Deciding knowledge in security protocols under some e-voting theories

Mouhebeddine Berrima, Narjes Ben Rajeb, Véronique Cortier

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Deciding knowledge in security protocols under some e-voting theories

Mouhebeddine Berrima — Narjes Ben Rajeb — Véronique Cortier

N° 6903

Avril 2009

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--6903--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
NANCY - GRAND EST

Deciding knowledge in security protocols under some e-voting theories

Mouhebeddine Berrima* , Narjes Ben Rajeb†, Véronique Cortier‡

Thème SYM — Systèmes symboliques
Équipe-Projet Cassis

Rapport de recherche n° 6903 — Avril 2009 — 29 pages

Abstract: In the last decade, formal methods have proved their interest when analyzing security protocols. Security protocols require in particular to reason about the attacker knowledge. Two standard notions are often considered in formal approaches: deducibility and indistinguishability relations. The first notion states whether an attacker can learn the value of a secret, while the latter states whether an attacker can notice some difference between protocol runs with different values of the secret.

Several decision procedures have been developed so far for both notions but none of them can be applied in the context of e-voting protocols, which require dedicated cryptographic primitives. In this work, we show that both deduction and indistinguishability are decidable in polynomial time for two theories modeling the primitives of e-voting protocols.

Key-words: security protocoles, formal methods, decidability, e-voting, equational theory, knowledge, deduction, statique équivalence

This work has been supported by the ANR-07-SESU-002 AVOTÉ.

* LIP2, Faculté des Sciences, Tunis
† LIP2, Institut National des Sciences Appliquées et de Technologie, Tunis
‡ Loria, CNRS, Nancy

Centre de recherche INRIA Nancy – Grand Est
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy
Téléphone : +33 3 83 59 30 00 — Télécopie : +33 3 83 27 83 19

Décision de la connaissance dans les protocoles de sécurité pour des théories liées au vote électronique

Résumé : Les méthodes formelles se sont révélées très utiles dans l'analyse des protocoles de sécurité. Les protocoles de sécurité demandent en particulier de pouvoir raisonner finement sur la connaissance d'un attaquant. Deux notions classiques sont souvent utilisées: la déduction et l'indistinguabilité. La première notion assure qu'un attaquant ne peut connaître la valeur du secret tandis que la deuxième assure qu'un attaquant ne peut pas faire la différence entre deux exécutions du protocole avec des valeurs différentes pour le secret.

Plusieurs procédure de décision ont été développées pour les deux notions mais aucune d'entre elles ne peut s'appliquer au contexte particulier des protocoles de vote, qui utilisent des primitives cryptographiques inhabituelles. Dans cet article, nous montrons que les relations de déduction et d'indistinguabilité sont toutes deux décidables en temps polynomial, pour deux théories équationnelles modélisant les primitives cryptographiques utilisées dans le vote électronique.

Mots-clés : protocoles de sécurité, méthodes formelles, décidabilité, vote électronique, théorie équationnelle, connaissance, deduction, équivalence statique

1 Introduction

Security protocols aim at securing communication over public networks. They achieve various goals such as secrecy, authenticity or anonymity, using cryptographic primitives like encryption and signatures. In the last decade, several decision procedures have been developed to check the security of cryptographic protocols. For example, secrecy is NP-complete when limiting the number of sessions [RT01]. Several tools have been developed for automatically analyzing security protocols (see e.g. [Bla01, ABB+05]).

In formal approaches, messages sent over a network are modeled by terms that can be seen as trees labeled by function symbols (like *encryption*, *decryption*, etc.), and whose leaves are data. The cryptographic functions properties are described by axioms that define an equational theory. The analysis of protocols then requires precise formulations of the knowledge (capability) of protocol participants and attackers. Many formal definitions explain the knowledge of an attacker in terms of message deducibility. Intuitively, deducibility focuses on the following question: given a set of messages ϕ and a secret s, can an attacker compute s from ϕ ?

However, this concept of deducibility is not always suitable for expressing the knowledge of an attacker. For instance, consider an e-voting protocol that transmits an encrypted choice value of a vote. In this case, it is not sufficient to ask whether an attacker can deduce the value, since he knows all possible values of a vote. A more powerful notion of indistinguishability has been introduced in the framework of applied pi calculus [AF01]: a secret is preserved if an attacker can never distinguish between protocol runs with different values of the secret. This notion is called static equivalence. The term static reflects the fact that this notion applies only to messages transmitted and ignores the protocol behavior. Decidability of both deduction and static equivalence have been studied (e.g. [AC06, Del06, CD07, CLS03]) for several equational theories including for instance exclusive or, homomorphic operators, blind signatures or subterm theories.

In this paper, we focus on e-voting protocols, a recent family of protocols. Such protocols should ensure in particular anonymity of the vote, receipt-freeness and possibly coercion-resistance [DKR09]. They make use of special cryptographic primitives such as re-encryption or trapdoor commitment. However none of the previous decidability results can be applied in the context of e-voting protocols, even for the two key notions of deduction and static equivalence.

We consider two particular equational theories used when modeling e-voting protocols. The first equational theory, denoted by E_{Lee} models the properties of re-encryption, particularly important in the Lee *et al* protocol [LBD+03]. The second equational theory, denoted by E_{Oka} models the properties of blind signatures schemes and trapdoor bit commitment scheme, particularly important in the Okamoto protocol [Oka96]. Our main contribution is to show that both deducibility and static equivalence are decidable in polynomial time for any of these two theories. This is a first (and necessary) step towards a decidability result in the active case. One ingredient of our proof is the locality property [McA93], for which we design an appropriate notion of *subterms*. For static equivalence, our proofs are also inspired from the technique developed in [AC06] for convergent subterm theories.

Detailed proof are provided in appendix for the reviewer convenience. They will appear in a technical report.

2 Preliminaries

In this section, we present some basic notions and notations. We suppose the reader familiar with rewriting systems [DP01].

2.1 Syntax

A signature Σ consists of a finite set of function symbols, each with an arity. We write $ar(f)$ for the arity of a function symbol f. A function symbol with arity 0 is a constant symbol. Given a signature Σ, an infinite set of names $\mathcal{N}$, and an infinite set of variables, the set of terms is defined by the grammar:

$L, M, N, T, U, V ::=$	terms
$k, \ldots, n, \ldots, s$	names
x, y, z	variables
$f(M_1, \ldots, M_k)$	function application

where f ranges over the function symbols of Σ and k matches the arity of f. A term is closed when it does not have free variables (but it may contain names and constant symbols). We write $fn(M)$ for the set of names that occur in the term M.

Given a signature Σ, an infinite set of names $\mathcal{N}$ and an infinite set of variables $\mathcal{X}$, we denote by $\mathcal{T}(\Sigma)$ (resp. $\mathcal{T}(\Sigma, \mathcal{X})$) the set of terms over $\Sigma \cup \mathcal{N}$ (resp. $\Sigma \cup \mathcal{N} \cup \mathcal{X}$. The former is called the set of *closed* terms over Σ, while the latter is called the set of terms over Σ. We denote by Σ_0 the set of the constant symbols of Σ. The size $|T|$ of a term T is defined by $|T| = 1$ if $T \in \mathcal{X} \cup \mathcal{N} \cup \Sigma_0$ and $|f(T_1, \ldots, T_k)| = 1 + \sum_{i=1}^{k} |T_i|$. A substitution is a function that maps variables to terms $\sigma : \mathcal{X} \to \mathcal{T}(\Sigma, \mathcal{X})$. We write $\sigma = \{T_1/x_1, \ldots, T_n/x_n\}$ to say that $x_i\sigma = T_i$ for $1 \leq i \leq n$ and $x\sigma = x$ for $x \neq x_i$. We define the domain of σ, denoted by $dom(\sigma)$, to be the set $\{x \in \mathcal{X} \mid x\sigma \neq x\}$.

A theory (Σ, E) is defined by a signature Σ and a set of equations E given by $\bigcup_{i=1}^{n}\{M_i = N_i\}$ with $M_i, N_i \in \mathcal{T}(\Sigma, \mathcal{X})$. The size of E, is given by $c_E = max_{1 \leq i \leq n}(|M_i|, |N_i|, ar(\Sigma) + 1)$, where $ar(\Sigma)$ is the maximal arity of a function symbol in Σ. We simply write E for the theory (Σ, E). The relation $=_E$ denotes the equational theory generated by (Σ, E) on $\mathcal{T}(\Sigma, \mathcal{X})$, that is an equivalence relation on terms closed under application of contexts and substitutions. We use the symbol == to denote syntactic equality between terms.

Let $\mathcal{R}$ be a rewrite system. We write $U \to V$ if U and V are terms and U may be rewritten to V (in one step) using a rule of $\mathcal{R}$. As usual, if $\mathcal{R}$ is convergent then $U\downarrow$ denoted the normal form of U. We write $\to_{\mathcal{R}}$ instead of $\to$ when the rewrite system is not clear from the context. If there exists a rule $l \to r$ of the rewriting system $\mathcal{R}$ and some substitution θ such that there exist terms U and V such that $U = l\theta$ and $V = r\theta$, then we say that the reduction $U \to V$ occurs *in head*, and we write $U \xrightarrow{h} V$.

A context C is a term with holes, or (more formally) a term with distinguished variables such that each of them occurs at most once in the context. When C is a context, with n distinguished variables $x_1, \ldots, x_n$, we may write $C[x_1, \ldots, x_n]$ instead of C in order to show the variables, and when $T_1, \ldots, T_n$

are terms we may also write $C[T_1, \ldots, T_n]$ for the result of replacing each variable x_i with the corresponding term T_i.

2.2 Frames

In the applied pi calculus [AF01], a message sequence is organized into a frame $\nu\widetilde{n}\sigma$, where $\widetilde{n}$ is a finite set of names (intuitively, the fresh names), ν is the restriction operator from the pi calculus, which intuitively introduces fresh names, and σ is a substitution of the form: $\{M_1/x_1, \ldots, M_k/x_k\}$ where $dom(\sigma) = \{x_1, \ldots, x_k\}$ and $M_1, \ldots, M_k$ are closed terms representing transmitted messages. If the M_i for $1 \leq i \leq n$ are in normal form, then we say that ϕ is in normal form. The variables enable us to refer to each M_i, for example for keeping track of their order of transmission. The free names, denoted $fn(\phi)$, is defined to be the set $\{n \mid n \in \bigcup_{i=1}^{k} fn(M_i) \text{ and } n \notin \widetilde{n}\}$.

2.3 Deduction

Given a theory E and a frame ϕ that represents the information available to an attacker, we may ask whether a given closed term M may be deduced from ϕ. This relation is written $\phi \vdash_E M$ (or shortly $\phi \vdash M$ when E is clear from the context). It is axiomatized by the following rules:

$$\frac{}{\nu\widetilde{n}.\sigma \vdash M} \text{ if } \exists x \in dom(\sigma) \text{ s.t } x\sigma = M \qquad \frac{}{\nu\widetilde{n}.\sigma \vdash s} \text{ if } s \notin \widetilde{n}$$

$$\frac{\phi \vdash M_1 \quad \phi \vdash M_k}{\phi \vdash f(M_1, \ldots, M_k)} \text{ if } f \in \Sigma \qquad \frac{\phi \vdash M \quad M =_E M'}{\phi \vdash M'}$$

Intuitively, the deducible messages are the messages of ϕ and the names that are not protected in ϕ, closed by equality in E and closed by application of functions. The following proposition provides a characterization of deduction [AC06].

Proposition 1 *Let M be a closed term and $\phi = \nu\widetilde{n}\sigma$ be a frame. Then $\phi \vdash_E M$ if and only if there exists a term ζ such that $fn(\zeta) \cap \widetilde{n} = \emptyset$ and $\zeta\sigma =_E M$.*

Such a term ζ is a *recipe* of M. It represents the attacker actions in order to obtain M. As an example, consider the equational theory E_{enc} of pairing and symmetric encryption. This signature is $\Sigma_{enc} = \{pair, enc, fst, snd, dec\}$. The function $enc(x, y)$ allows to encrypt a message x by the key y, while $dec(enc(x, y), y)$ extracts the message x from the ciphertext message $enc(x, y)$ by using the same key y. The theory E_{enc} is defined by the axioms :

$$fst(pair(x, y)) = x \qquad snd(pair(x, y)) = y \qquad dec(enc(x, y), y) = x$$

Let $\phi = \nu k, s.\{enc(s, k)/x, k/y\}$. Then $\phi \vdash k$ and $\phi \vdash s$. Furthermore, we have $k =_{E_{enc}} y\phi$ and $s =_{E_{enc}} dec(x, y)\phi$. In this case, a possible recipe for obtaining k is y and a possible recipe for obtaining s is $dec(x, y)$.

2.4 Static equivalence

We say that two terms M and N are equal in the frame ϕ under a theory E, and write it $(M =_E N)\phi$, if and only if $\phi = \nu\widetilde{n}.\sigma$, $M\sigma =_E N\sigma$

, and $\{\widetilde{n}\} \cap (fn(M) \cup fn(N)) = \emptyset$ for some names $\widetilde{n}$ and substitution σ. Then we say that two frames ϕ and ψ are statically equivalent, and write $\phi \approx_E \psi$, when $dom(\phi) = dom(\psi)$ and when, for all terms M and N, we have $(M =_E N)\phi$ if and only if $(M =_E N)\psi$. For example, consider again the theory E_{enc}. Let $\phi = \nu k.\{enc(s,k)/x, k/y\}$ and $\psi = \nu k.\{enc(s',k)/x, k/y\}$. We have $(dec(x,y) =_{E_{enc}} s)\phi$ but not $(dec(x,y) =_{E_{enc}} s)\psi$. Therefore ϕ and ψ are not statically equivalent.

3 E-voting theories

In this section, we present two e-voting theories: the theory E_{Lee}, used for modeling the properties of the primitives used in the protocol proposed by Lee *et al* [LBD+03] and and the theory E_{Oka}, used for modeling the properties of the primitives used in the protocol proposed by Okamoto [Oka96]. Their modeling has been taken from [DKR09].

3.1 DVP and re-encryption

The protocol due to Lee *et al* relies on two less used cryptographic primitives: re-encryption and designated verifier proofs (DVP) of re-encryption. A re-encryption of a ciphertext (obtained using a randomized encryption scheme) changes the random coins, without changing or revealing the plaintext. A DVP of the re-encryption proves that the two ciphertexts contain indeed the same plaintext. However, a designated verifier proof only convinces one intended person, e.g., the voter, that the re-encrypted ciphertext contains the original plaintext. (see [DKR09] for more explanation).

The theory modeling the protocol due to Lee *et al*, denoted by E_{Lee}, is defined by: $\Sigma_{Lee} = \{getpk, host, pk, checksign, sign, decrypt, rencrypt, penc, dvp, checkdvp, ok, f_0\}$ and the following equations :
(1) $getpk(host(x)) = x$
(2) $checksign(sign(x,y), pk(y)) = x$
(3) $decrypt(penc(x, pk(y), z), y) = x$
(4) $rencrypt(penc(x, pk(y), z), w) = penc(x, pk(y), f_0(z,w))$
(5) $checkdvp(dvp(x, rencrypt(x,y), y, pk(z)), x, rencrypt(x,y), pk(z)) = ok$
(6) $checkdvp(dvp(x,y,z,w), x, y, pk(w)) = ok$

The first equation models the fact that we can obtain the public key of each host (modeled by the functions *getpk* and *host*). The second equation models digital signatures as being signatures with message recovery, it means that the signature (modeled by the term $sign(x,y)$) of the message x by the key y, can be extracted using the *checksign* function and the public key corresponding to y. The third equation is used for modeling the asymmetric probabilistic encryption (modeled by the function *penc*) using a random coin, while the fourth equation models the re-encryption (modeled by the function *rencrypt*), that allows to obtain a different encryption of the same message with another random coin which is function of the original one and the one used during the re-encryption. In the equations (5) and (6), the *dvp* symbol allows to build a designated verifier proof of the fact that a message is a re-encryption of another one and *checkdvp* symbol allows the designated verifier to check that the proof is valid. Note that

checkdvp also succeeds for a fake *dvp* created using the designated verifier's private key.

We denote by $\mathcal{R}_{E_{Lee}}$, the convergent rewriting system associated to E_{Lee} (obtained by orienting the equations from left to right and applying the completion procedure [KB70]), it is defined by:

(1) $getpk(host(x)) \rightarrow x$

(2) $checksign(sign(x, y), pk(y)) \rightarrow x$

(3) $decrypt(penc(x, pk(y), z), y) \rightarrow x$

(4) $rencrypt(penc(x, pk(y), z), w) \rightarrow penc(x, pk(y), f_0(z, w))$

(5) $checkdvp(dvp(x, rencrypt(x, z), z, pk(y)), x, rencrypt(x, z), pk(y)) \rightarrow ok$

(6) $checkdvp(dvp(penc(x, pk(y), z), penc(x, pk(y), f_0(z, w)), w, pk(v)),$
$penc(x, pk(y), z), penc(x, pk(y), f_0(z, w)), pk(v)) \rightarrow ok$

(7) $checkdvp(dvp(x, y, z, w), x, y, pk(w)) \rightarrow ok$

3.2 Trapdoor bit-commitment

The protocol due to Okamoto is based on a trap-door bit commitment and blind signatures. A trap-door bit commitment scheme allows the agent who has performed the commitment to open it in many ways. Hence, trap-door bit commitment does not bind the voter to its vote. Blind signature schemes allow a person to get a message signed by another party without revealing any information about the message to the other party (see [DKR09] for more explanation).

The theory modeling the protocol due to Okamoto, denoted by E_{Oka}, is defined by:
$\Sigma_{Oka} = \{host, getpk, pk, open, sign, checksign, blind, unblind, tdcommit, f_1\}$ and the following axioms :
(1) $getpk(host(x)) = x$
(2) $checksign(sign(x, y), pk(y)) = x$
(3) $unblind(blind(x, y), y) = x$
(4) $unblind(sign(blind(x, y), z), y) = sign(x, y)$
(5) $open(tdcommit(x, y, z), y) = x$
(6) $tdcommit(x, f_1(y, z, w, x), w) = tdcommit(y, z, w)$

The equations (1) and (2) modeling public keys and digital signatures are the same as in previous section. The equations (3) and (4) model blind signatures [Cha82], allowing a person to get a message signed by another party without revealing any information about the message to the other party. The functions *blind* and *unblind* are similar to perfect symmetric key encryption. The fourth equation allows to extract a signature out of a blinded signature, when the blinding factor is known. Finally, the equations (5) and (6) model trap-door bit commitment, modeled by the functions *tdcommit* and *open*, that are again similar to perfect symmetric key encryption. The term $tdcommit(x, y, z)$ models the commitment of the message x under the key y using the trap-door z. The sixth equation expresses that a commitment $tdcommit(y, z, w)$ can be viewed as

a commitment of any value x. To open this commitment as x one has to know the key $f(y, z, w, x)$. Note that this is possible only if one knows the key z used to forge the commitment $tdcommit(y, z, w)$ and the trap-door w.

The main result of [ACD07] ensures that whenever deducibility and static equivalence are decidable for two disjoint theories[1], they are also decidable for their union. Thus, we decompose E_{Oka} into two disjoint sub-theories such that $E_{Oka} = E^1_{Oka} \cup E^2_{Oka}$, where E^1_{Oka} is composed of the first four equations, and E^2_{Oka} is composed of the two last equations. We further notice that the first theory actually corresponds to the equational theory of blind signatures for which both deduction and static equivalence have been proved decidable in polynomial time [AC06]. Thus for proving that deduction and static equivalence are decidable in polynomial time for Okamoto theory, it is sufficient to prove that both deduction and static equivalence are decidable in polynomial time for E^2_{Oka} since the combining algorithm of [ACD07] is done in polynomial time.

In the next we simply write E_{Oka} instead of E^2_{Oka} when it is clear from context, which is defined by the five-th and sex-th equations. The rewriting system associated to E_{Oka}, obtained by orienting the equations from left to right is not convergent. For make it convergent we add the two next equations:
$open(tdcommit(y, z, w), f_1(y, z, w, x)) \rightarrow x$
$f_1(x0, f_1(x, y, z, x0), z, x1) \rightarrow f_1(x, y, z, x1)$

The first rule is added by the completion algorithm [KB70] , and the second equation models the property of transitivity of the key used in the commitment. The convergent rewriting system associated to E_{Oka}, denoted by $\mathcal{R}_{E_{Oka}}$, is defined by the following rewrite rules:

(1) $open(tdcommit(x, y, z), y) \rightarrow x$

(2) $tdcommit(x, f_1(y, z, w, x), w) \rightarrow tdcommit(y, z, w)$

(3) $open(tdcommit(y, z, w), f_1(y, z, w, x)) \rightarrow x$

(4) $f_1(x0, f_1(x, y, z, x0), z, x1) \rightarrow f_1(x, y, z, x1)$

4 Decidability of deduction

In this section we study the decidability of deduction for both theories. In the remaining of the paper, E denotes any of the two theories E_{Lee} or E_{Oka}. Omitted proofs (under each theory) are given separately in appendix.

Our starting point is the locality technique introduced by [McA93], and used in [CLS03, CKRT05, LLT05, Del06]. Given a frame ϕ, a closed term M and a theory E, the proof of $\phi \vdash_E M$ is local if it involves only terms in the set of subterms of $\phi \cup \{M\}$ w.r.t an appropriate notion of subterms St_E. The set $St_E(\phi \cup \{M\})$ is also denoted by $St_E(\phi, M)$. Thus, we define an appropriate notion of subterms for each theory, that we use for proving the locality property.

Definition 1 *Let $M_1, \ldots, M_k \in \mathcal{T}(\Sigma_{Lee}, \mathcal{X})$. The appropriate notion of subterms for E_{Lee}, simply denoted by St_{Lee}, is defined as follows:*

- *$St_{Lee}(u) = u$ when u is a variable or a name,*

[1] Two theories are disjoint if they do not have common function symbols.

- $St_{Lee}(penc(M_1, pk(M_2), f_0(M_3, M_4))) = \{penc(M_1, pk(M_2), f_0(M_3, M_4))\} \cup$
  $St_{Lee}(M_1) \cup St_{Lee}(pk(M_2)) \cup St_{Lee}(f_0(M_3, M_4)) \cup \{penc(M_1, pk(M_2), M_3)\}$,
- $St_{Lee}(sign(M_1, M_2)) = \{sign(M_1, M_2)\} \cup St_{Lee}(M_1) \cup St_{Lee}(pk(M_2))$,
- $St_{Lee}(f(M_1, \ldots, M_k)) = \{f(M_1, \ldots, M_k)\} \cup \bigcup_{i=1}^{k} St_{Lee}(M_i)$ *otherwise*

Definition 2 *Let $M_1, \ldots, M_k \in \mathcal{T}(\Sigma_{Oka}, \mathcal{X})$. The appropriate notion of subterms for E_{Oka}, simply denoted by St_{Oka}, is defined as follows:*

- $St_{Oka}(u) = u$ *when u is a variable or a name*
- $St_{Oka}(f_1(M_1, M_2, M_3, M_4)) = \{f_1(M_1, M_2, M_3, M_4)\} \cup$
  $\bigcup_{i=1}^{4} St_{Oka}(M_i) \cup \{tdcommit(M_1, M_2, M_3)\}$
- $St_{Oka}(f(M_1, \ldots, M_k)) = \{f(M_1, \ldots, M_k)\} \cup \bigcup_{i=1}^{k} St_{Oka}(M_i)$ *otherwise*

The following lemma states the locality property for both theories.

Lemma 1 ***(locality)***
Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form, M be a closed term in normal form. If $\phi \vdash_E M$ then there exists a term ζ_M, called local recipe, such that:

- $fn(\zeta_M) \cap \widetilde{n} = \emptyset$ *and* $\zeta_M\sigma =_E M$.
- *for all $\zeta' \in St_E(\zeta_M)$, for all $\zeta'' \in St_E(\zeta')$ we have $\zeta''\sigma\downarrow \in St_E(\phi, \zeta'\sigma\downarrow) \cup \{\Sigma_0\}$. Moreover, if $\zeta'' = f(\zeta_1, \ldots, \zeta_k)$ and $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow) \xrightarrow{h} \zeta''\sigma\downarrow$ by applying a subterm rule [2] then we have $\zeta''\sigma\downarrow \in St_E(\phi) \cup \{\Sigma_0\}$.*

The algorithm allowing to decide $\phi \vdash_E M$ (Algorithm 1), is inspired from the frame saturation algorithm introduced in [AC06]. The idea is to compute by saturation all subterms of ϕ and M that are deducible from ϕ.

Algorithm 1: Algorithm of Deduction

Input: $\phi = \nu\widetilde{n}.\{M_1/x_1, \ldots, M_k/x_k\}$,$M$
Output: true/false
$S := St_E(\phi, M) \cup \Sigma_0 \cup fn(\phi)$
1 $T := \{(M_i, x_i) \mid i \in \{1..k\}\} \cup \{(n, n) \mid n \in \Sigma_0 \cup fn(\phi)\}$
$T' := \emptyset$
while $T \neq T'$ **do**
  $T' := T$
  for *all* $(t_1, \zeta_1) \ldots, (t_n, \zeta_n) \in T'$ *and for every function symbol* f **do**
2 **if** $f(t_1, \ldots, t_n) \xrightarrow{h} t$ *and* $t \in S$ *and* $t \notin \{t \mid (t, \zeta_t) \in T\}$ **then**
     $(t, f(\zeta_1, \ldots, \zeta_n)) \in T$
3 **if** $t = f(t_1, \ldots, t_n) \in S$ *and* $t \notin \{t \mid (t, \zeta_t) \in T\}$ **then**
     $(t, f(\zeta_1, \ldots, \zeta_n)) \in T$
if $(M, \zeta_M) \in T$ **then**
  return *true*
else
  return *false*

[2] A rule $l \to r$ is called *subterm rule* if $r \in St_E(l)$ or r is constant symbol.

This algorithm terminates since we add only subterms of ϕ and M.

The next proposition shows correctness and completeness of the algorithm for the subterms of a frame ϕ and a closed term M. Moreover, the recipes computed by the algorithm are minimal and local.

Proposition 2 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame such that $\sigma = \{M_1/x_1, \ldots, M_k/x_k\}$ is in normal form, M be a term in normal form and T be the set computed by the Algorithm 1.*

1. *$\forall M' \in St_E(\phi, M)$ we have $\phi \vdash_E M'$ iff there exists a pair $(M', \zeta_{M'}) \in T$.*
2. *Moreover, the recipe $\zeta_{M'}$ computed by the algorithm is minimal and local.*

Corollary 1 *For every frame ϕ in normal form and for every closed term M in normal form, $\phi \vdash_E M$ is decidable.*

Proof. Trivial from proposition 2 (the first part) since $M \in St_E(\phi, M)$. □

The complexity results for deduction and static equivalence are usually given as functions of the DAG-size of the terms. Our notion of DAG-size does not correspond to the usual DAG-size of a term since our notion of subterms is an extension of syntactic subterms. Here, we define the DAG-size of a term M, denoted $|M|_{dag}$, to be the number of distinct subterms w.r.t St_E. Both deduction and static equivalence are decidable in polynomial time.

Proposition 3 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form and M be a closed term in normal form.*

1. *$\phi \vdash_E M$ can be decided in time $\mathcal{O}((|\phi|_{dag} + |M|_{dag})^{ar(\Sigma)+2})$.*
2. *If $\phi \vdash_E M$, then there exits a local recipe ζ_M such that $fn(\zeta_M) \cap \widetilde{n} = \emptyset$, $\zeta_M\sigma =_E M$ and $|\zeta_M|_{dag} \leq |\phi|_{dag} + |M|_{dag}$.*

5 Decidability of static equivalence

This section is devoted to the proof of the decidability of static equivalence. Our approach is based on the result of [AC06] for convergent subterm theories. Intuitively, the idea consists in associating to each frame a finite set of equalities (modulo renaming) such that two frames are equivalent if and only if each frame satisfies the equalities of the other's set. Given a frame ϕ and a theory E, the construction of the set of equalities that characterizes a frame is based on the recipes of elements of a special set $sat_E(\phi)$ representing all deducible subterms of ϕ. In our approach, we extend the set $sat_E(\phi)$ by an additional finite set of terms called *critical* terms, denoted by $I_E(\phi)$. We call them critical terms because they can contribute to the distinction between two frames. Given a frame ϕ, we simply write $sat_{Lee}(\phi)$ and $sat_{Oka}(\phi)$ (resp. $I_{Lee}(\phi)$ and $I_{Oka}(\phi)$) for the set $sat_E(\phi)$ (resp. $I_E(\phi)$) computed under E_{Lee} and E_{Oka} respectively. Our algorithm consists in three steps.

Step 1: saturating frame We compute the set $sat_E(\phi)$ of deducible subterms of ϕ.

Definition 3 *Let $\phi = \nu\widetilde{n}.\{M_1/x_1, \ldots, M_n/x_n\}$ be a frame in normal form. Let $St_E(\phi)$ be the set of subterms of the terms M_i. The set $sat_E(\phi)$ is defined by*

$$sat_E(\phi) = \{M \mid \phi \vdash_E M \text{ and } M \in St_E(\phi) \cup \Sigma_0 \cup fn(\phi)\}$$

The set $sat_E(\phi)$ can be computed using Algorithm 1.

Step 2: adding critical terms We define the set $I_E(\phi)$ for each theory.

Definition 4 *Let $\phi = \nu\widetilde{n}.\{M_1/x_1, \ldots, M_n/x_n\}$ be a frame in normal form. The set $I_{Lee}(\phi)$ is the minimal set such that: If $M_1, M_2, M_3 \in sat_{Lee}(\phi)$, M is deducible from ϕ and $M \in St_{Lee}(penc(M_1, M_2, M_3))$ then $M \in I_{Lee}(\phi)$.*

Proposition 4 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form.*

1. *The set $sat_{Lee}(\phi) \cup I_{Lee}(\phi)$ can be computed in time $\mathcal{O}(|\phi|_{dag}^{2c_{E_{Lee}}+3})$.*
2. *For every $M \in sat_{Lee}(\phi) \cup I_{Lee}(\phi)$, there exists a term ζ_M such that $fn(\zeta_M) \cap \widetilde{n} = \emptyset$, $\zeta_M\sigma =_{E_{Lee}} M$, and $|\zeta_M|_{dag} \leq |\phi|_{dag}(c_{E_{Lee}} + 1)$.*

For the E_{Oka} theory, we do not need to add critical terms, that is, we consider $I_{Oka}(\phi) = \emptyset$.

In what follows, for each frame ϕ we assume fixed the set of local recipes computed by Algorithm 1, denoted by $\mathcal{L}(\phi)$, that corresponds to the terms of $sat_E(\phi) \cup I_E(\phi)$.

Step 3: introducing a finite set of equalities We associate to each frame a finite number of equalities $Eq_E(\phi)$.

Definition 5 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form. The set $Eq_E(\phi)$ is the set of equalities*

$$C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] = C_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}]$$

such that $(C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}])\phi$, $|C_1|, |C_2| \leq c_E$, $M_i, M'_i \in sat_E(\phi) \cup I_E(\phi)$ and $\zeta_{M_i}, \zeta_{M'_i} \in \mathcal{L}(\phi) \cup dom(\sigma)$. If ϕ' is a frame such that $(M =_E N)\phi'$ for every $(M = N) \in Eq_E(\phi)$, we write $\phi' \models Eq_E(\phi)$.

Decidability result: Static equivalence is decidable in polynomial time under both theories. We show (proposition 5) that it is actually sufficient to check for the set of equalities $Eq_E(\phi)$, that is $\phi \approx_E \phi'$ if and only if $\phi \models Eq_E(\phi')$ and $\phi' \models Eq_E(\phi)$. The proof relies on the two following (key) lemmas.

Lemma 2 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form, ζ_M and ζ_N be local recipes of some term T, i.e. $\zeta_M\sigma\downarrow = \zeta_N\sigma\downarrow = T$. For every frame ϕ' such that $\phi' \models Eq_E(\phi)$, we have $(\zeta_M =_E \zeta_N)\phi'$.*

Lemma 3 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form, M be a deducible term in normal form and ζ_M a recipe of M. Then there exists a local recipe of M, denoted by $\widehat{\zeta}_M$, such that for every frame ϕ' such that $\phi' \models Eq_E(\phi)$, we have $(\zeta_M =_E \widehat{\zeta}_M)\phi'$.*

The two lemmas allow us to conclude that it is sufficient to check small equalities.

Proposition 5 *Let ϕ and ϕ' be two frames in normal form. We have $\phi \approx_E \phi'$ if and only if $\phi \models Eq_E(\phi')$ and $\phi' \models Eq_E(\phi)$.*

Proof. ($\rightarrow$) By Definition of static equivalence if $\phi \approx_E \phi'$ then $\phi \models Eq_E(\phi')$ and $\phi' \models Eq_E(\phi)$.
($\leftarrow$) Assume that $\phi' \models Eq_E(\phi)$ and consider M, N such that there exists $\widetilde{n}, \sigma$ such that $\phi = \nu\widetilde{n}\sigma$, $(fn(M) \cup fn(N)) \cap \widetilde{n} = \emptyset$ and $(M =_E N)\phi$. Then $M\sigma =_E N\sigma$, so $(M\sigma)\downarrow == (N\sigma)\downarrow$. Let us show that $(M =_E N)\phi'$. Let $T = (M\sigma)\downarrow$. The terms M and N can be viewed as recipes of T. By lemma 3 there exists $\widehat{M}, \widehat{N}$ such that $(\widehat{M} =_E M)\phi'$ and $(\widehat{N} =_E N)\phi'$. Then, by lemma 2 we obtain that $(\widehat{M} =_E \widehat{N})\phi'$, thus we conclude by transitivity.
Conversely, if $(M =_E N)\phi'$ and $\phi \models Eq_E(\phi')$, we can prove that $(M =_E N)\phi$. We conclude $\phi \approx_E \phi'$. □

Theorem 1 *Let ϕ, ϕ' be two frames in normal form. $\phi \approx_E \phi'$ is decidable in polynomial time.*

Proof. The deciding procedure of static equivalence proceeds in two steps. Firstly, we construct $sat_E(\phi) \cup I_E(\phi)$ and $sat_E(\phi') \cup I_E(\phi')$. In the second step, we construct the sets $Eq_{E_E}(\phi)$ and $Eq_{E_E}(\phi')$. Finally, and according to proposition 5, we test if each frame satisfy the equality from other's set. Moreover, according to the proposition 4, the construction of $sat_E(\phi) \cup I_E(\phi)$ and $sat_E(\phi') \cup I_E(\phi')$ can be done in polynomial time and for each term M of $sat_E(\phi) \cup I_E(\phi)$ or $sat_E(\phi') \cup I_E(\phi')$, the term ζ_M has a polynomial DAG-size. Thus, we can prove, like in [AC06], that this procedure can be done in polynomial time (in the DAG-size of inputs terms). □

6 Conclusion

In this paper, we have proved that deduction and static equivalence are both decidable in polynomial time for two important equational theories: Lee *et al* and Okamoto theories. Decidability of deduction relies on the existence of a locality property with respect to an appropriate notion of subterms that we have defined for each theory. Decidability of static equivalence relies on result of [AC06] for convergent subterms theories and a special set of critical terms that we have introduced. For Okamoto theory we have applied a modular approach by using the combining algorithm of [ACD07]. A further work is to generalize the construction of critical terms in order to deal with a wider class of e-voting theories. As emphasized in introduction, our work is dedicated to the passive case, where an attacker can simply eavesdrop the communication in order to get some information. An important (and involved) development of our work is to design a decision procedure in the active case, where the adversary can fully interact with the protocol.
Acknowledgment. Many thanks to Stéphanie Delaune for suggestions and interesting help.

References

[ABB+05] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. The AVISPA

Tool for the automated validation of internet security protocols and applications. In K. Etessami and S. Rajamani, editors, *17th International Conference on Computer Aided Verification, CAV'2005*, volume 3576 of *Lecture Notes in Computer Science*, pages 281–285, Edinburgh, Scotland, 2005. Springer.

[AC04] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. In *Proc. 31st Int. Coll. Automata, Languages, and Programming (ICALP'2004)*, volume 3142 of *Lecture Notes in Computer Science*, pages 46–58, Turku, Finland, July 2004. Springer.

[AC06] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2):2–32, November 2006.

[ACD07] M. Arnaud, V. Cortier, and S. Delaune. Combining algorithms for deciding knowledge in security protocols. In *Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)*, volume 4720 of *Lecture Notes in Artificial Intelligence*, pages 103–117, Liverpool, UK, September 2007. Springer.

[AF01] 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.

[Bla01] B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Proc. of the 14th Computer Security Foundations Workshop (CSFW'01)*, Cape Breton, Nova Scotia, Canada, June 2001. IEEE Computer Society Press.

[CD07] V. Cortier and S. Delaune. Deciding knowledge in security protocols for monoidal equational theories. In *14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07)*, volume 4790 of *LNAI*, pages 196–210. Springer, 2007.

[Cha82] D. Chaum. Blind signatures for untraceable payments. In *CRYPTO*, pages 199–203, 1982.

[CKRT05] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. *Theoretical Computer Science*, 338(1-3):247–274, June 2005.

[CLS03] H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proc. of 18th Annual IEEE Symposium on Logic in Computer Science (LICS '03)*, pages 271–280, Los Alamitos, CA, 2003. IEEE Computer Society.

[Del06] S. Delaune. Easy intruder deduction problems with homomorphisms. *Information Processing Letters*, 97(6):213–218, March 2006.

[DKR09] S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 2009. To appear, available at `http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-jcs08.pdf`.

[DP01] N. Dershowitz and D. Plaisted. Rewriting. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, pages 535–610. Elsevier and MIT Press, 2001.

[KB70] D. E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, 1970.

[LBD+03] Lee, Boyd, Dawson, Kim, Yang, and Yoo. Providing receipt-freeness in mixnet-based voting protocols. In *ICISC: International Conference on Information Security and Cryptology*. LNCS, 2003.

[LLT05] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In Jürgen Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 308–322, Nara, Japan, April 2005. Springer.

[McA93] McAllester. Automatic recognition of tractability in inference relations. *JACM: Journal of the ACM*, 40, 1993.

[Oka96] T. Okamoto. An electronic voting scheme. In *IFIP World Conference on IT Tools*, pages 21–30, 1996.

[RT01] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *Proc. of the 14th Computer Security Foundations Workshop (CSFW'01)*, pages 174–190, Cape Breton, Nova Scotia, Canada, 2001. IEEE Computer Society Press.

Appendix

A Proofs of Section 4

We introduce the definition of a term by *composition* and a term by *decomposition*.

Definition 6 *Let E be a theory, $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form, and $t, t_i \in \mathcal{T}(\Sigma, \mathcal{X})$ for $i = 1..k$ be non closed terms, we say that:*

- *t is a term by decomposition if $t \stackrel{\text{def}}{=} f(t_1, \ldots, t_k)$ and $f(t_1\sigma\downarrow, \ldots, t_k\sigma\downarrow) \xrightarrow{h}_E t\sigma\downarrow$,*
- *t is a term by composition if t is a variable or if $t \stackrel{\text{def}}{=} f(t_1, \ldots, t_k)$ and $f(t_1\sigma\downarrow, \ldots, t_k\sigma\downarrow) == t\sigma\downarrow$.*

Let M be a term, $head(M)$ denotes the head function symbol of M.

A.1 Proofs under Lee *et al* theory

The next lemma will be used in the proof of locality lemma.

Lemma 4 *Let $\mathcal{R}_{E_{Lee}}$ be the convergent rewriting system associated to E_{Lee}. Let $M, M_1, \ldots, M_k$ be terms in normal form. If $f(M_1, \ldots, M_k)$ is not in normal form, then we have $M = f(M_1, \ldots, M_k)\downarrow$ iff $f(M_1, \ldots, M_k) \xrightarrow{h} M$.*

Proof. ($\rightarrow$) Let $M_1, \ldots, M_k$ are in normal form, $f(M_1, \ldots, M_k)$ is not in normal form, and $f(M_1, \ldots, M_k) \rightarrow^* M$. Since $M_1, \ldots, M_k$ are in normal form, then the first step of reduction is in head. If the rule (1), (2), (3), (5), (6) or (7) is applied then it is clear that the term obtained is in normal form. If the rule (4) is applied, it is easy to verify that $penc(M_1, pk(M_2), f_0(M_3, M_4))$ is in normal form whenever $penc(M_1, pk(M_2), M_3)$ and M_4 are in normal form. Then whatever the rule applied, we obtain always a term in normal form. Thus $f(M_1, \ldots, M_k) \xrightarrow{h} M'$ with M' in normal form. Since $\mathcal{R}_{E_{Lee}}$ is convergent, we conclude that M=M'.
($\leftarrow$) If $f(M_1, \ldots, M_k) \xrightarrow{h} M$, then by definition of $\downarrow$ we have $f(M_1, \ldots, M_k)\downarrow = M$. □ **Proof of lemma 1**
By proposition of characterization of deduction (proposition 1), there exists a term ζ_M satisfying the first condition. We choose one whose size is minimal. The second condition is proved by induction on the size of ζ_M.

Base case : ζ_M is a variable or a name, then the second condition hold since $St_{Lee}(\zeta_M) = \{\zeta_M\}$.

Induction step: Let $\zeta_M = f(\zeta_1, \ldots, \zeta_k)$ with ζ_i are the minimal recipes of $\zeta_i\sigma\downarrow$. By induction hypothesis we have for all $\zeta' \in St_{Lee}(\zeta_i)_{i=1..k}$, for all $\zeta'' \in St_{Lee}(\zeta')$ we have $\zeta''\sigma\downarrow \in St_{Lee}(\phi, \zeta'\sigma\downarrow) \cup \{\Sigma_{0_{Lee}}\}$. To conclude that for all $\zeta'' \in St_{Lee}(\zeta')$ we have $\zeta''\sigma\downarrow \in St_{Lee}(\phi, \zeta'\sigma\downarrow) \cup \{\Sigma_{0_{Lee}}\}$ for any $\zeta' \in St_{Lee}(\zeta_M)$, it is sufficient to show for all $\zeta'' \in St_{Lee}(\zeta_M)$, we have $\zeta''\sigma\downarrow \in St_{Lee}(\phi, M) \cup \{\Sigma_{0_{Lee}}\}$. For this, it is sufficient to prove that for all $i = 1..k$ we have $\zeta_i\sigma\downarrow \in St_{Lee}(\phi, M) \cup \{\Sigma_{0_{Lee}}\}$, since if $\zeta_i\sigma\downarrow \in St_{Lee}(\phi, M) \cup \{\Sigma_{0_{Lee}}\}$ then

for all $\zeta'' \in St_{Lee}(\zeta_i)$ we have $\zeta''\sigma\downarrow \in St_{Lee}(\phi, \zeta_i\sigma\downarrow) \cup \{\Sigma_{0_{Lee}}\} \subseteq St_{Lee}(\phi, M) \cup \{\Sigma_{0_{Lee}}\}$.

- If $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow)$ is in normal form, then for all $i = 1..k$ we have $\zeta_i\sigma\downarrow \in St_{Lee}(f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow))$ and we conclude.

- If $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow)$ is not in normal form. Since $\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow$ are in normal form then by lemma 4 we have $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow) \xrightarrow{h} M$, in this case we distinguish five cases according to f:

- If $f = checkdvp$, this case cannot appear by minimality of ζ_M, indeed ok would be a recipe smaller than ζ_M.
- If $f = getpk$, this implies k=1, so we have $\zeta_M = getpk(\zeta_1)$ and since $\zeta_M\sigma$ is reduced then $head(\zeta_1\sigma\downarrow) = host$. We distinguish several cases for ζ_1.
  - ζ_1 is a variable, so we have $\zeta_1\sigma\downarrow \in St_{Lee}(\phi)$, and since the applied rule is a subterm rule then $M \in St_{Lee}(\zeta_1\sigma\downarrow) \subseteq St_{Lee}(\phi)$, thus we conclude.
  - $\zeta_1 = g(\zeta'_1, \ldots, \zeta'_k)$ and $g(\zeta'_1\sigma\downarrow, \ldots, \zeta'_k\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$ by applying a rule different from (4). Then by induction hypothesis we have $\zeta_1\sigma\downarrow \in St_{Lee}(\phi) \cup \{\Sigma_{0_{Lee}}\}$, and since the applied rule is a subterm rule then $M \in St_{Lee}(\zeta_1\sigma\downarrow) \subseteq St_{Lee}(\phi) \cup \{\Sigma_{0_{Lee}}\}$, thus we conclude. If the rule (4) is applied, this case cannot appear because this implies $head(\zeta_1\sigma\downarrow) = penc$ and by equational theory $\zeta_M\sigma$ cannot reduced, contradiction.
  - $\zeta_1 = g(\zeta'_1, \ldots, \zeta'_k)$ and $g(\zeta'_1\sigma\downarrow, \ldots, \zeta'_k\sigma\downarrow)$ is in normal form with $g \neq host$, this case cannot appear because this implies that $\zeta_M\sigma$ cannot reduced, contradiction.
  - $\zeta_1 = host(\zeta'_1)$, this case cannot appear by minimality of ζ_M, because we have always ζ'_1 smaller than ζ_M.
- $f = checksign$, this implies k=2, so we have $\zeta_M = checksign(\zeta_1, \zeta_2)$ and since $\zeta_M\sigma$ is reduced then $head(\zeta_1\sigma\downarrow) = sign$ and $\zeta_2\sigma\downarrow \in St_{Lee}(\zeta_1\sigma\downarrow)$. Thus it is sufficient to prove that $\zeta_1\sigma\downarrow \in St_{Lee}(\phi, M)$. We distinguish several cases for ζ_1.
  - ζ_1 is a variable, so we have $\zeta_1\sigma\downarrow \in St_{Lee}(\phi)$, and since the applied rule is a subterm rule then $M \in St_{Lee}(\zeta_1\sigma\downarrow) \subseteq St_{Lee}(\phi)$, thus we conclude.
  - $\zeta_1 = g(\zeta'_1, \ldots, \zeta'_k)$ and $g(\zeta'_1\sigma\downarrow, \ldots, \zeta'_k\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$ by applying a rule different from (4). Then by induction hypothesis we have $\zeta_1\sigma\downarrow \in St_{Lee}(\phi) \cup \{\Sigma_{0_{Lee}}\}$, and since the applied rule is a subterm rule then $M \in St_{Lee}(\zeta_1\sigma\downarrow) \subseteq St_{Lee}(\phi) \cup \{\Sigma_{0_{Lee}}\}$, thus we conclude. If the rule (4) is applied, this case cannot appear because this implies $head(\zeta_1\sigma\downarrow) = penc$ and by equational theory $\zeta_M\sigma$ cannot reduced, contradiction.
  - $\zeta_1 = g(\zeta'_1, \ldots, \zeta'_k)$ and $g(\zeta'_1\sigma\downarrow, \ldots, \zeta'_k\sigma\downarrow)$ is in normal form with $g \neq sign$, this case cannot appear because this implies that $\zeta_M\sigma$ cannot reduced, contradiction.

- $\zeta_1 = sign(\zeta_1', \zeta_2')$, this case cannot appear by minimality of ζ_M, because we have always ζ_1' smaller than ζ_M.

- If $f = rencrypt$, this implies k=2, so we have $\zeta_M = rencrypt(\zeta_1, \zeta_2)$ and since $\zeta_M\sigma$ is reduced then $head(\zeta_1\sigma\downarrow) = penc$. By Definition of subterms, we know that $\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow \in St_{Lee}(M)$, then we conclude.

- If $f = decrypt$, this implies k=2, so we have $\zeta_M = decrypt(\zeta_1, \zeta_2)$ and since $\zeta_M\sigma$ is reduced then $head(\zeta_1\sigma\downarrow) = penc$ and $\zeta_2\sigma\downarrow \in St_{Lee}(\zeta_1\sigma\downarrow)$. Thus it is sufficient to prove that $\zeta_1\sigma\downarrow \in St_{Lee}(\phi, M)$. We distinguish several cases for ζ_1.

  - ζ_1 is a variable, so we have $\zeta_1\sigma\downarrow \in St_{Lee}(\phi)$,and since the applied rule is a subterm rule then $M \in St_{Lee}(\zeta_1\sigma\downarrow) \subseteq St_{Lee}(\phi)$, thus we conclude.
  - $\zeta_1 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$ by applying a rule different from (4). Then by induction hypothesis we have $\zeta_1\sigma\downarrow \in St_{Lee}(\phi) \cup \{\Sigma_{0_{Lee}}\}$, and since the applied rule is a subterm rule then $M \in St_{Lee}(\zeta_1\sigma\downarrow) \subseteq St_{Lee}(\phi) \cup \{\Sigma_{0_{Lee}}\}$, thus we conclude.
  - $\zeta_1 = rencrypt(\zeta_1', \zeta_2')$ and $rencrypt(\zeta_1'\sigma\downarrow, \zeta_2'\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$. This case cannot appear by minimality of ζ_M, because we have always $decrypt(\zeta_1', \zeta_2)$ smaller than ζ_M.
  - $\zeta_1 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow)$ is in normal form with $g \neq penc$, this case cannot appear because this implies that $\zeta_M\sigma$ cannot reduced, contradiction.
  - $\zeta_{M_1} = penc(\zeta_1', pk(\zeta_2'), \zeta_3')$. This case cannot appear by minimality of ζ_M, because we have ζ_1' smaller than ζ_M. □

A.2 Proofs under Okamoto theory

Lemma 5 *Let $\mathcal{R}_{E_{Oka}}$ be the convergent rewriting system associated to E_O. Let $M, M_1, \ldots, M_k$ be terms in normal form. If $f(M_1, \ldots, M_k)$ is not in normal form, then we have $M = f(M_1, \ldots, M_k)\downarrow$ iff $f(M_1, \ldots, M_k) \xrightarrow{h} M$.*

Proof. ($\rightarrow$) Let $M_1, \ldots, M_k$ are in normal form, $f(M_1, \ldots, M_k)$ is not in normal form, and $f(M_1, \ldots, M_k) \rightarrow^* M$. Since $M_1, \ldots, M_k$ are in normal form, then the first step of reduction is in head. If the rule (1) or (3) is applied then it is clear that the term obtained is in normal form. It remains the cases of the rules (2) and (4). Let us examine these two cases:

- For the case when the rule (2) is applied. Let M_1', M_2' be a terms such that $tdcommit(M_1, M_2, M_3) \xrightarrow{h} tdcommit(M_1', M_2', M_3)$ with M_2 is of the form $f_1(M_1', M_2', M_3, M_1)$. The only case in which the term $tdcommit(M_1', M_2', M_3)$ can be reduce is when M_2' is of the form $f_1(M_1'', M_2'', M_3, M_1')$ for some terms M_1'', M_2''. But in such case, we have $M_2 = f_1(M_1', f_1(M_1'', M_2'', M_3, M_1'), M_3, M)$ (for some term M) is not in normal form, contradiction. Thus we conclude that $tdcommit(M_1', M_2', M_3)$ is always in normal form.

- For the case when the rule (4) is applied. We have $f_1(M_1, M_2, M_3, M_4) \xrightarrow{h} f_1(M_1', M_2', M_3, M_4)$ with M_2 is of the form $f_1(M_1', M_2', M_3, M_1)$. The only

case in which $f_1(M_1', M_2', M_3, M_4)$ not in normal form, is the case when M_2' is of the form $f_1(M_1'', M_2'', M_3, M_1')$ for some terms M_1'', M_2''. But in such case, we have $M_2 = f_1(M_1', f_1(M_1'', M_2'', M_3, M_1'), M_3, M_1)$ is not in normal form, contradiction. Thus we conclude that if we applied the rule (4) on the terms in normal form, we obtain always a term in normal form.

Then whatever the rule applied, we obtain always a term in normal form. Thus $f(M_1, \ldots, M_k) \xrightarrow{h} M'$ with M' in normal form. Since $\mathcal{R}_{E_{Oka}}$ is convergent, we conclude that M=M'.
($\leftarrow$) If $f(M_1, \ldots, M_k) \xrightarrow{h} M$, then by definition of $\downarrow$ we have $f(M_1, \ldots, M_k)\downarrow = M$. □

Proof of lemma 1
By proposition 1, there exists a term ζ_M satisfying the first condition. We choose one whose size is minimal. The second condition is proved by induction on the size of ζ_M.

Base case : ζ_M is a variable or a name, then the second condition hold since $St_{Oka}(\zeta_M) = \{\zeta_M\}$.

Induction step: Let $\zeta_M = f(\zeta_1, \ldots, \zeta_k)$ with ζ_i are the minimal recipes of $\zeta_i\sigma\downarrow$. By induction hypothesis we have for all $\zeta' \in St_{Oka}(\zeta_i)_{i=1..k}$, for all $\zeta'' \in St_{Oka}(\zeta')$ we have $\zeta''\sigma\downarrow \in St_{Oka}(\phi, \zeta'\sigma\downarrow)$. To conclude that for all $\zeta'' \in St_{Oka}(\zeta')$ we have $\zeta''\sigma\downarrow \in St_{Oka}(\phi, \zeta'\sigma\downarrow)$ for any $\zeta' \in St_{Oka}(\zeta_M)$, it is sufficient to show for all $\zeta'' \in St_{Oka}(\zeta_M)$, we have $\zeta''\sigma\downarrow \in St_{Oka}(\phi, M)$. For this, it is sufficient to prove that for all $i = 1..k$ we have $\zeta_i\sigma\downarrow \in St_{Oka}(\phi, M)$, since if $\zeta_i\sigma\downarrow \in St_{Oka}(\phi, M)$ then for all $\zeta' \in St_{Oka}(\zeta_i)$ we have $\zeta'\sigma\downarrow \in St_{Oka}(\phi, \zeta_i\sigma\downarrow) \subseteq St_{Oka}(\phi, M)$.

- If $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow)$ is in normal form, so for all $i = 1..k$ we have $\zeta_i\sigma\downarrow \in St_{Oka}(f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow))$ and we conclude.

- If $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow)$ is not in normal form. Since $\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow$ are in normal form then by lemma 5 we have $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow) \xrightarrow{h} M$, in this case we distinguish some cases according to the rule applied:

- If the rule (1) is applied, then we have $\zeta_M = open(\zeta_1, \zeta_2)$. Since $\zeta_M\sigma$ is reduced to its normal form, then $head(\zeta_1\sigma\downarrow) = tdcommit$ and $\zeta_2\sigma\downarrow \in St_{Oka}(\zeta_1\sigma\downarrow)$. Thus it is sufficient to prove that $\zeta_1\sigma\downarrow \in St_{Oka}(\phi, M)$. We distinguish several cases for ζ_1:
  - ζ_1 is a variable, then $\zeta_1\sigma\downarrow \in St_{Oka}(\phi)$, and since the applied rule is a subterm rule then $M \in St_{Oka}(\zeta_1\sigma\downarrow) \subseteq St_{Oka}(\phi)$, thus we conclude.
  - $\zeta_1 = tdcommit(\zeta_1', \zeta_2', \zeta_3')$. This case cannot appear by minimality of ζ_M because we have always ζ_1' smaller than ζ_M.
  - $\zeta_1 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow)$ is in normal form with $g \neq tdcommit$, this case cannot appear because this implies that $\zeta_M\sigma$ cannot reduced, contradiction.
  - $\zeta_1 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$ by applying a rule different from (4). Then by induction hypothesis we have $\zeta_1\sigma\downarrow \in$

$St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, and since the applied rule is a subterm rule then $M \in St_{Oka}(\zeta_1\sigma\downarrow) \subseteq St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, thus we conclude. If the rule (4) is applied, this case cannot appear because this implies $head(\zeta_1\sigma\downarrow) = f_1$, thus by equational theory $\zeta_M\sigma$ cannot reduced, contradiction.

- If the rule (2) is applied, then we have $\zeta_M = tdcommit(\zeta_1, \zeta_2, \zeta_3)$. Since $\zeta_M\sigma$ is reduced to its normal form, then $head(\zeta_2\sigma\downarrow) = f_1$ and $\zeta_1\sigma\downarrow, \zeta_3\sigma\downarrow \in St_{Oka}(\zeta_2\sigma\downarrow)$. Thus it is sufficient to prove that $\zeta_2\sigma\downarrow \in St_{Oka}(\phi, M)$. We distinguish several cases for ζ_2:
  - ζ_2 is a variable, then $\zeta_2\sigma\downarrow \in St_{Oka}(\phi)$, and since the applied rule is a subterm rule then $M \in St_{Oka}(\zeta_2\sigma\downarrow) \subseteq St_{Oka}(\phi)$, thus we conclude.
  - $\zeta_2 = f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4')$. This case cannot appear by minimality of ζ_M because we have always $tdcommit(\zeta_1', \zeta_2', \zeta_3')$ smaller than ζ_M.
  - $\zeta_2 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow)$ is in normal form with $g \neq f_1$, this case cannot appear because this implies that $\zeta_M\sigma$ cannot reduced, contradiction.
  - $\zeta_2 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$ by applying the rule (1) or (3). Then by induction hypothesis we have $\zeta_1\sigma\downarrow \in St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, and since the applied rule is a subterm rule then
    $M \in St_{Oka}(\zeta_2\sigma\downarrow) \subseteq St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, thus we conclude. If the rule (2) is applied, this case cannot appear because this implies $head(\zeta_2\sigma\downarrow) = tdcommit$, thus by equational theory $\zeta_M\sigma$ cannot reduced, contradiction.
  - If $\zeta_2\sigma\downarrow$ is obtained by the rule (4), i.e. $\zeta_2 = f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4')$. This case cannot appear by minimality of ζ_M, because we have always $tdcommit(\zeta_1', \zeta_2', \zeta_3)$ smaller than ζ_M.
- If the rule (3) is applied, then we have $\zeta_M = open(\zeta_1, \zeta_2)$. Since $\zeta_M\sigma$ is reduced to its normal form then $head(\zeta_2\sigma\downarrow) = f_1$ and $\zeta_1\sigma\downarrow \in St_{Oka}(\zeta_2\sigma\downarrow)$. Thus it is sufficient to prove that $\zeta_2\sigma\downarrow \in St_{Oka}(\phi, M)$. We distinguish several cases for ζ_2:
  - ζ_2 is a variable, then $\zeta_2\sigma\downarrow \in St_{Oka}(\phi)$, and since the applied rule is a subterm rule then $M \in St_{Oka}(\zeta_2\sigma\downarrow) \subseteq St_{Oka}(\phi)$, thus we conclude.
  - $\zeta_2 = f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4')$. This case cannot appear by minimality of ζ_M because we have always ζ_4' smaller than ζ_M.
  - $\zeta_2 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow)$ is in normal form with $g \neq f_1$, this case cannot appear because this implies that $\zeta_M\sigma$ cannot reduced, contradiction.
  - $\zeta_2 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$ by applying the rule (1) or (3). Then by induction hypothesis we have $\zeta_1\sigma\downarrow \in St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, and since the applied rule is a subterm rule then
    $M \in St_{Oka}(\zeta_2\sigma\downarrow) \subseteq St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, thus we conclude. If the rule (2) is applied, this case cannot appear because this implies $head(\zeta_2\sigma\downarrow) = tdcommit$, thus by equational theory $\zeta_M\sigma$ cannot reduced, contradiction.

– If $\zeta_2\sigma\downarrow$ is obtained by the rule (4), i.e. $\zeta_2 = f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4')$. This case cannot appear by minimality of ζ_M, indeed ζ_4' will be smaller than ζ_M.

- If the rule (4) is applied, then we have $\zeta_M = f_1(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$. Since $\zeta_M\sigma$ is reduced to its normal form then $head(\zeta_2\sigma\downarrow) = f_1$ and $\zeta_1\sigma\downarrow, \zeta_3\sigma\downarrow \in St_{Oka}(\zeta_2\sigma\downarrow)$ and since $\zeta_4\sigma\downarrow \in St_{Oka}(\zeta_M\sigma\downarrow)$, thus it is sufficient to prove that $\zeta_2\sigma\downarrow \in St_{Oka}(\phi, M)$. We distinguish several cases for ζ_2:

  – ζ_2 is a variable, then $\zeta_2\sigma\downarrow \in St_{Oka}(\phi)$, and since the applied rule is a subterm rule then $M \in St_{Oka}(\zeta_2\sigma\downarrow) \subseteq St_{Oka}(\phi)$, thus we conclude.

  – $\zeta_2 = f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4')$ is by composition. This case cannot appear by minimality of ζ_M because we have always $f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4)$ smaller than ζ_M.

  – $\zeta_2 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow)$ is in normal form with $g \neq f_1$, this case cannot appear because this implies that $\zeta_M\sigma$ cannot reduced, contradiction.

  – $\zeta_2 = g(\zeta_1', \ldots, \zeta_k')$ and $g(\zeta_1'\sigma\downarrow, \ldots, \zeta_k'\sigma\downarrow) \xrightarrow{h} \zeta_1\sigma\downarrow$ by applying the rule (1) or (3). Then by induction hypothesis we have $\zeta_2\sigma\downarrow \in St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, and since the applied rule is a subterm rule then
  $M \in St_{Oka}(\zeta_2\sigma\downarrow) \subseteq St_{Oka}(\phi) \cup \{\Sigma_{0_{Oka}}\}$, thus we conclude. If the rule (2) is applied, this case cannot appear because this implies $head(\zeta_2\sigma\downarrow) = tdcommit$, thus by equational theory $\zeta_M\sigma$ cannot reduced, contradiction.

  – If $\zeta_2\sigma\downarrow$ is obtained by the rule (4), i.e. $\zeta_2 = f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4')$. This case is impossible by minimality of ζ_M, because we have $f_1(\zeta_1', \zeta_2', \zeta_3', \zeta_4)$ smaller than ζ_M. □

A.3 Decidability result for $\vdash_E$ under the two theories

Proof of proposition 2.
Proof of the first part:
($\rightarrow$) Let $M' \in St_E(\phi, M)$ and $\phi \vdash_E M'$, then by lemma 1 there exists a local recipe $\zeta_{M'}$ of M' s.t for all $\zeta' \in St_{Oka}(\zeta_M)$, for all $\zeta'' \in St_E(\zeta')$ we have $\zeta''\sigma\downarrow \in St_E(\phi, \zeta'\sigma\downarrow)$. We prove by induction on the size of $\zeta_{M'}$ that there exists $(M', \overline{\zeta}_{M'}) \in T$ with $\overline{\zeta}_{M'}$ is a recipe of M' computed by the algorithm.

Base case: If $\zeta_{M'}$ is a variable or a name, then by instruction 1 we have $(M', \overline{\zeta}_{M'}) \in T$ (with $\overline{\zeta}_{M'}$ is the variable chosen by the algorithm).

Inductive step: Let $\zeta_{M'} = f(\zeta_1, \ldots, \zeta_n)$. Since $\zeta_i\sigma\downarrow \in St_E(\phi, M')$ (because $\zeta_{M'}$ is local) and as consequence $\zeta_i\sigma\downarrow \in St_E(\phi, M)$ because $M' \in St_E(\phi, M)$, then by induction hypothesis we have $((\zeta_i\sigma)\downarrow, \overline{\zeta}_i) \in T$ for $i = 1..n$, with $\overline{\zeta}_i$ are the recipes of $(\zeta_i\sigma)\downarrow$ computed by the algorithm, thus:

- If $\zeta_{M'}\sigma\downarrow == f(\zeta_1\sigma\downarrow, \ldots, \zeta_n\sigma\downarrow)$, then by the instruction 3 of the Algorithm 1 we have $(M', \overline{\zeta}_{M'}) \in T$ (with $\overline{\zeta}_{M'} = f(\overline{\zeta}_1, \ldots, \overline{\zeta}_n)$).

- If $f(\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow)$ is not in normal form. Since $\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow$ are in normal form then by lemma 4 (or lemma 5) we have $f(\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow) \xrightarrow{h} M'$. Then by the instruction 2 of the Algorithm 1 we have $(M',\overline{\zeta}_{M'}) \in T$ (with $\overline{\zeta}_{M'} = f(\overline{\zeta}_1,\ldots,\overline{\zeta}_n)$).

($\leftarrow$) If there exists a pair $(M',\zeta_{M'}) \in T$, then (by construction of T) we have $\zeta_{M'}\sigma =_E M'$ and $fn(\zeta_{M'}) \cap \widetilde{n} = \emptyset$, thus by proposition 1 we have $\phi \vdash_E M'$.
Proof of the second part:
Let $M' \in St_E(\phi, M)$ s.t $\phi \vdash_E M'$. Consider $\zeta_{M'}$ a minimal local recipe of M'. We proceed by induction on the size of $\zeta_{M'}$ that $(M',\zeta_{M'})$ is computed by the algorithm, i.e $(M',\zeta_{M'}) \in T$. This will prove that recipes computed by the algorithm are local.

Base case: If $\zeta_{M'}$ is a variable or a name, then by instruction 1 we have $(M',\zeta_{M'}) \in T$.

Inductive step: Let $\zeta_{M'} = f(\zeta_1,\ldots,\zeta_n)$. Since $\zeta_i\sigma\downarrow \in St_E(\phi, M')$ (because $\zeta_{M'}$ is local) and as consequence $\zeta_i\sigma\downarrow \in St_E(\phi, M)$ because $M' \in St_E(\phi, M)$, moreover by minimality of $\zeta_{M'}$, the ζ_i are minimal local recipes. Then by induction hypothesis we have $((\zeta_i\sigma)\downarrow, \zeta_i) \in T$ for $i = 1..n$, thus:

- If $\zeta_{M'}\sigma\downarrow == f(\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow)$, then by the instruction 3 of the Algorithm 1 we have $(M',\zeta_{M'}) \in T$.
- If $f(\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow)$ is not in normal form. Since $\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow$ are in normal form then by lemma 4 (or lemma 5) we have $f(\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow) \xrightarrow{h} M'$. Then by the instruction 2 of the Algorithm 1 we have $(M',\zeta_{M'}) \in T$.

□

Proof of Proposition 3.
Let T be the set computed by the Algorithm 1. The set T is obtained in at most $|\phi|_{dag} + |M|_{dag}$ steps. At each step, we compute:

- Every closed term of the form $f(M_1,\ldots,M_k)$, where (M_i,ζ_i) are already in the set T. For each such term, we check whether it is an instance of some left-hand side of a rule. Thus we need at most $\mathcal{O}((|\phi|_{dag}+|M|_{dag})^{ar(\Sigma)+1})$ computations.
- Every closed term of the form $f(M_1,\ldots,M_k)$ that is also in $St_E(\phi, M)$, where (M_i,ζ_i) are already in the set T. In other words, for every term of the form $f(M_1,\ldots,M_k)$ in $St_E(\phi, M)$ (at most $|\phi|_{dag} + |M|_{dag}$ terms), we check whether each (M_i,ζ_i) is already in the set T. Thus we need at most $\mathcal{O}((|\phi|_{dag} + |M|_{dag})^2)$ computations.

Since $1 \leq ar(\Sigma)$, each step requires at most $\mathcal{O}((|\phi|_{dag} + |M|_{dag})^{ar(\Sigma)+1})$ computations and since there are at most $|\phi|_{dag} + |M|_{dag}$ steps, then T may be computed in time $\mathcal{O}((|\phi|_{dag}+|M|_{dag})^{ar(\Sigma)+2})$. It remains to check if there exits a pair $(M,\zeta_M) \in T$ (at most $|\phi|_{dag} + |M|_{dag}$ comparison), thus for deciding $\phi \vdash_E M$ we need at most $\mathcal{O}((|\phi|_{dag} + |M|_{dag})^{ar(\Sigma)+2})$.
For the second part of Proposition 3 we know by locality lemma that if $\phi \vdash_E M$ then there exists a local recipe ζ_M such that $fn(\zeta_M) \cap \widetilde{n} = \emptyset$, $\zeta_M\sigma =_E M$ and for every $\zeta'' \in St_E(\zeta_M)$ we have $\zeta''\sigma\downarrow \in St_E(\phi, M)$. Thus, the maximal DAG-size of ζ_M is $|\phi|_{dag} + |M|_{dag}$. □

B Proofs of Section 5

B.1 Proofs under Lee *et al* theory

Proof of proposition 4.
The set $sat_{Lee}(\phi)$ is computed in at most $|\phi|_{dag}$ steps. At each step we need at most (by proposition 3) $\mathcal{O}((|\phi|_{dag} + |\phi|_{dag})^{ar(\Sigma_{Lee})+2})$, then we conclude that $sat_{Lee}(\phi)$ is computed in time $\mathcal{O}(|\phi|_{dag}^{ar(\Sigma_{Lee})+3})$. The set $I_{Lee}(\phi)$ is obtained as follows:
For each term of the form $penc(M_1, M_2, M_3)$ with $M_i \in sat_{Lee}(\phi)$ (at most $|sat_{Lee}(\phi)|_{dag}^{c_{E_{Lee}}} \leq |\phi|_{dag}^{c_{E_{Lee}}}$ terms), and for each subterm of a such term (at most $c_{E_{Lee}}|\phi|_{dag}$ terms), we check whether it is deducible (by Proposition 3 we need at most $\mathcal{O}((|\phi|_{dag} + c_{E_{Lee}}|\phi|_{dag})^{ar(\Sigma)+2}))$. Thus we need at most $\mathcal{O}(|\phi|_{dag}^{2c_{E_{Lee}}+3})$. Then we conclude that the set $sat_{Lee}(\phi) \cup I_{Lee}(\phi)$ can be computed in time $\mathcal{O}(|\phi|_{dag}^{2c_{E_{Lee}}+3})$.

For the second part of Proposition, we know by Proposition 3, that for each deducible term M there exists a term ζ_M such that $fn(\zeta_M) \cap \widetilde{n} = \emptyset$, $\zeta_M\sigma =_{E_{Lee}} M$ and $|\zeta_M|_{dag} \leq |\phi|_{dag} + |M|_{dag}$. Thus the maximal DAG-size of a term in $sat_{Lee}(\phi) \cup I(\phi)$ is $|\phi|_{dag}(c_{E_{Lee}} + 1)$. □

For proving the decidability result for static equivalence, we need some additional results.

Proposition 6 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form, M be a deducible term in normal form s.t $M == f(M_1, \ldots, M_k)$, $f \neq penc$ and $M \notin sat_{Lee}(\phi)$. For every local recipe ζ_M of M, we have $\zeta_M = f(\zeta_{M_1}, \ldots, \zeta_{M_k})$ such that $\zeta_M\sigma\downarrow == f(\zeta_{M_1}\sigma\downarrow, \ldots, \zeta_{M_k}\sigma\downarrow)$ (i.e ζ_M is by composition).*

Proof. Let ζ_M be a local recipe of deducible term M in normal form such that $M == f(M_1, \ldots, M_k)$, $f \neq penc$ and $M \notin sat_{Lee}(\phi)$. We distinguish several cases according to ζ_M. If ζ_M is a variable, this case is impossible because this implies $M \in sat_{Lee}(\phi)$, else :
Let $\zeta_M = g(\zeta_1, \ldots, \zeta_k)$ and $\zeta_i\sigma\downarrow = N_i$.

- If $g(N_1, \ldots, N_k)$ is in normal form, thus $g = f$, $N_i = M_i$ and we conclude,
- If $g(N_1, \ldots, N_k)$ is not in normal form, since $N_1, \ldots, N_k$ are in normal form then by lemma 4 we have $g(N_1, \ldots, N_k) \xrightarrow{h} M$. This case is impossible because this implies $M \in sat_{Lee}(\phi)$. Indeed, since it does not exist a rewrite rule $L \to R$ such that $head(R) = f$ (since we consider $f \neq penc$), then M can only be obtained form subterm rule. So, by locality lemma we have $M \in St_{Lee}(\phi)$ and by Definition 3 we have $M \in sat_{Lee}(\phi)$ since M is deducible, contradiction. □

Proposition 7 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form, $\zeta_M = rencrypt(\zeta_{M_1}, \zeta_{M_2})$ be a local recipe of $M == penc(N_1, N_2, N_3)$ s.t $\zeta_M\sigma\downarrow = M$ and $M \notin sat_{Lee}(\phi)$, with $(\zeta_{M_i})_{i=1,2}$ are the local recipes of some terms M_i s.t $\zeta_{M_i}\sigma\downarrow = M_i$. If N_i are deducible and $N_i \notin sat_{Lee}(\phi)$ for some $i \in \{1, 2\}$, then there exits a deducible term N_3' such that $N_3 = f_0(N_3', M_2)$ and $penc(\zeta_{N_1}, \zeta_{N_2}, f_0(\zeta_{N_3'}, \zeta_{M_2})) =_{E_{Lee}} \zeta_M$, with $(\zeta_{N_i})_{i=1,2}, \zeta_{N_3'}$ are the locale recipes of N_i, N_3' s.t $\zeta_{N_i}\sigma\downarrow = N_i$ and $\zeta_{N_3'}\sigma\downarrow = N_3'$.*

Proof. We proceed by induction on the size of ζ_M.
Base case: ζ_M is a variable, then $\zeta_M\sigma \in \phi$, contradiction.
Inductive step: Since by equational theory we have $M_1 == penc(N_1, N_2, N_3')$ with $N_3' \in St_{Lee}(N_3)$, and $N_i \notin sat_{Lee}(\phi)$ for some $i \in \{1,2\}$, thus $M_1 \notin sat_{Lee}(\phi)$, because if $M_1 \in sat_{Lee}(\phi)$, and since N_i are deducible subterms of M_1, then $N_i \in St_{Lee}(\phi)$ and by Definition 3 we have $N_i \in sat_{Lee}(\phi)$ for every $i \in \{1,2\}$, contradiction. So, we distinguish several cases according to ζ_{M_1} :

- ζ_{M_1} is a variable, this case is impossible because this implies $M_1 \in sat_{Lee}(\phi)$, contradiction.

- $\zeta_{M_1} = f(\zeta_1, \ldots, \zeta_k)$ and $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow)$ is in normal form (ζ_{M_1} is by composition). Thus $\zeta_{M_1} = penc(\zeta_{N_1'}, \zeta_{N_2'}, \zeta_{N_3'})$ with $\zeta_{N_i'}$ are the local recipes of some terms N_i' s.t $\zeta_{N_i'}\sigma\downarrow = N_i'$ for $i \in \{1,2,3\}$. By equational theory we have $N_i' = N_i$ for $i = 1,2$ and we have $N_3' \in St_{Lee}(N_3)$. Thus we have
  $rencrypt(penc(\zeta_{N_1}, \zeta_{N_2}, \zeta_{N_3'}), \zeta_{M_2}) =_{E_{Lee}} penc(\zeta_{N_1}, \zeta_{N_2}, f_0(\zeta_{N_3'}, \zeta_{M_2}))$.

- $\zeta_{M_1} = f(\zeta_1, \ldots, \zeta_k)$ and $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow)$ is not in normal form.
  Since $\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow$ are in normal form then by lemma 4 we have $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow) \xrightarrow{h} M_1$. If $f \neq rencrypt$, then M_1 can only obtained by applying the rule (1), (2), (3), (5), (6) or (7), this case is impossible because by locality this implies $M_1 \in St_{Lee}(\phi) \cup \{ok\}$, and by Definition 3 $M_1 \in sat_{Lee}(\phi)$. Else, in this case we have $\zeta_{M_1} = rencrypt(\zeta_{M_1'}, \zeta_{M_2'})$ with $\zeta_{M_i'}$ are the local recipes of some terms M_i' s.t $\zeta_{M_i'}\sigma\downarrow = M_i'$.
  By induction hypothesis there exists a deducible term N_3'' such that $N_3' = f_0(N_3'', M_2')$ and $\zeta_{M_1} =_{E_{Lee}} penc(\zeta_{N_1}, \zeta_{N_2}, f_0(\zeta_{N_3''}, \zeta_{M_2'}))$, so we have $\zeta_M =_{E_{Lee}} rencrypt(\zeta_{M_1}, \zeta_{M_2}) = penc(\zeta_{N_1}, \zeta_{N_2}, f_0(f_0(\zeta_{N_3''}, \zeta_{M_2'}), \zeta_{M_2}))$ with $\zeta_{N_3'} = f_0(\zeta_{N_3''}, \zeta_{M_2'})$, thus we conclude. □

Proof of Lemma 2.
Assume that $\phi' \models Eq_{E_{Lee}}(\phi)$ and consider ζ_M, ζ_N such that $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$ and $(fn(\zeta_M) \cup fn(\zeta_N)) \cap \widetilde{n} = \emptyset$. Let us show that $(\zeta_M =_{E_{Lee}} \zeta_N)\phi'$. Let $T = \zeta_M\sigma\downarrow$.
We show by induction on the max of the size of ζ_M and ζ_N.
- **Base case:** ζ_M, ζ_N are variables, so $(\zeta_M, \zeta_N) \in Eq_{E_{Lee}}(\phi)$, and we conclude by $\phi' \models Eq_{E_{Lee}}(\phi)$.
- **Inductive step:** We distinguish two cases:
Case 1 : $T \in sat_{Lee}(\phi)$:

- If neither ζ_M nor ζ_N is a variable, then we rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1, \ldots, \zeta_k) = g(\zeta_1', \ldots, \zeta_n')$. Let $\overline{\zeta}_i, \overline{\zeta'}_i$ be the local recipes of $\zeta_i\sigma\downarrow, \zeta_i'\sigma\downarrow$ that belong to $Eq_{E_{Lee}}(\phi)$. By locality we have $\zeta_i\sigma\downarrow, \zeta_i'\sigma\downarrow \in St_{Lee}(\phi, T) \subseteq St_{Lee}(\phi)$ (since $T \in sat_{Lee}(\phi)$), then by Definition 3 we have $\zeta_i\sigma\downarrow, \zeta_i'\sigma\downarrow \in sat_{Lee}(\phi)$.
  Thus we have $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) = g(\overline{\zeta'}_1, \ldots, \overline{\zeta'}_n)) \in Eq_{E_{Lee}}(\phi)$, and we deduce $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) =_{E_{Lee}} g(\overline{\zeta'}_1, \ldots, \overline{\zeta'}_n))\phi'$ by $\phi' \models Eq_{E_{Lee}}(\phi)$. Moreover, by induction hypothesis we have $(\zeta_i =_{E_{Lee}} \overline{\zeta}_i)\phi'$ and $(\zeta_i' =_{E_{Lee}} \overline{\zeta'}_i)\phi'$, then we have $(f(\zeta_1, \ldots, \zeta_k) =_{E_{Lee}} f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k))\phi'$ and $(g(\zeta_1', \ldots, \zeta_n') =_{E_{Lee}} g(\overline{\zeta'}_1, \ldots, \overline{\zeta'}_n))\phi'$. Thus we conclude by transitivity.

- If ζ_M or ζ_N is a variable, let us say $\zeta_M = f(\zeta_1, \ldots, \zeta_k)$ and $\zeta_N = x$. We rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1, \ldots, \zeta_k) = x$. Let $\overline{\zeta}_i$ be the local recipes

of $\zeta_i\sigma\downarrow$ that belong to $Eq_{E_{Lee}}(\phi)$. Thus we have $(f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k) = x) \in Eq_{E_{Lee}}(\phi)$, and we deduce $(f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k) =_{E_{Lee}} x)\phi'$ by $\phi' \models Eq_{E_{Lee}}(\phi)$. Moreover, by induction hypothesis we have $(\zeta_i =_{E_{Lee}} \overline{\zeta}_i)\phi'$, then we have $(f(\zeta_1,\ldots,\zeta_k) =_{E_{Lee}} f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k))\phi'$. Thus we conclude by transitivity.

Case 2 : $T \notin sat_{Lee}(\phi)$: This implies that neither ζ_M or ζ_N are variables. We distinguish several cases :

- If ζ_M and ζ_N are terms by composition: We rewrite $\zeta_M = \zeta_N$ in $g(\zeta_1,\ldots,\zeta_n) = g(\zeta'_1,\ldots,\zeta'_n)$. Since $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$ then we have $g(\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow) == g(\zeta'_1\sigma\downarrow,\ldots,\zeta'_n\sigma\downarrow)$. So we have $\zeta_i\sigma\downarrow == \zeta'_i\sigma\downarrow$, thus $(\zeta_i =_{E_{Lee}} \zeta'_i)\phi$. Then by induction hypothesis we have $(\zeta_i =_{E_{Lee}} \zeta'_i)\phi'$. Since $=_{E_{Lee}}$ is closed by application of function symbol, we conclude that $(\zeta_M =_{E_{Lee}} \zeta_N)\phi'$.

- If ζ_M and ζ_N are terms by decomposition: we rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1,\ldots,\zeta_k) = g(\zeta'_1,\ldots,\zeta'_l)$. If the rule (1), (2), (3), (5), (6) or (7) is applied, then by locality we have $T \in St_{Lee}(\phi)\cup\{ok\}$ and by Definition 3 we obtain $T \in sat_{Lee}(\phi)$, contradiction. Thus the interesting case is when the rule (4) is applied. So we rewrite $\zeta_M = \zeta_N$ in $rencrypt(\zeta_1,\zeta_2) = rencrypt(\zeta'_1,\zeta'_2)$. Since $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$ then we have $\zeta_M\sigma\downarrow == \zeta_N\sigma\downarrow == T$ with T of the form $penc(T_1,T_2,f_0(T_3,T_4))$ where T_i are in normal form. By the equational theory we have $\zeta_1\sigma\downarrow == penc(T_1,T_2,T_3)$(i.1) and $\zeta_2\sigma\downarrow == T_4$(i.2). Moreover, we have $\zeta'_1\sigma\downarrow == penc(T_1,T_2,T_3)$(ii.1) and $\zeta'_2\sigma\downarrow == T_4$(ii.2). By (i.1) and (ii.1) we have $(\zeta_1 =_{E_{Lee}} \zeta'_1)\phi$ and by (i.2) and (ii.2) we have $(\zeta_2 =_{E_{Lee}} \zeta'_2)\phi$. Then by induction hypothesis we have $(\zeta_1 =_{E_{Lee}} \zeta'_1)\phi'$ and $(\zeta_2 =_{E_{Lee}} \zeta'_2)\phi'$. Since $=_{E_{Lee}}$ is closed by application of function symbol , we conclude that $(\zeta_M =_{E_{Lee}} \zeta_N)\phi'$.

- If ζ_M is a term by decomposition and ζ_N is a term by composition (or the inverse) : we rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1,\ldots,\zeta_k) = g(\zeta'_1,\ldots,\zeta'_l)$. Like in previous case, if the rule (1), (2), (3), (5), (6) or (7) is applied, then by locality we have $T \in St_{Lee}(\phi)\cup\{ok\}$ and by Definition 3 we obtain $T \in sat_{Lee}(\phi)$, contradiction. Thus the interesting case for the term by decomposition is when the rule (4) is applied. So we rewrite $\zeta_M = \zeta_N$ in $rencrypt(\zeta_1,\zeta_2) = penc(\zeta'_1,\zeta'_2,\zeta'_3)$.
  In what follows, let $(\zeta_i\sigma\downarrow = M_i)_{i=1,2}$ and $(\zeta'_i\sigma\downarrow = N_i)_{i=1,2,3}$.
  - If $N_i \in sat_{Lee}(\phi)$ for $i = 1,2,3$, since M_2 is deducible and we have $M_2 \in St_{Lee}(\phi)$ (because $M_2 \in St_{Lee}(N_3)$ and $N_3 \in sat_{Lee}(\phi)$) then by Definition 3 $M_2 \in sat_{Lee}(\phi)$. Moreover, since $M_1 \in St_{Lee}(penc(N_1,N_2,N_3))$ and it is deducible then by Definition 4 $M_1 \in I_{Lee}(\phi)$. Let $\overline{\zeta}_i, \overline{\zeta'}_i$ be the local recipes of M_i, N_i belonging to $Eq_{E_{Lee}}(\phi)$, thus we have $(rencrypt(\overline{\zeta}_1,\overline{\zeta}_2) = penc(\overline{\zeta'}_1,\overline{\zeta'}_2,\overline{\zeta'}_3)) \in Eq_{E_{Lee}}(\phi)$, and we deduce $(rencrypt(\overline{\zeta}_1,\overline{\zeta}_2) =_{E_{Lee}} penc(\overline{\zeta'}_1,\overline{\zeta'}_2,\overline{\zeta'}_3))\phi'$ by $\phi' \models Eq_{E_{Lee}}(\phi)$. Moreover, by induction hypothesis we have $(\zeta_i =_{E_{Lee}} \overline{\zeta}_i)\phi'$ and $(\zeta'_i =_{E_{Lee}} \overline{\zeta'}_i)\phi'$. Thus, since $=_{E_{Lee}}$ is stable by application of function symbol, we have $(rencrypt(\zeta_1,\zeta_2) =_{E_{Lee}} rencrypt(\overline{\zeta}_1,\overline{\zeta}_2))\phi'$ and $(penc(\zeta'_1,\zeta'_2,\zeta'_3) =_{E_{Lee}} penc(\overline{\zeta'}_1,\overline{\zeta'}_2,\overline{\zeta'}_3))\phi'$. Thus we conclude by transitivity.
  - Else, we distinguish two cases:

– If $N_3 \notin sat_{Lee}(\phi)$, since $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$ then by equational theory N_3 is of the form $f_0(N_4, N_5)$, and as ζ'_3 is local, so by proposition 6 ζ_{N_3} can only be of the form $f_0(\zeta'_4, \zeta'_5)$ (i.e it is by composition). So we can rewrite $\zeta_M = \zeta_N$ in $rencrypt(\zeta_1, \zeta_2) = penc(\zeta'_1, \zeta'_2, f_0(\zeta'_4, \zeta'_5))$. Since $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$, then $(\zeta_1 =_{E_{Lee}} penc(\zeta'_1, \zeta'_2, \zeta'_4))\phi$ and $(\zeta_2 =_{E_{Lee}} \zeta'_5)\phi$. Then by induction hypothesis we have $(\zeta_1 =_{E_{Lee}} penc(\zeta'_1, \zeta'_2, \zeta'_4))\phi'$ and $(\zeta'_2 =_{E_{Lee}} \zeta'_5)\phi'$, and we conclude.

– If $N_i \notin sat_{Lee}(\phi)$ for some $i \in \{1, 2\}$, then by proposition 7, there exists deducible N'_3 s.t $N_3 = f_0(N'_3, M_2)$, $\zeta_M =_{E_{Lee}} penc(\zeta_{N_1}, \zeta_{N_2}, f_0(\zeta_{N'_3}, \zeta_2))$ with $\zeta_{N'_3}\sigma\downarrow = N'_3$ and $\zeta_{N'_i}\sigma\downarrow = N_i$ for $i = 1, 2$. So it is sufficient to prove that $(penc(\zeta_{N'_1}, \zeta_{N'_2}, f_0(\zeta_{N'_3}, \zeta_2)) =_{E_{Lee}} penc(\zeta'_1, \zeta'_2, \zeta'_3))\phi'$, and since $penc(\zeta_{N'_1}\sigma\downarrow, \zeta_{N'_2}\sigma\downarrow, (f_0(\zeta_{N'_3}, \zeta_2))\sigma\downarrow)$ is in normal form (because by lemma 4 the reduction must be in head and moreover does not exists a rewrite rule $L \to R$ s.t $head(L) = penc$), thus we can proceed like in the first case where the two terms are by composition. □

The next lemma is adapted from the lemma 2 of [AC04].

Lemma 6 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form. For every context C s.t $fn(C) \cap \widetilde{n} = \emptyset$, for every $M_i \in sat_E(\phi)$, if $C[M_1, \ldots, M_k] \xrightarrow{h} T$ by applying syntactic subterm rule[3], then for every frame $\phi' \models Eq_E(\phi)$ such that $\phi' = \nu\widetilde{n'}\sigma'$ and $fn(C) \cap \widetilde{n'} = \emptyset$, $(C[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E \zeta_T)\phi'$ with ζ_{M_i}, ζ_T are the local recipes of M_i, T.*

Proof. Since the reduction is in head, then $C[M_1, \ldots, M_k]$ is an instance $L\theta$ of some term L, where $L \to R$ is a syntactic subterm rule.
We rewrite $L\theta$ in $C''_0[C^0_1[M_1, \ldots, M_k], \ldots, C^0_n[M_1, \ldots, M_k], M_1, \ldots, M_k]$ such that L is an instance of $C''_0[x_1, \ldots, x_n, y_1, \ldots, y_l]$ and for every path p in C''_0, leading to a variable x_i, $L|_p = x_i$, for every path p in C''_0, leading to a variable y_i, $L\theta|_p = M_i \in sat_{Lee}(\phi)$: C''_0 is the maximal context such that L and C_4 are instances of C''_0.
We transform again $L\theta$ in order to obtain a context of terms of $sat_{Lee}(\phi)$, such that the context is of the size smaller than $c_{E_{Lee}}(E_{Lee})$. For each variable x_i of C''_0:

- Either this variable is tested for equality under some y_j: there exists a path $p = p_1.p_2$ such that $C''_0|_{p_1} = y_j$ and $L|_{p_1.p_2} = x_i$. In this case, we defined $M''_i \stackrel{\text{def}}{=} x_i\theta$. Then $M''_i = C^0_i[M_1, \ldots, M_k]$ and is a subterm of M_j, and since M''_i is deducible, thus by Definition 3, we have $M''_i \in sat_{Lee}(\phi)$.
- Either this variable is unconstrained in L: for every path p in L such that $L|_p = x_i$, p is a path in C''_0 and $C''_0|_p = x_i$.

By renaming the variables in L and C''_0, we may assume that $x_1, \ldots, x_r$, are unconstrained in L and $x_{r+1}, \ldots, x_n$ are tested for equality under some variables.
We obtain that:
$L\theta == C''_0[C^0_1[M_1, \ldots, M_k], \ldots, C^0_r[M_1, \ldots, M_k], M''_{r+1}, \ldots, M''_n, M_1, \ldots, M_k]$,
with $M_i, M''_i \in sat_{Lee}(\phi)$.

[3] A rule $l \to r$ is a syntactic subterm rule if r is a syntactic subterm of l or a constant symbol.

We have to consider three cases depending on the form of $R\theta$, which is a subterm of $L\theta$ or a constant symbol.

- Either $R\theta$ is of the form:

  $$C_0'''[C_1^0[M_1,\ldots,M_k],\ldots,C_r^0[M_1,\ldots,M_k],M''_{r+1},\ldots,M''_n,M_1,\ldots,M_k]$$

  for some context C_0''' of small size. Since $L\theta \xrightarrow{h} R\theta$ and since the variables $x_1,\ldots,x_r$ are unconstrained, we also have
  $C_0''[a_1,\ldots,a_r,M''_{r+1},\ldots,M''_n,M_1,\ldots,M_k] \xrightarrow{h}$
  $C_0'''[a_1,\ldots,a_r,M''_{r+1},\ldots,M''_n,M_1,\ldots,M_k]$ where a_i's a fresh names. Thus
  $(C_0''[a_1,\ldots,a_r,\zeta_{M''_{r+1}},\ldots,\zeta_{M''_n},\zeta_{M_1},\ldots,\zeta_{M_k}] =_{E_{Lee}}$
  $C_0'''[a_1,\ldots,a_r,\zeta_{M''_{r+1}},\ldots,\zeta_{M''_n},\zeta_{M_1},\ldots,\zeta_{M_k}])\phi$. Let $\overline{\zeta}_{M''_i},\overline{\zeta}_{M_i}$ be the local recipes of $\zeta_{M''_i}\sigma\downarrow,\zeta_{M_i}\sigma\downarrow$ belonging to $Eq(\phi)$. By lemma 2, we have $(\overline{\zeta}_{M''_i}=\zeta_{M''_i})\phi'$ and $(\overline{\zeta}_{M_i}=\zeta_{M_i})\phi'$, thus we have
  $(C_0''[a_1,\ldots,a_r,\zeta_{M''_{r+1}},\ldots,\zeta_{M''_n},\zeta_{M_1},\ldots,\zeta_{M_k}] =_{E_{Lee}}$
  $C_0''[a_1,\ldots,a_r,\overline{\zeta}_{M''_{r+1}},\ldots,\overline{\zeta}_{M''_n},\overline{\zeta}_{M_1},\ldots,\overline{\zeta}_{M_k}])\phi'$ and
  $(C_0'''[a_1,\ldots,a_r,\zeta_{M''_{r+1}},\ldots,\zeta_{M''_n},\zeta_{M_1},\ldots,\zeta_{M_k}] =_{E_{Lee}}$
  $C_0'''[a_1,\ldots,a_r,\overline{\zeta}_{M''_{r+1}},\ldots,\overline{\zeta}_{M''_n},\overline{\zeta}_{M_1},\ldots,\overline{\zeta}_{M_k}])\phi'$. Moreover we have,
  $(C_0''[a_1,\ldots,a_r,\overline{\zeta}_{M''_{r+1}},\ldots,\overline{\zeta}_{M''_n},\overline{\zeta}_{M_1},\ldots,\overline{\zeta}_{M_k}] =_{E_{Lee}}$
  $C_0'''[a_1,\ldots,a_r,\overline{\zeta}_{M''_{r+1}},\ldots,\overline{\zeta}_{M''_n},\overline{\zeta}_{M_1},\ldots,\overline{\zeta}_{M_k}])\phi'$, because it belongs to $Eq(\phi)$ (since C_0'' and C_0''' are small contexts), then, by transitivity we deduce
  $(C_0''[a_1,\ldots,a_r,\zeta_{M''_{r+1}},\ldots,\zeta_{M''_n},\zeta_{M_1},\ldots,\zeta_{M_k}] =_{E_{Lee}}$
  $C_0'''[a_1,\ldots,a_r,\zeta_{M''_{r+1}},\ldots,\zeta_{M''_n},\zeta_{M_1},\ldots,\zeta_{M_k}])\phi'$. So we conclude by replacing each a_i by $C_i^0[\zeta_{M_1},\ldots,\zeta_{M_k}]$.

- Either $R\theta$ is a subterm M_0 of one of the M_i or M''_i. Since the variables $x_1,\ldots,x_r$ are unconstrained, we also have

  $$C_0''[a_1,\ldots,a_r,M''_{r+1},\ldots,M''_n,M_1,\ldots,M_k] \xrightarrow{h} M_0,$$

  where a_i's a fresh names. Since M_0 is deducible, then by Definition 3, we have $M_0 \in sat_{Lee}(\phi)$. Thus

  $$(C_0''[a_1,\ldots,a_r,\zeta_{M''_{r+1}},\ldots,\zeta_{M''_n},\zeta_{M_1},\ldots,\zeta_{M_k}] =_{E_{Lee}} \zeta_{M_0})\phi.$$

  Thus, we conclude like the previous case.

- Either $R\theta$ is a constant symbol. We conclude like the case above. □

Proof of Lemma 3.
We proceed by induction on the size of ζ_M.
- **Base case**: If ζ_M is a variable, then we can choose $\widehat{\zeta}_M = \zeta_M$, thus we have $(\zeta_M =_{E_{Lee}} \widehat{\zeta}_M)\phi'$.
- **Inductive step:** Let $\zeta_M = f(\zeta_1,\ldots,\zeta_n)$. Applying the induction hypothesis, there exists $\widehat{\zeta}_i$ local recipes of $(\zeta_i)\sigma\downarrow$ such that $(\zeta_i =_{E_{Lee}} \widehat{\zeta}_i)\phi'$. Since $=_{E_{Lee}}$ is closed by application of function symbol, then we have $(f(\widehat{\zeta}_1,\ldots,\widehat{\zeta}_n) =_{E_{Lee}} \zeta_M)\phi'(*)$. We distinguish two cases:
Case 1 : ζ_M is by composition. Then we have the term $f(\widehat{\zeta}_1,\ldots,\widehat{\zeta}_n)$ is local

recipe of M (see proof of locality lemma). Then we can choose $f(\widehat{\zeta_1},\ldots,\widehat{\zeta_n})$ for a local recipe of M.
Case 2 : $\zeta_M = f(\zeta_1,\ldots,\zeta_n)$ is by decomposition : If $f = rencrypt$, in this case we have $rencrypt(\widehat{\zeta_1},\widehat{\zeta_2})$ is local (see proof of locality lemma), thus we can proceed like in previous case, else (in this case $f(\widehat{\zeta_1},\ldots,\widehat{\zeta_n})$ is not always local); we rewrite $f(\widehat{\zeta_1},\ldots,\widehat{\zeta_n})$ in $C[\widehat{\zeta}_{M_1},\ldots,\widehat{\zeta}_{M_k}]$ such that $C[M_1,\ldots,M_k] \xrightarrow{h} M'$ and $M_i \in sat_{Lee}(\phi)$. By lemma 6 we have $(\widehat{\zeta}_{M'} =_{E_{Lee}} C[\widehat{\zeta}_{M_1},\ldots,\widehat{\zeta}_{M_k}])\phi'(**)$, with $\widehat{\zeta}_{M'}$ is local recipe of M because E_{Lee} is convergent. Thus we deduce by transitivity from (*) and (**) that $(\zeta_M =_{E_{Lee}} \widehat{\zeta}_{M'})\phi'$. Then we can choose $\widehat{\zeta}_{M'}$ for a local recipe of M. □

B.2 Proofs under Okamoto theory

Proof of Lemma 2.
Assume that $\phi' \models Eq_{E_{Oka}}(\phi)$ and consider ζ_M, ζ_N such that $(\zeta_M =_{E_{Oka}} \zeta_N)\phi$ and $(fn(\zeta_M) \cup fn(\zeta_N)) \cap \widetilde{n} = \emptyset$. Let us show that $(\zeta_M =_{E_{Oka}} \zeta_N)\phi'$. Let $T = \zeta_M\sigma\downarrow$.
We show by induction on the max of the size of ζ_M and ζ_N.
- **Base case:** ζ_M, ζ_N are variables, so $(\zeta_M, \zeta_N) \in Eq_{E_{Oka}}(\phi)$, and we conclude by $\phi' \models Eq_{E_{Oka}}(\phi)$.
- **Inductive step:** We distinguish two cases:
Case 1 : $T \in sat_{Oka}(\phi)$:

- If neither ζ_M nor ζ_N is a variable, then we rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1,\ldots,\zeta_k) = g(\zeta'_1,\ldots,\zeta'_n)$. Let $\overline{\zeta}_i, \overline{\zeta'}_i$ be the local recipes of $\zeta_i\sigma\downarrow, \zeta'_i\sigma\downarrow$ that belong to $Eq_{E_{Oka}}(\phi)$. By locality we have $\zeta_i\sigma\downarrow, \zeta'_i\sigma\downarrow \in St_{Oka}(\phi,T) \subseteq St_{Oka}(\phi)$ (since $T \in sat_{Oka}(\phi)$), then by Definition 3 we have $\zeta_i\sigma\downarrow, \zeta'_i\sigma\downarrow \in sat_{Oka}(\phi)$. Thus we have $(f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k) = g(\overline{\zeta'}_1,\ldots,\overline{\zeta'}_n)) \in Eq_{E_{Oka}}(\phi)$, and we deduce $(f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k) =_{E_{Oka}} g(\overline{\zeta'}_1,\ldots,\overline{\zeta'}_n))\phi'$ by $\phi' \models Eq_{E_{Oka}}(\phi)$. Moreover, by induction hypothesis we have $(\zeta_i =_{E_{Oka}} \overline{\zeta}_i)\phi'$ and $(\zeta'_i =_{E_{Oka}} \overline{\zeta'}_i)\phi'$, then we have $(f(\zeta_1,\ldots,\zeta_k) =_{E_{Oka}} f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k))\phi'$ and $(g(\zeta'_1,\ldots,\zeta'_n) =_{E_{Oka}} g(\overline{\zeta'}_1,\ldots,\overline{\zeta'}_n))\phi'$. Thus we conclude by transitivity.

- If ζ_M or ζ_N is a variable, let us say $\zeta_M = f(\zeta_1,\ldots,\zeta_k)$ and $\zeta_N = x$. We rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1,\ldots,\zeta_k) = x$. Let $\overline{\zeta}_i$ be the local recipes of $\zeta_i\sigma\downarrow$ that belong to $Eq_{E_{Oka}}(\phi)$. Thus we have $(f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k) = x) \in Eq_{E_{Oka}}(\phi)$, and we deduce $(f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k) =_{E_{Oka}} x)\phi'$ by $\phi' \models Eq_{E_{Oka}}(\phi)$. Moreover, by induction hypothesis we have $(\zeta_i =_{E_{Oka}} \overline{\zeta}_i)\phi'$, then we have $(f(\zeta_1,\ldots,\zeta_k) =_{E_{Oka}} f(\overline{\zeta}_1,\ldots,\overline{\zeta}_k))\phi'$. Thus we conclude by transitivity.

Case 2 : $T \notin sat_{Oka}(\phi)$: This implies that neither ζ_M or ζ_N are variables. We distinguish several several cases: In what follows, we consider $\zeta_i\sigma\downarrow = M_i$ and $\zeta'_i\sigma\downarrow = N_i$.

- If ζ_M and ζ_N are terms by composition: We rewrite $\zeta_M = \zeta_N$ in $g(\zeta_1,\ldots,\zeta_n) = g(\zeta'_1,\ldots,\zeta'_n)$. Since $(\zeta_M =_{E_{Oka}} \zeta_N)\phi$ then we have $g(\zeta_1\sigma\downarrow,\ldots,\zeta_n\sigma\downarrow) == g(\zeta'_1\sigma\downarrow,\ldots,\zeta'_n\sigma\downarrow)$. So we have $\zeta_i\sigma\downarrow == \zeta'_i\sigma\downarrow$, thus $(\zeta_i =_{E_{Oka}} \zeta'_i)\phi$. Then by induction hypothesis we have $(\zeta_i =_{E_{Oka}} \zeta'_i)\phi'$. Since $=_{E_{Oka}}$ is closed by application of function symbol, we conclude that $(\zeta_M =_{E_{Oka}} \zeta_N)\phi'$.

- If ζ_M is a term by decomposition and ζ_N is a term by composition (or the inverse) : we rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1, \ldots, \zeta_k) = g(\zeta'_1, \ldots, \zeta'_l)$. If the rule (1), (2) or (3) is applied, then by locality we have $T \in St_{Oka}(\phi)$ and by Definition 3 we obtain $T \in sat_{Oka}(\phi)$. Thus the interesting case for the term by decomposition is when the rule (4) is applied. So we rewrite $\zeta_M = \zeta_N$ in $f_1(\zeta_1, \zeta_2, \zeta_3, \zeta_4) = f_1(\zeta'_1, \zeta'_2, \zeta'_3, \zeta'_4)$.

  Since $(\zeta_M =_{E_{Oka}} \zeta_N)\phi$, then we have $M_2 == f_1(N_1, N_2, N_3, M_1)$. Moreover, by equational theory we have $(tdcommit(\zeta_1, \zeta_2, \zeta_3)\sigma)\downarrow == tdcommit(N_1, N_2, N_3)$ and $\zeta_4\sigma\downarrow == \zeta'_4\sigma\downarrow$, so we have $(tdcommit(\zeta_1, \zeta_2, \zeta_3) =_{E_{Oka}} tdcommit(\zeta'_1, \zeta'_2, \zeta'_3))\phi$ and $(\zeta_4 =_{E_{Oka}} \zeta'_4)\phi$. Applying induction hypothesis (since $tdcommit(\zeta_1, \zeta_2, \zeta_3)$ and ζ_4 (resp. $tdcommit(\zeta'_1, \zeta'_2, \zeta'_3)$ and ζ'_4) are subterms of ζ_M (resp. ζ_N)), we obtain $(tdcommit(\zeta_1, \zeta_2, \zeta_3) =_{E_{Oka}} tdcommit(\zeta'_1, \zeta'_2, \zeta'_3))\phi'$ and $(\zeta_4 =_{E_{Oka}} \zeta'_4)\phi'$, thus we conclude that $(\zeta_M =_{E_{Oka}} \zeta_N)\phi'$.

- If ζ_M and ζ_N are terms by decomposition: we rewrite $\zeta_M = \zeta_N$ in $f(\zeta_1, \ldots, \zeta_k) = g(\zeta'_1, \ldots, \zeta'_l)$. If the rule (1), (2) or (3) is applied, then by locality we have $T \in St_{Oka}(\phi)$ and by Definition 3 we obtain $T \in sat_{Oka}(\phi)$. Thus the interesting case is when the rule (4) is applied. So we rewrite $\zeta_M = \zeta_N$ in $f_1(\zeta_1, \zeta_2, \zeta_3, \zeta_4) = f_1(\zeta'_1, \zeta'_2, \zeta'_3, \zeta'_4)$.

  Since $(\zeta_M =_{E_{Oka}} \zeta_N)\phi$, then we have $\zeta_M\sigma\downarrow == \zeta_N\sigma\downarrow == T$ with T of the form $f_1(T_1, T_2, T_3, T_4)$ where T_i are in normal form. By equational theory we have $(tdcommit(\zeta_1, \zeta_2, \zeta_3)\sigma)\downarrow == tdcommit(T_1, T_2, T_3)$ (i.1) and $\zeta_4\sigma\downarrow == T_4$ (i.2). Moreover, we have $(tdcommit(\zeta'_1, \zeta'_2, \zeta'_3)\sigma)\downarrow == tdcommit(T_1, T_2, T_3)$ (ii.1) and $\zeta'_4\sigma\downarrow == T_4$ (ii.2). By (i.1) and (ii.1) we have $(tdcommit(\zeta_1, \zeta_2, \zeta_3) =_{E_{Oka}} tdcommit(\zeta'_1, \zeta'_2, \zeta'_3))\phi$, and by (i.2) and (ii.2) we have $(\zeta_4 =_{E_{Oka}} \zeta'_4)\phi$. Applying induction hypothesis (since $tdcommit(\zeta_1, \zeta_2, \zeta_3)$ and ζ_4 (resp. $tdcommit(\zeta'_1, \zeta'_2, \zeta'_3)$ and ζ'_4) are subterms of ζ_M (resp. ζ_N)), we obtain $(tdcommit(\zeta_1, \zeta_2, \zeta_3) =_{E_{Oka}} tdcommit(\zeta'_1, \zeta'_2, \zeta'_3))\phi'$ and $(\zeta_4 =_{E_{Oka}} \zeta'_4)\phi'$, thus we conclude that $(\zeta_M =_{E_{Oka}} \zeta_N)\phi'$. □

Also for this theory, the Lemma 6 holds. Its proof is identical under Lee *et al* theory.

Proof of Lemma 3.

We proceed by induction on the size of ζ_M.

- **Base case:** If ζ_M is a variable, then we can choose $\widehat{\zeta}_M = \zeta_M$, thus we have $(\zeta_M =_{E_{Oka}} \widehat{\zeta}_M)\phi'$.

- **Inductive step:** We distinguish two cases:

Case 1 : $\zeta_M = f(\zeta_1, \ldots, \zeta_n)$ is by composition: Applying the induction hypothesis, there exist $\widehat{\zeta}_i$ local recipes of $(\zeta_i)\sigma\downarrow$ s.t $(\zeta_i =_{E_{Oka}} \widehat{\zeta}_i)\phi'$. Then we have the term $f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n)$ is local recipe of M (see proof of locality lemma). Since $=_{E_{Oka}}$ is closed by application of function symbol, then we have $(f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n) =_{E_{Oka}} \zeta_M)\phi'$. Then we can choose $(f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n)$ for a local recipe of M.

Case 2 : $\zeta_M = f(\zeta_1, \ldots, \zeta_n)$ is by decomposition: Applying the induction hypothesis, there exists $\widehat{\zeta}_i$ local recipes of $(\zeta_i)\sigma\downarrow$ such that $(\zeta_i =_{E_{Oka}} \widehat{\zeta}_i)\phi'$, thus we have $(\zeta_M =_{E_{Oka}} f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n))\phi'(*)$ (because $=_{E_{Oka}}$ is closed by application

of function symbol). If $f(\widehat{\zeta_1},\ldots,\widehat{\zeta_n})$ is local then we can proceed like above case, else we distinguish several cases according to the applied rule:

- If the applied rule is the rule (1) or (3) (that is syntactic subterm rule), then we rewrite $f(\widehat{\zeta_1},\ldots,\widehat{\zeta_n})$ in $C[\widehat{\zeta}_{M_1},\ldots,\widehat{\zeta}_{M_k}]$ such that $C[M_1,\ldots,M_k] \xrightarrow{h} M'$ and $M_i \in sat_{Oka}(\phi)$. By lemma 6 we have $(\widehat{\zeta}_{M'} =_{E_{Oka}} C[\widehat{\zeta}_{M_1},\ldots,\widehat{\zeta}_{M_k}])\phi'$, with $\widehat{\zeta}_{M'}$ is local recipe of M because E_{Oka} is convergent. Then we deduce by transitivity from (*) and the last equations that $(\zeta_M =_{E_{Oka}} \widehat{\zeta}_{M'})\phi'$. Thus we can choose $\widehat{\zeta}_{M'}$ for a local recipe of M.

- If the applied rule is the rule (4), this implies $n = 4$ and $f = f_1$. Since ζ_M is by decomposition (i.e $f_1(\widehat{\zeta_1}\sigma\downarrow,\widehat{\zeta_2}\sigma\downarrow,\widehat{\zeta_3}\sigma\downarrow,\widehat{\zeta_4}\sigma\downarrow) \xrightarrow{h} M$), then $head((\widehat{\zeta_2}\sigma)\downarrow) = f_1$, $\zeta_1\sigma\downarrow,\zeta_3\sigma\downarrow \in St_{Oka}(\zeta_2\sigma\downarrow)$ and $\widehat{\zeta_4}\sigma\downarrow \in St_{Oka}(M)$. If $\widehat{\zeta_2}$ is a variable or $\widehat{\zeta_2}\sigma\downarrow$ is obtained by applying the rule (1) or (3) then by locality we have $\widehat{\zeta_2}\sigma\downarrow \in St_{Oka}(\phi)$, then we have $\widehat{\zeta_i}\sigma\downarrow \in St_{Oka}(\phi) \subseteq St_{Oka}(\phi,M)$ for $i = 1..3$, this implies that $f_1(\widehat{\zeta_1},\widehat{\zeta_2},\widehat{\zeta_3},\widehat{\zeta_4})$ is local (since $\widehat{\zeta_i}$ are local), contradiction. The rule (2) cannot be applied because give us $head((\widehat{\zeta_2}\sigma)\downarrow) \neq f_1$. Thus $\widehat{\zeta_2}$ is either by composition with $head(\widehat{\zeta_2}) = f_1$ or by decomposition by applying the rule (4). So, we have $\widehat{\zeta_2}$ of the form $f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta'}_4)$, thus $(f_1(\widehat{\zeta_1},f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta'}_4),\widehat{\zeta_3},\widehat{\zeta_4}) =_{E_{Oka}} f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta_4}))\phi$ with $(\widehat{\zeta_1} =_{E_{Oka}} \widehat{\zeta'}_4)\phi$ and $(\widehat{\zeta_3} =_{E_{Oka}} \widehat{\zeta'}_3)\phi$. By lemma 2 we have $(\widehat{\zeta_1} =_{E_{Oka}} \widehat{\zeta'}_4)\phi'$ and $(\widehat{\zeta_3} =_{E_{Oka}} \widehat{\zeta'}_3)\phi'$, thus we deduce $(f_1(\widehat{\zeta_1},f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta'}_4),\widehat{\zeta_3},\widehat{\zeta_4}) =_{E_{Oka}} f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta_4}))\phi'$(**). Let $\zeta_T = f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta_4})$. By induction hypothesis there exists local recipe $\widehat{\zeta_T}$ of $(\widehat{\zeta_T}\sigma)\downarrow$ s.t $(\zeta_T =_{E_{Oka}} \widehat{\zeta_T})\phi'$(***). Then we conclude by transitivity from (*), (**) and (***) that $(\zeta_M =_{E_{Oka}} \widehat{\zeta_T})\phi'$. Thus we can choose $\widehat{\zeta_T}$ for a local recipe of M.

- If the applied rule is the rule (4), this implies $n = 3$ and $f = tdcommit$. Since ζ_M is by decomposition, then $head((\widehat{\zeta_2}\sigma)\downarrow) = f_1$ and $\zeta_1\sigma\downarrow,\zeta_3\sigma\downarrow \in St_{Oka}(\zeta_2\sigma\downarrow)$. If $\widehat{\zeta_2}$ is a variable or $\widehat{\zeta_2}\sigma\downarrow$ is obtained by applying the rule (1) or (3) then by locality we have $\widehat{\zeta_2}\sigma\downarrow \in St_{Oka}(\phi)$, then we have $\widehat{\zeta_i}\sigma\downarrow \in St_{Oka}(\phi) \subseteq St_{Oka}(\phi,M)$ for $i = 1..3$, this implies that $tdcommit(\widehat{\zeta_1},\widehat{\zeta_2},\widehat{\zeta_3})$ is local (since $\widehat{\zeta_i}$ are local), contradiction. The rule (2) cannot be applied because give us $head((\widehat{\zeta_2}\sigma)\downarrow) \neq f_1$. Thus, $\widehat{\zeta_2}$ is either by composition with $head(\widehat{\zeta_2}) = f_1$ or by decomposition by applying the rule (4). So, we have $\widehat{\zeta_2}$ of the form $f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta'}_4)$, thus $(tdcommit(\widehat{\zeta_1},f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta'}_4),\widehat{\zeta_3}) =_{E_{Oka}} tdcommit(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3))\phi$ with $(\widehat{\zeta_1} =_{E_{Oka}} \widehat{\zeta'}_4)\phi$ and $(\widehat{\zeta_3} =_{E_{Oka}} \widehat{\zeta'}_3)\phi$. By lemma 2 we have $(\widehat{\zeta_1} =_{E_{Oka}} \widehat{\zeta'}_4)\phi'$ and $(\widehat{\zeta_3} =_{E_{Oka}} \widehat{\zeta'}_3)\phi'$, thus we deduce $(tdcommit(\widehat{\zeta_1},f_1(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3,\widehat{\zeta'}_4),\widehat{\zeta_3}) =_{E_{Oka}} tdcommit(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3))\phi'$(**). Let $\zeta_T = tdcommit(\widehat{\zeta'}_1,\widehat{\zeta'}_2,\widehat{\zeta'}_3)$. By induction hypothesis there exists local recipe $\widehat{\zeta_T}$ of $(\widehat{\zeta_T}\sigma)\downarrow$ s.t $(\zeta_T =_{E_{Oka}} \widehat{\zeta_T})\phi'$(***). Then we conclude by transitivity from (*), (**) and (***) that $(\zeta_M = \widehat{\zeta_T})\phi'$. Thus we can choose $\widehat{\zeta_T}$ for a local recipe of M. □

Centre de recherche INRIA Nancy – Grand Est
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399