Hierarchical combination of intruder theories

Yannick Chevalier, Michael Rusinowitch

Hierarchical Combination of Intruder Theories ⋆

Yannick Chevalier *,1 Michael Rusinowitch **

Abstract

Recently automated deduction tools have proved to be very effective for detecting attacks on cryptographic protocols. These analysis can be improved, for finding more subtle weaknesses, by a more accurate modelling of operators employed by protocols. Several works have shown how to handle a single algebraic operator (associated with a fixed intruder theory) or how to combine several operators satisfying disjoint theories. However several interesting equational theories, such as exponentiation with an abelian group law for exponents remain out of the scope of these techniques. This has motivated us to introduce a new notion of hierarchical combination for non disjoint intruder theories and to show decidability results for the deduction problem in these theories. We have also shown that under natural hypotheses hierarchical intruder constraints can be decided. This result applies to an exponentiation theory that appears to be more general than the one considered before.

Key words: Cryptographic protocols, Dolev-Yao intruder, combination of decision procedures, equational theories

1 Introduction

Recently many procedures have been proposed to determine whether cryptographic protocols are insecure in the Dolev-Yao model with respect to a finite number of protocol sessions [5,2,32,26,23,4,17]. Among the different approaches the symbolic ones [5,2,32,26,12,4,17] are based on reducing the problem to constraint solving in a term algebra. While these approaches rely on

⋆ Research partially supported by ACI-SI SATIN and by ARA-SSIA Cops
* IRIT, Team LiLac, Université Paul Sabatier, Toulouse, France.
**Loria–INRIA Lorraine, Cassis Project, Nancy, France.
Email addresses: ychevali@irit.fr (Yannick Chevalier), rusi@loria.fr (Michael Rusinowitch).
[1] Author also supported by ACI-Jeunes Chercheurs JC 9005

a perfect encryption hypothesis, the design of some protocols (see *e.g.* [35]) rely on lower-level primitives such as exponentiation or bitwise exclusive or (xor). These specifications may give rise to new attacks exploiting the underlying algebraic structure when it is not abstracted as perfect encryption. For examples of attacks exploiting *e.g.* the bitwise xor equational properties in the context of mobile communications see for instance [6].

Hence several protocol decision procedures have been designed for handling equational properties [30,15,8,24] of the cryptographic primitives. A very fruitful concept in this area is the notion of locality introduced by McAllester [25] which applies to several intruder theories [16,24]. When an intruder theory is *local* then we can restrict every intruder deduction to contain only subterms of its inputs, *i.e.* its hypotheses and its goal and this may lead to decidability of intruder constraints. In this article we extend this approach to a case where the signature can be divided into two disjoint sets and where the term algebra can be divided into two kinds of terms, say kinds 0 and 1, according to their root symbol. Then we give sufficient conditions so that we can restrict intruder deductions to deductions where all subterms of kind 1 that occur in the deduction are subterms of the inputs (i.e. some initially given terms and the goal term). Our goal is to bound the deductions using a "function" of kind 1 by the intruder, thus permitting subsequent analysis to focus on the deductions by "function" of kind 0.

This approach allows us to decide interesting intruder theories presented as non-disjoint combination of theories, and that were not considered before, by reducing them to simpler theories. For instance it allows one to combine the Abelian group theory of [27] with a theory of an exponential operator.

Related works. In [10] we have extended the combination algorithm for solving E-unification problems of [34,3] to solve intruder constraints on disjoint signatures. Here we show that we can handle some non-disjoint combinations. In [18] Delaune and Jacquemard consider theories presented by rewrite systems where the right-hand side of every rule is a ground term or a variable. Comon and Treinen [16,14] have also investigated general conditions on theories for deciding insecurity with passive intruders. In [1] different equational theories are considered for passive intruders only.

As an application, we have obtained a decidable intruder theory combining Abelian group and exponential which has less restrictions than any previous one: unlike [9] it permits the intruder to multiply terms outside exponents, which is natural with the Diffie-Hellman protocol where the prime decomposition of the module is public. The setting is also less restrictive than in [33] where bases of exponentials have to be constants and exponential terms must not appear inside exponents.

Outline. In Section 2 we present the topic of analysis of cryptographic pro-

tocol insecurity. In Section 3 we will first recall basic notions about terms, substitutions and term rewriting. In Section 4 we recall the definition of intruder systems from [10], we recall a model for cryptographic protocols and we define related constraint systems. In Section 5 we define a new notion of *mode*. We then derive a notion of *subterm value* from the mode, and study properties of term replacement operations. In Section 6 we define the notion of *well-moded intruders*. We also prove the existence of special sequences of deductions called *quasi well-formed derivations*. In Section 7 we define for a constraint system $\mathcal{C}$ a special kind of substitutions called *bound substitutions*. We prove that whenever a constraint system $\mathcal{C}$ is satisfiable it is also satisfied by a bound substitution. We also prove that these solutions do not increase the number of subterms of $\mathcal{C}$, *i.e.* after instantiating $\mathcal{C}$ with a bound solution, the number of subterms in the result is lesser or equal. We then give in Section 8 sufficient conditions for the decidability of some protocol-related decision problems. We then apply these conditions to prove the decidability of the protocol insecurity problem when an exponential operator is present.

2 Analysis of cryptographic protocols

2.1 An example

The Station-to-Station (STS) protocol (see e.g. [31]) is a cryptographic key agreement scheme that relies on Diffie-Hellman key construction method. It improves over Diffie-Hellman protocol by adding signatures to messages to block some simple man-in-the middle attacks. Hence STS protocol is classified as an authenticated key agreement with key confirmation protocol. Here is a simplified version of STS: Initially g is a generator of a cyclic group p, and these parameters are public; A(lice) generates a random number a and computes and sends the exponential $\exp(g, a)$ to B(ob); Bob generates a random number b and computes the exponential $\exp(g, b)$; Bob concatenates the exponentials, signs them using his private key K_B^{-1}, appends it to $\exp(g, b)$ and sends the resulting message to Alice. Alice verifies Bob's signature, concatenates the exponentials in reverse order, signs them using her private key K_A^{-1}, and sends the result to Bob.

1. $A \to B : \exp(g, a), A$
2. $B \to A : \exp(g, b), \{\exp(g, b), \exp(g, a)\}_{K_B^{-1}}$
3. $A \to B : \{\exp(g, a), \exp(g, b)\}_{K_A^{-1}}$

The ability for Alice and Bob to build a secret shared key $\exp(g, a \times b)$ relies

on the algebraic properties of exp and $\times$: for instance it exploits the property $\exp(\exp(g,a),b) = \exp(\exp(g,b),a) = \exp(g, a \times b)$. Moreover it also relies on the properties of asymmetric cryptography that can modelled at an abstract level by laws of type: $\{\{m\}_{K_A^{-1}}\}_{K_A} = m$ expressing that when applying K_A (to be more precise, an algorithm depending from K_A) to the signed message $\{m\}_{K_A^{-1}}$ one can retrieve m.

This example shows that the design and the analysis of cryptographic protocols is often based on algebraic properties of the functions involved in the messages. Moreover it is frequent that a property is expressed by combining several operators, as it is the case above where some useful properties involve both exp and $\times$.

2.2 Analysis in presence of algebraic properties

As we see the algebraic properties of primitives are important for many protocols to work properly. As a consequence they have to be handled appropriately when analysing the security of protocols.There exist two main settings for performing protocol analysis: the computational one and the Dolev-Yao one. In the computational setting one tries to reduce the security of protocols to the security of primitives (e.g. encryption), which is itself characterized by the fact that no adversary can efficiently recover any information about the encrypted message content, given the ciphertext and (in the case of a public key system) the encryption key. This approach when successful provides strong security guarantees. However it leads to complex proofs and is not easily amenable to automation. On the other hand the Dolev-Yao approach, sometimes called the *symbolic approach*, rather considers encryption and other functions as abstract datatypes and allows for more automation of security proofs.

Note that it is not worth attempting a computational security proof of a protocol if some flaws are already found in the Dolev-Yao model. Hence the two approaches can be viewed as complementary: to secure a protocol one may first check for flaws in the symbolic setting (possibly with automatic tools) and then, once they are corrected, try computational proofs.

However in order to get a more faithful analysis in the symbolic setting one has to model as much as possible the algebraic properties of the functions. A particularly important primitive is the modular exponentiation function, whose properties are seldom handled by verification tools. As mentionned above a challenge is also to consider the properties of several functions together. In important instance of this problem is the case of an exponentiation and an abelian group operator.

To model them we can use the following equational theory $\mathcal{E}^{exp,\times}$:

$$x \times (y \times z) = (x \times y) \times z \qquad (A)$$
$$x \times y = y \times x \qquad (C)$$
$$x \times 1 = x \qquad (U)$$
$$x \times \mathrm{i}(x) = 1 \qquad (I)$$
$$\exp(x, 1) = x \qquad (E_0)$$
$$\exp(\exp(x, y), z) = \exp(x, y \times z) \qquad (E_1)$$

In our approach to be detailed in the following the intruder abilities will be specified by a set of terms, such as $T = \{x \times y, \mathrm{i}(x), 1, \exp(x, y)\}$, representing the messages he can derive. For instance given x, y the intruder is able to construct $x \times y$. The difficulty when checking whether an intruder can derive a given message (e.g. in order to mount an attack) comes from the fact that we have to reason modulo an equational theory, and for instance we have to consider that $\exp(\exp(g, a), b)$ and $\exp(\exp(g, b), a)$ represents the same message.

In [10] we have shown that it was possible to perform a modular protocol analysis when the equational theory can be split in subtheories with disjoint functional signatures Note however this approach does not allow in the example above to separate the analysis on exp and $\times$ because of the equation (E_1).

Hence our first objective in this paper is to propose a method to reduce protocol analysis problems involving equational theories to simpler ones. The second objective is to apply the method to decide insecurity in the symbolic approach for protocols that use both exp and $\times$ with properties specified by $\mathcal{E}$. In that case the problem will be reduced to the decision of insecurity for protocols where only $\times$ occurs.

3 Terms and rewriting

3.1 Basic notions

We consider an infinite set of free constants C and an infinite set of variables $\mathcal{X}$. For all signatures $\mathcal{G}$ (*i.e.* sets of function symbols not in C with arities), we denote by $\mathrm{T}(\mathcal{G})$ (resp. $\mathrm{T}(\mathcal{G}, \mathcal{X})$) the set of terms over $\mathcal{G} \cup \mathrm{C}$ (resp. $\mathcal{G} \cup \mathrm{C} \cup \mathcal{X}$). The former is called the set of ground terms over $\mathcal{G}$, while the latter is simply

called the set of terms over $\mathcal{G}$. The arity of a function symbol f is denoted by $\text{AR}(f)$. Variables are denoted by x, y, terms are denoted by s, t, u, v, and finite sets of terms are written $E, F, ...$, and decorations thereof, respectively. We abbreviate $E \cup F$ by E, F, the union $E \cup \{t\}$ by E, t and $E \setminus \{t\}$ by $E \setminus t$.

Given a signature $\mathcal{G}$, a *constant* is either a free constant or a function symbol of arity 0 in $\mathcal{G}$. We define the set of atoms $\mathcal{A}$ to be the union of $\mathcal{X}$ and the set of constants. Given a term t we denote by $\text{Var}(t)$ the set of variables occurring in t and by $\text{Cons}(t)$ the set of constants occurring in t. We denote by $\text{Atoms}(t)$ the set $\text{Var}(t) \cup \text{Cons}(t)$. A substitution σ is an involutive mapping from $\mathcal{X}$ to $\text{T}(\mathcal{G}, \mathcal{X})$ such that $\text{Supp}(\sigma) = \{x | \sigma(x) \neq x\}$, the *support* of σ, is a finite set. The application of a substitution σ to a term t (resp. a set of terms E) is denoted $t\sigma$ (resp. $E\sigma$) and is equal to the term t (resp. E) where all variables x have been replaced by the term $\sigma(x)$. A substitution σ is *ground* with respect to $\mathcal{G}$ if the image of $\text{Supp}(\sigma)$ is included in $\text{T}(\mathcal{G})$. A unification problem is a pair of terms denoted by $s \stackrel{?}{=} t$. A unification system is a finite set of unification problems. A solution of a unification system is a substitution σ, called a *unifier*, such that for all pairs $s \stackrel{?}{=} t$ in the system we have $s\sigma = t\sigma$.

An *equational presentation* $\mathcal{H} = (\mathcal{G}, A)$ is defined by a set A of equations $u = v$ with $u, v \in \text{T}(\mathcal{G}, \mathcal{X})$ and u, v without free constants. For any equational presentation $\mathcal{H}$ the relation $=_{\mathcal{H}}$ denotes the equational theory generated by $(\mathcal{G}, A)$ on $\text{T}(\mathcal{G}, \mathcal{X})$, that is the smallest congruence containing all instances of axioms of A. Abusively we shall not distinguish between an equational presentation $\mathcal{H}$ over a signature $\mathcal{G}$ and a set A of equations presenting it and we denote both by $\mathcal{H}$. We will also often refer to $\mathcal{H}$ as an equational theory (meaning the equational theory presented by $\mathcal{H}$).

The *syntactic subterms* of a term t are denoted $\text{Sub}_{\text{syn}}(t)$ and are defined recursively as follows. If t is a variable or a constant then $\text{Sub}_{\text{syn}}(t) = \{t\}$. If $t = f(t_1, \ldots, t_n)$ then $\text{Sub}_{\text{syn}}(t) = \{t\} \cup \bigcup_{i=1}^{n} \text{Sub}_{\text{syn}}(t_i)$. The *positions* in a term t are sequences of integers defined recursively as follows, ϵ being the empty sequence. The term t is at position ϵ in t. We also say that ϵ is the root position. We write $p \leq q$ to denote that the position p is a prefix of position q. If u is a syntactic subterm of t at position p and if $u = f(u_1, \ldots, u_n)$ then u_i is at position $p \cdot i$ in t for $i \in \{1, \ldots, n\}$. We write $t_{|p}$ the subterm of t at position p. We denote by $t[p \leftarrow s]$ the term obtained by replacing in t the syntactic subterm at position p by s. If Π is a set of incomparable positions (with respect to the ordering on positions) in term t we denote by $t[\Pi \leftarrow v]$ the term obtained by putting v at all positions of t that are in Π. We write $t[s]$ to denote a term t where s is a syntactic subterm of t.

In this paper, we will consider two disjoint signatures $\mathcal{F}_0$ and $\mathcal{F}_1$, an equational theory $\mathcal{E}_0$ (resp. $\mathcal{E}_1$) on $\mathcal{F}_0$ (resp. $\mathcal{F}_0 \cup \mathcal{F}_1$). We denote by $\mathcal{F}$ the union of the signatures $\mathcal{F}_0$ and $\mathcal{F}_1$ and by $\mathcal{E}$ the union of the theories $\mathcal{E}_0$ and $\mathcal{E}_1$. We assume

that $\mathcal{E}$ is consistent (*i.e.* two free constants are not equal modulo $\mathcal{E}$). A term t in $\mathrm{T}(\mathcal{F}_0, \mathcal{X})$ (resp.$\mathrm{T}(\mathcal{F}_1, \mathcal{X})$) is called a *pure* 0-term (resp. *pure* 1-term). We denote by $\mathrm{TOP}(\cdot)$ the function that associates to each term t its root symbol. We also partition the set of variables $\mathcal{X}$ into two infinite sets $\mathcal{X}_0$ and $\mathcal{X}_1$.

3.2 Congruences and ordered rewriting

In this subsection we recall some properties of *ordered rewriting* [19] which has been a useful notion (*e.g.* [3]) for proving the correctness of combination of unification algorithms. Rewriting is the process of applying an oriented equation $l \to r$ to reduce a term t, by replacing an instance of its left-hand side $l\sigma$ by a corresponding instance of its right-hand side $r\sigma$. Knuth-Bendix completion method [19] attempts to transform a set of equations E into a set of oriented equations (or rewrite rules) R such that rewriting becomes a decision procedure for deciding the word problem in E. However the completion method may fail due to the impossibility of orienting an equation. To avoid failure Knuth-Bendix completion procedure can be extended to deal with unorientable equations obtaining the so-called *unfailing completion procedure* [22,19].

Let $<$ be a simplification ordering on $\mathrm{T}(\mathcal{G})$ [2] assumed to be total on $\mathrm{T}(\mathcal{G})$ and such that the minimum for $<$ is a constant $\mathrm{c_{min}} \in \mathrm{C}$ and non-free constants are smaller than any non-constant ground term.

Ordered rewriting is an extension of rewriting to unorientable equations: it is the process of applying an equation $u = v$ (or $v = u$) to reduce a term t, by replacing an instance of some side say $u\sigma$, by a corresponding instance of the other side $v\sigma$ under the condition that $u\sigma > v\sigma$.

Given a signature $\mathcal{G}$, we denote by $\mathrm{C_{spe_{\mathcal{G}}}}$ the set containing the constants in $\mathcal{G}$ and $\mathrm{c_{min}}$. For the signature $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$ defined earlier, we abbreviate $\mathrm{C_{spe_{\mathcal{F}}}}$ by $\mathrm{C_{spe}}$. Given a possibly infinite set of equations $\mathcal{O}$ on the signature $\mathrm{T}(\mathcal{G})$ we define the ordered rewriting relation $\to_{\mathcal{O}}$ by $s \to_{\mathcal{O}} s'$ iff there exists a position p in s, an equation $l = r$ in $\mathcal{O}$ and a substitution τ such that $s = s[p \leftarrow l\tau]$, $s' = s[p \leftarrow r\tau]$, and $r\tau < l\tau$.

It has been shown (see [22,19]) that by applying the unfailing completion procedure to a set of equations $\mathcal{H}$ we can derive a (possibly infinite) set of equations $\mathcal{O}$, called *o-completion* of $\mathcal{H}$ and such that, *first,* the congruence relations $=_{\mathcal{O}}$ and $=_{\mathcal{H}}$ are equal on $\mathrm{T}(\mathcal{F})$; and *second*, the ordered rewrite relation $\to_{\mathcal{O}}$ is convergent (*i.e.* terminating and confluent) on $\mathrm{T}(\mathcal{F})$. By the

[2] by definition $<$ satisfies for all $s, t, u \in \mathrm{T}(\mathcal{G})$ (i) $s < t[s]$ if s and $t[s]$ are different terms and (ii) $s < u$ implies $t[s] < t[u]$

termination of $\rightarrow_{\mathcal{O}}$ every ground term t admits at least one *normal form* t' which is by definition a term that cannot be rewritten.

From now on when we say *"the rewrite system $\rightarrow_{\mathcal{O}}$"* this will mean "the ordered rewrite relation $\rightarrow_{\mathcal{O}}$", when will say *"by convergence of $\mathcal{O}$"*, we will mean "by convergence of $\rightarrow_{\mathcal{O}}$ on ground terms". By convergence of $\mathcal{O}$ we can define $(t)\downarrow_{\mathcal{O}}$ as the unique normal form of the ground term t for $\rightarrow_{\mathcal{O}}$. If a term t is equal to its normal form we say that t is *normalised*. Given a ground substitution σ we denote by $(\sigma)\downarrow_{\mathcal{O}}$ the substitution with the same support such that for all variables $x \in \mathrm{Supp}(\sigma)$ we have $x(\sigma)\downarrow_{\mathcal{O}} = (x\sigma)\downarrow_{\mathcal{O}}$. A substitution σ is *normal* if $\sigma = (\sigma)\downarrow_{\mathcal{O}}$. In the following we will denote by R an o-completion of $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2$.

4 Formal Security Analysis of Protocols

4.1 Intruder systems

We first recall here the general definition of intruder systems, as is given in [10,11]. In the context of a security protocol (see *e.g.* [20,29] for a brief overview), we model messages as ground terms and intruder deduction rules as rewrite rules on sets of messages representing its knowledge. The intruder derives new messages from a given (finite) set of messages by applying intruder rules. Since we assume some equational axioms $\mathcal{H}$ are satisfied by the function symbols in the signature, all these derivations have to be considered *modulo* the equational congruence $=_{\mathcal{H}}$ generated by these axioms. An intruder deduction rule in our setting is specified by a term t in some signature $\mathcal{G}$. Given values for the variables of t the intruder is able to generate the corresponding instance of t. One may intuitively think of a term t modulo $\mathcal{H}$ as a function; The variables of t are then its formal parameters.

Definition 1 *An* intruder system $\mathcal{I}$ *is given by a triple* $\langle \mathcal{G}, \mathcal{S}, \mathcal{H} \rangle$ *where* $\mathcal{G}$ *is a signature,* $S \subseteq \mathrm{T}(\mathcal{G}, \mathcal{X})$ *and* $\mathcal{H}$ *is a set of equations between terms in* $\mathrm{T}(\mathcal{G}, \mathcal{X})$*. To each* $t \in S$ *we associate a* deduction rule $\mathrm{L}^t : \mathrm{Var}(t) \rightarrow t$ *and* $\mathrm{L}^{t,\mathrm{g}}$ *denotes the set of ground instances of the rule* L^t modulo $\mathcal{H}$*:*

$$\mathrm{L}^{t,\mathrm{g}} = \{l \rightarrow r \mid \exists \sigma, \textit{ground substitution on } \mathcal{G},\ l = \mathrm{Var}(t)\sigma \text{ and } r =_{\mathcal{H}} t\sigma\}$$

The set of rules $\mathrm{L}_{\mathcal{I}}$ *is defined as the union of the sets* $\mathrm{L}^{t,\mathrm{g}}$ *for all* $t \in \mathcal{S}$*.*
Each rule $l \rightarrow r$ in $\mathrm{L}_{\mathcal{I}}$ defines an intruder deduction relation $\rightarrow_{l \rightarrow r}$ between finite sets of terms. Given two finite sets of terms E and F we define $E \rightarrow_{l \rightarrow r} F$ if and only if $l \subseteq E$ and $F = E \cup \{r\}$. We denote $\rightarrow_{\mathcal{I}}$ the union of the relations $\rightarrow_{l \rightarrow r}$ for all $l \rightarrow r$ in $L_{\mathcal{I}}$ and by $\rightarrow^*_{\mathcal{I}}$ the transitive closure of $\rightarrow_{\mathcal{I}}$.

Example 1 *Let* $\rightarrow_{\mathcal{I}_\times}$ *be the relation between ground sets of terms defined*

by the Abelian group intruder $\mathcal{I}_\times = \langle\{\times, \mathrm{i}, 1\}, \{x \times y, \mathrm{i}(x), 1\}, \mathcal{E}_\times\rangle$*, where* $\mathcal{E}_\times$ *contains axioms* $(A), (C), (U), (I)$ *from Subsection 2.2. One has:*

$$a, b, c \times a \rightarrow_{\mathcal{I}_\times} a, b, c \times a, \mathrm{i}(a) \rightarrow_{\mathcal{I}_\times} a, b, c \times a, \mathrm{i}(a), c$$

The latter deduction resulting from the application of the rule $x, y \rightarrow x \times y$ *with* x *instantiated by* $\mathrm{i}(a)$*,* y *instantiated by* $c \times a$*, with right-hand side* c *which is equal to* $\mathrm{i}(a) \times (c \times a)$ *modulo the equational theory.*

Notice that by definition, given sets of terms E, E', F and F' such that $E =_\mathcal{G} E'$ and $F =_\mathcal{G} F'$ we have $E \rightarrow_\mathcal{I} F$ iff $E' \rightarrow_\mathcal{I} F'$. We simply denote by $\rightarrow$ the relation $\rightarrow_\mathcal{I}$ when there is no ambiguity about $\mathcal{I}$.

The next result will allow us to restrict our study to deductions with terms in normal form.

Lemma 1 *We assume that* R *is a rewrite system that is terminating and confluent on ground terms such that* $=_R$ *and* $=_\mathcal{H}$ *are the same relations. Then given two sets of ground terms* E *and* F*, there is a deduction* $E \rightarrow F$ *iff there is a deduction* $(E)\!\downarrow \rightarrow (F)\!\downarrow$*.*

A *derivation* D of length n, $n \geq 0$, is a sequence of steps of the form $E_0 \rightarrow_\mathcal{I} E_0 \cup \{t_1\} = E_1 \rightarrow_\mathcal{I} \cdots \rightarrow_\mathcal{I} E_n$ with finite sets of ground terms $E_0, \ldots E_n$, and ground terms $t_1, \ldots, t_n$, such that $E_i = E_{i-1} \cup \{t_i\}$ for every $i \in \{1, \ldots, n\}$. A derivation is *without stutter* if for all $i, j \in \{1, \ldots, n\}$, $E_i =_\mathcal{H} E_j$ implies $i = j$. The term t_n is called the *goal* of the derivation. We define $\overline{E}^\mathcal{I}$ to be the set of terms t such that there exists a derivation for intruder $\mathcal{I}$ starting from E of goal t. If there is no ambiguity on the deduction system $\mathcal{I}$ we write $\overline{E}$ instead of $\overline{E}^\mathcal{I}$.

From Lemma 1 one can easily prove that it suffices to consider deductions on sets of terms in normal form. In the sequel we will thus only consider derivations on sets of terms in normal form with rules yielding terms in normal form.

4.2 Protocol analysis

In this section we describe how protocols are modelled. The approach is standard [2,5,27]. Our semantics follows the one in [18]. We only consider a single session of the protocol since it is well-known how to reduce several sessions to this case.

In Dolev-Yao's model the intruder can intercept, block and/or redirect all messages sent by honest agents. He is also able to send messages by masquerading

his identity. Honest agents may know his identity, wrongly assume he is honest and communicate with him on that basis. He has complete control over the communication medium. We model this by considering that the intruder *is* the network: messages sent by honest agents are sent directly to the intruder and messages received by the honest agents are always sent by the intruder. From the intruder's point of view a finite execution of a protocol is therefore the interleaving of a finite sequence of messages he *has to* send and a finite sequence of messages he receives (and *adds* to his knowledge set).

We also assume the interaction of the intruder with one agent to be an atomic step. The intruder sends a message m to a honest agent, this agent tests the validity of this message and responds to it immediately. Alternatively an agent may initiate an execution and in this case we assume it reacts to a dummy message sent by the intruder.

A *step* is a triplet $(\text{RECV}(x); \text{SEND}(s); \text{COND}(e))$ where $x \in \mathcal{X}$, $s \in \mathrm{T}(\mathcal{G}, \mathcal{X})$ and e is a set of equations between terms of $\mathrm{T}(\mathcal{G}, \mathcal{X})$. The meaning of a step is that upon receiving message x, the honest agent checks the equations in e and sends the message s. An *execution* of a protocol is a finite sequence of steps.

Example 2 *Consider the following simple protocol where two agents named A(lice) and B(ob) communicate and where K is a symmetric key initially known by A only.*

$$
\begin{aligned}
&A \to B : \exp(M, B \times K)\\
&B \to A : B\\
&A \to B : K\\
&B \to A : M
\end{aligned}
$$

Alice sends some message M raised to the exponent $B \times K$ to Bob. Bob replies by sending back his name B. In third message Alice reveals the key K to Bob. Then Bob computes the inverses $i(K)$ and $i(B)$ of K and B respectively, in the group of exponents. Next, he raises the first message he received to the exponent $i(K) \times i(B)$. He derives M that he can send in the last message.

Hence by assuming the algebraic properties of the exponentiation operator exp*, and of the product and inverse $\times, i(\cdot)$ in the group of exponents, we can model this protocol as:*

$$
\begin{aligned}
&\text{RECV}(v_1); \text{SEND}(\exp(M, B \times K)); \text{COND}(\{v_1 = \mathrm{c}_{\min}\})\\
&\text{RECV}(v_2); \text{SEND}(B); \text{COND}(\emptyset)\\
&\text{RECV}(v_3); \text{SEND}(K); \text{COND}(\{v_3 = B\})\\
&\text{RECV}(v_4); \text{SEND}(\exp(v_2, \mathrm{i}(B) \times \mathrm{i}(v_4))); \text{COND}(\{v_2 = \exp(y, B \times\\
&v_4)\})\\
&\text{RECV}(v_5); \text{SEND}(\mathrm{c}_{\min}); \text{COND}(v_5 = M)
\end{aligned}
$$

Note that in this setting we can model that at some step i the message should

match the pattern t_i by adding an equation $v_i \stackrel{?}{=} t_i$ to $\mathcal{S}$, as is done in last step of the above example. An agent may also verify previously received messages when he get new information (for example when B receives the third message).

Let $\mathcal{I}=\langle \mathcal{G}, S, \mathcal{H} \rangle$ be an intruder system. A *configuration* is a couple $\langle P, N \rangle$ where P is a finite sequence of steps and N is a set of ground terms (the knowledge of the intruder). From the configuration $\langle (\text{RECV}(x); \text{SEND}(s); \text{COND}(e)) \cdot P, N \rangle$ a transition to (P', N') is possible iff there exists a ground substitution σ such that $x\sigma \in \overline{N}^{\mathcal{I}}$, $\sigma \models e$, $N' = N \cup \{s\sigma\}$ and $P' = P\sigma$. A *trace based-security* is a property that holds for a protocol if it holds for individual traces (runs of the protocol and intruder). Secrecy and many authentication properties can be reduced to the following *Reachability* problem:

Reachability

Input: an initial configuration $\langle P, N_0 \rangle$

Output: SAT iff there exists a reachable configuration $\langle \emptyset, M \rangle$

Protocol insecurity. A major security problem is to decide whether the intruder can deduce a secret m from a finite sequence of message exchanges P. This problem can be reduced to reachability which in turn is reduced to the resolution of some special constraint systems described below [18].

4.3 Constraint systems

We now introduce constraint systems that permit to model accurately the above reachability problems. We first extend the definition of unification systems to equational theories:

Definition 2 *(Unification systems modulo) Let $\mathcal{H}$ be a set of equational axioms on $\mathrm{T}(\mathcal{G}, \mathcal{X})$. An* $\mathcal{H}$-Unification system *$\mathcal{S}$ is a finite set of pairs of terms in $\mathrm{T}(\mathcal{G}, \mathcal{X})$ denoted by $\left\{u_i \stackrel{?}{=} v_i\right\}_{i \in \{1,\ldots,n\}}$. It is satisfied by a ground substitution σ, and we note $\sigma \models \mathcal{S}$, if for all $i \in \{1, \ldots, n\}$ $u_i\sigma =_{\mathcal{H}} v_i\sigma$.*

We say that a unification system is a *word problem* if it does not contain any variable.

Definition 3 *(Constraint systems) Let $\mathcal{I} = \langle \mathcal{G}, S, \mathcal{H} \rangle$ be an intruder system. An* $\mathcal{I}$-Constraint system *$\mathcal{C}$ is denoted: $((E_i \rhd v_i)_{i \in \{1,\ldots,n\}}, \mathcal{S})$ and it is defined by a sequence of couples $(E_i, v_i)_{i \in \{1,\ldots,n\}}$ with $v_i \in \mathcal{X}$ and $E_i \subseteq \mathrm{T}(\mathcal{G}, \mathcal{X})$ for $i \in \{1, \ldots, n\}$, and $E_{i-1} \subseteq E_i$ for $i \in \{2, \ldots, n\}$ and by an $\mathcal{H}$-unification system $\mathcal{S}$.*

A ground substitution σ satisfies a $\mathcal{I}$-Constraint system *$\mathcal{C}$ if for all $i \in \{1, \ldots, n\}$ we have $v_i\sigma \in \overline{E_i\sigma}$ and if $\sigma \models_{\mathcal{H}} \mathcal{S}$. We denote it by $\sigma \models_{\mathcal{I}} \mathcal{C}$.*

Constraint systems are denoted by $\mathcal{C}$ and decorations thereof. Note that if a substitution σ is a solution of a constraint system $\mathcal{C}$, by definition of constraint and unification systems the substitution $(\sigma)\downarrow_{\mathcal{O}}$ is also a solution of $\mathcal{C}$. In the context of cryptographic protocols the inclusion $E_{i-1} \subseteq E_i$ means that the knowledge of an intruder does not decrease as the protocol progresses.

Example 3 *We model the protocol of Example 2 by the following constraint system. First we gather all conditions in a unification system* $\mathcal{S}$

$$\mathcal{S} = \left\{ v_1 \stackrel{?}{=} \mathrm{c_{min}} \ , v_2 \stackrel{?}{=} \exp(y, B \times v_4) \ , \ v_3 \stackrel{?}{=} B \ , \ v_5 \stackrel{?}{=} M \right\}$$

The protocol execution for intruder $\mathcal{I}$ *with initial knowledge* $\{\mathrm{c_{min}}\}$ *is then expressed by the constraint:*

$$\begin{aligned}
\mathcal{C} = ((\ & \mathrm{c_{min}} \rhd v_1, \\
& \mathrm{c_{min}}, \exp(M, B \times K) \rhd v_2, \\
& \mathrm{c_{min}}, \exp(M, B \times K), B \rhd v_3, \\
& \mathrm{c_{min}}, \exp(M, B \times K), B, K \rhd v_4, \\
& \mathrm{c_{min}}, \exp(M, B \times K), B, K, \exp(v_2, \mathrm{i}(B) \times \mathrm{i}(v_4)) \rhd v_5), \\
\mathcal{S})&
\end{aligned}$$

We are not interested in general constraint systems but only in those related to protocols. In particular we need to express that a message to be sent by a honest principal at some step i should be built from previously received messages recorded in the variables $v_j, j < i$, and from the initial knowledge. To this end we define:

Definition 4 *(Deterministic Constraint Systems) We say that an* $\mathcal{I}$ *constraint system* $((E_i \rhd v_i)_{i\in\{1,\ldots,n\}}, \mathcal{S})$ *is* deterministic *if for all* i *in* $\{1, \ldots, n\}$ *we have* $\mathrm{Var}(E_i) \subseteq \{v_1, \ldots, v_{i-1}\}$

The decision problems we are interested in are the *satisfiability* and the *ordered satisfiability* of intruder constraint systems.

$\mathcal{I}$ **Satisfiability**

Input: an $\mathcal{I}$ deterministic constraint system $\mathcal{C}$

Output: SAT iff there exists a substitution σ such that: $\sigma \models_{\mathcal{I}} \mathcal{C}$.

In order to be able to combine solutions of constraints for the intruder theory $\mathcal{I}_1$ with solutions of constraint systems for intruders defined on a disjoint signature we have, as for unification, to introduce some ordering constraints to be satisfied by the solution. Intuitively, these ordering constraints prevent from introducing a cycle when building a global solution (Ordering constraints

can be arbitrary however we conjecture that some of them can be eliminated by a sharper analysis of the problem). This motivates us to define the *Ordered Satisfiability* problem:

$\mathcal{I}$ Ordered Satisfiability

Input: an $\mathcal{I}$ deterministic constraint system $\mathcal{C}$, X the set of all variables and C the set of all free constants occurring in $\mathcal{C}$ and a linear ordering $\prec$ on $X \cup C$.

Output: SAT iff there exists a substitution σ such that $\sigma \models_{\mathcal{I}} \mathcal{C}$ and for all $x \in X$ and $c \in C$, $x \prec c$ implies $c \notin \mathrm{Sub}(x\sigma)$

We are also interesting in modelling the case of a passive intruder, *i.e.* an ordered satisfiability problem in which a putative solution σ (a normal substitution) is given along with the constraint system. These can be viewed, once σ is applied, as special kind of constraint systems $((E_i \rhd v_i)_{i\in\{1,\ldots,n\}}, \mathcal{S})$ where the E_i do not contain any variable, and the unification system $\mathcal{S}$ contains only equations of type:

- $v_i \stackrel{?}{=} t_i$, where t_i a ground term;
- $t \stackrel{?}{=} t'$, where t' and t' are ground terms (word equations).

Moreover, we assume that for each $i \in \{1, \ldots, n\}$ there exists exactly one equation $v_i \stackrel{?}{=} t_i$ in $\mathcal{S}$. We say that constraint systems satisfying this requirements are *ground*.

$\mathcal{I}$ Deduction problem

Input: a ground $\mathcal{I}$ constraint system $\mathcal{C}$

Output: SAT iff all word equations are true and, for $1 \leq i \leq n$, we have $t_i \in \overline{E_i}$

5 Modes and replacements

5.1 Modes

We have seen above how to reduce protocol security problems to solving constraints on terms modulo equational theories. For this task we shall try to apply a modular approach and exploit the fact that equational theories in this context are often combination of simpler ones. When one considers the union of two equational theories over two disjoint signatures, a standard strategy for unification or constraint solving is to replace any subterm in the constraints, in a bottom-up fashion, by a new variable when the root of this subterm is below a symbol from another signature. In that way we can reduce the problem to constraint solving in pure sub-signatures.

$$\text{SIG} \ : \ \mathcal{F} \cup \mathcal{X} \to \{0,1,2\}$$
$$\text{SIG}(f) = \begin{cases} i \text{ if } f \in \mathcal{F}_i \cup \mathcal{X}_i \text{ for } i \in \{0,1\} \\ 2 \text{ otherwise, i.e. when f is a free constant} \end{cases}$$

Fig. 1. Definition of the SIG$(\cdot)$ function.

This decomposition technique cannot be applied as such in the case of non-disjoint signatures. We provide here a notion of *mode* that allows one (under some hypotheses) to decompose a term in parts without losing any deduction: the initial term can be rewritten by the equational theory iff one of its parts can be rewritten.

This notion of *mode* is different from the standard notion of *type*. The latter would impose that all considered terms must be well typed, while the former is utilised on ill moded terms to split them into well moded parts.

For all $f \in \mathcal{F} \cup \mathcal{X}$ we define a function that gives the *signature* $\text{SIG}(f)$ to which a symbol f belongs (see Figure 1). As usual we extend the function SIG to terms by setting, for a term t, $\text{SIG}(t) = \text{SIG}(\text{TOP}(t))$. In the following we assume that there exists a *mode* function $\text{M}(\cdot,\cdot)$ such that $\text{M}(f,i)$ is defined for every symbol $f \in \mathcal{F}$ and every integer i such that $1 \leq i \leq \text{AR}(f)$. Moreover we impose that for all f, i we have $\text{M}(f,i) \in \{0,1\}$ and $\text{M}(f,i) \leq \text{SIG}(f)$.

A position $p \cdot i$ (where p is a position and i a strictly positive integer) in a term t is *well-moded* with respect to M if and only if $\text{SIG}(t_{|p\cdot i}) = \text{M}(\text{TOP}(t_{|p}), i)$. We do not mention M when it is clear from context. If a position of t is not well-moded we say it is *ill-moded* in t. The root position of a term t is always ill-moded.

Let us now extend the well-moded notion:

- A term is well-moded if all its non root positions are well-moded;
- An equation $s = t$ is well-moded if s and t are well-moded and $\text{SIG}(s) = \text{SIG}(t)$; An equational presentation $\mathcal{H} = (\mathcal{G}, A)$ is well-moded if all equations $s = t$ in A are well-moded;
- A unification problem $s \stackrel{?}{=} t$ is well-moded if s and t are well-moded and $\text{SIG}(s) = \text{SIG}(t)$; A unification system $\left\{s_i \stackrel{?}{=} t_i\right\}_{i \in \mathcal{J}}$ is well-moded if s_i and t_i are well-moded and $\text{SIG}(s_i) = \text{SIG}(t_i)$ for all $i \in \mathcal{J}$;
- a substitution σ is well-moded if for any variable x we have $\text{SIG}(x) = \text{SIG}(x\sigma)$ and $x\sigma$ is a well-moded term.

We now proceed to prove that if an equational theory is well-moded then its completion is also well-moded. Since completion relies on syntactic unification,

the first step is to prove that there is a most general unifier of two well-moded terms that is well-moded.

Lemma 2 *Let t_1, t_2 be two well-moded terms with $\text{SIG}(t_1) = \text{SIG}(t_2)$. If they are unifiable there exists a well-moded most general unifier σ of t_1, t_2 such that $t_1\sigma$ is well-moded.*

PROOF. Assume t_1 and t_2 are unifiable with a most general unifier σ. We consider a derivation of σ from equation $\{t_1 = t_2\}$ using a rule-based unification algorithm (see e.g. [19]). We show by induction on the length of the derivation that for all equations $u = v$ in an intermediate system $\mathcal{IS}$, we have $\text{SIG}(u)$=$\text{SIG}(v)$ and u, v well-moded. This is initially true by assumption

If we apply a decomposition rule to a well-moded equation $f(\ldots, u, \ldots) = f(\ldots, v, \ldots)$ to get $u = v$, then $u = v$ is well-moded and $\text{SIG}(u) = \text{SIG}(v) = \text{M}(f, i)$ for some i. If we apply a replacement of $x = t$ in $u = v$, since $\text{SIG}(x) = \text{SIG}(t)$ and $u = v$ is well moded by induction hypothesis, the operation replaces occurrences of x by a well-moded term with a top symbol in the same signature. The other cases are trivial. We finally notice that σ, considered as a set of equations, is well-moded, and thus, when replacing variables by their value, that $t_1\sigma$ is well-moded. □

Proposition 1 *If $\mathcal{H}$ is a well-moded consistent equational presentation then there is a convergent rewrite system $\mathcal{O}$ that defines the same equational congruence and such that $\mathcal{O}$ is well-moded (when its rules are considered as equations).*

PROOF. We apply the unfailing completion procedure [19,22] to $\mathcal{H}$ to construct the convergent rewrite system $\mathcal{O}$. Let us prove by induction that all generated equations $l = r$ are well-moded. This is true at the start of the procedure by hypothesis on $\mathcal{H}$. Let us now assume that at some point a set of well-moded equations $\mathcal{H}$' has been generated, and that there exists a critical pair between two well-moded equations $l = r$ and $g = d$. The procedure unifies a non-variable subterm l' of l at a position p with the non-variable term g. Since l' and g are non-variable, their unifiability implies that $\text{TOP}(l') = \text{TOP}(g)$ and thus $\text{SIG}(l') = \text{SIG}(g)$. Since l is well-moded, the term l' is also well-moded. Thus the equation $l' = g$ is well-moded, and by Lemma 2 there exists a well-moded mgu σ of l' and g such that for any variable x we have $\text{SIG}(x\sigma) = \text{SIG}(x)$. Moreover we have $\text{SIG}(l') = \text{SIG}(g) = \text{SIG}(d)$ since $\mathcal{H}$' is well-moded. Thus the equation $r\sigma = l[p \leftarrow d\sigma]$ added to $\mathcal{H}$' is well-moded. By induction, all equations of the obtained equation system $\mathcal{O}$ are well-moded. □

We call a *subterm value* of a term t a syntactic subterm of t that is either t itself, an atom in t, or occurs at an ill-moded position in t. We denote $\text{Sub}(t)$ the set of subterm values of t. By extension, for a set of terms E, the set

$\mathrm{Sub}(E)$ is defined as the union of the subterm values of the elements of E. The subset of the maximal and strict subterm values of a term t plays an important role in the sequel. We call these subterm values the *factors* of t, and denote this set $\mathrm{Factors}(t)$. By definition this set is empty if t is itself an atom.

Example 4 *Consider two binary symbols f and g with $\mathrm{SIG}(f) = \mathrm{SIG}(g) = 1$ and:*

$$\begin{cases} \mathrm{M}(f,1) = \mathrm{M}(g,1) = 1 \\ \mathrm{M}(f,2) = \mathrm{M}(g,2) = 0 \end{cases}$$

Consider the term $t = f(f(g(a,b), f(c,c)), d)$. Its subterm values are a, b, $f(c,c)$, c, d, and its factors are a, b, $f(c,c)$ and d.

In the rest of this paper and unless otherwise indicated, *the notion of subterm will refer to subterm values.* From now on we assume that $\mathcal{E}$ is a well-moded equational presentation, and thus that R is a well-moded rewrite system. Under this assumption, one can prove that rewriting never overlaps subterm values (see Lemma 4 below). We will use in the sequel a direct consequence of the definition of subterms, which is that if $s \in \mathrm{Sub}(t) \setminus \{t\}$ then either s is an atom or occurs at an ill-moded position in t.

The following lemma is a simple property of consistent equational theories:

Lemma 3 *If $\mathcal{H}$ is a consistent equational theory then for any equation $l = r$ in a presentation of $\mathcal{H}$ if there exists a substitution τ such that $l\tau > r\tau$ then l is not a variable.*

Proof. By contradiction assume that l is a variable and that there exists a ground substitution τ such that $l\tau > r\tau$. By the subterm property of simplification orderings we have $l \notin \mathrm{Var}(r)$. Let τ_1 and τ_2 be two substitutions of support $\mathrm{Var}(r) \cup \{l\}$ and equal to τ on $\mathrm{Var}(r)$ and such that $l\tau_1$ and $l\tau_2$ are two different free constants. We have $l\tau_1 =_{\mathcal{H}} r\tau_1 = r\tau = r\tau_2 =_{\mathcal{H}} l\tau_2$. This contradicts the fact that $\mathcal{H}$ is consistent.

□

Lemma 4 *Assume that R is a set of well-moded equations, that $l = r \in R$, and that $s \to_R s'$ with $s = s[q \leftarrow l\tau]$, $s' = s[q \leftarrow r\tau]$, and $l\tau > r\tau$. If p is ill-moded in s and $q \leq p$ then there exists a position q' in l such that a variable occurs at position q' in l and $q \cdot q' \leq p$.*

Proof. Since l is well-moded p cannot be equal to $q \cdot j$ with j position of a function symbol in t. Hence p refers to a position in the substitution τ. □

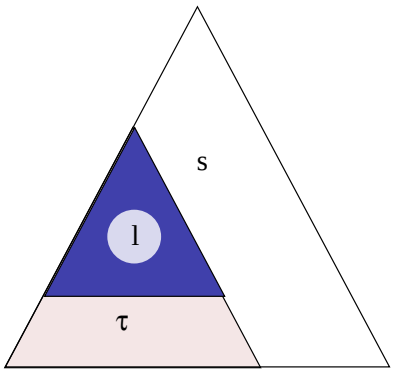

Fig. 2. Lemma 4 states that ill-moded positions do not occur in the dark zone since this part is well-moded

5.2 Normalisation and replacement

5.2.1 Subterms and normalisation

We now study the evolution of the subterms of a term t when t is being normalised. By considering the application of an equation in R with minimal right-hand side and assuming the theory is well-moded, we can prove that (ordered) rewriting by R preserves factors in normal form. Since R is convergent, this allows us to prove the following lemma.

Lemma 5 *Let t be a ground term with all its factors in normal form. If t' is minimal for $<$ among the terms u such that $t \to_R u$ then*

- *either* $\text{SIG}(t) = \text{SIG}(t')$ *and* $\text{Factors}(t') \subseteq \text{Factors}(t) \cup \text{C}_{\text{spe}}$ *or*
- $\text{SIG}(t) \neq \text{SIG}(t')$ *and* $t' \in \text{Factors}(t) \cup \text{C}_{\text{spe}}$.

Proof. Assume $t \to_R t'$ with t' minimal among the terms u such that $t \to_R u$. Let $l \to r \in R$ be the rule applied on t at position p with substitution σ in order to obtain t'. Since the factors are in normal form the position p is above or incomparable to any position of a factor of t and thus all positions p' above p (including p) are either ϵ or well-moded.

Let q be a position of a factor s of t. By Lemma 4 either q is incomparable with p, and thus s is also a factor of t' at position q, or there exists a variable x at a position p' in l such that $p \cdot p' \leq q$. Since q is a minimal ill-moded position in t, we have that s is either equal to or a factor of $x\sigma$.

By minimality of t' and by monotonicity of $<$ we can assume that variables of r are either variables of l or instantiated by the constant c_{min}. Since $\text{Var}(r)\sigma \subseteq \text{Var}(l)\sigma \cup \{\text{c}_{\text{min}}\}$ and since r is well-moded, we have

- $r\sigma$ is a factor of t and r is a variable,

- or $\text{Factors}(r\sigma) \subseteq \text{Factors}(t) \cup \text{C}_{\text{spe}}$.

Only two cases are possible:

1. $p \neq \epsilon$ or r is not a variable: If $p \neq \epsilon$ we have $\text{TOP}(t) = \text{TOP}(t')$, and thus $\text{SIG}(t) = \text{SIG}(t')$. Otherwise if $p = \epsilon$ then r is not a variable by assumption. Since by Lemma 3 l is not a variable either and since the equational theory is well-moded, one has $\text{SIG}(l) = \text{SIG}(r)$ and thus $\text{SIG}(t) = \text{SIG}(t')$. In both cases one has $\text{Factors}(t') \subseteq \text{Factors}(t) \cup \text{C}_{\text{spe}}$ and $\text{SIG}(t') = \text{SIG}(t)$.
2. $p = \epsilon$ and r is a variable of l: Notice first that since $p = \epsilon$ we have $t' = r\sigma$. Since the equational theory is well-moded we have $\text{SIG}(r) = \text{SIG}(l)$. Let f be a symbol of $\mathcal{F}$ such that r occurs as a i-th argument of f in l. Since l is well-moded we have $\text{M}(f, i) = \text{SIG}(r) = \text{SIG}(l)$. Since $p = \epsilon$ we have $\text{TOP}(t) = \text{TOP}(l)$ and thus $\text{M}(f, i) = \text{SIG}(t)$. There are two sub-cases:
   · If $r\sigma$ is at a position of a factor of t, then $r\sigma$ is ill-moded at this position, *i.e.* $\text{SIG}(r\sigma) \neq \text{M}(f, i)$, and therefore $\text{SIG}(r\sigma) \neq \text{SIG}(t)$ and we indeed have $t' \in \text{Factors}(t)$ and $\text{SIG}(t') \neq \text{SIG}(t)$;
   · Otherwise $r\sigma$ is well-moded, and since $\text{SIG}(r) = \text{SIG}(l)$ this implies that $\text{SIG}(r\sigma) = \text{SIG}(l\sigma)$ and thus $\text{SIG}(t') = \text{SIG}(t)$. One then easily sees that $\text{Factors}(t') \subseteq \text{Factors}(t) \cup \text{C}_{\text{spe}}$.

□

Lemma 6 *Let t be a term with all its factors in normal form. Then either*

- $(t)\!\downarrow \in \text{Factors}(t) \cup \text{C}_{\text{spe}}$ *and* $\text{SIG}((t)\!\downarrow) \neq \text{SIG}(t)$*;*
- *Or* $\text{SIG}((t)\!\downarrow) = \text{SIG}(t)$.

In both cases one has $\text{Sub}((t)\!\downarrow) \subseteq (\text{Sub}(t))\!\downarrow \cup \text{C}_{\text{spe}}$.

Proof. It suffices to apply Lemma 5 along a derivation normalising t such that at each step a minimal successor (with respect to $<$) for the relation $\rightarrow_R$ is chosen. □

Lemma 7 *For any normalised substitution σ, for any term m and for any $s \in \text{Sub}((m\sigma)\!\downarrow)$ one of the following holds:*

- $s \in \text{C}_{\text{spe}}$*;*
- *There is $u \in \text{Sub}(m)$ such that $(u\sigma)\!\downarrow = s$ and $\text{SIG}(u) = \text{SIG}(s)$;*
- *There exists $x \in \text{Var}(m)$ such that $s \in \text{Sub}(x\sigma)$.*

Proof. Let m and s be two terms and let σ be a ground substitution such that $s \in \text{Sub}((m\sigma)\!\downarrow)$. We have

$$\text{Sub}((m\sigma)\!\downarrow) \subseteq (\text{Sub}(m)\sigma)\!\downarrow \cup \text{Sub}(\text{Var}(m)\sigma) \cup \text{C}_{\text{spe}}$$

Assume there exists no $x \in \text{Var}(m)$ such that $s \in \text{Sub}(x\sigma)$ and $s \notin \text{C}_{\text{spe}}$. Let

$u \in \mathrm{Sub}(m)$ be minimal for the subterm relation such that $(u\sigma)\downarrow = s$. The above inclusion and $s \notin \mathrm{Sub}(\mathrm{Var}(m)\sigma) \cup \mathrm{C_{spe}}$ imply u is well-moded. If it is a constant we have necessarily $u = s$ and $\mathrm{SIG}(u) = \mathrm{SIG}(s)$. Assume now u is neither a constant or a variable and thus $\mathrm{Factors}(u)$ is not empty.

By minimality of u we have $s \notin ((\mathrm{Sub}(u) \setminus \{u\})\sigma)\downarrow$. Thus for all v in $\mathrm{Sub}(u) \setminus \{u\}$ the above inclusion (replacing m by v) imply $s \notin \mathrm{Sub}((v\sigma)\downarrow)$. Consider now a bottom-up normalisation of $u\sigma$ stopping at factors of u and let t be the obtained term. By Lemma 6 and $s \notin \mathrm{C_{spe}} \cup \mathrm{Factors}(t)$ we have $\mathrm{SIG}(t) = \mathrm{SIG}(s)$. By definition of t we have $\mathrm{SIG}(t) = \mathrm{SIG}(u)$. Therefore there exists $u \in \mathrm{Sub}(m)$ such that $(u\sigma)\downarrow = s$ and $\mathrm{SIG}(u) = \mathrm{SIG}(s)$. □

5.2.2 Replacement and normalisation

We now give conditions under which the replacement of a normal subterm s of a term t commutes with the normalisation of t. We denote $\delta_{u,v}$ the replacement of u by v such that if u appears at positions Π_u *as a subterm* (*i.e.* as a subterm value) of t then $t\delta_{u,v} = t[\Pi_u \leftarrow v]$. We denote in short δ_u the replacement $\delta_{u,\mathrm{c_{min}}}$.

We define the notion of *free terms*.A ground term s is *free* in a set of terms T with respect to a ground substitution σ if there is no $t \in T$ such that $(t\sigma)\downarrow = (s)\downarrow$. A term which is not free is said to be *bound* by σ in T. We will omit σ or T when they are clear from context. Since rewriting by R never overlaps subterm values, we can prove that normalisation and subterm replacement commute.

Lemma 8 *Let t be a ground term with all its factors in normal form, and let s be a ground term in normal form with $s \neq (t)\downarrow$ and $s \notin \mathrm{C_{spe}}$. Then we have $(t\delta_s)\downarrow = ((t)\downarrow\delta_s)\downarrow$.*

Proof. We consider a sequence of application of rules of R that normalises t such that, at each step a minimal successor for the relation $\rightarrow_R$ is chosen. Consider the sequence $t_1 = t, \ldots, t_n = (t)\downarrow$ of the intermediate terms. For $1 \leq i < n$ the term t_i is not in normal, and thus is in $\mathrm{Factors}(t_{i-1}) \cup \mathrm{C_{spe}}$. Thus by Lemma 5 and for $2 \leq i < n$ we have $\mathrm{SIG}(t_i) = \mathrm{SIG}(t_{i-1})$ and $\mathrm{Factors}(t_i) \subseteq \mathrm{Factors}(t_{i-1}) \cup \mathrm{C_{spe}}$. By iteration one thus obtains that for $i < n$ one has $\mathrm{SIG}(t_i) = \mathrm{SIG}(t)$ and $\mathrm{Factors}(t_i) \subseteq \mathrm{Factors}(t) \cup \mathrm{C_{spe}}$, and therefore the factors of t_i are in normal form for all $i \in \{1, \ldots, n\}$. Thus the rule $l_i \rightarrow r_i \in R$ applied on t_i is applied above (and without interfering with) the factors by Lemma 4. On the other hand the replacement is applied below (or at the level of) the factors of t_i.

Therefore the sequence $t_1 \rightarrow_R \ldots \rightarrow_R t_n$ implies the equalities $t_1\delta_s =_{\mathcal{E}} \ldots =_{\mathcal{E}} t_n\delta_s$, and thus by transitivity of the equality, $t\delta_s =_{\mathcal{E}} (t)\downarrow\delta_s$. We conclude by

convergence of R. □

Example 5 *Consider the equational theory $\mathcal{E} = \{f(g(x)) = x\}$. We have:*

– by definition of the mode function: $\begin{cases} \text{SIG}(f) \geq \text{M}(f,1) \\ \text{SIG}(g) \geq \text{M}(g,1) \end{cases}$

– since $f(g(x))$ is well-moded: $\begin{cases} \text{M}(f,1) = \text{SIG}(g) \\ \text{M}(g,1) = \text{SIG}(x) \end{cases}$

– since the theory is well-moded: $\text{SIG}(f) = \text{SIG}(x)$

This implies that, depending on the signature to which f belongs, we have either

$$\text{SIG}(f) = \text{SIG}(g) = \text{SIG}(x) = \text{M}(g,1) = \text{M}(f,1) = 0$$

or

$$\text{SIG}(f) = \text{SIG}(g) = \text{SIG}(x) = \text{M}(g,1) = \text{M}(f,1) = 1$$

Since there is no critical pairs and the right-hand side is a subterm of the left-hand side, the rewrite system obtained by unfailing completion is $f(g(x)) \to x$. Consider now the terms $t = f(g(a))$ and $s = g(a)$. In both choices of the mode function, the subterms of t are t and a, and thus $t\delta_s = t$. This shows how the notion of mode permits to define replacements compatible with normalisation.

Let s be a normalised ground term and let σ be a ground normal substitution. Next lemma shows that under the provision that a normalised term s is free in $\text{Sub}(t)$ for a ground substitution σ, the replacement of s in $(t\sigma)\!\downarrow$ yields the same result as the replacement of s in σ. This will permit to transfer a pumping argument on instantiated terms to a pumping argument on substitutions. The proof again relies on the convergence of R.

Lemma 9 *Let t be a term, σ be a normalised substitution and s be a ground term in normal form. Assume s is free in $\text{Sub}(t)$ for σ and let $\sigma' = (\sigma\delta_s)\!\downarrow$. We have:*

$$((t\sigma)\!\downarrow\delta_s)\!\downarrow = (t\sigma')\!\downarrow$$

Proof. Since R is ground convergent it is sufficient to prove:

$$(t\sigma)\!\downarrow\delta_s =_R t\sigma'$$

For all variables x we have $x\sigma' =_R x(\sigma\delta_s)$ by definition of σ', and thus:

$$t\sigma' =_R t(\sigma\delta_s)$$

Since s is free and normalised, there is no subterm r of t, even with r variable, such that $(r\sigma)\downarrow = s$, and thus such that $r\sigma = s$. Therefore we have, by definition of δ_s as a replacement on subterm values:

$$t(\sigma\delta_s) =_R (t\sigma)\delta_s$$

Moreover we have $(t\sigma)\downarrow =_R t\sigma$. Since σ is normalised we have $\mathrm{Sub}((t\sigma)\downarrow) \subseteq (\mathrm{Sub}(t)\sigma)\downarrow \cup \mathrm{Sub}(\sigma)$ and $\mathrm{Sub}(t\sigma) \subseteq \mathrm{Sub}(t)\sigma \cup \mathrm{Sub}(\sigma)$. Since s is free and normalised it is neither in $\mathrm{Sub}(t)\sigma$ nor in $(\mathrm{Sub}(t)\sigma)\downarrow$. Thus we have:

$$((t\sigma)\downarrow)\delta_s =_R (t\sigma)\delta_s$$

Hence we have $(t\sigma)\downarrow\delta_s =_R t\sigma'$ which completes the proof. □

Example 6 *Consider now the equational theory $\mathcal{E} = \{f(x,x) = 0\}$, the term $t = f(f(x,x), f(x, g(\mathrm{c}_{\min})))$ and the substitution σ such that $x\sigma = g(a)$, and consider the replacement δ_a. Using the notations of Lemma 9, we have $x\sigma' = g(\mathrm{c}_{\min})$, and thus $t\sigma' = f(f(g(\mathrm{c}_{\min}), g(\mathrm{c}_{\min})), f(g(\mathrm{c}_{\min}), g(\mathrm{c}_{\min})))$, while on the other hand $(t\sigma)\downarrow\delta_a = f(0, f(g(\mathrm{c}_{\min}), g(\mathrm{c}_{\min})))$. This example shows that even though s is in normal form, an extra normalisation is needed after replacement. Replacing one of the occurrence of x by $g(a)$ also shows why we need s to be free in Lemma 9.*

6 Well-moded intruder systems

From now on we will consider intruder systems over the signature $\mathcal{F}_0 \cup \mathcal{F}_1$ modulo the equational theory $\mathcal{E} = \mathcal{E}_0 \cup \mathcal{E}_1$ as defined in Section 3.1. Let $\mathcal{I}_1 = \langle \mathcal{F}, \mathcal{S}, \mathcal{E} \rangle$ be an intruder system where terms in $\mathcal{S}$ are well-moded. Such an intruder system is called a *well-moded intruder*. The nice structure of well-moded intruder will allow one to design an algorithm for intruder constraint solving, under some hypotheses.

We can show that there is at most one alternation of signature on all well-moded terms:

Lemma 10 *Every well-moded term t can be written $t = t'\sigma$ where t' is a pure 1-term (possibly a variable) and σ a substitution that maps all variables in its support to pure 0-terms.*

Proof. Since t is well moded, below an occurrence of a $\mathcal{F}_0$ symbol, we can find only $\mathcal{F}_0$ symbols. □

In the case of a well-moded intruder it is possible to split $\mathcal{S}$ into two sets of well-moded terms $\mathcal{S}_0$ and $\mathcal{S}_1$ such that for all terms t in $\mathcal{S}_i$ we have $\mathrm{SIG}(t) = i$

for $i \in \{0,1\}$ and such that $\mathcal{S}_0$ contains terms built from symbols of $\mathcal{F}_0$. This permits to extract from $\mathcal{I}_1$ a simpler intruder, namely $\mathcal{I}_0 = \langle \mathcal{F}_0, \mathcal{S}_0, \mathcal{E}_0 \rangle$. In the sequel, we will reduce some decision problems on $\mathcal{I}_1$ to decision problems on $\mathcal{I}_0$ under some adequate hypotheses. We define $E \to_{\mathcal{S}_0} F$ (resp. $E \to_{\mathcal{S}_1} F$, resp. $E \to_{\mathcal{S}} F$) if $E \to_{l \to r} F$ with $l \to r \in \mathrm{L}^{t,\mathrm{g}}$ for $t \in \mathcal{S}_0$ (resp. $\mathcal{S}_1$, resp. $\mathcal{S}$).

Properties of deduction rules. Under the assumption that $\mathcal{S}$ is well-moded, one can prove the following key lemmas. Lemma 12 states that when a term appears as a new subterm of a knowledge set, it has just been built by the intruder. Considering a derivation, this will permit to apply Lemma 14 iteratively in order to show that this term may be eliminated from the derivation. This is the main step of the proof that terms not appearing as instance subterms of the initial constraint systems can be replaced by smaller terms (with respect to the ordering $<$ on ground terms) in a solution to yield a smaller solution.

Lemma 11 *Assume that E, F and s are in normal form and $E \to_{\mathrm{L}^{u,\mathrm{g}}} F$ using rule $u \in \mathcal{S}$ with substitution τ, and such that $s \notin (F \cup \mathrm{C}_{\mathrm{spe}}) \setminus E$. If for all $x \in \mathrm{Var}(u)$ such that $x\tau = s$ we have $\mathrm{SIG}(x) \neq \mathrm{SIG}(s)$ then $(E\delta_s)\!\downarrow \to_{\mathrm{L}^{u,\mathrm{g}}} (F\delta_s)\!\downarrow$*

Proof. First let us assume that the rule is not a stutter (*i.e.* is such that $F \neq E$), and thus $(u\tau)\!\downarrow \notin E$. Then, let us notice that if u has no variables, the left-hand side of the deduction rule is empty, and thus the same rule can be applied on $(E\delta_s)\!\downarrow$. Since u is a pure term its atoms are constants in $\mathrm{C}_{\mathrm{spe}}$. Thus $s \notin (F \cup \mathrm{C}_{\mathrm{spe}}) \setminus E$ implies $s \notin \mathrm{Sub}((u)\!\downarrow)$, and thus $(F\delta_s)\!\downarrow = (E\delta_s)\!\downarrow \cup \{u\}$. The lemma is thus valid in this specific case. Let us now review the general case.

By definition of $\mathcal{S}$ the term u is well-moded. The restriction on $x\tau$ permits to ensure that all occurrences of r as a subterm in $\mathrm{Var}(u)\tau$ are ill-moded in $u\tau$. The restriction $s \notin (F \cup \mathrm{C}_{\mathrm{spe}}) \setminus E$ and the fact that the transition is not a stutter imply $(u\tau)\!\downarrow \neq s$. Since E is in normal form and u is well-moded the factors of $u\tau$ are in normal form and we can apply Lemma 9, which yields the desired result. □

Lemma 12 *Assume E and F are in normal form. If $E \to_{\mathcal{I}} F$ and $t \in \mathrm{Sub}(F) \setminus (\mathrm{Sub}(E) \cup \mathrm{C}_{\mathrm{spe}})$, then $F \setminus E = t$ and $E \to_{\mathrm{L}^{u,\mathrm{g}}} F$, with $u \in \mathcal{S}$ and $\mathrm{SIG}(u) = \mathrm{SIG}(t)$.*

Proof. The hypotheses permit to apply Lemma 6. If the rule is applied with substitution τ this implies $\mathrm{Sub}((u\tau)\!\downarrow) \subseteq \{(u\tau)\!\downarrow\} \cup \mathrm{Sub}(E) \cup \mathrm{C}_{\mathrm{spe}}$. Thus $t \notin \mathrm{Sub}(E) \cup \mathrm{C}_{\mathrm{spe}}$ implies $t = (u\tau)\!\downarrow$ and $t \notin \mathrm{C}_{\mathrm{spe}} \cup \mathrm{Factors}(u\tau)$. Thus by Lemma 6 $\mathrm{SIG}(t) = \mathrm{SIG}(u\tau) = \mathrm{SIG}(u)$. □

Lemma 13 *Let $D : E_0 \to \ldots \to E_n$ be a derivation such that there exists $s \in \mathrm{Sub}(E_i) \setminus (\mathrm{Sub}(E_0) \cup \mathrm{C_{spe}})$. Then there exists in D a step $E_{j-1} \to_{l_s \to s} E_j$ with $j \leq i$ and $l_s \to s \in \mathrm{L}^{u,\mathrm{g}}$ with $\mathrm{SIG}(u) = \mathrm{SIG}(s)$.*

Proof. Consider the minimal index j such that $s \in \mathrm{Sub}(E_j)$. By hypothesis we have $j > 0$ and $j \leq i$. Moreover by minimality of j we have $\mathrm{Sub}(E_j) \neq \mathrm{Sub}(E_{j-1})$. Since $s \notin \mathrm{C_{spe}}$ Lemma 12 implies that $E_j = E_{j-1}, s$, and that if $E_{j-1} \to_{l_s \to s} E_j$ with $l_s \to s \in \mathrm{L}^{u,\mathrm{g}}$ then $\mathrm{SIG}(u) = \mathrm{SIG}(s)$. □

Lemma 14 *Assume E, s and t are in normal form, $s \notin (E \cup \mathrm{C_{spe}})$, $s \neq t$ and $\mathrm{c_{min}} \in E$. Then $E, s \to E, s, t$ implies $(E\delta_s)\!\downarrow, s \to ((E,t)\delta_s)\!\downarrow, s$.*

Proof. Assume $E, s \to_{\mathrm{L}^{u,\mathrm{g}}} t$ and let τ be the normal substitution such that $\mathrm{Var}(u)\tau \subseteq E, s$ and $(u\tau)\!\downarrow = t$. We have $(t\delta_s)\!\downarrow = ((u\tau)\!\downarrow\delta_s)\!\downarrow$ by definition of t. Since E (and thus τ) is in normal form the factors of $u\tau$ are in normal form. Thus by Lemma 8 we have $((u\tau)\delta_s)\!\downarrow = (t\delta_s)\!\downarrow$.

The replacement δ_s is applied at all occurrences of s as a subterm of $u\tau$. Since u is well-moded and $u\tau \neq s$, this implies that all replacements occur at or below the level of variables of u. Given $x \in \mathrm{Var}(u)$ two cases may occur:

- If $\mathrm{SIG}(x) = \mathrm{SIG}(x\tau)$ the replacement is applied on all occurrences of s as subterm of the factors of $x\tau$;
- If $\mathrm{SIG}(x) \neq \mathrm{SIG}(x\tau)$ the replacement is applied on all occurrences of s as a subterm of $x\tau$.

From this we can construct a substitution τ' such that:

- $x\tau' = s$ if $x\tau = s$ and $\mathrm{SIG}(x) = \mathrm{SIG}(x\tau)$;
- $x\tau' = ((x\tau)\delta_s)\!\downarrow$ otherwise.

This substitution yields a rule in $\mathrm{L}^{u,\mathrm{g}}$ that, applied on $(E\delta_s)\!\downarrow, s$, permits to deduce $(t\delta_s)\!\downarrow$ by construction. □

6.1 Hypotheses on intruder systems

6.1.1 Locality hypothesis on intruder systems.

The previous lemma will be used in conjunction with an extra hypothesis that is related to the locality property [21]. Notice that this assumption is satisfied if the theory $\mathcal{E}_1$ is defined on $\mathcal{F}_1$ and $\mathcal{S}_1$ only contains pure 1-terms.

Hypothesis 1: If $E \to_{\mathcal{S}_1} E, r \to_{\mathcal{S}_1} E, r, t$ and $r \notin \mathrm{Sub}(E, t) \cup \mathrm{C_{spe}}$ then there is a set of terms F such that $E \to^*_{\mathcal{S}_0} F \to_{\mathcal{S}_1} F, t$.

Under this hypothesis when a subterm can be derived with several successive applications of rules in $\mathcal{S}_1$ it can be obtained with a unique application too. This allows one to bound the number of $\mathcal{S}_1$ rule applications in a derivation with respect to the number of subterms in the constraint system we attempt to solve.

Let us define the *closure* of $\mathcal{S}_1$ as the smallest set $\langle \mathcal{S}_1 \rangle$ of terms that contains $\mathcal{S}_1$ and such that if $s, s' \in \mathcal{S}_1$ and x is a variable of s of mode 1 then $s[x \leftarrow s'] \in \langle \mathcal{S}_1 \rangle$. By construction the set $\langle \mathcal{S}_1 \rangle$ contains only terms with head in $\mathcal{F}_1$ and thus contains only well-moded terms.

Note that in Hypothesis 1 the condition $r \notin \mathrm{Sub}(E, t) \cup \mathrm{C_{spe}}$ implies that $r \notin \mathrm{Sub}(E)$ and thus is of signature 1. Its ill-moded occurrences in the second rule application can be replaced by $\mathrm{c_{min}}$, and its well-moded occurrences can be replaced by composing a new deduction rule in the closure $\langle \mathcal{S}_1 \rangle$. Thus we can prove that for any set of terms $\mathcal{S}_1$ the set of terms $\langle \mathcal{S}_1 \rangle$ satisfies Hypothesis 1, the drawback of this construction being that $\langle \mathcal{S}_1 \rangle$ may be infinite.

6.1.2 Unique matching property

We consider now a unique matching property. That is, given an arbitrary ground term t, we require that the matching of t by a term s in $\mathcal{S}_1$ either fails (has no solution) or has a unique solution if the variables of signature 1 of s are already instantiated by ground terms.

> Hypothesis 2: For all terms $s \in \mathcal{S}_1$, for all substitutions τ such that $(\mathcal{X}_1 \cap \mathrm{Var}(s))\tau \subseteq \mathrm{T}(\mathcal{F})$ and for all ground terms t there is **at most one** ground substitution σ such that $s\tau\sigma =_{\mathcal{H}} t$, and this substitution can be computed.

In other words, a matching equation $t \stackrel{?}{=} s$ (with the above notations) determines a partial mapping from the set of ground substitutions of support $\mathcal{X}_1 \cap \mathrm{Var}(s)$ to the set of ground substitutions of support $\mathcal{X}_0 \cap \mathrm{Var}(s)$.

Notice that Hypothesis 2 is satisfied when the presentation $\mathcal{H}$ is a union of two presentations on disjoint signatures as in [10,11]: In this case one can choose a mode function such that the mode of the j-th argument of an operator in $\mathcal{F}_i$ is always i. With this choice the hypothesis is always true since all variables of a term $s \in \mathcal{S}_1$ are instantiated by the substitution τ.

6.1.3 Reducibility of $\mathcal{E}$ to $\mathcal{E}_0$

Let us define what we mean by reduction of an equational theory to another one.

Definition 5 *(Reduction algorithm) A computable function $\mathcal{A}(\_)$ is a* reduction algorithm *from an equational theory $(\mathcal{F}, \mathcal{E})$ to an equational theory $(\mathcal{F}', \mathcal{E}')$ iff for any general unification system S modulo $\mathcal{E}$, the result $\mathcal{A}(S)$ is a finite list of couples $((\mathcal{A}_i, S_i))_{1 \leq i \leq n}$ such that:*

$$Sol(S) = \bigcup_{i=1}^{n} \mathcal{A}_i(Sol(S_i))$$

where the S_i are general unification systems modulo $\mathcal{E}'$, the $\mathcal{A}_i$ are mappings from the set of substitutions to itself, and $Sol(S')$ denotes the set of solutions of system S'.

When only satisfiability of unification systems modulo $\mathcal{E}$ is considered, we will also call reduction algorithm a non-deterministic procedure that guesses one of the S_i. An example of reduction algorithm is *basic narrowing* for the equational theory $(\{e, d\}, \{d(e(x, y), y) = x\})$. For solving a general unification problem in this theory we can apply the basic narrowing procedure which is a combination of rewriting and instanciation (see e.g. [34]). The S_i are the systems derived by the basic narrowing procedure. We can solve these systems in the theory $(\{e, d\}, \emptyset)$ and we get $\mathrm{Sol}(S_i)$, for each i. The algorithm $\mathcal{A}_i$ applies the substitution that has been computed in the narrowing process to each element of $\mathrm{Sol}(S_i)$ in order to compute an element of $\mathrm{Sol}(S)$.

Moreover any solution of the initial problem S can be obtained that way.

Hypothesis 3: The equational theory $(\mathcal{F}, \mathcal{E})$ is reducible to $(\mathcal{F}_0, \mathcal{E}_0)$

Note that in the special case where $\mathcal{E}_1$ does not depend on symbols in $\mathcal{F}_0$ we can take for $\mathcal{A}(\_)$ a decomposition procedure similar to the one employed for unifiability in disjoint theories by [34,3].

A much more interesting example of reduction is given by the *finite variant property* from [13]. The reduction definition that we give here is similar to Comon-Lundh and Delaune's one, but is slightly more general since we neither specify how the reduction is to be done (by narrowing in their definition) nor impose conditions on $\mathcal{E}_0$ (which is required to be finitary in [13]). It turns out that, quite surprisingly, there is an example of an intruder system [7] which is reduced to an intruder equipped with the AU equational theory and for which ordered satisfiability of deterministic constraint systems is decidable. We believe that covering the associativity of the concatenation operator, an

important property in practice, is an advantage of our approach [3].

7 Minimal solutions of constraint systems

We show now that whenever a constraint system is satisfiable it admits a solution whose subterms can be obtained by instanciating subterms of the given constraint system. Thanks to Hypothesis 1 this will give a bound on the number of $\mathcal{S}_1$ rule applications.

Let σ be a normal ground substitution and $\mathcal{C}$ be a constraint system. We say that σ is *bound* in $\mathcal{C}$ if for every $s \in \mathrm{Sub}(\mathrm{Var}(\mathcal{C})\sigma)$ the term s is bound by σ in $\mathrm{Sub}(\mathcal{C})$. The goal of this section is to prove that whenever a constraint system $\mathcal{C}$ is satisfiable, there exists a normal ground substitution σ bound in $\mathcal{C}$ such that $\sigma \models \mathcal{C}$. The last key ingredient to this proof is the notion of quasi well-formed derivations.

Definition 6 *A derivation $E_0 \rightarrow^* E_n$ and of goal t is quasi well-formed if for every term $u \in \mathrm{Sub}(E_n)$ we have $\mathrm{SIG}(u) = 1$ implies $u \in \mathrm{Sub}(E_0, t) \cup \mathrm{C_{spe}}$.*

Our goal in the rest of this section will be to prove that for all E and t either $t \notin \overline{E}$ or there exists a quasi well-formed derivation starting from E of goal t if $\mathcal{I}$ satisfies Hypothesis 1, and to give some properties of these derivations. Let us from now on assume this is the case for the well-moded intruder system $\mathcal{I}$.

Lemma 15 *Assume $\mathrm{c_{min}} \in E$ and E is in normal form. If $t \in \overline{E}$ there exists a quasi well-formed derivation starting from E of goal t.*

Proof. Given a derivation $D : E \rightarrow^* F$ starting from E of goal t we define $\Omega_D = \{s \in \mathrm{Sub}(F) \mid \mathrm{SIG}(s) = 1 \text{ and } s \notin \mathrm{Sub}(E, t) \cup \mathrm{C_{spe}}\}$.

By contradiction assume there exists a term t and a set of terms E, both in normal form, such that

$$\min(\{|\Omega_D| \mid D \text{ starts from } E \text{ of goal } t\}) > 0$$

Among the derivations starting from E of goal t let D be a derivation such that $|\Omega_D|$ is minimal among the derivations starting from E of goal t. Let $D : E = E_0 \rightarrow E_1 \rightarrow \ldots \rightarrow E_n = F$ and $s \in \Omega_D$. Let us contradict the minimality of D.

[3] In this case, the $\mathcal{A}_i$ is a function built incrementally during the narrowing process, when one collects the unifiers applied so far.

Claim 1 *There exists an index $i_s < n$ such that $s = E_{i_s} \setminus E_{i_s-1}$ and $s \notin \mathrm{Sub}(E_{i_s-1})$ and $E_{i_s-1} \to_{\mathrm{L}^{u,\mathrm{g}}} E_{i_s}$ with $u \in \mathcal{S}_1$.*

Proof of the claim. Let i_s be minimal among the indices i such that $s \in \mathrm{Sub}(E_i)$. The claim is an application of Lemma 12 on this transition. $\diamond$

We now assume s is of maximal index, *i.e.* that no term t_j of signature 1 produced by rule in $\mathcal{S}_1$ with $j > i_s$ is in Ω_D. Moreover, for $j > i_s$ one can apply Lemma 14 to construct a derivation D':

$$E_0 \to^* E_{i_s} \to (E_{i_s+1}\delta_s)\downarrow, s \to \ldots \to (E_n\delta_s)\downarrow, s$$

Iterating the replacement of s by $\mathrm{c}_{\min}$ if necessary, we assume that $s \notin \mathrm{Sub}((E_j\delta_s)\downarrow)$ for $j \in \{0, \ldots, n\}$. If we extend $<$ as a total order on sets of terms, one easily see (see proof of Proposition 4, for example) that this iteration terminates, thus yielding sets of terms that do not contain s.

Note that $s \notin \mathrm{Sub}(t)$ implies that this derivation is also of goal t. Let us prove that we can construct a derivation also of goal t that does not contain s in the left-hand side of any rule.

Consider the rule $l \to r \in \mathrm{L}^{u,\mathrm{g}}$ applied from s to $(E_j\delta_s)\downarrow, s$ with a substitution τ (that is $l = \mathrm{Var}(u)\tau$ and $r = (u\tau)\downarrow$). We assume wlog that this rule is not a stutter. Assume $s \in l$. If for all variables x instantiated by s we have $\textsc{sig}(x) \neq \textsc{sig}(s)$, we can replace s by $\mathrm{c}_{\min}$ in $u\tau$, and therefore in l and r by Lemma 8. Since $s \notin \mathrm{Sub}(r)$ we have a transition from $(E_{j-1}\delta_s)\downarrow, s$ to $(E_j\delta_s)\downarrow, s$ with the rule $l, \mathrm{c}_{\min} \setminus s \to r$ in $\mathrm{L}^{u,\mathrm{g}}$ in which s does not appear on the left-hand side.

If there exists a variable $x \in \mathrm{Var}(u)$ such that $\textsc{sig}(x) = \textsc{sig}(s)$ and $x\tau = s$, then $\textsc{sig}(s) = 1$ implies that $\textsc{sig}(x) = 1$ and, since u is well-moded, $\textsc{sig}(u) = 1$, and therefore $u \in \mathcal{S}_1$. Since $j - 1 \geq i_s$ this implies we have the sequence:

$$(E_{j-1}\delta_s)\downarrow \to_{\mathcal{S}_1} (E_{j-1}\delta_s)\downarrow, s \to_{\mathcal{S}_1} (E_{j-1}\delta_s)\downarrow, s, t$$

with $s \notin \mathrm{Sub}((E_{j-1}\delta_s)\downarrow, t)$. Thus we can apply Hypothesis 1, which yields a derivation:

$$(E_{j-1}\delta_s)\downarrow \to^*_{\mathcal{S}_0} F \to_{\mathcal{S}_1} F, t$$

Lemma 12 implies that all terms of signature 1 in $\mathrm{Sub}(F)$ are also in $\mathrm{Sub}((E_{j-1}\delta_s)\downarrow)$.

By iterating along the transitions in the derivation D' we obtain a new derivation D'' in which s is on the left-hand side of no transition and that does not contain more subterms of signature 1. By removing the transition creating s in D'' we thus obtain a derivation starting from E of goal t that contradicts the minimality of D. Thus there exists quasi well-formed derivations starting from E of goal t.

□

First let us prove an auxiliary lemma that will be used to prove Proposition 2.

Lemma 16 *Let $D : E_0 \to^* E_n$ be a derivation without stutter, and let $t_i = E_i \setminus E_{i-1}$. Assume that, for index j we have $E_{j-1} \to_{\mathrm{L}^{u_j,\mathrm{g}}} E_j$, and $\mathrm{SIG}(u_j) = 1$, and $\mathrm{SIG}(t_j) = 0$, and $t_j \notin \mathrm{C}_{\mathrm{spe}}$. Then $t_j \in \mathrm{Sub}(E_0)$.*

Proof. Let i be the minimal index such that $t_j \in \mathrm{Sub}(E_i)$. We have $i \leq j$. By contradiction assume $i > 0$. Then by Lemma 13 and $t \in \mathrm{Sub}(E_i) \setminus \mathrm{Sub}(E_{i-1})$ we have $E_{i-1} \to_{\mathrm{L}^{u_i,\mathrm{g}}} E_i$ with $E_i = E_{i-1}, t$ and $\mathrm{SIG}(u) = \mathrm{SIG}(t) = 0$. The latter implies $i \neq j$, and therefore that the derivation contains a stutter. □

Lemma 16 permits to bound the number of applications of a rule in $\mathcal{S}_1$ in a quasi well-formed derivation.

Proposition 2 *If $t \in \overline{E}$ there exists a derivation D starting from E of goal t such that the number of rules in $\mathcal{S}_1$ applied in D is bounded by $|\mathrm{Sub}(E, t)|$.*

Proof. Since $t \in \overline{E}$ we can consider by Lemma 15 there exists a quasi well-formed derivation D starting from E of goal t. W.l.o.g. we assume that D is without stutter. Let $t_1, \ldots, t_n$ be the terms deduced by a rule in $\mathcal{S}_1$ in D. Since the derivation is without stutter n is the number of applications of rules in $\mathcal{S}_1$ in D. Let n_0 be the number of t_i of signature 0, and n_1 be the number of t_i of signature 1. Since D is quasi well-formed and by Lemma 16 we have:

$$\begin{cases} n_0 \leq |\{t \in \mathrm{Sub}(E) \,|\, \mathrm{SIG}(t) = 0\}| \\ n_1 \leq |\{t \in \mathrm{Sub}(E, t) \,|\, \mathrm{SIG}(t) = 1\}| \end{cases}$$

□

Actually, not only we can bound the number of applications of rules in $\mathcal{S}_1$ (Proposition 2), know that the result is a subterm of E, t for a quasi well-formed derivation starting from E of goal t, but under the same conditions we can also bound the possible values for subterms of variables of signature 1 in a rule of $\mathcal{S}_1$.

Proposition 3 *Let $D : E_0 \to_{\mathrm{L}^{u_1,\mathrm{g}}} \ldots \to_{\mathrm{L}^{u_n,\mathrm{g}}} E_n$ be a quasi well-formed derivation without stutter, let i be an index such that $\mathrm{SIG}(u_i) = 1$ and let $x \in \mathrm{Var}(u_i)$ be a variable with $\mathrm{SIG}(x) = 1$. Then we can choose the substitution τ_i with which the rule is applied such that $x\tau_i \in \mathrm{Sub}(E_0, t)$.*

Proof. Assume the substitution with which the i-th rule is applied is τ. Let $t_i = (u\tau)\!\downarrow$ and $s = x\tau$.
If $\mathrm{SIG}(s) = 0$ then $\mathrm{SIG}(s) \neq \mathrm{SIG}(x)$, u is well-moded and therefore $s \in \mathrm{Factors}(u\tau)$. Assume first that $s \in \mathrm{Sub}(t_i)$. Then by Lemma 16 and D quasi

well-formed we have $s \in \mathrm{Sub}(E_0, t)$. Assume now that $s \notin \mathrm{Sub}(t_i)$. Hence $s \neq t_i$, and by Lemma 9:

$$(u((\tau\delta_s)\downarrow))\downarrow = ((u\tau)\delta_s)\downarrow = (((u\tau))\downarrow\delta_s)\downarrow$$

Choosing $\tau_i = (\tau\delta_s)\downarrow$, we also have $t_i = (u_i\tau_i)\downarrow$, and in that case $x\tau_i \in \mathrm{Sub}(E_0)$.

If $\mathrm{SIG}(x\tau) = 1$, we have $x\tau \in \mathrm{Sub}(E_0, t)$ since the derivation D is quasi well-formed. □

7.1 Stability of derivations by replacement

Lemma 17 will be applied in Lemma 19 with s a free term. It shows that given some conditions on s, derivations are stable when replacing s by $\mathrm{c_{min}}$.

Lemma 17 *Let E and F be finite sets of normalised terms with $\mathrm{c_{min}} \in E$. Let s, t be two normalised terms not in $\mathrm{C_{spe}}$ with $s \in \overline{E} \setminus \mathrm{Sub}(E)$, and $t \in \overline{E \cup F}$. We have:*

$$(t\delta_s)\downarrow \in \overline{((E \cup F)\delta_s)\downarrow}$$

Proof. We note that $s \in \overline{E}\setminus\mathrm{Sub}(E)$ implies $(E\delta_s)\downarrow = E$ and thus $s \in \overline{(E\delta_s)\downarrow}$. By considering a derivation starting from $E\cup F$ of goal t and building s, we see that $t \in \overline{E, F}$ implies, by iteration of Lemma 14, that $(t\delta_s)\downarrow \in \overline{((E, F)\delta_s)\downarrow, s}$. Since $(E\delta_s)\downarrow = E$ and $s \in \overline{E}$, this implies $s \in \overline{((E, F)\delta_s)\downarrow}$ and thus $(t\delta_s)\downarrow \in \overline{((E, F)\delta_s)\downarrow}$ □

7.2 Existence and properties of bound solutions

In the rest of this section we consider a constraint system $\mathcal{C} = ((E_i \rhd v_i)_{1\leq i\leq n}, \mathcal{S})$ and a normal ground substitution σ that satisfies $\mathcal{C}$. We now prove that there exists a *bound* substitution that also satisfies $\mathcal{C}$. First we prove it is possible to replace one free term s of signature in $\mathrm{Sub}(\sigma)$ by the minimal constant $\mathrm{c_{min}}$.

Lemma 18 *Let $s \notin \mathrm{C_{spe}}$ be a term such that $s \in \mathrm{Sub}((E_k\sigma)\downarrow)$ for some $1 \leq k \leq n$. Then either there exists $i < k$ such that $s \in \mathrm{Sub}(v_i\sigma)$ or there exists $m \in \mathrm{Sub}(E_k)$ such that $(m\sigma)\downarrow = s$ and in that case either $\mathrm{SIG}(s) = \mathrm{SIG}(m)$ or m is a constant.*

Proof. Since the constraint system is deterministic we have

$$\mathrm{Sub}((E_k\sigma)\downarrow) \subseteq (\mathrm{Sub}(E_k)\sigma)\downarrow \cup \mathrm{Sub}(v_1\sigma, \ldots, v_{k-1}\sigma) \cup \mathrm{C_{spe}}$$

Assume that there is no $i < k$ such that $s \in \mathrm{Sub}(v_i\sigma)$. Then $s \notin \mathrm{C_{spe}}$ implies there exists $m \in \mathrm{Sub}(E_k)$ such that $(m\sigma)\downarrow = s$. By $s \notin \mathrm{C_{spe}}$ and Lemma 7 there exists $u \in \mathrm{Sub}(m)$ such that $(u\sigma)\downarrow = s$ and $\mathrm{SIG}(u) = \mathrm{SIG}(s)$. □

Lemma 19 *If there exists $x \in \mathrm{Var}(\mathcal{C})$ and $s \in \mathrm{Sub}(x\sigma)$ such that s is free in $\mathrm{Sub}(\mathcal{C})$ for σ then $(\sigma\delta_s)\downarrow \models \mathcal{C}$*

Proof. Let $\sigma' = (\sigma\delta_s)\downarrow$. Note that s free implies $s \notin \mathrm{C_{spe}}$.

First let us prove that $\sigma' \models \mathcal{S}$. Since s is free in $\mathrm{Sub}(\mathcal{C})$ Lemma 9 implies that for all equations $s \stackrel{?}{=} t$ in $\mathcal{S}$ we have $(s\sigma)\downarrow = (t\sigma)\downarrow$ implies $(s\sigma')\downarrow = (t\sigma')\downarrow$.

Let us now prove that for all $i \in \{1, \ldots, n\}$ if there is a derivation starting from $(E_i\sigma)\downarrow$ of goal $v_i\sigma$ then there is a derivation starting from $(E_i\sigma')\downarrow$ of goal $v_i\sigma'$. Let $j \in \{1, \ldots, n\}$ and consider the set:

$$\Omega_s = \{i \mid s \in \mathrm{Sub}((E_i\sigma)\downarrow, v_i\sigma)\}$$

If $j \notin \Omega_s$ we have $(E_j\sigma)\downarrow\delta_s = (E_j\sigma)\downarrow$ and $v_j\sigma = v_j\sigma\delta_s$. Since s is free Lemma 9 implies $(E_j\sigma')\downarrow = (E_j\sigma)\downarrow$ and $v_j\sigma' = v_j\sigma$. Thus by assumption there exists a derivation starting from $(E_j\sigma')\downarrow$ of goal $v_j\sigma'$.

Thus if $\Omega = \emptyset$ the Lemma is valid. Otherwise $\Omega \neq \emptyset$ and we can consider the minimum index i_0 in Ω. By minimality of i_0 and by Lemma 18 we have $s \notin \mathrm{Sub}((E_{i_0}\sigma)\downarrow)$ and thus $s \in \mathrm{Sub}(v_{i_0}\sigma)$. By Lemma 12 this implies $s \in \overline{(E_{i_0}\sigma)\downarrow}$.

For $j \in \Omega$ let $F_j = (E_j\sigma)\downarrow \setminus (E_{i_0}\sigma)\downarrow$. By $(E_j\sigma)\downarrow = (E_{i_0}\sigma)\downarrow \cup F_j$ and $s \in \overline{(E_{i_0}\sigma)\downarrow} \setminus \mathrm{Sub}((E_{i_0}\sigma)\downarrow)$ we can apply Lemma 17 to obtain a derivation D'_j starting from $((E_j\sigma)\downarrow\delta_s)\downarrow$ of goal $v_j\sigma'$. Since s is free Lemma 9 implies D'_j is a derivation starting from $(E_j\sigma')\downarrow$ of goal $v_j\sigma'$.

Thus for all $j \in \{1, \ldots, n\}$ there is a derivation starting from $(E_i\sigma')\downarrow$ of goal $v_i\sigma'$. □

The proof of next Proposition 4 is a direct consequence of Lemma 19 and exploits the well-foundedness of the order $<$ to prove it is possible to iteratively replace all free subterms.

We can now prove that a satisfiable constraint system is satisfied by a bound solution.

Proposition 4 *Let $\mathcal{C}$ be a satisfiable constraint system. There exists a normal bound substitution σ such that $\sigma \models \mathcal{C}$.*

Proof. Consider the set Σ of normal substitutions that satisfy $\mathcal{C}$. By hypothesis Σ is not empty. Let σ be a minimal substitution in Σ for the total ordering

$<$ on ground terms extended to substitutions by considering their co-domains as finite multisets of ground terms. Let us prove σ is bound to $\mathcal{C}$.

By contradiction assume there exists s free in $\mathrm{Sub}(\sigma)$ and let $\sigma' = \sigma\delta_s$. By monotony of $<$ we have $\sigma' < \sigma$. By definition of R we have $(\sigma')\downarrow \leq \sigma'$. By Lemma 19 we also have $(\sigma')\downarrow \models \mathcal{C}$. Thus $(\sigma')\downarrow \in \Sigma$ and $(\sigma')\downarrow < \sigma$ which contradicts the minimality of σ. □

In next lemma we prove that instantiating the constraint $\mathcal{C}$ by a bound substitution does not introduce any new subterm.

Lemma 20 *Let σ be a substitution bound by itself in $\mathrm{Sub}(\mathcal{C})$. We have:*

$$\mathrm{Sub}((\mathrm{Sub}(\mathcal{C})\sigma)\downarrow) = (\mathrm{Sub}(\mathcal{C})\sigma)\downarrow$$

Proof. Let $S = (\mathrm{Sub}(\mathcal{C})\sigma)\downarrow$. The inclusion $S \subseteq \mathrm{Sub}(S)$ is trivial. The inclusion $\mathrm{Sub}(S) \subseteq S$ follows directly from:

$$\mathrm{Sub}((\mathrm{Sub}(\mathcal{C})\sigma)\downarrow) \subseteq (\mathrm{Sub}(\mathcal{C})\sigma)\downarrow \cup \mathrm{Sub}(\mathrm{Var}(\mathcal{C})\sigma) \cup \mathrm{C}_{\mathrm{spe}}$$

Since σ is bound we have $\mathrm{Sub}(\mathrm{Var}(\mathcal{C})\sigma) \subseteq (\mathrm{Sub}(\mathcal{C})\sigma)\downarrow$ and by hypothesis we have $\mathrm{C}_{\mathrm{spe}} \subseteq \mathrm{Sub}(\mathcal{C})$. □

8 Sufficient conditions for decidability

We now give sufficient conditions for the decidability of the various decision problems. Given a well-moded intruder $\mathcal{I}$ we first treat the case of the $\mathcal{I}$ deduction problem in Section 8.1. Then we give sufficient conditions for the decidability of the $\mathcal{I}$ ordered satisfiability of deterministic constraint systems.

8.1 Deduction Problem

First we turn to *deduction problems*. Let $((E_i \rhd v_i)_{i\in\{1,\ldots,n\}}, \mathcal{S})$ be a ground constraint system for a well-moded intruder $\mathcal{I} = \langle \mathcal{F}, \mathcal{S}, \mathcal{E}\rangle$. Let also $\mathcal{S}_1 = \{t \in \mathcal{S} \mid \mathrm{SIG}(t) = 1\}$. Theorem 1 gives a sufficient condition for the decidability of the $\mathcal{I}$ deduction problem.

Theorem 1 *If:*

(1) $\mathcal{S}_1$ is finite,
(2) $\langle \mathcal{F}_0, \mathcal{S}_0, \mathcal{E}_0\rangle$ has a decidable deduction problem;
(3) Word problems are decidable for $\mathcal{E}$;

(4) Hypotheses 1 and 2 are satisfied.

Then the $\mathcal{I}$ deduction problem is decidable.

Notice that since ground constraint systems are also deterministic, other sufficient conditions will be given in Section 8.2. Our motivation for the introduction of deduction problems was that, contrary to the case of the union of disjoint signatures, this amounts to the reduction of ground problems to deterministic problems, which are likely to be more difficult to solve.

Given the third condition, it is clear that it suffices to prove that ground reachability problems are decidable. Given a set of terms E and a term t, both ground, our algorithm decides non-deterministically $t \in \overline{E}$. It consists in:

(1) guessing the number n — bounded by $|\mathrm{Sub}(E,t)|$ by Proposition 2 — of rules in $\mathcal{S}_1$ applied in a quasi well-formed derivation — it is sufficient to consider this case by Hypothesis 1 and Lemma 15 — starting from E and of goal t,
(2) then guessing for each of these rules:
   – the term $u \in \mathcal{S}_1$ actually employed, which is possible since $\mathcal{S}_1$ is finite,
   – the result r of the rule (in $\mathrm{Sub}(E,t)$ by Lemma 16 and the definition of quasi well-formed derivations),
   – for each variable x of u with $\mathrm{SIG}(x) = 1$, the instance of x in $\mathrm{Sub}(E,t)$ by Proposition 3

   Let u' be the term u with all its variables of signature 1 instantiated by ground terms.
(3) For each rule u, let σ be result of the matching of t by u' (abort if there is no solution). Notice that σ is ground and computable by Hypothesis 2,
(4) From the above computations, if t_i is the i-th term built by a $\mathcal{S}_1$ rule and σ_i is the associated ground substitution, form the ground reachability problems:

$$\bigwedge_{x \in \mathrm{Var}(u) \mathrm{SIG}(x)=0} E \cup \{t_1, \ldots, t_{i-1}\} \rhd_{\mathcal{S}_0} x\sigma_i$$

(5) Purify (which is possible because word equations are decidable) and solve with respect to intruder $\mathcal{I}_0$ the obtained reachability problems.

As a side remark, we believe that this algorithm can be transformed into a polynomial one if the ground reachability problems and if the matching problems can be solved in polynomial time. The procedure would compute a subset S (with $t \in S$) of terms reachable from E by checking one-step deduction between a set of terms and a term. One-step deduction test would be performed either by (pre-computed) rules of the form $\sigma_i \to t_i$ (with $t_i \in \mathrm{Sub}(E,t)$) or tests of $E' \rhd_{\mathcal{S}_0} s$ for s subterm of the σ_i.

We now state the main theorem of this article, which concerns the reduction of $\mathcal{I}$ ordered satisfiability problems to $\mathcal{I}_0$ ordered satisfiability problems.

Theorem 2 *We consider a well-moded intruder system $\langle \mathcal{F}, \mathcal{S}, \mathcal{E} \rangle$ such that $\mathcal{S}_1$ is finite, the intruder subsystem $\langle \mathcal{F}_0, \mathcal{S}_0, \mathcal{E}_0 \rangle$ has a decidable ordered constraint satisfiability problem and Hypotheses 1 and 3 are satisfied. Then the ordered constraint satisfiability problem for $\langle \mathcal{F}, \mathcal{S}, \mathcal{E} \rangle$ is decidable.*

Before giving a decision procedure for $\mathcal{I}$ intruder systems under the conditions of Theorem 2, we introduce the notions of past-bound terms and of complete prefix which permit to reduce to deterministic constraint systems.

8.2.1 Past-bound terms and complete prefixes

Let $\mathcal{C} = ((E_i \rhd v_i)_{1 \leq i \leq n}, \mathcal{S})$ be a constraint system and σ be a solution of $\mathcal{C}$. Given $t \in \mathrm{Sub}(\mathcal{C})$ let us define $I_t = \{j \mid (t\sigma)\!\downarrow \in \mathrm{Sub}((\mathrm{Sub}(E_j)\sigma)\!\downarrow, v_j\sigma)\}$. If $I_t \neq \emptyset$ we say that the term t is *deduction-bound*. In this case we define the *index* of t, and denote i_t, the minimum index in I_t. If $t \in \mathrm{Sub}(\mathcal{C})$ is deduction bound, we say it is *past-bound* if $t \in \mathrm{Sub}((\mathrm{Sub}(E_{j_t})\sigma)\!\downarrow)$ and *past-free* otherwise. Finally, given a past-bound term t of index i_t, we say that a term m is a *complete prefix* of t if:

(1) $\mathrm{SIG}(m) = \mathrm{SIG}((t\sigma)\!\downarrow)$ and $(m\sigma)\!\downarrow = (t\sigma)\!\downarrow$;
(2) For all factor u of m; either $(u\sigma)\!\downarrow$ is past-free or $\mathrm{SIG}(u) = \mathrm{SIG}((u\sigma)\!\downarrow)$
(3) $\mathrm{Var}(m) \subseteq \{v_1, \ldots, v_{i_t}\}$

Algorithm 1 Algorithm to compute complete prefixes

for all past-free and constant terms t **do**
  $\varphi_{\mathrm{p}}(t) = t$
end for
while there exists deduction bound $t \in \mathrm{Sub}(\mathcal{C})$ with $\varphi_{\mathrm{p}}(t)$ undefined **do**
  Let $t \in \mathrm{Sub}(\mathcal{C})$ with $\varphi_{\mathrm{p}}(t)$ undefined
  if $\varphi_{\mathrm{p}}(\cdot)$is defined on all factors of m **then**
    For all t' such that $(t\sigma)\!\downarrow = (t'\sigma)\!\downarrow$, define $\varphi_{\mathrm{p}}(t')$ as the term t where all factors u have been replaced by $\varphi_{\mathrm{p}}(u)$
  end if
end while

Lemma 21 *It is possible to compute a complete prefix of $(t\sigma)\!\downarrow$ for all past-bound terms t in* $\mathrm{Sub}(\mathcal{C})$.

Proof. Let $T_i \subseteq \mathrm{Sub}(\mathcal{C})$ be the set of past-bound terms t of index i for which Algorithm 1 does not compute a complete prefix. By contradiction assume

$\cup_{i=1}^{n} T_i \neq \emptyset$. Let i be minimal such that $T_i \neq \emptyset$, and let t be minimal in T_i for the subterm relation. By definition of the algorithm we assume t is not a constant, and thus $t \notin \mathrm{C}_{\mathrm{spe}}$. Since t is of index i we have $t \notin \mathrm{Sub}(\{v_1\sigma, \ldots, v_{i-1}\sigma\})$. Thus, by Lemma 7 there exists $m \in \mathrm{Sub}(t)$ such that m is a prefix of $(t\sigma)\!\downarrow$. By definition of T_i, we have $t \in T_i$ and $(m\sigma)\!\downarrow = (t\sigma)\!\downarrow$ imply that $m \in T_i$. Thus, by minimality of t for the subterm relation in T_i, we have $t = m$ and thus t is a prefix of $(t\sigma)\!\downarrow$. Since t is neither a variable nor a constant, the factors of t are defined. By minimality of t in T_i, for every past-bound factor u of t, $\varphi_{\mathrm{p}}(u)$ is defined and is a complete prefix of $(u\sigma)\!\downarrow$. One easily checks that $\varphi_{\mathrm{p}}(t)$ is then a complete prefix of t, thus contradicting $t \in T_i$, and therefore $\cup_{i=1}^{n} T_i = \emptyset$. □

Notice that Algorithm 1 only relies on the knowledge of the equivalence classes on terms in $\mathrm{Sub}(\mathcal{C})$ induced by the solution σ and on the signature of terms. Both can be guessed in linear time with respect to the size of the input constraint problem.

Lemma 22 *Assume $t \in \overline{E}$, and there exists a derivation from E to t such that all rules but the last one are $\mathcal{S}_0$ rules. Let $u \in \mathcal{S}_1$ be the term employed for the last deduction, and τ be the substitution applied. Then* $\mathrm{Var}(u)\tau \subseteq \overline{E}^{\mathcal{S}_0}$.

Proof. This follows directly from the hypotheses. □

Lemma 23 *Let σ be a solution of a constraint system $\mathcal{C} = ((E_i \rhd v_i)_{1 \leq i \leq n}, \mathcal{S})$, and t be a deduction-bound term such that* $\mathrm{SIG}(t) = 0$ *and t is of index i. Then if there exists a quasi well-formed derivation without stutter from $(E_i\sigma)\!\downarrow$ of goal $(v_\sigma)\!\downarrow$ containing a deduction $E \rightarrow_{\mathcal{S}_1} E, t$ then t is past-bound.*

Proof. Lemma 12 and the fact that the derivation is without stutter imply that $t \in \mathrm{Sub}((E_i\sigma)\!\downarrow)$ and thus $t \in \mathrm{Sub}((\mathrm{Sub}(E_i)\sigma)\!\downarrow)$. We conclude that t is past-bound from the fact that t is of index i. □

8.2.2 Algorithm

We present here a decision procedure for a well-moded intruder $\mathcal{I}$ that takes as input a constraint system $\mathcal{C} = ((E_i \rhd v_i)_{1 \leq i \leq n}, \mathcal{S})$ and a linear ordering $<_i$ on variables and constants of $\mathcal{C}$. Let $m = |\mathrm{Sub}(\mathcal{C})|$ be the number of subterms in $\mathcal{C}$.

Algorithm 2 Combination algorithm

Step 1: Choose a $m' \leq m$ and a sequence $(u_i)_{1\leq i\leq m'}$ of terms in $\mathcal{S}_1$, and for each u_i introduce $|\mathrm{Var}(u_i)|$ new variables $y^i_1, \ldots, y^i_{|\mathrm{Var}(u_i)|}$. Let χ_i ($i \in \{0,1\}$) be the subset of these variables of signature i.

Step 2: Choose an equivalence relation $\equiv_\sigma$ among subterms of $\mathcal{C} \cup \chi_1$. Let $Q = \{q_1, \ldots, q_n\}$ be a set of new variables each denoting an equivalence class. Add to $\mathcal{S}$ the equation $t \stackrel{?}{=} q$ for each $t \in q$ for each equivalence class $q \in Q$. Let $\mathcal{S}'$ be the obtained constraint system.

Step 3: Choose a subterm relation on $Q \cup \chi_0$ and a function $\mathrm{sig} : x \in Q \cup \chi_0 \mapsto \mathrm{SIG}(q)$.

Step 4: Guess a subset Q_1 of Q, and let $L = \{l_1, \ldots, l_k\}$ be the set $Q_1 \cup \{v_1, \ldots, v_n\}$ totally ordered by $<_d$ such that $i < j$ implies $v_i <_q v_j$ and form the constraint system $\mathcal{C}' = ((F_i \rhd l_i)_{1\leq i\leq k}, \mathcal{S}'')$ with

$$\begin{cases} F_1 = E_1 & \\ F_{i+1} = F_i \cup (E_{j+1} \setminus E_j) & \text{If } l_i = v_j \\ F_{i+1} = F_i, l_i & \text{Otherwise} \end{cases}$$

Step 5: Replace each past-bound term in $\mathcal{C}$' with a complete prefix and past-free terms with the representative q of their equivalence class, and let $\mathcal{C}''$ be the obtained constraint system.

Step 6: Guess a subset of m' constraints $F_i \rhd l_i$ in $\mathcal{C}''$. Replace the j-th of these constraints by $|\mathrm{Var}(u_j)|$ constraints $F_{\alpha_j} \rhd y^j_k$ for $k \in \{1, \ldots, |\mathrm{Var}(u_j)|\}$ and add an equation $l_{\alpha_j} \stackrel{?}{=} u_j$ to $\mathcal{S}''$;

Step 7: Reduce $\mathcal{S}''$ to a system of general unification modulo $\mathcal{E}_0$.

Step 8: Solve the resulting $\mathcal{I}_0$ deterministic intruder system with the linear constant restriction $<_i$.

8.2.3 Comments on the algorithm.

We assume in the following that the ordered satisfiability problem $(\mathcal{C}, <_i)$, with $\mathcal{C} = ((E_i \rhd v_i)_{1\leq i\leq n}, \mathcal{S})$, is satisfied by a bound substitution σ. Let $m = |\mathrm{Sub}(\mathcal{C})|$ be the number of subterms in $\mathcal{C}$.

Step 1: By Proposition 2 For each of the derivation starting from $(E_i\sigma)\downarrow$ of goal $(v_i\sigma)\downarrow$ there is at most m applications of a rule in $\mathcal{S}_1$. Actually, as we will merge the derivations of the intruder, there will be overall at most m' applications of a rule in $\mathcal{S}_1$. Since $\mathcal{S}_1$ is finite, the term u_i employed in the i-th of these rules can be guessed.

Step 2: The equivalence relation can be guessed since σ is bounded. Proposition 3 permits to extend this equivalence relation over χ_1.

Step 3: The choice of a subterm relation and of signature is needed to know whether a deduction-bound term is past-free or past-bound and to compute a complete prefix of it.

Step 4: Q_1 is the set of terms that are deduced by a rule of $\mathcal{S}_1$ that does not end a derivation starting from $(E_i\sigma)\downarrow$ of goal $(v_i\sigma)\downarrow$. The construction of $\mathcal{C}'$ consists in merging the derivation once the set Q_1 has been guessed. The ordering $<_d$ is the order of deduction. Notice that this construction leads to stutters since a variable v_i is also in an equivalence class. This is however more convenient for describing succinctly the construction.

Step 5: The choices made permit to compute a complete prefix of each past-bound term. Replacing a term by its complete prefix is preserves the satisfaction by σ. The obtained system $\mathcal{C}''$ will be deterministic once purified by Lemma 23.

Step 6: The replacement corresponds to the checking that the guessed rule u_j permits to construct l_j. The instance of the variables of u_j can be deduced using only rules in $\mathcal{S}_0$ by Lemma 22.

Step 7: The reduction can be done thanks to Hypothesis 3.

Step 8: The resolution is decidable by hypothesis on $\mathcal{I}_0$.

From these comments, one easily sees that the algorithm is complete. It can also easily be checked that it is correct.

8.3 Exponentiation

We present now an application of well-moded theories in the case of the exponentiation operator which is used *e.g.* with Diffie-Hellman scheme for the collaborative construction of a secret key by two principals.

In order to support properties of the exponential operator in cryptographic protocols analysis our goal is to prove the decidability of ordered satisfiability for an intruder able to exploit the properties of exponentiations. Notice that the specification of the exponentiation operation is dependent on the specification of the multiplication, and thus Theorem 1 of [10] cannot be applied directly.

Notice also that simple extensions of the theory we consider here would lead to undecidability of intruder constraints even when they are reduced to equational unification problems. See [28] for a survey of several exponentiation theories and their unification problems. The axiomatisation we consider here was to our knowledge first introduced in [30].

8.3.1 Intruder deduction system.

We consider the union $\mathcal{F}$ of the two signatures $\mathcal{F}_0 = \{\_ \times \_, \mathrm{i}(\_), 1\}$ and $\mathcal{F}_1 = \{\exp(\_,\_)\}$. We consider terms in $\mathrm{T}(\mathcal{F}, \mathcal{X})$ modulo the following equational

theory $\mathcal{E}^{exp,\times}$:

$$x \times (y \times z) = (x \times y) \times z \qquad (A)$$
$$x \times y = y \times x \qquad (C)$$
$$x \times 1 = x \qquad (U)$$
$$x \times \mathrm{i}(x) = 1 \qquad (I)$$
$$\exp(x, 1) = x \qquad (E_0)$$
$$\exp(\exp(x, y), z) = \exp(x, y \times z) \qquad (E_1)$$

Let $T = \{x \times y, \mathrm{i}(x), 1, \exp(x, y)\}$. We now consider the intruder system $\mathcal{I}_{\exp} = \langle \mathcal{F}, T, \mathcal{E}^{exp,\times} \rangle$ that represents the modular exponentiation operation as employed for Diffie-Hellman-like construction of secret keys.

8.3.1.1 Modes. One easily checks that for the following mode and signature functions the theory $\mathcal{E}^{exp,\times}$ is a well-moded theory:

- $\mathrm{M}(\times, 1) = \mathrm{M}(\times, 2) = \mathrm{M}(\mathrm{i}, 1) = 0$;
- $\mathrm{M}(\exp, 1) = 1$ and $\mathrm{M}(\exp, 2) = 0$;
- $\mathrm{SIG}(\times) = \mathrm{SIG}(\mathrm{i}) = \mathrm{SIG}(1) = 0$
- $\mathrm{SIG}(\exp) = 1$

According to this definition of mode and signature we define $\mathcal{E}^{exp,\times}$ to be the union of $\mathcal{E}_0 = \{(A), (C), (U), (I)\}$ and $\mathcal{E}_1 = \{(E_0), (E_1)\}$. The set $\mathcal{E}_0$ generates the theory of a free Abelian group whose generators are the atomic symbols in C. Meadows and Narendran have proved [30] that general unification modulo $\mathcal{E}^{exp,\times}$ can be reduced to general unification modulo $\mathcal{E}_0$.

$\mathcal{E}^{exp,\times}$ is reducible to $\mathcal{E}_0$, and thus Hypothesis 3 is satisfied.

8.3.1.2 Intruder $\mathcal{I}_{\mathrm{ag}}$. According to mode and signature functions, we can define a sub-intruder system by taking $\mathcal{S}_0 = \{x \times y, \mathrm{i}(x), 1\}$. Let $\mathcal{I}_{\mathrm{ag}}$ be the intruder $\langle \{\times, \mathrm{i}, 1\}, \{x \times y, \mathrm{i}(x), 1\}, \mathcal{E}_0 \rangle$. Taking $\mathcal{S}_1 = \mathcal{S} \setminus \mathcal{S}_0$, it is also clear that $\mathcal{S}_1$ is finite.

- $\mathcal{S}_1$ is finite;
- The $\mathcal{I}_{\mathrm{ag}}$ ordered constraint satisfiability problem is decidable in [11].

Lemma 24 *Let E be a finite set of terms in normal form, and let r, t be two*

terms in normal form such that:

$$E \rightarrow_{\mathcal{S}_1} E, r \rightarrow_{\mathcal{S}_1} E, r, t$$

If $r \notin \mathrm{Sub}(E, t)$ *and* $E \not\rightarrow E, t$ *then there exists a term* u *such that:*

$$E \rightarrow_{\mathcal{S}_0} E, u \rightarrow_{\mathcal{S}_1} E, u, t$$

Proof. Assume $r \notin \mathrm{Sub}(t)$ and $E \not\rightarrow E, t$. Since $r \notin \mathrm{Sub}(E)$ it is necessary an exponential by Lemma 12. Let σ be the substitution with which the first rule $x_1, y_1 \rightarrow \exp(x_1, y_1)$ is applied, and τ be the substitution with which the second rule $x_2, y_2 \rightarrow \exp(x_2, y_2)$ is applied. Since $E \not\rightarrow E, t$ one must have $r = x_2\tau$ or $r = y_2\tau$, and $r \notin \mathrm{Sub}(E)$ implies that $r \notin \mathrm{Sub}(x_1\sigma, y_1\sigma)$. Let us first assume that $x_2\tau = r$. In this case we have a derivation:

$$\begin{aligned} D_1 : x_1\sigma, y_1\sigma, y_2\tau &\rightarrow_{\mathcal{S}_0} x_1\sigma, y_1\sigma, y_2\tau, y_1\sigma \times y_2\tau \\ &\rightarrow_{\mathcal{S}_1} x_1\sigma, y_1\sigma, y_2\tau, y_1\sigma \times y_2\tau, (\exp(x_1\sigma, y_1\sigma \times y_2\tau))\downarrow = t \end{aligned}$$

Thus, if $y_2\tau \neq r$, we have $y_2\tau \in E$ and therefore a derivation as requested. If $y_2\tau = r$, by Lemma 11 and applying δ_r we also have a deduction:

$$\begin{aligned} x_1\sigma, y_1\sigma, \mathrm{c}_{\min}, y_1\sigma \times \mathrm{c}_{\min} &\rightarrow_{\mathcal{S}_1} \\ &x_1\sigma, y_1\sigma, \mathrm{c}_{\min}, y_1\sigma \times \mathrm{c}_{\min}, (\exp(x_1\sigma, y_1\sigma \times \mathrm{c}_{\min}))\downarrow = (t\delta_r)\downarrow \end{aligned}$$

Since $r \notin \mathrm{Sub}(t)$, this implies that if $x_2\tau = r$, there exists a sequence $E \rightarrow_{\mathcal{S}_0} E, r' \rightarrow_{\mathcal{S}_1} E, r', t$. On the other hand, if $x_2\tau \neq r$, then $x_2\tau \in E$, and we can directly apply Lemma 11 to find a deduction with only one rule in $\mathcal{S}_1$ such that $y_2\tau \neq r$. □

$\mathcal{I}_{\exp}$ satisfies Hypothesis 1.

It is finally shown in [30,13] that one can define a normal form for the equational theory $\mathcal{E}^{exp,\times}$ such that the first argument of an exponential operator is never itself an exponential operator. Given two ground terms t_1 and t_2 in normal form, and a variable x, it is then easy to prove (by case analysis on the top operators of t_1 and t_2 that the equation $\exp(t_1, x) \stackrel{?}{=} t_2$ has at most one ground solution σ.

$\mathcal{I}_{\exp}$ satisfies Hypothesis 2.

Gathering all the results given above, and applying Theorems 1 and 2, we have the following theorem.

Theorem 3 *The* $\mathcal{I}_{\exp}$ *deduction problem and the* $\mathcal{I}_{\exp}$ *ordered satisfiability problem are decidable.*

Notice that the former is a consequence of the latter. Actually, the reduction result for the deduction problem is mostly useful in the case where the ordered satisfiability problem for the underlying $\mathcal{I}_0$ intruder system is not decidable, or its decidability is not known, but its deduction problem is. It can be applied *e.g.* when reducing an intruder system to an AC intruder system $(\langle\{\times\}, \{x \times y\}, \{(A), (C)\}\rangle)$, for which the deduction problem is decidable, but the status of its ordered satisfiability problem is open.

8.3.1.3 Complexity. First let us examine the case of the deduction problem. Since satisfiability of linear equations over $\mathbb{Z}$ can be evaluated in polynomial time, the deduction problem for $\mathcal{I}_{\text{ag}}$ is in PTIME. The algorithm depicted above for solving the generated matching problems is also in PTIME. Thus we conjecture that the deduction problem for the $\mathcal{I}_{\text{exp}}$ intruder is in PTIME. Second, and given that unification modulo $\mathcal{E}^{exp,\times}$ is NP-complete [30], that the ordered satisfiability problem for the $\mathcal{I}_{\text{ag}}$ intruder is in NPTIME, that our reduction algorithm works in NPTIME, we also conjecture that ordered satisfiability problems for the $\mathcal{I}_{\text{exp}}$ intruder system is NP-complete.

9 Conclusion

We have introduced a combination scheme for intruder theories that extends disjoint combination. We have shown how it can be used to derive new decidability results for security protocols. The scheme relies on an extension of the notion of locality. Unfortunately it does not apply to homomorphism properties (handled in a specific way in [24]) because they are ill-moded by nature and more investigations are needed to see whether it can be extended in this direction.

References

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

[2] R. Amadio, D. Lugiez, V. Vanackère, On the symbolic reduction of processes with cryptographic functions, Theor. Comput. Sci. 290 (1) (2003) 695–740.

[3] F. Baader, K. U. Schulz, Unification in the union of disjoint equational theories. combining decision procedures., J. Symb. Comput. 21 (2) (1996) 211–243.

[4] D. Basin, S. Mödersheim, L. Viganò, An On-The-Fly Model-Checker for Security Protocol Analysis, in: E. Snekkenes, D. Gollmann (Eds.), Proceedings of ESORICS'03, LNCS 2808, Springer-Verlag, 2003, pp. 253–270.

[5] M. Boreale, Symbolic trace analysis of cryptographic protocols, in: Proceedings of the 28th ICALP'01, LNCS 2076, Springer-Verlag, Berlin, 2001, pp. 667–681.

[6] N. Borisov, I. Goldberg, D. Wagner, Intercepting mobile communications: the insecurity of 802.11, in: Proceedings of MOBICOM 2001, 2001, pp. 180–189.

[7] Y. Chevalier, M. Kourjieh, A symbolic intruder model for hash-collision attacks, in: M. Okada, I. Satoh (Eds.), Proceedings of the 11th Annual Asian Computing Science Conference (ASIAN'06), Vol. to appear of Lecture Notes in Computer Science, Springer-Verlag, 2006.

[8] Y. Chevalier, R. Kuesters, M. Rusinowitch, M. Turuani, An NP Decision Procedure for Protocol Insecurity with XOR, in: Proceedings of the Logic In Computer Science Conference, LICS'03, 2003, pp. 261–270.

[9] Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents, in: Proceedings of the Foundations of Software Technology and Theoretical Computer Science, FSTTCS'03, Lecture Notes in Computer Science, Springer, 2003, pp. 124–135.
URL `http://www.loria.fr/~chevalie/Research/expo-oracle.pdf`

[10] Y. Chevalier, M. Rusinowitch, Combining intruder theories., in: L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, M. Yung (Eds.), ICALP, Vol. 3580 of Lecture Notes in Computer Science, Springer, 2005, pp. 639–651.

[11] Y. Chevalier, M. Rusinowitch, Combining intruder theories, Research report 5495, INRIA, `http://www.inria.fr/rrrt/rr-5495.html`, long version of [10] (2005).

[12] Y. Chevalier, L. Vigneron, A Tool for Lazy Verification of Security Protocols, in: Proceedings of the Automated Software Engineering Conference (ASE'01), IEEE Computer Society Press, 2001, pp. 373–376.

[13] H. Comon-Lundh, S. Delaune, The finite variant property: How to get rid of some algebraic properties, in: Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05), Lecture Notes in Computer Science, Springer, Nara, Japan, 2005, pp. 294–307.

[14] H. Comon-Lundh, Intruder theories (ongoing work), in: I. Walukiewicz (Ed.), 7th International Conference, FOSSACS 2004, Vol. 2987 of Lecture Notes on Computer Science, Springer Verlag, Barcelona, Spain, 2004, pp. 1–4.

[15] H. Comon-Lundh, V. Shmatikov, Intruder Deductions, Constraint Solving and Insecurity Decision in Presence of Exclusive or, in: Proceedings of the Logic In Computer Science Conference, LICS'03, 2003, pp. 271–280.

[16] H. Comon-Lundh, R. Treinen, Easy intruder deductions., in: Verification: Theory and Practice, Vol. 2772 of Lecture Notes in Computer Science, 2003, pp. 225–242.

[17] R. Corin, S. Etalle, An improved constraint-based system for the verification of security protocols, in: SAS, LNCS, Springer-Verlag, 2002, pp. 326–341.

[18] S. Delaune, 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), ACM Press, Washington, D.C., USA, 2004, pp. 278–287.

[19] N. Dershowitz, J.-P. Jouannaud, Rewrite systems, in: Handbook of Theoretical Computer Science, Volume B, Elsevier, 1990, pp. 243–320.

[20] D. Dolev, A. Yao, On the Security of Public-Key Protocols, IEEE Transactions on Information Theory 2 (29).

[21] R. Givan, D. A. McAllester, New results on local inference relations., in: KR, 1992, pp. 403–412.

[22] J. Hsiang, M. Rusinowitch, On word problems in equational theories., in: ICALP, Vol. 267 of LNCS, Springer, 1987, pp. 54–71.

[23] R. Küsters, T. Wilke, Automata-based Analysis of Recursive Cryptographic Protocols, in: 21st Symposium on Theoretical Aspects of Computer Science (STACS 2004), Lecture Notes in Computer Science, Springer-Verlag, 2004, pp. 382–393.

[24] P. Lafourcade, D. Lugiez, 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), Lecture Notes in Computer Science, Springer, Nara, Japan, 2005, pp. 308–322.

[25] D. A. McAllester, Automatic recognition of tractability in inference relations., J. ACM 40 (2) (1993) 284–303.

[26] J. Millen, V. Shmatikov, Constraint solving for bounded-process cryptographic protocol analysis, in: ACM Conference on Computer and Communications Security, 2001, pp. 166–175.

[27] J. Millen, V. Shmatikov, Symbolic protocol analysis with an abelian group operator or Diffie-Hellman exponentiation, Journal of Computer Security 13(3) (2005) 515–564.

[28] D. Kapur, P. Narendran, L. Wang, An e-unification algorithm for analyzing protocols that use modular exponentiation., in: R. Nieuwenhuis (Ed.), RTA, Vol. 2706 of Lecture Notes in Computer Science, Springer, 2003, pp. 165–179.

[29] C. Meadows, The NRL protocol analyzer: an overview, Journal of Logic Programming 26 (2) (1996) 113–131.

[30] C. Meadows, P. Narendran, A unification algorithm for the group Diffie-Hellman protocol, in: Workshop on Issues in the Theory of Security (in conjunction with POPL'02), Portland, Oregon, USA, January 14-15, 2002.

[31] A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of applied cryptography, CRC Press, 2000.

[32] M. Rusinowitch, M. Turuani, Protocol insecurity with finite number of sessions is NP-complete, in: Proc.14th IEEE Computer Security Foundations Workshop, Cape Breton, Nova Scotia, 2001, pp. 174–190.

[33] V. Shmatikov, Decidable analysis of cryptographic protocols with products and modular exponentiation, in: Proceedings of ESOP'04, Vol. 2986 of Lecture Notes in Computer Science, Springer-Verlag, 2004, pp. 355–369,.

[34] M. Schmidt-Schauß, Unification in a combination of arbitrary disjoint equational theories, J. Symb. Comput. 8 (1/2) (1989) 51–99.

[35] T. Wu, The srp authentication and key exchange system, Tech. Rep. RFC 2945, IETF – Network Working Group, available at `http://www.ietf.org/rfc/rfc2945.txt` (september 2000).