Elementary Deduction Problem for Locally Stable Theories with Normal Forms[*]

Mauricio Ayala-Rincón [†]
Departamentos de Matemática e Computação
Grupo de Teoria da Computação
Universidade de Brasília, Brazil
ayala@unb.br

Maribel Fernández
Department of Informatics
King's College London, UK
maribel.fernandez@kcl.ac.uk

Daniele Nantes-Sobrinho[‡]
Departamento de Matemática
Grupo de Teoria da Computação
Universidade de Brasília, Brazil
dnantes@mat.unb.br

We present an algorithm to decide the intruder deduction problem (IDP) for a class of locally stable theories enriched with normal forms. Our result relies on a new and efficient algorithm to solve a restricted case of higher-order associative-commutative matching, obtained by combining the *Distinct Occurrences of AC-matching* algorithm and a standard algorithm to solve systems of linear Diophantine equations. A translation between natural deduction and sequent calculus allows us to use the same approach to decide the *elementary deduction problem* for locally stable theories. As an application, we model the theory of blind signatures and derive an algorithm to decide IDP in this context, extending previous decidability results.

Introduction

There are different approaches to model cryptographic protocols and to analyse their security properties [17]. One technique consists of proving that an attack requires solving an algorithmically hard problem; another consists of using a process calculus, such as the spi-calculus [3], to represent the operations performed by the participants and the attacker. In recent years, the deductive approach of Dolev and Yao [20], which abstracts from algorithmic details and models an attacker by a deduction system, has successfully shown the existence of flaws in well-known protocols. A deduction system under Dolev-Yao's approach specifies how the attacker can obtain new information from previous knowledge obtained either by eavesdropping the communication between honest protocol participants (in the case of a passive attacker), or by eavesdropping and fraudulently emitting messages (in the case of an active attacker). The *intruder deduction problem* (IDP) is the question of whether a passive eavesdropper can obtain a certain information from messages observed on the network.

Abadi and Cortier's approach [1] proposes conditions for analysing message deducibility and indistinguishability relations for security protocols modelled in the applied pi-calculus [2]. In particular, [1] shows that IDP is decidable for *locally stable* theories. However, to ensure the soundness of this approach, the definition of locally stable theories given in [1] needs to be modified (as confirmed via personal communication with the second author of [1]). In this work, we made the necessary modifications and propose a new approach to solve IDP in the context of locally stable theories.

[*] Work supported by grants from the CNPq/CAPES *Science without Borders* programme and FAPDF PRONEX.

[†] Author partially supported by CNPq.

[‡] Corresponding author. Author supported by CNPq

D. Kesner and P. Viana (Eds.): LSFA 2012
EPTCS 113, 2013, pp. 45–60, doi:10.4204/EPTCS.113.7

Our notion of locally stable theory is based on the existence of a finite and computable saturated set, but, unlike [1], our saturated sets include normal forms[1]. The new approach we propose in order to prove the decidability of IDP is based on an algorithm to solve a restricted case of higher-order associative-commutative matching (AC-matching). To design this algorithm we use well-known results for solving systems of linear Diophantine equations (SLDE) [12, 15, 22, 27], which we combine with a polynomial algorithm to solve the DO-ACM problem (Distinct Occurrences of AC-Matching) [8].

In the case where the signature of the equational theory contains, for each AC function symbol $\oplus$, its corresponding inverse $i_{\oplus}$, we obtain a decidability result which is polynomial with relation to the size of the saturated set (built from the initial knowledge of the intruder). Thanks to the use of the algorithm for solving SLDE over $\mathbb{Z}$, we avoid an exponential time search over the solution space in the case of AC symbols (improving over [1], where an exponential number of possible combinations have to be considered). For more details we refer the reader to the extended version of this paper [5].

After introducing the class of locally stable theories and proving the decidability of the IDP for protocols in this class, we show that the Elementary Deduction Problem (EDP) introduced in [29] is also decidable in polynomial time with relation to the size of a saturated set of terms. EDP is stated as follows: given a set Γ of messages and a message M, is there an E-context $C[\ldots]$ and messages $M_1,\ldots,M_k \in \Gamma$ such that $C[M_1,\ldots,M_k] \approx_E M$? Here, E is the equational theory modelling the protocol. We use this approach to model theories with blind signatures. As an application, using a previous result that links the decidability of the EDP to the decidability of the IDP when the theory E satisfies certain conditions, we obtain decidability of IDP for a subclass of locally stable theories combined with the theory B of blind signatures. In this way, we generalise a result from [1] (Section 5.2.4): it is not necessary to prove that the combination of the theories E and B is locally stable.

Related Work. The analysis of cryptographic protocols has attracted a lot of attention in the last years and several tools are available to try to identify possible attacks, see Maude-NPA [21], ProVerif [10], CryptoVerif [11], Avispa [4], Yapa [7].

Sequent calculus formulations of Dolev Yao intruders [28] have been used in a formulation of open bisimulation for the spi-calculus. In [29], deductive techniques for dealing with a protocol with blind signatures in mutually disjoint AC-convergent equational theories, containing a unique AC operator each, are considered. As an alternative approach, the intruder's deduction capability is modelled inside a sequent calculus modulo a rewriting system, following the approach of [9]. Then, the IDP is reduced in polynomial time to EDP.

By combining the techniques in [29] and [13], the IDP formulation for an Electronic Purse Protocol with blind signatures was proved to reduce in polynomial time to EDP for an AC-convergent theory containing three different AC operators and rules for exponentiation [26], extending the previous results. However, no algorithm was provided to decide EDP. More precisely, assuming that EDP is solved in time $O(f(n))$, it was proved that IDP reduces polynomially to EDP with complexity $O(n^k \times f(n))$, for some constant k. Thus, whenever the former problem is polynomial, the IDP is also polynomial.

Contributions. We present a technique to decide EDP or IDP in AC-convergent equational theories. Our approach is based on a "local stability" property inspired by [1], instead of proving that the deduction rules are "local" in the sense of [25] as done in many previous works [13, 16, 19, 24]. More precisely, the

[1] With this simple modification, the correctness proof in [1] can also be carried out, fixing a gap in Lemma 11.

main contributions of this paper are:

- We adapt and refine the technique proposed in [1], where deducibility and indistinguishability relations are claimed to be decidable in polynomial time for locally stable theories. First, we changed the definition of locally stable theories, adding normal forms, which are needed to carry out the decidability proofs. Second, we designed a new algorithm to decide IDP in locally stable theories. The algorithm provided in [1] is polynomial for the class of subterm theories (Proposition 10 in [1]), but the proof does not extend directly to locally stable theories (despite the statement in Proposition 16). Our algorithm relies on solving a restricted case of higher-order AC-matching problem that is used to decide the deduction relation. It is a combination of two standard algorithms: one for solving the DO-ACM problem [8] which has a polynomial bound in our case; and one for solving systems of Linear Diophantine Equations(SLDE), which is polynomial in $\mathbb{Z}$ [12, 15, 22, 27]. Using this algorithm we prove that IDP is decidable in polynomial time with respect to the saturated set of terms, for locally stable theories with inverses.
- A decidability result for the EDP for locally stable theories, which extends the work of Tiu and Goré [29]. As an application, we present a strategy to decide IDP for locally stable theories combined with blind signatures. Here, the combination of theories does not need to be locally stable.

In order to get the polynomial decidability result claimed in [1] for locally stable theories, we had to restrict to theories that contain, for each *AC* symbol in the signature, the corresponding inverse. The inverses are necessary when we interpret our term algebra inside the integers $\mathbb{Z}$ to solve SLDE (terms headed by the inverse function will be seen as negative integers). If the theory does not contain inverses, we would have to solve the SLDE for $\mathbb{N}$ which is a well known NP-complete problem.

1 Preliminaries

Standard rewriting notation and notions are used (e.g. [6]). We assume the following sets: a countably infinite set N of *names* (we use a,b,c,m to denote names); a countably infinite set X of *variables* (we use x,y,z to denote variables); and a finite *signature* Σ, consisting of function names and their arities. We write $arity(f)$ for the arity of a function f, and let $ar(\Sigma)$ be the maximal arity of a function symbol in Σ.

The set of *terms* is generated by the following grammar:

$$M,N := a\,|\,x\,|\,f(M_1,\ldots,M_n)$$

where f ranges over the function symbols of Σ and n matches the arity of f, a denotes a name in N (representing principal names, nonces, keys, constants involved in the protocol, etc) and x a variable. We denote by $V(M)$ the set of variables occurring in M. A message M is *ground* if $V(M) = \emptyset$. The *size* $|M|$ of a term M is defined by $|u| = 1$, if u is a name or a variable; and $|f(M_1,\ldots,M_n)| = 1+\sum_{i=1}^{n}|M_i|$.

The set of *positions* of a term M, denoted by $\mathscr{P}os(M)$, is defined by $\mathscr{P}os(M) := \{\varepsilon\}$, if M is a name or a variable; and $\mathscr{P}os(M) := \{\varepsilon\} \cup \bigcup_{i=1}^{n}\{ip\,|\,p \in \mathscr{P}os(M_i)\}$, if $M = f(M_1,\ldots,M_n)$ where $f \in \Sigma$. The position ε is called the *root* position. The size of $|M|$ coincides with the cardinality of $\mathscr{P}os(M)$. The set of *subterms* of M is defined as $st(M) = \{M|_p\,|\,p \in \mathscr{P}os(M)\}$, where $M|_p$ denotes the subterm of M at position p. For a set Γ of terms, the notion of subterm can be extended as usual: $st(\Gamma) := \bigcup_{M\in\Gamma} st(M)$. For $p \in \mathscr{P}os(M)$, we denote by $M[t]_p$ the term that is obtained from M by replacing the subterm at position p by t.

A term rewriting system (TRS) is a set $\mathscr{R}$ of oriented equations over terms in a given signature. For terms s and t, $s \rightarrow_{\mathscr{R}} t$ denotes that s rewrites to t using an instance of a rewriting rule in $\mathscr{R}$. The transitive, reflexive-transitive and equivalence closures of $\rightarrow_{\mathscr{R}}$ are denoted by $\overset{+}{\rightarrow}_{\mathscr{R}}, \overset{*}{\rightarrow}_{\mathscr{R}}$ and $\overset{*}{\leftrightarrow}_{\mathscr{R}}$, respectively. The equivalence closure of the rewriting relation, $\overset{*}{\leftrightarrow}_{\mathscr{R}}$, is denoted by $\approx_{\mathscr{R}}$.

Given a TRS $\mathscr{R}$ in which some function symbols are assumed to be AC, and two terms s and t, $s \rightarrow_{\mathscr{R}\cup AC} t$ if there exists w such that $s =_{AC} w$ and $w \rightarrow_{\mathscr{R}} t$, where $=_{AC}$ denotes equality modulo AC (according to the AC assumption on function symbols). For every term s, the set of normal forms $s\downarrow_{\mathscr{R}}$ (closed modulo AC) of s is the set of terms t such that $s \overset{*}{\rightarrow}_{\mathscr{R}\cup AC} t$ and t is irreducible for $\rightarrow_{\mathscr{R}\cup AC}$. $\mathscr{R}$ is said to be AC-convergent whenever it is AC-terminating and AC-confluent.

We equip the signature Σ with an equational theory $\approx_E$ induced by a set of Σ-equations E, that is, $\approx_E$ is the smallest equivalence relation that contains E and is closed under substitutions and compatible with Σ-contexts. An equational theory $\approx_E$ is said to be equivalent to a TRS $\mathscr{R}$ whenever $\approx_{\mathscr{R}} = \approx_E$. An equational theory $\approx_E$ is AC-convergent when it has an equivalent rewrite system $\mathscr{R}$ which is AC-convergent. In the next sections, given an AC-convergent equational theory $\approx_E$, normal forms of terms are computed with respect to the TRS $\mathscr{R}$ associated to $\approx_E$, unless otherwise specified. To simplify the notation we will denote by E the equational theory induced by the set of Σ-equations E. We will denote by Σ_E the signature used in the set of equations E. The *size* c_E of an equational theory E with an associated TRS $\mathscr{R}$ consisting of rules $\bigcup_{i=1}^{k}\{l_i \rightarrow r_i\}$ is defined as $c_E = max_{1\leq i\leq k}\{|l_i|, |r_i|, ar(\Sigma)+1\}$. For $\mathscr{R} = \emptyset$, define $c_E = ar(\Sigma)+1$.

Let $\Box$ be a new symbol which does not yet occur in $\Sigma \cup X$. A Σ-*context* is a term $t \in T(\Sigma, X \cup \{\Box\})$ and can be seen as a term with “holes”, represented by $\Box$, in it. Contexts are denoted by C. If $\{p_1,\dots,p_n\} = \{p \in \mathscr{P}os(C) \,|\, C|_p = \Box\}$, where p_i is to the left of p_{i+1} in the tree representation of C, then $C[T_1 \dots, T_n] := C[T_1]_{p_1} \dots [T_n]_{p_n}$. In what follows a context formed using only function symbols in Σ_E will be called an E-*context* to emphasize the equational theory E.

A term M is said to be an E-*alien* if M is headed by a symbol $f \notin \Sigma_E$ or a private name/constant. We write $M == N$ to denote syntactic equality of ground terms.

In the rest of the paper, we use signatures, terms and equational theories to model protocols. *Messages* exchanged between participants of a protocol during its execution are represented by terms. Equational theories and rewriting systems are used to model the cryptographic primitives in the protocol and the algebraic capabilities of an intruder.

2 Deduction Problem

Given a set Γ that represents the information available to an attacker, we may ask whether a given ground term M may be deduced from Γ using equational reasoning. This relation is written $\Gamma \vdash M$ and axiomatised in a natural deduction like system of inference rules.

Table 1: System $\mathscr{N}$: a natural deduction system for intruder equational deduction

$$\frac{M \in \Gamma}{\Gamma \vdash M}\,(id) \qquad \frac{\Gamma \vdash M_1 \;\ldots\; \Gamma \vdash M_n}{\Gamma \vdash f(M_1,\ldots,M_n)}\,(f_I)\; f \in \Sigma_E \qquad \frac{\Gamma \vdash N}{\Gamma \vdash M}\,(\approx) M \approx_E N$$

2.1 Locally Stable Theories

Let $\oplus$ be an arbitrary function symbol in Σ_E for an equational theory E. We write $\alpha \cdot_{\oplus} M$ for the term $M \oplus \ldots \oplus M$, α times ($\alpha \in \mathbb{N}$). Given a set S of terms, we write $sum_{\oplus}(S)$ for the set of arbitrary sums of terms in S, closed modulo AC:

$$sum_{\oplus}(S) = \{(\alpha_1 \cdot_{\oplus} T_1) \oplus \ldots \oplus (\alpha_n \cdot_{\oplus} T_n) \mid \alpha_i \geq 0, T_i \in S\}$$

Define $sum(S) = \bigcup_{i=1}^{k} sum_{\oplus_i}(S)$, where $\oplus_1,\ldots,\oplus_k$ are the AC-symbols of the theory.

For a rule $l \to r \in \mathscr{R}$ and a substitution θ such that

- either there exists a term s_1 such that $s =_{AC} s_1$, $s_1 =_{AC} l\theta$ and $t = r\theta$;
- or there exist terms s_1 and s_2 such that $s =_{AC} s_1 \oplus s_2$, $s_1 =_{AC} l\theta$ and $t =_{AC} r\theta \oplus s_2$.

we write $s \xrightarrow{h} t$ and say that the reduction occurs in the head.

As in [1] we associate with each set Γ of messages, a set of subterms in Γ that may be deduced from Γ by applying only "small" contexts. The concept of small is arbitrary — in the definition below, we have bound the size of an E-context C by c_E and the size of C' by c_E^2, but other bounds may be suitable. Notice that limiting the size of an E-context by c_E makes the context big enough to be an instance of any of the rules in the TRS $\mathscr{R}$ associated to E.

Definition 1 (Locally Stable)**.** *An AC-convergent equational theory E is* locally stable *if, for every finite set $\Gamma = \{M_1,\ldots,M_n\}$, where the terms M_i are ground and in normal form, there exists a finite and computable set $sat(\Gamma)$, closed modulo AC, such that*

1. $M_1,\ldots,M_n \in sat(\Gamma)$;
2. *if* $M_1,\ldots,M_k \in sat(\Gamma)$ *and* $f(M_1,\ldots,M_k) \in st(sat(\Gamma))$ *then* $f(M_1,\ldots,M_k) \in sat(\Gamma)$, *for* $f \in \Sigma_E$;
3. *if* $C[S_1,\ldots,S_l] \xrightarrow{h} M$, *where C is an E-context such that* $|C| \leq c_E$, *and* $S_1,\ldots,S_l \in sum_{\oplus}(sat(\Gamma))$, *for some AC symbol* $\oplus$, *then there exist an E-context* C', *a term* M', *and terms* $S'_1,\ldots,S'_k \in sum_{\oplus}(sat(\Gamma))$, *such that* $|C'| \leq c_E^2$, *and* $M \xrightarrow{*}_{\mathscr{R}\cup AC} M' =_{AC} C'[S'_1,\ldots,S'_k]$;
4. *if* $M \in sat(\Gamma)$ *then* $M\!\downarrow \in sat(\Gamma)$.
5. *if* $M \in sat(\Gamma)$ *then* $\Gamma \vdash M$.

Notice that the set $sat(\Gamma)$ may not be unique. Any set $sat(\Gamma)$ satisfying the five conditions is adequate for the results.

Remark 1. *The addition of rule 4 in the Definition 1 is necessary to prove case 1b of Lemma 1, where the rewriting reduction occurs in a term $M_i \in sat(\Gamma)$ in a position different from the "head". Normal forms are strictly necessary in the set $sat(\Gamma)$, they are essential to lift the applications of rewriting rules in the head of "small" contexts to applications of rewriting rules in arbitrary positions of "small" contexts. With this additional condition, Lemma 11 in [1] can also be proved. This fact was confirmed via personal communication with the second author of [1].*

The lemma and the corollary below, adapted from [1], are used in the proof of Theorem 2.

Lemma 1. *Let E be a locally stable theory and $\Gamma = \{M_1, \ldots, M_n\}$ a set of ground terms in normal form. For every E-context C_1, for every $M_i \in sat(\Gamma)$, for every term T such that $C_1[M_1, \ldots, M_k] \rightarrow_{\mathscr{R}\cup AC} T$, there exist an E-context C_2, and terms $M_i' \in sat(\Gamma)$, such that $T \xrightarrow{*}_{\mathscr{R}\cup AC} C_2[M_1', \ldots, M_l']$.*

Proof. Suppose that $C_1[M_1, \ldots, M_k] \rightarrow_{AC} T$, for an E-context C_1 and $M_i \in sat(\Gamma)$. The proof is divided in two cases:

1. The reduction happens inside one of the terms M_i:
   (a) if $M_i \xrightarrow{h} M_i'$ then by definition of $sat(\Gamma)$ (since E is locally stable), there exist an E-context C such that $|C| \leq c_E^2$ and $M_i' \xrightarrow{*} C[S_1, \ldots, S_l]$ where $S_j \in sum_{\oplus}(sat(\Gamma))$.
   Each $S_j \in sum_{\oplus}(sat(\Gamma))$ is of the form $S_j = (\alpha_1 \cdot_{\oplus} M_{j_1}) \oplus \ldots \oplus (\alpha_n \cdot_{\oplus} M_{j_n})$, for $M_{j_k} \in sat(\Gamma)$. That is, $S_j = C_j[M_{j_1}, \ldots, M_{j_k}]$, for $1 \leq j \leq l$. Therefore,
   $$\begin{aligned} C_1[M_1, \ldots, M_i, \ldots, M_k] \xrightarrow{h} C_1[M_1, \ldots, M_i', \ldots, M_k] \xrightarrow{*}_{AC} C_1[M_1, \ldots, C[S_1, \ldots, S_l], \ldots, M_k] \\ =_{AC} C_2[M_1^{''}, \ldots, M_s^{''}], \end{aligned} \tag{1}$$
   where $M_t^{''} \in sat(\Gamma)$, for $1 \leq t \leq s$.
   (b) if $M_i \rightarrow_{AC} M_i'$ in a position different from “head”, then
   $$C_1[M_1, \ldots, M_i, \ldots, M_k] \rightarrow C_1[M_1, \ldots, M_i', \ldots, M_k] \xrightarrow{*}_{AC} C_1[M_1, \ldots, M_i\downarrow, \ldots, M_k].$$
   By case 4 in Definition 1, $M_i\downarrow \in sat(\Gamma)$.
2. The case where the reduction does not occur inside the terms M_i: this case if very technical and will be omitted here. The complete proof can be found in the extended version of this paper.

□

As a consequence we obtain the following Corollary:

Corollary 1 ([1]). *Let E be a locally stable theory. Let $\Gamma = \{M_1, \ldots, M_n\}$ be a set of ground terms in normal form. For every E-context C_1, for every $M_i' \in sat(\Gamma)$, for every T in normal form such that $C_1[M_1', \ldots, M_k'] \xrightarrow{*}_{\mathscr{R}\cup AC} T$, there exist an E-context C_2 and terms $M_j{}'' \in sat(\Gamma)$ such that $T =_{AC} C_2[M_1^{''}, \ldots, M_l^{''}]$.*

Proof. The proof is the same as in [1]. □

In the following we show that any term M deducible from Γ is equal modulo AC to an E-context over terms in $sat(\Gamma)$.

Lemma 2 ([1]). *Let E be a locally stable theory. Let $\Gamma = \{M_1, \ldots, M_n\}$ be a finite set of ground terms in normal form, and M be a ground term in normal form. Then $\Gamma \vdash M$ if and only if there exist an E-context C and terms $M_1', \ldots, M_k' \in sat(\Gamma)$ such that $M =_{AC} C[M_1^{'}, \ldots, M_n^{'}]$.*

Proof. The proof is the same as in [1]. □

As a consequence of the previous results decidability of IDP for locally stable theories is obtained:

Theorem 1. *The Intruder Deduction Problem is decidable for locally stable theories.*

In the next section we will provide a complexity bound for the decidability of the intruder deduction problem for a restricted case of locally stable theories.

3 Locally Stable Theories with Inverses

In order to obtain the polynomial complexity bound of our decidability algorithm we will need to consider the existence of inverses for each *AC* symbol in the signature of our equational theory. Our algorithm will rely on solving systems of linear Diophantine equations over $\mathbb{Z}$ and the inverses will be interpreted as *negative integers*.

(*) *In the following results, let E be a locally stable theory whose signature Σ_E contains, for each AC function symbol $\oplus$, its corresponding* inverse $i_\oplus$.

That is, the following results are related to equational theories E containing the following equation:

$$x \oplus i_\oplus(x) = e_\oplus \tag{2}$$

for each AC-symbol $\oplus$ in Σ_E, where $i_\oplus$ is the unary function symbol representing the inverse of $\oplus$ and $e_\oplus$ is the corresponding neutral element.

Definition 2 (Locally Stable with Inverses)**.** *An AC-convergent equational theory E satisfying (*) is* locally stable *if, for every finite set $\Gamma = \{M_1, \ldots, M_n\}$, where the terms M_i are ground and in normal form, there exists a finite and computable set $sat(\Gamma)$, closed modulo AC, such that*

1. *$M_1, \ldots, M_n \in sat(\Gamma)$, $e_\oplus \in sat(\Gamma)$ for each $\oplus \in \Sigma_E$;*
2. *if $M_1, \ldots, M_k \in sat(\Gamma)$ and $f(M_1, \ldots, M_k) \in st(sat(\Gamma))$ then $f(M_1, \ldots, M_k) \in sat(\Gamma)$, for $f \in \Sigma_E$;*
3. *if $C[S_1, \ldots, S_l] \xrightarrow{h} M$, where C is an E-context such that $|C| \leq c_E$, and $S_1, \ldots, S_l \in sum_\oplus(sat(\Gamma))$, for some AC symbol $\oplus$, then there exist an E-context C', a term M', and terms $S'_1, \ldots, S'_k \in sum_\oplus(sat(\Gamma))$, such that $|C'| \leq c_E^2$, and $M \xrightarrow{*}_{\mathscr{R} \cup AC} M' =_{AC} C'[S'_1, \ldots, S'_k]$;*
4. *if $M \in sat(\Gamma)$ then $M \downarrow \in sat(\Gamma)$.*
5. *if $M \in sat(\Gamma)$ then $i_\oplus(M) \downarrow \in sat(\Gamma)$ for each AC symbol $\oplus$ in E.*
6. *if $M \in sat(\Gamma)$ then $\Gamma \vdash M$.*

Based on a well-founded ordering over the symbols in the language, we prove that a restricted case of higher-order AC-matching ("is there an E-context C such that $M =_{AC} C[M_1, \ldots, M_k]$ for some $M_1, \ldots, M_k \in sat(\Gamma)$?") can be solved in polynomial time in $|sat(\Gamma)|$ and $|M|$. This AC-matching problem is solved using the DO-ACM (Distinct-Occurrences of AC-matching) [8], where every variable in the term being matched occurs only once. In addition, we also use a standard and polynomial time algorithm for solving SLDE over $\mathbb{Z}$ [12, 15, 22, 27].

To facilitate the description of the algorithm below we have considered only one AC-symbol $\oplus$ whose corresponding inverse will be denoted by i. The proof can be extended similarly for theories with multiple AC-symbols each one with its corresponding inverse.

Lemma 3. *Let E be a locally stable theory satisfying (*), $\Gamma = \{M_1, \ldots, M_n\}$ a finite set of ground messages in normal form and M a ground term in normal form. Then the question of whether there exists an E-context C and $T_1, \ldots, T_k \in sat(\Gamma)$ such that $M =_{AC} C[T_1, \ldots, T_k]$ is decidable in polynomial time in $|M|$ and $|sat(\Gamma)|$.*

Proof. Given Γ, we construct the set $sat(\Gamma) = \{T_1, \dots, T_s\}$, which is computable and finite by Definition 1. We can then check whether $M \overset{?}{=}_{AC} C[T_1, \dots, T_k]$ for some E-context C and terms $T_1, \dots, T_k \in sat(\Gamma)$ using the following algorithm which is divided in its main component A), and procedures B) and C) for reducing linear Diophantine equations and selecting T_i's from $sat(\Gamma)$, respectively.

A) **Algorithm 1.**

1. For all positions p in M headed by $\oplus$ starting from the longest positions in decreasing order (positions seen as sequences) solve the *system of linear Diophantine equations* (see part B below) for $M|_p$ with $sat(\Gamma) \cup S$, where S is built incrementally from $sat(\Gamma)$, starting with $S_0 = \emptyset$, including all $M|_p$ that have solutions. In other words:

   Let $\mathscr{P}' = \{p_1, \dots, p_t\}$ be the set of positions of M such that $M|_p$ is headed with $\oplus$, organised in decreasing order. For each $p_j \in \mathscr{P}'$ let $M|_{p_j}$ be the subterm of M such that

   $$M|_{p_j} = n_{j_1} \oplus \dots \oplus n_{j_{kj}} \ (j = 1, \dots, t)$$

   Recursively find, but suppressing step 1 in this recursive call, solutions for the arguments $n_{j_{i_1}}, \dots, n_{j_{i_l}}$ of $M|_{p_j}$ with $n_{j_{im}} \in \{n_{j_1}, \dots, n_{j_{k_j}}\}$ with respective E-contexts $C_{j_{i_1}}, \dots, C_{j_{i_l}}$ such that

   $$n_{j_{im}} = C_{j_{im}}[T_1, \dots, T_{s_{im}}]$$

   where $T_q \in sat(\Gamma) \cup S_{j-1}$, $q = 1, \dots, s_{i_m}$.

   Then one checks satisfiability of the SLDE generated from $M|_{p_j}$ and $sat(\Gamma) \cup S_{j-1} \cup \{n_{j_{i_1}}, \dots, n_{j_{k_l}}\}$ (see steps B and C).

   If there is a solution then $S_j := S_{j-1} \cup \{n_{j_{i_1}}, \dots, n_{j_{k_l}}\} \cup \{M|_{p_j}\}$

2. Let $S := S_t$. Classify the terms in $sat(\Gamma) \cup S$ by size.

3. For each term $T_i \in sat(\Gamma) \cup S$ (from terms of maximal size to terms of minimal size) check:

   - For each position $q \in \mathscr{P}os(M)$ such that $T_i =_{AC} M|_q$ do
     Check whether the path between T_i and the root of M contains a $\oplus$:
     - if NOT, then delete $M|_q$ from M and move to T_{i+1}.
     - if YES (there is a $\oplus$) then M has a subterm N such that $N = n_1 \oplus \dots \oplus n_j[T_i] \oplus \dots \oplus n_k$ and N cannot be constructed from $sat(\Gamma) \cup S$. Therefore, M cannot be written as an E-context with terms from $sat(\Gamma)$.

4. Check whether the remaining part of M still contains E-aliens. If it is not the case, we have found an E-context C and terms $M_1, \dots, M_k \in sat(\Gamma)$ and $M =_{AC} C[M_1, \dots, M_k]$; otherwise such an E-context does not exist.

B) **Reduction to linear Diophantine equations.**

First, notice that, for each position p such that $M|_p$ is headed with $\oplus$ we have

$$M|_p = \alpha_1 m_1 \oplus \dots \oplus \alpha_r m_r \, , \, \alpha_j \in \mathbb{N} \tag{3}$$

where m_j is not headed with $\oplus$ and $\alpha_j m_j$ counts for $\underbrace{m_j \oplus \dots \oplus m_j}_{\alpha_j - times}$.

We want to prove that there are $\beta_1,\dots,\beta_q \in \mathbb{N}$ such that

$$\beta_1 T_1 \oplus \dots \oplus \beta_q T_q =_{AC} M|_p = \alpha_1 m_1 \oplus \dots \oplus \alpha_r m_r \tag{4}$$

This AC-equality is only possible when $T_i = \gamma_{1i} m_1 \oplus \dots \oplus \gamma_{ri} m_r$ for each i, $1 \leq i \leq q \leq s$ and $\gamma_{j_i} \in \mathbb{N}$.

That is, $\beta_1 T_1 \oplus \dots \oplus \beta_q T_q =_{AC} \alpha_1 m_1 \oplus \dots \oplus \alpha_r m_r$ if and only if

$$\begin{aligned} &\beta_1(\gamma_{1_1} m_1 \oplus \dots \oplus \gamma_{r_1} m_r) \oplus \beta_2(\gamma_{1_2} m_1 \oplus \dots \oplus \gamma_{r_2} m_r) \oplus \dots \\ &\dots \oplus \beta_q(\gamma_{1_q} m_1 \oplus \dots \oplus \gamma_{r_q} m_r) = \alpha_1 m_1 \oplus \dots \oplus \alpha_r m_r \end{aligned} \tag{5}$$

if and only if

$$\begin{aligned} &(\gamma_{1_1}\beta_1 \oplus \gamma_{1_2}\beta_2 \dots \oplus \gamma_{1_q}\beta_q) m_1 \oplus (\gamma_{2_1}\beta_1 \oplus \gamma_{2_2}\beta_2 \dots \oplus \gamma_{2_q}\beta_q) m_2 \oplus \dots \\ &\dots (\gamma_{r_1}\beta_1 \oplus \gamma_{r_2}\beta_2 \dots \oplus \gamma_{r_q}\beta_q) m_r = \alpha_1 m_1 \oplus \dots \oplus \alpha_r m_r \end{aligned} \tag{6}$$

if and only if

$$S = \begin{cases} \gamma_{1_1}\beta_1 \oplus \gamma_{1_2}\beta_2 \dots \oplus \gamma_{1_q}\beta_q = \alpha_1 \\ \gamma_{2_1}\beta_1 \oplus \gamma_{2_2}\beta_2 \dots \oplus \gamma_{2_q}\beta_q = \alpha_2 \\ \qquad\qquad \vdots \\ \gamma_{r_1}\beta_1 \oplus \gamma_{r_2}\beta_2 \dots \oplus \gamma_{r_q}\beta_q = \alpha_r \end{cases} \tag{7}$$

where S is a system of linear Diophantine equations over $\mathbb{Z}$ which can be solved in polynomial time [12, 15, 22, 27].

Remark 2. *We will interpret the equations 3 and 4 inside integer arithmetic. If there exists an index j such that $m_j = i(m'_j)$ and m'_j is not headed with i then $\alpha_j m_j = \alpha_j(i(m'_j))$ and we will take it as $(-\alpha_j)m'_j$. Therefore, we can take $\alpha_j \in \mathbb{Z}$, for all j. We can use the same reasoning to conclude that $\beta_j \in \mathbb{Z}$, for all $1 \leq j \leq q$ and $\gamma_{j_i} \in \mathbb{Z}$, for all i and j.*

C) **Selecting the $T'_j s$ from $sat(\Gamma)$.**

For each $T_i \in sat(\Gamma)$, $1 \leq i \leq s$ we want to check if $T_i = \gamma_{1_i} m_1 \oplus \dots \oplus \gamma_{r_i} m_r$.

Algorithm 2:

For each $T_i \in sat(\Gamma)$, $1 \leq i \leq s$, solve the equation $T_i \oplus x_i =_{AC} \alpha_1 m_1 \oplus \dots \oplus \alpha_r m_r$ where x_i is a fresh variable.

Since the $T'_i s$ and M are ground terms, this equation can be seen as an instance of the DO-ACM matching problem which can be solved in time $\mathscr{O}(|T_i \oplus x_i|.|M|_p|)$ [8].

If there exists $T_i \in sat(\Gamma)$ such that $T_i = \gamma^*_{1_i} m_1 \oplus \dots \oplus \gamma^*_{r_i} m_r \oplus u$, where u is not empty, $\gamma^*_{i_j} \in \mathbb{N}$ and the **Algorithm 2** can no longer be applied then T_i will not be selected.

Notice that each step of the algorithm can be done in polynomial time in $|M|$ and $|sat(\Gamma)|$. Therefore, the whole procedure is polynomial in $|M|$ and $sat(\Gamma)$. □

Remark 3. *For the proof we can adopt an ordering in which, for instance, variables are smaller than constants, constants smaller than function symbols, and function symbols are also ordered, but other suitable order can be used. Terms are compared by the associated lexicographical ordering built from this ordering on symbols.*

Example 1 (Finite Abelian Groups). *We consider the theory of Abelian Groups where the signature is $\Sigma_{AG} = \{+, 0, i\}$ for i the inverse function and $+$ the AC group operator. The equational theory E_{AG} is:*

$$E_{AG} = \left\{ \begin{array}{rcl} x+(y+z) & = & (x+y)+z \\ x+y & = & y+x \\ i(x+y) & = & i(y)+i(x) \end{array} \right. \qquad \begin{array}{rcl} x+0 & = & x \\ x+i(x) & = & 0 \end{array} \qquad \begin{array}{rcl} i(i(x)) & = & x \\ i(0) & = & 0 \end{array}$$

We define $\mathscr{R}_{AG}$ by orienting the equations from left to right (excluding the equations for associativity and commutativity). $\mathscr{R}_{AG}$ is AC-convergent. The size $c_{E_{AG}}$ of the theory is at least 5. In the following prove that E_{AG} is locally stable with inverses for finite models, i.e., we define a set $sat(\Gamma)$ satisfying the properties in the Definition 1. For a given set $\Gamma = \{M_1, \dots, M_k\}$ of ground terms in normal form, $sat(\Gamma)$ is the smallest set such that:

1. *$M_1, \dots, M_k \in sat(\Gamma)$;*
2. *$M_1, \dots, M_k \in sat(\Gamma)$ and $f(M_1, \dots, M_k) \in st(sat(\Gamma))$ then $f(M_1, \dots, M_k) \in sat(\Gamma)$, $f \in \Sigma_{AG}$;*
3. *if $M_i, M_j \in sat(\Gamma)$ and $M_i + M_j \xrightarrow{h} M$ via rule $x + i(x) \to 0$ then $M \downarrow \in sat(\Gamma)$;*
4. *if $M_j \in sat(\Gamma)$ then $i(M_j) \downarrow \in sat(\Gamma)$;*
5. *if $M_i =_{AC} M_j$ and $M_i \in sat(\Gamma)$ then $M_j \in sat(\Gamma)$.*

The set $sat(\Gamma)$ defined for Finite Abelian Groups is finite.

Although it was said in [1] that the theory of Abelian Groups is locally stable, no proof of such fact was found in the literature. With the proviso that the Abelian Group under consideration is finite, we have demonstrated that $|sat(\Gamma)|$ is exponential in the size of $|\Gamma|$.

These results give rise to the decidability of deduction for locally stable theories. Notice that polynomiality on $|sat(\Gamma)|$ relies on the use of the AC-matching algorithm proposed in Lemma 3. Unlike [1], we do not need to compute of the congruence class modulo AC of M (which may be exponential). This gives us a slightly different version of the decidability theorem:

Theorem 2. *Let E be a locally stable theory satisfying (*). If $\Gamma = \{M_1, \dots, M_n\}$ is a finite set of ground terms in normal form and M is a ground term in normal form, then $\Gamma \vdash M$ is decidable in polynomial time in $|M|$ and $|sat(\Gamma)|$.*

Proof. The result follows directly from Lemmas 3 and 2. □

In the following example we consider the *Pure AC-theory* which can be proven to be locally stable but does not contain the inverse of the AC-symbol $+$.

Example 2 (Pure *AC* Theory). *Σ_{AC} contains only constant symbols, the AC-symbol $\oplus$ and the equational theory contains only the AC equations for $\oplus$:*

$$AC = \left\{ \; x \oplus y = y \oplus x \qquad\qquad x \oplus (y \oplus z) = (x \oplus y) \oplus z \; \right\}$$

In this case, $E = AC$ and $\mathscr{R} = \emptyset$ is the AC-convergent TRS associated to E. Let $\Gamma = \{M_1, \dots, M_k\}$ be a finite set of ground terms in normal form. Let us define $sat(\Gamma)$ for the pure AC theory as the smallest set such that

1. *$M_1,\ldots,M_k \in sat(\Gamma)$;*
2. *if $M_i, M_j \in sat(\Gamma)$ and $M_i \oplus M_j \in st(sat(\Gamma))$ then $M_i \oplus M_j \in sat(\Gamma)$.*
3. *if $M_i =_{AC} M_j$ and $M_i \in sat(\Gamma)$ then $M_j \in sat(\Gamma)$.*

The set $sat(\Gamma)$ is finite since we add only terms whose size is smaller or equal than the maximal size of the terms in Γ. It is easy to see that the set $sat(\Gamma)$ satisfies the rules 1,2, 4 and 5. Since $\mathscr{R} = \emptyset$ it follows that 3 is also satisfied. Therefore, AC is locally stable.

The size of $sat(\Gamma)$:

- *Steps 1 and 2: only subterms in $sat(\Gamma)$ are added.*
- *Step 3: for each $M_i \in sat(\Gamma)$ add $M_j =_{AC} M_i \in sat(\Gamma)$. Notice that the number of terms added in $sat(\Gamma)$, in this case, depends on the number of occurrences of $\oplus$ in M_i. Suppose that M_i contains n occurrences of $\oplus$:*

  $$M_i = M_{i_1} \oplus \ldots \oplus M_{i_{n+1}}.$$

  There are $(n+1)!$ terms M_j such that $M_1 =_{AC} M_j$.

Suppose that each M_i in Γ contains n_i occurrences of $\oplus$.Then, $|M_i| = \sum_{j=1}^{n_i+1} |M_{i_j}| + n_i$. Let $n = \max_{1\leq i\leq k}\{n_i\}$. There exists an index r such that M_r contains $n_r = n$ occurrences of $\oplus$. Since $|\Gamma| = \sum_{i=1}^{k} |M_i|$ it follows that $n \leq |M_r| - \sum_{j=1}^{n+1} |M_{r_j}| \leq |\Gamma|$. Then the number of terms added in step 3 is $\sum_{i=1}^{k}(n_i+1)! \leq (n+1)! \cdot k \leq (|\Gamma|+1)! \cdot k$.

Remark 4. *In this case one can adapt Lemma 3 such that the algorithm would rely on solving systems of linear Diophantine equations over $\mathbb{N}$ which is NP-complete [27]. Therefore, the complexity of IDP for pure AC would be exponential, agreeing with previous results [23].*

4 Elementary Deduction Problem for Locally Stable Theories

To establish necessary concepts for the next results, we recall the well-known translation between natural deduction and sequent calculus systems to model the IDP as a proof search in sequent calculus, whose properties (such as cut or subformula) facilitate the study of decidability of deductive systems. For an AC-convergent equational theory E, the System $\mathscr{N}$ in Table 1 is equivalent to the (id)-rule of the sequent calculus (Table 2) introduced in [29]:

$$\frac{\overset{M\approx_E C[M_1,\ldots,M_k]}{\text{C[ ] an E-context, and } M_1,\ldots,M_k \in \Gamma}}{\Gamma \vdash M}\,(id)$$

Consequently, IDP for System $\mathscr{N}$ is equivalent to the *Elementary Deduction Problem*:

Definition 3. *Given an AC-convergent equational theory E and a sequent $\Gamma \vdash M$ ground and in normal form, the* elementary deduction problem *(EDP) for E, written $\Gamma \Vdash_E M$, is the problem of deciding whether the (id)-rule is applicable in $\Gamma \vdash M$.*

The theorem below decides EDP for locally stable theories :

Theorem 3. *Let E be a locally stable equational theory satisfying (*). Let $\Gamma \vdash M$ be a ground sequent in normal form. The* elementary deduction problem *for the theory E ($\Gamma \Vdash_E M$) is decidable in polynomial time in $|sat(\Gamma)|$ and $|M|$.*

Proof. By Lemma 3, the problem whether $M =_{AC} C[M_1,\dots,M_k]$ for an E-context C and terms $M_1,\dots,M_k \in sat(\Gamma)$ is decidable in polynomial time in $|sat(\Gamma)|$ and $|M|$. If $M =_{AC} C[M_1,\dots,M_k]$ for an E-context C and terms $M_1,\dots,M_k \in sat(\Gamma)$ then there exist an E-context C' and terms $M'_1,\dots,M'_n \in \Gamma$ such that $C[M'_1,\dots,M'_n] \overset{*}{\to}_{\mathscr{R}\cup AC} M$. It is enough to observe that for all $T \in sat(\Gamma)$, T can be constructed from the terms in Γ.

If there is no E-context C and terms $M_1,\dots,M_k \in sat(\Gamma)$ such that $M =_{AC} C[M_1,\dots,M_k]$ then, by Corollary 1, there are no E-context and terms $M'_1,\dots,M'_t \in sat(\Gamma)$ such that $C[M'_1,\dots,M'_t] \overset{*}{\to}_{\mathscr{R}\cup AC} M$. Therefore, there is no E-context C'' and terms $M''_1,\dots,M''_l \in \Gamma$ such that $C''[M''_1,\dots,M''_l] \overset{*}{\to}_{\mathscr{R}\cup AC} M$. Thus, the EDP for E is decidable in polynomial time in $|sat(\Gamma)|$ and $|M|$. □

4.1 Extension with Blind Signatures

Blind signature is a basic cryptographic primitive in e-cash. This concept was introduced by David Chaum in [14] to allow a bank (or anyone) sign messages without seeing them. David Chaum's idea was to use this homomorphic property in such a way that Alice can multiply the original message with a random (encrypted) factor that will make the resulting image meaningless to the Bank. If the Bank agrees to sign this random-looking data and return it to Alice, she is able to divide out the blinding factor such that the Bank's signature in the original message will appear.

Given a locally stable equational theory E, we extend the signature Σ_E with Σ_C, a set containing function symbols for "constructors" for blind signatures, in order to obtain decidability results for the extension of the IDP for System $\mathscr{N}$ taking into account some rules for blind signatures.

Extended Syntax

The signature Σ consists of function symbols and is defined by the union of two sets: $\Sigma = \Sigma_C \cup \Sigma_E$ (with $\Sigma_{\mathsf{E}} \cap \Sigma_C = \emptyset$), where

$$\Sigma_C = \{\mathsf{pub}(\_), \mathsf{sign}(\_,\_), \mathsf{blind}(\_,\_), \{\_\}_\_, <\_,\_>\}$$

represents the *constructors*, whose interpretations are: $\mathsf{pub}(M)$ gives the public key generated from a private key M; $\mathsf{blind}(M,N)$ gives M encrypted with N using blinding encryption; $\mathsf{sign}(M,N)$ gives M signed with a private key N; $\{M\}_N$ gives M encrypted with the key N using Dolev-Yao symmetric encryption; $\langle M,N\rangle$ constructs a pair of terms from M and N. Then the extended grammar of the set of *terms* or messages is given as

$$M,N := a \mid x \mid f(M_1,\dots,M_n) | \mathsf{pub}(M) | \mathsf{sign}(M,N) | \mathsf{blind}(M,N) | \{M\}_N | \langle M,N\rangle$$

Notice that, with the extension an E-alien term M is a term headed with $f \in \Sigma_C$ or M is a private name/constant. An E-alien subterm M of N is said to be an E-*factor* of N if there is another subterm F of N such that M is an immediate subterm of F and F is headed by a symbol $f \in \Sigma_E$. This notion can be extended to sets in the obvious way: a term M is an E-factor of Γ if it is an E-factor of a term in Γ. These notions were introduced in [29].

The operational meaning of each constructor will be defined by their corresponding inference rules in the sequent calculus to be described.

Extending the EDP to Model Blind Signatures

Following the approach proposed in [29], we extend EDP with blind signatures using the sequent calculus $\mathscr{S}$ described in Table 2. In this way, we can model intruder deduction for the combination of a locally stable theory E with blind signatures in a modular way: the theory E is used in the *id* rule, while blind signatures are modelled with additional deduction rules. As shown below, this approach has the advantage that we can derive decidability results for the intruder deduction problem without needing to prove that the combined theory is locally stable (in contrast with the results in the previous section and in [1]).

Table 2: System $\mathscr{S}$: Sequent Calculus for the Intruder

$$\frac{\overset{M\approx_E C[M_1,\ldots,M_k]}{\text{C[ ] an E-context,}M_1,\ldots,M_k\in\Gamma}}{\Gamma\vdash M}\,(id) \qquad \frac{\Gamma\vdash M \qquad \Gamma,M\vdash T}{\Gamma\vdash T}\,(cut)$$

$$\frac{\Gamma,\langle M,N\rangle,M,N\vdash T}{\Gamma,\langle M,N\rangle\vdash T}\,(p_L) \qquad \frac{\Gamma\vdash M \qquad \Gamma\vdash N}{\Gamma\vdash\langle M,N\rangle}\,(p_R)$$

$$\frac{\Gamma\vdash M \qquad \Gamma\vdash K}{\Gamma\vdash\{M\}_K}\,(e_R) \qquad \frac{\Gamma,\{M\}_K\vdash K \qquad \Gamma,\{M\}_K,M,K\vdash N}{\Gamma,\{M\}_K\vdash N}\,(e_L)$$

$$\frac{\Gamma\vdash M \qquad \Gamma\vdash K}{\Gamma\vdash\mathsf{sign}(M,K)}\,(\mathsf{sign}_R) \qquad \frac{\Gamma\vdash M \qquad \Gamma\vdash K}{\Gamma\vdash\mathsf{blind}(M,K)}\,(\mathsf{blind}_R)$$

$$\frac{\Gamma,\mathsf{sign}(M,K),\,\mathsf{pub}(L),M\vdash N}{\Gamma,\mathsf{sign}(M,K),\,\mathsf{pub}(L)\vdash N}\,(\mathsf{sign}_L)K=_{AC}L$$

$$\frac{\Gamma,\mathsf{blind}(M,K)\vdash K \qquad \Gamma,\mathsf{blind}(M,K),M,K\vdash N}{\Gamma,\mathsf{blind}(M,K)\vdash N}\,(\mathsf{blind}_{L_1})$$

$$\frac{\Gamma,\mathsf{sign}(\mathsf{blind}(M,R),K)\vdash R \qquad \Gamma,\mathsf{sign}(\mathsf{blind}(M,R),K),\mathsf{sign}(M,K),R\vdash N}{\Gamma,\mathsf{sign}(\mathsf{blind}(M,R),K)\vdash N}\,(\mathsf{blind}_{L_2})$$

$$\frac{\Gamma\vdash A \qquad \Gamma,A\vdash M}{\Gamma\vdash M}\,(acut),\,A\text{ is an }E\text{-factor of }\Gamma\cup\{M\}$$

Analysing the system $\mathscr{S}$ one can make the following observations:

1. The rules p_L,e_L,sign_L,blind_{L1}, blind_{L2} and *acut* are called *left rules* with $\langle M,N\rangle$, $\{M\}_K$, $\mathsf{sign}(M,K)$, $\mathsf{blind}(M,K)$, $\mathsf{sign}(\mathsf{blind}((M,R),K)$ and A as *principal term*, respectively. The rules p_R,e_R,sign_R and blind_R are called *right rules*.

2. The rule $(acut)$, called *analytic cut* is necessary to prove cut rule *admissibility*. A complete proof can be found in [26, 29].

Remark 5. *Considerations about locally stable theories with blind signatures:*

1. *All the results proved on Section 2 are valid under this extension with blind signatures since the results depend only on the equational theory E and on the symbols in Σ_E. Unlike example 5.2.4 [1], the theory of Blind Signatures is not considered as part of the equational theory, the functions are abstracted in the set of constructors with the operational meaning represented in the sequent calculus.*

2. *In [29] it is shown that the intruder deduction problem for $\mathscr{S}$ is* polynomially reducible *to the EDP for E:* if the EDP problem in E has complexity $f(m)$ then the deduction problem $\Gamma \vdash M$ in $\mathscr{S}$ has complexity $O(n^k.f(n))$ for some constant k[2]. *This result was proved for an AC-convergent equational theory E containing only one AC symbol and extended to finite a combination of disjoint AC-convergent equational theories each one containing only one AC-symbol.*

3. *In [26], it was proved that deduction in $\mathscr{S}$ reduces polynomially to EDP in the case of the AC-convergent equational theory EP, which contains three different AC-symbols and rules for exponentiation and cannot be split into disjoint parts.*

As a consequence of the results mentioned in the above remark, we can state the following result:

Corollary 2. *Let E be a locally stable theory satisfying (*) containing only one AC-symbol or formed by a finite and disjoint combination of AC-symbols. Let Γ a finite set of ground terms in normal form and M a ground term in normal form. The IDP for the theory E combined with blind signatures ($\Gamma \vdash M$) is decidable in polynomial time in $|sat(\Gamma)|$ and $|M|$.*

5 Conclusion

We have shown that the IDP is decidable for locally stable theories. In order to obtain the polynomiality result, a restriction on the equational theory is necessary: the theory must contain inverses of all AC-symbols. We have proposed an algorithm to solve a restricted case of higher-order AC-matching by using the DO-ACM matching algorithm combined with an algorithm to solve linear Diophantine equations over $\mathbb{Z}$. Based on this algorithm, we obtain a polynomial decidability result for IDP for a class of locally stable theories with inverses. Our algorithm does not need to compute the set of normal forms modulo AC of a given term (which may be exponential). Therefore, we can conclude that the deducibility relation is decidable in polynomial time for a very restricted class of equational theories, it does not work for all locally stable theories as [1] has claimed. It also decides the IDP for the combination of locally stable theories with the theory of blind signatures, using a translation between natural deduction and sequent calculus.

References

[1] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 367(1-2):2–32, 2006. doi:10.1016/j.tcs.2006.08.032.

[2] Here, m is the size of the input of EDP and n is the cardinality of the set $St(\Gamma \cup \{M\})$ defined in [29]

[2] M. Abadi and C. Fournet. Mobile Values, New Names, and Secure Communication. In *Proc. 28th ACM SIGPLAN-SIGACT symposium on Principles of programming languages (POPL'01)*, pages 104–115, 2001. doi:10.1145/360204.360213.

[3] M. Abadi and A.D. Gordon A Calculus for Cryptographic Protocols: The spi Calculus. *Information and Computation* , 148(1): 1–70, 1999. doi:10.1006/inco.1998.2740.

[4] A. Armando *et al*. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In *Proc. 17th Computer Aided Verification (CAV'05)*, volume 3576, pages 281–285. Springer-Verlag 2005. doi:10.1007/11513988_27.

[5] M. Ayala-Rincón, M. Fernández and D. Nantes-Sobrinho. Elementary Deduction Problems for Locally Stable Theories with Normal Forms (extended version). http://www.mat.unb.br/~dnantes/Publications.

[6] F. Baader and T. Nipkow. *Term Rewriting and All That*. CUP, 1998.

[7] M. Baudet, V. Cortier and S. Delaune. YAPA: A Generic Tool for Computing Intruder Knowledge. In *Proc. of 20th International Conference on Rewriting Techniques and Applications (RTA'09)*, volume 5595 of *LNCS*, pages 148-163. Springer, 2009. arXiv:1005.0737, doi:10.1007/978-3-642-02348-4_11.

[8] D. Benanav, D. Kapur, P. Narendran, and L. Wang. Complexity of matching problems. In *Journal of Symbolic Computation*, 3(1/2): 203–216, 1987. doi:10.1007/3-540-15976-2_22.

[9] V. Bernat and H. Comon-Lundh. Normal proofs in intruder theories. In *Proc. 11th Asian Computing Science Conference, Advances in Computer Science - Secure Software and Related Issues (ASIAN'06)*, volume 4435 of *LNCS*, pages 151–166. Springer-Verlag, 2006. doi:10.1007/978-3-540-77505-8_12.

[10] B. Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In *Proc. 14th IEEE Computer Security Foundations Workshop (CSFW'01)*, pages 82–96, IEEE Comp. Soc., 2001. http://doi.ieeecomputersociety.org/10.1109/CSFW.2001.930138.

[11] B. Blanchet. A Computationally Sound Mechanized Prover for Security Protocols. In *IEEE Transactions on Dependable and Secure Computing*, volume 5 (4), pages 193–207, 2008. doi:10.1109/TDSC.2007.1005

[12] A. Boudet, E. Contejean and H. Devie. A new AC Unification Algorithm with an Algorithm for Solving Systems of Linear Diophantine Equations. In *Proc. 5th Annual Symposium on Logic in Computer Science (LICS '90)*, pages 289–299, 1990. doi:10.1109/LICS.1990.113755.

[13] B. Bursuc, H. Comon-Lundh, and S. Delaune. Deducibility constraints, equational theory and electronic money. In *Rewriting, Computation and Proof, Essays Dedicated to Jean-Pierre Jouannaud on the occasion of his 60th Birthday*, volume 4600 of *LNCS*, pages 196–212. Springer-Verlag, 2007. doi:10.1007/978-3-540-73147-4_10.

[14] D. Chaum. Blind Signatures for Untraceable Payments. In *Proc. of Advances in Cryptology (CRYPTO'82)*, pages 199–203, Plenum Press, 1982. http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF.

[15] M. Clausen and A. Fortenbacher. Efficient Solution of Linear Diophantine Equations. In *Journal of Symbolic Computation*, Volume 8(1-2), pages 201–216, 1989. doi:10.1016/S0747-7171(89)80025-2.

[16] H. Comon-Lundh and V. Shmatikov. Intruder Deduction, Constraint Solving and Insecurity Decisions in Presence of Exclusive or. In *Proc. 18th IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 271–280. IEEE Comp. Soc., 2003. http://doi.ieeecomputersociety.org/10.1109/LICS.2003.1210067.

[17] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.

[18] S. Delaune. *Vérification des protocoles cryptographiques et propriétés algébriques*. PhD thesis, École Normale Supérieure de Cachan, 2006. http://tel.archives-ouvertes.fr/tel-00132677/en/.

[19] S. Delaune. Easy Intruder Deduction Problems with Homomorphisms. *Information Processing Letters*, volume 97(6), pages 213–218, 2006. doi:10.1016/j.ipl.2005.11.008.

[20] D. Dolev and A. Yao. On the security of public keys protocols. In *IEEE Transactions on Information Theory*, volume 29(2), pages 198–208, 1983. http://doi.ieeecomputersociety.org/10.1109/SFCS.1981.32.

[21] S. Escobar, C. Meadows and J. Meseguer. Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties. In *Foundations of Security Analysis and Design V, FOSAD 2007/2008/2009 Tutorial Lectures*, volume 5705 of *LNCS*, pages 1–50. Springer-Verlag, 2007. doi:10.1007/978-3-642-03829-7_1.

[22] M. A. Frumkin. Polynomial time Algorithms in the Theory of Linear Diophantine Equations. In *Proc. of Fundamentals of Computation Theory*, volume 56 of *LNCS*, pages 386–392, Springer-Verlag, 1977. doi:10.1007/3-540-08442-8_106.

[23] P. Lafourcade, D. Lugiez and R. Treinen. Intruder Deduction for *AC*-Like Equational Theories with Homomorphisms In *Proc. 16th International Conference on Term Rewriting and Applications (RTA'05)*, volume 3467 of *LNCS*, pages 308–322, Springer-Verlag, 2005. doi:10.1007/978-3-540-32033-3_23.

[24] P. Lafourcade. Intruder Deduction for the equational theory of exclusive-or with commutative and distributive encryption. In *Electr. Notes Theor. Comput. Sci.*, volume 171(4): 37–57, 2007. doi:10.1016/j.entcs.2007.02.054.

[25] D. McAllester. Automatic recognition of tractability in inference relations. *Journal of the ACM*, volume 40, pages 284–303, 1990. doi:10.1145/151261.151265.

[26] D. Nantes-Sobrinho and M. Ayala-Rincón. Reduction of the Intruder Deduction Problem into Equational Elementary Deduction for Electronic Purse Protocols with Blind Signatures. In *Proc. 17th Int. Workshop on Logic, Language, Information and Computation (WoLLIC'10)*, volume 6188 of *LNCS*, pages 218–231, Springer-Verlag, 2010. doi:10.1007/978-3-642-13824-9_18.

[27] C. Papadimitriou. Computational Complexity. Addison-Wesley, Inc.

[28] A. Tiu. A trace based simulation for the spi calculus: An extended abstract. In *Proc. 5th Asian Symposium on Programming Languages and Systems (APLAS'07)*, volume 4807 of *LNCS*, pages 367–382, Springer-Verlag, 2007. arXiv:0901.2166.

[29] A. Tiu and R. Goré and J. Dawson. A proof theoretic analysis of intruder theories. In *Proc. 20th International Conference on Rewriting Techniques and Applications (RTA'09)*, volume 5595 of *LNCS*, pages 103–117. Springer-Verlag, 2009. doi:10.2168/LMCS-6(3:12)2010.