Hierarchical Combination of Intruder Theories *

Yannick Chevalier , Michaël Rusinowitch

[1] IRIT Université Paul Sabatier, France
email: ychevali@irit.fr
[2] LORIA-INRIA-Lorraine, France
email: rusi@loria.fr

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 intruder theories and to show decidability results for the deduction problem in these theories. Under a simple hypothesis, we were able to simplify this deduction problem. This simplification is then applied to prove the decidability of constraint systems w.r.t. an intruder relying on exponentiation theory.

1 Introduction

Recently many procedures have been proposed to decide insecurity of cryptographic protocols in the Dolev-Yao model w.r.t. a finite number of protocol sessions [1, 4, 24, 22]. Among the different approaches the symbolic ones [22, 9, 3] are based on reducing the problem to constraint solving in a term algebra. While these approaches rely on a perfect encryption hypothesis, the design of some protocols (see *e.g.* [26]) rely on lower-level primitives such as exponentiation or bitwise exclusive or (xor). These specification may give rise to new attacks exploiting the underlying algebraic structure when it is not abstracted as perfect encryption. For attacks exploiting the bitwise xor equational properties in the context of mobile communications see for instance [5].

Hence several protocol decision procedures have been designed for handling equational properties [21, 11, 6, 18] of the cryptographic primitives. A very fruitful concept in this area is the notion of locality introduced by McAllester [19] which applies to several intruder theories [12, 18]. 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. Here we extend this approach to a case where the signature

* supported by ACI-SI SATIN, ACI-Jeune Chercheur JC9005

can be divided into two disjoint sets and where the term algebra can be divided into two types of terms, say 0 and 1 type, according to their root symbol. Then we give sufficient conditions so that we can restrict intruder deductions to deductions where all subterms of type 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 of terms of type 1 by the intruder, thus permitting subsequent analysis to focus deductions of terms of type 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 [23] with a theory of an exponential operator.

Related works. In [8] we have extended the combination algorithm for solving E-unification problems of [2] to solve intruder constraints on disjoint signatures. Here we show that we can handle some non-disjoint combinations. In [13] 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 [12, 10] have also investigated general conditions on theories for deciding insecurity with passive intruders.

As an application, we have obtained a decidable intruder theory combining Abelian group and exponential which has less restrictions than any previous one: unlike [7] 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 [25] where bases of exponentials have to be constants and exponential terms must not appear inside exponents.

Outline. In Section 2 we will first recall basic notions about terms, substitutions, term rewriting and define a new notion of *mode*. We then derive a notion of *subterm value* from the mode, and study properties of term replacement operations. We recall the definition of intruder systems in Section 3, and define the notion of *well-moded intruders*. We also prove the existence of special sequences of deductions called *quasi well-formed derivations*. Then we define constraint systems in Section 4. In Section 5 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 $\mathcal{C}$ of type 1, *i.e.* after instanciating $\mathcal{C}$ with a bound solution, the number of subterms of type 1 in the result is lesser or equal. We then give in Section 6 an application of these results to an interesting class of security protocols.

2 Terms, subterms and modes

2.1 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 $\textsc{ar}(f)$. 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 $\mathrm{Var}(t)$ the set of variables occurring in t and by $\mathrm{Cons}(t)$ the set of constants occurring in t. We denote by $\mathrm{Atoms}(t)$ the set $\mathrm{Var}(t) \cup \mathrm{Cons}(t)$. A substitution σ is an involutive mapping from $\mathcal{X}$ to $\mathrm{T}(\mathcal{G},\mathcal{X})$ such that $\mathrm{Supp}(\sigma) = \{x|\sigma(x) \neq x\}$, 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* w.r.t. $\mathcal{G}$ if the image of $\mathrm{Supp}(\sigma)$ is included in $\mathrm{T}(\mathcal{G})$.

An *equational presentation* $\mathcal{H} = (\mathcal{G}, A)$ is defined by a set A of equations $u = v$ with $u, v \in \mathrm{T}(\mathcal{G},\mathcal{X})$ 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 $\mathrm{T}(\mathcal{G},\mathcal{X})$, 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 $\mathrm{Sub}_{\mathrm{syn}}(t)$ and are defined recursively as follows. If t is a variable or a constant then $\mathrm{Sub}_{\mathrm{syn}}(t) = \{t\}$. If $t = f(t_1, \ldots, t_n)$ then $\mathrm{Sub}_{\mathrm{syn}}(t) = \{t\} \cup \bigcup_{i=1}^{n} \mathrm{Sub}_{\mathrm{syn}}(t_i)$. 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 $t(s_1, \ldots, s_m)$ a term that admits $s_1 \ldots s_m$ among its syntactic subterms. 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 $\textsc{top}(\cdot)$ 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 $\mathcal{X}_1$.

2.2 Congruences and ordered rewriting

In this subsection we shall introduce the notion of *ordered rewriting* [14] which has been useful (*e.g.* [2]) for proving the correctness of combination of unification

algorithms. Let $<$ be a simplification ordering on $\mathrm{T}(\mathcal{G})$ [1] 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.

Given a signature $\mathcal{G}$, we denote by $\mathrm{C}_{\mathrm{spe}_{\mathcal{G}}}$ the set containing the constants in $\mathcal{G}$ and $\mathrm{c}_{\min}$. For the the signature $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$ defined earlier, we abbreviate $\mathrm{C}_{\mathrm{spe}_{\mathcal{F}}}$ by $\mathrm{C}_{\mathrm{spe}}$. Given a possibly infinite set of equations $\mathcal{O}$ on the signature $\mathrm{T}(\mathcal{G})$ we define the ordered rewriting relation $\rightarrow_{\mathcal{O}}$ by $s \rightarrow_{\mathcal{O}} s'$ 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 $l\tau > r\tau$. It has been shown (see [16, 14]) 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 $\rightarrow_{\mathcal{O}}$ is convergent (*i.e.* terminating and confluent) on $\mathrm{T}(\mathcal{F})$.

From now on when we will 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 $\rightarrow_{\mathcal{O}}$. A ground term t is in *normal form*, or *normalized*, if $t = (t)\downarrow_{\mathcal{O}}$. 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 $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2$.

2.3 Modes

When one considers the union of two equational theories over two disjoint signatures, a standard processing is to decompose the terms according to the signature of their inner symbols into a set of equations whose members are pure terms (i.e. built with symbols from a single signature). The rational for this decomposition is that by construction, in the case of disjoint signatures, the rewrite system obtained by o-completion is the union of two independent rewrite systems, each one operating on pure terms. This decomposition cannot be applied *as is* in the case of non-disjoint signatures. We provide here a notion of *mode* that allows one (under some hypothesis) to decompose terms in *subterm values* such that that the left-hand sides of rules in the o-completion never overlap two terms in the decomposition of a term. This notion of *mode* is different from the standard notion of *type* that would define how terms can be built.

In the following we assume that there exists a *mode* function $\mathrm{M}(\cdot,\cdot)$ such that $\mathrm{M}(f,i)$ is defined for every symbol $f \in \mathcal{F}$ and every integer i such that $1 \leq i \leq \mathrm{AR}(f)$. For all f, i we have $\mathrm{M}(f,i) \in \{0,1\}$ and for all $f \in \mathcal{F}_0$ and for all i, $\mathrm{M}(f,i) = 0$.

For all $f \in \mathcal{F} \cup \mathcal{X}$ we define a function that gives the *class* $\mathrm{SIG}(f)$ of a symbol:

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

[1] by definition $<$ satisfies for all $s,t,u \in \mathrm{T}(\mathcal{G})$ $s \leq t[s]$ and $s < u$ implies $t[s] < t[u]$

The function SIG is extended to terms by taking $\text{SIG}(t) = \text{SIG}(\text{TOP}(t))$.

A position different from ϵ in a term t is *well-moded* if it can be written $p \cdot i$ (where p is a position and i a nonnegative integer) such that $\text{SIG}(t_{|p \cdot i}) = \text{M}(\text{TOP}(t_{|p}), i)$. In other words the position in a term is well-moded if the subterm at that position is of the expected type w.r.t. the function symbol immediately above it. A term is well-moded if all its non root positions are well-moded. If a non root position of t is not well-moded we say it is *ill-moded* in t. An equational presentation $\mathcal{H} = (\mathcal{G}, A)$ is well-moded if for all equations $u = v$ in A the terms u and v are well-moded and $\text{SIG}(u) = \text{SIG}(v)$. One can prove that if an equational theory is well-moded then its completion is also well-moded.

We call a *subterm value* of a term t a syntactic subterm of t that is either atomic or occurs at an ill-moded position of t[2]. We denote $\text{Sub}(t)$ the set of subterm values of t. By extension, for a set of terms E, the set $\text{Sub}(E)$ 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 $\text{Factors}(t)$.

Example 1. Consider two binary symbols f and g with $\text{SIG}(f) = \text{SIG}(g) = \text{M}(f, 1) = \text{M}(g, 1) = 1$ and $\text{M}(f, 2) = \text{M}(g, 2) = 0$, and $t = f(f(g(a, b), f(c, c)), d)$. 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.

2.4 Normalisation and replacement

Subterms and normalisation We now study the evolution of the subterms of a term t when t is being normalized. Assuming the theory is well-moded, we can prove that (ordered) rewriting by R preserves factors in normal form. Since R is convergent, this permits to prove the following lemma.

Lemma 1. *Let t be a term with all its factors in normal form. Then either* $(t)\downarrow \in \text{Factors}(t) \cup \text{C}_{\text{spe}}$ *or* $\text{SIG}((t)\downarrow) = \text{SIG}(t)$. *Moreover* $\text{Sub}((t)\downarrow) \subseteq (\text{Sub}(t))\downarrow \cup \text{C}_{\text{spe}}$.

Replacement and normalization We now give conditions under which the replacement of a normal subterm s of a term t commutes with the normalisation of t. First let us define replacement with respect to the subterm value relation on terms. If Π is a set of non-comparable 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 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 $\delta_{u,\text{c}_{\min}}$.

[2] Note that the root position of a term is *always* ill-moded.

We define the notion of *free terms* to express that a term s is not in a set of terms T once a substitution σ has been applied. A term s is *free* in 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 feel free to omit σ or T when they are clear from context. Since rewriting by R never overlaps subterm values, we can prove that normalization and subterm replacement commute.

Lemma 2. *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 $(t\delta_s)\downarrow = ((t)\downarrow\delta_s)\downarrow$.*

Example 2. Consider the equational theory $\mathcal{E} = \{f(g(x)) = x\}$. The only valid mode functions set either the mode of the argument of f and g to 0 or to 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 thus $t\delta_s = t$. This shows how the notion of mode permits to define replacements compatible with normalization.

Let s be a normalized ground term with $\mathrm{SIG}(s) = 1$ and σ be a ground normal substitution. Next lemma shows that under the provision that a normalized term s is free in $\mathrm{Sub}(t)$ 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 3. *Let t be a term, σ be a normalized substitution and s be a ground term in normal form with $\mathrm{SIG}(s) = 1$. Assume s is free in $\mathrm{Sub}(t)$ for σ and let $\sigma' = (\sigma\delta_s)\downarrow$. We have:*

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

Example 3. Consider now the equational theory $\mathcal{E} = \{f(x, x) = 0\}$, the term $t = f(f(x, x), f(x, \mathrm{c_{min}}))$ and $x\sigma = a$, and consider the replacement δ_a. Using the notations of Lemma 3, we have $\sigma' = \{x \mapsto \mathrm{c_{min}}\}$, and thus $t\sigma' = f(f(\mathrm{c_{min}}, \mathrm{c_{min}}), f(\mathrm{c_{min}}, \mathrm{c_{min}}))$, while on the other hand $(t\sigma)\downarrow\delta_a = f(0, f(\mathrm{c_{min}}, \mathrm{c_{min}}))$. This example shows even though s is in normal form, an extra normalization is needed after replacement. Replacing one of the occurrence of x by a also shows why we need s to be free in Lemma 3.

3 Intruder deduction systems

We first recall here the general definition of intruder systems, as is given in [8]. Then we define the *well-moded intruder* in which we are interested in this paper. In the context of a security protocol (see *e.g.* [20] for a brief overview), we model messages as ground terms and intruder deduction rules as rewrite rules on sets of messages representing the knowledge of an intruder. 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.

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 $\rightarrow_{\mathcal{I}}$. Note 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 $\mathcal{I}$.

Example 4. Let $\rightarrow_{\mathcal{I}_\times}$ be the relation between ground sets of terms defined by the Abelian group intruder $\mathcal{I}_\times = \langle \{\times, \mathrm{i}, 1\}, \{x \times y, \mathrm{i}(x), 1\}, \mathcal{E}_\times \rangle$. One has:

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

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.

A *derivation* D of length n, $n \geq 0$, is a sequence of steps of the form $E_0 \rightarrow_{\mathcal{I}} E_0, t_1 \rightarrow_{\mathcal{I}} \cdots \rightarrow_{\mathcal{I}} E_n$ 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 $i \in \{1, \ldots, n\}$. The term t_n is called the *goal* of the derivation. We define $\overline{E}^{\mathcal{I}}$ to be equal to the set $\{t \mid \exists F \text{ s.t. } E \rightarrow^*_{\mathcal{I}} F \text{ and } t \in F\}$ *i.e.* the set of terms that can be derived from E. If there is no ambiguity on the deduction system $\mathcal{I}$ we write $\overline{E}$ instead of $\overline{E}^{\mathcal{I}}$.

With this definition of deduction, one can easily prove that it suffices to consider deductions on sets of terms in normal form. We will thus only consider derivations on sets of terms in normal form. 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 2.1. Let $\mathcal{I}_1 = \langle \mathcal{F}, \mathcal{S}, \mathcal{E}_0 \cup \mathcal{E}_1 \rangle$ be an intruder system where terms in $\mathcal{S}$ are well-moded.

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 $E \rightarrow_{\mathcal{S}_0} F$ (resp. $E \rightarrow_{\mathcal{S}_1} F$, resp. $E \rightarrow_{\mathcal{S}} F$) if $E \rightarrow_{l \rightarrow r} F$ with $l \rightarrow r \in \mathrm{L}^{t,\mathrm{g}}$ 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 4 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 5 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 (w.r.t. $<$) in a solution to yield a smaller solution.

Lemma 4. *Assume E and F are in normal form. If $E \rightarrow_{\mathcal{S}} F$ and $t \in \mathrm{Sub}(F) \setminus (\mathrm{Sub}(E) \cup \mathrm{C_{spe}})$, then $F \setminus E = t$ and $E \rightarrow_{\mathrm{L}^u} F$, with $u \in \mathcal{S}$ and $\mathrm{SIG}(u) = \mathrm{SIG}(t)$.*

Proof. The hypotheses permit to apply Lemma 1. If the rule is applied with substitution τ this implies $\mathrm{Sub}((u\tau)\downarrow) \subseteq \{(u\tau)\downarrow\} \cup \mathrm{Sub}(E) \cup \mathrm{C_{spe}}$. Thus $t \notin \mathrm{Sub}(E) \cup \mathrm{C_{spe}}$ implies $t = (u\tau)\downarrow$ and $t \notin \mathrm{C_{spe}} \cup \mathrm{Factors}(u\tau)$. Thus by Lemma 1 $\mathrm{SIG}(t) = \mathrm{SIG}(u\tau) = \mathrm{SIG}(u)$. □

Lemma 5. *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 $E, s \rightarrow E, s, t$ implies $(E\delta_s)\downarrow, s \rightarrow ((E,t)\delta_s)\downarrow, s$.*

Locality hypothesis on intruder systems. The previous lemma will be used in conjunction with an extra hypothesis that is related to the locality property [15].

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

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. We can prove that for any set of terms $\mathcal{S}_1$ the set of terms $\langle \mathcal{S}_1 \rangle$ satisfies Hypothesis 1.

4 Constraint systems

We introduce now the constraint systems to be solved for checking protocols. It is shown in [8] how these constraint systems permit to express the reachability of a state in a protocol execution.

Definition 2. *(Unification systems) 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 couples of terms in $\mathrm{T}(\mathcal{G}, \mathcal{X})$ denoted by $\{u_i \stackrel{?}{=} v_i\}_{i \in \{1,\ldots,n\}}$. It is satisfied by a ground substitution σ, and we note $\sigma \models \mathcal{S}$, if for all $i \in \{1, \ldots, n\}$ we have $u_i\sigma =_{\mathcal{H}} v_i\sigma$.*

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 $\mathcal{S}$.*

*An $\mathcal{I}$-*Constraint system *$\mathcal{C}$ is satisfied by a ground substitution σ if for all $i \in \{1, \ldots, n\}$ we have $v_i\sigma \in \overline{E_i\sigma}$ and if $\sigma \models_{\mathcal{H}} \mathcal{S}$. If a ground substitution σ satisfies a constraint system $\mathcal{C}$ 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: after receiving a message a honest agent will respond to it. This response can be added to the knowledge of an intruder who listens to all communications.

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 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 $\mathrm{Var}(E_i) \subseteq \{v_1, \ldots, v_{i-1}\}$*

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 cycle when building a global solution. This motivates us to define the *Ordered Satisfiability* problem:

Ordered Satisfiability

Input:	an $\mathcal{I}$-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 $c \notin \mathrm{Sub}_{\mathrm{syn}}(x\sigma)$

5 Minimal solutions

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 $s \in \mathrm{Sub}(\mathrm{Var}(\mathcal{C})\sigma)$, if $\mathrm{SIG}(s) = 1$ then 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 5. *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 $u \in \mathrm{Sub}(E_0, t) \cup \mathrm{C_{spe}}$.*

Let $\mathcal{I}=\langle \mathcal{F}, \mathcal{S}, \mathcal{E} \rangle$ be a well-moded intruder that satisfies HYPOTHESIS 1 w.r.t. this mode function.

Lemma 6. *Assume $\mathrm{c_{min}} \in E$ and E is in normal form. If $t \in \overline{E}^{\mathcal{S}}$ there exists a quasi well-formed derivation starting from E of goal t.*

Lemma 7. *Let E and F be finite sets of normalized terms with $\mathrm{c_{min}} \in E$. Let s, t be two normalized terms not in $\mathrm{C_{spe}}$ with $s \in \overline{E} \setminus \mathrm{Sub}(E)$, $\mathrm{SIG}(s) = 1$ and $t \in \overline{E \cup F}$. We have:*

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

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

Proposition 1. *Let $\mathcal{C}$ be a satisfiable constraint system. There exists a normal bound substitution σ such that $\sigma \models \mathcal{C}$.*

If we denote $\mathrm{Sub}_1(T)$ the terms of signature 1 in $\mathrm{Sub}(T)$, this implies the equality: $\mathrm{Sub}_1((\mathrm{Sub}_1(\mathcal{C})\sigma)\downarrow) = (\mathrm{Sub}_1(\mathcal{C})\sigma)\downarrow$

6 Application to Security Protocols

We present now a decision procedure for the exponentiation operator which is used *e.g.* with Diffie-Hellman scheme for the collaborative construction of a secret key by two principals. We define the *union* of two intruder systems as the intruder system having the deduction rules of both intruder systems.

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. Note that the specification of the exponentiation operation is dependent on the specification of the multiplication, and thus Theorem 1 of [8] cannot be applied directly.

Note 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 [17] for a survey of several exponentiation theories and their unification problems. The axiomatization we consider here was to our knowledge first introduced in [21].

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

$$\begin{aligned}
x \cdot (y \cdot z) &= (x \cdot y) \cdot z && (A)\\
x \cdot y &= y \cdot x && (C)\\
x \cdot 1 &= x && (U)\\
x \cdot \mathrm{i}(x) &= 1 && (I)\\
\exp(x, 1) &= x && (E_0)\\
\exp(\exp(x, y), z) &= \exp(x, y \cdot z) && (E_1)
\end{aligned}$$

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

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

According to this definition of mode and signature we define $\mathcal{E}$ 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. We denote by R an o-completion of $\mathcal{E}$ with the same congruence classes as $\mathcal{E}$ and such that for each term $t = \exp(t_1, t_2)$, if t is in normal form for R then t_1 is not an exponential term (*i.e.* $\text{SIG}(t_1) \neq 1$) [3].

Let $T = \{x \cdot y, \text{i}(x), 1, \exp(x, y)\}$. We now consider the intruder system $\mathcal{I}_{\exp} = \langle \mathcal{F}, T, \mathcal{E} \rangle$ that represents the modular exponentiation operation as employed for Diffie-Hellman-like construction of secret keys. According to mode and signature functions, this permits to define two intruder systems by taking $\mathcal{S}_0 = \{x \cdot y, \text{i}(x), 1\}$ and $\mathcal{S}_1 = \{\exp(x, y)\}$. Let $\mathcal{I}_{\text{ag}}$ be the intruder $\langle \{\cdot, \text{i}, 1\}, \{x \cdot y, \text{i}(x), 1\}, \mathcal{E}_0 \rangle$. In the rest of this section we present and justify an algorithm that runs in NP time and permits to reduce ordered satisfiability for $\mathcal{I}_{\exp}$ deterministic constraint systems to ordered satsifiability for $\mathcal{I}_{\text{ag}}$ deterministic constraint systems. Before proceeding further, let us first prove that the intruder $\mathcal{I}_{\exp}$ satisfies HYPOTHESIS 1.

Lemma 8. *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 $r \notin \text{Sub}(E, t)$ 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 $r \notin \text{Sub}(t)$ and $E \not\rightarrow E, t$. Since $r \notin \text{Sub}(E)$ it is necessary an exponential by Lemma 4. Let τ be the substitution with which the second rule $x, y \rightarrow \exp(x, y)$ is applied. Since $E \not\rightarrow E, t$ one must have either $r = x\tau$ or $r = y\tau$.

First let us prove that w.l.o.g. one can assume $r \neq y\tau$. If $x\tau$ is not an exponential, then since E and r are in normal form, so is $\exp(x\tau, y\tau)$, and thus $r \in \text{Sub}(t)$, which contradicts the hypothesis. If $x\tau$ is an exponential, say $x\tau = \exp(x_1\tau, y_1\tau)$, then:

$$\exp(x\tau, r) =_{\mathcal{E}} t' = \exp(x_1\tau, y_1\tau \times r)$$

By convergence of R we have $(t')\downarrow = t$. Since either $x\tau \in E$ or $r = x\tau$, the assumption $r \notin \text{Sub}(E)$ implies that r is not a strict subterm of $x\tau$, and thus

[3] such a system R can be obtained by o-completion with a suitable ordering

$r \notin \mathrm{Sub}(x_1\tau, y_1\tau)$. Since the factors of t' are in normal form and $r \neq t$, we have $(t'\delta_r)\downarrow = (t\delta_r)\downarrow$, and thus $r \notin \mathrm{Sub}(t)$ implies $(t'\delta_r)\downarrow = t$. In turn, this implies that $x\tau, \mathrm{c}_{\min} \rightarrow t$ is ground instance of a rule in $\mathcal{S}_1$ that can be applied on E, r to deduce t.

The claim and $E \not\vdash t$ implies $x\tau = r$ and $y\tau \neq r$ and thus $y\tau \in E$. It suffices now to consider the ground instance $s_1, s_2 \rightarrow (\exp(s_1, s_2))\downarrow = r$ of the rule that permits to deduce r from E. Since $s_1, s_2 \in E$ we have the following derivation:

$$E \rightarrow_{\mathcal{S}_0} E, s_2 \times y\tau \rightarrow_{\mathcal{S}_1} E, s_2 \times y\tau, (\exp(s_1, s_2 \times y\tau))\downarrow$$

The equality E_2 implies that this last term is equal to t. □

As a consequence the exponential intruder enjoys quasi well-formed derivations and by Proposition 1, a satisfiable constraint system can be satisfied by a bound substitution. Thus we can bound the number of exponential subterms in quasi well-formed derivations. We can therefore design a correct, complete and terminating algorithm for solving the $\mathcal{I}_{\exp}$-constraints.

Properties of bound solutions 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 *indice* of t, and denote i_t, the minimum indice 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 indice 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. $\mathrm{Var}(m) \subseteq \{v_1, \ldots, v_{i_t}\}$

Lemma 9. *It is possible to compute a complete prefix of* $(t\sigma)\downarrow$ *for all past-bound terms* t *in* $\mathrm{Sub}(\mathcal{C})$.

Algorithm We present here a decision procedure for the exponential intruder $\mathcal{I}_{\exp}$ 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 $\mathcal{C}$.

Step 1: Choose m triples $(e_i, x_i, y_i)_{i \in \{1,\ldots,m\}}$ of new variables and m^2 variables $\{y_{i,j}\}_{i,j \in \{1,\ldots,m\}}$. Add to $\mathcal{S}$ equations $e_i \stackrel{?}{=} \exp(x_i, y_i)$ for $i \in \{1, \ldots, m\}$ and $y_i \cdot y_{i,j} \stackrel{?}{=} y_j$ for $i, j \in \{1, \ldots, m\}$. Let $\mathcal{S}_e$ be the obtained unification problem and X_e be the set of these new variables.

Step 2: Choose an equivalence $\equiv_\sigma$ relation among subterms of $\mathcal{C}$ and $\mathcal{S}_e$. Let $Q = \{q_1, \ldots, q_n\}$ be a set of new variables each denoting an equivalence class. Add to $\mathcal{S}_e$ 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. Choose a subterm relation on Q.

Step 3: Guess a subset of Q_d of Q, and let $L = Q \cup \{v_1, \ldots, v_n\}$ and let $L = \{l_1, \ldots, l_k\}$. Let $<$ be a total order on L such that $i < j$ implies $v_i < v_j$ 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 4: Replace each past-bound term in $\mathcal{C}$' with a complete prefix and past-free terms with the representative q of their equivalence class. Reduce with equation (E_1) to form the constraint system $\mathcal{C}''$.

Step 5: Guess which constraints $E \rhd v$ in $\mathcal{C}''$ must be solved by derivations ending with a rule in $\mathcal{S}_1$, and reduce them (if possible) to constraints to solve with $\mathcal{S}_0$

Step 6: Reduce $\mathcal{S}''$ to a system of general unification modulo $\mathcal{E}_0$ according to algorithm employed in [21], p. 7, proof of main theorem and purify the deduction constraints.

Step 7: Solve the resulting $\mathcal{I}_{\text{ag}}$ deterministic intruder system with the linear constant restriction $<_i$.

Comments on the algorithm. We assume in the following that the ordered satisfiability problem $(\mathcal{C}, <_i)$ is satisfied by a ground substitution σ_0.

Step 1: If $\mathcal{C}$ is satisfiable, it is satisfied by a bound substitution for which there are less than m different exponential terms. The $y_{i,j}$ will denote the exponents that we have to build so that $\exp(e_i, y_{i,j}) = e_j$.

Step 2: The subterm relation and the equivalence classes are needed to compute past-free and past-bound terms.

Step 3: The construction amounts to concatenating all derivations from $(E_i\sigma)\downarrow$ of goal $v_i\sigma$ into one derivation that has to deduce the terms $v_i\sigma$ at some point and in which in some steps the set of term is arbitrarily extended (case $l_i = v_j$). From this pseudo-derivation we extract in turn all applications of the $\mathcal{S}_1$ rule and all applications of the $\mathcal{S}_0$ rule that yield a past-free term. The first one permits a complete reduction at next step of the algorithm, while the second one permits to ensure that the resulting constraint system is determinitic once past-free terms are replaced by variables. The rational for this is that by definition the normal form q of a past-free term will be deduced (*i.e.* appear in a constraint $F \rhd q$) before a term in this equivalence class (that will be replaced by the variable q) appears in any knowledge set.

Step 4: Note here that if a $\mathcal{S}_1$ rule permits to deduce a non-exponential term q, this term is past-bound. Thus the replacement made at previous step permits to ensure that q will never appear again in the deduction part of the constraint system, and thus that erasing this constraint during the reduction will not turn the constraint system into a non-deterministic one. If a $\mathcal{S}_1$ rule permits to deduce an exponential term, it will be seen as a constant when solving the resulting constraint system w.r.t. the $\mathcal{I}_{\text{ag}}$ intruder. It is thus safe to erase the constraint in this case.

Step 5: In [21] unification systems with constants modulo $\mathcal{E}$ are reduced to general unification systems modulo $\mathcal{E}_0$ containing the exp as a free binary symbol. We go one step further and turn this unification system into a unification system with linear constant restrictions but without non-constant free symbols in order to syntactically eliminate the exp symbol. The deduction constraints are purified by replacing all equivalence classes of *exponential* terms by a representative *constant*.

As a consequence of this algorithm we have a decidability result for ordered satisfiability w.r.t. exponential intruder.

Proposition 2. *The ordered satisfiability problem for deterministic constraints and intruder $\mathcal{I}_{\text{exp}}$ is decidable (with complexity NP).*

7 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 [18]) because they are ill-moded by nature and more investigations are needed to see whether it can be extended in this direction.

References

1. R. Amadio, D. Lugiez, and V. Vanackère. On the symbolic reduction of processes with cryptographic functions. *Theor. Comput. Sci.*, 290(1):695–740, 2003.
2. F. Baader and K. U. Schulz. Unification in the union of disjoint equational theories. combining decision procedures. *J. Symb. Comput.*, 21(2):211–243, 1996.
3. D. Basin, S. Mödersheim, and L. Viganò. An On-The-Fly Model-Checker for Security Protocol Analysis. In Einar Snekkenes and Dieter Gollmann, editors, *Proceedings of ESORICS'03*, LNCS 2808, pages 253–270. Springer-Verlag, 2003.
4. M. Boreale. Symbolic trace analysis of cryptographic protocols. In *Proceedings of the 28th ICALP'01*, LNCS 2076, pages 667–681. Springer-Verlag, Berlin, 2001.
5. N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. In *Proceedings of MOBICOM 2001*, pages 180–189, 2001.
6. Y. Chevalier, R. Kuesters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. In *Proceedings of the Logic In Computer Science Conference, LICS'03*, June 2003.
7. Y. Chevalier, R. Küsters, M. Rusinowitch, and 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, December 2003.
8. Y. Chevalier and M. Rusinowitch. Combining intruder theories. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *ICALP*, volume 3580 of *Lecture Notes in Computer Science*, pages 639–651. Springer, 2005.

9. Y. Chevalier and 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.
10. H. Comon-Lundh. Intruder theories (ongoing work). In Igor Walukiewicz, editor, *7th International Conference, FOSSACS 2004*, volume 2987 of *Lecture Notes on Computer Science*, pages 1–4, Barcelona, Spain, March 2004. Springer Verlag.
11. H. Comon-Lundh and 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*, pages 271–280, 2003.
12. H. Comon-Lundh and R. Treinen. Easy intruder deductions. In *Verification: Theory and Practice*, volume 2772 of *Lecture Notes in Computer Science*, pages 225–242, 2003.
13. S. Delaune and F. Jacquemard. A decision procedure for the verification of security protocols with explicit destructors. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 278–287, Washington, D.C., USA, October 2004. ACM Press.
14. N. Dershowitz and J-P. Jouannaud. Rewrite systems. In *Handbook of Theoretical Computer Science, Volume B*, pages 243–320. Elsevier, 1990.
15. R. Givan and D. A. McAllester. New results on local inference relations. In *KR*, pages 403–412, 1992.
16. J. Hsiang and M. Rusinowitch. On word problems in equational theories. In *ICALP*, volume 267 of *LNCS*, pages 54–71. Springer, 1987.
17. D. Kapur, P. Narendran, and L. Wang. An e-unification algorithm for analyzing protocols that use modular exponentiation. In Robert Nieuwenhuis, editor, *RTA*, volume 2706 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 2003.
18. P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for ac-like equational theories with homomorphisms. In *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, Lecture Notes in Computer Science, Nara, Japan, April 2005. Springer. To appear.
19. David A. McAllester. Automatic recognition of tractability in inference relations. *J. ACM*, 40(2):284–303, 1993.
20. C. Meadows. The NRL protocol analyzer: an overview. *Journal of Logic Programming*, 26(2):113–131, 1996.
21. C. Meadows and 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.
22. J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *ACM Conference on Computer and Communications Security*, pages 166–175, 2001.
23. J. Millen and V. Shmatikov. Symbolic protocol analysis with an abelian group operator or Diffie-Hellman exponentiation. *Journal of Computer Security*, 2005.
24. M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *Proc.14th IEEE Computer Security Foundations Workshop*, Cape Breton, Nova Scotia, June 2001.
25. V. Shmatikov. Decidable analysis of cryptographic protocols with products and modular exponentiation. In *Proceedings of ESOP'04*, volume 2986 of *Lecture Notes in Computer Science*, pages 355–369,. Springer-Verlag, 2004.
26. T. Wu. The srp authentication and key exchange system. Technical Report RFC 2945, IETF – Network Working Group, september 2000. available at http://www.ietf.org/rfc/rfc2945.txt.