term that can be represented by N_i with $\mathrm{fv}(N_i) \subseteq \mathrm{dom}(\theta)\backslash\{y_j, z_j\}_{j\geq i}$ (*i.e.* a recipe that can only re-use previously received messages). We are able to show that whenever the message submitted by the attacker is accepted by the ballot box, then $N_i\theta_i\Sigma$ is necessarily an id_i-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$.

A key result of our proof is that the final frames are in static equivalence, for any behavior of the corrupted users (reflected in the N_i).

Proposition 6. *Let $N_i\theta_i\Sigma$ be id_i-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $i \in \{3, \ldots, n\}$, we have:*

$$\nu\tilde{n}.(\theta_{sub}|\theta_{ct})\sigma_{\tilde{N}}\Sigma_L \approx_s \nu\tilde{n}.(\theta_{sub}|\overline{\theta}_{ct})\sigma_{\tilde{N}}\Sigma_R.$$

where $\sigma_{\tilde{N}} = \{^{ball_1}/_{x_1},\ ^{ball_2}/_{x_2},\ ^{N_j}/_{x_j}|\ j \in \{3, \ldots, n\}\}$.

5.2 Attacks

Our two previous results of ballot secrecy hold provided all the administrative components (bulletin box, receipt generator, decryption service, and auditor) behave honestly. However, in order to enforce the level of trust, the voting system should remain secure even if some administrative components are corrupted. We describe below two cases of corruption where ballot secrecy is no longer guaranteed.

Dishonest decryption service. The decryption service is a very sensitive component since it has access to the decryption key a_1 of the public key used for the election. Therefore, a corrupted decryption service can very easily decrypt all encrypted ballots and thus learns the votes as soon as he has access to the communication between the voters and the bulletin box (these communications being conducted on the *public* Internet network). Even if we did not find any explicit mention of this, we believe that the designers of the protocol implicitly assume that a corrupted decryption would not be able to control (some of) the communication over the Internet. However, a corrupted decryption service can learn the votes even *without access to Internet.* Indeed, the ballots are sent by the bulletin box in the same order they arrived to the bulletin box. Assume for example that the decryption service knows that Alice has voted first (or last). It can then very easily learns her vote when decrypting the first ballot it receives. More generally, provided the decryption service has access to some information on the order of the votes, it then gains some knowledge on the votes.

Dishonest bulletin box and receipt generator. Clearly, if the bulletin box and the receipt generator collude, they can compute $a_1 = a_3 - a_2$ and they can then decrypt all incoming encrypted ballots. More interestingly, a corrupted receipt generator does not need the full cooperation of the bulletin box for breaking ballot secrecy. Indeed, assume that the receipt generator has access, for some voter V, to the blinding factor s_V used by the bulletin to blind the ballot. Recall that the receipt generator retrieves $f(o)^{s_V}$ when generating the receipt codes (by computing $\breve{w}\breve{x}^{-a_3}$). Therefore, the receipt generator can compute $f(o')^{s_V}$ for any possible voting option o'. Comparing with the obtained values with $f(o)^{s_V}$ it would easily deduce the chosen option o. Of course, the more blinding factors the receipt generator can get, the more voters it can attack. Therefore, the security of the protocol strongly relies on the security of the blinding factors which generation and distribution are left unspecified in the documentation. The bulletin box can also perform a similar attack, provided it can learn some coding function d_V and additionally, provided that it has access to the SMS sent by the receipt generator, which is probably a too strong corruption scenario.

6 Further corruption cases using ProVerif

In order to study further corruption cases, we have used ProVerif, the only tool that can analyse equivalence properties in the context of security protocols. Of course, we needed to simplify the equational theory since ProVerif does not handle associative and commutative (AC) symbols and our theory needs four of them. So we have considered the theory E' defined by the equations of Figure 6, except equation (5) that represents homomorphic combination of ciphertexts and we have replaced AC symbols $+$ and $*$ by free function symbols f and g. Using this simplified theory, it is clear that we can miss some attacks, but testing corruption assumptions is still relevant even if the attacker is a bit weaker than in our first study.

As ProVerif is designed to prove equivalences between processes that differ only by terms, we need to use another tool, ProSwapper [15], to model the shuffle done by the decryption service. More precisely, we actually used their algorithm to compute directly a shuffle in our ProVerif specification.

The results are displayed in Table 1 and 2 and have been obtained with a standard (old) laptop[1]. In these tables, ✓ indicates that ballot secrecy is satisfied, × shows that there is an attack, and - indicates that ProVerif was not able to conclude. No indication of times means that we do not proceed to a test in ProVerif but, as we already knew that there was an attack. In particular, all the attacks described in Section 5.2 are displayed in the tables.

Our case study with ProVerif indicates that ballot secrecy is still preserved even when the Receipt Generator is corrupted (as well as several voters), at

[1] 2.00 Ghz processor with 2 GB of RAM Memory

Table 1: Results and computation times for the protocol without auditor.

Corr. Voters Corr. Players	0	1	2	5	10
None	✓ 0.4"	✓ 0.9"	✓ 2.4"	✓ 16.1"	✓ 20'59"
Ballot Box (B)	- >1h				
Receipt Generator (R)	✓ 1.1"	✓ 2.4"	✓ 5.7"	✓ 1'15"	✓ 39'30"
Decryption Service (D)	× 0.2"	×			
B + R	× 0.3"	×			
D+B, D+R, D+R+B	x				

Table 2: Results and computation times for the protocol with auditor.

Corr. Voters Corr. Players	0	1	2	3	4
None	✓ 0.6"	✓ 1,8"	✓ 4.1"	✓ 27.7"	✓ 11'1"
Ballot Box (B)	- >1h				
Receipt Generator (R)	✓ 1.1"	✓ 1.9"	✓ 5.9"	✓ 29.1"	✓ 10'33"
Auditor (A)	✓ 0.4"	✓ 1.9"	✓ 2.6"	✓ 5.8"	✓ 12.1"
R + A	✓ 0.6"	✓ 1.9"	✓ 5.5"	✓ 14.5"	✓ 34.4"
B+R, B+R+A, D D + any other combination	x				

least in the simplified theory. Unfortunately, ProVerif was not able to conclude in the case the Ballot Box is corrupted.

7 Discussion

We have proposed the first formal proof that the e-voting protocol recently used in Norway indeed satisfies ballot secrecy, even when all but two voters are corrupted and even without the auditor. As expected, ballot secrecy is no longer guaranteed if both the bulletin box and the receipt generator are corrupted. Slightly more surprisingly, the protocol is not secure either if the decryption service is corrupted, as discussed in Section 5.2. More cases of corruption need to be studied, in particular when the bulletin board alone is corrupted, we leave this as future work. In addition, it remains to study other security properties such as coercion-resistance or verifiability. Instead of doing additional (long and technical) proofs, a further step consists in developing a procedure for automatically checking for equivalences. Of course, this is a difficult problem. A first decision procedure has been proposed in [9] but is limited to subterm convergent theories. An implementation has recently been proposed [8] but it does not support such a complex equational theory. An alternative step would be to develop a sound procedure that over-approximate the relation, losing completeness in the spirit of ProVerif [6] but tailored to privacy properties.

We would like to emphasize that the security proofs have been conducted in a symbolic thus abstract model. This provides a first level of certification, ruling out "logical" attacks. However, a full computational proof should be developed, identifying in particular the security assumptions.

It is also important to note that the security of the protocol strongly relies on the way initial secrets are pre-distributed. For example, three private decryption keys a_1, a_2, a_3 (such that $a_1 + a_2 = a_3$) need to be securely distributed among (respectively) the bulletin board, the receipt generator and the decryptor. Also, a table $(id, s(id))$ containing the blinding factor for each voter needs to be securely distributed to bulletin board and a table (id, d_{id}) containing a permutation for each voter needs to be securely distributed to the receipt generator. Moreover, anyone with access with both the codes mailed to the voters and to the SMS emitted by the receipt generator would immediately learn the values of all the votes. We did not find in the documentation how and by who all these secret values were distributed. It should certainly be clarified as it could be a weak point of the system.

References

[1] `http://www.dw-world.de/dw/article/0,,4069101,00.html`.

[2] Web page of the norwegian government on the deployment of e-voting. `http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html`.

[3] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. of the 28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115, January 2001.

[4] B. Adida. Helios: Web-based Open-Audit Voting. In *USENIX Security'08: 17th USENIX Security Symposium*, pages 335–348. USENIX Association, 2008.

[5] D. Bernhard, V. Cortier, O. Pereira, B. Smyth, and B. Warinschi. Adapting Helios for provable ballot secrecy. In *ESORICS'11: 16th European Symposium on Research in Computer Security*, LNCS. Springer, 2011. To appear.

[6] B. Blanchet. An automatic security protocol verifier based on resolution theorem proving (invited tutorial). In *20th International Conference on Automated Deduction (CADE-20)*, Tallinn, Estonia, July 2005.

[7] B. Blanchet, M. Abadi, and C. Fournet. Automated verification of selected equivalences for security protocols. In *20th IEEE Symposium on Logic in Computer Science (LICS 2005)*, pages 331–340. IEEE Computer Society, June 2005.

[8] V. Cheval, H. Comon-Lundh, and S. Delaune. Trace equivalence decision: Negative tests and non-determinism. In *18th ACM Conference on Computer and Communications Security (CCS'11)*. ACM Press, Oct. 2011. To appear.

[9] V. Cortier and S. Delaune. A method for proving observational equivalence. In *CSF'09: 22nd Computer Security Foundations Symposium*, pages 266–276. IEEE Computer Society, 2009.

[10] V. Cortier and B. Smyth. Attacking and fixing Helios: An analysis of ballot secrecy. In *CSF'11: 24th Computer Security Foundations Symposium*, pages 297–311. IEEE Computer Society, 2011.

[11] S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, 2009.

[12] A. J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the diebold accuvote-ts voting machine. `http://itpolicy.princeton.edu/voting/`, 2006.

[13] A. Fujioka, T. Okamoto, and K. Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In *AUSCRYPT'92: Workshop on the Theory and Application of Cryptographic Techniques*, volume 718 of *LNCS*, pages 244–251. Springer, 1992.

[14] K. Gjøsteen. Analysis of an internet voting protocol. Cryptology ePrint Archive, Report 2010/380, 2010. `http://eprint.iacr.org/`.

[15] P. Klus, B. Smyth, and M. D. Ryan. ProSwapper: Improved equivalence verifier for ProVerif. `http://www.bensmyth.com/proswapper.php`, 2010.

[16] S. Kremer, M. D. Ryan, and B. Smyth. Election verifiability in electronic voting protocols. In *ESORICS'10: 15th European Symposium on Research in Computer Security*, volume 6345 of *LNCS*, pages 389–404. Springer, 2010.

[17] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing Receipt-Freeness in Mixnet-Based Voting Protocols. In *ICISC'03: 6th International Conference on Information Security and Cryptology*, volume 2971 of *LNCS*, pages 245–258. Springer, 2004.

[18] J. Liu. A Proof of Coincidence of Labeled Bisimilarity and Observational Equivalence in Applied Pi Calculus. `http://lcs.ios.ac.cn/~jliu/papers/LiuJia0608.pdf`, 2011.

[19] T. Okamoto. Receipt-Free Electronic Voting Schemes for Large Scale Elections. In *SP'97: 5th International Workshop on Security Protocols*, volume 1361 of *LNCS*, pages 25–35. Springer, 1998.

[20] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp. Security analysis of india's electronic voting machines. In *Proc. 17th ACM Conference on Computer and Communications Security (CCS 2010)*, Chicago, IL, October 2010.

A Proof of Static equivalence

A.1 Definitions and notations

Definition 7. *Let $N_3, \dots, N_n$ be free terms. We use the following notations, for $n \in \mathbb{N}$, $i \in \{1, 2\}$ and $j \in \{1, \dots, n\}$:*

$$
\begin{array}{llll}
e_i & = \mathsf{penc}(x^i_{vote}, t_i, \mathsf{pk}(a_1)) & \mathit{pfk}_i & = \mathsf{pfk}_1(id_i, t_i, x^i_{vote}, e_i) \\
sig_i & = \mathsf{sign}((e_i, \mathit{pfk}_i), id_i) & ball_i & = (e_i, \mathit{pfk}_i, sig_i) \\
hv_i & = \mathsf{hash}((\mathsf{vk}(id_i), e_i, \mathit{pfk}_i, sig_i)) & s_j & = \mathsf{s}(id_j) \\
e'_j & = \mathsf{renc}(\Pi_1(x_j), a_2) & \mathit{pfk}'_j & = \mathsf{pfk}_2(idp_j, a_2, \Pi_1(x_j), e'_j) \\
e''_j & = \mathsf{blind}(e'_j, s_j) & \mathit{pfk}''_j & = \mathsf{pfk}_2(idp_j, s_j, e'_j, e''_j) \\
ball'_j & = (x_j, e'_j, \mathit{pfk}'_j, e''_j, \mathit{pfk}''_j) & hbb_j & = \mathsf{hash}((idp_j, x_j)) \\
pr_j & = \mathsf{p}(id_j) & r_j & = \mathsf{d}(pr_j, \mathsf{dec}(\Pi_6(p_j), a_3)) \\
hbr_j & = \mathsf{hash}((idp_j, \Pi_1(p_j), \Pi_2(p_j), \Pi_3(p_j))) & sig^R_j & = \mathsf{sign}(hbr_j, id_R) \\
hbpr_j & = \mathsf{hash}((idp_j, \Pi_1(p_j), \Pi_2(p_j))) & dec_j & = \mathsf{dec}(d_j, a_1) \\
\sigma & = \{{}^{v_1}/x^1_{vote}\} & \tau & = \{{}^{v_2}/x^1_{vote}\} \\
\Sigma_L & = \{{}^{v_1}/_{x^1_{vote}}, {}^{v_2}/_{x^2_{vote}}\} & \Sigma_R & = \{{}^{v_2}/_{x^1_{vote}}, {}^{v_1}/_{x^2_{vote}}\}
\end{array}
$$

$$
\begin{array}{ll}
R & = \{{}^{\mathsf{dec}(\Pi_1(x_1), a_1)}/_{result_1}\} | \{{}^{\mathsf{dec}(\Pi_1(x_2), a_1)}/_{result_2}\} \\
\overline{R} & = \{{}^{\mathsf{dec}(\Pi_1(x_2), a_1)}/_{result_1}\} | \{{}^{\mathsf{dec}(\Pi_1(x_1), a_1)}/_{result_2}\} \\
\theta = & \{{}^{\mathsf{pk}(a_1)}/_{g_1}\} | \{{}^{\mathsf{pk}(a_2)}/_{g_2}\} | \{{}^{\mathsf{pk}(a_3)}/_{g_3}\} | \{{}^{\mathsf{vk}(id_R)}/_{idp_R}\} | \{{}^{ballot_1}/_{b_1}\} | \{{}^{ballot_2}/_{b_2}\} | \\
 & \{\{{}^{\mathsf{vk}(id_i)}/_{idp_i}\} |\ i = 1..n\} | \{\{{}^{\mathsf{dec}(\Pi_1(x_i), a_1)}/_{result_i}\} |\ i = 3..n\} | \\
 & \{\{{}^{\mathsf{d}(\mathsf{p}(id_i), \mathsf{dec}(\mathsf{blind}(\mathsf{renc}(\Pi_1(x_i), a_2), \mathsf{s}(id_i)), a_3))}/_{y_i}\} | \\
 & \{{}^{\mathsf{sign}(\mathsf{hash}((\mathsf{vk}(id_i), x_i)), id_R)}/_{z_i}\} |\ i = 1..n\},
\end{array}
$$

Some notation around θ (Note that $\theta^{res}_n = \theta^d$) :

$$
\begin{array}{l}
\theta^d = \{{}^{\mathsf{pk}(a_1)}/_{g_1}\} | \{{}^{\mathsf{pk}(a_2)}/_{g_2}\} | \{{}^{\mathsf{pk}(a_3)}/_{g_3}\} | \{{}^{\mathsf{vk}(id_R)}/_{idp_R}\} | \{\{{}^{\mathsf{penc}(x^{vote}_i, r_i, \mathsf{pk}(a_1))}/_{e_i}\} | \\
\quad \{{}^{\mathsf{pfk}_1(id_i, r_i, x^{vote}_i, e_i)}/_{\mathit{pfk}_i}\} | \{{}^{\mathsf{sign}((e_i, \mathit{pfk}_i), id_i)}/_{sig_i}\} |\ i = 1, 2\} | \\
\quad \{\{{}^{\mathsf{vk}(id_i)}/_{idp_i}\} |\ i = 1..n\} | \{\{{}^{\mathsf{d}(\mathsf{p}(id_i), \mathsf{dec}(\mathsf{blind}(\mathsf{renc}(\Pi_1(x_i), a_2), \mathsf{s}(id_i)), a_3))}/_{y_i}\} | \\
\quad \{{}^{\mathsf{sign}(\mathsf{hash}((\mathsf{vk}(id_i), x_i)), id_R)}/_{z_i}\} |\ i = 1..n\} | \{\{{}^{\mathsf{dec}(\Pi_1(x_i), a_1)}/_{result_i}\} |\ i = 3..n\},
\end{array}
$$

$$
\begin{array}{l}
\theta^d_0 = \{{}^{\mathsf{pk}(a_1)}/_{g_1}\} | \{{}^{\mathsf{pk}(a_2)}/_{g_2}\} | \{{}^{\mathsf{pk}(a_3)}/_{g_3}\} | \{{}^{\mathsf{vk}(id_R)}/_{idp_R}\} | \{\{{}^{\mathsf{penc}(x^{vote}_i, r_i, \mathsf{pk}(a_1))}/_{e_i}\} | \\
\quad \{{}^{\mathsf{pfk}_1(id_i, r_i, x^{vote}_i, e_i)}/_{\mathit{pfk}_i}\} | \{{}^{\mathsf{sign}((e_i, \mathit{pfk}_i), id_i)}/_{sig_i}\} |\ i = 1, 2\} | \\
\quad \{\{{}^{\mathsf{vk}(id_i)}/_{idp_i}\} |\ i = 1..n\},
\end{array}
$$

$$
\begin{aligned}
\theta_1 &= \theta^d_0 \cup \{{}^{\mathsf{d}(\mathsf{p}(id_1), \mathsf{dec}(\mathsf{blind}(\mathsf{renc}(\Pi_1(x_1), a_2), \mathsf{s}(id_1)), a_3))}/_{y_1}\} \\
&\quad \cup \{{}^{\mathsf{sign}(\mathsf{hash}((\mathsf{vk}(id_1), x_1)), id_R)}/_{z_1}\} \\
\theta_i &= \theta_{i-1} \cup \{{}^{\mathsf{d}(\mathsf{p}(id_i), \mathsf{dec}(\mathsf{blind}(\mathsf{renc}(\Pi_1(x_i), a_2), \mathsf{s}(id_i)), a_3))}/_{y_i}\} \\
&\quad \cup \{{}^{\mathsf{sign}(\mathsf{hash}((\mathsf{vk}(id_i), x_i)), id_R)}/_{z_i}\}
\end{aligned}
$$

$$
\begin{aligned}
\theta^{res}_3 &= \theta_n \cup \{{}^{\mathsf{dec}(\Pi_1(x_3), a_1)}/_{result_3}\} \\
\theta^{res}_i &= \theta^{res}_{i-1} \cup \{{}^{\mathsf{dec}(\Pi_1(x_i), a_1)}/_{result_i}\} \text{ for } i = 4..n.
\end{aligned}
$$

Given $N_3, \ldots, N_k$ such that $N_i\theta_i\Sigma$ is an id_i-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $i \in \{3, \ldots, k\}$, we define :

$$\sigma^k_{\tilde{N}} = \{{}^{ballot_1}/_{x_1},\ {}^{ballot_2}/_{x_2},\ {}^{N_j}/_{x_j} |\ j \in \{3, \ldots, k\}\}$$
$$\sigma^n_{\tilde{N}} = \sigma_{\tilde{N}}$$

A.2 Proving static equivalence

Our aim is to prove this proposition :

Proposition 6. *Let $N_i\theta_i\Sigma$ be id_i-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $i \in \{3, \ldots, n\}$, we have:*

$$\nu\tilde{n}.(\theta_{sub}|\theta_{ct})\sigma_{\tilde{N}}\Sigma_L \approx_s \nu\tilde{n}.(\theta_{sub}|\overline{\theta}_{ct})\sigma_{\tilde{N}}\Sigma_R.$$

where $\sigma_{\tilde{N}} = \{{}^{ball_1}/_{x_1},\ {}^{ball_2}/_{x_2},\ {}^{N_j}/_{x_j} |\ j \in \{3, \ldots, n\}\}$.

Since one can see that, with notations defined above, $\theta_{sub}|\theta_{ct} = \theta|R$ and $\theta_{sub}|\overline{\theta}_{ct} = \theta|\overline{R}$, we will prove this proposition which is equivalent :

Proposition 8. *Let $N_i\theta_i\Sigma$ be id_i-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $i \in \{3, \ldots, n\}$, we have :*

$$\nu\tilde{n}.(\theta|R)\sigma_{\tilde{N}}\Sigma_L \approx_s \nu\tilde{n}.(\theta|\overline{R})\sigma_{\tilde{N}}\Sigma_R.$$

Let us introduce useful lemmas in order to do the proof of the proposition 8.

Lemma 9. *Let $\phi = \nu\tilde{n}.\theta$ and $\phi' = \nu\tilde{n}.\theta'$ be frames such that $\theta = \theta' \cup \{{}^{M\theta'}/_y\}$ with free M. Then :*

$$\phi\Sigma_L \approx_s \phi\Sigma_R \Longleftrightarrow \phi'\Sigma_L \approx_s \phi'\Sigma_R.$$

Proof. $\Longrightarrow$ Let N, P be terms such that $(\text{fn}(N) \cup \text{fn}(P)) \cap \tilde{n} = \emptyset$ and $\text{fv}(N) \cup \text{fv}(P) \in \text{dom}(\theta')$. Suppose that $N\theta'\Sigma_L =_E P\theta'\Sigma_L$. We also have $N\theta\Sigma_L =_E P\theta\Sigma_L$ and, since $\phi\Sigma_L \approx_s \phi\Sigma_R$, then $N\theta\Sigma_R =_E P\theta\Sigma_R$. As $\text{fv}(N) \cup \text{fv}(P) \in \text{dom}(\theta')$, we finally have $N\theta'\Sigma_R =_E P\theta'\Sigma_R$.

$\Longleftarrow$ Let N, P be terms such that $(\text{fn}(N) \cup \text{fn}(P)) \cap \tilde{n} = \emptyset$ and $\text{fv}(N) \cup \text{fv}(P) \in \text{dom}(\theta)$. Suppose that $N\theta\Sigma_L =_E P\theta\Sigma_L$. There are two cases :

- If $y \notin \text{fv}(N) \cup \text{fv}(P)$ then we have $N\theta'\Sigma_L =_E P\theta'\Sigma_L$. Since $\phi'\Sigma_L \approx_s \phi'\Sigma_R$, then $N\theta'\Sigma_R =_E P\theta'\Sigma_R$ and, finally, $N\theta\Sigma_R =_E P\theta\Sigma_R$.

- If $y \in \text{fv}(N) \cup \text{fv}(P)$ then, suppose, w.l.o.g. that $y \in \text{fv}(N)$, then $\exists p$ such that $N|_p = y$ and we have $N[M]_p\theta' = N\theta$. Thus, we have : $N\theta\Sigma_L =_E N[M]_p\theta'\Sigma_L =_E P\theta'\Sigma_L =_E P\theta\Sigma_L$. ($y \notin \text{fv}(P)$ otherwise we substitute all y by M in P as done in N.) Using the fact that $\phi'\Sigma_L \approx_s \phi'\Sigma_R$, we have $N[M]_p\theta'\Sigma_R =_E P\theta'\Sigma_R$ and, finally, $N\theta\Sigma_R =_E P\theta\Sigma_R$.

□

Lemma 10. *Let $\phi_2 = \nu\tilde{n}.\theta_2$. Then, we have :*

$$\phi_2\sigma^2_{\tilde{N}}\Sigma_L \approx_s \phi_2\sigma^2_{\tilde{N}}\Sigma_R.$$

Proof. Note that the adversary can arbitrarily combine ciphertexts from the frame with ciphertexts in the frame or freshly constructed ciphertexts, thus we enrich the frame ϕ^{dev} with any such combination of ciphertexts. Formally, for any $\alpha_1, \alpha_2 \in \mathbb{N}$ and free terms K, P, R, we define $C_{\alpha_1,\alpha_2,K,P,R}$ as follows :

$$\mathsf{penc}(P \diamond_{i=1}^{2} \alpha_i.x_i^{vote}, R *_{i=1}^{2} r_i^{\alpha_i}, \mathsf{pk}(a_1^{\delta'(\alpha_1,\alpha_2)} + K))$$

with $\delta'(a,b) = 0$ if $a = b = 0$ and $\delta'(a,b) = 1$ otherwise, $a_1^0 = \epsilon$, the null term, and $a_1^1 = a_1$. We define the extended frame ϕ_e below.

$$\begin{aligned}\phi_e =& \nu\tilde{n}.(\theta_2^d | \{^{C_{\alpha_1,\alpha_2,K,P,R}}/_{x_{\alpha_1,\alpha_2,K,P,R}} \mid \alpha_1, \alpha_2 \in \mathbb{N} \text{ and terms } K, P, R \text{ such that} \\ & (\mathrm{fn}(K) \cup \mathrm{fn}(P) \cup \mathrm{fn}(R)) \cap \tilde{n} = \emptyset,\ \mathrm{fv}(K,P,R) \subseteq \mathrm{dom}(\phi_e).\})\end{aligned}$$

Note that ϕ_e is infinite. Using Lemma 9, it is sufficient to show $\phi_e\Sigma_L \approx_s \phi_e\Sigma_R$. We introduce the following two claims.

Claim 1. *Let M be a term such that fv$(M) \subseteq$ dom$(\phi_e) = \emptyset$ and fn$(M) \cap \tilde{n} = \emptyset$. If $M\phi_e\Sigma \longrightarrow U$ for some $\Sigma \in \{\Sigma_L, \Sigma_R\}$, then there exists N such that $U =_{AC} N\phi_e\Sigma$ and $M\phi_e\Sigma' \longrightarrow N\phi_e\Sigma'$ for any $\Sigma' \in \{\Sigma_L, \Sigma_R\}$.*

Claim 2. *Let M, N be two terms such that (fv$(M) \cup$ fv$(N)) \subseteq$ dom$(\phi_e) = \emptyset$ and fn$(M, N) \cap \tilde{n} = \emptyset$. If $M\phi_e\Sigma =_{AC} N\phi_e\Sigma$ for some $\Sigma \in \{\Sigma_L, \Sigma_R\}$, then $M\phi_e =_{AC} N\phi_e$.*

The above claims allow the construction of our proof. Let M, N be two terms such that $\mathrm{fn}(M,N) \cap \tilde{n} = \emptyset$, $\mathrm{fv}(M,N) \subseteq \mathrm{dom}(\phi_e)$ and $M\phi_e\Sigma_L =_E N\phi_e\Sigma_L$. Thus $(M\phi_e\Sigma_L){\downarrow} =_{AC} (N\phi_e\Sigma_L){\downarrow}$. Applying repeatedly Claim 1, we deduce that there exists M' such that $(M\phi_e\Sigma_L){\downarrow} =_{AC} M'\phi_e\Sigma_L$ and $M\phi_e\Sigma_R \longrightarrow^* M'\phi_e\Sigma_R$. Similarly, there exists N' such that $(N\phi_e\Sigma_L){\downarrow} =_{AC} N'\phi_e\Sigma_L$ and $N\phi_e\Sigma_R \longrightarrow^* N'\phi_e\Sigma_R$. From $M'\phi_e\Sigma_L =_{AC} N'\phi_e\Sigma_L$ and Claim 2, we deduce $M'\phi_e =_{AC} N'\phi_e$. Therefore, $M'\phi_e\Sigma_R =_{AC} N'\phi_e\Sigma_R$ and thus $M\phi_e\Sigma_R =_E N\phi_e\Sigma_R$.

Proof of Claim 1 : This result is proved by inspection of the rewrite rules. More precisely, assume that $M\phi_e\Sigma \longrightarrow U$ for some $\Sigma \in \{\Sigma_L, \Sigma_R\}$. It means that there exists a rewriting rule $l \longrightarrow r \in \mathcal{R}_E$ and a position p such that $M\phi_e\Sigma|_p =_{AC} l\theta$ for some θ. p cannot occur below M since $\phi_e\Sigma$ is in normal form. If $M|_p = l\theta'$ for some θ' then we conclude that we can rewrite M as expected. The only interesting case is thus when $M|_p$ is not an instance of l but $M\phi_e\Sigma|_p$ is. By inspection of the rules, $l \longrightarrow r$ can only correspond to one of the five equations (3), (4), (5), (6) and (7). The case of equations (3) or (4) is ruled out by the fact that a_1 is not deducible from $\phi_e\Sigma$. This is the same for the case of equation (7) since id_i are not deducible from $\phi_e\Sigma$. If the rule is corresponding to (5), then it must be the case that $M|_p = x \circ y$ with x, y variables of $\mathrm{dom}(\phi_e)$. By construction of ϕ_e, we have that $(x \circ y)\phi_e \to z\phi_e$ (applying the rule corresponding to Equation (5)), thus the result. The last case is when the rule is corresponding to Equation (6). This must be the case that $M|_p = \mathsf{renc}(x, K)$ with $x \in \mathrm{dom}(\phi_e)$ and K a term such that $\mathrm{fn}(K) \cap \tilde{n} = \emptyset$ and $\mathrm{fv}(K) \subseteq \mathrm{dom}(\phi_e)$. By construction of ϕ_e, we have that $\mathsf{renc}(x, K) \to y\phi_e$ and we have the result.

Proof of Claim 2 : Assume by contradiction that there exist M, N two terms such that $M\phi_e\Sigma =_{AC} N\phi_e\Sigma$ for some $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $M\phi_e \neq_{AC}$

$N\phi_e$. Consider M, N two minimal terms that satisfy this property. By case inspection, it must be the case that M and N are both variables. Thus, we have $x\phi_e\Sigma =_{AC} y\phi_e\Sigma$ and $x\phi_e \neq_{AC} y\phi_e$ with $x, y \in \mathrm{dom}(\phi_e)$ and $x \neq y$. Then, we have $head(x\phi_e\Sigma) \in \{\mathsf{blind}, \mathsf{penc}, \mathsf{pfk}_1, \mathsf{sign}\}$. But, by construction of ϕ_e, Σ does not change the randomness used in penc or in pfk_1 and the secret ids in blind or sign, thus, randomness or id uniquely determine the variable, which implies $x = y$, contradiction. □

Lemma 11. *We have :*

- $\nu\tilde{n}.\theta \nvdash a_i + U$*, for* $i = 1, 3$ *and any term* U*.*
- $\nu\tilde{n}.\theta \nvdash r_i * U$*, for* $i = 1, 2$ *and any term* U*.*
- $\nu\tilde{n}.\theta \nvdash id_i$*, for* $i = 1, 2$*.*
- $\nu\tilde{n}.\theta \nvdash \mathsf{p}(id_i)$*, for* $i = 1, 2$*.*

Proof. We define four properties :

1. Let N be a deducible term such that $\exists\ p$ such that $N|_p = a_i + U$ for $i \in \{1, 2, 3\}$ and any term U. There are two cases :
   - $U = \epsilon$ $(a_i + \epsilon = a_i)$ and $p = p'.2$ such that $N|_{p'} = f(N', a_i)$ with $f \in \{\mathsf{dec}, \mathsf{renc}\}$.
   - $p = p'.1.q$ such that $N|_{p'} =_{AC} \mathsf{pk}(a_i + U')$ for some U' and $\forall\ q' < q$, $head(N|_{p'.1.q'}) = +$.
2. Let N be a deducible term such that $\exists\ p$ such that $N|_p = r_i * U$ for $i \in \{1, 2\}$ and any term U. There are two cases :
   - $p = p'.2.q$ such that $N|_{p'} =_{AC} \mathsf{penc}(P_1, r_i * U, K_1)$ and $\forall\ q' < q$, $head(N|_{p'.2.q'}) = *$.
   - $p = p'.2.q$ such that $N|_{p'} =_{AC} \mathsf{pfk}_1(P_1, r_i * U, P_2, P_3)$ and $\forall\ q' < q$, $head(N|_{p'.2.q'}) = *$.
3. Let N be a deducible term such that $\exists\, p$ such that $N|_p = id_i$ for $i \in \{1, 2\}$. There are four cases :
   - $p = p'.1$ and $N|_{p'} = \mathsf{vk}(id_i)$.
   - $p = p'.1$ and $N|_{p'} = \mathsf{p}(id_i)$.
   - $p = p'.1$ and $N|_{p'} = \mathsf{s}(id_i)$.
   - $p = p'.1$ and $N|_{p'} = \mathsf{pfk}_1(id_i, P_1, P_2, P_3)$.
   - $p = p'.2$ and $N|_{p'} = \mathsf{sign}(N', id_i)$.
4. Let N be a deducible term such that $\exists\ p$ such that $N|_p = \mathsf{p}(id_i)$ for $i \in \{1, 2\}$. Then, $p = p'.1$ and $N|_{p'} = \mathsf{d}(\mathsf{p}(id_i), M)$.

We can see that these properties imply the undeducibility of $a_i + U$, $r_i * U$, id_i and $\mathsf{p}(id_i)$. Let us prove these properties by induction on the number of steps needed to deduce N.

Base Case : All terms in the frame θ verify these properties.

Induction Hypothesis : Let $M_1, \ldots, M_k$ be terms in normal form, deducible in $i-1$ steps verifying the properties. We are going to prove that $f(M_1, \ldots, M_k)\!\downarrow$ also verifies them. There are two main cases :

- If $f(M_1, \ldots, M_k)$ is in normal form, then it is obvious that the result is true.

- If it is not in normal form, then, since $M_1, \ldots, M_k$ are in normal form, the reduction occurs in head.

  - If the applied rule is different from (4), (5) and (6), then the result is a subterm of $M_1, \ldots, M_k$ and it is verifying the properties, using the induction hypothesis.

  - If the rule (4) is applied, then $\mathsf{dec}(M_1, M_2) \longrightarrow \mathsf{blind}(T_1, T_2)$ with T_1 and T_2 subterms of M_1, M_2 and are verifying the property by induction hypothesis. Then, $\mathsf{blind}(T_1, T_2)$ verify the properties.

  - If the rule (5) is applied, then $\circ(M_1, M_2) \longrightarrow \mathsf{penc}(T_1 \circ T_2, R_1 * R_2, P)$ with T_1, T_2, R_1, R_2, P subterms of M_1, M_2. The result may be not in normal form if $\mathit{head}(T_1) = \mathit{head}(T_2) = \mathsf{penc}$ and if encryptions use the same key, then the rule (5) is applied again. It can be applied several time, but the reduction will stop since M_1 and M_2 are terms with fixed length. Then the result will be of the form $\mathsf{penc}(\ldots \mathsf{penc}(T'_1 \circ T'_2, R'_1 * R'_2, P') \ldots, R_1 * R_2, P)$ where all terms are subterms of M_1 and M_2. Then, each penc, in normal form, will verify the properties. Thus, the result, in normal form, is verifying the properties too.

  - Finally, if the rule (6) is applied, then $\mathsf{renc}(M_1, M_2) \longrightarrow \mathsf{penc}(T, R, \mathsf{pk}(P_1 + P_2))$ with T, R, P_1 and P_2 subterms of M_1 and M_2. Thanks to the induction hypothesis, we can see that the the result is satisfying the property. Indeed, whatever the case where a_i is a subterm of P_1 or P_2, $\exists\ P'$ such that $P_1 + P_2 =_{AC} a_i + P'$.

□

Note. *If, $\forall\ U$, $r_i * U$ and $a_i + U$ are not deducible, then using $U = \epsilon$ such that $r_i * U = r_i$ or $a_i + U = a_i$, we have that r_i and a_i are not deducible too.*

Lemma 12. *Let $\phi = \nu\tilde{n}.\overline{\theta_n}$ and N a minimal recipe of $(N\phi)\!\downarrow$ such that $N = f(N_1, \ldots, N_k)$ with $f \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$. Then :*

$$(N\phi)\!\downarrow = f((N_1\phi)\!\downarrow, \ldots, (N_k\phi)\!\downarrow)$$

Proof. Let us prove this by induction on the depth of N.

Base Case : $N = f(N_1, \dots, N_k)$ with N_1, …, N_k variables or names.

- If $f \in \{\mathsf{fst}, \mathsf{snd}\}$, since $\nexists\ x \in \mathrm{dom}(\phi)$ such that $head(x\phi) = \mathsf{pair}$, we conclude immediately.
- If $f = \mathsf{dec}$ and $N = \mathsf{dec}(N_1, N_2)$, then $N_1 \in \{e_1, e_2\}$ but if there is a reduction, it means that we have $N_2\phi = a_1$ which is impossible as a_1 is not deducible by Lemma 11.
- If $f = \mathsf{unblind}$ and $N = \mathsf{unblind}(N_1, N_2)$, then $N_1 \in \{y_1, y_2\}$ since y_k which are reducing are removing from the frame. But if there is a reduction, it means that we have $N_2\phi = id_i$ which is impossible as id_i are not deducible by Lemma 11.

Induction Hypothesis : We suppose that $\forall$ term M with a depth ≥ 1 satisfies the property. Let $N = f(N_1, \dots, N_k)$ of a depth equal to $n+1$ with N_i of depths $\leq n$. If $f((N_1\phi){\downarrow}, \dots, (N_k\phi){\downarrow}$ is in normal form, we conclude easily. Suppose that $f((N_1\phi){\downarrow}, \dots, (N_k\phi){\downarrow}$ is not in normal form.

- If $f \in \{\mathsf{fst}, \mathsf{snd}\}$ and $N = f(N_1)$. The case where N_1 is a variable is excluded. Then $N_1 = g(N'_1, \dots, N'_k)$ with $g \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{pair}, \mathsf{snd}, \mathsf{unblind}\}$.
  - If $g \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, using the induction hypothesis, we have $(N_1\phi){\downarrow} = g((N'_1\phi){\downarrow}, \dots, (N'_k\phi){\downarrow})$ and, thus, $(N\phi){\downarrow} = f((N_1\phi){\downarrow})$.
  - If $g = \mathsf{pair}$ we have a contradiction with the minimality of N.
- If $f = \mathsf{dec}$ and $N = \mathsf{dec}(N_1, N_2)$. The case where N_1 is a variable is excluded. Then $N_1 = g(N'_1, \dots, N'_k)$ with $g \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{penc}, \mathsf{renc}, \mathsf{snd}, \mathsf{unblind}, \circ\}$.
  - If $g \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, we conclude thanks to the induction hypothesis.
  - If $g = \mathsf{penc}$, there is a contradiction with the minimality of N.
  - Finally, the case when $g \in \{\mathsf{renc}, \circ\}$. We can have a finite (since depths are finite) sequence of $\mathsf{renc}(\circ(\mathsf{renc}(\circ(\dots))))$ or $\circ(\mathsf{renc}(\circ(\dots)))$. But if there is a reduction with the dec function, then we must have $N_1\phi =_E \mathsf{penc}(W_1, W_2, \mathsf{pk}(W_3))$ with $W_3 =_E N_2\phi$. Moreover, N_2 is deducible, then $\mathsf{pk}(W_3)$ is also deducible and can not contain a_i. Since there is no variable in the frame referring to such a key, it must come from one (or two in the case of a sequence finishing by $\circ$) $\mathsf{penc}(P_1, P_2, \mathsf{pk}(P_3))$ subterm of N_1, a contradiction with the minimality of N.
- If $f = \mathsf{unblind}$ and $N = \mathsf{unblind}(N_1, N_2)$. The case where N_1 is a variable is excluded. Then $N_1 = g(N'_1, \dots, N'_k)$ with $g \in \{\mathsf{blind}, \mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$.
  - If $g \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, we conclude thanks to the induction hypothesis.
  - If $g = \mathsf{blind}$, there is a contradiction with the minimality of N.

□

Definition 13. *Let $|.|$ be a measure of the length of a term M such that :*

- $|u| = 1$ *for u a constant,*
- $|f(u_1, \dots, u_n)| = \sum |u_i|$ *for all $f \in \{+, *, \circ, \diamond\}$.*
- $|f(u_1, \dots, u_n)| = 1 + \sum |u_i|$ *otherwise.*

We define another measure L which is defined as $L(M) = (\#(M), |M|)$ with $\#(M)$ the number of symbols $\circ$ under renc or penc symbols.

Lemma 14. *Let $k \geq 3$, $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ be an id_k-valid ballot. We suppose that $\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \approx_s \theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$. Then, we have, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$:*

- $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E (M, N, P)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma$ *with free M, N, P.*
- $N\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{pfk}_1(id_k, N_1, N_2, N_3)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma$ *with free N_1, N_2, N_3.*
- $M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{penc}(N_2, N_1, U)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma$ *with free U or $U = \mathsf{pk}(a_i + U')$ with free U' and $a_i \in \{a_1, a_2, a_3\}$.*

Proof. Let $k \in \{3, \dots, n\}$. Let N_k such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ is a id$_k$-valid ballot. Let N'_k minimal in size - according to the measure of length L defined in Definition 13 - such that :

$$N'_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \qquad (\star)$$

Using Definition 5, we have $N'_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L = (N_1, N_2, N_3)$.

- Let suppose that N'_k is a variable. Since $\nexists\ x \in \mathrm{dom}(\theta_{k-1})$ such that $x\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\ \Sigma_L$ is a id$_k$-valid ballot, there is a contradiction.
- Thus, $N'_k = f(P_1, \dots, P_m)$ with $f \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{pair}, \mathsf{snd}, \mathsf{unblind}\}$ since only equations (1), (2), (3) and (7) can lead to (N_1, N_2, N_3).
  - If $f \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, using Lemma 12, we have a contradiction with the fact that $head(N'_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L) = \mathsf{pair}$.
  - If $f = \mathsf{pair}$, then $N'_k = (M, N, P)$, with some free M, N, P. Thus we have :

    $$N'_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E (M, N, P)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L.$$

    Since $(N_k =_E (M, N, P))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ and $\phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \approx_s \phi_{k-1}\sigma_{\tilde{N}}^{k-1}$ Σ_R, we have $(N_k =_E (M, N, P))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$. Thus, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$, we have :

    $$N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E (M, N, P)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$

Moreover, Definition 5 gives us now that $N\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E \mathsf{pfk}_1(id_k, P_1, P_2, P_3)$.

- N cannot be a variable since there is no $x \in \mathrm{dom}(\theta_{k-1})$ such that $x\theta_{k-1}\sigma_{\tilde{N}}^{k-1}$ $\Sigma_L = \mathsf{pfk}_1(id_k, P_1, P_2, P_3)$.
- Thus, $N = f(N_1, \ldots, N_p)$ with $f \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{pfk}_1, \mathsf{snd}, \mathsf{unblind}\}$ since only equations (1), (2), (3) and (7) can lead to $\mathsf{pfk}_1(id_k, P_1, P_2, P_3)$.
  - If $f \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, using Lemma 12, we have a contradiction with the fact that $head(N\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L) = \mathsf{pfk}_1$.
  - If $f = \mathsf{pfk}_1$, then $N = \mathsf{pfk}_1(id_3, N_1, N_2, N_3)$, with some free N_1, N_2, N_3. Since $(N =_E \mathsf{pfk}_1(id_3, N_1, N_2, N_3))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ and $\phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ $\approx_s \phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$, we have $(N =_E \mathsf{pfk}_1(id_3, N_1, N_2, N_3))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$. Thus, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$, we have :
  $$N\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{pfk}_1(id_3, N_1, N_2, N_3)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$

Finally, Definition 5 gives us that $M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E \mathsf{penc}(N_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L, N_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L, U)$ for some term U.

- If M is a variable, then $M \in \{e_1, e_2\}$. In that case, we would have $N_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}$ $\Sigma_L =_E r_1$ (or r_2) with free N_1 which would mean that r_1 (or r_2) is deducible which is in contradiction with Lemma 11.
- Thus, $M = f(N_1, \ldots, N_p)$ with $f \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{penc}, \mathsf{renc}, \mathsf{snd}, \mathsf{unblind}, \circ\}$ since only equations (1) to (3) and (5) to (7) can lead to $\mathsf{penc}(P_1, P_2, P_3)$.
  - If $f \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, using Lemma 12, we have a contradiction with the fact that $head(M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L) = \mathsf{penc}$.
  - If $f = \mathsf{renc}$ i.e. $M = \mathsf{renc}(M_1, M_2)$. The case where M_1 is a variable is excluded thanks to the fact that r_i is not deducible. Then $M_1 = g(M_1', \ldots, M_p')$ with $g \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{penc}, \mathsf{renc}, \mathsf{unblind}, \circ\}$ since $head(M_1\theta_{k-1}\ \sigma_{\tilde{N}}^{k-1}\Sigma_L) = \mathsf{penc}$.
    - ∗ If $g \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, using Lemma 12, we have a contradiction with the fact that $head(M_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L) = \mathsf{penc}$.
    - ∗ If $g = \mathsf{renc}$ and $M_1 = \mathsf{renc}(M_1', M_2')$, we have a contradiction with the minimality of M since $\mathsf{renc}(M_1', M_2' + M_2)$ is a smaller recipe than $\mathsf{renc}(\mathsf{renc}(M_1', M_2'), M_2)$.
    - ∗ If $g = \circ$ and $M_1 = M_1' \circ M_2'$, we also have a contradiction with the minimality of M since $\mathsf{renc}(M_1', M_2) \circ \mathsf{renc}(M_2', M_2)$ is a smaller recipe according to the Definition 13 of the measure L.
    - ∗ If $g = \mathsf{penc}$ and $M_1 = \mathsf{penc}(M_1', M_2', M_3')$. We have two cases :

- If M'_3 is a variable, then $M'_3 \in \{g_1, g_2, g_3\}$ and we have $M = \mathsf{renc}(\mathsf{penc}(M'_1, M'_2, g_i), M_2)$ with free M'_1, M'_2 and M_2. In that case, we have :
$$\begin{aligned} M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L &=_E \mathsf{renc}(\mathsf{penc}(M'_1, M'_2, g_i), M_2)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \ (\dagger) \\ &=_E \mathsf{penc}(M'_1, M'_2, \mathsf{pk}(a_i + M_2))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \end{aligned}$$
Thanks to the fact that $\phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \approx_s \phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$ and $(\dagger)$, we also have that :
$$\begin{aligned} M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R &=_E \mathsf{renc}(\mathsf{penc}(M'_1, M'_2, g_i), M_2)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R \\ &=_E \mathsf{penc}(M'_1, M'_2, \mathsf{pk}(a_i + M_2))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R \end{aligned}$$
Then, we have, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$:
$$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{penc}(M'_1, M'_2, \mathsf{pk}(a_i + M_2))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$
Moreover, since $M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E \mathsf{penc}(N_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L, N_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L, U)$ we have that $M'_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E N_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ and $M'_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E N_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$. Using the fact that $\phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \approx_s \phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$, these equalities hold with Σ_R. Finally, we have, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$:
$$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{penc}(N_2, N_1, \mathsf{pk}(a_i + M_2))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$
- If $M'_3 = h(M''_1, \dots, M''_q)$ with $h \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{pk}, \mathsf{snd}, \mathsf{unblind}\}$, we can conclude easily with a contradiction when $h \neq \mathsf{pk}$ according to Lemma 12. If $h = \mathsf{pk}$ then we have a contradiction with the minimality of M since $\mathsf{penc}(M'_1, M'_2, \mathsf{pk}(M''_1 + M_2))$ is smaller than $\mathsf{renc}(\mathsf{penc}(M''_1, M''_2, \mathsf{pk}(M''_3)), M_2)$.

– If $f = \mathsf{penc}$ i.e. $M = \mathsf{penc}(M_1, M_2, M_3)$ with free M_1, M_2, M_3, we immediately conclude that, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$:
$$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{penc}(M_1, M_2, M_3)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$
Using the fact that $M_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E N_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma$ and $M_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E N_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma$, we have, with free M_3 and $\Sigma \in \{\Sigma_L, \Sigma_R\}$:
$$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{penc}(N_2, N_1, M_3)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$

– If $f = \circ$ i.e. $M = M_1 \circ M_2$. The case where M_1 or M_2 is a variable is excluded thanks to the fact that r_i is not deducible. Then $M_1 = h_1(M'_1, \dots, M'_p)$ and $M_2 = h_2(M''_1, \dots, M''_q)$ with $h_i \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{penc}, \mathsf{renc}, \ \mathsf{unblind}, \circ\}$ since $\mathit{head}(M_i\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L) = \mathsf{penc}$ for $i = 1, 2$.

  ∗ If $\exists\ i$ such that $h_i \in \{\mathsf{dec}, \mathsf{fst}, \mathsf{snd}, \mathsf{unblind}\}$, we have a contradiction using Lemma 12.

- $*$ If $h_1, h_2 = \mathsf{penc}$, we have $M_1 = \mathsf{penc}(M_1', M_2', K)$ and $M_2 = \mathsf{penc}(M_1'', M_2'', K')$ with K and K' such that $K\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E K'\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ which is in contradiction with the minimality of M since $\mathsf{penc}(M_1' \diamond M_1'', M_2' * M_2'', K)$ is a smaller recipe than $\mathsf{penc}(M_1', M_2', K) \circ \mathsf{penc}(M_1'', M_2'', K')$.
- $*$ If $h_1 \in \{\mathsf{renc}, \circ\}$ and $h_2 \in \{\mathsf{penc}, \mathsf{renc}, \circ\}$. If $h_1 = \mathsf{renc}$ and $M_1 = \mathsf{renc}(M_1', M_2')$, we can apply the same discussion on h_1 we did on f when $f = \mathsf{renc}$ in a previous case. According to this, the only possible case is when $M_1' = \mathsf{penc}(M_1'', M_2'', M_3'')$. If $g_1 = \circ$ and $M_1 = M_1' \circ M_2'$, we have an iteration of the current subcase. But these iterations must stop since M is not of an unlimited length and, thanks to the contradiction of minimality in some cases, the remaining global case is when $M = \circ_{i=1}^{n} \mathsf{renc}(P_i, Q_i) \circ M'$ with M' a null term or $\mathsf{penc}(M_1', M_2', M_3')$ and $P_i = \mathsf{penc}(M_1^i, M_2^i, M_3^i)$ with M_3^i variable, using the discussion on renc case.

Suppose that $M' = \mathsf{penc}(M_1', M_2', M_3')$, then $M_3'\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ is deducible. In order for M to be reduced, we must have the same keys in both M' and $\circ_{i=1}^{n}\mathsf{renc}(P_i, Q_i)$. But since M_3^i is a variable, $M_3^i \in \{g_1, g_2, g_3\}$, the resulting key of re-encryption is not deducible, according to Lemma 11. Indeed, the resulting key is like $\mathsf{pk}(\alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 + U)$ with some integers α_i and a deducible term U (we using the notation that $a_i + a_i = 2a_i$) and since there are no variable leading to such a key, we must have $M_3' = \mathsf{pk}(\alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 + U)$ which is not possible. Then, we must have $M' = \epsilon$.

Thus, we have $M = \circ_{i=1}^{n}\mathsf{renc}(P_i, Q_i)$ with $P_i = \mathsf{penc}(M_1^i, M_2^i, M_3^i)$ and M_3^i variable. Suppose that $\exists\ 1 \leq i, j \leq n$ such that $M_3^i \neq M_3^j$, let us take, for example, $M_3^i = g_1$ and $M_3^j = g_2$. Then, we should have $a_1 + q_i = a_2 + q_j$ which implies that $q_j = a_1 + z_j$ et then that $a_2 + U$ is deducible which is in contradiction with 11. Moreover, in order to have a reduction, all Q_i must be equal. Then we take, the minimal one, Q_1 and, we have : $M = \circ_{i=1}^{n}\mathsf{renc}(\mathsf{penc}(M_1^i, M_2^i, x), Q_1)$ with $x \in \{g_1, g_2, g_3\}$ and free M_1^i, M_2^i, Q_1.

Then, we have :
$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L = \circ_{i=1}^{n}\mathsf{renc}(\mathsf{penc}(M_1^i, M_2^i, x), Q_i)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ (††)
$\quad =_E \mathsf{penc}(\diamond_{i=1}^{n} M_1^i, *_{i=1}^{n} M_2^i, \mathsf{pk}(a_j + Q_1))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$
Thanks to the fact that $\phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \approx_s \phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$ and (††), we also have that :
$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R = \circ_{i=1}^{n}\mathsf{renc}(\mathsf{penc}(M_1^i, M_2^i, x), Q_i)\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$
$\quad =_E \mathsf{penc}(\diamond_{i=1}^{n} M_1^i, *_{i=1}^{n} M_2^i, \mathsf{pk}(a_j + Q_1))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R.$
Then, we have, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$:

$$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{penc}(M_1', M_2', \mathsf{pk}(a_i + M_3'))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$

Moreover, since $M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E \mathsf{penc}(N_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L, N_1\theta_{k-1}$

$\sigma_{\tilde{N}}^{k-1}\Sigma_L, U)$ we have that $M_1'\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L =_E N_2\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ and $M_2'\theta_{k-1}\ \sigma_{\tilde{N}}^{k-1}\Sigma_L =_E N_1\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$. Using the fact that $\phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L \approx_s \phi_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_R$, these equalities hold with Σ_R. Finally, we have, for $\Sigma \in \{\Sigma_L, \Sigma_R\}$:

$$M\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma =_E \mathsf{penc}(N_2, N_1, \mathsf{pk}(a_i + M_3'))\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma.$$

□

Lemma 15. *Let φ_1 and φ_2 be two frames such that $\varphi_1 \approx_s \varphi_2$. Let a a name such that $a \in bn(\varphi_1) \cap bn(\varphi_2)$ and $\mathsf{p}(a)$ is not deducible. Let $U_i = \mathsf{d}(\mathsf{p}(a), U_i'')$ in normal form for $i = 1, 2$ such that U_i does not appear in φ_i. Then, we have, for $x \notin dom(\varphi_1) \cup dom(\varphi_2)$:*

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \varphi_2 \cup \{^{U_2}/_x\}.$$

Proof. Let n_1 be a fresh name and $\delta : U_1 \mapsto n_1$ the function which replace any occurrence of U_1 by n_1. Let us prove that :

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \nu.n_1(\varphi_1 \cup \{^{n_1}/_x\}).$$

Let $\varphi_1' = \varphi_1 \cup \{^{U_1}/_x\}$ and $\varphi_1'' = \nu.n_1(\varphi_1 \cup \{^{n_1}/_x\})$. Let M and N terms such that $(M = N)\varphi_1''$. Then, we have, with $\varphi_1'' = \nu\tilde{n}.\sigma_1''$, $(M\sigma_1'')[n_1 \mapsto U_1] =_E (N\sigma_1'')[n_1 \mapsto U_1]$ since the equationnal theory is stable by names substitutions. Now, since $n_1 \notin \text{fn}(M) \cup \text{fn}(N)$, we have $M(\sigma_1''[n_1 \mapsto U_1]) =_E N(\sigma_1''[n_1 \mapsto U_1])$ but $\sigma_1''[n_1 \mapsto U_1] = \sigma_1'$ with $\varphi_1' = \nu\tilde{m}.\sigma_1'$. So we have $(M = N)\varphi_1'$ too.

Now let M and N terms such that $(M = N)\varphi_1'$. Then we have :

$$(M\sigma_1')\!\downarrow =_{AC} (N\sigma_1')\!\downarrow$$

Thus,

$$(M\sigma_1')\!\downarrow \delta =_{AC} (N\sigma_1')\!\downarrow \delta$$

Claim 1: *If $U \longrightarrow V$ then $U\delta \longrightarrow V\delta$.*

Proof. (Claim 1) Let U be a term. Since $U \longrightarrow V$, there exists a rule $l \longrightarrow r$, a substitution θ and a position p such that $U|_p = l\theta$ and $V = U[r\theta]_p$. Then $\forall\ p'$ such that $U|_{p'} = U_1$, we have that p' cannot be a suffix of p, since U_1 is in normal form. Let $U' = U[X]_p$, then $U\delta = U'\delta[(l\theta)\delta]_p$. Since l does not contain d, we have that $U'\delta[l\theta\delta]_p = U'\delta[l(\theta\delta)]$. Using the rewriting rule, we have $U'\delta[l(\theta\delta)] \longrightarrow U'\delta[r(\theta\delta)]_p$. Finally, $U'\delta[r(\theta\delta)]_p = (U'[r\theta]_p)\delta = V\delta$, that is $U\delta \longrightarrow V\delta$. □

Let us prove that $(M\sigma_1')\!\downarrow \delta =_E (M\sigma_1'\delta)\!\downarrow$. If $M\sigma_1'$ is in normal form, we have that $(M\sigma_1'\delta)\!\downarrow =_E (M\sigma_1')\!\downarrow \delta$. If it is not, then, it exists $W_1, \dots, W_n$ such that $W_1 = M\sigma_1'$, $W_n = (M\sigma_1')\!\downarrow$ and $W_i \longrightarrow W_{i+1}$ for $i = 1..n-1$. Using Claim 1, we have that $W_i\delta \longrightarrow W_{i+1}\delta$ for $i = 1..n-1$ and then that $((M\sigma_1')\delta)\!\downarrow =_{AC} (M\sigma_1')\!\downarrow \delta$. Thus, using the same argument for $N\sigma_1'$, we have :

$$M\sigma_1'\delta =_E N\sigma_1'\delta$$

Since a, which is a restricted name, M and N cannot contain a. Moreover, $\mathsf{p}(a)$ is not deducible, thus we cannot have the case where $M = \mathsf{d}(x, y)$ with $x\sigma_1'\delta = \mathsf{p}(a)$. Then, we have :

$$M(\sigma_1'\delta) =_E N(\sigma_1'\delta)$$

Since U_1 does not appear in φ_i, we have :

$$M\sigma_1'' =_E N\sigma_1''$$

And we have $(M = N)\varphi_1''$, which proves the static equivalence above. Then, using the same development on φ_2 we have, for $i = 1, 2$ and two fresh names n_1, n_2 :

$$\varphi_i \cup \{^{U_i}/_x\} \approx_s \nu.n_i(\varphi_i \cup \{^{n_i}/_x\}).$$

Since $\varphi_1 \approx_s \varphi_2$, we have that $\nu.n_1(\varphi_1 \cup \{^{n_1}/_x\}) \approx_s \nu.n_2(\varphi_2 \cup \{^{n_2}/_x\})$ and using what we just proved, we get :

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \varphi_2 \cup \{^{U_2}/_x\}.$$

□

Lemma 16. *Let φ_1 and φ_2 be two frames such that $\varphi_1 \approx_s \varphi_2$. Let a a name such that $a \in bn(\varphi_1) \cap bn(\varphi_2)$ and is not deducible. Let $U_i = \mathsf{sign}(U_i', a)$ in normal form for $i = 1, 2$ and U_i do not appear in φ_i. Then, we have, for $x \notin dom(\varphi_1) \cup dom(\varphi_2)$:*

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \varphi_2 \cup \{^{U_2}/_x\}.$$

Proof. Let n_1 be a fresh name and $\delta : U_1' \mapsto n_1$ the function which replace any occurrence of U_1' by n_1. Let us prove that :

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \nu.n_1(\varphi_1 \cup \{^{\mathsf{sign}(n_1,a)}/_x\}).$$

Let $\varphi_1' = \varphi_1 \cup \{^{U_1}/_x\}$ and $\varphi_1'' = \nu.n_1(\varphi_1 \cup \{^{\mathsf{sign}(n_1,a)}/_x\})$. Let M and N terms such that $(M = N)\varphi_1''$. Then, we have, with $\varphi_1'' = \nu\tilde{n}.\sigma_1''$, $(M\sigma_1'')[\mathsf{sign}(n_1, a) \mapsto U_1] =_E (N\sigma_1'')[\mathsf{sign}(n_1, a) \mapsto U_1]$ since the equationnal theory is stable by names substitutions. Now, since $n_1 \notin \text{fn}(M) \cup \text{fn}(N)$, we have $M(\sigma_1''[\mathsf{sign}(n_1, a) \mapsto U_1]) =_E N(\sigma_1''[\mathsf{sign}(n_1, a) \mapsto U_1])$ but $\sigma_1''[\mathsf{sign}(n_1, a) \mapsto U_1] = \sigma_1'$ with $\varphi_1' = \nu\tilde{m}.\sigma_1'$. So we have $(M = N)\varphi_1'$ too.

Now let M and N terms such that $(M = N)\varphi_1'$. Then we have :

$$(M\sigma_1')\!\downarrow =_{AC} (N\sigma_1')\!\downarrow$$
$$(M\sigma_1')\!\downarrow \delta =_{AC} (N\sigma_1')\!\downarrow \delta$$

Claim 2: *If $U \longrightarrow V$ then $U\delta \longrightarrow V\delta$.*

Proof. (Claim 2) Let U be a term. Since $U \longrightarrow V$, $\exists$ a rule $l \longrightarrow r$, a substitution θ and a position p such that $U|_p = l\theta$ and $V = U[r\theta]_p$. Then, $\forall$ p' such that $U|_{p'} = U_1$, we have that p' cannot be a suffix of p, since U_1 is in normal form. Let $U' = U[X]_p$, then $U\delta = U'\delta[l\theta\delta]_p$. Using the equational theory, the only interesting case is when $l\theta \longrightarrow r\theta$ is equation $\mathsf{checksign}(M, \mathsf{vk}(id), \mathsf{sign}(M, id)) =$

Ok where $M = U_1'$ and $id = a$. Then, we can easily see that $l\theta\delta \longrightarrow r\theta\delta$ since $l\theta\delta = \mathsf{checksign}(n_1, a, \mathsf{sign}(n_1, a))$ and $r\theta = r\theta\delta$. In other cases, we have $l\theta\delta \longrightarrow r\theta\delta$ since modification implies by δ do not interfere. Thus, we have $U'\delta[l\theta\delta] \longrightarrow U'\delta[r(\theta\delta)]_p$. Finally, $U'\delta[r\theta\delta]_p = (U'[r\theta]_p)\delta = V\delta$, that is $U\delta \longrightarrow V\delta$. □

Let us prove that $(M\sigma_1')\downarrow \delta =_E (M\sigma_1'\delta)\downarrow$. If $M\sigma_1'$ is in normal form, we have that $(M\sigma_1'\delta)\downarrow =_E (M\sigma_1')\downarrow \delta$. If it is not, then, it exists $W_1, \ldots, W_n$ such that $W_1 = M\sigma_1'$, $W_n = (M\sigma_1')\downarrow$ and $W_i \longrightarrow W_{i+1}$ for $i = 1..n-1$. Using Claim 2, we have that $W_i\delta \longrightarrow W_{i+1}\delta$ for $i = 1..n-1$ and then that $((M\sigma_1')\delta)\Downarrow =_{AC} (M\sigma_1')\Downarrow \delta$. Thus, using the same argument for $N\sigma_1'$, we have :

$$M\sigma_1'\delta =_E N\sigma_1'\delta$$

Since a, which is a restricted name, M and N cannot contain a. Then, we have :

$$M(\sigma_1'\delta) =_E N(\sigma_1'\delta)$$

Since U_1 does not appear in φ_i, we have :

$$M\sigma_1'' =_E N\sigma_1''$$

And we have $(M = N)\varphi_1''$, which proves the static equivalence above. Then, using the same development on φ_2 we have, for $i = 1, 2$ and two fresh names n_1, n_2 :

$$\varphi_i \cup \{^{U_i}/_x\} \approx_s \nu.n_i(\varphi_i \cup \{^{\mathsf{sign}(n_i,a)}/_x\}).$$

Since $\varphi_1 \approx_s \varphi_2$, we have that $\nu.n_1(\varphi_1 \cup \{^{\mathsf{sign}(n_1,a)}/_x\}) \approx_s \nu.n_2(\varphi_2 \cup \{^{\mathsf{sign}(n_2,a)}/_x\})$ and using what we just proved, we get :

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \varphi_2 \cup \{^{U_2}/_x\}.$$

□

Lemma 17. *Let ϕ and ψ be frames such that $\phi \cup \{^t/_x\} \approx_s \psi \cup \{^{t'}/_x\}$ for some terms t and t'. Then :*

$$\phi \cup \{^t/_x\} \cup \{^t/_y\} \approx_s \psi \cup \{^{t'}/_x\} \cup \{^{t'}/_y\}.$$

Proof. Let $\phi \cup \{^t/_x\} \cup \{^t/_y\} = \phi''$, $\psi \cup \{^{t'}/_x\} \cup \{^{t'}/_y\} = \psi''$, $\phi \cup \{^t/_x\} = \phi'$ and $\psi \cup \{^{t'}/_x\} = \psi'$. Let M, N be terms such that $(M = N)\phi''$. If $y \notin \mathrm{fv}(M) \cup \mathrm{fv}(N)$ then since $\phi' \approx_s \psi'$, the fact that $(M = N)\psi''$ is straightforward. If $y \in \mathrm{fv}(M) \cup \mathrm{fv}(N)$, let $\delta : y \mapsto x$, we have : $(P\delta)\phi' = P\phi''$ and $(P\delta)\psi' = P\psi''$ for all term P. Thus :

$$M\phi'' =_E N\phi''$$
$$(M\delta)\phi' =_E (N\delta)\phi'$$

Since $\phi' \approx_s \psi'$ and $((M\delta) = (N\delta))\phi'$, we have :

$$(M\delta)\psi' =_E (N\delta)\psi'$$
$$M\psi'' =_E N\psi''$$

□

Lemma 18. *Let φ_1 and φ_2 be two frames such that $\varphi_1 \approx_s \varphi_2$. Let a a name such that $a \in bn(\varphi_1) \cap bn(\varphi_2)$ and is not deducible. Let $U_i = \mathsf{dec}(U'_i, a)$ in normal form for $i = 1, 2$ and U_i do not appear in φ_i. Then, we have, for $x \notin dom(\varphi_1) \cup dom(\varphi_2)$:*

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \varphi_2 \cup \{^{U_2}/_x\}.$$

Proof. Let n_1 be a fresh name and $\delta : U_1 \mapsto n_1$ the function which replace any occurrence of U_1 by n_1. Let us prove that :

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \nu.n_1(\varphi_1 \cup \{^{n_1}/_x\}).$$

Let $\varphi'_1 = \varphi_1 \cup \{^{U_1}/_x\}$ and $\varphi''_1 = \nu.n_1(\varphi_1 \cup \{^{n_1}/_x\})$. Let M and N terms such that $(M = N)\varphi''_1$. Then, we have, with $\varphi''_1 = \nu\tilde{n}.\sigma''_1$, $(M\sigma''_1)[n_1 \mapsto U_1] =_E (N\sigma''_1)[n_1 \mapsto U_1]$ since the equationnal theory is stable by names substitutions. Now, since $n_1 \notin \text{fn}(M) \cup \text{fn}(N)$, we have $M(\sigma''_1[n_1 \mapsto U_1]) =_E N(\sigma''_1[n_1 \mapsto U_1])$ but $\sigma''_1[n_1 \mapsto U_1] = \sigma'_1$ with $\varphi'_1 = \nu\tilde{m}.\sigma'_1$. So we have $(M = N)\varphi'_1$ too.

Now let M and N terms such that $(M = N)\varphi'_1$. Then we have :

$$(M\sigma'_1)\!\downarrow =_{AC} (N\sigma'_1)\!\downarrow$$

Thus,

$$(M\sigma'_1)\!\downarrow \delta =_{AC} (N\sigma'_1)\!\downarrow \delta$$

Claim 3: *If $U \longrightarrow V$ then $U\delta \longrightarrow V\delta$.*

Proof. (Claim 3) Let U be a term. Since $U \longrightarrow V$, there exists a rule $l \longrightarrow r$, a substitution θ and a position p such that $U|_p = l\theta$ and $V = U[r\theta]_p$. Then $\forall\ p'$ such that $U|_{p'} = U_1$, we have that p' cannot be a suffix of p, since U_1 is in normal form. Let $U' = U[X]_p$, then $U\delta = U'\delta[(l\theta)\delta]_p$. Since l does not contain dec, we have that $U'\delta[l\theta\delta]_p = U'\delta[l(\theta\delta)]$. Using the rewriting rule, we have $U'\delta[l(\theta\delta)] \longrightarrow U'\delta[r(\theta\delta)]_p$. Finally, $U'\delta[r(\theta\delta)]_p = (U'[r\theta]_p)\delta = V\delta$, that is $U\delta \longrightarrow V\delta$. □

Let us prove that $(M\sigma'_1)\!\downarrow \delta =_E (M\sigma'_1\delta)\!\downarrow$. If $M\sigma'_1$ is in normal form, we have that $(M\sigma'_1\delta)\!\downarrow =_E (M\sigma'_1)\!\downarrow \delta$. If it is not, then, it exists $U_1, \ldots, U_n$ such that $U_1 = M\sigma'_1$, $U_n = (M\sigma'_1)\!\downarrow$ and $U_i \longrightarrow U_{i+1}$ for $i = 1..n-1$. Using Claim 1, we have that $U_i\delta \longrightarrow U_{i+1}\delta$ for $i = 1..n-1$ and then that $((M\sigma'_1)\delta)\!\downarrow =_{AC} (M\sigma'_1)\!\downarrow \delta$. Thus, using the same argument for $N\sigma'_1$, we have :

$$M\sigma'_1\delta =_E N\sigma'_1\delta$$

Since a, which is a restricted name, M and N cannot contain a. Then, we have :

$$M(\sigma'_1\delta) =_E N(\sigma'_1\delta)$$

Since U_1 does not appear in φ_i, we have :

$$M\sigma''_1 =_E N\sigma''_1$$

And we have $(M = N)\varphi_1''$, which proves the static equivalence above. Then, using the same development on φ_2 we have, for $i = 1, 2$ and two fresh names n_1, n_2 :

$$\varphi_i \cup \{^{U_i}/_x\} \approx_s \nu.n_i(\varphi_i \cup \{^{n_i}/_x\}).$$

Since $\varphi_1 \approx_s \varphi_2$, we have that $\nu.n_1(\varphi_1 \cup \{^{n_1}/_x\}) \approx_s \nu.n_2(\varphi_2 \cup \{^{n_2}/_x\})$ and using what we just proved, we get :

$$\varphi_1 \cup \{^{U_1}/_x\} \approx_s \varphi_2 \cup \{^{U_2}/_x\}.$$

□

Lemma 19. *Let $N_i\theta_{i-1}\sigma_{\tilde{N}}^{i-1}\Sigma$ be id$_i$-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $i = 3..n$. Let $\phi_{i-1}^{res} = \nu\tilde{n}.\theta_{i-1}^{res}$. We have :*

$$\phi_{i-1}^{res}\sigma_{\tilde{N}}\Sigma_L \approx_s \phi_{i-1}^{res}\sigma_{\tilde{N}}\Sigma_R \Longrightarrow \phi_i^{res}\sigma_{\tilde{N}}\Sigma_L \approx_s \phi_i^{res}\sigma_{\tilde{N}}\Sigma_R.$$

Proof. As a first remark : for $i = 3..n$, since $N_i\theta_{i-1}\sigma_{\tilde{N}}^{i-1}\Sigma$ is a id$_i$-valid ballot, then we know that, using Lemma 14 :

- $N_i\theta_n\sigma_{\tilde{N}}\Sigma =_E (W_i, X_i, Z_i)\theta_n\sigma_{\tilde{N}}\Sigma$ with free W_i, W_i, Z_i and $\Sigma \in \{\Sigma_L, \Sigma_R\}$.

- $W_i\theta_n\sigma_{\tilde{N}}\Sigma =_E \mathsf{penc}(W_i', W_i'', U_i)\theta_n\sigma_{\tilde{N}}\Sigma$ with $\Sigma \in \{\Sigma_L, \Sigma_R\}$, free W_i', W_i'' and free U_i or $U_i = \mathsf{pk}(a_i + U_i')$ with free U_i' and $a_i \in \{a_1, a_2, a_3\}$.

Then, we have two cases :

- $U_i\theta_n\sigma_{\tilde{N}}\Sigma =_E \mathsf{pk}(a_1)$. Then, we have :

  $$\begin{aligned} result_i\theta_i^{res}\sigma_{\tilde{N}}\Sigma &=_E \mathsf{dec}(\mathsf{penc}(W_i'\theta_{i-1}^{res}\sigma_{\tilde{N}}\Sigma, W_i''\theta_{i-1}^{res}\sigma_{\tilde{N}}\Sigma, \mathsf{pk}(a_1)), a_1) \\ &=_E W_i'\theta_{i-1}^{res}\sigma_{\tilde{N}}\Sigma. \end{aligned}$$

  Then, we have $result_i\theta_i^{res}\sigma_{\tilde{N}}\Sigma =_E W\theta_{i-1}^{res}\sigma_{\tilde{N}}\Sigma$ where W is free. Let $\theta' = \theta_{i-1}^{res}\sigma_{\tilde{N}}$ and $\theta = \theta' \cup \{^{M\theta'}/_{result_i}\} = \theta_i^{res}\sigma_{\tilde{N}}$. Using Lemma 9, since $\phi_{i-1}^{res}\sigma_{\tilde{N}}\Sigma_L \approx_s \phi_{i-1}^{res}\sigma_{\tilde{N}}\Sigma_R$, we conclude.

- $U\theta_n\sigma_{\tilde{N}}\Sigma \neq_E \mathsf{pk}(a_1)$. Then, $result_i\theta_i^{res}\sigma_{\tilde{N}}\Sigma =_E \mathsf{dec}(\mathsf{penc}(W_i', W_i'', U_i)\theta_{i-1}^{res}$ $\sigma_{\tilde{N}}^{i-1}\Sigma, a_1)$. Then, we have two cases. The first one when $\exists\ j$ such that $result_j\theta_i^{res}\sigma_{\tilde{N}}\Sigma =_E result_i\theta_i^{res}\sigma_{\tilde{N}}$. In that case, we use Lemma 17 to conclude. The second one when the first case do not happen is solved using directly Lemma 18 since a_1 is restricted and not deducible.

□

Lemma 20. *Let $N_i\theta_i\sigma_{\tilde{N}}\Sigma$ be id$_i$-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $i = 3..n$.*

$$\begin{array}{lclcl} result_1\sigma_{\tilde{N}}\Sigma_L & =_E & v_1 & =_E & result_1\sigma_{\tilde{N}}\Sigma_R \\ result_2\sigma_{\tilde{N}}\Sigma_L & =_E & v_2 & =_E & result_2\sigma_{\tilde{N}}\Sigma_R. \end{array}$$

Proof. Obvious. □

Now let us return to Proposition 8 and start to prove it.

Proposition 8. *Let $N_i\theta_i\Sigma$ be id_i-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $i \in \{3, \ldots, n\}$, we have :*

$$\nu\tilde{n}.(\theta|R)\sigma_{\tilde{N}}\Sigma_L \approx_s \nu\tilde{n}.(\theta|\overline{R})\sigma_{\tilde{N}}\Sigma_R.$$

Proof. The proposition will be proved using two consecutive induction.

First, let us show that : for any $i \geq 2$, let $\phi_i = \nu\tilde{n}.\theta_i$ then $\phi_i\sigma^i_{\tilde{N}}\Sigma_L \approx_s \phi_i\sigma^i_{\tilde{N}}\Sigma_R$.
Base Case : Using Lemma 10, we show that $\phi_2\sigma^2_{\tilde{N}}\Sigma_L \approx_s \phi_2\sigma^2_{\tilde{N}}\Sigma_R$.

Induction step : Assume now that $\phi_i\sigma^i_{\tilde{N}}\Sigma_L \approx_s \phi_i\sigma^i_{\tilde{N}}\Sigma_R$ and let us show that $\phi_{i+1}\sigma^{i+1}_{\tilde{N}}\Sigma_L \approx_s \phi_{i+1}\sigma^{i+1}_{\tilde{N}}\Sigma_R$.
Using Lemma 15 with $U_1 = (y_i\theta_i\sigma^i_{\tilde{N}}\Sigma_L)\downharpoonleft = \mathsf{d}(\mathsf{p}(id_i), U'_1)$ and $U_2 = (y_i\theta_i\sigma^i_{\tilde{N}}\Sigma_R)\downharpoonleft = \mathsf{d}(\mathsf{p}(id_i), U'_2)$, we prove that $\theta_i \cup \{^{U_1}/_{y_i}\}\sigma^{i+1}_{\tilde{N}}\Sigma_L \approx_s \theta_i \cup \{^{U_2}/_{y_i}\}\sigma^{i+1}_{\tilde{N}}\Sigma_R$. Then, using this new equivalence and Lemma 16 with $U_1 = (z_i\theta_i\sigma^{i+1}_{\tilde{N}}\Sigma_L)\downarrow = \mathsf{sign}(U'_1, id_R)$ and $U_2 = (z_i\theta_i\sigma^{i+1}_{\tilde{N}}\Sigma_L)\downharpoonleft = \mathsf{sign}(U'_2, id_R)$, we have now that $\phi_{i+1}\sigma^{i+1}_{\tilde{N}}$ $\Sigma_L \approx_s \phi_{i+1}\sigma^{i+1}_{\tilde{N}}\Sigma_R$.
Thus, we deduct :

$$\phi_n\sigma_{\tilde{N}}\Sigma_L \approx_s \phi_n\sigma_{\tilde{N}}\Sigma_R$$

and we can note $\phi_n = \phi^{res}_2$.

Now let us show that : for any $i \geq 2$, $\phi^{res}_i = \nu\tilde{n}.\theta^{res}_i$ then $\phi^{res}_i\sigma_{\tilde{N}}\Sigma_L \approx_s \phi^{res}_i\sigma_{\tilde{N}}\Sigma_R$.
Base Case : Using the fact that $\phi_n = \phi^{res}_2$, the base case is proved by the first induction.

Induction step : Assume now that $\phi^{res}_i\sigma_{\tilde{N}}\Sigma_L \approx_s \phi^{res}_i\sigma_{\tilde{N}}\Sigma_R$ and let us show that $\phi^{res}_{i+1}\sigma_{\tilde{N}}\Sigma_L \approx_s \phi^{res}_{i+1}\sigma_{\tilde{N}}\Sigma_R$.
Using Lemma 19, we can prove the induction step adding each result one by one and, finally, we have :

$$\phi\sigma_{\tilde{N}}\Sigma_L \approx_s \phi\sigma_{\tilde{N}}\Sigma_R \text{ with } \phi = \nu\tilde{n}.\theta.$$

Now using Lemmas 9 and 20, we prove the final static equivalence :

$$\phi_1 = \nu\tilde{n}.(\theta|R)\sigma_{\tilde{N}}\Sigma_L \approx_s \phi_2 = \nu\tilde{n}.(\theta|\overline{R})\sigma_{\tilde{N}}\Sigma_R.$$

□

From Proposition 8, we can enunciate a corollary.

Corollary 21. *For $i = 0 \ldots n$, $j = 3 \ldots n$, and $N_k\theta_k\Sigma$ be id_k-valid ballots for $\Sigma \in \{\Sigma_L, \Sigma_R\}$ and $k = 3 \ldots n$, we have :*

$$\nu\tilde{n}.\theta_i\sigma^i_{\tilde{N}}\Sigma_L \approx_s \nu\tilde{n}.\theta_i\sigma^i_{\tilde{N}}\Sigma_R$$
$$\nu\tilde{n}.\theta'_j\sigma_{\tilde{N}}\Sigma_L \approx_s \nu\tilde{n}.\theta'_j\sigma_{\tilde{N}}\Sigma_R$$

B Proof of Theorem 4

Let us remind the Theorem we need to prove.

Theorem 4. *Let n be the number of voters. The Norwegian e-voting protocol process specification satisfies ballot secrecy without the auditing process, even with $n-2$ voters are corrupted, provided that the other components are honest.*

$$\begin{aligned} &A'_n[V\{{}^{c_1}/_{c_{auth}}, {}^{c_{RV_1}}/_{c_{RV}}\}\sigma \mid V\{{}^{c_2}/_{c_{auth}}, {}^{c_{RV_2}}/_{c_{RV}}\}\tau] \\ &\qquad\qquad \approx_l \overline{A'}_n\,[V\{{}^{c_1}/_{c_{auth}}, {}^{c_{RV_1}}/_{c_{RV}}\}\tau | V\{{}^{c_2}/_{c_{auth}}, {}^{c_{RV_2}}/_{c_{RV}}\}\sigma] \end{aligned}$$

where $\sigma = \{{}^{v_1}/_{x_{vote}}\}$ and $\tau = \{{}^{v_2}/_{x_{vote}}\}$.

Let us introduce the relation we will use to prove labeled bisimilarity.

B.1 Partial evolutions of protocol specification

First, we will introduce partial evolutions of the protocol process specification and remind some notations used. Note that correct modeling of sub-processes have not been depicted but one can see that describing partial evolutions of sub-processes can be seen as a modeling description. Then, as an example, B_n, the ballot box correspond to $B^1_{1,n}$ in that case, without auditor. It avoids a annoying and non-useful applied-pi description, since it is easy to remove all lines dealing with an auditor's stuff, as the full description was depicted in the article.

Definition 22. *Notations and partial evolutions for honest voters. ($i \in \{1,2\}$)*

$$\begin{array}{ll@{\qquad\qquad}ll}
V_i^1 & = \overline{c_{out}}\langle ball_i\rangle.V_i^2 & e_i & = \mathsf{penc}(x^i_{vote}, t_i, \mathsf{pk}(a_1)) \\
V_i^2 & = \overline{c_i}\langle ball_i\rangle.V_i^3 & pfk_i & = \mathsf{pfk}_1(id_i, t_i, x^i_{vote}, e_i) \\
V_i^3 & = c_{RV_i}(rec_i).V_i^4 & sig_i & = \mathsf{sign}((e_i, pfk_i), id_i) \\
V_i^4 & = c_i(con_i).V_i^5 & ball_i & = (e_i, pfk_i, sig_i) \\
V_i^5 & = \overline{c_{out}}\langle con_i\rangle.V_i^6 & hv_i & = \mathsf{hash}((\mathsf{vk}(id_i), e_i, pfk_i, sig_i)) \\
V_i^6 & = \overline{c_{out}}\langle rec_i\rangle.V_i^7 & & \\
V_i^7 & = \text{if } \phi_{\mathsf{v}}(idp_R, id_i, hv_i, con_i, x_i^{vote}, rec_i) \text{ then } V_i^8 \text{ else } 0 & & \\
V_i^8 & = \overline{c_i}\langle \mathsf{Ok}\rangle & &
\end{array}$$

Definition 23. *Notations and partial evolutions for the ballot box. ($i \in \{1,\ldots,n\}$)*

$$\begin{array}{ll@{\qquad}ll}
B^1_{i,n} & = c_i(x_i).B^{1.1}_{i,n} & e'_i & = \mathsf{renc}(\Pi_1(x_i), \mathsf{s}(id_i)) \\
B^{1.1}_{i,n} & = \text{if } \phi_{\mathsf{b}}(idp_i, x_i) \text{ then } B^{1.2}_{i,n} \text{ else } 0 & pfk'_i & = \mathsf{pfk}_2(id_i, a_2, \Pi_1(x_i), e'_i) \\
B^{1.2}_{i,n} & = \overline{c_{BR}}\langle ball'_i\rangle.B^2_{i,n} & e''_i & = \mathsf{blind}(e'_i, \mathsf{s}(id_i)) \\
B^2_{i,n} & = c_{BR}(q_i).B^3_{i,n} & pfk''_i & = \mathsf{pfk}_2(id_i, \mathsf{s}(id_i), e'_i, e''_i) \\
B^3_{i,n} & = \text{if } \phi_{\mathsf{s}}(idp_R, hbb_i, q_i) \text{ then } B^{3.1}_{i,n} \text{ else } 0 & ball'_i & = (x_i, e'_i, pfk'_i, e''_i, pfk''_i) \\
B^{3.1}_{i,n} & = \overline{c_i}\langle q_i\rangle.B^{3.2}_{i,n} & hbb_i & = \mathsf{hash}((\mathsf{vk}(id_i), x_i)) \\
B^{3.2}_{i,n} & = c_i(sy_i).B^1_{i+1,n} & & \\
B^{3.2}_{n,n} & = c_n(sy_n).B^4_{1,n} & & \\
B^4_{i,n} & = \overline{c_{BD}}\langle \Pi_1(x_i)\rangle.B^4_{i+1,n} & & \\
B^4_{n,n} & = \overline{c_{BD}}\langle \Pi_1(x_n)\rangle & &
\end{array}$$

Definition 24. *Notations et and partial evolutions for the receipt generator. ($i \in \{1,\ldots,n\}$)*

$$\begin{array}{llll}
R^1_{i,n} & = c_{BR}(p_i).R^2_{i,n} & & \\
R^2_{i,n} & = \text{if } \phi_{\mathsf{r}}(idp_i, p_i) \text{ then } R^3_{i,n} \text{ else } 0 & & \\
R^3_{i,n} & = \overline{c_{RV_i}}\langle r_i\rangle.R^4_{i,n} & r_i & = \mathsf{d}(\mathsf{p}(id_i), \mathsf{dec}(\Pi_6(p_i), a_3)) \\
R^4_{i,n} & = \overline{c_{BR}}\langle sig^R_i\rangle.R^1_{i+1,n} & hbr_i & = \mathsf{hash}((idp_i, \Pi_1(p_i), \Pi_2(p_i), \Pi_3(p_i))) \\
R^4_{n,n} & = \overline{c_{BR}}\langle sig^R_n\rangle & sig^R_i & = \mathsf{sign}(hbr_i, id_R)
\end{array}$$

Definition 25. *Notations and partial evolutions for the decryption service, we distinguish two cases : one without a swap (D) and one with swap ($\overline{D}$).(i* $\in \{1, \dots, n\}$*)*

$$\begin{array}{llll}
dec_i & = \mathsf{dec}(d_i, a_1) & \overline{D}^1_{i,n} & = c_{BD}(d_j).\overline{D}^1_{i+1,n} \\
 & & \overline{D}^1_{n,n} & = c_{BD}(d_n).\overline{D}^2_1 \\
D^1_{i,n} & = c_{BD}(d_i).D^1_{i+1,n} & \overline{D}^2_{1,n} & = \overline{c_{out}}\langle dec_2\rangle.\overline{D}^2_{2,n} \\
D^1_{n,n} & = c_{BD}(d_n).D^2_{1,n} & \overline{D}^2_{2,n} & = \overline{c_{out}}\langle dec_1\rangle.\overline{D}^2_{3,n} \\
D^2_{i,n} & = \overline{c_{out}}\langle dec_i\rangle.D^2_{i+1,n} & \overline{D}^2_{i,n} & = \overline{c_{out}}\langle dec_i\rangle.\overline{D}^2_{i+1,n} \\
D^2_{n,n} & = \overline{c_{out}}\langle dec_n\rangle & \overline{D}^2_{n,n} & = \overline{c_{out}}\langle dec_n\rangle
\end{array}$$

Definition 26. *Partial evolutions of global process representing the enrichment of the frame as the process advances.*

$$\begin{array}{ll}
\tilde{n} = & (a_1, a_2, id_1, id_2, id_R, c_1, c_2, c_{RV_1}, c_{RV_2}, c_{BR}, c_{BD}) \\
\Gamma = & \{^{\mathsf{pk}(a_1)}/_{g_1}, ^{\mathsf{pk}(a_2)}/_{g_2}, ^{\mathsf{pk}(a_3)}/_{g_3}, ^{\mathsf{vk}(id_1)}/_{idp_1}, \dots, ^{\mathsf{vk}(id_n)}/_{idp_n}, ^{\mathsf{vk}(id_R)}/_{idp_R}\}
\end{array}$$

$$\begin{array}{ll}
A_0 = & \nu\tilde{n}.\,[\_|\Gamma] \\
A_1 = & \nu(\tilde{n}, t_1).\,[\_|\{^{ball_1}/_{b_1}\}|\Gamma] \\
A_2 = & \nu(\tilde{n}, t_1, x_1).\,[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\Gamma] \\
A_3 = & \nu(\tilde{n}, t_1, x_1, p_1).\,\left[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\Gamma\right] \\
A_4 = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1).\,\left[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}|\Gamma\right] \\
A_5 = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1).\,\Big[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}| \\
 & \{^{sig^R_1}/_{q_1}\}|\Gamma\Big] \\
A_6 = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1).\,\Big[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}| \\
 & \{^{sig^R_1}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\Gamma\Big] \\
A_7 = & A_6\,[\_|\{^{rec_1}/_{y_1}\}] \\
A_8 = & A_7\,[\_|\{^{con_1}/_{z_1}\}] \\
A_9 = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2).\,\big[\_|\{\{^{ball_i}/_{b_i}\}|i = 1, 2\}|\{^{ball_1}/_{x_1}\}| \\
 & \{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}|\{^{sig^R_1}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\big] \\
A_{10} = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2).\,\big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}|i = 1, 2\}| \\
 & \{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}|\{^{sig^R_1}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\big] \\
A_{11} = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2).\,\Big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}|\{^{ball'_i}/_{p_i}\} \\
 & |i = 1, 2\}|\{^{r_1}/_{rec_1}\}|\{^{sig^R_1}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\Big] \\
A_{12} = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2, rec_2).\,\big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}| \\
 & \{^{ball'_i}/_{p_i}|\{^{r_i}/_{rec_i}\}\}|i = 1, 2\}|\{^{sig^R_1}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\big] \\
A_{13} = & \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2, rec_2, q_2).\,\big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}| \\
 & \{^{ball'_i}/_{p_i}|\{^{r_i}/_{rec_i}\}|\{^{sig^R_i}/_{q_i}\}\}|i = 1, 2\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\big]
\end{array}$$

$$
\begin{array}{l}
A_{14} = \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2, rec_2, q_2, con_2).\,[\_\,|\{\{{}^{ball_i}/_{b_i}\}| \\
\qquad \{{}^{ball_i}/_{x_i}\}|\{{}^{ball'_i}/_{p_i}|\{{}^{r_i}/_{rec_i}\}|\{{}^{sig_i^R}/_{q_i}\}|\{{}^{q_1}/_{con_1}\}\}|i=1,2\}| \\
\qquad \{{}^{rec_1}/_{y_1}\}|\{{}^{con_1}/_{z_1}\}|\Gamma] \\
A_{15} = A_{14}\,[\_\,|\{{}^{rec_2}/_{y_2}\}]
\end{array}
$$

For $i \in \{3,\ldots,n\}$ *:*

$$
\begin{array}{rl}
\tilde{m}_i = & \{(p_k, q_k)|k \in \{3,\ldots,i-1\}\} \\
\Lambda = & \{\{{}^{ball_i}/_{b_i}\}|\{{}^{ball_i}/_{x_i}\}|\{{}^{ball'_i}/_{p_i}|\{{}^{r_i}/_{rec_i}\}|\{{}^{sig_i^R}/_{q_i}\}|\{{}^{q_1}/_{con_1}\}|\{{}^{rec_1}/_{y_1}| \\
 & \{{}^{con_1}/_{z_1}\}\}|i=1,2\} \\
\Lambda_i = & \{\{{}^{N_k}/_{x_k}\}|\{{}^{ball'_k}/_{p_k}\}|\{{}^{r_k}/_{y_k}\}|\{{}^{sig_k^R}/_{q_k}\}|\{{}^{q_k}/_{z_k}\}|\{{}^{W_k}/_{sy_k}\}| \\
 & k \in \{3,\ldots,i-1\}\}
\end{array}
$$

$$
\begin{array}{rl}
A_i^1 = & \nu(\tilde{n}, \tilde{m}_i).\,[\_\,|\Lambda_i|\Lambda|\Gamma] \\
A_i^2 = & A_i^1\,\left[\_\,|\{{}^{N_i}/_{x_i}\}\right] \\
A_i^3 = & \nu(\tilde{n}, \tilde{m}_i, p_i).\,\left[\_\,|\{{}^{N_i}/_{x_i}\}|\{{}^{ball'_i}/_{p_i}\}|\Lambda_i|\Lambda|\Gamma\right] \\
A_i^4 = & A_i^3\,[\_\,|\{{}^{r_i}/_{y_i}\}] \\
A_i^5 = & \nu(\tilde{n}, \tilde{m}_{i+1}).\,\left[\_\,|\{{}^{N_i}/_{x_i}\}|\{{}^{ball'_i}/_{p_i}\}|\{{}^{r_i}/_{y_i}\}|\{{}^{sig_i^R}/_{q_i}\}|\Lambda_i|\Lambda|\Gamma\right] \\
A_i^6 = & \nu(\tilde{n}, \tilde{m}_{i+1}).\,\left[\_\,|\{{}^{N_i}/_{x_i}\}|\{{}^{ball'_i}/_{p_i}\}|\{{}^{r_i}/_{y_i}\}|\{{}^{sig_i^R}/_{q_i}\}|\{{}^{q_i}/_{z_i}\}|\Lambda_i|\Lambda|\Gamma\right]
\end{array}
$$

For $i \in \{1,\ldots,n\}$ *:*

$$
\begin{array}{rl}
\tilde{d}_i = & \{d_k|k \in \{1,\ldots,i-1\}\} \\
\Omega_i = & \{\{{}^{\Pi_1(x_k)}/_{d_k}\}|k \in \{1,\ldots,i-1\}\} \\
A'_i = & \nu(\tilde{n}, \tilde{m}_{n+1}, \tilde{d}_i).\,[\_\,|\Omega_i|\Lambda_{n+1}|\Lambda|\Gamma] \\
A''_1 = & A'_n\,\left[\_\,|\{{}^{dec_1}/_{result_1}\}\right] \\
A''_i = & A''_{i-1}\,\left[\_\,|\{{}^{dec_i}/_{result_i}\}\right]
\end{array}
$$

$$
\begin{array}{rl}
\overline{A}''_1 = & A'_n\,\left[\_\,|\{\{{}^{dec_2}/_{result_1}\}\right] \\
\overline{A}''_2 = & \overline{A}''_1\,\left[\_\,|\{\{{}^{dec_1}/_{result_2}\}\right] \\
\overline{A}''_i = & \overline{A}''_{i-1}\,\left[\_\,|\{{}^{dec_i}/_{result_i}\}\right]
\end{array}
$$

B.2 Relation

Now we can define the relation.

Definition 27. *Given integer $n \geq 2$, $\forall\ 3 \leq j \leq n$, let M_j and N_j terms such that $N_j\theta_{j-1}\sigma_{\tilde{N}}^{j-1}\Sigma_L$ is an id_j-valid ballot, and such that $fv(M_j) \cup fv(N_j) \subseteq dom(A_j^1)$ and $(fn(M_j) \cup fn(N_j)) \cap bn(A_j^1) = \emptyset$. We consider the smallest relation $\mathcal{R}$ which is closed under structural equivalence and includes the following pairs of extended processes :*

$$A_0\,\left[V_1^1|V_2^1|B_{1,n}^1|R_{1,n}^1|D_{1,n}^1\right] \sim_{\mathcal{R}} A_0\,\left[V_1^1|V_2^1|B_{1,n}^1|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tag{1}$$

$$A_1\,\left[V_1^2|V_2^1|B_{1,n}^1|R_{1,n}^1|D_{1,n}^1\right]\sigma \sim_{\mathcal{R}} A_1\,\left[V_1^2|V_2^1|B_{1,n}^1|R_{1,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{2}$$

$$A_2\,\left[V_1^3|V_2^1|B_{1,n}^{1.1}|R_{1,n}^1|D_{1,n}^1\right]\sigma \sim_{\mathcal{R}} A_2\,\left[V_1^3|V_2^1|B_{1,n}^{1.1}|R_{1,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{3}$$

$$A_2\,\left[V_1^3|V_2^1|B_{1,n}^{1.2}|R_{1,n}^1|D_{1,n}^1\right]\sigma \sim_{\mathcal{R}} A_2\,\left[V_1^3|V_2^1|B_{1,n}^{1.2}|R_{1,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{4}$$

$$A_3\,\big[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^2|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_3\left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^2|\overline{D}_{1,n}^1\right]\tau \tag{5}$$

$$A_3\,\big[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^3|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_3\left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^3|\overline{D}_{1,n}^1\right]\tau \tag{6}$$

$$A_4\,\big[V_1^4|V_2^1|B_{1,n}^2|R_{1,n}^4|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_4\left[V_1^4|V_2^1|B_{1,n}^2|R_{1,n}^4|\overline{D}_{1,n}^1\right]\tau \tag{7}$$

$$A_5\,\big[V_1^4|V_2^1|B_{1,n}^3|R_{2,n}^1|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_5\left[V_1^4|V_2^1|B_{1,n}^3|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{8}$$

$$A_5\,\big[V_1^4|V_2^1|B_{1,n}^{3.1}|R_{2,n}^1|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_5\left[V_1^4|V_2^1|B_{1,n}^{3.1}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{9}$$

$$A_6\,\big[V_1^5|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_6\left[V_1^5|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{10}$$

$$A_7\,\big[V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_7\left[V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{11}$$

$$A_8\,\big[V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_8\left[V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{12}$$

$$A_8\,\big[V_1^8|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_8\left[V_1^8|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{13}$$

$$A_8\,\big[V_2^1|B_{2,n}^1|R_{2,n}^1|D_{1,n}^1\big]\,\sigma \sim_{\mathcal{R}} A_8\left[V_2^1|B_{2,n}^1|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau \tag{14}$$

$$A_9\,\big[V_2^2|B_{2,n}^1|R_{2,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_9\left[V_2^2|B_{2,n}^1|R_{2,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{15}$$

$$A_{10}\,\big[V_2^3|B_{2,n}^{1.1}|R_{2,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{10}\left[V_2^3|B_{2,n}^{1.1}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{16}$$

$$A_{10}\,\big[V_2^3|B_{2,n}^{1.2}|R_{2,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{10}\left[V_2^3|B_{2,n}^{1.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{17}$$

$$A_{11}\,\big[V_2^3|B_{2,n}^2|R_{2,n}^2|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{11}\left[V_2^3|B_{2,n}^2|R_{2,n}^2|\overline{D}_{1,n}^1\right]\Sigma_R \tag{18}$$

$$A_{11}\,\big[V_2^3|B_{2,n}^2|R_{2,n}^3|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{11}\left[V_2^3|B_{2,n}^2|R_{2,n}^3|\overline{D}_{1,n}^1\right]\Sigma_R \tag{19}$$

$$A_{12}\,\big[V_2^4|B_{2,n}^2|R_{2,n}^4|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{12}\left[V_2^4|B_{2,n}^2|R_{2,n}^4|\overline{D}_{1,n}^1\right]\Sigma_R \tag{20}$$

$$A_{13}\,\big[V_2^4|B_{2,n}^3|R_{3,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{13}\left[V_2^4|B_{2,n}^3|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{21}$$

$$A_{13}\,\big[V_2^4|B_{2,n}^{3.1}|R_{3,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{13}\left[V_2^4|B_{2,n}^{3.1}|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{22}$$

$$A_{14}\,\big[V_2^5|B_{2,n}^{3.2}|R_{3,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{14}\left[V_2^5|B_{2,n}^{3.2}|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{23}$$

$$A_{15}\,\big[V_2^6|B_{2,n}^{3.2}|R_{3,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_{15}\left[V_2^6|B_{2,n}^{3.2}|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{24}$$

$$A_3^1\,\big[V_2^7|B_{2,n}^{3.2}|R_{3,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_3^1\left[V_2^7|B_{2,n}^{3.2}|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{25}$$

$$A_3^1\,\big[V_2^8|B_{2,n}^{3.2}|R_{3,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_3^1\left[V_2^8|B_{2,n}^{3.2}|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{26}$$

($i \in \{3,\dots,n\}$, $R_{n+1,n}^1 = 0$)

$$A_i^1\,\big[B_{i,n}^1|R_{i,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_i^1\left[B_{i,n}^1|R_{i,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{27}$$

$$A_i^1\,\big[B_{i,n}^{1.1}\{{}^{M_i}/_{x_i}\}|R_{i,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_i^1\left[B_{i,n}^{1.1}\{{}^{M_i}/_{x_i}\}|R_{i,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{28}$$

$$A_i^2\,\big[B_{i,n}^{1.2}|R_{i,n}^1|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_i^2\left[B_{i,n}^{1.2}|R_{i,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{29}$$

$$A_i^3\,\big[B_{i,n}^2|R_{i,n}^2|D_{1,n}^1\big]\,\Sigma_L \sim_{\mathcal{R}} A_i^3\left[B_{i,n}^2|R_{i,n}^2|\overline{D}_{1,n}^1\right]\Sigma_R \tag{30}$$

$$A_i^3\left[B_{i,n}^2|R_{i,n}^3|D_{1,n}^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^3\left[B_{i,n}^2|R_{i,n}^3|\overline{D}_{1,n}^1\right]\Sigma_R \tag{31}$$

$$A_i^4\left[B_{i,n}^2|R_{i,n}^4|D_{1,n}^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^4\left[B_{i,n}^2|R_{i,n}^4|\overline{D}_{1,n}^1\right]\Sigma_R \tag{32}$$

$$A_i^5\left[B_{i,n}^3|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^5\left[B_{i,n}^3|R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{33}$$

$$A_i^5\left[B_{i,n}^{3.1}|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^5\left[B_{i,n}^{3.1}|R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{34}$$

$$A_i^6\left[B_{i,n}^{3.2}|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^6\left[B_{i,n}^{3.2}|R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{35}$$

($i \in \{1,\ldots,n\}, j \in \{3,\ldots,n\}$)

$$A_i'\left[B_{i,n}^4|D_{i,n}^1\right]\Sigma_L \sim_{\mathcal{R}} A_i'\left[B_{i,n}^4|\overline{D}_{i,n}^1\right]\Sigma_R \tag{36}$$

$$A_{n+1}'\left[D_{1,n}^2\right]\Sigma_L \sim_{\mathcal{R}} A_{n+1}'\left[\overline{D}_{1,n}^2\right]\Sigma_R \tag{37}$$

$$A_1''\left[D_{2,n}^2\right]\Sigma_L \sim_{\mathcal{R}} \overline{A}_1''\left[\overline{D}_{2,n}^2\right]\Sigma_R \tag{38}$$

$$A_{j-1}''\left[D_{j,n}^2\right]\Sigma_L \sim_{\mathcal{R}} \overline{A}_{j-1}''\left[\overline{D}_{j,n}^2\right]\Sigma_R \tag{39}$$

$$A_n''\left[0\right]\Sigma_L \sim_{\mathcal{R}} \overline{A}_n''\left[0\right]\Sigma_R \tag{40}$$

($i \in \{3,\ldots,n\}$)

$$A_i^1\left[\{^{M_i}/_{x_i}\}|R_{i,n}^1|D_{1,n}^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^1\left[\{^{M_i}/_{x_i}\}|R_{i,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R \tag{41}$$

B.3 Useful lemmas

Let us introduce useful lemmas which will be used to prove that the constructed relation satisfies the property of Definition 2.

Definition 5. *Let $id \in \{id_1,\ldots,id_n\}$. A term N is said to be a* id - valid ballot *if $\phi_{\mathsf{b}}(id,N) = \mathsf{true}$, equivalently :*

$$\left\{\begin{array}{rcl} N & = & (N_1,N_2,N_3) \\ \mathsf{checksign}((N_1,N_2),\mathsf{vk}(id),N_3) & =_E & \mathsf{Ok} \\ \mathsf{checkpfk}_1(\mathsf{vk}(id),N_1,N_2) & =_E & \mathsf{Ok} \end{array}\right. .$$

Lemma 28. *Let N be a id-valid ballot, thus $N = (N_1,N_2,N_3)$. Let*

$$\begin{array}{llll} N_{renc} & = \mathsf{renc}(N_1,a_2), & N_{blind} & = \mathsf{blind}(N_{renc},\mathsf{s}(id)), \\ N_{hash} & = \mathsf{hash}((\mathsf{vk}(id),N_1,N_2,N_3)), & N' & = (N,N_{renc},N_{pfk}^1,N_{blind},N_{pfk}^2). \\ N_{pfk}^1 & = \mathsf{pfk}_2(idp,a_2,N_1,N_{renc}), & N_{pfk}^2 & = \mathsf{pfk}_2(idp,\mathsf{s}(id),N_{renc},N_{blind}), \\ R_{sign} & = \mathsf{sign}(N_{hash},id_R) & & \end{array}$$

Then we have $\phi_{\mathsf{b}}(idp,N) =_E \phi_{\mathsf{r}}(idp,N') =_E \phi_{\mathsf{s}}(idp_R,N_{hash},R_{sign}) =_E \mathsf{true}$ with $idp = \mathsf{vk}(id)$.

Proof. Let N be a id-valid ballot. By definition, we have that $\phi_{\mathsf{b}}(id,N) = \mathsf{true}$. According to the definition of N', we have that $N' = (N_1',N_2',N_3',N_4',N_5')$ with $N_1' = N = (N_1,N_2,N_3)$. Moreover, we know that $\mathsf{checkpfk}_1(idp,N_1,N_2) =_E \mathsf{checksign}((N_1,N_2),idp,N_3) =_E \mathsf{Ok}$ since $\phi_{\mathsf{b}}(idp,N) = \mathsf{true}$. In addition, we have :

$$\begin{aligned}
&\mathsf{checkpfk}_2(idp, N'_2, N'_3) =_E \mathsf{checkpfk}_2(\mathsf{vk}(id), N_{renc}, N^1_{pfk})\\
&\qquad =_E \mathsf{checkpfk}_2(\mathsf{vk}(id), \mathsf{renc}(N_1, a_2), \mathsf{pfk}_2(idp, a_2, N_1, \mathsf{renc}(N_1, a_2)))\\
&\qquad =_E \mathsf{Ok}
\end{aligned}$$

and

$$\begin{aligned}
&\mathsf{checkpfk}_2(idp, N'_4, N'_5) =_E \mathsf{checkpfk}_2(\mathsf{vk}(id), N_{blind}, N^2_{pfk})\\
&\qquad =_E \mathsf{checkpfk}_2(\mathsf{vk}(id), N_{blind}, \mathsf{pfk}_2(\mathsf{vk}(id), \mathsf{s}(id), N_{renc}, N_{blind}))\\
&\qquad \text{where } N_{blind} = \mathsf{blind}(N_{renc}, \mathsf{s}(id))\\
&\qquad =_E \mathsf{Ok}.
\end{aligned}$$

Then, we have $\phi_{\mathsf{r}}(idp, N') = \mathsf{true}$. Finally, we have :

$$\begin{aligned}
\mathsf{checksign}(N_{hash}, idp_R, R_{sign}) &=_E \mathsf{checksign}(N_{hash}, idp_R, \mathsf{sign}(N_{hash}, id_R))\\
&=_E \mathsf{Ok}
\end{aligned}$$

which prove that $\phi_{\mathsf{s}}(idp_R, N_{hash}, R_{sign}) = \mathsf{true}$. □

Lemma 29. *Let N be a term such that, for some N_{rand} :*

$$\begin{aligned}
N &= (N_1, N_2, N_3)\\
N_1 &= \mathsf{penc}(v, N_{rand}, \mathsf{pk}(a_1))\\
N_2 &= \mathsf{pfk}_1(id, N_{rand}, v, N_1)\\
N_3 &= \mathsf{sign}((N_1, N_2), id).
\end{aligned}$$

Let $R_{rec} = \mathsf{dec}(N_{blind}, a_3)$, with N_{blind}, R_{sign} and N_{hash} the same as in Lemma 28. Then, N is a id-valid ballot and we have :

$$\phi_{\mathsf{v}}(idp_R, id, N_{hash}, R_{sign}, v, N_{rec}) = \mathsf{true}.$$

Proof. Let N be this term. Then, N clearly satisfies Definition 5, and :

$$\begin{aligned}
&\mathsf{unblind}(\mathsf{dec}(N_{blind}, a_3), \mathsf{s}(id)) =_E \mathsf{unblind}(\mathsf{dec}(\mathsf{blind}(N_{renc}, \mathsf{s}(id)), a_3), \mathsf{s}(id))\\
&\qquad = \mathsf{unblind}(\mathsf{dec}(\mathsf{blind}(\mathsf{renc}(N_1, a_2), \mathsf{s}(id)), a_3), \mathsf{s}(id))\\
&\qquad = \mathsf{unblind}(\mathsf{dec}(\mathsf{blind}(\mathsf{renc}(\mathsf{penc}(v, N_{rand}, \mathsf{pk}(a_1)), a_2), \mathsf{s}(id)), a_3), \mathsf{s}(id))\\
&\qquad \overset{(6)}{=_E} \mathsf{unblind}(\mathsf{dec}(\mathsf{blind}(\mathsf{penc}(v, N_{rand}, \mathsf{pk}(a_1 + a_2)), \mathsf{s}(id)), a_3), \mathsf{s}(id))\\
&\qquad = \mathsf{unblind}(\mathsf{dec}(\mathsf{blind}(\mathsf{penc}(v, N_{rand}, \mathsf{pk}(a_3)), \mathsf{s}(id)), a_3), \mathsf{s}(id))\\
&\qquad \overset{(4)}{=_E} \mathsf{unblind}(\mathsf{blind}(v, \mathsf{s}(id)), \mathsf{s}(id)\\
&\qquad \overset{(7)}{=_E} v.
\end{aligned}$$

Moreover :

$$\begin{aligned}
\mathsf{checksign}(N_{hash}, idp_R, R_{sign}) &=_E \mathsf{checksign}(N_{hash}, idp_R, \mathsf{sign}(N_{hash}, id_R))\\
&=_E \mathsf{Ok}
\end{aligned}$$

which prove that $\phi_{\mathsf{v}}(idp_R, id, N_{hash}, R_{sign}, v, N_{rec}) = \mathsf{true}$. □

B.4 Proof for the relation

Let us prove that $\mathcal{R}$ satisfies the three properties of Definition 2.

Internal Reductions : We must show for all extended processes A and B, where $A \mathcal{R} B$, that if $A \longrightarrow A'$ for some A', then $B \longrightarrow B'$ and $A' \mathcal{R} B'$ for some B'. We observe that if $A \mathcal{R} B$ by (1), (10), (11), (14), (23), (24), (27), (31), (34), (35) or (37) to (40) then there is no extended process A' such that $A \longrightarrow A'$. We proceed by case analysis on the remaining cases.

(2) We have

$$A \equiv A_1 \left[V_1^2|V_2^1|B_{1,n}^1|R_{1,n}^1|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_1 \left[V_1^2|V_2^1|B_{1,n}^1|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_1 \left[\overline{c_1}\langle ball_1\rangle.V_1^3|V_2^1|c_1(x_1).B_{1,n}^{1.1}|R_{1,n}^1|D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.1}|R_{1,n}^1|D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_1 \left[\overline{c_1}\langle ball_1\rangle.V_1^3|V_2^1|c_1(x_1).B_{1,n}^{1.1}|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau$$

that $B \longrightarrow B'$ where

$$B^{'} = A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.1}|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

Since

$$A' = A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.1}|R_{1,n}^1|D_{1,n}^1\right] \sigma \ \mathcal{R} \ B',$$

we derive $A' \mathcal{R} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(3) We have

$$A \equiv A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.1}|R_{1,n}^1|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.1}|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_2 \left[V_1^3|V_2^1|\text{if } \phi_{\mathsf{b}}(idp_1, x_1) \text{ then } B_{1,n}^{1.2} \text{ else } 0|R_{1,n}^1|D_{1,n}^1\right] \sigma.$$

Since x_1 refers to $ball_1$, it follows from Lemma 29 applied to $ball_1\sigma$ that it is a id_1-valid ballot and from Lemma 28 that $\phi_{\mathsf{b}}(idp_1, x_1)\{^{ball_1}/_{x_1}\}\sigma = \mathsf{true}$ and

$$A' \equiv A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.2}|R_{1,n}^1|D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_2 \left[V_1^3|V_2^1|\text{if } \phi_{\mathsf{b}}(idp_1, x_1) \text{ then } B_{1,n}^{1.2} \text{ else } 0|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau$$

and from Lemma 29 and Lemma 28 applied to $ball_1\tau$, since $\phi_{\mathsf{b}}(idp_1, x_1)$ $\{^{ball_1}/_{x_1}\}\tau = \mathsf{true}$, that $B \longrightarrow B'$ where

$$B^{'} = A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.2}|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

Since

$$A' \equiv A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.2}|R_{1,n}^1|D_{1,n}^1\right] \sigma \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(4) We have

$$A \equiv A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.2}|R_{1,n}^1|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_2 \left[V_1^3|V_2^1|B_{1,n}^{1.2}|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_2 \left[V_1^3|V_2^1|\overline{c_{BR}}\langle ball_1' \rangle.B_{1,n}^2|c_{BR}(p_1).R_{1,n}^2|D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^2|D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_2 \left[V_1^3|V_2^1|\overline{c_{BR}}\langle ball_1' \rangle.B_{1,n}^2|c_{BR}(p_1).R_{1,n}^2|\overline{D}_{1,n}^1\right] \tau$$

that $B \longrightarrow B'$ where

$$B^{'} = A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^2|\overline{D}_{1,n}^1\right] \tau.$$

Since

$$A' = A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^2|D_{1,n}^1\right] \sigma \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(5) We have

$$A \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^2|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^2|\overline{D}_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|\text{if } \phi_{\mathsf{r}}(idp_1, p_1) \text{ then } R_{1,n}^3 \text{ else } 0|D_{1,n}^1\right] \sigma$$

and it follows from Lemma 28, since $ball_1\sigma$ is verifying Lemma 29, that $\phi_{\mathsf{r}}(idp_1, p_1)\{^{ball_1}/_{x_1}, {}^{ball_1'}/_{p_1}\}\sigma = \mathsf{true}$, thus

$$A' \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^3|D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|\text{if } \phi_{\mathsf{r}}(idp_1, p_1) \text{ then } R_{1,n}^3 \text{ else } 0|\overline{D}_{1,n}^1\right] \tau$$

and Lemma 28 and Lemma 29 applied to $ball_1\tau$ that $\phi_{\mathsf{r}}(idp_1, p_1)\{^{ball_1}/_{x_1}, {}^{ball_1'}/_{p_1}\}\tau = \mathsf{true}$ thus $B \longrightarrow B'$ where

$$B^{'} = A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^3|\overline{D}_{1,n}^1\right] \tau.$$

Since

$$A' = A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^3|D_{1,n}^1\right] \sigma \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(6) We have

$$A \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^3|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_3 \left[V_1^3|V_2^1|B_{1,n}^2|R_{1,n}^3|\overline{D}_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_3 \left[c_{RV_1}(rec_1).V_1^4|V_2^1|B_{1,n}^2|\overline{c_{RV_1}}\langle r_1\rangle.R_{1,n}^4|D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_4 \left[V_1^4|V_2^1|B_{1,n}^2|R_{1,n}^4|D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_3 \left[c_{RV_1}(rec_1).V_1^4|V_2^1|B_{1,n}^2|\overline{c_{RV_1}}\langle r_1\rangle.R_{1,n}^4|\overline{D}_{1,n}^1\right] \tau$$

that $B \longrightarrow B'$ where

$$B^{'} = A_4 \left[V_1^4|V_2^1|B_{1,n}^2|R_{1,n}^4|\overline{D}_{1,n}^1\right] \tau$$

. Since

$$A' = A_4 \left[V_1^4|V_2^1|B_{1,n}^2|R_{1,n}^4|D_{1,n}^1\right] \sigma \ \mathcal{R} \ B'$$

, we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(7) We have

$$A \equiv A_4 \left[V_1^4|V_2^1|B_{1,n}^2|R_{1,n}^4|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_4 \left[V_1^4|V_2^1|B_{1,n}^2|R_{1,n}^4|\overline{D}_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_4 \left[V_1^4|V_2^1|c_{BR}(q_1).B_{1,n}^3|\overline{c_{BR}}\langle sig_1^R\rangle.R_{2,n}^1|D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_5 \left[V_1^4|V_2^1|B_{1,n}^3|R_{2,n}^1|D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_4 \left[V_1^4|V_2^1|c_{BR}(q_1).B_{1,n}^3|\overline{c_{BR}}\langle sig_1^R\rangle.R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau$$

that $B \longrightarrow B'$ where

$$B^{'} = A_5 \left[V_1^4|V_2^1|B_{1,n}^3|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

Since

$$A' = A_5 \left[V_1^4|V_2^1|B_{1,n}^3|R_{2,n}^1|D_{1,n}^1\right] \sigma \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(8) We have

$$A \equiv A_5 \left[V_1^4|V_2^1|B_{1,n}^3|R_{2,n}^1|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_5 \left[V_1^4|V_2^1|B_{1,n}^3|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_5\left[V_1^4|V_2^1|\text{if } \phi_{\mathsf{s}}(idp_R, q_1) \text{ then } B_{1,n}^{3.1} \text{ else } 0|R_{2,n}^1|D_{1,n}^1\right]\sigma$$

and it follows from Lemma 28 and Lemma 29 applied to $ball_1\sigma$ that $\phi_{\mathsf{s}}(idp_R, q_1)\ \{^{ball_1}/_{x_1}, {}^{ball'_1}/_{p_1}, {}^{sig_1^R}/_{q_1}\}\sigma = \mathsf{true}$ and

$$A' \equiv A_5\left[V_1^4|V_2^1|B_{1,n}^{3.1}|R_{2,n}^1|D_{1,n}^1\right]\sigma.$$

It follows from

$$B \equiv A_5\left[V_1^4|V_2^1|\text{if } \phi_{\mathsf{s}}(idp_R, q_1) \text{ then } B_{1,n}^{3.1} \text{ else } 0|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau$$

and from Lemma 28 and Lemma 29 applied to $ball_1\tau$ that $\phi_{\mathsf{s}}(idp_R, q_1)\{^{ball_1}/_{x_1}, {}^{ball'_1}/_{p_1}, {}^{sig_1^R}/_{q_1}\}\tau = \mathsf{true}$ and $B \longrightarrow B'$ where

$$B^{'} = A_5\left[V_1^4|V_2^1|B_{1,n}^{3.1}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau.$$

Since

$$A' = A_5\left[V_1^4|V_2^1|B_{1,n}^{3.1}|R_{2,n}^1|D_{1,n}^1\right]\sigma\ \mathcal{R}\ B',$$

we derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(9) We have

$$A \equiv A_5\left[V_1^4|V_2^1|B_{1,n}^{3.1}|R_{2,n}^1|D_{1,n}^1\right]\sigma \text{ and } B \equiv A_5\left[V_1^4|V_2^1|B_{1,n}^{3.1}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_5\left[c_1(con_1).V_1^5|V_2^1|\overline{c_1}\langle q_1\rangle.B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right]\sigma$$

and

$$A' \equiv A_6\left[V_1^5|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right]\sigma.$$

It follows from

$$B \equiv A_5\left[c_1(con_1).V_1^5|V_2^1|\overline{c_1}\langle q_1\rangle.B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau$$

that $B \longrightarrow B'$ where

$$B^{'} = A_6\left[V_1^5|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau.$$

Since

$$A' = A_6\left[V_1^5|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right]\sigma\ \mathcal{R}\ B',$$

we derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(12) We have

$$A \equiv A_8\left[V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right]\sigma \text{ and } B \equiv A_8\left[V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right]\tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_8 \left[\text{if } \phi_{\mathsf{v}}(idp_R, id_1, hv_1, con_1, x_1^{vote}, rec_1) \text{ then } V_1^8 \text{ else } 0 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | D_{1,n}^1\right] \sigma$$

and it follows from Lemma 29 applied to $ball_1\sigma$ that $\phi_{\mathsf{v}}(idp_R, id_1, hv_1, con_1, x_1^{vote}, rec_1)\{^{ball_1}/_{x_1}, ^{ball'_1}/_{p_1}, ^{sig_1^R}/_{q_1}, ^{r_1}/_{rec_1}, ^{q_1}/_{con_1}\}\sigma = \mathsf{true}$ and

$$A' \equiv A_8 \left[V_1^8 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_8 \left[\text{if } \phi_{\mathsf{v}}(idp_R, id_1, hv_1, con_1, x_1^{vote}, rec_1) \text{ then } V_1^8 \text{ else } 0 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | \overline{D}_{1,n}^1\right] \tau$$

and the Lemma 29 applied to $ball_1\tau$ that $\phi_{\mathsf{v}}(idp_R, id_1, hv_1, con_1, x_1^{vote}, rec_1)$ $\{^{ball_1}/_{x_1}, ^{ball'_1}/_{p_1}, ^{sig_1^R}/_{q_1}, ^{r_1}/_{rec_1}, ^{q_1}/_{con_1}\}\tau = \mathsf{true}$ and $B \longrightarrow B'$ where

$$B^{'} = A_8 \left[V_1^8 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | \overline{D}_{1,n}^1\right] \tau.$$

Since

$$A' = A_8 \left[V_1^8 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | D_{1,n}^1\right] \sigma \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(13) We have

$$A \equiv A_8 \left[V_1^8 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | D_{1,n}^1\right] \sigma \text{ and } B \equiv A_8 \left[V_1^8 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | D_{1,n}^1\right] \tau.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_8 \left[\overline{c_1}\langle \mathsf{Ok} \rangle | V_2^1 | c_1(sy_1).B_{2,n}^1 | R_{2,n}^1 | D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_8 \left[V_2^1 | B_{2,n}^1 | R_{2,n}^1 | D_{1,n}^1\right] \sigma.$$

It follows from

$$B \equiv A_8 \left[\overline{c_1}\langle \mathsf{Ok} \rangle | V_2^1 | c_1(sy_1).B_{2,n}^1 | R_{2,n}^1 | \overline{D}_{1,n}^1\right] \tau$$

that $B \longrightarrow B'$ where

$$B^{'} = A_8 \left[V_2^1 | B_{2,n}^1 | R_{2,n}^1 | \overline{D}_{1,n}^1\right] \tau.$$

Since

$$A' = A_8 \left[V_2^1 | B_{2,n}^1 | R_{2,n}^1 | D_{1,n}^1\right] \sigma \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(15) We have

$$A \equiv A_9 \left[V_2^2 | B_{2,n}^1 | R_{2,n}^1 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_9 \left[V_2^2 | B_{2,n}^1 | R_{2,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_9 \left[\overline{c_2}\langle ball_2\rangle.V_2^3|c_2(x_2).B_{2,n}^{1.1}|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_{10} \left[V_2^3|B_{2,n}^{1.1}|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L.$$

It follows from

$$B \equiv A_9 \left[\overline{c_2}\langle ball_2\rangle.V_2^3|c_2(x_2).B_{2,n}^{1.1}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_{10} \left[V_2^3|B_{2,n}^{1.1}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R.$$

Since

$$A' = A_{10} \left[V_2^3|B_{2,n}^{1.1}|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B'$$

, we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(16) We have

$$A \equiv A_{10} \left[V_2^3|B_{2,n}^{1.1}|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_{10} \left[V_2^3|B_{2,n}^{1.1}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{10} \left[V_2^3|\text{if } \phi_{\mathsf{b}}(idp_2, x_2) \text{ then } B_{2,n}^{1.2} \text{ else } 0|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L.$$

Since x_2 refers to $ball_2$, it follows from Lemma 29 applied to $ball_2\Sigma_L$ that it is a id_2-valid ballot and from Lemma 28 that $\phi_{\mathsf{b}}(idp_2, x_2)\{^{ball_2}/_{x_2}\}\Sigma_L = \mathsf{true}$ and

$$A' \equiv A_{10} \left[V_2^3|B_{2,n}^{1.2}|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L.$$

It follows from

$$B \equiv A_{10} \left[V_2^3|\text{if } \phi_{\mathsf{b}}(idp_2, x_2) \text{ then } B_{2,n}^{1.2} \text{ else } 0|R_{2,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R$$

and from Lemma 29 and Lemma 28 applied to $ball_2\Sigma_R$, since $\phi_{\mathsf{b}}(idp_2, x_2)$ $\{^{ball_2}/_{x_2}\}\Sigma_R = \mathsf{true}$, that $B \longrightarrow B'$ where

$$B^{'} = A_{10} \left[V_2^3|B_{2,n}^{1.2}|R_{1,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R.$$

Since

$$A' \equiv A_{10} \left[V_2^3|B_{2,n}^{1.2}|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(17) We have

$$A \equiv A_{10} \left[V_2^3|B_{2,n}^{1.2}|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_{10} \left[V_2^3|B_{2,n}^{1.2}|R_{1,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{10}\left[V_2^3|\overline{c_{BR}}\langle \mathit{ball}'_2\rangle.B^2_{2,n}|c_{BR}(p_2).R^2_{2,n}|D^1_{1,n}\right]\Sigma_L$$

and

$$A' \equiv A_{11}\left[V_2^3|B^2_{2,n}|R^2_{2,n}|D^1_{1,n}\right]\Sigma_L.$$

It follows from

$$B \equiv A_{10}\left[V_2^3|\overline{c_{BR}}\langle \mathit{ball}'_2\rangle.B^2_{2,n}|c_{BR}(p_2).R^2_{2,n}|\overline{D}^1_{1,n}\right]\Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_{11}\left[V_2^3|B^2_{2,n}|R^2_{2,n}|\overline{D}^1_{1,n}\right]\Sigma_R.$$

Since

$$A' = A_{11}\left[V_2^3|B^2_{2,n}|R^2_{2,n}|D^1_{1,n}\right]\Sigma_L \;\mathcal{R}\; B',$$

we derive $A' \;\mathcal{R}\; B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(18) We have

$$A \equiv A_{11}\left[V_2^3|B^2_{2,n}|R^2_{2,n}|D^1_{1,n}\right]\Sigma_L \text{ and } B \equiv A_{11}\left[V_2^3|B^2_{2,n}|R^2_{2,n}|\overline{D}^1_{1,n}\right]\Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{11}\left[V_2^3|B^2_{2,n}|\text{if } \phi_{\mathsf{r}}(\mathit{idp}_2, p_2) \text{ then } R^3_{2,n} \text{ else } 0|D^1_{1,n}\right]\Sigma_L$$

and it follows from Lemma 28, since $\mathit{ball}_2\Sigma_L$ is verifying Lemma 29, that $\phi_{\mathsf{r}}(\mathit{idp}_2, p_2)\{^{\mathit{ball}_2}/_{x_2}, ^{\mathit{ball}'_2}/_{p_2}\}\sigma = \mathsf{true}$, thus

$$A' \equiv A_{11}\left[V_2^3|B^2_{2,n}|R^3_{2,n}|D^1_{1,n}\right]\Sigma_L.$$

It follows from

$$B \equiv A_{11}\left[V_2^3|B^2_{2,n}|\text{if } \phi_{\mathsf{r}}(\mathit{idp}_2, p_2) \text{ then } R^3_{2,n} \text{ else } 0|\overline{D}^1_{1,n}\right]\Sigma_R$$

and Lemma 28 and Lemma 29 applied to $\mathit{ball}_2\Sigma_R$ that $\phi_{\mathsf{r}}(\mathit{idp}_2, p_2)\{^{\mathit{ball}_2}/_{x_2}, ^{\mathit{ball}'_2}/_{p_2}\}\Sigma_R = \mathsf{true}$ thus $B \longrightarrow B'$ where

$$B^{'} = A_{11}\left[V_2^3|B^2_{2,n}|R^3_{2,n}|\overline{D}^1_{1,n}\right]\Sigma_L.$$

Since

$$A' = A_{11}\left[V_2^3|B^2_{2,n}|R^3_{2,n}|D^1_{1,n}\right]\Sigma_L \;\mathcal{R}\; B',$$

we derive $A' \;\mathcal{R}\; B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(19) We have

$$A \equiv A_{11}\left[V_2^3|B^2_{2,n}|R^3_{2,n}|D^1_{1,n}\right]\Sigma_L \text{ and } B \equiv A_{11}\left[V_2^3|B^2_{2,n}|R^3_{2,n}|\overline{D}^1_{1,n}\right]\Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{11}\left[c_{RV_2}(rec_2).V_2^4|B_{2,n}^2|\overline{c_{RV_2}}\langle r_2\rangle.R_{2,n}^4|D_{1,n}^1\right]\Sigma_L$$

and

$$A' \equiv A_{12}\left[V_2^4|B_{2,n}^2|R_{2,n}^4|D_{1,n}^1\right]\Sigma_L.$$

It follows from

$$B \equiv A_{11}\left[c_{RV_2}(rec_2).V_2^4|B_{2,n}^2|\overline{c_{RV_2}}\langle r_2\rangle.R_{2,n}^4|\overline{D}_{1,n}^1\right]\Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_{12}\left[V_2^4|B_{2,n}^2|R_{2,n}^4|\overline{D}_{1,n}^1\right]\Sigma_R.$$

Since

$$A' = A_{12}\left[V_2^4|B_{2,n}^2|R_{2,n}^4|D_{1,n}^1\right]\Sigma_L \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(20) We have

$$A \equiv A_{12}\left[V_2^4|B_{2,n}^2|R_{2,n}^4|D_{1,n}^1\right]\Sigma_L \text{ and } B \equiv A_{12}\left[V_2^4|B_{2,n}^2|R_{2,n}^4|\overline{D}_{1,n}^1\right]\Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{12}\left[V_2^4|c_{BR}(q_2).B_{2,n}^3|\overline{c_{BR}}\langle sig_2^R\rangle.R_{3,n}^1|D_{1,n}^1\right]\Sigma_L$$

and

$$A' \equiv A_{13}\left[V_2^4|B_{2,n}^3|R_{3,n}^1|D_{1,n}^1\right]\Sigma_L.$$

It follows from

$$B \equiv A_{12}\left[V_2^4|c_{BR}(q_2).B_{2,n}^3|\overline{c_{BR}}\langle sig_2^R\rangle.R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_{13}\left[V_2^4|B_{2,n}^3|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R.$$

Since

$$A' = A_{13}\left[V_2^4|B_{2,n}^3|R_{3,n}^1|D_{1,n}^1\right]\Sigma_L \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(21) We have

$$A \equiv A_{13}\left[V_2^4|B_{2,n}^3|R_{3,n}^1|D_{1,n}^1\right]\Sigma_L \text{ and } B \equiv A_{13}\left[V_2^4|B_{2,n}^3|R_{3,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{13}\left[V_2^4|\text{if } \phi_{\mathsf{s}}(idp_R, q_2) \text{ then } B_{2,n}^{3.1} \text{ else } 0|R_{3,n}^1|D_{1,n}^1\right]\Sigma_L$$

and it follows from Lemma 28 and Lemma 29 applied to $ball_2\Sigma_L$ that $\phi_{\mathsf{s}}(idp_R, q_2)\{^{ball_2}/_{x_2}, ^{ball_2'}/_{p_2}, ^{sig_2^R}/_{q_2}\}\Sigma_L = \mathsf{true}$ and

$$A' \equiv A_{13}\left[V_2^4 | B_{2,n}^{3.1} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L.$$

It follows from

$$B \equiv A_{13}\left[V_2^4 | \text{if } \phi_{\mathsf{s}}(idp_R, q_2) \text{ then } B_{2,n}^{3.1} \text{ else } 0 | R_{3,n}^1 | \overline{D}_{1,n}^1\right]\Sigma_R$$

and Lemma 28 and Lemma 29 applied to $ball_2\Sigma_R$ that $\phi_{\mathsf{s}}(idp_R, q_2)\{^{ball_2}/_{x_2}, ^{ball_2'}/_{p_2}, ^{sig_2^R}/_{q_2}\}\Sigma_R = \mathsf{true}$ and $B \longrightarrow B'$ where

$$B^{'} = A_{13}\left[V_2^4 | B_{2,n}^{3.1} | R_{3,n}^1 | \overline{D}_{1,n}^1\right]\Sigma_R.$$

Since

$$A' = A_{13}\left[V_2^4 | B_{2,n}^{3.1} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(22) We have

$$A \equiv A_{13}\left[V_2^4 | B_{2,n}^{3.1} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L \text{ and } B \equiv A_{13}\left[V_2^4 | B_{2,n}^{3.1} | R_{3,n}^1 | \overline{D}_{1,n}^1\right]\Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{13}\left[c_2(con_2).V_2^5 | \overline{c_2}\langle q_2\rangle.B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L$$

and

$$A' \equiv A_{14}\left[V_2^5 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L.$$

It follows from

$$B \equiv A_{13}\left[c_2(con_2).V_2^5 | \overline{c_2}\langle q_2\rangle.B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right]\Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_{14}\left[V_2^5 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right]\Sigma_R.$$

Since

$$A' = A_{14}\left[V_2^5 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(25) We have

$$A \equiv A_3^1\left[V_2^7 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L \text{ and } B \equiv A_3^1\left[V_2^7 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right]\Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_3^1\left[\text{if } \phi_{\mathsf{v}}(idp_R, id_2, hv_2, con_2, x_2^{vote}, rec_2) \text{ then } V_2^8 \text{ else } 0 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right]\Sigma_L$$

and it follows from Lemma 29 applied to $ball_2\Sigma_L$ that $\phi_{\mathsf{v}}(idp_R, id_2, hv_2, con_2, x_2^{vote}, rec_2)\{{}^{ball_2}/_{x_2}, {}^{ball'_2}/_{p_2}, {}^{sig_2^R}/_{q_2}, {}^{r_2}/_{rec_2}, {}^{q_2}/_{con_2}\}\Sigma_L = \mathsf{true}$ and

$$A' \equiv A_3^1 \left[V_2^8 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L.$$

It follows from

$$B \equiv A_3^1 \left[\text{if } \phi_{\mathsf{v}}(idp_R, id_2, hv_2, con_2, x_2^{vote}, rec_2) \text{ then } V_2^8 \text{ else } 0 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R$$

and the Lemma 29 applied to $ball_2\Sigma_R$ that $\phi_{\mathsf{v}}(idp_R, id_2, hv_2, con_2, x_2^{vote}, rec_2)$ $\{{}^{ball_2}/_{x_2}, {}^{ball'_2}/_{p_2}, {}^{sig_2^R}/_{q_2}, {}^{r_2}/_{rec_2}, {}^{q_2}/_{con_2}\}\Sigma_R = \mathsf{true}$ and $B \longrightarrow B'$ where

$$B^{'} = A_3^1 \left[V_2^8 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

Since

$$A' = A_3^1 \left[V_2^8 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(26) We have

$$A \equiv A_3^1 \left[V_2^8 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_3^1 \left[V_2^8 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_3^1 \left[\overline{c_2}\langle \mathsf{Ok}\rangle | c_2(sy_2).B_{3,n}^1 | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_3^1 \left[B_{3,n}^1 | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L.$$

It follows from

$$B \equiv A_3^1 \left[\overline{c_2}\langle \mathsf{Ok}\rangle | c_2(sy_2).B_{3,n}^1 | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_3^1 \left[B_{3,n}^1 | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

Since

$$A' = A_3^1 \left[B_{3,n}^1 | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(28) We have

$$A \equiv A_i^1 \left[B_{i,n}^{1.1}\{{}^{M_i}/_{x_i}\} | R_{i,n}^1 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_i^1 \left[B_{i,n}^{1.1}\{{}^{M_i}/_{x_i}\} | R_{i,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_{i-1}$ such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ are id$_k$-valid ballots for $k = 3 \ldots i-1$, and a term M_i such that

$$\text{fv}(M_i) \cup \bigcup_{3 \leq j \leq i-1} \text{fv}(N_j) \subseteq \text{dom}(A_i^1) \text{ and } (\text{fn}(M_i) \cup \bigcup_{3 \leq j \leq i-1} \text{fn}(N_j)) \cap \text{bn}(A_i^1) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_i^1 \left[\text{if } \phi_{\mathsf{b}}(idp_i, x_i)\{^{M_i}/_{x_i}\} \text{ then } P \text{ else } 0|R^1_{i,n}|D^1_{1,n}\right] \Sigma_L$$

with $P = B^{1.2}_{i,n}$. We also have

$$B \equiv A_i^1 \left[\text{if } \phi_{\mathsf{b}}(idp_i, x_i)\{^{M_i}/_{x_i}\} \text{ then } P \text{ else } 0|R^1_{i,n}|\overline{D}^1_{1,n}\right] \Sigma_R.$$

We proceed by case analysis on the structure of A':

- If $A' \equiv A_i^2 \left[P|R^1_{i,n}|D^1_{1,n}\right] \Sigma_L$, then $M_i\theta_{i-1}\sigma_{\tilde{N}}^{i-1}\Sigma_L$, which is equal to $x_i\Sigma_L$ in the A_i^1 context, must have passed $\phi_{\mathsf{b}}^{id_i}$, is a id$_i$-valid ballot. From Corollary 21, since we deduce that $x_i\Sigma_R$, in the A_i^1 context, is also a valid ballot and then $B \longrightarrow B' = A_i^2 \left[B^{1.2}_{i,n}|R^1_{i,n}|\overline{D}^1_{1,n}\right] \Sigma_R$. Since $A' \equiv A_i^2 \left[B^{1.2}_{i,n}|R^1_{i,n}|D^1_{1,n}\right] \Sigma_L \ \mathcal{R} \ B'$, we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

- If $A' \equiv A_i^1 \left[0\{^{M_i}/_{x_i}\}|R^1_{i,n}|D^1_{1,n}\right] \Sigma_L$, then $x_i\Sigma_L$, in the A_i^1 context, must not have passed $\phi_{\mathsf{b}}^{id_i}$, then $x_i\Sigma_L$ is not id$_i$-valid ballot. From Corollary 21, we deduce that $x_i\Sigma_R$ is not a valid ballot either and then $B \longrightarrow B' = A_i^1 \left[0\{^{M_i}/_{x_i}\}|R^1_{i,n}|\overline{D}^1_{1,n}\right] \Sigma_R$. Since $A' \equiv A_i^1 [0$ $\{^{M_i}/_{x_i}\}|R^1_{i,n}|D^1_{1,n}] \Sigma_L \ \mathcal{R} \ B'$, we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(29) We have

$$A \equiv A_i^2 \left[B^{1.2}_{i,n}|R^1_{i,n}|D^1_{1,n}\right] \Sigma_L \text{ and } B \equiv A_i^2 \left[B^{1.2}_{i,n}|R^1_{i,n}|\overline{D}^1_{1,n}\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_i$ such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ are id$_k$-valid ballots for $k = 3 \ldots i$, and such that

$$\bigcup_{3\leq j\leq i} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_i^1) \text{ and } \bigcup_{3\leq j\leq i} \mathrm{fn}(N_j)) \cap \mathrm{bn}(A_i^1) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_i^2 \left[\overline{c_{BR}}\langle ball'_i\rangle.B^2_{i,n}|c_{BR}(p_i).R^2_{i,n}|D^1_{1,n}\right] \Sigma_L$$

and

$$A' \equiv A_i^3 \left[B^2_{i,n}|R^2_{i,n}|D^1_{1,n}\right] \Sigma_L.$$

It follows from

$$B \equiv A_i^2 \left[\overline{c_{BR}}\langle ball'_i\rangle.B^2_{i,n}|c_{BR}(p_i).R^2_{i,n}|\overline{D}^1_{1,n}\right] \Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_i^3 \left[B^2_{i,n}|R^2_{i,n}|\overline{D}^1_{1,n}\right] \Sigma_R.$$

Since

$$A' \equiv A_i^3 \left[B_{i,n}^2 | R_{i,n}^2 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(30) We have

$$A \equiv A_i^3 \left[B_{i,n}^2 | R_{i,n}^2 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_i^3 \left[B_{i,n}^2 | R_{i,n}^2 | \overline{D}_{1,n}^1\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_i$ such that $N_k \theta_{k-1} \sigma_{\tilde{N}}^{k-1} \Sigma_L$ are id_k-valid ballots for $k = 3 \ldots i$, and such that

$$\bigcup_{3 \leq j \leq i} \text{fv}(N_j) \subseteq \text{dom}(A_i^1) \text{ and } \bigcup_{3 \leq j \leq i} \text{fn}(N_j)) \cap \text{bn}(A_i^1) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_i^3 \left[B_{i,n}^2 | \text{if } \phi_{\mathsf{r}}(idp_i, p_i) \text{ then } R_{i,n}^3 \text{ else } 0 | D_{1,n}^1\right] \Sigma_L$$

and it follows from Lemma 28, since $N_i \theta_{i-1} \sigma_{\tilde{N}}^{i-1} \Sigma_L$ is a id_i-valid ballot, that $\phi_{\mathsf{r}}(idp_i, p_i)\{^{ball_i}/_{x_i}, {}^{ball'_i}/_{p_i}\}\Sigma_L = \mathsf{true}$, thus

$$A' \equiv A_i^3 \left[B_{i,n}^2 | R_{i,n}^3 | D_{1,n}^1\right] \Sigma_L.$$

It follows from

$$B \equiv A_i^3 \left[B_{i,n}^2 | \text{if } \phi_{\mathsf{r}}(idp_i, p_i) \text{ then } R_{i,n}^3 \text{ else } 0 | \overline{D}_{1,n}^1\right] \Sigma_R$$

and from Lemma 28 that $\phi_{\mathsf{r}}(idp_i, p_i)\{^{ball_i}/_{x_i}, {}^{ball'_i}/_{p_i}\}\Sigma_R = \mathsf{true}$ since $N_i \theta_{i-1} \ \sigma_N^{i-1} \Sigma_R$ is a id_i-valid ballot. Thus $B \longrightarrow B'$ where

$$B^{'} = A_i^3 \left[B_{i,n}^2 | R_{i,n}^3 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

Since

$$A' \equiv A_i^3 \left[B_{i,n}^2 | R_{i,n}^3 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(32) We have

$$A \equiv A_i^4 \left[B_{i,n}^2 | R_{i,n}^4 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_i^4 \left[B_{i,n}^2 | R_{i,n}^4 | \overline{D}_{1,n}^1\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_i$ such that $N_k \theta_{k-1} \sigma_{\tilde{N}}^{k-1} \Sigma_L$ are id_k-valid ballots for $k = 3 \ldots i$, and such that

$$\bigcup_{3 \leq j \leq i} \text{fv}(N_j) \subseteq \text{dom}(A_i^1) \text{ and } \bigcup_{3 \leq j \leq i} \text{fn}(N_j)) \cap \text{bn}(A_i^1) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_i^4 \left[c_{BR}(q_i).B_{i,n}^3 | \overline{c_{BR}} \langle sig_i^R \rangle.R_{i+1,n}^1 | D_{1,n}^1\right] \Sigma_L$$

and
$$A' \equiv A_i^5\left[B_{i,n}^3|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L.$$

It follows from
$$B \equiv A_i^4\left[c_{BR}(q_i).B_{i,n}^3|\overline{c_{BR}}\langle sig_i^R\rangle.R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R$$

that $B \longrightarrow B'$ where
$$B^{'} = A_i^5\left[B_{i,n}^3|R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R.$$

Since
$$A' \equiv A_i^5\left[B_{i,n}^3|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L\ \mathcal{R}\ B',$$

we derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(33) We have
$$A \equiv A_i^5\left[B_{i,n}^3|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L \text{ and } B \equiv A_i^5\left[B_{i,n}^3|R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R$$

for some $i \in \{3,\dots,n\}$, $N_3,\dots,N_i$ such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ are id_k-valid ballots for $k = 3\dots i$, and such that
$$\bigcup_{3\le j\le i}\mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_i^1) \text{ and } \bigcup_{3\le j\le i}\mathrm{fn}(N_j)) \cap \mathrm{bn}(A_i^1) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that
$$A \equiv A_i^5\left[\text{if } \phi_{\mathsf{s}}(idp_R,q_i) \text{ then } B_{i,n}^{3.1} \text{ else } 0|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L$$

and it follows from Lemma 28, since $N_i\theta_{i-1}\sigma_{\tilde{N}}^{i-1}\Sigma_L$ is a id_i-valid ballot, that $\phi_{\mathsf{s}}(idp_R,q_i)\{^{ball_i}/_{x_i},{}^{ball'_i}/_{p_i},{}^{sig_i^R}/_{q_i}\}\Sigma_L = \mathsf{true}$, thus
$$A' \equiv A_i^5\left[B_{i,n}^{3.1}|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L.$$

It follows from
$$B \equiv A_i^5\left[\text{if } \phi_{\mathsf{s}}(idp_R,q_i) \text{ then } B_{i,n}^{3.1} \text{ else } 0|R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R$$

and from Lemma 28 that $\phi_{\mathsf{s}}(idp_R,q_i)\{^{ball_i}/_{x_i},{}^{ball'_i}/_{p_i},{}^{sig_i^R}/_{q_i}\}\Sigma_R = \mathsf{true}$ since $N_i\theta_{i-1}\sigma_{\tilde{N}}^{i-1}\Sigma_R$ is a id_i-valid ballot. Thus $B \longrightarrow B'$ where
$$B^{'} = A_i^5\left[B_{i,n}^{3.1}|R_{i+1,n}^1|\overline{D}_{1,n}^1\right]\Sigma_R.$$

Since
$$A' \equiv A_i^5\left[B_{i,n}^{3.1}|R_{i+1,n}^1|D_{1,n}^1\right]\Sigma_L\ \mathcal{R}\ B',$$

we derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(36) We have

$$A \equiv A'_i \left[B^4_{i,n}|D^1_{1,n}\right] \Sigma_L \text{ and } B \equiv A'_i \left[B^4_{i,n}|\overline{D}^1_{1,n}\right] \Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k \theta_{k-1} \sigma^{k-1}_{\tilde{N}} \Sigma_L$ are id_k-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3 \leq j \leq n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A^1_n) \text{ and } \bigcup_{3 \leq j \leq n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A^1_n) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A'_i \left[\overline{c_{BD}}\langle \Pi_1(x_i)\rangle.B^4_{i+1,n}|c_{BD}(d_i).D^1_{i+1,n}\right] \Sigma_L$$

and

$$A' \equiv A'_{i+1} \left[B^4_{i+1,n}|D^1_{i+1,n}\right] \Sigma_L.$$

It follows from

$$B \equiv A'_i \left[\overline{c_{BD}}\langle \Pi_1(x_i)\rangle.B^4_{i+1,n}|c_{BD}(d_i).\overline{D}^1_{i+1,n}\right] \Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A'_{i+1} \left[B^4_{i+1,n}|\overline{D}^1_{i+1,n}\right] \Sigma_R.$$

Since

$$A' \equiv A'_{i+1} \left[B^4_{i+1,n}|D^1_{i+1,n}\right] \Sigma_L \mathrel{\mathcal{R}} B',$$

we derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

Labelled Reductions : We must show for all extended processes A and B, where $A \mathrel{\mathcal{R}} B$, that if $A \xrightarrow{\alpha} A'$ for some A', then $B \longrightarrow^* \xrightarrow{\alpha} \longrightarrow^* B'$ and $A' \mathrel{\mathcal{R}} B'$ for some B'. We observe that if $A \mathrel{\mathcal{R}} B$ by an other relation than (1), (10), (11), (14), (23), (24), (27), (31), (34), (35) or (37) to (40) then there is no extended process A' such that $A \xrightarrow{\alpha} A'$. We proceed by case analysis on the remaining cases.

(1) We have

$$A \equiv A_0 \left[V^1_1|V^1_2|B^1_{1,n}|R^1_{1,n}|D^1_{1,n}\right] \text{ and } B \equiv A_0 \left[V^1_1|V^1_2|B^1_{1,n}|R^1_{1,n}|\overline{D}^1_{1,n}\right]$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_0 \left[\nu t_1.\overline{c_{out}}\langle ball_1\rangle.V^2_1|V^1_2|B^1_{1,n}|R^1_{1,n}|D^1_{1,n}\right]$$

and

$$A' \equiv A_1 \left[V^2_1|V^1_2|B^1_{1,n}|R^1_{1,n}|D^1_{1,n}\right] \sigma$$

where $\alpha = \nu b_1.\overline{c_{out}}\langle b_1\rangle$ and $b_1 \notin \mathrm{dom}(A_0)$. It follows from

$$B \equiv A_0 \left[\nu t_1.\overline{c_{out}}\langle ball_1\rangle.V^2_1|V^1_2|B^1_{1,n}|R^1_{1,n}|\overline{D}^1_{1,n}\right]$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_1 \left[V_1^2|V_2^1|B_{1,n}^1|R_{1,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

We have

$$A_1 \left[V_1^2|V_2^1|B_{1,n}^1|R_{1,n}^1|D_{1,n}^1\right] \sigma \mathrel{\mathcal{R}} B',$$

and derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(10) We have

$$A \equiv A_6 \left[V_1^5|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_6 \left[V_1^5|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau$$

If $A \xrightarrow{\alpha} A'$ such that $\text{fv}(\alpha) \subseteq \text{dom}(A)$ and $\text{bn}(\alpha) \cap \text{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_6 \left[\overline{c_{out}}\langle rec_1\rangle.V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_7 \left[V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma$$

where $\alpha = \nu y_1.\overline{c_{out}}\langle y_1\rangle$ and $y_1 \notin \text{dom}(A_6)$. It follows from

$$B \equiv A_6 \left[\overline{c_{out}}\langle rec_1\rangle.V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_7 \left[V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

We have

$$A_7 \left[V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma \mathrel{\mathcal{R}} B',$$

and derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(11) We have

$$A \equiv A_7 \left[V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_7 \left[V_1^6|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau$$

If $A \xrightarrow{\alpha} A'$ such that $\text{fv}(\alpha) \subseteq \text{dom}(A)$ and $\text{bn}(\alpha) \cap \text{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_7 \left[\overline{c_{out}}\langle con_1\rangle.V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_8 \left[V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma$$

where $\alpha = \nu z_1.\overline{c_{out}}\langle z_1\rangle$ and $z_1 \notin \text{dom}(A_7)$. It follows from

$$B \equiv A_7 \left[\overline{c_{out}}\langle con_1\rangle.V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_8 \left[V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau.$$

We have

$$A_8 \left[V_1^7|V_2^1|B_{1,n}^{3.2}|R_{2,n}^1|D_{1,n}^1\right] \sigma \mathrel{\mathcal{R}} B',$$

and derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(14) We have

$$A \equiv A_8 \left[V_2^1|B_{2,n}^1|R_{2,n}^1|D_{1,n}^1\right] \sigma \text{ and } B \equiv A_8 \left[V_2^1|B_{2,n}^1|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_8 \left[\nu t_2.\overline{c_{out}}\langle ball_2\rangle.V_2^2|B_{2,n}^1|R_{2,n}^1|D_{1,n}^1\right] \sigma$$

and

$$A' \equiv A_9 \left[V_2^2|B_{2,n}^1|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L$$

where $\alpha = \nu b_2.\overline{c_{out}}\langle b_2\rangle$ and $b_2 \notin \mathrm{dom}(A_8)$. It follows from

$$B \equiv A_8 \left[\nu t_2.\overline{c_{out}}\langle ball_2\rangle.V_2^2|B_{2,n}^1|R_{2,n}^1|\overline{D}_{1,n}^1\right] \tau$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_9 \left[V_2^2|B_{2,n}^1|R_{2,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R.$$

We have

$$A_9 \left[V_2^2|B_{2,n}^1|R_{2,n}^1|D_{1,n}^1\right] \Sigma_L \mathrel{\mathcal{R}} B',$$

and derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(23) We have

$$A \equiv A_{14} \left[V_2^5|B_{2,n}^{3.2}|R_{3,n}^1|D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_{14} \left[V_2^5|B_{2,n}^{3.2}|R_{3,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_{14} \left[\overline{c_{out}}\langle rec_2\rangle.V_2^6|B_{2,n}^{3.2}|R_{3,n}^1|D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_{15} \left[V_2^6|B_{2,n}^{3.2}|R_{3,n}^1|D_{1,n}^1\right] \Sigma_L$$

where $\alpha = \nu y_2.\overline{c_{out}}\langle\langle\rangle y_2\rangle$ and $y_2 \notin \mathrm{dom}(A_{14})$. It follows from

$$B \equiv A_{14} \left[\overline{c_{out}}\langle rec_2\rangle.V_2^6|B_{2,n}^{3.2}|R_{3,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_{15}\left[V_2^6 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

We have

$$A_{15}\left[V_2^6 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R}\ B',$$

and derive $A' \ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(24) We have

$$A \equiv A_{15}\left[V_2^6 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_{15}\left[V_2^6 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_{15}\left[\overline{c_{out}}\langle con_2\rangle.V_2^7 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_3^1\left[V_2^7 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L$$

where $\alpha = \nu z_2.\overline{c_{out}}\langle z_2\rangle$ and $z_2 \notin \mathrm{dom}(A_{15})$. It follows from

$$B \equiv A_{15}\left[\overline{c_{out}}\langle con_2\rangle.V_2^7 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_3^1\left[V_2^7 | B_{2,n}^{3.2} | R_{3,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

We have

$$A_3^1\left[V_2^7 | B_{2,n}^{3.2} | R_{3,n}^1 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R}\ B',$$

and derive $A' \ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(27) We have

$$A \equiv A_i^1\left[B_{i,n}^1 | R_{i,n}^1 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_i^1\left[B_{i,n}^1 | R_{i,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_{i-1}$ such that $N_k\theta_{k-1}\sigma_N^{k-1}\Sigma_L$ are id_k-valid ballots for $k = 3 \ldots i-1$ and

$$\bigcup_{3 \le j \le i-1} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_i^1) \text{ and } \bigcup_{3 \le j \le i-1} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_i^1) = \emptyset.$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_i^1\left[c_i(x_i).B_{i,n}^{1.1} | R_{i,n}^1 | D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_i^1\left[B_{i,n}^{1.1}\{^{M_i}/_{x_i}\} | R_{i,n}^1 | D_{1,n}^1\right] \Sigma_L$$

where $\alpha = c_i(M_i)$ for some term M_i such that $\mathrm{fn}(\alpha) \cap \mathrm{bn}(A_i^1) = \emptyset$. It follows from

$$B \equiv A_i^1 \left[c_i(x_i).B_{i,n}^{1.1} | R_{i,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_i^1 \left[B_{i,n}^{1.1}\{^{M_i}/_{x_i}\} | R_{i,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

We have

$$A_i^1 \left[B_{i,n}^{1.1}\{^{M_i}/_{x_i}\} | R_{i,n}^1 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B',$$

and derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(31) We have

$$A \equiv A_i^3 \left[B_{i,n}^2 | R_{i,n}^3 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_i^3 \left[B_{i,n}^2 | R_{i,n}^3 | \overline{D}_{1,n}^1\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_i$ such that $N_k \theta_{k-1} \sigma_N^{k-1} \Sigma_L$ are id_k-valid ballots for $k = 3 \ldots i$ and

$$\bigcup_{3 \leq j \leq i} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_i^1) \text{ and } \bigcup_{3 \leq j \leq i} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_i^1) = \emptyset.$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_i^3 \left[B_{i,n}^2 | \overline{c_{RV_i}}\langle r_i \rangle.R_{i,n}^4 | D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_i^4 \left[B_{i,n}^2 | R_{i,n}^4 | D_{1,n}^1\right] \Sigma_L$$

where $\alpha = \nu y_i.\overline{c_{RV_i}}\langle y_i \rangle$ and $y_i \notin \mathrm{dom}(A_i^3)$. It follows from

$$B \equiv A_i^3 \left[B_{i,n}^2 | \overline{c_{RV_i}}\langle r_i \rangle.R_{i,n}^4 | \overline{D}_{1,n}^1\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_i^4 \left[B_{i,n}^2 | R_{i,n}^4 | \overline{D}_{1,n}^1\right] \Sigma_R.$$

We have

$$A_i^4 \left[B_{i,n}^2 | R_{i,n}^4 | D_{1,n}^1\right] \Sigma_L \ \mathcal{R} \ B',$$

and derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(34) We have

$$A \equiv A_i^5 \left[B_{i,n}^{3.1} | R_{i+1,n}^1 | D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_i^5 \left[B_{i,n}^{3.1} | R_{i+1,n}^1 | \overline{D}_{1,n}^1\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_i$ such that $N_k \theta_{k-1} \sigma_N^{k-1} \Sigma_L$ are id_k-valid ballots for $k = 3 \ldots i$ and

$$\bigcup_{3 \leq j \leq i} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_i^1) \text{ and } \bigcup_{3 \leq j \leq i} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_i^1) = \emptyset.$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A_i^5 \left[\overline{c_i}\langle q_i\rangle.B_{i,n}^{3.2}|R_{i+1,n}^1|D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_i^6 \left[B_{i,n}^{3.2}|R_{i+1,n}^1|D_{1,n}^1\right] \Sigma_L$$

where $\alpha = \nu z_i.\overline{c_i}\langle z_i\rangle$ and $z_i \notin \mathrm{dom}(A_i^5)$. It follows from

$$B \equiv A_i^5 \left[\overline{c_i}\langle q_i\rangle.B_{i,n}^{3.2}|R_{i+1,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_i^6 \left[B_{i,n}^{3.2}|R_{i+1,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R.$$

We have

$$A_i^6 \left[B_{i,n}^{3.2}|R_{i+1,n}^1|D_{1,n}^1\right] \Sigma_L \ \mathcal{R}\ B',$$

and derive $A' \ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(35) We have

$$A \equiv A_i^6 \left[B_{i,n}^{3.2}|R_{i+1,n}^1|D_{1,n}^1\right] \Sigma_L \text{ and } B \equiv A_i^6 \left[B_{i,n}^{3.2}|R_{i+1,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R$$

for some $i \in \{3, \ldots, n\}$, $N_3, \ldots, N_i$ such that $N_k\theta_{k-1}\sigma_N^{k-1}\Sigma_L$ are id_k-valid ballots for $k = 3 \ldots i$ and

$$\bigcup_{3\leq j\leq i} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_i^1) \text{ and } \bigcup_{3\leq j\leq i} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_i^1) = \emptyset.$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then there are two cases :

– If $3 \leq i < n$.

$$A_i^6 \left[c_i(sy_i).B_{i+1,n}^1|R_{i+1,n}^1|D_{1,n}^1\right] \Sigma_L$$

and

$$A' \equiv A_{i+1}^1 \left[B_{i+1,n}^1|R_{i+1,n}^1|D_{1,n}^1\right] \Sigma_L$$

where $\alpha = c_i(W_i)$ for some term W_i such that $\mathrm{fn}(\alpha) \cap \mathrm{bn}(A_i^6) = \emptyset$. It follows from

$$B \equiv A_i^6 \left[c_i(sy_i).B_{i+1,n}^1|R_{i+1,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv A_{i+1}^1 \left[B_{i+1,n}^1|R_{i+1,n}^1|\overline{D}_{1,n}^1\right] \Sigma_R.$$

We have

$$A_{i+1}^1 \left[B_{i+1,n}^1|R_{i+1,n}^1|D_{1,n}^1\right] \Sigma_L \ \mathcal{R}\ B',$$

and derive $A' \ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

- If $i = n$. $A_n^6\left[c_n(sy_n).B^4_{1,n}|D^1_{1,n}\right]\Sigma_L$ and $A' \equiv A'_1\left[B^4_{1,n}|D^1_{1,n}\right]\Sigma_L$ where $\alpha = c_n(W_n)$ for some term W_n such that $\mathrm{fn}(\alpha) \cap \mathrm{bn}(A_n^6) = \emptyset$. It follows from $B \equiv A_n^6\left[c_n(sy_n).B^4_{1,n}|\overline{D}^1_{1,n}\right]\Sigma_R$ that $B \xrightarrow{\alpha} B'$ where $B' \equiv A'_1\left[B^4_{1,n}|\overline{D}^1_{1,n}\right]\Sigma_R$. We have $A'_1\left[B^4_{1,n}|D^1_{1,n}\right]\Sigma_L \mathrel{\mathcal{R}} B'$, and derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(37) We have

$$A \equiv A'_{n+1}\left[D^2_{1,n}\right]\Sigma_L \text{ and } B \equiv A'_{n+1}\left[\overline{D}^2_{1,n}\right]\Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ are id_k-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3 \leq j \leq n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_n^1) \text{ and } \bigcup_{3 \leq j \leq n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_n^1) = \emptyset.$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A'_{n+1}\left[\overline{c_{out}}\langle dec_1\rangle.D^2_{2,n}\right]\Sigma_L$$

and

$$A' \equiv A''_1\left[D^2_{2,n}\right]\Sigma_L$$

where $\alpha = \nu\ result_1.\overline{c_{out}}\langle result_1\rangle$ and $result_1 \notin \mathrm{dom}(A'_{n+1})$. It follows from

$$B \equiv A'_{n+1}\left[\overline{c_{out}}\langle dec_2\rangle.\overline{D}^2_{2,n}\right]\Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv \overline{A}''_1\left[\overline{D}^2_{2,n}\right]\Sigma_R.$$

We have

$$A''_1\left[D^2_{2,n}\right]\Sigma_L \mathrel{\mathcal{R}} B',$$

and derive $A' \mathrel{\mathcal{R}} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(38) We have

$$A \equiv A''_1\left[D^2_{2,n}\right]\Sigma_L \text{ and } B \equiv \overline{A}''_1\left[\overline{D}^2_{2,n}\right]\Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ are id_k-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3 \leq j \leq n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_n^1) \text{ and } \bigcup_{3 \leq j \leq n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_n^1) = \emptyset.$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then it must be the case that

$$A \equiv A''_1\left[\overline{c_{out}}\langle dec_2\rangle.D^2_{3,n}\right]\Sigma_L$$

and

$$A' \equiv A''_2\left[D^2_{3,n}\right]\Sigma_L$$

where $\alpha = \nu\ result_2.\overline{c_{out}}\langle result_2\rangle$ and $result_2 \notin \mathrm{dom}(A''_1)$. It follows from

$$B \equiv \overline{A}''_1 \left[Out[c_{out}]dec_1.\overline{D}^2_{3,n}\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv \overline{A}''_2 \left[\overline{D}^2_{3,n}\right] \Sigma_R.$$

We have

$$A''_2 \left[D^2_{3,n}\right] \Sigma_L\ \mathcal{R}\ B',$$

and derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(39) We have

$$A \equiv A''_{i-1} \left[D^2_{i,n}\right] \Sigma_L \text{ and } B \equiv \overline{A}''_{i-1} \left[\overline{D}^2_{i,n}\right] \Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k \theta_{k-1} \sigma^{k-1}_{\tilde{N}} \Sigma_L$ are id_k-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3 \le j \le n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A^1_n) \text{ and } \bigcup_{3 \le j \le n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A^1_n) = \emptyset.$$

If $A \xrightarrow{\alpha} A'$ such that $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(A)$ and $\mathrm{bn}(\alpha) \cap \mathrm{bn}(B) = \emptyset$, then there are two cases :

– If $3 \le i < n$.

$$A''_{i-1} \left[\overline{c_{out}}\langle dec_i\rangle.D^2_{i+1,n}\right] \Sigma_L \text{ and } A' \equiv A''_i \left[D^2_{1+1,n}\right] \Sigma_L$$

where $\alpha = \nu\ result_i.\overline{c_{out}}\langle result_i\rangle$ and $result_i \notin \mathrm{dom}(A''_{i-1})$. It follows from

$$B \equiv \overline{A}''_{i-1} \left[\overline{c_{out}}\langle dec_i\rangle.\overline{D}^2_{i+1,n}\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv \overline{A}''_i \left[\overline{D}^2_{i+1,n}\right] \Sigma_R.$$

We have

$$A''_i \left[D^2_{1+1,n}\right] \Sigma_L\ \mathcal{R}\ B',$$

and derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

– If $i = n$.

$$A''_{n-1} \left[\overline{c_{out}}\langle dec_n\rangle\right] \Sigma_L \text{ and } A' \equiv A''_n\, [0]\, \Sigma_L$$

where $\alpha = \nu\ result_n.\overline{c_{out}}\langle result_n\rangle$ and $result_n \notin \mathrm{dom}(A''_{n-1})$. It follows from

$$B \equiv \overline{A}''_{n-1} \left[\overline{c_{out}}\langle dec_n\rangle\right] \Sigma_R$$

that $B \xrightarrow{\alpha} B'$ where

$$B' \equiv \overline{A}''_n\, [0]\, \Sigma_R.$$

We have

$$A''_n\, [0]\, \Sigma_L\ \mathcal{R}\ B',$$

and derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

B.5 Proving the Theorem 4

As $\mathcal{R}$ is verifying the three properties of Definition 2, we have to show that for all extended processes A and B, where $A\mathcal{R}B$, that $A \approx_s B$. Using Lemma 9, it is sufficient to prove that $A''_n\,[0]\,\Sigma_L \approx_s \overline{A}''_n\,[0]\,\Sigma_R$ for any N_i such that $N_i\theta_{i-1}\sigma_{\tilde{N}}^{i-1}\Sigma$ are id$_i$-valid ballots. As $A''_n\,[0]\,\Sigma_L$ is mapped in $\tilde{n}.(\theta|R)\sigma_{\tilde{N}}\Sigma_L$ and $\overline{A}''_n\,[0]\,\Sigma_R$ is mapped in $\tilde{n}.(\theta|\overline{R})\sigma_{\tilde{N}}\Sigma_R$, we conclude using Proposition 8.

■

C Proof of Theorem 3

Let us remind the Theorem we need to prove.

Theorem 3. *Let n be the number of voters. The Norwegian e-voting protocol process specification satisfies ballot secrecy with the auditing process, even with $n-2$ voters are corrupted, provided that the other components are honest.*

$$A_n[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\sigma \mid V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\tau]$$
$$\approx_l \overline{A}_n\,[V\{^{c_1}/_{c_{auth}}, ^{c_{RV_1}}/_{c_{RV}}\}\tau | V\{^{c_2}/_{c_{auth}}, ^{c_{RV_2}}/_{c_{RV}}\}\sigma]$$

where $\sigma = \{^{v_1}/_{x_{vote}}\}$ and $\tau = \{^{v_2}/_{x_{vote}}\}$.

Let us introduce the relation we will use to prove labeled bisimilarity.

C.1 Partial evolutions of protocol specification

First, we will introduce partial evolutions of the protocol process specification and remind some notations used. One can note that the notations are the same as those we used in the previous section when proving Theorem 4, since we redefine them here, there are no possible confusion.

Definition 30. *Notations and partial evolutions for honest voters. ($i \in \{1,2\}$)*

$$\begin{array}{ll}
V_i^1 = \overline{c_{out}}\langle ball_i\rangle.V_i^2 & e_i \quad = \mathsf{penc}(x_{vote}^i, t_i, \mathsf{pk}(a_1)) \\
V_i^2 = \overline{c_i}\langle ball_i\rangle.V_i^3 & pfk_i \;\, = \mathsf{pfk}_1(id_i, t_i, x_{vote}^i, e_i) \\
V_i^3 = c_{RV_i}(rec_i).V_i^4 & sig_i \;\, = \mathsf{sign}((e_i, pfk_i), id_i) \\
V_i^4 = c_i(con_i).V_i^5 & ball_i = (e_i, pfk_i, sig_i) \\
V_i^5 = \overline{c_{out}}\langle con_i\rangle.V_i^6 & hv_i \;\;\, = \mathsf{hash}((\mathsf{vk}(id_i), e_i, pfk_i, sig_i)) \\
V_i^6 = \overline{c_{out}}\langle rec_i\rangle.V_i^7 & \\
V_i^7 = \text{if } \phi_{\mathsf{v}}(idp_R, id_i, hv_i, con_i, x_i^{vote}, rec_i) \text{ then } V_i^8 \text{ else } 0 & \\
V_i^8 = \overline{c_i}\langle \mathsf{Ok}\rangle &
\end{array}$$

Definition 31. *Notations and partial evolutions for the ballot box. ($i \in \{1,\dots,n\}$)*

$$\begin{array}{llll}
B_{i,n}^1 & = c_i(x_i).B_{i,n}^{1.1} & e'_i & = \mathsf{renc}(\Pi_1(x_i), \mathsf{s}(id_i)) \\
B_{i,n}^{1.1} & = \text{if } \phi_{\mathsf{b}}(idp_i, x_i) \text{ then } B_{i,n}^{1.2} \text{ else } 0 & pfk'_i & = \mathsf{pfk}_2(id_i, a_2, \Pi_1(x_i), e'_i) \\
B_{i,n}^{1.2} & = \overline{c_{BR}}\langle ball'_i\rangle.B_{i,n}^2 & e''_i & = \mathsf{blind}(e'_i, \mathsf{s}(id_i)) \\
B_{i,n}^2 & = c_{BR}(q_i).B_{i,n}^3 & pfk''_i & = \mathsf{pfk}_2(id_i, \mathsf{s}(id_i), e'_i, e''_i) \\
B_{i,n}^3 & = \text{if } \phi_{\mathsf{s}}(idp_R, hbb_i, q_i) \text{ then } B_{i,n}^{3.1} \text{ else } 0 & ball'_i & = (x_i, e'_i, pfk'_i, e''_i, pfk''_i) \\
B_{i,n}^{3.1} & = \overline{c_i}\langle q_i\rangle.B_{i,n}^{3.2} & hbb_i & = \mathsf{hash}((\mathsf{vk}(id_i), x_i)) \\
B_{i,n}^{3.2} & = c_i(sy_i).B_{i+1,n}^1 & & \\
B_{n,n}^{3.2} & = c_n(sy_n).B_{1,n}^4 & &
\end{array}$$

$$\begin{aligned}
B^4_{i,n} &= \overline{c_{BD}}\langle \Pi_1(x_i)\rangle.B^4_{i+1,n}\\
B^4_{n,n} &= \overline{c_{BD}}\langle \Pi_1(x_n)\rangle.B^5_{1,n}\\
B^5_{i,n} &= \overline{c_{BA}}\langle x_i\rangle.B^5_{i+1,n}\\
B^5_{n,n} &= \overline{c_{BA}}\langle x_n\rangle
\end{aligned}$$

Definition 32. *Notations et and partial evolutions for the receipt generator. ($i \in \{1,\dots,n\}$)*

$$\begin{aligned}
R^1_{i,n} &= c_{BR}(p_i).R^2_{i,n}\\
R^2_{i,n} &= \text{if } \phi_{\mathsf{r}}(idp_i,p_i) \text{ then } R^3_{i,n} \text{ else } 0\\
R^3_{i,n} &= \overline{c_{RV_i}}\langle r_i\rangle.R^4_{i,n}\\
R^4_{i,n} &= \overline{c_{BR}}\langle sig^R_i\rangle.R^1_{i+1,n}\\
R^4_{n,n} &= \overline{c_{BR}}\langle sig^R_n\rangle.R^5_{1,n}\\
R^5_{i,n} &= \overline{c_{RA}}\langle (idp_i, hbpr_i, hbr_i)\rangle.R^5_{i+1,n}\\
R^5_{n,n} &= \overline{c_{BR}}\langle (idp_i, hbpr_i, hbr_i)\rangle
\end{aligned}$$

$$\begin{aligned}
r_i &= \mathsf{d}(\mathsf{p}(id_i), \mathsf{dec}(\Pi_6(p_i), a_3))\\
hbr_i &= \mathsf{hash}((idp_i, \Pi_1(p_i), \Pi_2(p_i), \Pi_3(p_i)))\\
sig^R_i &= \mathsf{sign}(hbr_i, id_R)
\end{aligned}$$

Definition 33. *Notations and partial evolutions for the decryption service, we distinguish two cases : one without a swap (D) and one with swap ($\overline{D}$).($i \in \{1,\dots,n\}$)*

$$\begin{aligned}
dec_i &= \mathsf{dec}(d_i, a_1)\\
D^1_{i,n} &= c_{BD}(d_i).D^1_{i+1,n}\\
D^1_{n,n} &= c_{BD}(d_n).D^2_{1,n}\\
D^2_1 &= \overline{c_{DA}}\langle \mathsf{hash}((d_1,\dots,d_n))\rangle.D^2_2\\
D^2_2 &= c_{DA}(h).D^3_{1,n}\\
D^3_{i,n} &= \overline{c_{out}}\langle dec_i\rangle.D^3_{i+1,n}\\
D^3_{n,n} &= \overline{c_{out}}\langle dec_n\rangle
\end{aligned}$$

$$\begin{aligned}
\overline{D}^1_{i,n} &= c_{BD}(d_j).\overline{D}^1_{i+1,n}\\
\overline{D}^1_{n,n} &= c_{BD}(d_n).\overline{D}^2_1\\
\overline{D}^2_1 &= \overline{c_{DA}}\langle \mathsf{hash}((d_1,\dots,d_n))\rangle.\overline{D}^2_2\\
\overline{D}^2_2 &= c_{DA}(h).\overline{D}^3_{1,n}\\
\overline{D}^3_{1,n} &= \overline{c_{out}}\langle dec_2\rangle.\overline{D}^2_{2,n}\\
\overline{D}^3_{2,n} &= \overline{c_{out}}\langle dec_1\rangle.\overline{D}^2_{3,n}\\
\overline{D}^3_{i,n} &= \overline{c_{out}}\langle dec_i\rangle.\overline{D}^2_{i+1,n}\\
\overline{D}^3_{n,n} &= \overline{c_{out}}\langle dec_n\rangle
\end{aligned}$$

Definition 34. *Partial evolutions for the auditor. ($j \in \{1,\dots,n\}$)*

$$\begin{aligned}
AD^1 &= c_{DA}(h_d).AD^2_{1,n}\\
AD^2_{j,n} &= c_{BA}(ba_j).AD^2_{j+1,n}\\
AD^2_{n,n} &= c_{BA}(ba_n).AD^3_{1,n}\\
AD^3_{j,n} &= c_{RA}(ha_j).AD^3_{j+1,n}\\
AD^3_{n,n} &= c_{RA}(ha_n).AD^4_1\\
AD^4_1 &= \text{if } \phi_{\mathsf{a}}(ba_1, ha_1, idp_1, \dots, ba_n, ha_n, idp_n, h, h_d) \text{ then } AD^4_2 \text{ else } 0\\
AD^4_2 &= \overline{c_{DA}}\langle \mathsf{Ok}\rangle
\end{aligned}$$

Definition 35. *Partial evolutions of global process representing the enrichment of the frame as the process advances.*

$$\begin{aligned}
\tilde{n} &= (a_1, a_2, id_1, id_2, id_R, c_1, c_2, c_{RV_1}, c_{RV_2}, c_{BR}, c_{BD})\\
\Gamma &= \{^{\mathsf{pk}(a_1)}/_{g_1}, ^{\mathsf{pk}(a_2)}/_{g_2}, ^{\mathsf{pk}(a_3)}/_{g_3}, ^{\mathsf{vk}(id_1)}/_{idp_1}, \dots, ^{\mathsf{vk}(id_n)}/_{idp_n}, ^{\mathsf{vk}(id_R)}/_{idp_R}\}
\end{aligned}$$

$$\begin{aligned}
A_0 &= \nu\tilde{n}.\,[\_\,|\Gamma]\\
A_1 &= \nu(\tilde{n}, t_1).\,[\_\,|\{^{ball_1}/_{b_1}\}|\Gamma]\\
A_2 &= \nu(\tilde{n}, t_1, x_1).\,[\_\,|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\Gamma]
\end{aligned}$$

$$
\begin{aligned}
A_3 =&\ \nu(\tilde{n}, t_1, x_1, p_1). \Big[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\Gamma\Big] \\
A_4 =&\ \nu(\tilde{n}, t_1, x_1, p_1, rec_1). \Big[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}|\Gamma\Big] \\
A_5 =&\ \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1). \Big[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}| \\
&\ \{^{sig_1^R}/_{q_1}\}|\Gamma\Big] \\
A_6 =&\ \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1). \Big[\_|\{^{ball_1}/_{b_1}\}|\{^{ball_1}/_{x_1}\}|\{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}| \\
&\ \{^{sig_1^R}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\Gamma\Big] \\
A_7 =&\ A_6\,[\_|\{^{rec_1}/_{y_1}\}] \\
A_8 =&\ A_7\,[\_|\{^{con_1}/_{z_1}\}] \\
A_9 =&\ \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2). \big[\_|\{\{^{ball_i}/_{b_i}\}|i=1,2\}|\{^{ball_1}/_{x_1}\}| \\
&\ \{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}|\{^{sig_1^R}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\Big] \\
A_{10} =&\ \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2). \big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}|i=1,2\}| \\
&\ \{^{ball'_1}/_{p_1}\}|\{^{r_1}/_{rec_1}\}|\{^{sig_1^R}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\Big] \\
A_{11} =&\nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2). \Big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}|\{^{ball'_i}/_{p_i}\} \\
&\ |i=1,2\}|\{^{r_1}/_{rec_1}\}|\{^{sig_1^R}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\Big] \\
A_{12} =&\nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2, rec_2). \big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}| \\
&\ \{^{ball'_i}/_{p_i}|\{^{r_i}/_{rec_i}\}\}|i=1,2\}|\{^{sig_1^R}/_{q_1}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\Big] \\
A_{13} =&\ \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2, rec_2, q_2). \big[\_|\{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}| \\
&\ \{^{ball'_i}/_{p_i}|\{^{r_i}/_{rec_i}\}|\{^{sig_i^R}/_{q_i}\}\}|i=1,2\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma\Big] \\
A_{14} =&\ \nu(\tilde{n}, t_1, x_1, p_1, rec_1, q_1, con_1, t_2, x_2, p_2, rec_2, q_2, con_2). \big[\_|\{\{^{ball_i}/_{b_i}\}| \\
&\ \{^{ball_i}/_{x_i}\}|\{^{ball'_i}/_{p_i}|\{^{r_i}/_{rec_i}\}|\{^{sig_i^R}/_{q_i}\}|\{^{q_1}/_{con_1}\}\}|i=1,2\}| \\
&\ \{^{rec_1}/_{y_1}\}|\{^{con_1}/_{z_1}\}|\Gamma] \\
A_{15} =&A_{14}\,[\_|\{^{rec_2}/_{y_2}\}]
\end{aligned}
$$

For $i \in \{3, \ldots, n\}$ *:*

$$
\begin{aligned}
\tilde{m}_i =&\ \{(p_k, q_k)|k \in \{3, \ldots, i-1\}\} \\
\Lambda =&\ \ \{\{^{ball_i}/_{b_i}\}|\{^{ball_i}/_{x_i}\}|\{^{ball'_i}/_{p_i}|\{^{r_i}/_{rec_i}\}|\{^{sig_i^R}/_{q_i}\}|\{^{q_1}/_{con_1}\}|\{^{rec_1}/_{y_1}| \\
&\ \ \{^{con_1}/_{z_1}\}\}|i=1,2\} \\
\Lambda_i =&\ \ \{\{^{N_k}/_{x_k}\}|\{^{ball'_k}/_{p_k}\}|\{^{r_k}/_{y_k}\}|\{^{sig_k^R}/_{q_k}\}|\{^{q_k}/_{z_k}\}|\{^{W_k}/_{sy_k}\}| \\
&\ \ k \in \{3, \ldots, i-1\}\}
\end{aligned}
$$

$$
\begin{aligned}
A_i^1 =&\ \nu(\tilde{n}, \tilde{m}_i). [\_|\Lambda_i|\Lambda|\Gamma] \\
A_i^2 =&\ A_i^1\,\big[\_|\{^{N_i}/_{x_i}\}\big] \\
A_i^3 =&\ \nu(\tilde{n}, \tilde{m}_i, p_i). \Big[\_|\{^{N_i}/_{x_i}\}|\{^{ball'_i}/_{p_i}\}|\Lambda_i|\Lambda|\Gamma\Big] \\
A_i^4 =&\ A_i^3\,[\_|\{^{r_i}/_{y_i}\}] \\
A_i^5 =&\ \nu(\tilde{n}, \tilde{m}_{i+1}). \Big[\_|\{^{N_i}/_{x_i}\}|\{^{ball'_i}/_{p_i}\}|\{^{r_i}/_{y_i}\}|\{^{sig_i^R}/_{q_i}\}|\Lambda_i|\Lambda|\Gamma\Big] \\
A_i^6 =&\ \nu(\tilde{n}, \tilde{m}_{i+1}). \Big[\_|\{^{N_i}/_{x_i}\}|\{^{ball'_i}/_{p_i}\}|\{^{r_i}/_{y_i}\}|\{^{sig_i^R}/_{q_i}\}|\{^{q_i}/_{z_i}\}|\Lambda_i|\Lambda|\Gamma\Big]
\end{aligned}
$$

for $i \in \{1, \ldots, n\}$

$$
\begin{aligned}
\tilde{d}_i =&\ \ \{d_k|k \in \{1, \ldots, i-1\}\} \\
\Omega_i =&\ \ \{\{^{\Pi_1(x_k)}/_{d_k}\}|k \in \{1, \ldots, i-1\}\} \\
A_i^7 =&\ \nu(\tilde{n}, \tilde{m}_{n+1}, \tilde{d}_i). [\_|\Omega_i|\Lambda_{n+1}|\Lambda|\Gamma]
\end{aligned}
$$

$$\begin{aligned}
\tilde{ba}_i &= \{ba_k | k \in \{1, \ldots, i-1\}\}\\
\Theta_i &= \{\{^{\Pi_1(x_k)}/_{d_k}\} | k \in \{1, \ldots, i-1\}\}\\
A_i^8 &= \nu(\tilde{n}, \tilde{m}_{n+1}, \tilde{d}_{n+1}, h_d, \tilde{ba}_i).\ [\_ | \Theta_i | \{^{\mathsf{hash}((d_1,\ldots,d_n))}/_{h_d}\} |\\
&\quad \Omega_{n+1} | \Lambda_{n+1} | \Lambda | \Gamma]\\
\tilde{ha}_i &= \{ha_k | k \in \{1, \ldots, i-1\}\}\\
\Delta_i &= \{\{^{\Pi_1(x_k)}/_{d_k}\} | k \in \{1, \ldots, i-1\}\}\\
A_i^9 &= \nu(\tilde{n}, \tilde{m}_{n+1}, \tilde{d}_{n+1}, h_d, \tilde{ba}_{n+1}, \tilde{ha}_i).\ [\_ | \Delta_i | \Theta_{n+1} | \{^{\mathsf{hash}((d_1,\ldots,d_n))}/_{h_d}\} | \Omega_{n+1} |\\
&\quad \Lambda_{n+1} | \Lambda | \Gamma]\\
A' &= \nu(\tilde{n}, \tilde{m}_{n+1}, \tilde{d}_{n+1}, h_d, \tilde{ba}_{n+1}, \tilde{ha}_{n+1}, h).\ [\_ | \{^{\mathsf{Ok}}/_{h}\} | \Delta_{n+1} | \Theta_{n+1} |\\
&\quad \{^{\mathsf{hash}((d_1,\ldots,d_n))}/_{h_d}\} | \Omega_{n+1} | \Lambda_{n+1} | \Lambda | \Gamma]\\
A_1'' &= A'\ [\_ | \{^{dec_1}/_{result_1}\}]\\
A_i'' &= A_{i-1}''\ [\_ | \{^{dec_i}/_{result_i}\}]
\end{aligned}$$

$$\begin{aligned}
\overline{A}_1'' &= A'\ [\_ | \{\{^{dec_2}/_{result_1}\}]\\
\overline{A}_2'' &= \overline{A}_1''\ [\_ | \{\{^{dec_1}/_{result_2}\}]\\
\overline{A}_i'' &= \overline{A}_{i-1}''\ [\_ | \{^{dec_i}/_{result_i}\}]
\end{aligned}$$

C.2 Relation

Now we can define the relation.

Definition 36. *Given integer $n \geq 2$, $\forall\ 3 \leq j \leq n$, let M_j and N_j terms such that $N_j \theta_{j-1} \sigma_{\tilde{N}}^{j-1} \Sigma_L$ is an id_j-valid ballot, and such that $fv(M_j) \cup fv(N_j) \subseteq dom(A_j^1)$ and $(fn(M_j) \cup fn(N_j)) \cap bn(A_j^1) = \emptyset$. We consider the smallest relation $\mathcal{R}$ which is closed under structural equivalence and includes the following pairs of extended processes :*

$$A_0 \left[V_1^1 | V_2^1 | B_{1,n}^1 | R_{1,n}^1 | D_{1,n}^1 | AD^1\right] \sim_{\mathcal{R}} A_0 \left[V_1^1 | V_2^1 | B_{1,n}^1 | R_{1,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tag{1}$$

$$A_1 \left[V_1^2 | V_2^1 | B_{1,n}^1 | R_{1,n}^1 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_1 \left[V_1^2 | V_2^1 | B_{1,n}^1 | R_{1,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{2}$$

$$A_2 \left[V_1^3 | V_2^1 | B_{1,n}^{1.1} | R_{1,n}^1 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_2 \left[V_1^3 | V_2^1 | B_{1,n}^{1.1} | R_{1,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{3}$$

$$A_2 \left[V_1^3 | V_2^1 | B_{1,n}^{1.2} | R_{1,n}^1 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_2 \left[V_1^3 | V_2^1 | B_{1,n}^{1.2} | R_{1,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{4}$$

$$A_3 \left[V_1^3 | V_2^1 | B_{1,n}^2 | R_{1,n}^2 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_3 \left[V_1^3 | V_2^1 | B_{1,n}^2 | R_{1,n}^2 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{5}$$

$$A_3 \left[V_1^3 | V_2^1 | B_{1,n}^2 | R_{1,n}^3 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_3 \left[V_1^3 | V_2^1 | B_{1,n}^2 | R_{1,n}^3 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{6}$$

$$A_4 \left[V_1^4 | V_2^1 | B_{1,n}^2 | R_{1,n}^4 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_4 \left[V_1^4 | V_2^1 | B_{1,n}^2 | R_{1,n}^4 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{7}$$

$$A_5 \left[V_1^4 | V_2^1 | B_{1,n}^3 | R_{2,n}^1 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_5 \left[V_1^4 | V_2^1 | B_{1,n}^3 | R_{2,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{8}$$

$$A_5 \left[V_1^4 | V_2^1 | B_{1,n}^{3.1} | R_{2,n}^1 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_5 \left[V_1^4 | V_2^1 | B_{1,n}^{3.1} | R_{2,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{9}$$

$$A_6 \left[V_1^5 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_6 \left[V_1^5 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{10}$$

$$A_7 \left[V_1^6 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | D_{1,n}^1 | AD^1\right] \sigma \sim_{\mathcal{R}} A_7 \left[V_1^6 | V_2^1 | B_{1,n}^{3.2} | R_{2,n}^1 | \overline{D}_{1,n}^1 | AD^1\right] \tau \tag{11}$$

$$A_8\left[V_1^7|V_2^1|B^{3.2}_{1,n}|R^1_{2,n}|D^1_{1,n}|AD^1\right]\sigma \sim_{\mathcal{R}} A_8\left[V_1^7|V_2^1|B^{3.2}_{1,n}|R^1_{2,n}|\overline{D}^1_{1,n}|AD^1\right]\tau \tag{12}$$

$$A_8\left[V_1^8|V_2^1|B^{3.2}_{1,n}|R^1_{2,n}|D^1_{1,n}|AD^1\right]\sigma \sim_{\mathcal{R}} A_8\left[V_1^8|V_2^1|B^{3.2}_{1,n}|R^1_{2,n}|\overline{D}^1_{1,n}|AD^1\right]\tau \tag{13}$$

$$A_8\left[V_2^1|B^1_{2,n}|R^1_{2,n}|D^1_{1,n}|AD^1\right]\sigma \sim_{\mathcal{R}} A_8\left[V_2^1|B^1_{2,n}|R^1_{2,n}|\overline{D}^1_{1,n}|AD^1\right]\tau \tag{14}$$

$$A_9\left[V_2^2|B^1_{2,n}|R^1_{2,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_9\left[V_2^2|B^1_{2,n}|R^1_{2,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{15}$$

$$A_{10}\left[V_2^3|B^{1.1}_{2,n}|R^1_{2,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{10}\left[V_2^3|B^{1.1}_{2,n}|R^1_{2,n}|\overline{D}^1_{1,n}\right]|AD^1\Sigma_R \tag{16}$$

$$A_{10}\left[V_2^3|B^{1.2}_{2,n}|R^1_{2,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{10}\left[V_2^3|B^{1.2}_{2,n}|R^1_{2,n}|\overline{D}^1_{1,n}\right]|AD^1\Sigma_R \tag{17}$$

$$A_{11}\left[V_2^3|B^2_{2,n}|R^2_{2,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{11}\left[V_2^3|B^2_{2,n}|R^2_{2,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{18}$$

$$A_{11}\left[V_2^3|B^2_{2,n}|R^3_{2,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{11}\left[V_2^3|B^2_{2,n}|R^3_{2,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{19}$$

$$A_{12}\left[V_2^4|B^2_{2,n}|R^4_{2,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{12}\left[V_2^4|B^2_{2,n}|R^4_{2,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{20}$$

$$A_{13}\left[V_2^4|B^3_{2,n}|R^1_{3,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{13}\left[V_2^4|B^3_{2,n}|R^1_{3,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{21}$$

$$A_{13}\left[V_2^4|B^{3.1}_{2,n}|R^1_{3,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{13}\left[V_2^4|B^{3.1}_{2,n}|R^1_{3,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{22}$$

$$A_{14}\left[V_2^5|B^{3.2}_{2,n}|R^1_{3,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{14}\left[V_2^5|B^{3.2}_{2,n}|R^1_{3,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{23}$$

$$A_{15}\left[V_2^6|B^{3.2}_{2,n}|R^1_{3,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{15}\left[V_2^6|B^{3.2}_{2,n}|R^1_{3,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{24}$$

$$A_3^1\left[V_2^7|B^{3.2}_{2,n}|R^1_{3,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_3^1\left[V_2^7|B^{3.2}_{2,n}|R^1_{3,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{25}$$

$$A_3^1\left[V_2^8|B^{3.2}_{2,n}|R^1_{3,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_3^1\left[V_2^8|B^{3.2}_{2,n}|R^1_{3,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{26}$$

($i \in \{3,\ldots,n\}$, $R^1_{n+1,n} = R^5_{1,n}$)

$$A_i^1\left[B^1_{i,n}|R^1_{i,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^1\left[B^1_{i,n}|R^1_{i,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{27}$$

$$A_i^1\left[B^{1.1}_{i,n}\{^{M_i}/_{x_i}\}|R^1_{i,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^1\left[B^{1.1}_{i,n}\{^{M_i}/_{x_i}\}|R^1_{i,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{28}$$

$$A_i^2\left[B^{1.2}_{i,n}|R^1_{i,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^2\left[B^{1.2}_{i,n}|R^1_{i,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{29}$$

$$A_i^3\left[B^2_{i,n}|R^2_{i,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^3\left[B^2_{i,n}|R^2_{i,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{30}$$

$$A_i^3\left[B^2_{i,n}|R^3_{i,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^3\left[B^2_{i,n}|R^3_{i,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{31}$$

$$A_i^4\left[B^2_{i,n}|R^4_{i,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^4\left[B^2_{i,n}|R^4_{i,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{32}$$

$$A_i^5\left[B^3_{i,n}|R^1_{i+1,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^5\left[B^3_{i,n}|R^1_{i+1,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{33}$$

$$A_i^5\left[B^{3.1}_{i,n}|R^1_{i+1,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^5\left[B^{3.1}_{i,n}|R^1_{i+1,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{34}$$

$$A_i^6\left[B^{3.2}_{i,n}|R^1_{i+1,n}|D^1_{1,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^6\left[B^{3.2}_{i,n}|R^1_{i+1,n}|\overline{D}^1_{1,n}|AD^1\right]\Sigma_R \tag{35}$$

($i \in \{1,\dots,n\}, j \in \{3,\dots,n\}$)

$$A_i^7\left[B^4_{i,n}|R^5_{1,n}|D^1_{i,n}|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_i^7\left[B^4_{i,n}|R^5_{1,n}|\overline{D}^1_{i,n}|AD^1\right]\Sigma_R \tag{36}$$

$$A_{n+1}^7\left[B^5_{1,n}|R^5_{1,n}|D^2_1|AD^1\right]\Sigma_L \sim_{\mathcal{R}} A_{n+1}^7\left[B^5_{1,n}|R^5_{1,n}|\overline{D}^2_1|AD^1\right]\Sigma_R \tag{37}$$

$$A_i^8\left[B^5_{i,n}|R^5_{1,n}|D^2_2|AD^2_{i,n}\right]\Sigma_L \sim_{\mathcal{R}} A_i^8\left[B^5_{i,n}|R^5_{1,n}|\overline{D}^2_2|AD^2_{i,n}\right]\Sigma_R \tag{38}$$

$$A_i^9\left[R^5_{i,n}|D^2_2|AD^3_{i,n}\right]\Sigma_L \sim_{\mathcal{R}} A_i^9\left[R^5_{i,n}|\overline{D}^2_2|AD^3_{i,n}\right]\Sigma_R \tag{39}$$

$$A_{n+1}^9\left[D^2_2|AD^4_1\right]\Sigma_L \sim_{\mathcal{R}} A_{n+1}^9\left[\overline{D}^2_2|AD^4_1\right]\Sigma_R \tag{40}$$

$$A_{n+1}^9\left[D^2_2|AD^4_2\right]\Sigma_L \sim_{\mathcal{R}} A_{n+1}^9\left[\overline{D}^2_2|AD^4_2\right]\Sigma_R \tag{41}$$

$$A'\left[D^2_{1,n}\right]\Sigma_L \sim_{\mathcal{R}} A'\left[\overline{D}^2_{1,n}\right]\Sigma_R \tag{42}$$

$$A''_1\left[D^2_{2,n}\right]\Sigma_L \sim_{\mathcal{R}} \overline{A}''_1\left[\overline{D}^2_{2,n}\right]\Sigma_R \tag{43}$$

$$A''_{j-1}\left[D^2_{j,n}\right]\Sigma_L \sim_{\mathcal{R}} \overline{A}''_{j-1}\left[\overline{D}^2_{j,n}\right]\Sigma_R \tag{44}$$

$$A''_n\left[0\right]\Sigma_L \sim_{\mathcal{R}} \overline{A}''_n\left[0\right]\Sigma_R \tag{45}$$

($i \in \{3,\dots,n\}$)

$$A_i^1\left[\{^{M_i}/_{x_i}\}|R^1_{i,n}|D^1_{1,n}\right]\Sigma_L \sim_{\mathcal{R}} A_i^1\left[\{^{M_i}/_{x_i}\}|R^1_{i,n}|\overline{D}^1_{1,n}\right]\Sigma_R \tag{46}$$

C.3 Proof for the relation

The proof is quite the same as the one without auditor since most of equivalences are identical except that we add a auditor part in parallel, or rename some partial states of processes. There modified cases are equivalences (37) to (41) which are basically representing the auditor's behaviour and can only evolve with internal reduction.

Internal Reductions : We must show for all extended processes A and B, where $A\ \mathcal{R}\ B$, that if $A \longrightarrow A'$ for some A', then $B \longrightarrow B'$ and $A'\ \mathcal{R}\ B'$ for some B'.

(37) We have

$$A \equiv A_{n+1}^7\left[B^5_{1,n}|R^5_{1,n}|D^2_1|AD^1\right]\Sigma_L \text{ and } B \equiv A_{n+1}^7\left[B^5_{1,n}|R^5_{1,n}|\overline{D}^2_1|AD^1\right]\Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ are id$_k$-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3\leq j\leq n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_n^1) \text{ and } \bigcup_{3\leq j\leq n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_n^1) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A_{n+1}^7 \left[B_{1,n}^5|R_{1,n}^5|\overline{c_{DA}}\langle\mathsf{hash}((d_1, \ldots, d_n))\rangle.D_2^2|c_{DA}(h_d).AD_{1,n}^2\right] \Sigma_L$$

and

$$A' \equiv A_1^8 \left[B_{1,n}^5|R_{1,n}^5|D_2^2|AD_{1,n}^2\right] \Sigma_L.$$

It follows from

$$B \equiv A_{n+1}^7 \left[B_{1,n}^5|R_{1,n}^5|\overline{c_{DA}}\langle\mathsf{hash}((d_1, \ldots, d_n))\rangle.\overline{D}_2^2|c_{DA}(h_d).AD_{1,n}^2\right] \Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A_1^8 \left[B_{1,n}^5|R_{1,n}^5|\overline{D}_2^2|AD_{1,n}^2\right] \Sigma_R.$$

Since

$$A' \equiv A_1^8 \left[B_{1,n}^5|R_{1,n}^5|D_2^2|AD_{1,n}^2\right] \Sigma_L \ \mathcal{R} \ B',$$

we derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(38) We have

$$A \equiv A_i^8 \left[B_{i,n}^5|R_{1,n}^5|D_2^2|AD_{i,n}^2\right] \Sigma_L \text{ and } B \equiv A_1^8 \left[B_{i,n}^5|R_{1,n}^5|\overline{D}_2^2|AD_{i,n}^2\right] \Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k\theta_{k-1}\sigma_{\tilde{N}}^{k-1}\Sigma_L$ are id$_k$-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3\leq j\leq n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_n^1) \text{ and } \bigcup_{3\leq j\leq n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A_n^1) = \emptyset.$$

We have two cases :

- If $1 \leq i < n$.

  $$A_i^8 \left[\overline{c_{BA}}\langle x_i\rangle.B_{i+1,n}^5|R_{1,n}^5|D_2^2|c_{BA}(ba_i).AD_{i+1,n}^2\right] \Sigma_L$$

  and

  $$A' \equiv A_{i+1}^8 \left[B_{i+1,n}^5|R_{1,n}^5|D_2^2|AD_{i+1,n}^2\right] \Sigma_L.$$

  It follows from

  $$B \equiv A_i^8 \left[\overline{c_{BA}}\langle x_i\rangle.B_{i+1,n}^5|R_{1,n}^5|\overline{D}_2^2|c_{BA}(ba_i).AD_{i+1,n}^2\right] \Sigma_R$$

  that $B \xrightarrow{\alpha} B'$ where

  $$B' \equiv A_{i+1}^8 \left[B_{i+1,n}^5|R_{1,n}^5|\overline{D}_2^2|AD_{i+1,n}^2\right] \Sigma_R.$$

  We have

  $$A_{i+1}^8 \left[B_{i+1,n}^5|R_{1,n}^5|D_2^2|AD_{i+1,n}^2\right] \Sigma_L \ \mathcal{R} \ B',$$

  and derive $A' \ \mathcal{R} \ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

- If $i = n$.
  $$A_n^8\left[\overline{c_{BA}}\langle x_n\rangle|R^5_{1,n}|D^2_2|c_{BA}(ba_n).AD^3_{1,n}\right]\Sigma_L$$
  and
  $$A' \equiv A_1^9\left[R^5_{1,n}|D^2_2|AD^3_{1,n}\right]\Sigma_L.$$
  It follows from
  $$B \equiv A_n^8\left[\overline{c_{BA}}\langle x_n\rangle|R^5_{1,n}|\overline{D}^2_2|c_{BA}(ba_n).AD^3_{1,n}\right]\Sigma_R$$
  that $B \xrightarrow{\alpha} B'$ where
  $$B' \equiv A_1^9\left[R^5_{1,n}|\overline{D}^2_2|AD^3_{1,n}\right]\Sigma_R.$$
  We have
  $$A_1^9\left[R^5_{1,n}|D^2_2|AD^3_{1,n}\right]\Sigma_L\ \mathcal{R}\ B',$$
  and derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(39) We have

$$A \equiv A_i^9\left[R^5_{i,n}|D^2_2|AD^3_{i,n}\right]\Sigma_L \text{ and } B \equiv A_1^9\left[R^5_{i,n}|\overline{D}^2_2|AD^3_{i,n}\right]\Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k\theta_{k-1}\sigma^{k-1}_{\tilde{N}}\Sigma_L$ are id$_k$-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3\leq j\leq n}\mathrm{fv}(N_j) \subseteq \mathrm{dom}(A_n^1) \text{ and } \bigcup_{3\leq j\leq n}\mathrm{fn}(N_j)\cap\mathrm{bn}(A_n^1) = \emptyset.$$

We have two cases :

- If $1 \leq i < n$.
  $$A_i^9\left[\overline{c_{RA}}\langle(idp_i, hbpr_i, hbr_i)\rangle.R^5_{i+1,n}|D^2_2|c_{RA}(ha_i).AD^3_{i+1,n}\right]\Sigma_L$$
  and
  $$A' \equiv A_{i+1}^9\left[R^5_{i+1,n}|D^2_2|AD^3_{i+1,n}\right]\Sigma_L.$$
  It follows from
  $$B \equiv A_i^9\left[\overline{c_{RA}}\langle(idp_i, hbpr_i, hbr_i)\rangle.R^5_{i+1,n}|\overline{D}^2_2|c_{RA}(ha_i).AD^3_{i+1,n}\right]\Sigma_R$$
  that $B \xrightarrow{\alpha} B'$ where
  $$B' \equiv A_{i+1}^9\left[R^5_{i+1,n}|\overline{D}^2_2|AD^3_{i+1,n}\right]\Sigma_R.$$
  We have
  $$A_{i+1}^9\left[R^5_{i+1,n}|D^2_2|AD^3_{i+1,n}\right]\Sigma_L\ \mathcal{R}\ B',$$
  and derive $A'\ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

- If $i = n$.

  $$A^9_n\left[\overline{c_{RA}}\langle(idp_n, hbpr_n, hbr_n)\rangle|D^2_2|c_{RA}(ha_n).AD^4_1\right]\Sigma_L$$

  and

  $$A' \equiv A^9_{n+1}\left[D^2_2|AD^4_1\right]\Sigma_L.$$

  It follows from

  $$B \equiv A^9_n\left[\overline{c_{RA}}\langle(idp_n, hbpr_n, hbr_n)\rangle|\overline{D}^2_2|c_{RA}(ha_n).AD^4_1\right]\Sigma_R$$

  that $B \xrightarrow{\alpha} B'$ where

  $$B' \equiv A^9_{n+1}\left[\overline{D}^2_2|AD^4_1\right]\Sigma_R.$$

  We have

  $$A^9_{n+1}\left[D^2_2|AD^4_1\right]\Sigma_L \ \mathcal{R}\ B',$$

  and derive $A' \ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(40) We have

$$A \equiv A^9_{n+1}\left[D^2_2|AD^4_1\right]\Sigma_L \text{ and } B \equiv A^9_{n+1}\left[\overline{D}^2_2|AD^4_1\right]\Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k\theta_{k-1}\sigma^{k-1}_{\tilde{N}}\Sigma_L$ are id$_k$-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3\leq j\leq n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A^1_n) \text{ and } \bigcup_{3\leq j\leq n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A^1_n) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A^9_{n+1}\left[D^2_2|\text{if } \phi_{\mathsf{a}}(ba_1, ha_1, idp_1, \ldots, ba_n, ha_n, idp_n, h, h_d) \text{ then } P \text{ else } 0\right]\Sigma_L$$

with $P = AD^4_2$. Since $M_i\theta_{i-1}\sigma^{i-1}_{\tilde{N}}\Sigma_L$, which is equal to $x_i\Sigma_L$ in the A^1_i context, is a id$_i$-valid ballot for $i \in \{1, \ldots, n\}$, using 28, it is obvious that the ϕ_{a} is passed. (The auditor is just creating what the receipt generator did, since these two ones are not cheating, it must be correct.) Then

$$A' \equiv A^9_{n+1}\left[D^2_2|AD^4_2\right]\Sigma_L.$$

It follows from

$$B \equiv A^9_{n+1}\left[\overline{D}^2_2|\text{if } \phi_{\mathsf{a}}(ba_1, ha_1, idp_1, \ldots, ba_n, ha_n, idp_n, h, h_d) \text{ then } P \text{ else } 0\right]\Sigma_R$$

and the fact that $M_i\theta_{i-1}\sigma^{i-1}_{\tilde{N}}\Sigma_R$ are also id$_i$-valid ballots that $B \longrightarrow B'$ where

$$B^{'} = A^9_{n+1}\left[\overline{D}^2_2|AD^4_2\right]\Sigma_R.$$

Since

$$A' \equiv A^9_{n+1}\left[D^2_2|AD^4_2\right]\Sigma_L \ \mathcal{R}\ B',$$

we derive $A' \ \mathcal{R}\ B'$ by the closure of $\mathcal{R}$ under structural equivalence.

(41) We have

$$A \equiv A^9_{n+1}\left[D^2_2 | AD^4_2\right]\Sigma_L \text{ and } B \equiv A^9_{n+1}\left[\overline{D}^2_2 | AD^4_2\right]\Sigma_R$$

for some $N_3, \ldots, N_n$ such that $N_k\theta_{k-1}\sigma^{k-1}_{\tilde{N}}\Sigma_L$ are id_k-valid ballots for $k = 3 \ldots n$, and such that

$$\bigcup_{3 \leq j \leq n} \mathrm{fv}(N_j) \subseteq \mathrm{dom}(A^1_n) \text{ and } \bigcup_{3 \leq j \leq n} \mathrm{fn}(N_j) \cap \mathrm{bn}(A^1_n) = \emptyset.$$

If $A \longrightarrow A'$, then it must be the case that

$$A \equiv A^9_{n+1}\left[c_{DA}(h).D^3_{1,n} | \overline{c_{DA}}\langle \mathsf{Ok} \rangle\right]\Sigma_L$$

and

$$A' \equiv A'\left[D^3_{1,n}\right]\Sigma_L.$$

It follows from

$$B \equiv A^9_{n+1}\left[c_{DA}(h).\overline{D}^3_{1,n} | \overline{c_{DA}}\langle \mathsf{Ok} \rangle.AD^3_{1,n}\right]\Sigma_R$$

that $B \longrightarrow B'$ where

$$B^{'} = A'\left[\overline{D}^3_{1,n}\right]\Sigma_R.$$

Since

$$A' \equiv A'\left[D^3_{1,n}\right]\Sigma_L \mathcal{R} B',$$

we derive $A' \mathcal{R} B'$ by the closure of $\mathcal{R}$ under structural equivalence.

C.4 Proving the Theorem 3

As $\mathcal{R}$ is verifying the three properties of Definition 2, we have to show that for all extended processes A and B, where $A\mathcal{R}B$, that $A \approx_s B$. Using Lemma 9, it is sufficient to prove that $A''_n[0]\Sigma_L \approx_s \overline{A}''_n[0]\Sigma_R$ for any N_i such that $N_i\theta_{i-1}\sigma^{i-1}_{\tilde{N}}\Sigma$ are id_i-valid ballots. As $A''_n[0]\Sigma_L$ is mapped in $\tilde{n}.(\theta|R)\sigma_{\tilde{N}}\Sigma_L$ and $\overline{A}''_n[0]\Sigma_R$ is mapped in $\tilde{n}.(\theta|\overline{R})\sigma_{\tilde{N}}\Sigma_R$, we conclude using Proposition 8.

■

RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399