Deciding knowledge in security protocols under (many more) equational theories

Martín Abadi
Computer Science Department, University of California at Santa Cruz, USA

Véronique Cortier
Loria, INRIA & CNRS, Nancy, France

Abstract

In the analysis of security protocols, the knowledge of attackers is often described in terms of message deducibility and indistinguishability relations. In this paper, we pursue the study of these two relations. We establish general decidability theorems for both. These theorems require only loose, abstract conditions on the equational theory for messages. They subsume previous results for a syntactically defined class of theories that allows basic equations for functions such as encryption, decryption, and digital signatures. They also apply to many other useful theories, for example with blind digital signatures, homomorphic encryption, XOR, and other associative-commutative functions.

1 Introduction

The design and analysis of security protocols typically relies on reasoning about the knowledge of honest protocol participants and attackers. In formal approaches, two main kinds of definitions have been given for this knowledge.

- Many formal methods define knowledge in terms of deduction (e.g., [12, 16, 17, 20]).

  Given some messages ϕ and another message M, one asks whether M can be computed ("deduced") from ϕ. For example, whether an attacker can obtain a session key from a set of messages and some prior knowledge can be cast as a deduction problem.

- Some formal methods complement deduction with an indistinguishability equivalence relation (e.g., [2, 3]). Indistinguishability is also prominent in computational approaches to cryptography (e.g., [11, 15]).

  Given two lists of messages ϕ and ψ, one asks whether they can be distinguished. For example, ϕ and ψ may be transcripts of the messages for two sessions of a protocol, each with a different value for a parameter, and then the equivalence would express that the value of this parameter is not revealed by session transcripts. The choice of this value may remain secret even though an attacker may be able to compute every possible value for the parameter—as would be the case if the parameter is a boolean or a password drawn from a small dictionary.

In both cases, messages are represented by formal expressions, and correspondingly the computations allowed are "black-box" symbolic manipulations on those expressions. These symbolic manipulations are sometimes as powerful as probabilistic polynomial-time computations on bitstrings (e.g., [4]). In both cases, too, the definitions concern observations on messages at a particular point in time. Accordingly, the equivalence relation is sometimes called static equivalence, and the deduction relation should perhaps be called static deduction. Despite the static character of these relations, they are useful in analyzing the dynamics of protocols and attacks. In particular, proof methods for safety properties often rely on deduction, and process equivalences can be reduced to static equivalences plus standard bisimulation conditions.

In this paper we pursue the study of deduction and static equivalence. Both of these relations depend on the underlying equational theory that governs the function symbols that appear in expressions, in particular function symbols that represent cryptographic operations. Our goal is to obtain characterizations and decidability results that hold for a wide class of equational theories. We aim to support the standard uses of function symbols for representing encryption, digital signatures, and the like. We also aim to allow some elaborate features of particular schemes, such as blinding for digital signatures. Finally, we aim to support associativity and commutativity properties, in particular for the XOR (exclusive or) operation.

Several of the equational theories that we treat are important in applications. Therefore, deduction and (to a lesser extent) static equivalence under some of these theories have already played a role in the context of various frameworks and tools for protocol analysis (e.g., [2, 20]). However, usually, special techniques are developed for each particular case.

Only a few general decidability results appear in the literature. In a recent paper [1], we have shown that deduction and static equivalence are decidable in PTIME for a syntactically defined class of equational theories, the convergent subterm theories. These theories allow basic equations for functions such as encryption, decryption, and digital signatures. Noting that deduction and static equivalence are undecidable for some other equational theories, we have also shown that static equivalence can be undecidable even when deduction is not. Comon-Lundh and Treinen [9] have studied the decidability of deduction for a class of equational theories incomparable with ours. Their work, and all the work cited below, considers only deduction and not static equivalence unless otherwise noted. Delaune and Jacquemard [10] have shown that deduction is decidable for a subclass of convergent subterm theories, also considering active attacks. (Section 6 mentions other, ongoing related work that addresses active attackers.) None of these previous results allows associativity and commutativity properties. In fact, even results on specific theories with AC (associative-commutative) functions are rare. Three important exceptions are decidability results for deduction with XOR [6, 8], in an Abelian group [8], and under certain "AC-like" theories with homomorphisms [14].

Thus, prior work typically relies on syntactic restrictions on equational theories, focusing on one particular theory at a time or on syntactically defined classes of theories. In this paper, we adopt a different perspective: we assume only loose, abstract conditions on the underlying equational theories. In this respect, we are inspired by Comon-Lundh's current investigations [7] (discussed further in Section 6).

Under those assumptions, we establish general decidability theorems for both deduction and static equivalence. These theorems subsume the previous ones for convergent subterm theories. They also apply to many other useful theories, for example with blind digital signatures, homomorphic encryption, XOR, and other AC functions. Several of the decidability results that we obtain are new.

Checking that a particular theory satisfies the hypotheses of our theorems may involve some work, though often less than direct proofs of decidability. In some cases, it may also involve some (fairly elementary and pleasant) mathematics, such as facts on $\mathbb{Z}$-modules. We expect that some of the techniques that we employ in our examples may be reused in the study of other theories.

The next section, Section 2, introduces notations and definitions. In Section 3, we present the hypotheses of our theorems. We give some examples of theories that satisfy these hypotheses in Section 4. We prove the theorems in Section 5. Finally, we conclude in Section 6.

2 Basic definitions

Next we review definitions from previous work, particularly from the applied pi calculus [2]. Much of the material in this section is borrowed or adapted from previous work. In Section 2.1 we give the syntax of expressions. In Section 2.2 we explain a representation for the information available to an observer who has seen messages exchanged in the course of a protocol execution. In Sections 2.3 and 2.4 we present the relations $\vdash$ and $\approx_s$, which provide the two formalizations of the knowledge that the observer has on the basis of that information.

2.1 Syntax

A *signature* Σ consists of a finite set of function symbols, such as enc and pair, each with an arity. Let $\mathsf{ar}(\Sigma)$ be the maximal arity of a function symbol in Σ. 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
$\quad k, \ldots, n, \ldots, s$	name
$\quad x, y, z$	variable
$\quad f(M_1, \ldots, M_l)$	function application

where f ranges over the function symbols of Σ and l matches the arity of f. Although names, variables, and constant symbols have similarities, we find it clearer to keep them separate. A term is closed when it does not have free variables (but it may contain names and constant symbols). We write $fn(M)$ for the set of names that occur in the term M. We use meta-variables u, v, w to range over names and variables. The *size* $|T|$ of a term T is defined by $|u| = 1$ and $|f(T_1, \ldots, T_l)| = 1 + \sum_{i=1}^{l} |T_i|$. We write $\mathsf{st}(T)$ for the set of subterms of T.

We equip the signature Σ with an equational theory E, that is, an equivalence relation on terms that is closed under substitutions of terms for variables or names and closed under application of contexts. We write $M =_E N$ when M and N are closed terms and the equation $M = N$ is in E. We use the symbol $==$ to denote syntactic equality of closed terms. As in these definitions, we often focus on closed terms for simplicity.

2.2 Assembling terms into frames

After a protocol execution, an attacker may know a sequence of messages $M_1, \ldots, M_l$. This means that it knows each message but it also knows in which order it received the messages. So it is not enough for us to say that the attacker knows the set of terms $\{M_1, \ldots, M_l\}$. Furthermore, we should distinguish the names that the attacker had before the execution from those that were freshly generated and which may remain secret from the attacker; both kinds of names may appear in the terms.

Such a sequence of messages can be organized into a *frame* $\nu\widetilde{n}\sigma$, where $\widetilde{n}$ is a finite set of names (intuitively, the fresh names), and σ is a substitution of the form:

$$\{{}^{M_1}/_{x_1}, \ldots, {}^{M_l}/_{x_l}\} \quad \text{with} \quad dom(\sigma) \stackrel{\text{def}}{=} \{x_1, \ldots, x_l\}$$

The variables enable us to refer to each M_i, for example for keeping track of their order of transmission. We always assume that the terms M_i are closed. The size of a frame $\phi = \nu\widetilde{n}\{{}^{M_1}/_{x_1}, \ldots, {}^{M_l}/_{x_l}\}$ is $|\phi| \stackrel{\text{def}}{=} \sum_{i=1}^{l} |M_i|$. The set $fn(\phi)$ of free names of ϕ consists of the free names of the M_i that are not in $\widetilde{n}$.

2.3 Deduction

Given 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 $\phi \vdash M$ (following Schneider [20]). It is axiomatized by the rules:

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

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

Intuitively, the deducible messages are the terms of ϕ and the names that are not protected in ϕ, closed by equality in E and closed by application of functions.

We have the following characterization of deduction [1]:

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

Example 1 *As a first example, we consider the theory of an encryption scheme that has an homomorphism property. This property is simply that the encryption of a pair is the pair of the encryptions; the literature (e.g., [18]) suggests other homomorphism properties. This property is modeled by the equation:*

$$\mathsf{enc}(\langle x, y\rangle, z) = \langle \mathsf{enc}(x, z), \mathsf{enc}(y, z)\rangle$$

We also assume an analogous equation for decryption:

$$\mathsf{dec}(\langle x, y\rangle, z) = \langle \mathsf{dec}(x, z), \mathsf{dec}(y, z)\rangle$$

As usual, we write $\langle x, y\rangle$ instead of $\mathsf{pair}(x, y)$. The signature Σ_1 is $\{\mathsf{pair}, \mathsf{enc}, \mathsf{fst}, \mathsf{snd}, \mathsf{dec}\}$, and the theory E_1 is defined by the axioms:

$$\begin{array}{rcl}
\mathsf{enc}(\langle x, y\rangle, z) & = & \langle \mathsf{enc}(x, z), \mathsf{enc}(y, z)\rangle \\
\mathsf{dec}(\langle x, y\rangle, z) & = & \langle \mathsf{dec}(x, z), \mathsf{dec}(y, z)\rangle \\
\mathsf{fst}(\langle x, y\rangle) & = & x \\
\mathsf{snd}(\langle x, y\rangle) & = & y \\
\mathsf{dec}(\mathsf{enc}(x, y), y) & = & x
\end{array}$$

Suppose for example that the attacker listens to two messages: $\mathsf{enc}(\langle n_1, n_2\rangle, k)$ and $\mathsf{enc}(n_3, \mathsf{enc}(n_1, k))$. Since $\mathsf{enc}(\langle n_1, n_2\rangle, k) =_{E_1} \langle \mathsf{enc}(n_1, k), \mathsf{enc}(n_2, k)\rangle$, the corresponding frame can be written

$$\begin{array}{rcl}
\phi_1 & = & \nu(n_1, n_2, n_3, k) \\
& & \{\langle \mathsf{enc}(n_1, k), \mathsf{enc}(n_2, k)\rangle / x_1, \\
& & \ \mathsf{enc}(n_3, \mathsf{enc}(n_1, k)) / x_2\}
\end{array}$$

Then $\phi_1 \vdash \mathsf{enc}(n_1, k)$, $\phi_1 \vdash \mathsf{enc}(n_2, k)$, and $\phi_1 \vdash n_3$. Furthermore, $\mathsf{enc}(n_1, k) =_{E_1} \mathsf{fst}(x_1)\phi$, $\mathsf{enc}(n_2, k) =_{E_1} \mathsf{snd}(x_1)\phi$, and $n_3 =_{E_1} \mathsf{dec}(x_2, \mathsf{fst}(x_1))\phi$.

2.4 Static equivalence

Given two frames ϕ and ψ that represent the information available to an attacker in two “possible worlds” (e.g., two different runs of a protocol), we may ask whether the attacker may distinguish ϕ and ψ, more precisely whether the attacker may differentiate ϕ and ψ by applying them (roughly) as substitutions and obtaining observably different results. This scenario motivates the following definitions.

We say that two terms M and N are equal in the frame φ for the equational theory E, and write $(M =_E N)\varphi$, if and only if $\varphi = \nu\widetilde{n}\sigma$, $M\sigma =_E N\sigma$, 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 $\varphi \approx_s \psi$, when $dom(\varphi) = dom(\psi)$ and when, for all terms M and N, we have $(M =_E N)\varphi$ if and only if $(M =_E N)\psi$.

Example 2 *Let $\phi_1 \stackrel{def}{=} \nu k\{k/y, \mathsf{enc}(n_1, k)/z\}$ and $\phi_2 \stackrel{def}{=} \nu k\{k/y, \mathsf{enc}(n_2, k)/z\}$, where k, n_1, and n_2 are distinct names. Using the equation $\mathsf{dec}(\mathsf{enc}(x, y), y) = x$, the attacker can tell the difference between these two frames by checking whether the decryption of z with y produces n_1. In other words, we have $(\mathsf{dec}(z, y) =_{E_1} n_1)\phi_1$ but not $(\mathsf{dec}(z, y) =_{E_1} n_1)\phi_2$. Therefore, $\phi_1 \not\approx_s \phi_2$.*

Example 3 *Let $\phi_1 \stackrel{def}{=} \nu\widetilde{n}\{M/x_1, M/x_2, N/x_3\}$ and $\phi_2 \stackrel{def}{=} \nu\widetilde{n}\{M/x_1, N/x_2, M/x_3\}$. In general, these frames are not statically equivalent, since x_1 and x_2 are always equal in the frame ϕ_1 but not in the frame ϕ_2. On the other hand, the* *same terms can be deduced from these two frames. As this example illustrates, the association of terms with variables affects static equivalence but not deduction.*

3 The hypotheses

We establish decidability results for equational theories that satisfy three properties. The purpose of this section is to define and start to explain these three properties; Section 4 explains them further through examples.

3.1 AC-convergence

Our first hypothesis is an adaptation of the standard notion of convergence for theories with AC symbols.

Let E an equational theory, and let $\oplus_1, \ldots, \oplus_k$ be the binary functional symbols such that the equations $x \oplus_i (y \oplus_i z) = (x \oplus_i y) \oplus_i z$ (associativity) and $x \oplus_i y = y \oplus_i x$ (commutativity) are in E.

For two terms U and V, we write $U =_{\mathsf{AC}} V$ if U and V are equal in the theory induced by the equations $x \oplus_i (y \oplus_i z) = (x \oplus_i y) \oplus_i z$ and $x \oplus_i y = y \oplus_i x$ for $1 \leq i \leq k$. When this theory is empty (because we have no AC symbols), $=_{\mathsf{AC}}$ is simply syntactic equality.

When $\mathcal{R}$ is a rewriting system, we write $U \rightarrow_{\mathsf{AC}} V$ if there exists W such that $U =_{\mathsf{AC}} W$ and $W \rightarrow V$. The relation $\rightarrow^*_{\mathsf{AC}}$ denotes the reflexive and transitive closure of $\rightarrow_{\mathsf{AC}}$.

Definition 1 (AC-convergent) *An equational theory E is* AC-convergent *if there exists a finite rewriting system $\mathcal{R}$ such that:*

- *$\mathcal{R}$ is* AC-terminating, *that is, for every closed term U, there is no infinite sequence $U \rightarrow_{\mathsf{AC}} U_1 \rightarrow_{\mathsf{AC}} \cdots U_k \rightarrow_{\mathsf{AC}} \cdots$.*

  For every term U, the set of normal forms $U\!\downarrow$ (closed modulo AC) of U is the set of terms V such that $U \rightarrow^*_{\mathsf{AC}} V$ and V has no successor for $\rightarrow_{\mathsf{AC}}$.

- *$\mathcal{R}$ is* AC-confluent, *that is, for every closed terms U, U_1, and U_2 such that $U \rightarrow_{\mathsf{AC}} U_1$ and $U \rightarrow_{\mathsf{AC}} U_2$, there exist V_1 and V_2 such that $U_1 \rightarrow^*_{\mathsf{AC}} V_1$, $U_2 \rightarrow^*_{\mathsf{AC}} V_2$, and $V_1 =_{\mathsf{AC}} V_2$.*

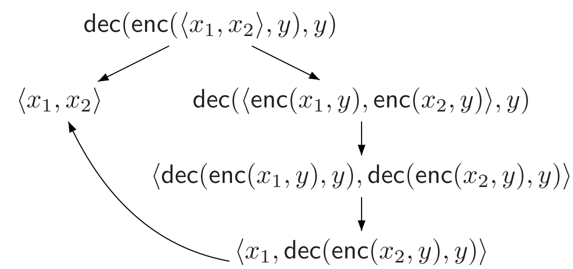
- *For all closed terms U and V, the equality $U =_E V$ holds if and only if there exists a term $T \in (U\!\downarrow \cap V\!\downarrow)$.*

By AC-convergence, the set $U\!\downarrow$ is always finite and for all $V, W \in U\!\downarrow$, the equality $V =_{\mathsf{AC}} W$ holds. AC-convergence immediately implies the decidability of equations on closed terms.

In what follows, E is an AC-convergent equational theory and $\mathcal{R}$ is a rewriting system associated with E that satisfies the conditions of Definition 1. If $\mathcal{R}$ consists of a finite set of rules $\bigcup_{i=1}^{k} \{M_i \rightarrow N_i\}$, the size c_E of the theory E is defined as $c_E = \max_{1 \leq i \leq k}(|M_i|, |N_i|, \mathsf{ar}(\Sigma) + 1)$. As a special case, $c_E = \mathsf{ar}(\Sigma) + 1$ when $\mathcal{R}$ is empty.

Note that E need not have AC symbols. A theory defined by a convergent rewriting system without AC symbol is of course an AC-convergent theory. In that case, we may simply say that the theory is convergent.

Example 4 *Let us consider again the theory E_1 of an encryption scheme with a homomorphism property. We consider the rewriting system $\mathcal{R}_1$ obtained from E_1 by orienting the equations from left to right. With this choice of $\mathcal{R}_1$, the theory E_1 is convergent. Indeed, the only critical pair is joinable.*



Example 5 *The theory of XOR is also AC-convergent. The XOR operator is represented by the $\oplus$ function symbol, with the following properties:*

$$E_2 = \left\{ \begin{array}{rcl} x \oplus (y \oplus z) & = & (x \oplus y) \oplus z \\ x \oplus y & = & y \oplus x \\ x \oplus x & = & 0 \\ x \oplus 0 & = & x \end{array} \right\}$$

where 0 is a constant symbol and the signature Σ_2 is $\{0, \oplus\}$. We associate to E_2 the rewriting system $\mathcal{R}_2$:

$$\mathcal{R}_2 = \left\{ \begin{array}{rcl} x \oplus x & \rightarrow & 0 \\ x \oplus 0 & \rightarrow & x \end{array} \right\}$$

Using this choice of $\mathcal{R}_2$, it is easy to verify that E_2 is AC-convergent.

3.2 Local stability

Our second hypothesis roughly says that, for every frame, there is a finite set of terms deducible from the frame that satisfies certain closure conditions. Stating this hypotheses precisely requires a few auxiliary definitions and notations.

Assume that there exists some rule $M_0 \rightarrow N_0$ of the rewriting system $\mathcal{R}$ and some substitution θ such that either there exists a term U_1 such that $U =_{\mathsf{AC}} U_1$, $U_1 = M_0\theta$, and $V = N_0\theta$, or there exist terms U_1 and U_2 such that $U =_{\mathsf{AC}} U_1 \oplus U_2$ for some AC symbol $\oplus$, $U_1 = M_0\theta$, and $V =_{\mathsf{AC}} N_0\theta \oplus U_2$. Then we say that the reduction $U \rightarrow V$ occurs in head, and we write $U \xrightarrow{h} V$.

We write $\alpha \cdot_\oplus M$ for the term $M \oplus \cdots \oplus M$, α times (for $\alpha \in \mathbb{N}^*$). We simply write αM when the AC symbol is clear from the context. Given a set of terms S and a set of names $\widetilde{n}$, we write $\mathsf{sum}_\oplus(S, \widetilde{n})$ for the set of arbitrary sums of terms of S and other names, closed modulo AC-rewriting:

$$\mathsf{sum}_\oplus(S, \widetilde{n}) \stackrel{\text{def}}{=} \left\{ \begin{array}{c|l} (\alpha_1 \cdot_\oplus T_1) \oplus \cdots \oplus (\alpha_n \cdot_\oplus T_n) & \alpha_i, \beta_i \in \mathbb{N}^*, \\ \oplus & n_i \notin \widetilde{n}, \\ (\beta_1 \cdot_\oplus n_1) \oplus \cdots \oplus (\beta_k \cdot_\oplus n_k) & T_i \in S \end{array} \right\}$$

Typically, the names in $\widetilde{n}$ will be private, and the others public. Then we define $\mathsf{sum}(S, \widetilde{n})$ as the union of the $\mathsf{sum}_\oplus(S, \widetilde{n})$ for any AC symbol $\oplus$ of the theory.

In our previous paper [1], the main step of the proof of the decidability of $\vdash$ and $\approx_s$ for convergent subterm theories was the existence, for each frame ϕ, of a set $\mathsf{sat}(\phi)$ stable by application of "small" contexts. We generalize this condition by requiring that the application of a rewriting rule to a "small" context C applied to arbitrary sums of terms in $\mathsf{sat}(\phi)$ is again a "small" context C' applied to sums of terms in $\mathsf{sat}(\phi)$. The definition of "small" is partly arbitrary; we bound the size of C by c_E and the size of C' by ${c_E}^2$, but other finite size bounds may be suitable.

Definition 2 (locally stable) *An AC-convergent equational theory E is* locally stable *if, for every frame $\phi = \nu\widetilde{n}\{M_1/x_1, \ldots, M_k/x_k\}$, where the terms M_i are closed and in normal form, there exists a finite (computable) set $\mathsf{sat}(\phi)$, closed modulo AC, such that*

1. *for every $1 \leq i \leq k$, $M_i \in \mathsf{sat}(\phi)$, and for every $n \in fn(\phi)$, $n \in \mathsf{sat}(\phi)$,*
2. *if $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and $f(M_1, \ldots, M_k) \in \mathsf{st}(\mathsf{sat}(\phi))$, then $f(M_1, \ldots, M_k) \in \mathsf{sat}(\phi)$,*
3. *if $C[S_1, \ldots, S_l] \xrightarrow{h} M$, where C is a context such that $|C| \leq c_E$ and $fn(C) \cap \widetilde{n} = \emptyset$, and where $S_1, \ldots, S_l \in \mathsf{sum}_\oplus(\mathsf{sat}(\phi), \widetilde{n})$ for some AC symbol $\oplus$ (or $S_i \in \mathsf{sat}(\phi)$ if there is no AC symbol), then there exist a context C', a term M', and $S'_1, \ldots, S'_k \in \mathsf{sum}_\oplus(\mathsf{sat}(\phi), \widetilde{n})$ (or $S'_1, \ldots, S'_k \in \mathsf{sat}(\phi)$ if there is no AC symbol), such that $|C'| \leq c_E^2$, $fn(C') \cap \widetilde{n} = \emptyset$, and $M \to^*_{\mathsf{AC}} M' =_{\mathsf{AC}} C'[S'_1, \ldots, S'_k]$,*
4. *if $M \in \mathsf{sat}(\phi)$ then $\phi \vdash M$.*

The set $\mathsf{sat}(\phi)$ need not be unique, nor minimal. Any set that satisfies the four conditions is adequate for our present purposes.

Example 6 *For the equational theory E_1 of Example 1, given a frame ϕ in normal form, the set $\mathsf{sat}(\phi)$ is simply obtained by adding subterms of ϕ deducible from ϕ. For example, the deducible subterms of the frame ϕ_1 of Example 1 are $\mathsf{enc}(n_1, k)$, $\mathsf{enc}(n_2, k)$, and n_3, so $\mathsf{sat}(\phi_1)$ is the set*

$$\{\langle \mathsf{enc}(n_1, k), \mathsf{enc}(n_2, k)\rangle, \mathsf{enc}(n_3, \mathsf{enc}(n_1, k)), \mathsf{enc}(n_1, k), \mathsf{enc}(n_2, k), n_3\}$$

In Section 4.2 we prove that this construction satisfies the requirements.

In general, establishing that an equational theory is locally stable may be difficult. We give other examples of locally stable theories in Section 4.

3.3 Local finiteness and local decidability

For our third hypothesis, we consider a certain set of "small" equations that a frame satisfies. One of our results says that this set characterizes the frame. The third hypothesis, which this section presents, pertains to deciding whether another frame satisfies this set. In fact, this section discusses two versions of the third hypothesis, called local finiteness and local decidability. Either is sufficient for our purposes; the former has been more attractive in applications; the latter is more general. As the use of equations may suggest, we rely on the third hypothesis in the study of static equivalence but not deduction.

For each frame $\phi = \nu\widetilde{n}\sigma$, we assume a fixed set of terms $\mathcal{R}(\phi) = \{\zeta_M \mid M \in \mathsf{sat}(\phi)\}$ such that for each ζ_M, $fn(\zeta_M) \cap \widetilde{n} = \emptyset$ and $\zeta_M\sigma =_E M$. Intuitively, the term ζ_M explains how M may be obtained from the terms of ϕ. Since all the terms of $\mathsf{sat}(\phi)$ are deducible, such a set exists by Proposition 1. For instance, for Example 6, the terms associated with $\mathsf{enc}(n_1, k)$, $\mathsf{enc}(n_2, k)$, and n_3 are respectively $\zeta_{\mathsf{enc}(n_1,k)} = \mathsf{fst}(x_1)$, $\zeta_{\mathsf{enc}(n_2,k)} = \mathsf{snd}(x_1)$, and $\zeta_{n_3} = \mathsf{dec}(x_2, \mathsf{fst}(x_1))$.

With each frame ϕ, we associate a set of "small" equations $\mathsf{Eq}(\phi)$ such that two frames are equivalent if and only if they satisfy the equations of each other's set (see Proposition 7).

Definition 3 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame in normal form. The set $\mathsf{Eq}(\phi)$ is the set of equations of the form*

$$C_1[\chi_1, \ldots, \chi_k] = C_2[\chi'_1, \ldots, \chi'_l]$$

where $(C_1[\chi_1, \ldots, \chi_k] =_E C_2[\chi'_1, \ldots, \chi'_l])\phi$, $(fn(C_1) \cup fn(C_2)) \cap \widetilde{n} = \emptyset$, $|C_1| \leq c_E$, $|C_2| \leq c_E^2$, and the χ_i and χ'_i are in the set $\mathsf{sum}_\oplus(\mathcal{R}(\phi), \widetilde{n})$ for some AC symbol $\oplus$ (or χ_i and χ'_i are in $\mathcal{R}(\phi)$ if there is no AC symbol).

When ϕ and ψ are frames and $(M =_E N)\psi$ for every $(M = N) \in \mathsf{Eq}(\phi)$, we say that ψ satisfies the equations of $\mathsf{Eq}(\phi)$, and write $\psi \models \mathsf{Eq}(\phi)$.

Definition 4 (locally decidable) *A locally stable equational theory is* locally decidable *if the question of whether* $\psi \models \mathsf{Eq}(\phi)$*, for frames* ϕ *and* ψ*, is decidable.*

The set $\mathsf{Eq}(\phi)$ may in general be infinite since the χ_i may be of arbitrary size. Local finiteness means that the set $\mathsf{Eq}(\phi)$ is always equivalent to a finite set of equations.

Definition 5 (locally finite) *A locally stable equational theory is* locally finite *if, for every frame* ϕ*, there exists a finite (computable) set of equations* $\mathsf{Eq}'(\phi)$ *such that, for every frame* ψ*:*

$$\psi \models \mathsf{Eq}(\phi) \quad \textit{if and only if} \quad \psi \models \mathsf{Eq}'(\phi)$$

This property suffices for local decidability:

Proposition 2 *Every locally finite equational theory is locally decidable.*

Local finiteness is always true when there are no AC symbols since then the set $\mathsf{Eq}(\phi)$ contains only finitely many equations up to renaming:

Proposition 3 *Let* E *be a locally stable equational theory with no AC symbols. Then, for any frame* ϕ*, there exists a finite set of equations* $\mathsf{Eq}'(\phi)$ *such that for every frame* ψ*, we have* $\psi \models \mathsf{Eq}(\phi)$ *if and only if* $\psi \models \mathsf{Eq}'(\phi)$*. In other words,* E *is locally finite.*

Each equation of $\mathsf{Eq}(\phi)$ is of the form $C_1[\chi_1, \ldots, \chi_k] = C_2[\chi'_1, \ldots, \chi'_l]$ with χ_i, χ'_i in $\mathcal{R}(\phi)$. Thus it contains a finite number of names (bounded by $c_E + c_E^2$). The set $\mathsf{Eq}'(\phi)$ is obtained from $\mathsf{Eq}(\phi)$ by renaming the names on a fixed set of names.

In Section 4 we present some non-trivial examples of locally finite theories with AC symbols. Establishing local finiteness is our preferred way of proving local decidability for such theories. Here we show that at least an (infinite) subset of $\mathsf{Eq}(\phi)$ may always be replaced by a finite number of equations.

Definition 6 *Let* $\phi = \nu\widetilde{n}\sigma$ *be a frame. Let* N *be a set of public names (that is, such that* $N \cap \widetilde{n} = \emptyset$*). We write* $\mathsf{Eq}_{\oplus}(\phi, N)$ *for the set of equations of the form* $\chi_1 = \chi_2$ *such that* $\chi_1, \chi_2 \in \mathsf{sum}_{\oplus}(\mathcal{R}(\phi), \widetilde{n})$*,* $fn(\chi_1) \cup fn(\chi_2) \subseteq N$*, and* $(\chi_1 =_E \chi_2)\phi$*.*

Note that $\mathsf{Eq}_{\oplus}(\phi, N)$ is a subset of $\mathsf{Eq}(\phi)$. We show that the set $\mathsf{Eq}_{\oplus}(\phi, N)$ may always be replaced by a finite number of equations if N is a finite set of public names.

Proposition 4 *Let* $\phi = \nu\widetilde{n}\sigma$ *be a frame and* N *a finite set of names such that* $N \cap \widetilde{n} = \emptyset$*. There exists a finite set* $\mathsf{Eq}_{b\oplus}(\phi, N) \subseteq \mathsf{Eq}_{\oplus}(\phi, N)$*, such that for every frame* ψ*:*

$$\psi \models \mathsf{Eq}_{\oplus}(\phi, N) \quad \textit{if and only if} \quad \psi \models \mathsf{Eq}_{b\oplus}(\phi, N)$$

In addition, the cardinality of $\mathsf{Eq}_{b\oplus}(\phi)$ *is at most the cardinality of* $\mathsf{sat}(\phi)$ *plus the cardinality of* N*.*

This proposition can be proved using elementary results on $\mathbb{Z}$-modules. (Facts on $\mathbb{Z}$-module may be found in [19], for example.) Assume that $\mathsf{sat}(\phi) = \{M_1, \ldots, M_k\}$, $N = \{n_1, \ldots, n_l\}$, and let $\Gamma \in \mathbb{Z}^{k+l}$. For $1 \leq i \leq k+l$, Γ_i denotes the ith coefficient of Γ, and $\widehat{\Gamma}$ denotes the equation:

$$\begin{aligned} &\bigoplus_{\Gamma_i > 0, i \leq k} \Gamma_i \zeta_{M_i} \oplus \bigoplus_{\Gamma_i > 0, i > k} \Gamma_i n_i \\ &\qquad = \bigoplus_{\Gamma_i < 0, i \leq k} (-\Gamma_i) \zeta_{M_i} \oplus \bigoplus_{\Gamma_i < 0, i > k} (-\Gamma_i) n_i \end{aligned}$$

Let $\mathsf{Eq}'_{\oplus}(\phi, N) = \{\widehat{\Gamma} \mid \Gamma \in \mathbb{Z}^{k+l}, (\widehat{\Gamma})\phi\}$. It is easy to verify that for any frame ψ, $\psi \models \mathsf{Eq}_{\oplus}(\phi, N)$ if and only if $\psi \models \mathsf{Eq}'_{\oplus}(\phi, N)$. It is also easy to verify (simplifying the equations) that $\mathsf{Eq}'_{\oplus}(\phi, N)$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}^{k+l}$ and thus can be generated by a finite number of vectors $V_1, \ldots, V_r$ with $r \leq k+l$. We define $\mathsf{Eq}_{b\oplus}(\phi, N) = \{\widehat{V_1}, \ldots, \widehat{V_r}\}$. It is then easy to conclude that, for any frame ψ, $\psi \models \mathsf{Eq}_{\oplus}(\phi, N)$ if and only if $\psi \models \mathsf{Eq}_{b\oplus}(\phi, N)$.

Example 7 *Consider for example a pure AC theory with only one AC symbol* $+$ *(and no other function symbol), and the frame*

$$\begin{aligned} \phi_2 \quad = \quad & \nu(n_1, n_2, n_3) \\ & \{3n_1 + 2n_2 + 4n_3/x_1, \\ & \; n_2 + 3n_3/x_2, \\ & \; n_1 + 2n_3/x_3, \\ & \; 3n_2 + n_3/x_4\} \end{aligned}$$

The set $\mathsf{Eq}(\phi_2)$ *consists of the equations of the form* $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 + T = \alpha'_1 x_1 + \alpha'_2 x_2 + \alpha'_3 x_3 + \alpha'_4 x_4 + T'$ *with* $\alpha_i, \alpha'_i \in \mathbb{N}$*, and* T *and* T' *sums of names distinct from* n_1*,* n_2*, and* n_3*. By convention, if* $\alpha_i = 0$ *(resp.* $\alpha'_i = 0$*) then the term* $\alpha_i x_i$ *(resp.* $\alpha'_i x_i$*) does not appear in the sum. Since the equation is true for* ϕ_2*, we must have* $T = T'$*, thus it is sufficient to consider the equations of the form* $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 = \alpha'_1 x_1 + \alpha'_2 x_2 + \alpha'_3 x_3 + \alpha'_4 x_4$ *with* $\alpha_i, \alpha'_i \in \mathbb{N}$*. Adopting the convention that a negative term* αx *(with* $\alpha < 0$*) in an equation actually appears on the other side of the equation, it is sufficient to consider the equations of the form* $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 = 0$*, with* $\alpha_i, \alpha'_i \in \mathbb{Z}$*. For example, the equation* $3x_1 - 2x_2 + x_3 = 0$ *stands for the equation* $3x_1 + x_3 = 2x_2$*. Then, the set of vectors* $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ *such that the equation* $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 = 0$ *holds for* ϕ_2 *is exactly the set of vectors* U *of* $\mathbb{Z}^4$ *such that* $AU = 0$ *with*

$$A = \begin{pmatrix} 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

By using classical elementary operations on rows and *columns, we find that $AU = 0$ if and only if*

$$U = \lambda \begin{pmatrix} 1 \\ 1 \\ -3 \\ -1 \end{pmatrix}$$

for $\lambda \in \mathbb{Z}$. We deduce that the set of equations satisfied by ϕ_2 is exactly the set of equations of the form: $\lambda x_1 + \lambda x_2 = 3\lambda x_3 + \lambda x_4$. Thus, in order to decide whether a frame ψ satisfies $\mathsf{Eq}(\phi_2)$, it is sufficient to check whether ψ satisfies the single equation $x_1 + x_2 = 3x_3 + x_4$.

4 Examples

In this section, we give examples of locally stable and locally finite equational theories. In Section 5, we prove that local stability implies the decidability of deduction, and that local stability and local finiteness imply the decidability of static equivalence.

Several equational theories related to cryptographic operations are locally stable and locally finite. In particular, we prove that the convergent subterm theories of our previous work [1] are locally stable. We show that a theory of homomorphic encryption, a simple theory for addition, and a theory for blind signatures (which are not subterm theories) are also locally stable. These equational theories do not have AC symbols, so local finiteness follows from Proposition 3. As examples of theories with AC symbols, we prove that the pure AC theory and a theory of the XOR operator are locally stable and locally finite. The proofs of these properties require only a few lines, and thus are much simpler than direct proofs of decidability. One can also show that the theory of Abelian groups is locally stable and locally finite, but in that case the proofs are quite tedious—probably more than direct proofs of the decidability of deduction and static equivalence.

As the examples may suggest, proving local stability often requires a precise understanding of the cryptographic primitives represented by an equational theory. In particular, removing some equations need not always preserve local stability.

4.1 Convergent subterm theories

A *convergent subterm theory* is simply a theory defined by a finite set of equations $\bigcup_{i=1}^{k}\{M_i = N_i\}$, where N_i is either a subterm of M_i or a constant symbol, such that the rewriting system obtained by orienting the equations from left to right is convergent. We have proved [1] that both deduction and static equivalence are decidable in PTIME for convergent subterm theories.

Destructor-constructor rules like those for pairing, encryption, and digital signatures may be expressed in convergent subterm theories:

$$\begin{array}{rcl} \mathsf{fst}(\langle x, y\rangle) & = & x \\ \mathsf{snd}(\langle x, y\rangle) & = & y \\ \mathsf{dec}(\mathsf{enc}(x, y), y) & = & x \\ \mathsf{check}(x, \mathsf{sign}(x, \mathsf{sk}(y)), \mathsf{pk}(y)) & = & \mathsf{ok} \end{array}$$

Convergent subterm theories also enable us to capture the theory of an inverse function:

$$\{I(I(x)) = x, I(x) \times x = 1, x \times I(x) = 1\}$$

Other usual equations (such as $x \times 1 = x$, $1 \times x = x$, and $I(1) = 1$) may be added, provided the theory remains convergent.

More examples may be found in our previous paper [1]. It is easy to verify that the definition of $\mathsf{sat}(\phi)$ given there fits our requirements for local stability.

Proposition 5 *Every convergent subterm theory is a locally finite theory.*

4.2 Homomorphism

We consider again the equational theory E_1 (defined in Example 1), which represents an encryption scheme with a homomorphism property. The size of the theory is 7.

Comon-Lundh and Treinen [9] have investigated a very similar equational theory. They showed that its deduction relation is decidable in PTIME. Here we show that E_1 is locally stable, and it is obviously locally finite (since it has no AC symbol). These properties will imply that both deduction and static equivalence are decidable.

Let $\phi = \nu\widetilde{n}\{M_1/x_1, \ldots, M_k/x_k\}$ be any frame in normal form. We define $\mathsf{sat}(\phi)$ to be the smallest set such that:

1. for every $1 \leq i \leq k$, $M_i \in \mathsf{sat}(\phi)$, and for every $n \in fn(\phi)$, $n \in \mathsf{sat}(\phi)$,

2. if $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and $f(M_1, \ldots, M_k) \in \mathsf{st}(\mathsf{sat}(\phi))$, then $f(M_1, \ldots, M_k) \in \mathsf{sat}(\phi)$,

3. if $M_1, M_2 \in \mathsf{sat}(\phi)$ and $\mathsf{dec}(M_1, M_2) \xrightarrow{h} M$ and the rule $\mathsf{dec}(\mathsf{enc}(x, y), y) \rightarrow x$ has been applied, or $\mathsf{fst}(M_1) \xrightarrow{h} M$, or $\mathsf{snd}(M_1) \xrightarrow{h} M$, then $M \in \mathsf{sat}(\phi)$.

The set $\mathsf{sat}(\phi)$ is finite since we add only subterms of terms of ϕ. It trivially satisfies conditions 1, 2, and 4 of Definition 2. Let us show that it satisfies condition 3. Let $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and assume that $C[M_1, \ldots, M_k] \xrightarrow{h} M$ where $|C| \leq 7$. The case where C is a single hole is covered by the fact that the terms are in normal form. The other cases are covered by rule 3 except in the following cases:

- $C = \mathsf{enc}(\_,\_)$, $C = \mathsf{enc}(\_,T)$, or $C = \mathsf{enc}(T,\_)$ where $fn(T) \cap \widetilde{n} = \emptyset$ and $|T| \leq 5$.
  - For $\mathsf{enc}(M_1, M_2) \to M$ with $M_1, M_2 \in \mathsf{sat}(\phi)$: In this case, M_1 must be of the form $M_1 = \langle M_1', M_2' \rangle$ and $M = \langle \mathsf{enc}(M_1', M_2), \mathsf{enc}(M_2', M_2) \rangle$. By rule 3, we know that both M_1' and M_2' are in $\mathsf{sat}(\phi)$ since $\mathsf{fst}(M_1) \to M_1'$ and $\mathsf{snd}(M_1) \to M_2'$. Thus M is a context over terms of $\mathsf{sat}(\phi)$ where the context may be chosen as $C' = \langle \mathsf{enc}(\_,\_), \mathsf{enc}(\_,\_) \rangle$ since $|C'| = 7 \leq 7^2 = 49$.
  - For $\mathsf{enc}(M_1, T) \to M$ with $M_1 \in \mathsf{sat}(\phi)$, $fn(T) \cap \widetilde{n} = \emptyset$, and $|T| \leq 5$: We have similarly that $M = \langle \mathsf{enc}(M_1', T), \mathsf{enc}(M_2', T) \rangle$ with M_1' and M_2' in $\mathsf{sat}(\phi)$. Thus M is a context over terms of $\mathsf{sat}(\phi)$ where the context may be chosen as $C' = \langle \mathsf{enc}(\_, T), \mathsf{enc}(\_, T) \rangle$ since $|C'| \leq 5 + 2|T| \leq 15 \leq 7^2 = 49$.
  - For $\mathsf{enc}(T, M_2) \to M$ with $M_2 \in \mathsf{sat}(\phi)$, $fn(T) \cap \widetilde{n} = \emptyset$, and $|T| \leq 5$: We must have $T = \langle T_1, T_2 \rangle$ with $|T_1| + |T_2| \leq 4$. We obtain $M = \langle \mathsf{enc}(T_1, M_2), \mathsf{enc}(T_2, M_2) \rangle$, so M is a context over terms of $\mathsf{sat}(\phi)$ where the context may be chosen as $C' = \langle \mathsf{enc}(T_1, \_), \mathsf{enc}(T_2, \_) \rangle$ since $|C'| \leq 5 + |T_1| + |T_2| \leq 9 \leq 49$.
- $C = \mathsf{dec}(\_,\_)$, $C = \mathsf{dec}(\_,T)$, or $C = \mathsf{dec}(T,\_)$ where $fn(T) \cap \widetilde{n} = \emptyset$ and $|T| \leq 5$, and the rule $\mathsf{dec}(\langle x, y \rangle, z) \to \langle \mathsf{dec}(x, z), \mathsf{dec}(y, z) \rangle$ has been applied.

  These three cases are very similar to the three cases above.

4.3 Addition

We consider a simple theory for addition. Let Σ_3 be any signature that contains 0, s, pred, and plus, with the equations:

$$E_3 = \left\{ \begin{array}{rcl} \mathsf{plus}(x, s(y)) & = & \mathsf{plus}(s(x), y) \\ \mathsf{plus}(x, 0) & = & x \\ \mathsf{pred}(s(x)) & = & x \end{array} \right\}$$

The size c_{E_3} of this theory is at least 4 (and possibly higher if Σ_3 contains symbols other than 0, s, pred, and plus). We define $\mathcal{R}_3$ by simply orienting the equations from left to right. Using this choice of $\mathcal{R}_3$, it is easy to verify that E_3 is convergent. (Note that E_3 has no AC symbol.) For local stability, when $\phi = \nu\widetilde{n}\{M_1/x_1, \ldots, M_k/x_k\}$ is any frame in normal form, we define $\mathsf{sat}(\phi)$ to be the smallest set such that:

1. for every $1 \leq i \leq k$, $M_i \in \mathsf{sat}(\phi)$, and for every $n \in fn(\phi)$, $n \in \mathsf{sat}(\phi)$,
2. if $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and $f(M_1, \ldots, M_k) \in \mathsf{st}(\mathsf{sat}(\phi))$, then $f(M_1, \ldots, M_k) \in \mathsf{sat}(\phi)$,
3. if $\mathsf{pred}(M) \xrightarrow{h} M'$ and $M \in \mathsf{sat}(\phi)$ then $M' \in \mathsf{sat}(\phi)$.

The set $\mathsf{sat}(\phi)$ is finite since we add only subterms of terms of ϕ. The set $\mathsf{sat}(\phi)$ trivially satisfies conditions 1, 2, and 4 of Definition 2. Let us show that it satisfies condition 3. Assume that $C[M_1, \ldots, M_k] \xrightarrow{h} M$ with $M_i \in \mathsf{sat}(\phi)$ and $|C| \leq c_{E_3}$. The only non-trivial case is the one where $\mathsf{plus}(M_1, M_2) \xrightarrow{h} M'$ with $M_1, M_2 \in \mathsf{sat}(\phi)$ and the rule $\mathsf{plus}(x, s(y)) \to \mathsf{plus}(s(x), y)$ has been applied. We must have that $M_2 = s(M_2')$. Hence $\mathsf{pred}(M_2) \xrightarrow{h} M_2'$, so $M_2' \in \mathsf{sat}(\phi)$. Now, we have $M' = \mathsf{plus}(s(M_1), M_2')$, with $M_1, M_2' \in \mathsf{sat}(\phi)$ and $|\mathsf{plus}(s(\_),\_)| = 4 \leq 4^2$, so condition 3 is satisfied.

Note that, were we to omit the equation $\mathsf{pred}(s(x)) = x$ in our equational theory, the proof of local stability would no longer be valid.

4.4 Blind signatures

We consider a theory recently introduced by Kremer and Ryan [13] in order to model blind signatures and related constructs in their analysis of a protocol for electronic voting. This theory treats signatures much like that of Section 4.1, with four differences: the checking construct is called checksign (rather than check); checking does not require plaintext; there is no separate signature-key computation (no function sk); and, most importantly, this theory also describes signature blinding and unblinding functions. Let Σ_4 be any signature that contains open, commit, getpk, host, checksign, sign, unblind, and blind, with the equations:

$$E_4 = \left\{ \begin{array}{rcl} \mathsf{open}(\mathsf{commit}(x, y), y) & = & x \\ \mathsf{getpk}(\mathsf{host}(x)) & = & x \\ \mathsf{checksign}(\mathsf{sign}(x, y), \mathsf{pk}(y)) & = & x \\ \mathsf{unblind}(\mathsf{blind}(x, y), y) & = & x \\ \mathsf{unblind}(\mathsf{sign}(\mathsf{blind}(x, y), z), y) & = & \mathsf{sign}(x, z) \end{array} \right\}$$

The size c_{E_4} of the theory is at least 7 (and possibly higher if Σ_4 contains additional symbols). We define $\mathcal{R}_4$ by simply orienting the equations from left to right. The theory E_4 is clearly convergent. To prove that E_4 is locally stable, we extend the definition of subterms by requiring that $\mathsf{sign}(M_1, M_3)$ is a subterm of $\mathsf{sign}(\mathsf{blind}(M_1, M_2), M_3)$. More formally, we define:

$$\begin{array}{l} \mathsf{st}_{\mathsf{ext}}(u) = u \\ \mathsf{st}_{\mathsf{ext}}(\mathsf{sign}(\mathsf{blind}(M_1, M_2), M_3)) = \\ \quad \{\mathsf{sign}(M_1, M_3)\} \cup \{\mathsf{sign}(\mathsf{blind}(M_1, M_2), M_3)\} \\ \quad \cup\, \mathsf{st}_{\mathsf{ext}}((\mathsf{blind}(M_1, M_2)) \cup \mathsf{st}_{\mathsf{ext}}(M_3) \\ \mathsf{st}_{\mathsf{ext}}(f(M_1, \ldots, M_k)) = \\ \quad \{f(M_1, \ldots, M_k)\} \cup \bigcup_{i=1}^{k} \mathsf{st}_{\mathsf{ext}}(M_i) \\ \qquad \text{otherwise (that is, for other terms)} \end{array}$$

When $\phi = \nu\widetilde{n}\{M_1/x_1, \ldots, M_k/x_k\}$ is any frame in normal form, we define $\mathsf{sat}(\phi)$ to be the smallest set such that:

1. for every $1 \leq i \leq k$, $M_i \in \mathsf{sat}(\phi)$, and for every $n \in \mathit{fn}(\phi)$, $n \in \mathsf{sat}(\phi)$,

2. if $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and $f(M_1, \ldots, M_k) \in \mathsf{st}(\mathsf{sat}(\phi))$, then $f(M_1, \ldots, M_k) \in \mathsf{sat}(\phi)$,

3. if $C[M_1, \ldots, M_k] \xrightarrow{h} M$, $M_i \in \mathsf{sat}(\phi)$ and $M \in \mathsf{st}_{\mathsf{ext}}(\mathsf{sat}(\phi))$ then $M \in \mathsf{sat}(\phi)$.

The set $\mathsf{sat}(\phi)$ is finite since we add only extended subterms of terms of ϕ. The set $\mathsf{sat}(\phi)$ trivially satisfies conditions 1, 2, and 4 of Definition 2. Let us show that it satisfies condition 3. Assume that $C[M_1, \ldots, M_k] \xrightarrow{h} M$ with $M_i \in \mathsf{sat}(\phi)$ and $|C| \leq c_{E_4}$. If one of the four first rules of $\mathcal{R}_4$ has been applied, then M is a subterm of $C[M_1, \ldots, M_k]$. Thus either $M = C'[M_1, \ldots, M_k]$ for some context C' and condition 3 is satisfied or M is a subterm of one of the M_i, thus $M \in \mathsf{sat}(\phi)$ and condition 3 is satisfied. If the fifth rule of $\mathcal{R}_4$ has been applied, then three (non-trivial) cases may arise.

- If $M_2 \xrightarrow{h} M$ then M is an extended subterm of M_2, so $M \in \mathsf{sat}(\phi)$ and condition 3 is satisfied.

- Similarly, if $\mathsf{unblind}(M_1, M_2) \xrightarrow{h} M$ then M is an extended subterm of M_1, so $M \in \mathsf{sat}(\phi)$ and condition 3 is satisfied.

- Finally, suppose that $\mathsf{unblind}(\mathsf{sign}(M_1, M_2), M_3) \xrightarrow{h} M$. It must be the case that $M_1 = \mathsf{blind}(M_1', M_3)$. Since $\mathsf{unblind}(M_1, M_3) \xrightarrow{h} M_1'$ and M_1' is a subterm of M_1, we have $M_1' \in \mathsf{sat}(\phi)$. Now, since $M = \mathsf{sign}(M_1', M_2)$ and $|\mathsf{sign}(\_, \_)| = 3 \leq 7^2$, condition 3 is satisfied.

4.5 Pure AC theory

We consider the case where the signature contains only constant symbols and AC symbols $\oplus_1, \ldots, \oplus_k$ and the equational theory E_5 contains only the AC equations for each symbol:

$$E_5 = \bigcup_{i=1}^{k} \left\{ \begin{array}{rcl} (x \oplus_i y) \oplus_i z & = & x \oplus_i (y \oplus_i z) \\ x \oplus_i y & = & y \oplus_i x \end{array} \right\}$$

With the empty rewriting system $\mathcal{R}_5 = \emptyset$, E_5 is an AC-convergent theory. When $\phi = \nu\widetilde{n}\{M_1/x_1, \ldots, M_k/x_k\}$ is any frame, we define $\mathsf{sat}(\phi)$ to be the smallest set such that:

1. for every $1 \leq i \leq k$, $M_i \in \mathsf{sat}(\phi)$, and for every $n \in \mathit{fn}(\phi)$, $n \in \mathsf{sat}(\phi)$,

2. if $M_1, M_2 \in \mathsf{sat}(\phi)$ and $M_1 \oplus_i M_2 \in \mathsf{st}(\mathsf{sat}(\phi))$, then $M_1 \oplus_i M_2 \in \mathsf{sat}(\phi)$,

3. if $M_1 =_{\mathsf{AC}} M_2$ and $M_1 \in \mathsf{sat}(\phi)$ then $M_2 \in \mathsf{sat}(\phi)$.

The set $\mathsf{sat}(\phi)$ is finite since we add only terms smaller or equal than the maximal size of the terms of ϕ. The set $\mathsf{sat}(\phi)$ trivially satisfies conditions 1, 2, and 4 of Definition 2. It also satisfies condition 3 since the rewriting system $\mathcal{R}_5$ is empty. Thus E_5 is locally stable.

Now, for any frame $\phi = \nu\widetilde{n}\sigma$, the set of equations $\mathsf{Eq}(\phi)$ simply consists of $\mathsf{Eq}_{\oplus}(\phi, \mathcal{N} - \widetilde{n})$. Since names that do not appear in ϕ need not be considered, $\mathsf{Eq}_{\oplus}(\phi, \mathcal{N} - \widetilde{n})$ is equivalent to $\mathsf{Eq}_{\oplus}(\phi, N)$ where N is the set of free names of ϕ, in the sense that for any frame ψ, $\psi \models \mathsf{Eq}_{\oplus}(\phi, \mathcal{N} - \widetilde{n})$ if and only if $\psi \models \mathsf{Eq}_{\oplus}(\phi, N)$. By Proposition 4, we conclude that the equational theory E_5 is locally finite.

4.6 XOR

We consider the theory E_2 of the XOR operator (defined in Example 4).

We have seen that E_2 is AC-convergent. We wish to verify that E_2 is locally stable. When $\phi = \nu\widetilde{n}\{M_1/x_1, \ldots, M_k/x_k\}$ is any frame in normal form, we define $\mathsf{sat}(\phi)$ to be the smallest set, closed under AC, such that:

1. for every $1 \leq i \leq k$, $M_i \in \mathsf{sat}(\phi)$, and for every $n \in \mathit{fn}(\phi)$, $n \in \mathsf{sat}(\phi)$, and $0 \in \mathsf{sat}(\phi)$,

2. if $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and $f(M_1, \ldots, M_k) \in \mathsf{st}(\mathsf{sat}(\phi))$, then $f(M_1, \ldots, M_k) \in \mathsf{sat}(\phi)$,

3. if $M_1, M_2 \in \mathsf{sat}(\phi)$, then $(M_1 \oplus M_2)\!\downarrow \subseteq \mathsf{sat}(\phi)$,

4. if a is a name not in $\widetilde{n}$ and if $M \oplus a \rightarrow_{\mathsf{AC}} M'$ with $M' \in \mathsf{st}(\mathsf{sat}(\phi))$, then $M' \in \mathsf{sat}(\phi)$.

Let us first show that $\mathsf{sat}(\phi)$ is finite. Let the set $\mathsf{sst}(\phi)$ of *simple subterms* of ϕ be the set of subterms of ϕ whose head symbol is not $\oplus$. Let $S = \{T_1 \oplus \cdots \oplus T_n \mid T_i \in \mathsf{sst}(\phi), T_i \neq 0, T_i = T_j \Rightarrow i = j\}$ be the set of sums of distinct terms of $\mathsf{sst}(\phi)$. The set S is finite and $\mathsf{sat}(\phi) \subseteq S$. Indeed, it is easy to show that S satisfies the four conditions above, using that $\mathsf{st}(S) = S$.

The set $\mathsf{sat}(\phi)$ trivially satisfies conditions 1, 2, and 4 of Definition 2. Let us show that it satisfies condition 3. Let $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and C be a context such that $\mathit{fn}(C) \cap \widetilde{n} = \emptyset$ and assume that $C[M_1, \ldots, M_k] \xrightarrow{h} M$. We have that $C[M_1, \ldots, M_k] =_{\mathsf{AC}} \bigoplus_{i=1}^{k} M_i \oplus \bigoplus_{i=1}^{n} a_i$, where each a_i is a name not in $\widetilde{n}$ or the constant 0. Let us show that one of the normal forms of $C[M_1, \ldots, M_k]$ is a context of terms in $\mathsf{sat}(\phi)$. Applying recursively rule 3, we obtain that $(\bigoplus_{i=1}^{k} M_i)\!\downarrow \subseteq \mathsf{sat}(\phi)$. Now, applying recursively rule 4, we obtain that $C[M_1, \ldots, M_k]\!\downarrow =_{\mathsf{AC}} M' \oplus \bigoplus_{j=1}^{r} a_{i_j}$, with $M' \in \mathsf{sat}(\phi)$. By AC-convergence, we know that $M \rightarrow^*_{\mathsf{AC}}=_{\mathsf{AC}} M' \oplus \bigoplus_{j=1}^r a_{i_j}$ with $M' \oplus \bigoplus_{j=1}^r a_{i_j} \in \mathsf{sum}_\oplus(\mathsf{sat}(\phi), \widetilde{n})$, since none of the a_{i_j} is 0 (for otherwise the term would not be in normal form), so the context C' that simply consists of a hole satisfies the required conditions.

Like in the pure AC case, for any frame ϕ, the set of equation $\mathsf{Eq}(\phi)$ simply consists of $\mathsf{Eq}_\oplus(\phi, \mathcal{N} - \widetilde{n})$ since the only constant is 0 and 0 is itself in $\mathsf{sat}(\phi)$. Since names that do not appear in ϕ do not need to be considered, $\mathsf{Eq}_\oplus(\phi, \mathcal{N} - \widetilde{n})$ is equivalent to $\mathsf{Eq}_\oplus(\phi, N)$ where N is the set of free names of ϕ, in the sense that for any frame ψ, $\psi \models \mathsf{Eq}_\oplus(\phi, \mathcal{N} - \widetilde{n})$ if and only if $\psi \models \mathsf{Eq}_\oplus(\phi, N)$. Thus, by Proposition 4, the equational theory E_2 is locally finite.

Note that, in this example, we can also conclude without using Proposition 4. Indeed, we can consider the set $\mathsf{Eq}'(\phi)$ that consists of the equations

$$\bigoplus_{j=1}^{k_1} \zeta_{M_{i_j}} \oplus \bigoplus_{j=1}^{k_2} n_{i_j} = \bigoplus_{j=k_1+1}^{l_1} \zeta_{M_{i_j}} \oplus \bigoplus_{j=k_2+1}^{l_2} n_{i_j}$$

such that

$$\left(\bigoplus_{j=1}^{k_1} \zeta_{M_{i_j}} \oplus \bigoplus_{j=1}^{k_2} n_{i_j} =_E \bigoplus_{j=k_1+1}^{l_1} \zeta_{M_{i_j}} \oplus \bigoplus_{j=k_2+1}^{l_2} n_{i_j}\right) \phi$$

$n_{i_j} \in fn(\phi)$, and $l \neq j \implies M_{i_l} \neq M_{i_j}, n_{i_l} \neq n_{i_j}$. Clearly, $\mathsf{Eq}'(\phi)$ is finite and it is easy to verify that, for any frame ψ, $\psi \models \mathsf{Eq}_\oplus(\phi, \widetilde{n})$ if and only if $\psi \models \mathsf{Eq}'(\phi)$.

5 Decidability results

In this section, we state and prove our decidability results for deduction and static equivalence.

5.1 Decidability of deduction

Theorem 1 *For locally stable equational theories, deduction is decidable.*

The proof is based on the following lemma.

Lemma 1 *Let E be a locally stable theory. Let $\phi = \nu\widetilde{n}\sigma$ be a frame. For every context C_1 such that $fn(C_1) \cap \widetilde{n} = \emptyset$, for every $M_i \in \mathsf{sat}(\phi)$, for every term T such that $C_1[M_1, \ldots, M_k] \rightarrow_{\mathsf{AC}} T$, there exist a context C_2 such that $fn(C_2) \cap \widetilde{n} = \emptyset$, and terms $M'_i \in \mathsf{sat}(\phi)$, such that $T \rightarrow^*_{\mathsf{AC}} C_2[M'_1, \ldots, M'_l]$.*

This lemma is a weak version of Lemma 3 presented in Section 5.2. Applying repeatedly this lemma leads to the following corollary.

Corollary 1 *Let E be a locally stable theory. Let $\phi = \nu\widetilde{n}\sigma$ be a frame. For every context C_1 such that $fn(C_1) \cap \widetilde{n} = \emptyset$, for every $M_i \in \mathsf{sat}(\phi)$, for every term T in normal form such that $C_1[M_1, \ldots, M_k] \rightarrow^*_{\mathsf{AC}} T$, there exist a context C_2 such that $fn(C_2) \cap \widetilde{n} = \emptyset$, and terms $M'_i \in \mathsf{sat}(\phi)$, such that $T =_{\mathsf{AC}} C_2[M'_1, \ldots, M'_l]$.*

Assuming Lemma 1, let $\phi = \nu\widetilde{n}\sigma$ be a frame, C_1 be a context such that $fn(C_1) \cap \widetilde{n} = \emptyset$, $M_i \in \mathsf{sat}(\phi)$, and T a term in normal form such that $C_1[M_1, \ldots, M_k] \rightarrow^*_{\mathsf{AC}} T$. Either $C_1[M_1, \ldots, M_k] =_{\mathsf{AC}} T$ and we are done or we have $C_1[M_1, \ldots, M_k] \rightarrow_{\mathsf{AC}} T' \rightarrow^*_{\mathsf{AC}} T$. By Lemma 1, there exist a context C_2 such that $fn(C_2) \cap \widetilde{n} = \emptyset$, and terms $M'_i \in \mathsf{sat}(\phi)$, such that $T' \rightarrow^*_{\mathsf{AC}} C_2[M'_1, \ldots, M'_l]$. By AC-confluence of the equational theory and since T is in normal form, $C_2[M'_1, \ldots, M'_l] \rightarrow^*_{\mathsf{AC}} T$. Since the equational theory is AC-terminating, we repeat this transformation until we obtain that $T =_{\mathsf{AC}} C_3[M''_1, \ldots, M''_l]$ for some terms $M''_i \in \mathsf{sat}(\phi)$ and some context C_3.

We show that for any term deducible from a frame ϕ, one of its normal forms is a context over terms in $\mathsf{sat}(\phi)$.

Proposition 6 *Let $\phi = \nu\widetilde{n}\sigma$ be a frame, M be a closed term, and $M\!\downarrow$ its set of normal forms. Then $\phi \vdash M$ if and only if there exist a term $T \in M\!\downarrow$, a context C, and terms $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ such that $fn(C) \cap \widetilde{n} = \emptyset$ and $T == C[M_1, \ldots, M_k]$.*

If there exists $T \in M\!\downarrow$ such that $T == C[M_1, \ldots, M_k]$ with $fn(C) \cap \widetilde{n} = \emptyset$, then $T =_E C[\zeta_{M_1}, \ldots, \zeta_{M_k}]\sigma$, by construction of $\zeta_{M_1}, \ldots, \zeta_{M_k}$. Therefore, by Proposition 1, $\phi \vdash T$, so $\phi \vdash M$.

Conversely, if $\phi \vdash M$, then by Proposition 1, there exists ζ such that $fn(\zeta) \cap \widetilde{n} = \emptyset$ and $M =_E \zeta\sigma$. Thus there exists $T' \in (M\!\downarrow \cap (\zeta\sigma)\!\downarrow)$. Since $\zeta\sigma \rightarrow^*_{\mathsf{AC}} T'$, applying Corollary 1, we obtain that $T' =_{\mathsf{AC}} C[M_1, \ldots, M_k]$ for some $M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and C such that $fn(C) \cap \widetilde{n} = \emptyset$. Thus we end the proof by choosing $T == C[M_1, \ldots, M_k]$.

We derive that $\phi \vdash M$ can be decided by checking whether one of the terms in $M\!\downarrow$ is of the form $C[M_1, \ldots, M_k]$ with $M_i \in \mathsf{sat}(\phi)$.

5.2 Decidability of static equivalence

Theorem 2 *For locally decidable equational theories, static equivalence is decidable. A fortiori, for locally finite equational theories, static equivalence is decidable.*

The proof is based on two main lemmas that we prove in the Appendix.

Lemma 2 *Let E be a locally stable theory. Let $\phi = \nu\widetilde{n}\sigma$ and $\psi = \nu\widetilde{n'}\sigma'$ be two frames such that $\psi \models \mathsf{Eq}(\phi)$. For all contexts C_1 and C_2 such that $(fn(C_1) \cup fn(C_2)) \cap \widetilde{n} = \emptyset$, for all terms $M_i, M'_i \in$*

$\mathsf{sat}(\phi)$, *if* $C_1[M_1,\ldots,M_k] =_{\mathsf{AC}} C_2[M'_1,\ldots,M'_l]$, *then* $(C_1[\zeta_{M_1},\ldots,\zeta_{M_k}] =_E C_2[\zeta_{M'_1},\ldots,\zeta_{M'_l}])\psi$.

Lemma 3 *Let* E *be a locally stable theory. Let* $\phi = \nu\widetilde{n}\sigma$ *be a frame. For every context* C_1 *such that* $fn(C_1) \cap \widetilde{n} = \emptyset$, *for every* $M_i \in \mathsf{sat}(\phi)$, *for every term* T *such that* $C_1[M_1,\ldots,M_k] \rightarrow_{\mathsf{AC}} T$, *there exist a context* C_2 *such that* $fn(C_2) \cap \widetilde{n} = \emptyset$, *and terms* $M'_i \in \mathsf{sat}(\phi)$, *such that* $T \rightarrow^*_{\mathsf{AC}} C_2[M'_1,\ldots,M'_l]$ *and for every frame* $\psi \models \mathsf{Eq}(\phi)$, $(C_1[\zeta_{M_1},\ldots,\zeta_{M_k}] =_E C_2[\zeta_{M'_1},\ldots,\zeta_{M'_l}])\psi$.

As for Corollary 1, applying repeatedly Lemma 3 leads to the following corollary.

Corollary 2 *Let* E *be a locally stable theory. Let* $\phi = \nu\widetilde{n}\sigma$ *be a frame. For every context* C_1 *such that* $fn(C_1) \cap \widetilde{n} = \emptyset$, *for every* $M_i \in \mathsf{sat}(\phi)$, *for every term* T *in normal form such that* $C_1[M_1,\ldots,M_k] \rightarrow^*_{\mathsf{AC}} T$, *there exist a context* C_2 *such that* $fn(C_2) \cap \widetilde{n} = \emptyset$, *and terms* $M'_i \in \mathsf{sat}(\phi)$, *such that* $T =_{\mathsf{AC}} C_2[M'_1,\ldots,M'_l]$ *and for every frame* $\psi \models \mathsf{Eq}(\phi)$, $(C_1[\zeta_{M_1},\ldots,\zeta_{M_k}] =_E C_2[\zeta_{M'_1},\ldots,\zeta_{M'_l}])\psi$.

In order to check whether two frames satisfy the same equations, we show (using these two lemmas) that it is sufficient to check whether they satisfy the same "small" equations.

Proposition 7 *Let* E *be a locally stable theory. For all frames* ϕ *and* ψ, *we have* $\phi \approx_s \psi$ *if and only if* $\phi \models \mathsf{Eq}(\psi)$ *and* $\psi \models \mathsf{Eq}(\phi)$.

By definition of static equivalence, if $\phi \approx_s \psi$ then $\phi \models \mathsf{Eq}(\psi)$ and $\psi \models \mathsf{Eq}(\phi)$.

Conversely, assume now that $\psi \models \mathsf{Eq}(\phi)$ and consider M and N such that there exist $\widetilde{n}$ and σ 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 $((M\sigma)\!\downarrow \cap (N\sigma)\!\downarrow) \neq \emptyset$. Let $T \in ((M\sigma)\!\downarrow \cap (N\sigma)\!\downarrow)$. Since $M\sigma \rightarrow^*_{\mathsf{AC}} T$, applying Corollary 2, we obtain that there exist $M_1,\ldots,M_k \in \mathsf{sat}(\phi)$ and C_M such that $fn(C_M) \cap \widetilde{n} = \emptyset$, $T =_{\mathsf{AC}} C_M[M_1,\ldots,M_k]$, and $(M =_E C_M[\zeta_{M_1},\ldots,\zeta_{M_k}])\psi$. Since $N\sigma \rightarrow^*_{\mathsf{AC}} T$, we obtain similarly that there exist $M'_1,\ldots,M'_l \in \mathsf{sat}(\phi)$ and C_N such that $fn(C_N) \cap \widetilde{n} = \emptyset$, $T =_{\mathsf{AC}} C_N[M'_1,\ldots,M'_l]$, and $(N =_E C_N[\zeta_{M'_1},\ldots,\zeta_{M'_l}])\psi$. Moreover, since $C_M[M_1,\ldots,M_k] =_{\mathsf{AC}} C_N[M'_1,\ldots,M'_l]$, we derive from Lemma 2 that $(C_M[\zeta_{M_1},\ldots,\zeta_{M_k}] =_E C_N[\zeta_{M'_1},\ldots,\zeta_{M'_l}])\psi$, thus $(M =_E N)\psi$. Symmetrically, if $(M =_E N)\psi$ and $\phi \models \mathsf{Eq}(\psi)$, then $(M =_E N)\phi$. We conclude that $\phi \approx_s \psi$.

Therefore, given ϕ and ψ, we may consider $\mathsf{Eq}(\phi)$ and $\mathsf{Eq}(\psi)$ in order to decide whether $\phi \approx_s \psi$. By local decidability of the theory, we can decide whether $\phi \models \mathsf{Eq}(\psi)$ and $\psi \models \mathsf{Eq}(\phi)$.

6 Conclusion

In this paper we study message deducibility and static equivalence, two formal representations for knowledge in the analysis of security protocols. This study yields a general, positive result: message deducibility and static equivalence are decidable under a wide class of equational theories. This class includes, in particular, standard theories for basic cryptographic primitives. It also includes some less standard, more advanced examples: theories of XOR, homomorphic encryption, blind signatures, addition, and pure AC theories. We succeed in giving a unified treatment for this disparate collection of theories, with a body of techniques that apply to all of them plus special techniques for verifying that particular theories belong in the class.

We have not considered complexity issues for the corresponding decision procedures. Their performances obviously depend on the choice of equational theory, and we do not expect them to be very good in many cases. The second author is currently working on implementing a variant of our procedures for specific theories. We expect that the resulting algorithms will be efficient enough to be applicable in practice.

As indicated in the introduction, deduction and static equivalence are static notions, but they play an important role in analyses with respect to active attacks. Nevertheless, it remains challenging to obtain decidability results with respect to active attacks. This problem is addressed in recent and ongoing work. That work is still largely under way, so detailed descriptions may be premature, but we briefly mention some interesting developments. Going beyond the work of Delaune and Jacquemard [10] (described in the introduction), Baudet [5] has proved that both deduction and static equivalence are decidable under convergent subterm theories. Comon-Lundh [7] is studying the decidability of deduction under general equational theories, including associativity and commutativity properties. Overall, this field appears as a lively one, with increasingly sophisticated techniques and powerful theorems. We may therefore look forward to much progress in algorithmic reasoning about the knowledge of active attackers in security protocols.

Acknowledgments

We are grateful to Michael Rusinowitch and Mathieu Baudet for very helpful discussions.

Martín Abadi's work was partly supported by the National Science Foundation under Grants CCR-0204162 and CCR-0208800. Véronique Cortier's work was partly supported by the IST AVISPA `http://www.avispa-project.org` and the ACI Jeunes Chercheurs JC9005.

References

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

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

[3] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148(1):1–70, Jan. 1999.

[4] M. Abadi and P. Rogaway. Reconciling two views of cryptography (The computational soundness of formal encryption). *Journal of Cryptology*, 15(2):103–127, 2002.

[5] M. Baudet. Private communication. 2005.

[6] Y. Chevalier, R. Kuester, M. Rusinowitch, and M. Turani. An NP decision procedure for protocol insecurity with xor. In *Proceedings of the 18th Annual IEEE Symposium on Logic In Computer Science (LICS'03)*, pages 261–270, 2003.

[7] H. Comon-Lundh. Intruder theories (ongoing work). In *Foundations of Software Science and Computation Structures (FoSSaCS'04)*, volume 2987 of *LNCS*, pages 1–4. Springer, 2004.

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

[9] H. Comon-Lundh and R. Treinen. Easy intruder deductions. Technical Report LSV-03-8, Laboratoire Spécification et Vérification, ENS de Cachan, France, 2003.

[10] S. Delaune and F. Jacquemard. A decision procedure for the verification of security protocols with explicit destructors. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 278–287, Washington, D.C., USA, October 2004. ACM Press.

[11] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, Apr. 1984.

[12] R. Kemmerer, C. Meadows, and J. Millen. Three systems for cryptographic protocol analysis. *Journal of Cryptology*, 7(2):79–130, Spring 1994.

[13] S. Kremer and M. D. Ryan. Analysis of an electronic voting protocol in the applied pi-calculus. In M. Sagiv, editor, *Programming Languages and Systems –Proceedings of the 14th European Symposium on Programming (ESOP'05)*, volume 3444 of *LNCS*, pages 186–200, Edinburgh, U.K., April 2005. Springer.

[14] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for ac-like equational theories with homomorphisms. In *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *LNCS*, pages 308–322, Nara, Japan, April 2005. Springer.

[15] P. Lincoln, J. Mitchell, M. Mitchell, and A. Scedrov. A probabilistic poly-time framework for protocol analysis. In *Proceedings of the Fifth ACM Conference on Computer and Communications Security*, pages 112–121, 1998.

[16] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Tools and Algorithms for the Construction and Analysis of Systems*, volume 1055 of *LNCS*, pages 147–166. Springer, 1996.

[17] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6(1–2):85–128, 1998.

[18] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. In R. DeMillo, D. Dobkin, A. Jones, and R. Lipton, editors, *Foundations of Secure Computation*, pages 169–180. Academic Press, 1978.

[19] P. Samuel. *Algebraic Theory of Numbers*. Hermann, 1970.

[20] S. Schneider. Security properties and CSP. In *IEEE Symposium on Security and Privacy*, pages 174–187, 1996.

Appendix: Proof of Lemmas 2 and 3

Definition 7 *The set $\mathcal{P}(M)$ of* paths *of a term M is defined inductively by:*

$$\begin{array}{rcl}\mathcal{P}(u) & = & \epsilon \\ \mathcal{P}(f(M_1,\ldots,M_n)) & = & \epsilon \cup \bigcup_{i=1}^{n} i\cdot\mathcal{P}(M_i) \quad \textit{for } i\leq n\end{array}$$

The subterm of M at position $p \in \mathcal{P}(M)$, written $M|_p$, is defined inductively by:

$$\begin{array}{rcl}M|_\epsilon & = & M \\ f(M_1,\ldots,M_n)|_{i\cdot p} & = & M_i|_p \quad \textit{for } i\leq n\end{array}$$

Lemma 2. *Let E be a locally stable theory. Let $\phi = \nu\widetilde{n}\sigma$ and $\psi = \nu\widetilde{n'}\sigma'$ be two frames such that $\psi \models \mathsf{Eq}(\phi)$. For all contexts C_1 and C_2 such that $(fn(C_1) \cup fn(C_2)) \cap \widetilde{n} = \emptyset$, for all terms $M_i, M'_i \in \mathsf{sat}(\phi)$, if $C_1[M_1,\ldots,M_k] =_{\mathsf{AC}} C_2[M'_1,\ldots,M'_l]$, then $(C_1[\zeta_{M_1},\ldots,\zeta_{M_k}] =_E C_2[\zeta_{M'_1},\ldots,\zeta_{M'_l}])\psi$.*

This lemma is proved by induction on the sum of the sizes of C_1 and C_2.

Base case: If $|C_1|, |C_2| \leq c_E$, then the equation

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

is in $\mathsf{Eq}(\phi)$ since $|C_1| \leq c_E$ and $|C_2| \leq c_E \leq c_E^2$, so $\psi \models \mathsf{Eq}(\phi)$ implies $(C_1[\zeta_{M_1},\ldots,\zeta_{M_k}] =_E C_2[\zeta_{M'_1},\ldots,\zeta_{M'_l}])\psi$.

Inductive step: If neither C_1 nor C_2 is a hole, then $C_1 == f(C_1^1,\ldots,C_1^r)$ and $C_2 == f(C_2^1,\ldots,C_2^r)$. There are two cases.

- f is not an AC symbol. Then, for every $1 \leq i \leq r$, $C_1^i[M_1, \ldots, M_k] =_{\mathsf{AC}} C_2^i[M'_1, \ldots, M'_l]$. By applying the induction hypothesis, we obtain $(C_1^i[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C_2^i[\zeta_{M'_1}, \ldots, \zeta_{M'_l}])\psi$, so $(C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}])\psi$.

- f is an AC symbol $\oplus$. We write $C_1 = C_1^1 \oplus \cdots \oplus C_1^r \oplus x_1 \oplus \cdots \oplus x_p$ and $C_2 = C_2^1 \oplus \cdots \oplus C_2^{r'} \oplus y_1 \oplus \cdots \oplus y_{p'}$ in such a way that the head symbol of the C_1^i and C_2^j is not $\oplus$, C_1^i and C_2^j are not holes, and the x_i and y_j refer to the holes of C_1 and C_2. If the equation can be split, with $C_1 =_{\mathsf{AC}} C'_1 \oplus C''_1$ and $C_2 =_{\mathsf{AC}} C'_2 \oplus C''_2$ such that $(C'_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C'_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}])\phi$ and $(C''_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C''_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}])\phi$, then we conclude as above, applying the induction hypothesis. On the other hand, if the equation cannot be split, for every $1 \leq i \leq r$, $N_i \stackrel{\text{def}}{=} C_1^i[M_1, \ldots, M_k]$ is not equal to some $C_2^j[M'_1, \ldots, M'_l]$ so it must be a subterm of some M'_j. Since each M'_j is in $\mathsf{sat}(\phi)$ and by applying recursively rule 2 of Definition 2, we get that N_i is in $\mathsf{sat}(\phi)$, thus there exists $\zeta_{N_i} \in \mathcal{R}(\phi)$ such that $\zeta_{N_i}\sigma =_E N_i$. Symmetrically, for every $1 \leq j \leq r$, $N'_j \stackrel{\text{def}}{=} C_1^j[M'_1, \ldots, M'_k]$ is not equal to some $C_1^i[M_1, \ldots, M_l]$, so $N'_j \in \mathsf{sat}(\phi)$ and there exists $\zeta_{N'_j} \in \mathcal{R}(\phi)$ such that $\zeta_{N'_j}\sigma =_E N'_j$.
  - From $N_i == C_1^i[M_1, \ldots, M_k]$ and applying the induction hypothesis, we get $\zeta_{N_i}\sigma' =_E C_1^i[\zeta_{M_1}, \ldots, \zeta_{M_k}]\sigma'$ and similarly, $\zeta_{N'_j}\sigma' =_E C_2^j[\zeta_{M_1}, \ldots, \zeta_{M_k}]\sigma'$.
  - Renaming the $C_1^i[M_1, \ldots, M_k]$ by N_i in our initial equation, we get $N_1 \oplus \cdots \oplus N_r \oplus M_1 \oplus \cdots \oplus M_p = N'_1 \oplus \cdots \oplus N'_{r'} \oplus M'_1 \oplus \cdots \oplus M'_{p'}$. Applying the base case, we get $(\zeta_{N_1} \oplus \cdots \oplus \zeta_{N_r} \oplus \zeta_{M_1} \oplus \cdots \oplus \zeta_{M_p} =_E \zeta_{N'_1} \oplus \cdots \oplus \zeta_{N'_{r'}} \oplus \zeta_{M'_1} \oplus \cdots \oplus \zeta_{M'_{p'}})\sigma$. Since this equation is in $\mathsf{Eq}(\phi)$, we deduce $(\zeta_{N_1} \oplus \cdots \oplus \zeta_{N_r} \oplus \zeta_{M_1} \oplus \cdots \oplus \zeta_{M_p} =_E \zeta_{N'_1} \oplus \cdots \oplus \zeta_{N'_{r'}} \oplus \zeta_{M'_1} \oplus \cdots \oplus \zeta_{M'_{p'}})\sigma'$.

  Combining these equations, we get

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

If C_1 or C_2 is a hole, then let us say $C_1 == f(C_1^1, \ldots, C_1^r)$ and $C_2 == \_$. Let $M, M_1, \ldots, M_k \in \mathsf{sat}(\phi)$ and assume $C_1[M_1, \ldots, M_k] =_{\mathsf{AC}} M$. Again we consider two cases.

- f is not an AC symbol. Then we have

$$f(C_1^1[M_1, \ldots, M_k], \ldots, C_1^r[M_1, \ldots, M_k]) =_{\mathsf{AC}} M$$

  For every $1 \leq i \leq r$, let $N_i \stackrel{\text{def}}{=} C_1^i[M_1, \ldots, M_k]$. Thus, each N_i is a subterm of M, so it is in $\mathsf{st}(\mathsf{sat}(\phi))$. Since each M_j is in $\mathsf{sat}(\phi)$ and by applying repeatedly rule 2 of Definition 2, we get that N_i is in $\mathsf{sat}(\phi)$. Thus there exists $\zeta_{N_i} \in \mathcal{R}(\phi)$ such that $\zeta_{N_i}\sigma =_E N_i$.
  - From $N_i == C_1^i[M_1, \ldots, M_k]$ and applying the induction hypothesis, we get $\zeta_{N_i}\sigma' =_E C_1^i[\zeta_{M_1}, \ldots, \zeta_{M_k}]\sigma'$.
  - From $M =_{\mathsf{AC}} f(N_1, \ldots, N_r)$ and applying the base case, we get $\zeta_M\sigma' =_E f(\zeta_{N_1}, \ldots, \zeta_{N_r})\sigma'$.

  Combining these equations, we get

$$(\zeta_M =_E C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}])\psi$$

- f is an AC symbol $\oplus$. We write $C_1 = C_1^1 \oplus \cdots \oplus C_1^r \oplus x_1 \oplus \cdots \oplus x_p$ and $C_2 = x$, and we have $C_1^1[M_1, \ldots, M_k] \oplus \ldots \oplus C_1^r[M_1, \ldots, M_k] \oplus M'_1 \oplus \ldots \oplus M'_p =_{\mathsf{AC}} M$. Each $N_i \stackrel{\text{def}}{=} C_1^i[M_1, \ldots, M_k]$ is a subterm of $M \in \mathsf{sat}(\phi)$ thus is in $\mathsf{sat}(\phi)$. Again, there exists $\zeta_{N_i} \in \mathcal{R}(\phi)$ such that $\zeta_{N_i}\sigma =_E N_i$.
  - From $N_i == C_1^i[M_1, \ldots, M_k]$ and applying the induction hypothesis, we get $\zeta_{N_i}\sigma' =_E C_1^i[\zeta_{M_1}, \ldots, \zeta_{M_k}]\sigma'$.
  - From $N_1 \oplus \ldots \oplus N_r \oplus M'_1 \oplus \ldots \oplus M'_p =_{\mathsf{AC}} M$ and by the equation $\zeta_{N_1} \oplus \cdots \oplus \zeta_{N_r} \oplus \zeta_{M'_1} \oplus \cdots \oplus \zeta_{M'_p} =_E \zeta_M$ is in $\mathsf{Eq}(\phi)$, we get $(\zeta_{N_1} \oplus \cdots \oplus \zeta_{N_r} \oplus \zeta_{M'_1} \oplus \cdots \oplus \zeta_{M'_p} =_E \zeta_M)\sigma'$.

  Combining these equations, we get

$$(C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E \zeta_M)\psi$$

Lemma 3. *Let E be a locally stable theory. Let $\phi = \nu\widetilde{n}\sigma$ be a frame. For every context C_1 such that $fn(C_1) \cap \widetilde{n} = \emptyset$, for every $M_i \in \mathsf{sat}(\phi)$, for every term T such that $C_1[M_1, \ldots, M_k] \rightarrow_{\mathsf{AC}} T$, there exist a context C_2 such that $fn(C_2) \cap \widetilde{n} = \emptyset$, and terms $M'_i \in \mathsf{sat}(\phi)$, such that $T \rightarrow^*_{\mathsf{AC}} C_2[M'_1, \ldots, M'_l]$ and for every frame $\psi \models \mathsf{Eq}(\phi)$, $(C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}])\psi$.*

An easy case is when the reduction occurs inside one of the M_i: $M_i \rightarrow_{\mathsf{AC}} M'_i$. By definition of $\mathsf{sat}(\phi)$ (since E is locally stable), we know that there exists C such that $|C| \leq c_E^2$, $fn(C) \cap \widetilde{n} = \emptyset$, and $M'_i \rightarrow^*_{\mathsf{AC}} C[M''_1, \ldots, M''_l]$ where $M''_i \in \mathsf{sat}(\phi)$. In addition, the equation $\zeta_{M_i} = C[\zeta_{M''_1}, \ldots, \zeta_{M''_l}]$ is in $\mathsf{Eq}(\phi)$ (since $|C| \leq c_E^2$), thus $(\zeta_{M_i} =_E C[\zeta_{M''_1}, \ldots, \zeta_{M''_l}])\psi$. We obtain that

$$T == C_1[M_1, \ldots, M_{i-1}, M'_i, M_{i+1}, \ldots, M_k] \rightarrow^*_{\mathsf{AC}} C_1[M_1, \ldots, C[M''_1, \ldots, M''_l], \ldots, M_k]$$

and

$$\left(\begin{array}{c}(C_1[\zeta_{M_1},\ldots,\zeta_{M_k}]\\ =_E\\ C_1[\zeta_{M_1},\ldots,C[\zeta_{M''_1},\ldots,\zeta_{M''_l}],\ldots,\zeta_{M_k}]\end{array}\right)\psi$$

We now consider the case where the reduction does not occur inside the terms M_i. We can assume that

for every path p of C_1,
if $C_1|_p[M_1,\ldots,M_k]$ is in $\mathsf{sat}(\phi)$, (*)
then $C_1|_p$ is the single hole context.

Indeed, if there exists a path p of C_1 such that $T_1 \stackrel{\text{def}}{=} C_1|_p[M_1,\ldots,M_k] \in \mathsf{sat}(\phi)$ and $C_1|_p$ is not a hole then $C_1[M_1,\ldots,M_k] == C'_1[T_1,M_1,\ldots,M_k]$ where $T_1, M_i \in \mathsf{sat}(\phi)$ and C'_1 is a context strictly smaller than C_1. In that case, we consider $C'_1[T_1,M_1,\ldots,M_k]$ instead of $C_1[M_1,\ldots,M_k]$ and we apply the transformation again until property (*) holds.

We have

$$C_1[M_1,\ldots,M_k] == C_3[M''\oplus M'\oplus\bigoplus_{i=1}^{r} C'_i[M_1,\ldots,M_k],M_1,\ldots,M_k]$$

where $M' = M'_1\oplus\ldots\oplus M'_l$, $M'' = M''_1\oplus\ldots\oplus M''_l$ with $M'_i\oplus M''_i\in\mathsf{sat}(\phi)$, the head symbol of the C'_i is not $\oplus$, C'_i is not a single hole, and $T_1 \stackrel{\text{def}}{=} M'\oplus\bigoplus_{i=1}^{r} C'_i[M_1,\ldots,M_k]$ is an instance $M_0\theta$ (modulo AC) of the left-hand side of some rule $M_0\to N_0$ of the rewriting system associated with E.

For each variable x of M_0, we consider the occurrences of $x\theta$ in T_1.

1. Either $x\theta$ occurs as a subterm of one of the M_i or M'_i;

2. or there exists a subterm of T_1, of the form $N_1\oplus\ldots\oplus N_p$ with $N_i =_{\mathsf{AC}} N'_i\oplus N''_i\in\mathsf{sat}(\phi)$ for some N''_i such that $x\theta =_{\mathsf{AC}} N'_1\oplus\ldots\oplus N'_p$;

3. or there exists a subterm of T_1, of the form $N_1\oplus\ldots\oplus N_p\oplus\bigoplus_{i=1}^{r'} C''_i[M_1,\ldots,M_k]$ (modulo AC), where the head symbols of the C''_i are not $\oplus$ and the C''_i are not a hole, and $x\theta =_{\mathsf{AC}} N'_1\oplus\ldots\oplus N'_p\oplus\bigoplus_{i=1}^{r'} C''_i[M_1,\ldots,M_k]$ with $N_i =_{\mathsf{AC}} N'_i\oplus N''_i\in\mathsf{sat}(\phi)$ for some N''_i, thus the N'_i are subterms of terms of $\mathsf{sat}(\phi)$.

Note that case 3 cannot occur simultaneously with case 1 or case 2 for the same variable x. Indeed, if case 3 occurs simultaneously with case 1 or case 2, we have that some $C''_i[M_1,\ldots,M_k]$ is a subterm of some M_i or M'_i, thus applying recursively rule 2 of Definition 2, we get that $C''_i[M_1,\ldots,M_k]\in\mathsf{sat}(\phi)$, which contradicts property (*) (since C''_i is not a hole).

Without loss of generality, we assume that the variables of M_0 are $x_1,\ldots,x_{k_1},y_1,\ldots,y_{k_2}$ where the variables x_i are in case 1 or case 2 and the variables y_j are in case 3. For each variable y_j, we consider the l occurrences of y_j in T_1.

$$\begin{aligned} y_j\theta &=_{\mathsf{AC}} N_1^1\oplus\ldots\oplus N_{k_1}^1\oplus\textstyle\bigoplus_{i=1}^{r_1} C_i^1[M_1,\ldots,M_k]\\ &\;\vdots\\ &=_{\mathsf{AC}} N_1^l\oplus\ldots\oplus N_{k_l}^l\oplus\textstyle\bigoplus_{i=1}^{r_l} C_i^l[M_1,\ldots,M_k]\end{aligned}$$

where the N_i^j are subterms of terms in $\mathsf{sat}(\phi)$ and the head symbols of the C_i^j are not $\oplus$.

We write $cl(C_i^j[M_1,\ldots,M_k])$ for the class of $C_i^j[M_1,\ldots,M_k]$ modulo AC, and we associate a fresh name symbol $a_{cl(C_i^j[M_1,\ldots,M_k])}$ with the class of each $C_i^j[M_1,\ldots,M_k]$. Therefore, $a_{cl(C_{i_1}^{j_1}[M_1,\ldots,M_k])}$ and $a_{cl(C_{i_2}^{j_2}[M_1,\ldots,M_k])}$ are the same symbol whenever $C_{i_1}^{j_1}[M_1,\ldots,M_k] =_{\mathsf{AC}} C_{i_2}^{j_2}[M_1,\ldots,M_k]$. In each equation

$$\begin{aligned} &N_1^{j_1}\oplus\ldots\oplus N_{k_{j_1}}^{j_1}\oplus\bigoplus_{i=1}^{r_{j_1}} C_i^{j_1}[M_1,\ldots,M_k]\\ &\quad=_{\mathsf{AC}} N_1^{j_2}\oplus\ldots\oplus N_{k_{j_2}}^{j_2}\oplus\bigoplus_{i=1}^{r_{j_2}} C_i^{j_2}[M_1,\ldots,M_k]\end{aligned}$$

every $C_i^{j_1}[M_1,\ldots,M_k]$ must be equal modulo AC to one of the $C_i^{j_2}[M_1,\ldots,M_k]$. Indeed, if $C_i^{j_1}[M_1,\ldots,M_k]$ were equal to some subterm of the $N_i^{j_2}$, $C_i^{j_1}[M_1,\ldots,M_k]$ would be a term of $\mathsf{sat}(\phi)$, contradicting property (*). Thus, we obtain that

$$\begin{aligned} &N_1^1\oplus\ldots\oplus N_{k_1}^1\oplus\textstyle\bigoplus_{i=1}^{r_1} a_{C_i^1[M_1,\ldots,M_k]}\\ &\;\vdots\\ =_{\mathsf{AC}}\;&N_1^l\oplus\ldots\oplus N_{k_l}^l\oplus\textstyle\bigoplus_{i=1}^{r_l} a_{C_i^l[M_1,\ldots,M_k]} \stackrel{\text{def}}{=} T_{y_j}\end{aligned}$$

We consider the substitution θ' such that $x_i\theta' = x_i\theta$ and $y_j\theta' = T_{y_j}$. We define $\theta''(a_{cl(C_i^j[M_1,\ldots,M_k])}) = C_i^j[M_1,\ldots,M_k]$.

We also consider the term T_2 that is obtained from $\bigoplus_{i=1}^{r} C'_i[M_1,\ldots,M_k]$ by replacing each $C_i^j[M_1,\ldots,M_k]$ with $a_{cl(C_i^j[M_1,\ldots,M_k])}$.

We have $T_2 == C_2[S_1,\ldots,S_k]$ for some context C_2 such that $|{}_\oplus C_2|\le|M_0|\le c_E$ and $S_i\in\mathsf{sum}_\oplus(\mathsf{sat}(\phi),\widetilde{n})$. Since $M''\oplus T_2$ is an instance $M_0\theta'$ of M_0 we have $M'\oplus M''\oplus T_2\to_{\mathsf{AC}} M'\oplus N_0\theta'$. Applying condition 3 of Definition 2, there exist $S'_i\in\mathsf{sum}_\oplus(\mathsf{sat}(\phi),\widetilde{n})$, there exists a context C', such that $|C'|\le c_E^2$, $fn(C')\cap\widetilde{n}=\emptyset$, and $M'\oplus N_0\theta'\to^*_{\mathsf{AC}} C'[S'_1,\ldots,S'_l]$. Applying the substitution θ'', we deduce that $M'\oplus N_0\theta =_{\mathsf{AC}} M'\oplus N_0\theta'\theta''\to^*_{\mathsf{AC}}$

$C'[S'_1, \dots, S'_l]\theta''$. Note that $C'[S'_1, \dots, S'_l]\theta''$ is a context of terms of $\mathsf{sat}(\phi)$:

$$C'[S'_1, \dots, S'_l]\theta'' = C''[M_1, \dots, M_k, S'_1, \dots, S'_l]$$

To each sum $S = \alpha_1 M_1 \oplus \cdots \oplus \alpha_n M_n \oplus \beta_1 n_1 \oplus \cdots \oplus \beta_k n_k$ in $\mathsf{sum}_\oplus(\mathsf{sat}(\phi), \widetilde{n})$, we associate the term $\zeta_S = \alpha_1 \cdot_\oplus \zeta_{M_1} \oplus \cdots \oplus \alpha_n \cdot_\oplus \zeta_{M_n} \oplus \beta_1 \cdot_\oplus n_1 \oplus \cdots \oplus \beta_k \cdot_\oplus n_k$.

Now, since the equation $\zeta_{M' \oplus M''} \oplus C_2[\zeta_{S_1}, \dots, \zeta_{S_k}] = C'[\zeta_{S'_1}, \dots, \zeta_{S'_l}]$ is in $\mathsf{Eq}(\phi)$, we deduce

$$(\zeta_{M' \oplus M''} \oplus C_2[\zeta_{S_1}, \dots, \zeta_{S_k}] = C'[\zeta_{S'_1}, \dots, \zeta_{S'_l}])\psi$$

If $a_{cl(C_{i_1}^{j_1}[M_1, \dots, M_k])} = a_{cl(C_{i_2}^{j_2}[M_1, \dots, M_k])}$, we have

$$C_{i_1}^{j_1}[M_1, \dots, M_k] =_{\mathsf{AC}} C_{i_2}^{j_2}[M_1, \dots, M_k]$$

thus (by Lemma 2) we have

$$(C_{i_1}^{j_1}[\zeta_{M_1}, \dots, \zeta_{M_k}] = C_{i_2}^{j_2}[\zeta_{M_1}, \dots, \zeta_{M_k}])\psi$$

So we can reconstruct $M'' \oplus T_1$ and obtain

$$\zeta_{M' \oplus M''} \oplus \bigoplus_{i=1}^{r} C'_i[\zeta_{M_1}, \dots, \zeta_{M_k}] = C''[\zeta_{M_1}, \dots, \zeta_{M_k}, \zeta_{S'_1}, \dots, \zeta_{S'_l}])\psi$$

which allows us to conclude the proof of Lemma 3.