RAIRO-Theor. Inf. Appl. 45 (2011) 269–299
DOI: 10.1051/ita/2011119

Available online at:
www.rairo-ita.org

DECIDING KNOWLEDGE IN SECURITY PROTOCOLS UNDER SOME E-VOTING THEORIES [*]

Mouhebeddine Berrima[1], Narjes Ben Rajeb[2] and Véronique Cortier[3]

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.

Mathematics Subject Classification. 68Q85.

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

Keywords and phrases. Security protocols, formal methods, decidability, e-voting, equational theory, deduction, static equivalence.

[*] *This work has been partially supported by the ANR-07-SESU-002 project AVOTÉ.*

[1] LIP2, Faculté des Sciences, Tunis, Tunisia. berrima.mouheb@gmail.com

[2] LIP2, Institut National des Sciences Appliquées et de Technologie, Tunis, Tunisia.

[3] Loria, INRIA & CNRS, Nancy, France.

protocols. For example, secrecy is NP-complete when limiting the number of sessions [21]. Several tools have been developed for automatically analyzing security protocols (see *e.g.* [3,6]).

In formal approaches, the analysis of protocols often requires precise formulations of the knowledge (capability) of protocol participants and attackers. Indeed, most of security goals of voting protocols can be expressed or encoded in terms of attacker knowledge (see *e.g.* [13]). 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 [2]: 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.* [1,5,10–12]) 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 [14]. 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. In parallel to our work, Ciobâcă *et al.* [9] have developed a new decision procedure, inspired from [5]. Their procedure in particular terminates for the trapdoor commitment primitive, yielding a first decidability result. However, no decidability result is provided for re-encryption or designated verifier proofs.

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 and designated verifier proofs, particularly important in the Lee *et al.* protocol [18]. 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 [20]. 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 [19], for which we design an appropriate notion of *subterms*. For static equivalence, our proofs are also inspired from the technique developed in [1] for convergent subterm theories.

Outline of the paper: In Section 1, we introduce some basic notions and notations as well as deducibility and static equivalence notions. In Section 2 we present the two studied theories modeling the e-voting protocols. We present our decidability results for deduction in Section 3, and our decidability results for static equivalence in Section 4. In last section we conclude by summarizing our results.

1. Preliminaries

In this section, we present some basic notions and notations following [2]. We suppose the reader familiar with rewriting systems [15].

1.1. 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 use $fn(M)$ to denote the set of names that occur in the term M, and $head(M)$ to denote the head function symbol of 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 $=_E$ is obtained from the equations of E by reflexive, symmetric and transitive closure. Moreover, it is 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. Given two terms U and V, if there exists a rule $l \to r$ of the rewriting system $\mathcal{R}$ and some substitution θ 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.

1.2. Frames

In the applied pi calculus [2], a message sequence is organized into a frame $\nu\widetilde{n}\sigma$, where $\widetilde{n}$ is a finite set of names (intuitively, the fresh ones), ν is the restriction operator which intuitively introduces fresh names, and σ is a substitution of the form: $\{M_1/x_1, \ldots, M_k/x_k\}$ with $dom(\sigma) = \{x_1, \ldots, x_k\}$ 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 of a frame ϕ, denoted $fn(\phi)$, are defined to be the set $\{n \mid n \in \bigcup_{i=1}^{k} fn(M_i) \text{ and } n \notin \widetilde{n}\}$.

We introduce the definition of a term by *composition* and a term by *decomposition* with respect to a frame and a theory.

Definition 1.1. 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 $i = 1 \ldots k$, we say that:

- t is a term by decomposition if $t == f(t_1, \ldots, t_k)$ 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 $t == f(t_1, \ldots, t_k)$ and $f(t_1\sigma\downarrow, \ldots, t_k\sigma\downarrow) == t\sigma\downarrow$.

1.3. 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:

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

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

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 [1].

Proposition 1.2. *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.

Example 1.3. As an example, consider the equational theory E_{enc} of pairing and symmetric encryption. The signature is $\Sigma_{enc} = \{pair, enc, fst, snd, dec\}$. The function *enc* allows to encrypt a message x by a key y, *dec* allows to extract a message x from a ciphertext message $enc(x, y)$ by using the same key y, whereas *fst* and *snd* are functions that represent the projection functions on respectively the first and the second component of a pair $pair(x, y)$. The theory E_{enc} is defined by the axioms:

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

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 recipe for obtaining k is y and a recipe for obtaining s is $dec(x, y)$.

1.4. 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 $(M =_E N)\psi$.

Example 1.4. For example, consider again the theory E_{enc} defined in Example 1.3. 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.

2. 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.* [18] and the theory E_{Oka}, used for modeling the properties of the primitives used in the protocol proposed by Okamoto [20]. Their modeling has been taken from [14].

2.1. DVP and re-encryption

The protocol due to Lee *et al.* relies on two particular 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 can only convince one intended person, *e.g.*, the voter, that the re-encrypted ciphertext contains the original plaintext. (see [14] for more explanation).

We consider the signature $\Sigma_{Lee} = \{getpk, host, pk, checksign, sign, decrypt, rencrypt, penc, dvp, checkdvp, ok, f_0\}$. The functional symbols are of respective arity 1, 1, 1, 2, 2, 2, 2, 3, 4, 4, 0, 2. The theory E_{Lee} is then defined by 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 one can obtain the public key of each host (modeled by the functions *getpk* and *host*). In this model, it is indeed assumed that $host(x)$ is the host associated to the public key x. 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. The term $penc(m, pk(a), r)$ represents the encryption of m with the public key $pk(a)$ with the random coin r. The fourth equation models the re-encryption primitive (modeled by the function *rencrypt*). Indeed, it is possible to obtain a different encryption of the same message with another random coin, which is modeled by a function f_0 of the original one and the one used during the re-encryption. In 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. This is crucial in the context of e-voting protocols to protect a voter against coercion. Indeed, this primitive prevents a voter from proving to a third party that he has voted in a certain way.

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 [16]. It is defined by the following rewrite rules:

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

(3) $decrypt(penc(x, pk(y), z), y) \to x$
(4) $rencrypt(penc(x, pk(y), z), w) \to penc(x, pk(y), f_0(z, w))$
(5) $checkdvp(dvp(x, rencrypt(x, z), z, pk(y)), x, rencrypt(x, z), pk(y)) \to ok$
(6) $checkdvp(dvp(penc(x, pk(y), z), penc(x, pk(y), f_0(z, w)), w, pk(v)),$
$penc(x, pk(y), z), penc(x, pk(y), f_0(z, w)), pk(v)) \to ok$
(7) $checkdvp(dvp(x, y, z, w), x, y, pk(w)) \to ok.$

As a preliminary result, it is easy to show that (by inspection of the rewrite rules) applying a functional symbol to terms in normal form yields a term in normal form after at most one rewrite step (that must occur in head).

Lemma 2.1. *Let $\mathcal{R}_{E_{Lee}}$ be the convergent rewriting system associated to E_{Lee}. Let $M, M_1, \ldots, M_k \in \mathcal{T}(\Sigma_{Lee}, \mathcal{X})$ 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. ($\to$) Let $M_1, \ldots, M_k$ be terms in normal form and assume that $f(M_1, \ldots, M_k)$ is not in normal form, and $f(M_1, \ldots, M_k) \to^* M$. 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. 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 $f(M_1, \ldots, M_k){\downarrow} = M$. □

2.2. Trapdoor bit-commitment

The protocol due to Okamoto is based on a trap-door bit commitment scheme and on blind signatures. A trap-door bit commitment scheme allows an agent to open his commitment 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 [14] for more explanation).

We consider the signature $\Sigma_{Oka} = \{host, getpk, pk, open, sign, checksign, blind, unblind, tdcommit, f_1\}$. The functional symbols are of respective arity 1, 1, 1, 2, 2, 2, 2, 2, 3, 4. The theory E_{Oka} is defined by the following equations:

(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) $tdcommit(x, f_1(y, z, w, x), w) = tdcommit(y, z, w)$
(7) $f_1(x0, f_1(x, y, z, x0), z, x1) = f_1(x, y, z, x1).$

Equations (1) and (2) modeling public keys and digital signatures are the same as in previous section. Equations (3) and (4) model blind signatures [7], 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, 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 $\mathit{tdcommit}(x, y, z)$ models the commitment of the message x under the key y using the trap-door z. The sixth equation expresses that a commitment $\mathit{tdcommit}(y, z, w)$ can be viewed as a commitment of any value x. To open this commitment as x one has to know the key $f_1(y, z, w, x)$. Note that this is possible only if one knows the key z and the trap-door w used to forge the commitment $\mathit{tdcommit}(y, z, w)$. The last equation models the transitivity of the commitment key, *i.e.* if a key k, allowing to open a commitment of v as a commitment of v_1, uses a key k' allowing to open the commitment of v_1 as a commitment of v_2, then the key k allows to open the commitment of v as the commitment of v_2.

The main result of [4] 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 last three 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 [1]. 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 combination algorithm of [4] is done in polynomial time.

In the next we simply write E_{Oka} instead of E^2_{Oka}, which is defined by equations (5)–(7).

The rewriting system associated to E_{Oka} is obtained by orienting the equations from left to right and applying the Knuth-Bendix completion algorithm [16], which yields the following additional equation:

$$\mathit{open}(\mathit{tdcommit}(y, z, w), f_1(y, z, w, x)) \rightarrow x.$$

Thus the convergent rewriting system associated to E_{Oka}, denoted by $\mathcal{R}_{E_{Oka}}$, is defined by the following rewrite rules:

(1) $\mathit{open}(\mathit{tdcommit}(x, y, z), y) \rightarrow x$
(2) $\mathit{tdcommit}(x, f_1(y, z, w, x), w) \rightarrow \mathit{tdcommit}(y, z, w)$
(3) $\mathit{open}(\mathit{tdcommit}(y, z, w), f_1(y, z, w, x)) \rightarrow x$
(4) $f_1(x0, f_1(x, y, z, x0), z, x1) \rightarrow f_1(x, y, z, x1)$.

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

As for the E_{Lee} theory, we can show again that applying a functional symbol to terms in normal form yields a term in normal form after at most one rewrite step (that must occur in head).

Lemma 2.2. *Let $\mathcal{R}_{E_{Oka}}$ be the convergent rewriting system associated to E_{Oka}. Let $M, M_1, \ldots, M_k \in \mathcal{T}(\Sigma_{Oka}, \mathcal{X})$ 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 $M_1, \ldots, M_k$ be terms in normal form. Assume that $f(M_1, \ldots, M_k)$ 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 occurs in head. If the rule (1) or (3) is applied then it is clear that the term obtained is in normal form. There remain 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 two terms such that $tdcommit(M_1, M_2, M_3) \xrightarrow{h} tdcommit(M_1', M_2', M_3)$ with M_2 of the form $f_1(M_1', M_2', M_3, M_1)$. The only case where the term $tdcommit(M_1', M_2', M_3)$ can be reduced further 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 of the form $f_1(M_1', M_2', M_3, M_1)$. The only case where $f_1(M_1', M_2', M_3, M_4)$ is not in normal form, is the case where 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 $M_2 = f_1(M_1', f_1(M_1'', M_2'', M_3, M_1'), M_3, M_1)$, which is not in normal form, contradiction.

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 $f(M_1, \ldots, M_k)\downarrow = M$. □

3. Decidability of deduction

Our first main contribution is to prove the decidability of deduction for both theories.

Theorem 3.1. *The relations $\vdash_{E_{Lee}}$ and $\vdash_{E_{Oka}}$ can be decided in polynomial time.*

The rest of this section is devoted to the proof of the theorem. In the remaining of the paper, E denotes any of the two theories E_{Lee} or E_{Oka}.

3.1. Locality

Our starting point is the locality technique introduced by [19], and used in [8,10,12,17]. 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. Hence, the locality property guarantees that the number of computations to obtain a deducible term is bounded by the number of terms that can be involved in a local proof. The set $St_E(\phi \cup \{M\})$ is also denoted by $St_E(\phi, M)$. Thus, we introduce an appropriate notion of subterms for each theory, that we use for proving the locality property.

We simply write St_{Lee} (resp. St_{Oka}) instead of $St_{E_{Lee}}$ (resp. $St_{E_{Oka}}$).

Definition 3.2. The set $St_{Lee}(M)$ of (extended syntactic) subterms of a term $M \in \mathcal{T}(\Sigma_{Lee}, \mathcal{X})$ is defined as follows:

- $St_{Lee}(u) = u$ when u is a variable or a name,
- $St_{Lee}(penc(M_1, pk(M_2), f_0(M_3, M_4)))$=$\{penc(M_1, pk(M_2), f_0(M_3, M_4))\} \cup St_{Lee}(M_1) \cup St_{Lee}(pk(M_2)) \cup St_{Lee}(f_0(M_3, M_4)) \cup \{penc(M_1, pk(M_2), M_3)\}$,
- $St_{Lee}(sign(M_1, M_2)) = \{sign(M_1, M_2)\} \cup St_{Lee}(M_1) \cup St_{Lee}(pk(M_2))$,
- $St_{Lee}(f(M_1, \ldots, M_k)) = \{f(M_1, \ldots, M_k)\} \cup \bigcup_{i=1}^{k} St_{Lee}(M_i)$ otherwise.

Definition 3.3. The set $St_{Oka}(M)$ of (extended syntactic) subterms of a term $M \in \mathcal{T}(\Sigma_{Oka}, \mathcal{X})$ 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 definition of subterms St_{Lee} and St_{Oka} is extended to frames as expected. The following lemma states the locality property for both theories.

Lemma 3.4 (locality). *Let E be E_{Lee} or E_{Oka} and let Σ_{0_E} be the set of constant symbols for the equational theory E. 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 $\zeta''\sigma{\downarrow} \in St_E(\phi, \zeta'\sigma{\downarrow}) \cup \Sigma_{0_E}$. 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 $\zeta''\sigma{\downarrow} \in St_E(\phi) \cup \Sigma_{0_E}$.*

Proof. Due to the characterization of deduction (Prop. 1.2), 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 $St_E(\zeta_M) = \{\zeta_M\}$.
Induction step: Let $\zeta_M = f(\zeta_1, \ldots, \zeta_k)$. By minimality of ζ_M, the terms ζ_i are minimal recipes of $\zeta_i\sigma{\downarrow}$. By induction hypothesis we have for all $\zeta' \in St_E(\zeta_i)_{i=1\ldots k}$, for all $\zeta'' \in St_E(\zeta')$ we have $\zeta''\sigma{\downarrow} \in St_E(\phi, \zeta'\sigma{\downarrow}) \cup \Sigma_{0_E}$. To conclude that for all

[2] A rule $l \to r$ is called *subterm rule* if $r \in St_E(l)$ or r is constant symbol. Note in particular that rule (2) of $\mathcal{R}_{Oka}$ is a subterm rule.

$\zeta'' \in St_E(\zeta')$ we have $\zeta''\sigma\!\downarrow \in St_E(\phi, \zeta'\sigma\!\downarrow) \cup \Sigma_{0_E}$ for any $\zeta' \in St_E(\zeta_M)$, it is sufficient to show for all $\zeta'' \in St_E(\zeta_M)$, we have $\zeta''\sigma\!\downarrow \in St_E(\phi, M) \cup \Sigma_{0_E}$. For this, it is sufficient to prove that for all $i = 1 \dots k$ we have $\zeta_i\sigma\!\downarrow \in St_E(\phi, M) \cup \Sigma_{0_E}$, since if $\zeta_i\sigma\!\downarrow \in St_E(\phi, M) \cup \Sigma_{0_E}$ then for all $\zeta'' \in St_E(\zeta_i)$ we have $\zeta''\sigma\!\downarrow \in St_E(\phi, \zeta_i\sigma\!\downarrow) \cup \Sigma_{0_E} \subseteq St_E(\phi, M) \cup \Sigma_{0_E}$. For the second condition, it is sufficient to show that if $f(\zeta_1\sigma\!\downarrow, \dots, \zeta_k\sigma\!\downarrow) \xrightarrow{h} \zeta''\sigma\!\downarrow$ by applying a subterm rule then $M \in St_E(\phi) \cup \Sigma_{0_E}$. Indeed, for any strict subterm of ζ_M, we can conclude by induction hypothesis.

– If $f(\zeta_1\sigma\!\downarrow, \dots, \zeta_k\sigma\!\downarrow)$ is in normal form, then for all $i = 1 \dots k$ we have $\zeta_i\sigma\!\downarrow \in St_E(f(\zeta_1\sigma\!\downarrow, \dots, \zeta_k\sigma\!\downarrow))$ and we conclude.

– If $f(\zeta_1\sigma\!\downarrow, \dots, \zeta_k\sigma\!\downarrow)$ is not in normal form. In this case, we treat each theory separately.

(1) Under $\mathbf{E_{Lee}}$ theory:

If $f(\zeta_1\sigma\!\downarrow, \dots, \zeta_k\sigma\!\downarrow)$ is not in normal form. Since $\zeta_1\sigma\!\downarrow, \dots, \zeta_k\sigma\!\downarrow$ are in normal form then by Lemma 2.1 we have $f(\zeta_1\sigma\!\downarrow, \dots, \zeta_k\sigma\!\downarrow) \xrightarrow{h} M$. We distinguish five cases according to f:

– If $f = \mathit{checkdvp}$, this case cannot appear by minimality of ζ_M, indeed ok would be a recipe smaller than ζ_M.

– If $f = \mathit{getpk}$, this implies $k = 1$, so we have $\zeta_M = \mathit{getpk}(\zeta_1)$ and since $\zeta_M\sigma$ can be reduced then $\mathit{head}(\zeta_1\sigma\!\downarrow) = \mathit{host}$. 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.
- $\zeta_1 = g(\zeta'_1, \dots, \zeta'_k)$ and $g(\zeta'_1\sigma\!\downarrow, \dots, \zeta'_k\sigma\!\downarrow) \xrightarrow{h} \zeta_1\sigma\!\downarrow$ by applying a rule different from (4). Then by induction hypothesis we have $\zeta_1\sigma\!\downarrow \in St_{Lee}(\phi) \cup \Sigma_{0_{Lee}}$. Moreover, 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 $\mathit{head}(\zeta_1\sigma\!\downarrow) = \mathit{penc}$ and by equational theory E_{Lee}, $\mathit{getpk}(\zeta_1\sigma\!\downarrow)$ cannot be reduced, contradiction.
- $\zeta_1 = g(\zeta'_1, \dots, \zeta'_k)$ and $g(\zeta'_1\sigma\!\downarrow, \dots, \zeta'_k\sigma\!\downarrow)$ is in normal form with $g \neq \mathit{host}$, this case cannot appear because this implies that $\mathit{getpk}(\zeta_1\sigma\!\downarrow)$ cannot reduced, contradiction.
- $\zeta_1 = \mathit{host}(\zeta'_1)$, this case cannot appear by minimality of ζ_M, because we have ζ'_1 smaller than ζ_M.

– $f = \mathit{checksign}$, this implies $k = 2$, so we have $\zeta_M = \mathit{checksign}(\zeta_1, \zeta_2)$ and since $\zeta_M\sigma$ can be reduced then $\mathit{head}(\zeta_1\sigma\!\downarrow) = \mathit{sign}$ and $\zeta_2\sigma\!\downarrow \in St_{Lee}(\zeta_1\sigma\!\downarrow)$. Thus it is sufficient to prove that $\zeta_1\sigma\!\downarrow \in St_{Lee}(\phi, M)$ and $M \in St_{Lee}(\phi) \cup \Sigma_{0_E}$. 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.
- $\zeta_1 = g(\zeta'_1, \dots, \zeta'_k)$ and $g(\zeta'_1\sigma\!\downarrow, \dots, \zeta'_k\sigma\!\downarrow) \xrightarrow{h} \zeta_1\sigma\!\downarrow$ by applying a rule different from (4). Then by induction hypothesis we have $\zeta_1\sigma\!\downarrow \in St_{Lee}(\phi) \cup \Sigma_{0_{Lee}}$. 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 E_{Lee}, $checksign(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow)$ cannot be 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 $checksign(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow)$ cannot be reduced, contradiction.
- $\zeta_1 = sign(\zeta'_1, \zeta'_2)$, this case cannot appear by minimality of ζ_M, because we have 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 $\zeta_M\sigma$ can be reduced then $head(\zeta_1\sigma\downarrow) = penc$. We have that $\zeta_1\sigma$ is of the form $penc(M_1, pk(M_2), M_3)$ and $M = penc(M_1, pk(M_2), f_0(M_3, \zeta_2\sigma\downarrow))$. By Definition 3.2 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 $\zeta_M\sigma$ can be 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 $\zeta_1\sigma\downarrow \in St_{Lee}(\phi, M)$ and $M \in St_{Lee}(\phi) \cup \Sigma_{0_E}$. 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 $decrypt(\zeta'_1, \zeta_2)$ 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 $decrypt(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow)$ cannot be reduced, contradiction.
- $\zeta_1 = penc(\zeta'_1, pk(\zeta'_2), \zeta'_3)$. This case cannot appear by minimality of ζ_M, because we have ζ'_1 smaller than ζ_M.

(2) Under $\mathbf{E_{Oka}}$ theory:
$f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow)$ is not in normal form. Since $\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow$ are in normal form then by Lemma 2.2 we have $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow) \xrightarrow{h} M$. We distinguish several cases depending on which rule has been applied:

– If the rule (1) is applied, then we have $\zeta_M = open(\zeta_1, \zeta_2)$. Since $\zeta_M\sigma$ can be reduced, 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 $\zeta_1\sigma\downarrow \in St_{Oka}(\phi, M)$ and $M \in St_{Oka}(\phi) \cup \Sigma_{0_E}$. 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 since ζ'_1 is 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 $\mathit{open}(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow)$ cannot be 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 $\mathit{head}(\zeta_1\sigma\downarrow) = f_1$, thus by equational theory E_{Oka}, $\mathit{open}(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow)$ cannot be reduced, contradiction.

– If the rule (2) is applied, then we have $\zeta_M = \mathit{tdcommit}(\zeta_1, \zeta_2, \zeta_3)$. Since $\zeta_M\sigma$ can be reduced, then $\mathit{head}(\zeta_2\sigma\downarrow) = f_1$ and $\zeta_1\sigma\downarrow, \zeta_3\sigma\downarrow \in St_{Oka}(\zeta_2\sigma\downarrow)$. Thus it is sufficient to prove that $\zeta_2\sigma\downarrow \in St_{Oka}\ (\phi, M)$ and $M \in St_{Oka}\ (\phi) \cup \Sigma_{0_E}$. 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 since $\mathit{tdcommit}(\zeta'_1, \zeta'_2, \zeta'_3)$ is 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 $\mathit{tdcommit}(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow, \zeta_3\sigma\downarrow)$ cannot be 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 $\mathit{head}(\zeta_2\sigma\downarrow) = \mathit{tdcommit}$, thus by equational theory E_{Oka}, $\mathit{tdcommit}(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow, \zeta_3\sigma\downarrow)$ cannot be reduced, contradiction.

– If the rule (3) is applied, then we have $\zeta_M = \mathit{open}(\zeta_1, \zeta_2)$. Since $\zeta_M\sigma$ can be reduced, then $\mathit{head}(\zeta_2\sigma\downarrow) = f_1$ and $\zeta_1\sigma\downarrow \in St_{Oka}(\zeta_2\sigma\downarrow)$. Thus it is sufficient to prove that $\zeta_2\sigma\downarrow \in St_{Oka}\ (\phi, M)$ and $M \in St_{Oka}\ (\phi) \cup \Sigma_{0_E}$. 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 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 $\mathit{open}(\zeta_1\sigma\downarrow, \zeta_2\sigma\downarrow)$ cannot be 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 (4) is applied, then we have $\zeta_M = f_1(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$. Since $\zeta_M\sigma$ can be reduced to its normal form then $\mathit{head}(\zeta_2\sigma\!\downarrow) = f_1$ and $\zeta_1\sigma\!\downarrow, \zeta_3\sigma\!\downarrow \in \mathit{St}_{Oka}(\zeta_2\sigma\!\downarrow)$ and since $\zeta_4\sigma\!\downarrow \in \mathit{St}_{Oka}(\zeta_M\sigma\!\downarrow)$, thus it is sufficient to prove that $\zeta_2\sigma\!\downarrow \in \mathit{St}_{Oka}(\phi, M)$. We distinguish several cases for ζ_2:

- ζ_2 is a variable, then we conclude.
- $\zeta_2 = f_1(\zeta'_1, \zeta'_2, \zeta'_3, \zeta'_4)$. This case cannot appear by minimality of ζ_M since $f_1(\zeta'_1, \zeta'_2, \zeta'_3, \zeta_4)$ is smaller than ζ_M.
- $\zeta_2 = g(\zeta'_1, \dots, \zeta'_k)$ and $g(\zeta'_1\sigma\!\downarrow, \dots, \zeta'_k\sigma\!\downarrow)$ is in normal form with $g \neq f_1$, this case cannot appear because this implies that $f_1(\zeta_1\sigma\!\downarrow, \zeta_2\sigma\!\downarrow, \zeta_3\sigma\!\downarrow, \zeta_4\sigma\!\downarrow)$ cannot be reduced, contradiction.
- $\zeta_2 = g(\zeta'_1, \dots, \zeta'_k)$ and $g(\zeta'_1\sigma\!\downarrow, \dots, \zeta'_k\sigma\!\downarrow) \xrightarrow{h} \zeta_1\sigma\!\downarrow$ by applying the rule (1) or (3). Then by induction hypothesis we have $\zeta_2\sigma\!\downarrow \in \mathit{St}_{Oka}(\phi) \cup \Sigma_{0_{Oka}}$, and since the applied rule is a subterm rule then $M \in \mathit{St}_{Oka}(\zeta_2\sigma\!\downarrow) \subseteq \mathit{St}_{Oka}(\phi) \cup \Sigma_{0_{Oka}}$, thus we conclude. If the rule (2) is applied, this case cannot appear because this implies $\mathit{head}(\zeta_2\sigma\!\downarrow) = \mathit{tdcommit}$, thus by equational theory E_{Oka}, $f_1(\zeta_1\sigma\!\downarrow, \zeta_2\sigma\!\downarrow, \zeta_3\sigma\!\downarrow, \zeta_4\sigma\!\downarrow)$ cannot be reduced, contradiction. □

Example 3.5. Consider the equational theory E_{Oka}, the frame $\phi = \nu m, n, r, s.\{f_1(m, n, r, s)/x_1, r/x_2, s/x_3, n/x_4\}$ and $M = m$. We have that $\phi \vdash M$. The recipe $\zeta_M = \mathit{open}(\mathit{tdcommit}(x_3, x_1, x_2), x_4)$ satisfies the conditions given in Lemma 3.4.

3.2. Deciding deduction

We propose an algorithm to decide $\phi \vdash_E M$ for both the Lee and the Okamoto theories. Our algorithm, named Algorithm 1 and presented in Figure 1, is inspired from the frame saturation algorithm introduced in [1]. The idea is to compute by saturation all subterms of ϕ and M that are deducible from ϕ.

The next proposition shows correctness and completeness of the algorithm for the subterms of a frame ϕ and a closed term M. It relies on the locality property proved in the previous section. Moreover, the recipes computed by the algorithm are local and minimal (in size).

Proposition 3.6. *Let $\phi = \nu\tilde{n}\sigma$ be a frame such that $\sigma = \{M_1/x_1, \dots, M_k/x_k\}$ is in normal form, M be a term in normal form and T be the set computed by the Algorithm 1. Then $\forall M' \in \mathit{St}_E(\phi, M)$ we have $\phi \vdash_E M'$ iff there exists a local recipe $\zeta_{M'}$ of M', of minimal size among local recipes of M', such that $(M', \zeta_{M'}) \in T$.*

Proof. ($\rightarrow$) Since M' is deducible, then by Lemma 3.4, there exists a local recipe $\zeta_{M'}$ of M'. We proceed by induction on the size of $\zeta_{M'}$ to prove that there exists a minimal local recipe $\overline{\zeta}_{M'}$ of M' s.t $(M', \overline{\zeta}_{M'}) \in T$ and $|\overline{\zeta}_{M'}| \leq |\zeta_{M'}|$. This will show that $\overline{\zeta}_{M'}$ is of minimal size among local recipes of M'.

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

FIGURE 1. Algorithm of deduction.

Base case: If $\zeta_{M'}$ is a variable or a name, then by instruction 1 we have $(M', \overline{\zeta}_{M'}) \in T$ (where $\overline{\zeta}_{M'}$ is the variable chosen by the algorithm). Moreover $\overline{\zeta}_{M'}$ is minimal and local since $St_E(\overline{\zeta}_{M'}) = \{\overline{\zeta}_{M'}\}$.

Inductive step: Let $\zeta_{M'} = f(\zeta_1, \dots, \zeta_n)$. 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 $i = 1 \dots n$, with $\overline{\zeta}_i$ are the recipes of $(\zeta_i\sigma)\downarrow$ computed by the algorithm, thus:

- If $\zeta_{M'}\sigma\downarrow == f(\zeta_1\sigma\downarrow, \dots, \zeta_n\sigma\downarrow)$, then by the instruction 3 of the Algorithm 1 we have $(M', \overline{\zeta}_{M'}) \in T$ (with $\overline{\zeta}_{M'} = f(\overline{\zeta}_1, \dots, \overline{\zeta}_n)$ or $\overline{\zeta}_{M'}$ is some local recipe such that $|\overline{\zeta}_{M'}| < |f(\overline{\zeta}_1, \dots, \overline{\zeta}_n)|$). Moreover $\overline{\zeta}_{M'}$ is local either because it was already computed by the algorithm or because $f(\zeta_1, \dots, \zeta_n)$ is local and $\overline{\zeta}_i$ are the local recipes of $\zeta_i\sigma\downarrow$ for $i = 1 \dots n$.
- If $f(\zeta_1\sigma\downarrow, \dots, \zeta_n\sigma\downarrow)$ is not in normal form. Since $\zeta_1\sigma\downarrow, \dots, \zeta_n\sigma\downarrow$ are in normal form then by Lemma 2.1 (or Lem. 2.2) we have $f(\zeta_1\sigma\downarrow, \dots, \zeta_n\sigma\downarrow) \xrightarrow{h} M'$. Then by the instruction 2 of the Algorithm 1 we have

$(M', \overline{\zeta}_{M'}) \in T$ (with $\overline{\zeta}_{M'} = f(\overline{\zeta}_1, \ldots, \overline{\zeta}_n)$ or $\overline{\zeta}_{M'}$ is some local recipe such that $|\overline{\zeta}_{M'}| < |f(\overline{\zeta}_1, \ldots, \overline{\zeta}_n)|$). Moreover $\overline{\zeta}_{M'}$ is local either because it was already computed by the algorithm or because $f(\zeta_1, \ldots, \zeta_n)$ is local and $\overline{\zeta}_i$ are the local recipes of $\zeta_i\sigma\downarrow$ for $i = 1 \ldots n$.

Now let us prove the minimality of $\overline{\zeta}_{M'}$. By induction hypothesis, we know that $|\overline{\zeta}_i| \leq |\zeta_i|$ thus $|f(\overline{\zeta}_1, \ldots, \overline{\zeta}_n)| \leq |f(\zeta_1, \ldots, \zeta_n)|$. Since $|\overline{\zeta}_{M'}| \leq |f(\overline{\zeta}_1, \ldots, \overline{\zeta}_n)|$ we deduce $|\overline{\zeta}_{M'}| \leq \zeta_{M'}$.

($\leftarrow$) 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 1.2 we have $\phi \vdash_E M'$. □

Corollary 3.7. *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 3.6 since $M \in St_E(\phi, M)$. □

The complexity results for deduction and static equivalence are as usually given as functions of the DAG-size of the terms, where 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. We are now ready to show that deduction is decidable in polynomial time for both theories.

Proposition 3.8. *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 $|\zeta_M|_{dag} \leq |\phi|_{dag} + |M|_{dag}$.*

Proof. 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 $(M, \zeta) \in T$ (at most $|\phi|_{dag} + |M|_{dag}$ comparisons), 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 3.8 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 $\zeta''\sigma\!\downarrow\, \in St_E(\phi, M)$. The algorithm constructs a shared DAG for all the recipes that increases of at most one at each step (obtained either by the rule 2 or the rule 3). Thus, the maximal DAG-size of ζ_M is $|\phi|_{dag} + |M|_{dag}$, because the algorithm terminates at most in $|\phi|_{dag} + |M|_{dag}$ steps. □

4. Decidability of static equivalence

Our second main contribution is to prove the decidability of static equivalence for both theories.

Theorem 4.1. *The relations $\approx_{E_{Lee}}$ and $\approx_{E_{Oka}}$ can be decided in polynomial time.*

The rest of this section is devoted to the proof of the theorem. Our approach is based on the result of [1] 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. Therefore, the set of equalities that characterizes a frame is constructed on the local recipes of elements of $sat_E(\phi) \cup I_E(\phi)$. 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. These sets are defined in the next (sub)section. We prove the main steps of Theorem 4.1 in Section 4.2. Section 4.3 then contains the remaining proof of the two main technical lemmas.

4.1. Computing a finite set of equalities

We define in this section the set of small equalities we will consider to check for static equivalence.

Step 1: deducible subterms. We define the set $sat_E(\phi)$ to be the set of *deducible subterms* of ϕ.

Definition 4.2. Let $\phi = \nu\tilde{n}.\{M_1/x_1, \ldots, M_n/x_n\}$ 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

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

Thanks to Proposition 3.8, the set $sat_E(\phi)$ can be computed in polynomial time using Algorithm 1.

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

Definition 4.3. 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, for any $M_1, M_2, M_3 \in sat_{Lee}(\phi)$, for any M deducible from ϕ such that $M \in St_{Lee}(penc(M_1, M_2, M_3))$, then $M \in I_{Lee}(\phi)$.

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

Proposition 4.4. *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form.*

(1) *The set $sat_E(\phi) \cup I_E(\phi)$ can be computed in polynomial time.*

(2) *For every $M \in sat_E(\phi) \cup I_E(\phi)$, there exists a term ζ_M such that $fn(\zeta_M) \cap \widetilde{n} = \emptyset$, $\zeta_M\sigma =_E M$, and ζ_M has a polynomial DAG-size.*

Proof. For E_{Lee} theory, the set $sat_{Lee}(\phi)$ is computed in at most $|\phi|_{dag}$ steps. At each step we need at most (by Prop. 3.8) $\mathcal{O}((|\phi|_{dag} + |M|_{dag})^{ar(\Sigma_{Lee})+2})$ with $M \in St_{Lee}(\phi)$. Since for each $M \in St_{Lee}(\phi)$ we have $|M|_{dag} \leq |\phi|_{dag}$, we conclude that $sat_{Lee}(\phi)$ is computed in time $\mathcal{O}(|\phi|_{dag}^{ar(\Sigma_{Lee})+3})$. Moreover the DAG representation of $sat_{Lee}(\phi)$ can be obtained from the DAG representation of ϕ by simply adding edges. Thus $|sat_{Lee}(\phi)|_{dag} \leq |\phi|_{dag}$. 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 $|sat_{Lee}(\phi)|_{dag}^3 \leq |\phi|_{dag}^3$ terms), and for each subterm M of a such term (at most $2|\phi|_{dag}^3$ terms), we check whether it is deducible (by Prop. 3.8 we need at most $\mathcal{O}((|\phi|_{dag} + |M|_{dag})^{ar(\Sigma)+2})$). Thus we need at most $\mathcal{O}(|\phi|_{dag}^6)$. Then we conclude that the set $sat_{Lee}(\phi) \cup I_{Lee}(\phi)$ can be computed in polynomial time.

For the second part of proposition, we know by Proposition 3.8, 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 ζ_M when M in $sat_{Lee}(\phi) \cup I_{Lee}(\phi)$ is $|\phi|_{dag}(c_{E_{Lee}} + 1)$.

For E_{Oka} theory, we can easily conclude since I_{Oka} is empty. □

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 correspond to the terms of $sat_E(\phi) \cup I_E(\phi)$.

Example 4.5. We consider the equational theory E_{Lee}.
Let $\phi = \nu s, m, n\{penc(s, pk(k), m)/x_1, k/x_2, f_0(m, n)/x_3, n/x_4\}$ be a frame in normal form. By Definition 4.2 we have $sat_{Lee}(\phi) = \{M_1, M_2, M_3, M_4, M_5, M_6\}$, where $M_1 = penc(s, pk(k), m)$, $M_2 = k$, $M_3 = f_0(m, n)$, $M_4 = n$, $M_5 = s$ and $M_6 = pk(k)$. By Definition 4.3 we have $I_{Lee}(\phi) = sat_{Lee}(\phi) \cup \{penc(M_i, M_j, M_k) \mid 1 \leq i, j, k \leq 6\}$.

The local recipes for each term of the set $sat_{Lee}(\phi)$ computed by the Algorithm 1 are: $\zeta_{M_1} = x_1$, $\zeta_{M_2} = x_2$, $\zeta_{M_3} = x_3$, $\zeta_{M_4} = x_4$, $\zeta_{M_5} = decrypt(x_1, x_2)$, $\zeta_{M_6} = pk(x_2)$. The local recipes for each term of the set $I_{Lee}(\phi)$ (after removing the terms of $sat_{Lee}(\phi)$) are of the form $penc(\zeta_{M_i}, \zeta_{M_j}, \zeta_{M_k})$ with $1 \leq i, j, k \leq 6$ except the recipe of the term $penc(M_5, M_6, M_3)$, it is of the form $rencrypt(x_1, x_4)$.

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

Definition 4.6. Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form. The set $Eq_E(\phi)$ is the set of equalities

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

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

Given a frame ϕ, we simply write $Eq_{Lee}(\phi)$ (resp. $Eq_{Oka}(\phi)$) instead of $Eq_{E_{Lee}}(\phi)$ (resp. $Eq_{E_{Oka}}(\phi)$).

Example 4.7. We continue Example 4.5. By Definition 4.6, we obtain several trivial and redundant equalities in $Eq_{Lee}(\phi)$ except the following equality: $\zeta_{M_7} = penc(\zeta_{M_5}, \zeta_{M_6}, \zeta_{M_3})$, that is, $rencrypt(x_1, x_4) = penc(decrypt(x_1, x_2), pk(x_2), x_3)$. This equality allows to an intruder to decide if two frames are statically equivalent or not. Intuitively, this equality corresponds to the ability of an intruder that can check about the random coin used for probabilistic encryption of the message referred by x_1.

4.2. Proof of decidability for static equivalence

Our goal is to show that for checking for static equivalence of two frames, it is actually sufficient to consider the set of equalities $Eq_E(\phi)$ introduced in the previous section. That is, $\phi \approx_E \phi'$ if and only if $\phi \models Eq_E(\phi')$ and $\phi' \models Eq_E(\phi)$. This result relies on the two following (key) lemmas.

Lemma 4.8. *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 4.9. *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 w.r.t ϕ, 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 proof of these two lemmas is left for the next section. They allow us to conclude that it is indeed sufficient to check for small equalities.

Proposition 4.10. *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 4.9 there exists $\widehat{M}, \widehat{N}$

such that $(\widehat{M} =_E M)\phi'$ and $(\widehat{N} =_E N)\phi'$. Then, by Lemma 4.8 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 $\phi \approx_E \phi'$. □

Therefore, our algorithm consists in reducing the problem of decidability of static equivalence to decide whether each frame satisfy the equality from other's set.

We are now ready to conclude the proof of Theorem 4.1.

Proof. Let E be E_{Lee} or E_{Oka}. The decision procedure of static equivalence proceeds in three steps. First, 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 4.10, we test if each frame satisfy the equality from other's set. Moreover, according to the Proposition 4.4, 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 conclude that this procedure can be done in polynomial time (in the DAG-size of inputs terms). □

4.3. Proofs of the two key lemmas

The end of this section is devoted to the proofs of the two key lemmas (Lems. 4.8 and 4.9). We first state and prove two preliminary results that will be used for proving Lemma 4.8 under E_{Lee}.

Proposition 4.11. *Let $\phi = \nu\tilde{n}\sigma$ be a frame in normal form, $M \in \mathcal{T}(\Sigma_{Lee}, \mathcal{X})$ 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. The case ζ_M is a variable is impossible because this would imply $M \in sat_{Lee}(\phi)$. Thus $\zeta_M = g(\zeta_1, \ldots, \zeta_k)$. Let $N_i = \zeta_i\sigma\downarrow$.

- If $g(N_1, \ldots, N_k)$ is in normal form, then $g = f$, $N_i = M_i$ 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 2.1 we have $g(N_1, \ldots, N_k) \xrightarrow{h} M$. Let us show that 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 from subterm rule. So, by locality lemma we have $M \in St_{Lee}(\phi)$ and by Definition 4.2 we have $M \in sat_{Lee}(\phi)$ since M is deducible, contradiction. □

Proposition 4.12. *Let $\phi = \nu\tilde{n}\sigma$ be a frame in normal form, $M \in \mathcal{T}(\Sigma_{Lee}, \mathcal{X})$ of the form $penc(N_1, N_2, N_3)$ and $\zeta_M = rencrypt(\zeta_{M_1}, \zeta_{M_2})$ its local recipe s.t $\zeta_M\sigma\downarrow = M$ and $M \notin sat_{Lee}(\phi)$. The terms $(\zeta_{M_i})_{i=1,2}$ are the local recipes of* *some terms M_i s.t $\zeta_{M_i}\sigma\downarrow = M_i$. Assume both N_1, N_2 are deducible and there exists $i \in \{1,2\}$ such that $N_i \notin sat_{Lee}(\phi)$. 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 $(\zeta_{N_i})_{i=1,2}, \zeta_{N'_3}$ local recipes of N_i, N'_3, such that $\zeta_{N_i}\sigma\downarrow = N_i$ 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: We must have $M_1 = penc(N_1, N_2, N'_3)$ with $N_3 = f_0(N'_3, M_2)$ thus $N'_3 \in St_{Lee}(N_3)$. Since $N_i \notin sat_{Lee}(\phi)$ for some $i \in \{1,2\}$, we must have $M_1 \notin sat_{Lee}(\phi)$. Indeed, assume $M_1 \in sat_{Lee}(\phi)$, Then since N_1, N_2 are deducible subterms of M_1, we would have $N_1, N_2 \in St_{Lee}(\phi)$ and by Definition 4.2 we would have $N_i \in sat_{Lee}(\phi)$ for every $i \in \{1,2\}$, contradiction. So, we distinguish several cases depending on 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 $\zeta_{M_1} = penc(\zeta_1, \zeta_2, \zeta_3)$ and $\zeta_1, \zeta_2, \zeta_3$ are local recipes of N_1, N_2, N'_3 respectively. $\zeta_{N'_i}\sigma\downarrow = N'_i$ for $i \in \{1,2,3\}$. By equational theory E_{Lee} we have $N'_i = N_i$ for $i = 1,2$ and we have $N'_3 \in St_{Lee}(N_3)$. Thus we have $rencrypt(\zeta_{M_1}, \zeta_{M_2}) =_{E_{Lee}} penc(\zeta_1, \zeta_2, f_0(\zeta_3, \zeta_{M_2}))$, and we conclude.
- $\zeta_{M_1} = f(\zeta_1, \ldots, \zeta_k)$ 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 2.1 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 4.2 $M_1 \in sat_{Lee}(\phi)$. 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 $rencrypt(\zeta_{M_1}, \zeta_{M_2}) =_{E_{Lee}} penc(\zeta_{N_1}, \zeta_{N_2}, f_0(f_0(\zeta_{N''_3}, \zeta_{M'_2}), \zeta_{M_2}))$ with $\zeta_{N'_3} = f_0(\zeta_{N''_3}, \zeta_{M'_2})$, thus we conclude. □

Proof of Lemma 4.8.
(*) Proof under E_{Lee}: Assume that $\phi' \models Eq_{Lee}(\phi)$ and consider ζ_M, ζ_N local recipes 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, then by Definition 4.6 we have $(\zeta_M = \zeta_N) \in Eq_{Lee}(\phi)$, and we conclude by $\phi' \models Eq_{Lee}(\phi)$.
– **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 $f(\zeta_1, \ldots, \zeta_k) = g(\zeta'_1, \ldots, \zeta'_n)$. 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 4.2 we have $\zeta_i\sigma\downarrow, \zeta'_i\sigma\downarrow \in sat_{Lee}(\phi)$. Let $\overline{\zeta}_i, \overline{\zeta'}_i$

be the local recipes of $\zeta_i\sigma{\downarrow}, \zeta'_i\sigma{\downarrow}$ computed by Algorithm 1. By construction of $Eq_{Lee}(\phi)$, we have $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) = g(\overline{\zeta'}_1, \ldots, \overline{\zeta'}_n)) \in Eq_{Lee}(\phi)$, and we deduce $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) =_{E_{Lee}} g(\overline{\zeta'}_1, \ldots, \overline{\zeta'}_n))\phi'$ by $\phi' \models Eq_{Lee}(\phi)$. Moreover, by induction hypothesis (since $|\overline{\zeta}_i| \leq |\zeta_i|$ and $|\overline{\zeta'}_i| \leq |\zeta'_i|$) 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 $\zeta_i\sigma{\downarrow}$ computed by Algorithm 1. We have $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) = x) \in Eq_{Lee}(\phi)$, and we deduce $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) =_{E_{Lee}} x)\phi'$ by $\phi' \models Eq_{Lee}(\phi)$. Moreover, by induction hypothesis (since $|\overline{\zeta}_i| \leq |\zeta_i|$) 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 nor 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 4.2 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 E_{Lee} 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 converse): 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 4.2 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 $(\zeta'_i\sigma{\downarrow} = N_i)_{i=1,2,3}$.

(i) Assume first that $N_i \in sat_{Lee}(\phi)$ for $i = 1, 2, 3$. Since M_2 is deducible and $M_2 \in St_{Lee}(\phi)$ (because $M_2 \in St_{Lee}(N_3)$ and $N_3 \in sat_{Lee}(\phi)$) then by Definition 4.2 $M_2 \in sat_{Lee}(\phi)$. Moreover, since $M_1 \in St_{Lee}(penc(N_1, N_2, N_3))$ and it is deducible then by Definition 4.3 $M_1 \in I_{Lee}(\phi)$. Let $\overline{\zeta}_i, \overline{\zeta'}_i$ be the local recipes of M_i, N_i computed by Algorithm 1. We have $(rencrypt(\overline{\zeta}_1, \overline{\zeta}_2) = penc(\overline{\zeta'}_1, \overline{\zeta'}_2, \overline{\zeta'}_3)) \in Eq_{Lee}(\phi)$, and we deduce $(rencrypt(\overline{\zeta}_1, \overline{\zeta}_2) =_{E_{Lee}} penc(\overline{\zeta'}_1, \overline{\zeta'}_2, \overline{\zeta'}_3))\phi'$ by $\phi' \models Eq_{Lee}(\phi)$. Moreover, by induction hypothesis (since $|\overline{\zeta}_i| \leq |\zeta_i|$ and $|\overline{\zeta'}_i| \leq |\zeta'_i|$) we have $(\zeta_i =_{E_{Lee}} \overline{\zeta}_i)\phi'$ and $(\zeta'_i =_{E_{Lee}} \overline{\zeta'}_i)\phi'$. Thus, since $=_{E_{Lee}}$ is closed 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.

(ii) Else, we distinguish two cases:

- If $N_3 \notin sat_{Lee}(\phi)$, since $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$ then by equational theory E_{Lee} N_3 is of the form $f_0(N_4, N_5)$, and as ζ'_3 is local, so by Proposition 4.11 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 4.12, there exists a deducible term 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 $(penc(\zeta_{N_1}, \zeta_{N_2}, f_0(\zeta_{N'_3}, \zeta_2)) =_{E_{Lee}} penc(\zeta'_1, \zeta'_2, \zeta'_3))\phi'$. 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 2.1 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.

(**) Proof under E_{Oka}: Assume that $\phi' \models Eq_{Oka}(\phi)$ and consider ζ_M, ζ_N local recipes such that $(\zeta_M =_{E_{Oka}} \zeta_N)\phi$ and $(fn(\zeta_M) \cup fn(\zeta_N)) \cap \widetilde{n} = \emptyset$. Let $T = \zeta_M\sigma\!\downarrow$. We show by induction on the max of the size of ζ_M and ζ_N that $(\zeta_M =_{E_{Oka}} \zeta_N)\phi'$.
– **Base case:** ζ_M, ζ_N are variables, then by Definition 4.6 we have $(\zeta_M = \zeta_N) \in Eq_{Oka}(\phi)$, and we conclude by $\phi' \models Eq_{Oka}(\phi)$.
– **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 $f(\zeta_1, \ldots, \zeta_k) = g(\zeta'_1, \ldots, \zeta'_n)$. 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 4.2 we have $\zeta_i\sigma\!\downarrow, \zeta'_i\sigma\!\downarrow \in sat_{Oka}(\phi)$. Let $\overline{\zeta}_i, \overline{\zeta'}_i$ be the local recipes of $\zeta_i\sigma\!\downarrow, \zeta'_i\sigma\!\downarrow$ computed by Algorithm 1. We have $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) = g(\overline{\zeta'}_1, \ldots, \overline{\zeta'}_n)) \in Eq_{Oka}(\phi)$, and we deduce $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) =_{E_{Oka}} g(\overline{\zeta'}_1, \ldots, \overline{\zeta'}_n))\phi'$ by $\phi' \models Eq_{Oka}(\phi)$. Moreover, by induction hypothesis (since $|\overline{\zeta}_i| \leq |\zeta_i|$ and $|\overline{\zeta'}_i| \leq |\zeta'_i|$) 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 $Eq_{Oka}(\phi)$. Thus we have $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) = x) \in Eq_{Oka}(\phi)$, and we deduce $(f(\overline{\zeta}_1, \ldots, \overline{\zeta}_k) =_{E_{Oka}} x)\phi'$ by $\phi' \models Eq_{Oka}(\phi)$. Moreover, by induction hypothesis (since $|\overline{\zeta}_i| \leq |\zeta_i|$) 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 nor 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 $(\zeta_M =_{E_{Oka}} \zeta_N)\phi$ 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 converse): 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 4.2 we obtain $T \in sat_{Oka}(\phi)$, 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 $f_1(\zeta_1, \zeta_2, \zeta_3, \zeta_4) = f_1(\zeta'_1, \zeta'_2, \zeta'_3, \zeta'_4)$, with ζ_M is a term by decomposition and ζ_N is a term by composition. Let $M_i = \zeta_i\sigma\!\downarrow$ and $N_i = \zeta'_i\sigma\!\downarrow$.

Since $(\zeta_M =_{E_{Oka}} \zeta_N)\phi$, then we have $M_2 = f_1(N_1, N_2, N_3, M_1)$, $M_3 = N_3$, and $M_4 = N_4$. Moreover, by equational theory E_{Oka} 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 smaller than 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 4.2 we obtain $T \in sat_{Oka}(\phi)$, contradiction. Thus the interesting case is when the rule (4) is applied. So we rewrite $\zeta_M = \zeta_N$ in $f_1(\zeta_1, \zeta_2, \zeta_3, \zeta_4) = f_1(\zeta'_1, \zeta'_2, \zeta'_3, \zeta'_4)$. Let $M_i = \zeta_i\sigma\!\downarrow$ and $N_i = \zeta'_i\sigma\!\downarrow$.

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 E_{Oka} 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 $(\zeta_M =_{E_{Oka}} \zeta_N)\phi'$. □

Proposition 4.13. *Let $\phi = \nu\tilde{n}\sigma$ be a frame in normal form, $\zeta_M = decrypt(\zeta'_1, \zeta_2)$ and $\zeta_N = decrypt(rencrypt(\zeta'_1, \zeta'_2), \zeta_2)$ with ζ_2, ζ'_1 and ζ'_2 are the local recipes of $\zeta_2\sigma\!\downarrow, \zeta'_1\sigma\!\downarrow$ and $\zeta'_2\sigma\!\downarrow$ respectively. If we have $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$, then for every frame ϕ' such that $\phi' \models Eq_{Lee}(\phi)$, we have $(\zeta_M =_{E_{Lee}} \zeta_N)\phi'$.*

Proof. We proceed by induction on the sum of the sizes of ζ_M and ζ_N.
– **Base case:** If $|\zeta_M| \leq c_{E_{Lee}}$ and $|\zeta_N| \leq c_{E_{Lee}}$, then we have $(\zeta_M = \zeta_N) \in Eq_{Lee}(\phi)$. Thus we conclude form $\phi' \models Eq_{Lee}(\phi)$.

– **Inductive step:** We distinguish several cases according to ζ'_1:

- If ζ'_1 is a variable or $\zeta'_1\sigma\!\downarrow$ is obtained by a subterm rule, then by locality lemma we have $\zeta'_1\sigma\!\downarrow \in St_{Lee}(\phi)$. From Definition 4.2 we derive that $\zeta'_1\sigma\!\downarrow \in sat_{Lee}(\phi)$ and consequently $\zeta_2\sigma\!\downarrow \in sat_{Lee}(\phi)$ (because from the equality $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$ we have $\zeta_2\sigma\!\downarrow \in St_{Lee}(\zeta'_1\sigma\!\downarrow)$). Moreover since ζ'_2 is unconstrained in $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$, then we can replace ζ'_2 by a fresh name a and we get $(decrypt(rencrypt(\zeta'_1, a), \zeta_2) =_{E_{Lee}} decrypt(\zeta'_1, \zeta_2))\phi$, that belongs to $Eq_{Lee}(\phi)$. From $\phi' \models Eq_{Lee}(\phi)$, we have $(decrypt(rencrypt(\zeta'_1, a), \zeta_2) =_{E_{Lee}} decrypt(\zeta'_1, \zeta_2))\phi'$, and we conclude by replacing a by ζ'_2.
- If $\zeta'_1 = penc(\zeta''_1, \zeta''_2, \zeta''_3)$ with ζ''_i are the local recipes of $\zeta''_i\sigma\!\downarrow$. Then from the equality $(\zeta_M =_{E_{Lee}} \zeta_N)\phi$ we must have $(pk(\widehat{\zeta_2}) =_{E_{Lee}} \widehat{\zeta''}_2)\phi$. By Lemma 4.8, we get $(pk(\widehat{\zeta_2}) =_{E_{Lee}} \widehat{\zeta''}_2)\phi'$ (since $pk(\widehat{\zeta_2})$ is local because $pk(\widehat{\zeta_2}\sigma\!\downarrow)$ is irreducible). Then we conclude that $(\zeta_M =_{E_{Lee}} \zeta_N)\phi'$.
- If $\zeta'_1 = rencrypt(\zeta''_1, \zeta''_2)$. Then by E_{Lee} theory we have $(decrypt (rencrypt(\zeta''_1, \zeta''_2)) =_{E_{Lee}} decrypt(\zeta''_1, \zeta_2))\phi$. By induction hypothesis we get $(decrypt(rencrypt(\zeta''_1, \zeta''_2), \zeta_2) =_{E_{Lee}} decrypt(\zeta''_1, \zeta_2))\phi'$. Thus by E_{Lee} theory we derive that $(\zeta_M =_{E_{Lee}} \zeta_N)\phi'$. □

Proof of Lemma 4.9.

(1) Proof under $\mathbf{E_{Lee}}$: 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 $\zeta_M = f(\zeta_1, \ldots, \zeta_n)$. By 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 $(f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n) =_{E_{Lee}} \zeta_M)\phi'(0)$. We distinguish two cases:

Case 1: ζ_M is by composition. Then $f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n)$ is a local recipe of M (see the proof of the locality lemma). Thus we can choose $f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n)$ as a local recipe of M.

Case 2: $\zeta_M = f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n)$ is by decomposition. We distinguish several cases according to the applied rule:

• If the rule 4 is applied, then $f = rencrypt$. We have $rencrypt(\widehat{\zeta}_1, \widehat{\zeta}_2)$ is local (see the proof of the locality lemma). Then we can choose $rencrypt(\widehat{\zeta}_1, \widehat{\zeta}_2)$ as a local recipe of M since $(rencrypt(\widehat{\zeta}_1, \widehat{\zeta}_2) =_{E_{Lee}} rencrypt(\zeta_1, \zeta_2))\phi'$.

• If the rule 1 is applied, then $f = getpk$ and $n = 1$. Since ζ_M is by decomposition, *i.e.* $getpk(\widehat{\zeta}_1) \xrightarrow{h} M$, then $head(\widehat{\zeta}_1\sigma\!\downarrow) = host$. If $\widehat{\zeta}_1$ is a variable or $\widehat{\zeta}_1\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Lee}(\phi)$ and we conclude that $getpk(\widehat{\zeta}_1)$ is local. Then we choose $getpk(\widehat{\zeta}_1)$ as a local recipe of M. The rule 4 cannot be applied to get $\widehat{\zeta}_1\sigma\!\downarrow$ because $head(\widehat{\zeta}_1\sigma\!\downarrow) \neq host$. If $\widehat{\zeta}_1$ is by composition, then $\widehat{\zeta}_1 = host(\widehat{\zeta'}_1)$. By the E_{Lee} theory we get

$getpk(host(\widehat{\zeta'}_1)) =_{E_{Lee}} \widehat{\zeta'}_1$ (1). Then from equations (0) and (1) we can choose $\widehat{\zeta'}_1$ as a local recipe of M.

• If the rule 2 is applied, then $f = checksign$ and $n = 2$. Since ζ_M is by decomposition, *i.e.* $checksign(\widehat{\zeta}_1, \widehat{\zeta}_2) \xrightarrow{h} M$, then $head(\widehat{\zeta}_1\sigma\!\downarrow) = sign$ and $\widehat{\zeta}_2\sigma\!\downarrow \in St_{Lee}(\widehat{\zeta}_1\sigma\!\downarrow)$. If $\widehat{\zeta}_1$ is a variable or $\widehat{\zeta}_1\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Lee}(\phi)$ and we conclude that $\widehat{\zeta}_2\sigma\!\downarrow \in St_{Lee}(\phi)$. Thus $getpk(\widehat{\zeta}_1, \widehat{\zeta}_2)$ is local. Then we choose $getpk(\widehat{\zeta}_1, \widehat{\zeta}_2)$ as a local recipe of M. The rule 4 cannot be applied to get $\widehat{\zeta}_1\sigma\!\downarrow$ because $head(\widehat{\zeta}_1\sigma\!\downarrow) \neq sign$. If $\widehat{\zeta}_1$ is by composition, then $\widehat{\zeta}_1 = sign(\widehat{\zeta'}_1, \widehat{\zeta'}_2)$. Moreover, since rule 2 is applied, we must have $(pk(\widehat{\zeta'}_2) =_{E_{Lee}} \widehat{\zeta}_2)\phi$. By Lemma 4.8, we get $(pk(\widehat{\zeta'}_2) =_{E_{Lee}} \widehat{\zeta}_2)\phi'$ (since $pk(\widehat{\zeta'}_2)$ is local because $pk(\widehat{\zeta'}_2\sigma\!\downarrow)$ is irreducible). Thus we deduce $(checksign(sign(\widehat{\zeta'}_1, \widehat{\zeta'}_2), \widehat{\zeta}_2) =_{E_{Lee}} \widehat{\zeta'}_1)\phi'$ (2). Then from equations (0) and (2) we can choose $\widehat{\zeta'}_1$ as a local recipe of M.

• If the rule 3 is applied, then $f = decrypt$ and $n = 2$. Since ζ_M is by decomposition, *i.e.* $decrypt(\widehat{\zeta}_1, \widehat{\zeta}_2) \xrightarrow{h} M$, then $head(\widehat{\zeta}_1\sigma\!\downarrow) = penc$ and $\widehat{\zeta}_2\sigma\!\downarrow \in St_{Lee}(\widehat{\zeta}_1\sigma\!\downarrow)$. If $\widehat{\zeta}_1$ is a variable or $\widehat{\zeta}_1\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, we have $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Lee}(\phi)$ and we conclude that $\widehat{\zeta}_2\sigma\!\downarrow \in St_{Lee}(\phi)$. Thus $decrypt(\widehat{\zeta}_1, \widehat{\zeta}_2)$ is local. Then we choose $decrypt(\widehat{\zeta}_1, \widehat{\zeta}_2)$ as a local recipe of M. If rule 4 is applied, thus we have $\widehat{\zeta}_1 = rencrypt(\widehat{\zeta'}_1, \widehat{\zeta'}_2)$. By Proposition 4.13 we get $(decrypt(rencrypt(\widehat{\zeta'}_1, \widehat{\zeta'}_2), \widehat{\zeta}_2) =_{E_{Lee}} decrypt(\widehat{\zeta'}_1, \widehat{\zeta}_2))\phi'$ (3). Applying induction hypothesis on $decrypt(\widehat{\zeta'}_1, \widehat{\zeta}_2)$, we get that there exists a local recipe $\widehat{\zeta}_M$ such that $(decrypt(\widehat{\zeta'}_1, \widehat{\zeta}_2) =_{E_{Lee}} \widehat{\zeta}_M)\phi'$ (4). Then we conclude from equations (0), (3) and (4) that we can choose $\widehat{\zeta}_M$ as a local recipe of M. If $\widehat{\zeta}_1$ is by composition, then we have $\widehat{\zeta}_1 = penc(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3)$. Moreover, since rule 3 is applied, we must have $(\widehat{\zeta'}_2 =_{E_{Lee}} pk(\widehat{\zeta}_2))\phi$. By Lemma 4.8, we get $(\widehat{\zeta'}_2 =_{E_{Lee}} pk(\widehat{\zeta}_2))\phi'$ (since $pk(\widehat{\zeta}_2)$ is local because $pk(\widehat{\zeta}_2\sigma\!\downarrow)$ is irreducible). Thus we get $(decrypt(penc(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3), \widehat{\zeta}_2) =_{E_{Lee}} \widehat{\zeta'}_1)\phi'$ (5). Then form equations (0) and (5) we can choose $\widehat{\zeta'}_1$ as a local recipe of M.

• If the rule 5 or 6 is applied, then $f = checkdvp$, $n = 4$ and $M = ok$. Since ζ_M is by decomposition, *i.e.* $checkdvp(\widehat{\zeta}_1\sigma\!\downarrow, \ldots, \widehat{\zeta}_4\sigma\!\downarrow) \xrightarrow{h} M$, then $head(\widehat{\zeta}_1\sigma\!\downarrow) = dvp$ and $\widehat{\zeta}_i\sigma\!\downarrow \in St_{Lee}(\widehat{\zeta}_1\sigma\!\downarrow)$ for $i = 2 \ldots 4$. If $\widehat{\zeta}_1$ is a variable or $\widehat{\zeta}_1\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Lee}(\phi)$ and we derive that $\widehat{\zeta}_i\sigma\!\downarrow \in St_{Lee}(\phi)$ for $i = 2 \ldots 4$. Thus by Definition 4.2 we have $\widehat{\zeta}_i\sigma\!\downarrow \in sat_{Lee}(\phi)$ for $i = 1 \ldots 4$. Let $\overline{\zeta}_i$ be the local recipes of $\widehat{\zeta}_i\sigma\!\downarrow$ for $i = 1 \ldots 4$ used for the construction of the set $Eq_{Lee}(\phi)$. By Definition 4.6 we have $(checkdvp(\overline{\zeta}_1, \overline{\zeta}_2, \overline{\zeta}_3, \overline{\zeta}_4) = ok) \in Eq_{Lee}(\phi)$. Moreover, by Lemma 4.8, $(\widehat{\zeta}_i =_{E_{Lee}} \overline{\zeta}_i)\phi'$, thus $(checkdvp(\widehat{\zeta}_1, \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4) =_{E_{Lee}} checkdvp(\overline{\zeta}_1, \overline{\zeta}_2, \overline{\zeta}_3, \overline{\zeta}_4) =_{E_{Lee}} ok)\phi'$(6). Then from equations (0) and (6) we can choose ok as a local recipe of M. The rule 4 cannot be applied to get $\widehat{\zeta}_1\sigma\!\downarrow$ because $head(\widehat{\zeta}_1\sigma\!\downarrow) \neq dvp$.

If $\widehat{\zeta}_1$ is by composition, so $(checkdvp(dvp(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4), \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4) = ok)\phi$ with $(\widehat{\zeta'}_1 =_{E_{Lee}} \widehat{\zeta}_2)\phi$, $(\widehat{\zeta'}_2 =_{E_{Lee}} \widehat{\zeta}_3)\phi$ and $(\widehat{\zeta'}_4 =_{E_{Lee}} \widehat{\zeta}_4)\phi$. By Lemma 4.8 we have $(\widehat{\zeta'}_1 =_{E_{Lee}} \widehat{\zeta}_2)\phi'$, $(\widehat{\zeta'}_2 =_{E_{Lee}} \widehat{\zeta}_3)\phi'$ and $(\widehat{\zeta'}_4 =_{E_{Lee}} \widehat{\zeta}_4)\phi'$, thus we deduce $(checkdvp(dvp(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4), \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4) = ok)\phi'$ (6'). Then from equations (0) and (6') we can choose *ok* as a local recipe of M.

• If the rule 7 is applied, then $f = checkdvp$, $n = 4$ and $M = ok$. Since ζ_M is by decomposition, *i.e.* $checkdvp(\widehat{\zeta}_1\sigma\!\downarrow, \ldots, \widehat{\zeta}_4\sigma\!\downarrow) \xrightarrow{h} M$, then $head(\widehat{\zeta}_1\sigma\!\downarrow) = dvp$, $head(\widehat{\zeta}_4\sigma\!\downarrow) = pk$ and $\widehat{\zeta}_i\sigma\!\downarrow\, \in St_{Lee}(\widehat{\zeta}_1\sigma\!\downarrow)$ for $i = 2\ldots3$. If $\widehat{\zeta}_1$ is a variable or $\widehat{\zeta}_1\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, we have $\widehat{\zeta}_1\sigma\!\downarrow\, \in St_{Lee}(\phi)$ and we derive that $\widehat{\zeta}_i\sigma\!\downarrow\, \in St_{Lee}(\phi)$ for $i = 2\ldots3$. Thus by Definition 4.2 we have $\widehat{\zeta}_i\sigma\!\downarrow\, \in sat_{Lee}(\phi)$ for $i = 1\ldots3$. Let $\overline{\zeta}_i$ be the local recipes of $\widehat{\zeta}_i\sigma\!\downarrow$ for $i = 1\ldots4$ used for the construction of the set $Eq_{Lee}(\phi)$. Whatever $\zeta_4\sigma\!\downarrow\, \in sat_{Lee}(\phi)$ or not, we have by Definition 4.6, $(checkdvp(\overline{\zeta}_1, \overline{\zeta}_2, \overline{\zeta}_3, \overline{\zeta}_4) = ok) \in Eq_{Lee}(\phi)$, because if $\widehat{\zeta}_4\sigma\!\downarrow\, \notin sat_{Lee}(\phi)$, we know by Proposition 4.11, that $\widehat{\zeta}_4$ can be only of the from $pk(\widehat{\zeta'}_4)$ and since by the E_{Lee} theory we have $\widehat{\zeta'}_4\sigma\!\downarrow\, \in St_{Lee}(\widehat{\zeta}_1\sigma\!\downarrow)$, we deduce by Definition 4.2 that $\widehat{\zeta'}_4\sigma\!\downarrow\, \in sat_{Lee}(\phi)$ and as consequence we deduce that $(checkdvp(\overline{\zeta}_1, \overline{\zeta}_2, \overline{\zeta}_3, pk(\overline{\zeta'}_4)) = ok) \in Eq_{Lee}(\phi))$ with $\overline{\zeta'}_4$ is the local recipe of $\widehat{\zeta'}_4\sigma\!\downarrow$. Moreover, we deduce from Lemma 4.8 that $(\widehat{\zeta}_i =_{E_{Lee}} \overline{\zeta}_i)\phi'$. Thus $(checkdvp(\widehat{\zeta}_1, \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4) =_{E_{Lee}} checkdvp(\overline{\zeta}_1, \overline{\zeta}_2, \overline{\zeta}_3, \overline{\zeta}_4) =_{E_{Lee}} ok)\phi'$ (7). Then from equations (0) and (7) we can choose *ok* as a local recipe of $M = ok$. The rule 4 cannot be applied to get $\widehat{\zeta}_1\sigma\!\downarrow$ because $head(\widehat{\zeta}_1\sigma\!\downarrow) \neq dvp$.

If $\widehat{\zeta}_1$ is by composition, so $(checkdvp(dvp(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4), \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4) = ok)\phi$ with $(\widehat{\zeta'}_1 =_{E_{Lee}} \widehat{\zeta}_2)\phi$, $(\widehat{\zeta'}_2 =_{E_{Lee}} \widehat{\zeta}_3)\phi$ and $(pk(\widehat{\zeta'}_4) =_{E_{Lee}} \widehat{\zeta}_4)\phi$. By Lemma 4.8 we have $(\widehat{\zeta'}_1 =_{E_{Lee}} \widehat{\zeta}_2)\phi'$, $(\widehat{\zeta'}_2 =_{E_{Lee}} \widehat{\zeta}_3)\phi'$ and $(pk(\widehat{\zeta'}_4) =_{E_{Lee}} \widehat{\zeta}_4)\phi'$ (because $pk(\widehat{\zeta'}_4)$ is local since $pk(\widehat{\zeta'}_4\sigma\!\downarrow)$ is irreducible), thus we deduce that $(checkdvp(dvp(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4), \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4) = ok)\phi'$ (7'). Then from equations (0) and (7') we can choose *ok* as a local recipe of M.

(2) Proof under $\mathbf{E_{Oka}}$: 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:** Let $\zeta_M = f(\zeta_1, \ldots, \zeta_n)$. By 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 $=_{E_{Oka}}$ is closed by application of function symbol, then $(f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n) =_{E_{Oka}} \zeta_M)\phi'(0)$. We distinguish two cases:

Case 1: $\zeta_M = f(\zeta_1, \ldots, \zeta_n)$ is by composition. Then $f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n)$ is a local recipe of M (see the proof of the locality lemma). Thus we can choose $f(\widehat{\zeta}_1, \ldots, \widehat{\zeta}_n)$ as a local recipe of M.

Case 2: $\zeta_M = f(\zeta_1, \ldots, \zeta_n)$ is by decomposition. We distinguish several cases according to the the applied rule:

• If the rule 1 is applied, then $f = open$ and $n = 2$. Since ζ_M is by decomposition, *i.e.* $open(\widehat{\zeta}_1, \widehat{\zeta}_2) \xrightarrow{h} M$, then $head(\widehat{\zeta}_1\sigma\!\downarrow) = tdcommit$ and $\widehat{\zeta}_2\sigma\!\downarrow\, \in St_{Oka}(\widehat{\zeta}_1\sigma\!\downarrow)$. If $\widehat{\zeta}_1$ is a variable or $\widehat{\zeta}_1\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Lee}(\phi)$ and we deduce that $\widehat{\zeta}_2\sigma\!\downarrow \in St_{Lee}(\phi)$. Thus $open(\widehat{\zeta}_1, \widehat{\zeta}_2)$ is local. Then we can choose $open(\widehat{\zeta}_1, \widehat{\zeta}_2)$ as a local recipe of M. The rule 4 cannot be applied to get $\widehat{\zeta}_1\sigma\!\downarrow$ because $head(\widehat{\zeta}_1\sigma\!\downarrow) \neq tdcommit$. If $\widehat{\zeta}_1$ is by composition, then $\widehat{\zeta}_1 = tdcommit(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3)$. Moreover, since rule 1 is applied, we must have $(\widehat{\zeta'}_2 =_{E_{Oka}} \widehat{\zeta}_2)\phi$. By Lemma 4.8, we get $(\widehat{\zeta'}_2 =_{E_{Lee}} \widehat{\zeta}_2)\phi'$. Thus $(open(tdcommit(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3), \widehat{\zeta}_2) =_{E_{Oka}} \widehat{\zeta'}_1)\phi'$ (1). Then form equations (0) and (1) we can choose $\widehat{\zeta'}_1$ as a local recipe of M.

- If the rule 3 is applied, then $f = open$ and $n = 2$. Since ζ_M is by decomposition, *i.e.* $open(\widehat{\zeta}_1, \widehat{\zeta}_2) \xrightarrow{h} M$, then $head(\widehat{\zeta}_2\sigma\!\downarrow) = f_1$ and $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Oka}(\widehat{\zeta}_2\sigma\!\downarrow)$. If $\widehat{\zeta}_2$ is a variable or $\widehat{\zeta}_2\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, $\widehat{\zeta}_2\sigma\!\downarrow \in St_{Lee}(\phi)$ and we and we derive that $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Lee}(\phi)$. Thus $open(\widehat{\zeta}_1, \widehat{\zeta}_2)$ is local. Then we can choose $open(\widehat{\zeta}_1, \widehat{\zeta}_2)$ as a local recipe of M. The rule 2 cannot be applied to get $\widehat{\zeta}_2\sigma\!\downarrow$ because $head(\widehat{\zeta}_2\sigma\!\downarrow) \neq f_1$. If $\widehat{\zeta}_2$ is by composition with $head(\widehat{\zeta}_2) = f_1$ or by decomposition by applying the rule (4), then in the both cases we have $\widehat{\zeta}_2$ of the form $f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4)$, and $(open(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4)) =_{E_{Oka}} \widehat{\zeta'}_4)\phi$ (*). We wish to show that

$$(open(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4)) =_{E_{Oka}} \widehat{\zeta'}_4)\phi'. \qquad (2)$$

We distinguish two cases:

- If $\widehat{\zeta}_1$ is a variable or $\widehat{\zeta}_1\sigma\!\downarrow$ is obtained by applying a subterm rule, then by the locality lemma, $\widehat{\zeta}_1\sigma\!\downarrow \in St_{Oka}(\phi)$ and we derive that $\widehat{\zeta'}_i\sigma\!\downarrow \in St_{Oka}(\phi)$ for $i = 1, 2, 3$. By Definition 4.2 we get $\widehat{\zeta}_1\sigma\!\downarrow \in sat_{Oka}(\phi)$ and $\widehat{\zeta'}_i\sigma\!\downarrow \in sat_{Oka}(\phi)$ for $i = 1, 2, 3$. Since $\widehat{\zeta'}_4$ is unconstrained in the equation (*), then we can replace $\widehat{\zeta'}_4$ by a fresh name a and we get $(open(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, a)) =_{E_{Oka}} a)\phi$, that belongs to $Eq_{Oka}(\phi)$. Then from $\phi' \models Eq_{Oka}(\phi)$ we get $(open(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, a)) =_{E_{Oka}} a)\phi'$ and we derive that $(open(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4)) =_{E_{Oka}} \widehat{\zeta'}_4)\phi'$ (2).
- If $\widehat{\zeta}_1$ is by composition with $head(\widehat{\zeta}_2) = tdcommit$ or by decomposition by applying the rule (2), then in the both cases we have $\widehat{\zeta}_1$ of the form $tdcommit(\widehat{\zeta''}_1, \widehat{\zeta''}_2, \widehat{\zeta''}_3)$, with $(\widehat{\zeta''}_1 =_{E_{Oka}} \widehat{\zeta'}_1)\phi$ for $i = 1, 2, 3$. By Lemma 4.8 we get $(\widehat{\zeta''}_1 =_{E_{Oka}} \widehat{\zeta'}_1)\phi'$ for $i = 1, 2, 3$ and we derive that $(open(tdcommit(\widehat{\zeta''}_1, \widehat{\zeta''}_2, \widehat{\zeta''}_3), f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4)) =_{E_{Oka}} \widehat{\zeta'}_4)\phi'$ (2).

Then from equations (0) and (2) we can choose $\widehat{\zeta'}_4$ as a local recipe of M.

- If the applied rule is the rule (4), then $n = 4$ 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 a subterm rule, then by the locality lemma, $\widehat{\zeta}_2\sigma\!\downarrow \in St_{Oka}(\phi)$, and we derive that $\widehat{\zeta}_i\sigma\!\downarrow \in St_{Oka}(\phi, M)$ for $i = 1 \ldots 4$. Thus $f_1(\widehat{\zeta}_1, \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4)$ is local. Then we can choose $f_1(\widehat{\zeta}_1, \widehat{\zeta}_2, \widehat{\zeta}_3, \widehat{\zeta}_4)$ as a local recipe of M. The rule (2) cannot be applied to get $\widehat{\zeta}_2\sigma\!\downarrow$ because $head(\widehat{\zeta}_2\sigma\!\downarrow) \neq f_1$. If $\widehat{\zeta}_2$ is by composition with $head(\widehat{\zeta}_2) = f_1$ or by decomposition by applying the rule (4), then in both cases 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 4.8 we have $(\widehat{\zeta}_1 =_{E_{Oka}} \widehat{\zeta'}_4)\phi'$ and $(\widehat{\zeta}_3 =_{E_{Oka}} \widehat{\zeta'}_3)\phi'$, thus we deduce $(f_1(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4), \widehat{\zeta}_3, \widehat{\zeta}_4) =_{E_{Oka}} f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta}_4))\phi'(3)$.

Let $\zeta_T = f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta}_4)$. By induction hypothesis there exists a local recipe $\widehat{\zeta}_T$ of $(\widehat{\zeta}_T\sigma)\downarrow$ such that $(\zeta_T =_{E_{Oka}} \widehat{\zeta}_T)\phi'(4)$. Then we conclude from equations (0), (3) and (4) that $(\zeta_M =_{E_{Oka}} \widehat{\zeta}_T)\phi'$. Thus we can choose $\widehat{\zeta}_T$ as a local recipe of M.

• If the applied rule is the rule (2), then $n = 3$ and $f = \mathit{tdcommit}$. Since ζ_M is by decomposition, then $\mathit{head}(\widehat{\zeta}_2\sigma\downarrow) = f_1$ 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 a subterm rule, then by the locality lemma, $\widehat{\zeta}_2\sigma\downarrow \in St_{Oka}(\phi)$, and we derive that $\widehat{\zeta}_i\sigma\downarrow \in St_{Oka}(\phi) \subseteq St_{Oka}(\phi, M)$ for $i = 1 \ldots 3$, thus $\mathit{tdcommit}(\widehat{\zeta}_1, \widehat{\zeta}_2, \widehat{\zeta}_3)$ is local. Then we choose $\mathit{tdcommit}(\widehat{\zeta}_1, \widehat{\zeta}_2, \widehat{\zeta}_3)$ as a local recipe of M. The rule (2) cannot be applied to get $\widehat{\zeta}_2\sigma\downarrow$ because $\mathit{head}(\widehat{\zeta}_2\sigma\downarrow) \neq f_1$. If $\widehat{\zeta}_2$ is by composition with $\mathit{head}(\widehat{\zeta}_2) = f_1$ or by decomposition by applying the rule (4), then in both cases we have $\widehat{\zeta}_2$ of the form $f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4)$, thus $(\mathit{tdcommit}(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4), \widehat{\zeta}_3) =_{E_{Oka}} \mathit{tdcommit}(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3))\phi$ with $(\widehat{\zeta}_1 =_{E_{Oka}} \widehat{\zeta'}_4)\phi$ and $(\widehat{\zeta}_3 =_{E_{Oka}} \widehat{\zeta'}_3)\phi$. By Lemma 4.8 we have $(\widehat{\zeta}_1 =_{E_{Oka}} \widehat{\zeta'}_4)\phi'$ and $(\widehat{\zeta}_3 =_{E_{Oka}} \widehat{\zeta'}_3)\phi'$, thus we deduce $(\mathit{tdcommit}(\widehat{\zeta}_1, f_1(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3, \widehat{\zeta'}_4), \widehat{\zeta}_3) =_{E_{Oka}} \mathit{tdcommit}(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3))\phi'(5)$.

Let $\zeta_T = \mathit{tdcommit}(\widehat{\zeta'}_1, \widehat{\zeta'}_2, \widehat{\zeta'}_3)$. By induction hypothesis there exists a local recipe $\widehat{\zeta}_T$ of $(\widehat{\zeta}_T\sigma)\downarrow$ such that $(\zeta_T =_{E_{Oka}} \widehat{\zeta}_T)\phi'(6)$. Then we conclude from equations (0), (5) and (6) that $(\zeta_M = \widehat{\zeta}_T)\phi'$. Thus we can choose $\widehat{\zeta}_T$ as a local recipe of M. □

5. 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 [1] for convergent subterms theories and a special set of critical terms that we have introduced. For Okamoto theory we have also applied a modular approach by using the combining algorithm of [4], which allowed us to prove the decidability of deduction and static equivalence for a smaller theory.

It would also be interesting to implement our procedure, possibly by integrating our approach in existing tools such as YAPA [5] or KISS [9]. Indeed, none of the existing tools can currently handle the Lee theory, in particular due to the re-encryption primitives and to designated verifier proofs.

A further work is to generalize the construction of critical terms in order to cope with a wider class of equational theories. Indeed, it can be noticed that similar techniques are used in proofs both for the Lee *et al.* and the Okamoto theories. It seems natural to try to abstract these two proofs by identifying a more general argument, that would allow to cover more equational theories. Moreover, 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.

Acknowledgements. We are very grateful to Stéphanie Delaune for pointing us out the interest of e-voting theories and her very helpful suggestions in the proof of decidability for deduction.

References

[1] M. Abadi and V. Cortier, Deciding knowledge in security protocols under equational theories. *Theoret. Comput. Sci.* **367** (2006) 2–32.

[2] M. Abadi and C. Fournet, Mobile values, new names, and secure communication. *SIGPLAN Not.* **36** (2001) 104–115.

[3] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P.H. 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 *Proc. of the 17th International Conference on Computer Aided Verification, CAV'2005. Lect. Notes Comput. Sci.* **3576** (2005) 281–285.

[4] M. Arnaud, V. Cortier and S. Delaune, Combining algorithms for deciding knowledge in security protocols, in *Proc. of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'2007). Lect. Notes Comput. Sci.* **4720** (2007) 103–117.

[5] M. Baudet, V. Cortier and S. Delaune, YAPA: A generic tool for computing intruder knowledge, in *Proc. of the 20th International Conference on Rewriting Techniques and Applications (RTA'09). Lect. Notes Comput. Sci.* **5595** (2009) 148–163.

[6] B. Blanchet, An efficient cryptographic protocol verifier based on prolog rules, in *Proc. of the 14th Computer Security Foundations Workshop CSFW'01.* IEEE Computer Society Press (2001).

[7] D. Chaum, Blind signatures for untraceable payments, in *Proc. of the 8th Annual International Cryptology Conference (CRYPTO'82)* (1982) 199–203.

[8] Y. Chevalier, R. Kusters, M. Rusinowitch and M. Turuani, An NP decision procedure for protocol insecurity with XOR. *Theoret. Comput. Sci.* **338** (2005) 247–274.

[9] Ş. Ciobâcă, S. Delaune and S. Kremer, Computing knowledge in security protocols under convergent equational theories, in *Proc. of the 22nd International Conference on Automated Deduction (CADE'09)* (2009).

[10] H. Comon-Lundh and V. Shmatikov, Intruder deductions, constraint solving and insecurity decision in presence of exclusive or, in *Proc. of the 18th Annual IEEE Syposium on Logic in Computer Science (LICS-03).* IEEE Computer Society (2003) 271–280.

[11] V. Cortier and S. Delaune, Deciding knowledge in security protocols for monoidal equational theories, in *Proc. of the 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07). Lect. Notes Artif. Int.* **4790** (2007) 196–210.

[12] S. Delaune, Easy intruder deduction problems with homomorphisms. *Inform. Process. Lett.* **97** (2006) 213–218.

[13] S. Delaune, S. Kremer and M.D. Ryan, Verifying properties of electronic voting protocols, in *Proc. of the IAVoSS Workshop On Trustworthy Elections (WOTE'06)* (2006) 45–52.

[14] S. Delaune, S. Kremer and M.D. Ryan, Verifying privacy-type properties of electronic voting protocols. *J. Comput. Security* **17** (2009) 435–487.

[15] N. Dershowitz and D.A. Plaisted, Rewriting, in *Handbook of Automated Reasoning*. J.A. Robinson and A. Voronkov, Eds. Elsevier and MIT Press (2001) 535–610.

[16] D.E. Knuth and P.B. Bendix, Simple word problems in universal algebras, in *Computational Problems in Abstract Algebra*. J. Leech, Eds. Pergamon Press (1970) 263–297.

[17] P. Lafourcade, D. Lugiez and R. Treinen, Intruder deduction for AC-like equational theories with homomorphisms, in *Proc. of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*. Springer (2005).

[18] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, Providing receipt-freeness in mixnet-based voting protocols, in *Proc. of the 6th International Conference on Information Security and Cryptology (ICISC'03)*. Springer (2003).

[19] D.A. McAllester, Automatic recognition of tractability in inference relations. *J. ACM* **40** (1993) 284–303.

[20] T. Okamoto, An electronic voting scheme, in *Proc. of the 14th IFIP World Conference on IT Tools* (1996) 21–30.

[21] 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)*. IEEE Computer Society Press (2001) 174–190.

Communicated by Ch. Choffrut.
Received December 11, 2009. Accepted February 7, 2011.